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

Customer Release Notes

VSP Operating System Software

Software Release 9.3.1.0
December 2025

INTRODUCTION:

This document provides specific information for version 9.3.1.0 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:

Operational Enhancements
"*show license*" command improvement (VOSS-34131)
Radius VSA for IGMP Version and Fast-Leave (VOSS-33733)
Radius VSA for IGMP Querier Address (VOSS-33944)
SSH to system-ID - ability to delete "known_hosts" file (VOSS- 33999)

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 9.3.1.0 FROM PREVIOUS RELEASES:

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

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
VOSS4900.9.3.1.0_edoc.tar	Logs Reference	39956480
VOSS4900.9.3.1.0.md5	MD5 Checksums	611
VOSS4900.9.3.1.0_mib_sup.txt	MIB - supported object names	1579893
VOSS4900.9.3.1.0_mib.txt	MIB - objects in the OID compile order	8700279
VOSS4900.9.3.1.0_mib.zip	Archive of all MIB files	1289346
VOSS4900.9.3.1.0_oss-notice.html	Open-source software - Master copyright file	2889462
VOSS4900.9.3.1.0.sha512	SHA512 Checksums	1722
VOSS4900.9.3.1.0.tgz	Release 9.3.1.0 archived software distribution	325608315
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
VOSS7400.9.3.1.0_edoc.tar	Logs Reference	39956480
VOSS7400.9.3.1.0.md5	MD5 Checksums	611
VOSS7400.9.3.1.0_mib_sup.txt	MIB - supported object names	1581925
VOSS7400.9.3.1.0_mib.txt	MIB - objects in the OID compile order	8700279
VOSS7400.9.3.1.0_mib.zip	Archive of all MIB files	1289346
VOSS7400.9.3.1.0_oss-notice.html	Open-source software - Master copyright file	2889462
VOSS7400.9.3.1.0.sha512	SHA512 Checksums	1722
VOSS7400.9.3.1.0.tgz	Release 9.3.1.0 archived software distribution	325254404
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 VOSS4900.9.3.1.0.tgz
software activate 9.3.1.0.GA
```

or

