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

Customer Release Notes

VSP Operating System Software

Software Release 8.1.10.0
July 2021

INTRODUCTION:

This document provides specific information for version 8.1.10.0 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 8.1.10.0 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 8.1.10.0 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:

ExtremeAccess 1400 Series

File Name	Module or File Type	File Size (bytes)
VOSS1400.8.1.10.0.sha512	SHA512 Checksums	1254
VOSS1400.8.1.10.0.md5	MD5 Checksums	430
VOSS1400.8.1.10.0.tgz	Release 8.1.10.0 archived software distribution	320388901
VOSS1400.8.1.10.0_mib.zip	Archive of all MIB files	1160825
VOSS1400.8.1.10.0_mib.txt	MIB file	7702240
VOSS1400.8.1.10.0_mib_sup.txt	MIB file	1045725
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669

Virtual Services Platform 4400 Series

File Name	Module or File Type	File Size (bytes)
VOSS4400.8.1.10.0.sha512	SHA512 Checksums	1402
VOSS4400.8.1.10.0.md5	MD5 Checksums	482
VOSS4400.8.1.10.0.tgz	Release 8.1.10.0 archived software distribution	110330351
VOSS4400.8.1.10.0_mib.zip	Archive of all MIB files	1160825
VOSS4400.8.1.10.0_mib.txt	MIB file	7702240
VOSS4400.8.1.10.0_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)
VOSS4900.8.1.10.0.sha512	SHA512 Checksums	1554
VOSS4900.8.1.10.0.md5	MD5 Checksums	538
VOSS4900.8.1.10.0.tgz	Release 8.1.10.0 archived software distribution	242440475
VOSS4900.8.1.10.0_mib.zip	Archive of all MIB files	1160825
VOSS4900.8.1.10.0_mib.txt	MIB file	7702240
VOSS4900.8.1.10.0_mib_sup.txt	MIB file	1385881
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020
TPVM_4900_8.1.9.0.img	Third Party Virtual Machine (TPVM)	1677066240

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7200.8.1.10.0.sha512	SHA512 Checksums	1402
VOSS7200.8.1.10.0.md5	MD5 Checksums	482
VOSS7200.8.1.10.0.tgz	Release 8.1.10.0 archived software distribution	124675604
VOSS7200.8.1.10.0_mib.zip	Archive of all MIB files	1160825
VOSS7200.8.1.10.0_mib.txt	MIB file	7702240
VOSS7200.8.1.10.0_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)
VOSS7400.8.1.10.0.sha512	SHA512 Checksums	1554
VOSS7400.8.1.10.0.md5	MD5 Checksums	538
VOSS7400.8.1.10.0.tgz	Release 8.1.10.0 archived software distribution	242100475
VOSS7400.8.1.10.0_mib.zip	Archive of all MIB files	1160825
VOSS7400.8.1.10.0_mib.txt	MIB file	7702240
VOSS7400.8.1.10.0_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)
VOSS8200.8.1.10.0.sha512	SHA512 Checksums	1402
VOSS8200.8.1.10.0.md5	MD5 Checksums	482
VOSS8200.8.1.10.0.tgz	Release 8.1.10.0 archived software distribution	124674823
VOSS8200.8.1.10.0_mib.zip	Archive of all MIB files	1160825
VOSS8200.8.1.10.0_mib.txt	MIB file	7702240
VOSS8200.8.1.10.0_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)
VOSS8400.8.1.10.0.sha512	SHA512 Checksums	1402
VOSS8400.8.1.10.0.md5	MD5 Checksums	482
VOSS8400.8.1.10.0.tgz	Release 8.1.10.0 archived software distribution	185914802
VOSS8400.8.1.10.0_mib.zip	Archive of all MIB files	1160825
VOSS8400.8.1.10.0_mib.txt	MIB file	7702240
VOSS8400.8.1.10.0_mib_sup.txt	MIB file	1369354
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020

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 VOSS4400.8.1.10.0.tgz
software activate 8.1.10.0.GA
```

or

