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

Customer Release Notes

VSP Operating System Software

Software Release 8.1.9.0
March 2021

INTRODUCTION:

This document provides specific information for version 8.1.9.0 of agent software for the VSP Operating System Software.

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

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/

IMPORTANT NOTES BEFORE UPGRADING TO THIS RELEASE:

If upgrading systems from either release 4.2.1.0 or release 4.2.1.1 that have ISIS enabled link(s) configured with HMAC-MD5 authentication, then you need to perform the procedure described in the section ***SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES*** in order to avoid potential network connectivity loss.

If upgrading systems running 4.1.X releases which also have TACACS+ enabled, refer to the section ***SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES*** for upgrade instructions.

If upgrading systems running 6.0.x releases or older, refer to the section ***SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES*** for instructions about the need to step-through a 6.1.x release prior to going to 7.1.x or greater release.

UPGRADE CONSIDERATION WHEN UPGRADING TO 8.1.9.0 FROM PREVIOUS RELEASE:

If you have a vlan X with vrrp instance of 37 provisioned and functional on a node running with several other vlans with dvr enabled, upon upgrade to 8.1.9.0 VRRP configuration for instance 37 is removed from that vlan X. This would cause traffic loss for those devices of that vlan X. Recommend renumbering the vrrp instance ids to other than 37 and 38 on that Vlan before upgrading.
DVR uses the same multicast addresses as vrrp id 37 and 38 for its DVR controller and leaf implementation.

PLATFORMS SUPPORTED:

Virtual Services Platform 4400 Series
- Virtual Services Platform VSP 4450GSX-PWR+
- Virtual Services Platform VSP 4450GSX-DC
- Virtual Services Platform VSP 4450GTS-DC
- Virtual Services Platform VSP 4450GTX-HT-PWR+

Virtual Services Platform 4900 Series
- Virtual Services Platform VSP 4900-48P
- Virtual Services Platform VSP4900-12MXU-12XE
- Virtual Services Platform VSP4900-24S
- Virtual Services Platform VSP4900-24XE

Virtual Services Platform 7200 Series
- Virtual Services Platform VSP 7254XSQ
- Virtual Services Platform VSP 7254XTQ

Virtual Services Platform 7400 Series
- Virtual Services Platform VSP 7432CQ
- Virtual Services Platform VSP 7400-48Y-8C

Virtual Services Platform 8200 Series
- Virtual Services Platform 8284XSQ

Virtual Services Platform 8400 Series
- Virtual Services Platform 8404
- Virtual Services Platform 8404C

ExtremeAccess Platform XA1400 Series
- ExtremeAccess Platfrom 1440
- ExtremeAccess Platform 1480

SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES:

1. The following procedure should be followed when upgrading systems running one of the following two releases, 4.2.1.0 or 4.2.1.1 which also have ISIS enabled links with HMAC-MD5 authentication on:

   Disable ISIS authentication throughout the network a system at a time, a link at a time by disabling it on either side of each link, ensuring the link is stable before moving to the next. When a system has been reconfigured free of ISIS HMAC-MD5 authentication in all of its links, save the configuration file and perform the upgrade to release 4.2.3.0 or greater. After all these systems have been upgraded to release 4.2.3.0 or greater, you may re-enable authentication a system at a time, a link at a time and save the configuration file in each of the involved systems.

   Example:

   ```
   VSP:1(config)#interface gigabitethernet x/y
   VSP:1(config-if)#no isis hello-auth
   VSP:1(config-if)#save config
   VSP:1(config-if)# PERFORM THE UPGRADE
   VSP:1(config)#interface gigabitethernet x/y
   VSP:1(config-if)# isis hello-auth type hmac-md5 key <keyname> [key-id
   <keyed>]
   VSP:1(config-if)#save config
   ```

2. The following procedure should be followed when upgrading systems running 4.1.X releases which also have TACACS+ enabled on:

   When you upgrade from VOSS 4.1.X to VOSS 4.2 or a higher release, the TACACS+ host configurations will be lost. After the upgrade, the TACACS+ host configurations will not take effect so you must reconfigure them. After you make the configurations, you must save the changes on the device. You should also save the configuration to a file to retain the configuration settings.

3. Upgrading DVR configurations from releases 6.0.1.1 and earlier to 6.0.1.2 and beyond.
   a. All DVR nodes must be upgraded to the same release.
   b. All DVR leaves should be upgraded first.