```
software add VOSS7400.9.3.1.0.tgz
software activate 9.3.1.0.GA
```

CHANGES IN THIS RELEASE:

New Features in This Release

Operational Enhancements

"*show license*" command improvement (VOSS-34131)

The existing CLI command *show license* was enhanced with extra details based on user experience in previous release.

Switch:1 (config) # show license
****
Command Execution Time: Mon Nov 06 10:44:54 2025 PDT
****
BASE License: Available
PREMIER License: <Trial | Perpetual | Subscription | Not Available>
Perpetual MACSEC License: Not Available
Subscription License Level: <Trial | Standard | Advanced | Pilot | Not Available>, expires in <x> days
****

Radius VSA for IGMP Version and Fast-Leave (VOSS-33733)

On a VLAN interface we can now enable IGMP Version 3 and Fast-Leave by extending the current functionality of the Extreme-Dyn-Config Radius VSA. For IGMP, the operations executed on the VLAN interface are the following:

- Changing IGMP version to IGMPv3:
  - Disable IGMP Fast-Leave, if enabled
  - Change version to IGMPv3
  - Enable compatibility mode
- Enabling IGMP Fast-Leave:
  - On a VLAN IGMPv2 interface: enable IGMP Fast-Leave
  - On a VLAN IGMPv3 interface:
    - enable IGMPv3 explicit-host-tracking
    - enable IGMP Fast-Leave

When all the EAP/NEAP clients that are using the previously applied dynamic IGMP settings are unauthenticated, the dynamic settings are reverted.

The IGMP changes are applied on-the-fly. If IGMP Snooping or IGMP Multicast Lite is enabled through RADIUS VSA the new settings will be applied on the associated VLAN interface.

Use Cases

MHMV

- Regular port
  - if one VLAN attribute is received from the RADIUS Server, the IGMP VSA is applied on them
  - if no VLAN attribute is received, the IGMP VSA is applied on the default VLAN
- Flex-UNI port:
  - if one ISID attribute is received from the RADIUS Server, the IGMP VSA is applied on the associated platform VLAN
  - if no ISID attribute is received, the IGMP VSA is applied on the platform VLAN associated with the default untagged ISID

MHSA

- Regular port:
  - if one or more VLAN attributes are received from the RADIUS Server, the IGMP VSA is applied on only one VLAN, usually is the last one received
  - if no VLAN attribute is received, the IGMP VSA is applied on the default VLAN
- Flex-UNI port:
  - if one or more ISID attributes are received from the RADIUS Server, the IGMP VSA is applied on all the platform VLANs associated with those ISIDs
  - if no ISID attribute is received, the IGMP VSA is applied on all the VLANs that contain the client port

MIB changes

Functionality was extended for ***rcEapMultiHostStatusDynamicSettings*** and r***cEapPortDynamicSettings*** to display the following tokens: "IGMPV3", "IGMPFAST".

New mib objects were added in ***rcIgmpInterfaceExtnEntry****:*

- rcIgmpInterfaceExtnVersionOrigin,
- rcIgmpInterfaceExtnFastLeaveEnableOrigin,
- rcIgmpInterfaceExtnExplicitHostTrackingEnableOrigin,
- rcIgmpInterfaceExtnCompatibilityModeEnableOrigin.

Radius VSA for IGMP Querier Address (VOSS-33944)

The IGMP Querier address can be configured only with IPv4 addresses.
The address received will be used to configure:

- the IGMP Snooping Querier address if the VLAN interface is configured for IGMP Snooping (in this case we must also enable the IGMP Snooping Querier)
- the IGMP Routed SPB Querier address if the VLAN interface is configured for Multicast Lite or Routed Multicast

VSA Extreme-Dynamic-Client-Assignments was extended to support IGMP Querier Address:

Format: create=vlan|pvlan|none, pv=Primary VLANID, sv=secondary VLANID, vni=L2-ISID, ev=EGRESS-VLAN-tag, vn=vlan-name, vnin=isid-name, mvni=MVPN-ISID, **igmpqaddr=<IPv4 address>**

The querier address will be applied on the VLAN interface specified in the save VSA as a **pv** argument.

The current support was updated with the token “none” for **create** argument of the VSA Extreme-Dynamic-Client-Assignments to use an existing VLAN.

Mib changes

rcEapStoredVSAsContent functionality was extended to display the IGMP Querier Address using the following format: "igmpqaddr=<IPv4 address> ".

New mib objects were added in ***rcIgmpInterfaceExtnTable***:

- rclgmpInterfaceExtnSnoopQuerierEnableOrigin,
- rclgmpInterfaceExtnSnoopQuerierAddrOrigin,
- rclgmpInterfaceExtnRoutedSpbQuerierAddrOrigin

SSH to system-ID - ability to delete "known_hosts" file (VOSS- 33999)

When a factory reset is done on a switch, it resets the ssh key as well. After this a new ssh to this system-ID will not be possible because the remote host has changed, so the original switch can never ssh again to the remote host unless we factory reset the switch that is originating the ssh connection.

Starting with 9.3.1 this can be resolved without a factory reset, by deleting the file /intflash/.ssh/known_hosts from CLI with this command *#delete /intflash/.ssh/known_hosts*

Old Features Removed From This Release
None

Problems Resolved in This Release	
CFD-12204	An ACL applied to a private VLAN does not filter packets entering through UNI ports, but it works correctly on NNI ports.
CFD-13396	The Layer 2 VLAN I-SID entry is missing from the IO tables.
CFD-13854	The *"show io resources interface"* command displays incorrect resource information.
CFD-13965	ISIS hello-auth key configuration may be lost after a power outage event.
CFD-14785	When a supplicant duplicates the first response from an EAP authentication, the RADIUS server will reject authentication if it receives unexpected AVP values.
CFD-14822	The DHCP server stops functioning after swapping IP addresses between two existing DHCP static hosts.
CFD-14948	A data forwarding issue was identified in environments utilizing vIST where MAC addresses move rapidly between access points (APs). This behavior resulted in a mismatch between hardware and software forwarding tables, leading to packet drops.
CFD-15064	Some BGP configuration does not appear in the running configuration when a dynamically created SD-WAN VRF exists.
CFD-15087	Switch reboots when ZTP+ license configs are not acknowledged (Fix for the issue identified in FN-2025-519 License Check)
CFD-15107	Fabric Attach interface authentication may fail after a 9.x.x software upgrade until key is reconfigured.
CFD-15125	In a specific scenario involving inter-VRF static routes, a static route entry may fail to be programmed into the hardware forwarding tables.
CFD-15272	The SSH implementation uses SHA-1 for ssh-rsa keys, which is considered insecure.
CFD-15334	When using Air Gap Mode in XIQ-SE and connectivity to XIQ-SE is blocked, there are excessive ZTP+ discovery started/ failed log messages on switch.
CFD-15348	ZTP+ upgrade fails when XIQ-SE is using SCP passwords that contain the "@" symbol.
CFD-15349	When configuring an OSPF interface while interface is physically down, the default cost configuration of the interface will be overwritten with an incorrect value.
CFD-15423, VOSS-34384	During authenticator-initiated EAP authentication, if the client sends an EAPOL-Start packet, the EAP process incorrectly drops a MAC address on the port because it assumes the maximum MAC limit has been reached. Once this condition is encountered on the port all further authentication attempts will be blocked until the switch is restarted.
CFD-15472	Disconnect Requests with RADIUS VSA PORTBOUNCE does not clear the NEAP session on the affected port.
CFD-15491	EDM web user IDs allow only 32-character passwords, while CLI user IDs allow up to 80 characters.

Fixes from Previous Releases
VOSS 9.3.1.0 incorporates all fixes and content from previous releases including VOSS 8.10.8.0, VOSS 9.0.5.1, VOSS 9.1.3.0, VOSS 9.2.2.0 and VOSS 9.3.0.0.

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-13455	In a vIST configuration, a short outage may occur after a DVR leaf reboots. A fix for this issue is targeted for 9.3.2.0 release.
CFD-13639	In an MA environment, prefixes might be installed wrongly on OSPF ASBR routing table. A fix for this issue is targeted for 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.
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. A fix for this issue is targeted for 9.4.0.0 release. **Workaround**: have the VIST NNI converted to static.
CFD-15427	Unable to ping Anycast Gateway IP from the switch A fix for this issue is targeted for 9.2.3.0 release. **Workaround:** use the command *#show ip anycast-gateway interfaces* and verify the "OPER STATE" column to see if Anycast GW interface is UP or DOWN.

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.

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