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

Customer Release Notes

VSP Operating System Software

Software Release 9.3.3.0

June 2026

INTRODUCTION:

This document provides specific information for version 9.3.3.0 of agent software for 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:

None

IMPORTANT NOTES BEFORE UPGRADING TO THIS RELEASE:

Please see “VOSS Release Notes for version 9.3.0.0” available at
https://www.extremenetworks.com/support/release-notes

UPGRADE CONSIDERATIONS WHEN UPGRADING TO 9.3.3.0 FROM PREVIOUS RELEASES:

Please see “VOSS Release Notes for version 9.3.0.0” 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 backwards 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-enable it after both OSPF peers are upgraded to 9.3.3.

PLATFORMS SUPPORTED:

Please see “VOSS Release Notes for version 9.3.0.0” 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)
FabricIPSecGW_VM_5.2.0.0.ova	Fabric Ipsec Gateway Virtual Machine	4034211840
restconf_yang.tgz	YANG Model	506020
TPVM_Ubuntu20.04_04_14Apr2022.qcow2	Third Party Virtual Machine	4641982464
VOSS4900.9.3.3.0_edoc.tar	Logs Reference	39976960
VOSS4900.9.3.3.0.md5	MD5 Checksums	611
VOSS4900.9.3.3.0_mib_sup.txt	MIB - supported object names	1579893
VOSS4900.9.3.3.0_mib.txt	MIB - objects in the OID compile order	8700279
VOSS4900.9.3.3.0_mib.zip	Archive of all MIB files	1289344
VOSS4900.9.3.3.0_oss-notice.html	Open-source software - Master copyright file	2596248
VOSS4900.9.3.3.0.sha512	SHA512 Checksums	1722
VOSS4900.9.3.3.0.tgz	Release 9.3.3.0 archived software distribution	325537699
VOSSv9.3.0_HELP_EDM_gzip.zip	EDM Help file	5119759

Virtual Services Platform 7400 Series

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_Ubuntu20.04_04_14Apr2022.qcow2	Third Party Virtual Machine (TPVM)	4641982464
VOSS7400.9.3.3.0_edoc.tar	Logs Reference	39976960
VOSS7400.9.3.3.0.md5	MD5 Checksums	611
VOSS7400.9.3.3.0_mib_sup.txt	MIB - supported object names	1581925
VOSS7400.9.3.3.0_mib.txt	MIB - objects in the OID compile order	8700279
VOSS7400.9.3.3.0_mib.zip	Archive of all MIB files	1289344
VOSS7400.9.3.3.0_oss-notice.html	Open-source software - Master copyright file	2596248
VOSS7400.9.3.3.0.sha512	SHA512 Checksums	1722
VOSS7400.9.3.3.0.tgz	Release 9.3.3.0 archived software distribution	325188788
VOSSv9.3.0_HELP_EDM_gzip.zip	EDM Help file	5119759

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 VOSS4900.9.3.3.0.tgz
software activate 9.3.3.0.GA
```

or