4. Upgrading from releases 6.0.x and earlier
   a. Direct upgrade from 6.0.x or earlier releases to 7.x releases is not supported.
   b. Please upgrade to a 6.1.x release first (Release 6.1.6.0 or higher is recommended). Then upgrade to the desired 7.x release (Release 7.1.1.0 or higher recommended), 8.0.x release or 8.1.x release.

Review items 5, 6, and 7 if the ISIS L1 area is **`00.1515.fee1.900d.1515.fee1.900d`**, 00.0000.0000 or all zero's.

5. Legacy ZTF Procedures for Releases 7.0.0.0 - 7.1.2.0, 8.0.0.0, 8.0.1.0, and 8.0.5.0
   a. Boot with factory-defaults fabric.
   b. ISIS manual-area set to 00.0000.0000, Dynamically Learned Area (DLA) displayed as 00.0000.0000 and ISIS enabled with other parameters.
   c. HELLO PDUs not sent.
   d. Listen on active ISIS interfaces for ISIS HELLO with non-zero Area ID. Zeros of any length up to 13 bytes are considered a zero value.
   e. When an ISIS HELLO with a non-zero Area ID is received, use that area ID as the DLA and start sending HELLO with DLA on all ISIS interfaces.
   f. DLA set and displayed as learned in the previous step.
   g. Saving the configuration will save into the configuration file `manual-area 00.0000.0000`.
   h. Boot with the saved configuration. The ZTF procedures are triggered. ISIS interfaces in passive mode not sending ISIS HELLOs. Only process incoming ISIS HELLO with non-zero Area ID.

   Note: You can reach the fourth step by manually configuring the ISIS/SPBM with a manual-area equal to 0 (all values of 0, regardless of the length of zeros, are considered the same) and enabling ISIS.

6. Modified ZTF Procedures for Releases 7.1.3.0+ and 8.0.6.0+
   a. Boot with factory-defaults fabric
   b. ISIS manual-area set to 00.1515.fee1.900d.1515.fee1.900d, Dynamically Learned Area (DLA) is blank and ISIS enabled with other parameters.
   c. HELLO PDUs not sent
   d. Listen on active ISIS interfaces for ISIS HELLO with and Area ID not equal to **`00.1515.fee1.900d.1515.fee1.900d`**.
   e. When an ISIS HELLO with an Area ID not equal to **`00.1515.fee1.900d.1515.fee1.900d`** is received, use that Area ID as the DLA and start sending HELLO with DLA on all ISIS interfaces.

f. DLA set and displayed as learned in the previous step.
g. Saving the configuration file will save into the configuration file `manual-area 00.1515.fee1.900d.1515.fee1.900d`.
h. Boot with the saved configuration. ZTF procedures are triggered. ISIS interfaces in passive mode not sending ISIS HELLO's, only processing incoming ISIS HELLO with an Area ID note equal to **`00.1515.fee1.900d.1515.fee1.900d`**.

Note: You can reach the fourth step by manually configuring the ISIS/SPBM with a manual-area equal to 00.1515.fee1.900d.1515.fee1.900d and enabling ISIS.

7. Migration to a Release supporting Modified ZTF such as 7.1.3.0+ or 8.0.6.0+

a. From Pre-ZTF feature Release such as 6.1.6.0

The following considerations should be taken into account when upgrading to this release from a pre-ZTF release:

i. Check the ISIS manual area (show isis manual-area).
ii. Determine if the manual area equals 00.1515.fee1.900d.1515.fee1.900d.
iii. This is a normal Area ID before the upgrade. After the upgrade, ZTF procedures, as previously described, will be triggered.
- If the existing behavior is desired, the ISIS manual area used in the network needs to be changed to a different value. Note, if ISIS is the management network used to get to the node, it will not form an ISIS adjacency after the upgrade and not join the network. This will isolate the node. The changes to the manual area within the topology should be made before any upgrades are performed.

b. From a Release Running Legacy ZTF such as 7.1.2.0

The following considerations should be taken into account when upgrading to a release supporting Modified ZTF from a Legacy ZTF release.

