

Customer Release Notes

VSP Operating System Software

Software Release 9.1.3.0

September 2025

INTRODUCTION:

This document provides specific information for version 9.1.3.0 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 9.1.0.0" available at
<https://www.extremenetworks.com/support/release-notes>

UPGRADE CONSIDERATIONS WHEN UPGRADING TO 9.1.3.0 FROM PREVIOUS RELEASES:

Please see "VOSS Release Notes for version 9.1.0.0" available at
<https://www.extremenetworks.com/support/release-notes>

PLATFORMS SUPPORTED:

Please see "VOSS Release Notes for version 9.1.0.0" 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
VOSS4900.9.1.3.0_edoc.tar	Logs Reference	63242240
VOSS4900.9.1.3.0.md5	MD5 Checksums	611
VOSS4900.9.1.3.0_mib_sup.txt	MIB - supported object names	1562513
VOSS4900.9.1.3.0_mib.txt	MIB - objects in the OID compile order	8375015
VOSS4900.9.1.3.0_mib.zip	Archive of all MIB files	1247574
VOSS4900.9.1.3.0_oss-notice.html	Open-source software - Master copyright file	2889456
VOSS4900.9.1.3.0.sha512	SHA512 Checksums	1722
VOSS4900.9.1.3.0.tgz	Release 9.1.3.0 archived software distribution	328431263
VOSSv9.1.0_HELP_EDM_gzip.zip	EDM Help file	5569440

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
VOSS7400.9.1.3.0_edoc.tar	Logs Reference	63242240
VOSS7400.9.1.3.0.md5	MD5 Checksums	611
VOSS7400.9.1.3.0_mib_sup.txt	MIB - supported object names	1563972
VOSS7400.9.1.3.0_mib.txt	MIB - objects in the OID compile order	8375015
VOSS7400.9.1.3.0_mib.zip	Archive of all MIB files	1247574
VOSS7400.9.1.3.0_oss-notice.html	Open-source software - Master copyright file	2889456
VOSS7400.9.1.3.0.sha512	SHA512 Checksums	1722
VOSS7400.9.1.3.0.tgz	Release 9.1.3.0 archived software distribution	327988865
VOSSv9.1.0_HELP_EDM_gzip.zip	EDM Help file	5569440

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 VOSS4900.9.1.3.0.tgz
software activate 9.1.3.0.GA
```

or

```
software add VOSS7400.9.1.3.0.tgz
software activate 9.1.3.0.GA
```

CHANGES IN THIS RELEASE:

New Features in This Release

None

Old Features Removed From This Release

None

Problems Resolved in This Release

CFD-12921	ARP Spoofing: In the log the system detected duplicate IP and MAC correctly, but without blocking the MAC
CFD-12987	Unicast flooded packets hitting both vIST nodes due to the gateway MAC address missing are being dropped downstream by both vIST nodes and not routed out to devices on SMLT
CFD-13404	Intermittent authentication failures when TACACS+ Single connection mode is used on switch and multiple connection mode on TACACS Server
CFD-13498	Cluster member advertises wrong Virtual BMAC after receiving configuration from XIQ-SE workflow
CFD-13575	VSP4900/7400: FabricIPSecGW_VM_5.2.0.0.ova stopped working after upgrade from 9.0.4 to 9.1.0
CFD-13656	Frequent VRRP v3 transitions on multiple VLANs
CFD-13782	Previously working NNI link doesn't come up after a switch reboot and stays in NNI-AUTH-FAIL auto-sense state on one end and NNI-ONBOARDING on the other switch
CFD-13876	Flex-UNI and ISIS configuration is allowed on same port if Flex-UNI command was issued prior to ISIS command
CFD-14170	"TPVM_Ubuntu20.04_04_14Apr2022.qcow2" file-checksum results mismatch with the Extreme portal
CFD-14236	The output of commands "show isis spbm unicast-fib" and "show isis spbm unicast-fib summary" are the same
CFD-14261	An unexpected reboot with core file may be encountered when 'show ip dhcp-server leases' command is executed concurrently from 2 CLI sessions
CFD-14292	Can configure a secondary VRRP IP using the same subnet via the web interface and not CLI
CFD-14326	In EDM, DHCP Snoop Bindings shows only the HEX value of the IP addresses, under the address column, instead of the standard IP address format within Enterprise Device Manager
CFD-14369	With a particular configuration for Extreme-Dynamic-ACL VSAs, a switch may reboot due to a memory leak
CFD-14395	Looped AUTO-SENSE ports show as NNI in 'show int gig auto-sense' instead of LOOP
CFD-14456	"default logging level" does not apply the specified value in the command

Problems Resolved in This Release	
CFD-14524, CFD-14783	If a management VLAN with VLAN ID 4047 is manually configured (instead of using the SDWAN auto-created one) then the interface might not respond to ICMP/ARP requests
CFD-14540, CFD-15095	EDM: RemoteAddr and UpdateSourceInterface are not displayed correctly in BGP peer tab
VOSS-33759	High CPU utilization may be encountered on the edge node in a vIST configuration due to core IPV6 routed traffic(L2VSN) using the nodal BMAC as source BMAC, which causes a continuous mac migration while IPv4 routed traffic is also received by that node
CFD-14848	iBGP peers are not updating properly when attempting to use AS_PATH prepending to change the route, which is causing routing issues
CFD-14949	A switch may unexpectedly reboot with core file after BGP peer bounce

Fixes from Previous Releases
VOSS 9.1.3.0 incorporates all fixes and content from previous releases including VOSS 8.10.8.0, VOSS 9.0.5.1 and VOSS 9.1.2.0

OUTSTANDING ISSUES:

CFD-11778	A loop may occur for few seconds before LACP SMLT comes up A fix for this issue is available starting with 9.3.0.0 release
CFD-13260	L3 connectivity lost to all devices over the Fabric Extend link when ISIS remote is enabled, but there is no ISIS remote interface Workaround: disable ISIS remote A fix for this issue is available starting with 9.3.0.0 release
CFD-13322	IPv6 FHS DHCP-Snooping does not work in Fabric mode A fix for this issue is available starting with 9.3.0.0 release
CFD-13329	ARP Inspection: Intermittent connectivity issues when ARP Inspection is enabled on a Fabric node A fix for this issue is available starting with 9.3.0.0 release
CFD-13455	In a vIST configuration, a short outage may occur after a DVR leaf reboots
CFD-13639	In a MA environment, prefixes might be installed wrongly on OSPF ASBR routing table
CFD-13833	Endpoint-tracking enabled on MLT causes MLT to flap
CFD-14159	EAP packets hitting CPU even when ingress on NNI
CFD-14867	Many indiscards packets are observed on the management interface

Please see "VOSS Release Notes for version 9.1.0.0" available at <https://www.extremenetworks.com/support/release-notes> for details regarding Known Issues.

KNOWN LIMITATIONS:

Please see "VOSS Release Notes for version 9.1.0.0" 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 © 2025 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