```
software add VOSS7400.9.3.3.0.tgz
software activate 9.3.3.0.GA
```

CHANGES IN THIS RELEASE:

New Features in This Release
None

Old Features Removed From This Release
None

Problems Resolved in This Release	
CFD-16205	A memory leak related to LLDP may cause memory utilization to reach critical levels (95%), triggering an unexpected reboot of the switch.
CFD-16262	The switch may not respond to pings to the ISIS source IP address when SPBM BVLANs are configured as 4031 and 4032.
CFD-16301	DVR Core switches do not transmit sFlow and application telemetry packets to the XIQ-SE analytics engine collector when static route redistribution is enabled for DVR.
CFD-16350	EAP incorrectly allows the mvni RADIUS attribute on VLANs with an IP address when *ip spb-multicast enable* is also present, even though CLI blocks this combination. This causes static settings (ip spb-multicast enable, upnp-filter) to be removed when the last user leaves.
CFD-16555	The switch may not be accessible on the management VLAN despite remaining accessible via SSH and SNMP.
CFD-16569	SSH connections using ISIS system-ID fail with a timeout when the RADIUS server is unreachable and the RADIUS server timeout is set to 2 seconds or more.
CFD-16579	A long list of RADIUS Vendor-Specific Attributes (VSAs) may cause the switch to reboot unexpectedly.
CFD-16599	The *show khi performance memory* command displays an invalid block count for SMLT socket buffer memory.
CFD-16608	Stale DVR host entries remain in the I/O table on DVR controllers after a DVR-enabled VLAN is removed.

Problems Resolved in This Release	
CFD-16619	VRF names of 16 characters configured via CLI exceed the SNMP MIB limit of 15 characters, causing SNMP errors and XIQ-SE configuration enforcement failures on Fabric Extend logical interfaces.
CFD-16642	*show khi resource-scaling* reports incorrect resource utilization for a Transparent UNI (T-UNI) in a vIST cluster.
CFD-16648	When EAP-TEAP authentication is used with identity privacy enabled, the *show eapol session-stats interface* command displays user as “anonymous” instead of the actual RADIUS-authenticated username.
CFD-16661	When RADIUS is configured for web authentication, the switch does not generate SNMP authentication traps or syslog messages for failed web login attempts.
VOSS-34910, CFD-16518	DHCP snooping bindings are lost when the RADIUS server becomes unreachable and are not re-populated after the RADIUS server becomes reachable again.
VOSS-34911, CFD-16483	MHSA (Multi-Host Single Authentication) does not correctly override all previous authentication states and VLAN assignments on the port when a new authentication occurs.
CFD-16683	The ZTP+ process fails on VSP 7400 with an error, unpicklingError exception, preventing zero-touch provisioning from completing even after repeated factory-default reboots.
CFD-16694	Setting the “tftp boot-file-name” with a specific character when configuring the DHCP server options causes undesired results for the DHCP server.
CFD-16732	In a vIST area border node pair, ARP entries are learned with mismatched primary/secondary BVLANs between the hardware table and control plane, causing packets destined for remote areas to be dropped.
CFD-16810	The EAP subsystem incorrectly reports "Maximum allowed MAC reached" and drops new MAC addresses on EAP-enabled ports, preventing devices such as printers from connecting to the network.
CFD-16840, CFD-16911	When TACACS authorization is enabled, a file descriptor leak may cause a switch reset.
CFD-16863	The 'run spbm' configuration script incorrectly uses the peer system-ID as the SMLT virtual BMAC when the default system-ID and system-ID+1 are used as the local and peer identifiers.
CFD-16873	The *'show run module port'* command displays duplicate port interface headers when DHCP snooping and ARP inspection are configured.
CFD-16938	Under scaled conditions, the *show fulltech* command may result in a switch reboot.
CFD-16967	An unexpected reboot of the switch may originate in the port_state_fsm_task thread.
CFD-17003	DHCPv6 address assignment fails for 3rd-party clients when VRRP version 3 is configured on the routing interface.
CFD-17026	EAP authentication intermittently fails because the RADIUS State attribute is missing from Access-Request packets.
CFD-17044	When selecting a source MAC/IP for silent device wake-up ARPs/PINGs, the auto-sense survive reboot engine incorrectly retrieves the wrong MAC address in the case where the Anycast GW remote Router IP&MAC should be used.
VOSS-35194	OSPF HMAC-SHA-256 and HMAC-SHA-1 authentication fails to establish adjacency with third-party routers due to an interoperability issue in the authentication key handling.

Fixes from Previous Releases
VOSS 9.3.3.0 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 and VOSS 9.3.2.0.

OUTSTANDING ISSUES:

Please see “VOSS Release Notes for version 9.3.0.0” 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-13639	In an MA environment, prefixes might be installed wrongly on OSPF ASBR routing table. A fix for this issue is available starting with 9.4.0.0 release.
CFD-14993	Silent devices that send only a few GARP packets within the first seconds after link-up fail to authenticate via NEAP on auto-sense ports. **Workaround**: Use manual EAP configuration with auto-sense disabled or configure auto-sense data i-sid at port level. A fix for this issue is available starting with VOSS 9.4.0.0 release.
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-15424	A loop may occur for few seconds between the moment the SMLTs and auto-sense NNIs are brought UP and the moment the vIST comes UP. **Workaround**: have the VIST NNI converted to static. A fix for this issue is available starting with 9.4.0.0 release
CFD-15920	After changing the L3VSN i-sid on a VRF, routes in the VRF are installed in the dataplane with an egress object pointing to the old i-sid, causing loss of reachability until the switch is rebooted. A fix for this issue is available starting with VOSS 9.4.0.0 release.
CFD-16361	A memory leak may occur when processing NodeAlias IPv4 protocol info entries. **Workaround**: Globally disable node-alias or Disable node-alias on ports without auto-sense enabled. A fix for this issue is targeted to VOSS 9.4.1.0 release.
CFD-16720	On PoE capable switches, the PD detection type configuration change (from 802.3at_and_legacy to 802.3at-only) is not persistent after saving the configuration and rebooting **Workaround**: Re-apply the PD detection type configuration after each reboot. A fix for this issue is targeted to VOSS 9.4.1.0 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.
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-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. **Workaround**: Configure the maximum number of SSH session to 6 or lower (default is 4). A fix for this issue is targeted to VOSS 9.4.1.0 release.
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. A fix for this issue is targeted to VOSS 9.4.1.0 release.
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
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. A fix for this issue is targeted to VOSS 9.4.1.0 release.

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. A fix for this issue is targeted to VOSS 9.4.1.0 release.

KNOWN LIMITATIONS:

Please see “VOSS Release Notes for version 9.3.0.0” 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