- Check the ISIS manual area (show isis manual-area).
- Determine if the manual area equals 00.0000.0000 or is a 00 of any length.
- This Area ID triggered the ZTF procedures before the upgrade. After the upgrade, ZTF procedures, as previously described, will NOT be triggered.
- If the existing behavior is desired, replace the value of ISIS manual area with 00.1515.fee1.900d.1515.fee1.900d. Note, if ISIS is the management network used to get to the node, it will not form an ISIS adjacency after the upgrade and not join the network. This will isolate the node. The change should be made before the upgrade.
- Determine if the manual area equals 00.1515.fee1.900d.1515.fee1.900d.
  - This is a normal Area ID before the upgrade. After the upgrade to a release implementing
- Modified ZTF, the ZTF procedures, as previously described, will be triggered.
- If this is not desired, replace the value of ISIS manual area with a different value. Note, if ISIS is the management network used to get to the node, it will not form an ISIS adjacency after the upgrade and not join the network. This will isolate the node. The change should be made before the upgrade.

NOTES FOR UPGRADE:

Please see “Release Notes for VSP Operating System Software (VOSS)” for software release 8.1.5 available at https://www.extremenetworks.com/support/release-notes for details regarding Known Limitations.

FILE NAMES FOR THIS RELEASE:

Virtual Services Platform 4400 Series

File Name	Module or File Type	File Size (bytes)
VOSS4400.8.1.9.0.sha512	SHA512 Checksums	1549
VOSS4400.8.1.9.0.md5	MD5 Checksums	589
VOSS4400.8.1.9.0.tgz	Release 8.1.9.0 archived software distribution	110261133
VOSS4400.8.1.9.0_mib.zip	Archive of all MIB files	1160789
VOSS4400.8.1.9.0_mib.txt	MIB file	7702128
VOSS4400.8.1.9.0_mib_sup.txt	MIB file	1364272
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 4900 Series`

File Name	Module or File Type	File Size (bytes)
VOSS4900.8.1.9.0.sha512	SHA512 Checksums	1701
VOSS4900.8.1.9.0.md5	MD5 Checksums	645
VOSS4900.8.1.9.0.tgz	Release 8.1.9.0 archived software distribution	239086836
VOSS4900.8.1.9.0_mib.zip	Archive of all MIB files	1160789
VOSS4900.8.1.9.0_mib.txt	MIB file	7702128
VOSS4900.8.1.9.0_mib_sup.txt	MIB file	1385881
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7200.8.1.9.0.sha512	SHA512 Checksums	1549
VOSS7200.8.1.9.0.md5	MD5 Checksums	589
VOSS7200.8.1.9.0.tgz	Release 8.1.9.0 archived software distribution	124606489
VOSS7200.8.1.9.0_mib.zip	Archive of all MIB files	1160789
VOSS7200.8.1.9.0_mib.txt	MIB file	7702128
VOSS7200.8.1.9.0_mib_sup.txt	MIB file	1369354
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 7400 Series

File Name	Module or File Type	File Size (bytes)
VOSS7400.8.1.9.0.sha512	SHA512 Checksums	1547
VOSS7400.8.1.9.0.md5	MD5 Checksums	532
VOSS7400.8.1.9.0.tgz	Release 8.1.9.0 archived software distribution	238741747
VOSS7400.8.1.9.0_mib.zip	Archive of all MIB files	1160789
VOSS7400.8.1.9.0_mib.txt	MIB file	7702128
VOSS7400.8.1.9.0_mib_sup.txt	MIB file	1380078
VOSS7400v815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020
TPVM_7400_8.1.9.0.img	Third Party Virtual Machine (TPVM)	1677066240

Virtual Services Platform 8200 Series

File Name	Module or File Type	File Size (bytes)
VOSS8200.8.1.9.0.sha512	SHA512 Checksums	1549
VOSS8200.8.1.9.0.md5	MD5 Checksums	589
VOSS8200.8.1.9.0.tgz	Release 8.1.9.0 archived software distribution	124609703
VOSS8200.8.1.9.0_mib.zip	Archive of all MIB files	1160789
VOSS8200.8.1.9.0_mib.txt	MIB file	7702128
VOSS8200.8.1.9.0_mib_sup.txt	MIB file	1369354
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 8400 Series

File Name	Module or File Type	File Size (bytes)
VOSS8400.8.1.9.0.sha512	SHA512 Checksums	1549
VOSS8400.8.1.9.0.md5	MD5 Checksums	589
VOSS8400.8.1.9.0.tgz	Release 8.1.9.0 archived software distribution	185831489
VOSS8400.8.1.9.0_mib.zip	Archive of all MIB files	1160789
VOSS8400.8.1.9.0_mib.txt	MIB file	7702128
VOSS8400.8.1.9.0_mib_sup.txt	MIB file	1369354
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020

