6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

Customer Release Notes

VSP Operating System Software

Software Release 9.4.1.0

July 2026

INTRODUCTION:

This document describes important information about this release for platforms that support the VSP Operating System Software.

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 VOSS 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:

Third Party Virtual Machine (TPVM) has a new version, the image file is included for platform supporting VM, see File Names for this Release section.

IMPORTANT NOTES BEFORE UPGRADING TO THIS RELEASE:

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

UPGRADE CONSIDERATIONS WHEN UPGRADING TO 9.4.1.0 FROM PREVIOUS RELEASES:

Please see “VOSS 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 VOSS 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.

PLATFORMS SUPPORTED:

Please see “VOSS 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:

Virtual Services Platform 4900 Series

File Name	Module or File Type	File Size (bytes)
dictionary.fabricengine	RADIUS dictionary	3502
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	3747785216
VOSS4900.9.4.1.0_edoc.tar	Logs Reference	40079360
VOSS4900.9.4.1.0.md5	MD5 Checksums	670
VOSS4900.9.4.1.0_mib_sup.txt	MIB - supported object names	1586270
VOSS4900.9.4.1.0_mib.txt	MIB - objects in the OID compile order	8731915
VOSS4900.9.4.1.0_mib.zip	Archive of all MIB files	1294010
VOSS4900.9.4.1.0_oss-notice.html	Open-source software - Master copyright file	2597473
VOSS4900.9.4.1.0.sha512	SHA512 Checksums	1877
VOSS4900.9.4.1.0.tgz	Release 9.4.1.0 archived software distribution	327431921
VOSSv9.4.0_HELP_EDM_gzip.zip	EDM Help file	5281220

Virtual Services Platform 7400 Series

File Name	Module or File Type	File Size (bytes)
dictionary.fabricengine	RADIUS dictionary	3502
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
VOSS7400.9.4.1.0_edoc.tar	Logs Reference	40079360
VOSS7400.9.4.1.0.md5	MD5 Checksums	670
VOSS7400.9.4.1.0_mib_sup.txt	MIB - supported object names	1588532
VOSS7400.9.4.1.0_mib.txt	MIB - objects in the OID compile order	8731915
VOSS7400.9.4.1.0_mib.zip	Archive of all MIB files	1294010
VOSS7400.9.4.1.0_oss-notice.html	Open-source software - Master copyright file	2597473
VOSS7400.9.4.1.0.sha512	SHA512 Checksums	1877

File Name	Module or File Type	File Size (bytes)
VOSS7400.9.4.1.0.tgz	Release 9.4.1.0 archived software distribution	328567601
VOSSv9.4.0_HELP_EDM_gzip.zip	EDM Help file	5281220

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 VOSS4900.9.4.1.0.tgz
software activate 9.4.1.0.GA
```

or

```
software add VOSS7400.9.4.1.0.tgz
software activate 9.4.1.0.GA
```

CHANGES IN THIS RELEASE:

New Features in This Release
None

Old Features Removed From This Release
None

Problems Resolved in This Release	
CFD-15157	IPv6 traffic traversing the fabric fails for some destinations while other destinations remain reachable, causing inconsistent connectivity.
CFD-15518	Ports do not learn the source MAC address from PROFINET traffic sent by Siemens PLC devices, which breaks forwarding for that endpoint.
CFD-15540	The routed management VLAN is not handled correctly on 7400 clusters when associated with an MSTP instance other than 0.
CFD-16361	A memory leak may occur when processing NodeAlias IPv4 protocol info entries.
CFD-16680	CLI command "*show ip bgp advertised-routes*" reports a total route count of -1 even when advertised routes are present.
CFD-16720	On PoE capable switches, the PD detection type configuration change is not persistent after saving the configuration and rebooting.
CFD-17039	Deleting and recreating a VRF tied to anycast gateway VLANs causes an error when re-enabling anycast on the VLAN, as the switch incorrectly reports that the anycast interface already exists.

Problems Resolved in This Release	
CFD-17147	An ACL entry with a /32 destination IP mask matches all IP addresses instead of a single host address.
CFD-17155	CLI command "*certificate generate-csr relaxed*" fails in 9.x releases, preventing CSR generation with the relaxed option.
CFD-17189	Command execution fails for existing CLI sessions when the SSH session-limit is configured for 7 or 8 and exceeded, with TACACS authorization enabled.
VOSS-35043	Only the first channel of a channelized auto-sense port inherits the auto-sense and link administrative states; the remaining channels keep default pre-auto-sense settings.
VOSS-35101	**Enhancement** The following FA Client Element Types were added for the Fabric Attach Server: 19 — Building security/access 20 — PDU/battery backup 21 — PoE lighting 22 — Nutanix server solution 23 — Placeholder 1 24 — Placeholder 2 63 — FA Client Unknown ➢ The switch recognizes all newly added types when receiving FA packets. ➢ The types are also provided via RADIUS access request. ➢ The types can be displayed with *"show fa elements"* CLI command.
VOSS-35192	The DHCP server sends Option 43 with zero length even when no vendor option data is configured, which can cause clients to reject offers.
VOSS-35239	**Enhancement** "*show license output*" CLI command was enhanced with "Subscription License Refresh Date: <YYYY-MM-DD hh:mm:ss>" to let the user know when the subscription license was refreshed by the cloud in case of an EP1 license. An output is displayed "License check failed, license assignment will expire in X days" when the switch fails to synchronize with the cloud and gives information of when the license will expire, unless the switch manages to synchronize with the cloud in the meantime.
CFD-17219	When NEAP authentication is rejected by RADIUS and the NEAP quiet timer is running, a subsequent successful EAP authentication on the same port is terminated when the quiet timer expires, causing an unexpected session teardown.
CFD-17294	When BGP is configured with 4-byte AS numbers, the MED attribute is not applied correctly during route selection, resulting in different route preference behavior compared to 2-byte AS configuration.
CFD-17302	When a BGP route with the shortest AS path is withdrawn by the originating router, iBGP peers do not properly propagate the update, leaving a stale route instead of switching to the available longer AS-path route received via eBGP.

Fixes from Previous Releases
VOSS 9.4.1.0 incorporates all fixes and content from previous releases including VOSS 8.10.9.0, VOSS 9.0.5.1, VOSS 9.1.3.0, VOSS 9.2.3.0, VOSS 9.3.3.0 and VOSS 9.4.0.0.

OUTSTANDING ISSUES:

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

CFD-13433	RESTCONF TACACS+ authentication fails intermittently after extended uptime, requiring the RESTCONF application to be restarted.
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-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. A fix for this issue is targeted for 9.4.2.0 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
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.
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	After upgrading from 8.8.1.0 to any higher release, 25 GbE fiber links with autonegotiation disabled on the VIM5-4YE module fail to come up if FEC is set to "auto". **Workaround:** disable FEC or manually set it to Clause 108.

KNOWN LIMITATIONS:

Please see "VOSS 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.