ExtremeAccess 1400 Series

File Name	Module or File Type	File Size (bytes)
VOSS1400.8.1.9.0.sha512	SHA512 Checksums	1401
VOSS1400.8.1.9.0.md5	MD5 Checksums	537
VOSS1400.8.1.9.0.tgz	Release 8.1.9.0 archived software distribution	320366656
VOSS1400.8.1.9.0_mib.zip	Archive of all MIB files	1160789
VOSS1400.8.1.9.0_mib.txt	MIB file	7702128
VOSS1400.8.1.9.0_mib_sup.txt	MIB file	1045725
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669

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 VOSS4400.8.1.9.0.tgz
software activate 8.1.9.0.GA
```

or

```
software add VOSS4900.8.1.9.0.tgz
software activate 8.1.9.0.GA
```

or

```
software add VOSS7200.8.1.9.0.tgz
software activate 8.1.9.0.GA
```

or

```
software add VOSS7400.8.1.9.0.tgz
software activate 8.1.9.0.GA
```

or

```
software add VOSS8200.8.1.9.0.tgz
software activate 8.1.9.0.GA
```

or

```
software add VOSS8400.8.1.9.0.tgz
software activate 8.1.9.0.GA
```

or

```
software add VOSS1400.8.1.9.0.tgz
software activate 8.1.9.0.GA
```

COMPATIBILITY:

This software release is managed with Enterprise Device Manager (EDM), which is integrated into the agent software.

CHANGES IN THIS RELEASE:

New Features in This Release
None.

Old Features Removed From This Release
None.

Problems Resolved in This Release	
VOSS-17657	TACACS: Local RWA user has RO rights after logging on successfully if tacacs is enabled, no server is configured and previous login was unsuccessful.
VOSS-18005	Software add/activate wouldn't complete when closing the session they were issued from
VOSS-18565	SSIO's tMainTask at 53% CPU during intensive SNMP polling
VOSS-18815	XA1440 reset with core unexpectedly
VOSS-18892	Switch rebooted when 8418XSQ removed and replaced with another 8418XSQ in same slot
VOSS-18899	LLDP-MED not assigning ip phone to voice vlan
VOSS-18988	Traffic sourced from CLIP starts taking non GRT VRF default route when a L3-vsn added to the VRF
VOSS-19177	tMainTask running within process SSIO is causing constant 60% CPU churn polling I/O card data
VOSS-19302	In specific conditions, incoming traffic from one B-VID might be dropped by the device.
VOSS-19361	VSP 8404C rebooted by inserting line cards multiple times
VOSS-19411	"show khi cpp port-statistics spbm-internal-ports" showing output incorrectly and incompletely
VOSS-19436	SPB BMAC's learned on C-UNI port
VOSS-19438	"60 percent of fbufs are in use: " message periodically logging on the distribution switch every 15 minutes
VOSS-19448	VSP4900-48P Ports 2, 10, 18, 26, 34, 42 frequently flap
VOSS-19472	Switch may reboot when IPv6 configuration is present
VOSS-19593	Mellanox QSFP+ to SFP+ adaptor not reporting correct DDI values
VOSS-19788	VSP stopped responding to console and SSH
VOSS-19817	Cannot configure 10.20.0.255 as NTP server
VOSS-19893	Switch reset with core file immediately after XMC saved config
VOSS-20111	Default OSPF backbone areas created within VRF context are counted in the total OSPF areas, even when not in use, thereby reducing OSPF Area scaling limits
VOSS-20125	VSP8404 rebooted with core file
VOSS-20156	VSP8404 7.1.0.0 cored due to Memory reached critical
VOSS-20372	DVR: show command anomalies when IP address is max 15 characters long.
VOSS-20469	Sflow Task ~30% higher CPU utilization after upgrade
VOSS-20556	Unable to login to switch in enhanced security mode and then followed by complete freeze

Problems Resolved in This Release	
VOSS-20625	VSP4900 - LLDP floods on flex-uni untagged port

Fixes from Previous Releases
VOSS 8.1.9.0 incorporates all fixes from prior releases, up to and including VOSS 7.1.7.0 and VOSS 8.0.9.0.

OUTSTANDING ISSUES:

Please see “Release Notes for VSP Operating System Software (VOSS)” for software release 8.1.5 available at https://www.extremenetworks.com/support/release-notes for details regarding Known Issues.

KNOWN LIMITATIONS:

Please see “Release Notes for VSP Operating System Software (VOSS)” for software release 8.1.5 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.

Trademarks