```
software add VOSS4900.8.1.10.0.tgz
software activate 8.1.10.0.GA
```

or

```
software add VOSS7200.8.1.10.0.tgz
software activate 8.1.10.0.GA
```

or

```
software add VOSS7400.8.1.10.0.tgz
software activate 8.1.10.0.GA
```

or

```
software add VOSS8200.8.1.10.0.tgz
software activate 8.1.10.0.GA
```

or

```
software add VOSS8400.8.1.10.0.tgz
```

```
software activate 8.1.10.0.GA
```

or

```
software add VOSS1400.8.1.10.0.tgz
software activate 8.1.10.0.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
New informational messages about FDB table scaling limit being reached were added (VOSS-21395): *VSP-4900-48P:1(config)#1 2021-06-02T08:04:52.255Z VSP-4900-48P CP1 - 0x00000609 - 00000000 GlobalRouter SW INFO Number of MAC entries passed the 80% threshold of total MACs allowed.* *1 2021-06-02T08:05:04.118Z VSP-4900-48P CP1 - 0x00000609 - 00000000 GlobalRouter SW INFO Number of MAC entries passed the 85% threshold of total MACs allowed.* *VSP-4900-48P:1(config)#1 2021-06-02T08:05:20.418Z VSP-4900-48P CP1 - 0x00000609 - 00000000 GlobalRouter SW INFO Number of MAC entries passed the 90% threshold of total MACs allowed.* *VSP-4900-48P:1(config)#1 2021-06-02T08:05:34.047Z VSP-4900-48P CP1 - 0x00000609 - 00000000 GlobalRouter SW INFO Number of MAC entries passed the 95% threshold of total MACs allowed.* *VSP-4900-48P:1(config)#1 2021-06-02T08:05:42.627Z VSP-4900-48P CP1 - 0x00000610 - 00000000 GlobalRouter SW INFO Number of Mac Entries Reached 40985 Mac Address learning stopped. MAC 00:03:03:00:bf:ce*

Old Features Removed From This Release
None.

Problems Resolved in This Release	
VOSS-18066	VSP7400 Potential semaphore deadlock caused crash in process SSIO
VOSS-18664	VSP7400 hung requiring cold reboot to recover
VOSS-18953	VSP 7400 failed with no apparent reason and caused network outage until vIST formed with its peer (took 27 minutes after the cold boot)
VOSS-18959	VSP 7400: VRRP to DVR conversion caused about 80% reachability Loss
VOSS-19435	VLACP sequence number mismatch on all NNI's
VOSS-19457	VSP8200: Crashes after inserting new VSP7400 into network.
VOSS-19544	Unicast packet duplication and flooding in fabric
VOSS-19585	VSP8400 port has link up but Rx does not receive any traffic until a reboot/reseat
VOSS-19626	Link gets down (due to VLACP) when the MACSEC re-key happens (4billion frames later)
VOSS-19916	VSP7400 stopped working - before outage memory utilization went up

Problems Resolved in This Release	
VOSS-15387, VOSS-20207	VSP4450 - frequent silent resets and a core dump in ‘bcmINTR’ without backtrace
VOSS-20265	25G ports are unable to establish link with FEC, and also showing high FCS errors
VOSS-20310	VSP8200: Ports 1/1 thru 1/23 all reset at same time and has occurred twice in as many days
VOSS-20312	High SSIO tMainTask utilization while processing a large number of l3 vsn route add operations
VOSS-20386	While making a change to BGP the node rebooted with core file
VOSS-20395	VSP7400: Switch hangs up and requires to reboot
VOSS-20412	DVR: high ssio tMainTask utilization causing delays in programming datapath records.
VOSS-20422	VRRP not transitioning to backup
VOSS-20533	VSP 4900 crash when specific LLDP packets expose a memory leak
VOSS-20581	Slow memory leak in cbcp-main.x due to processing rcIpInsertDhcpOption82 packets
VOSS-20736	Switch rebooted with core dump when processing specific malformed DHCP packets
VOSS-20745	VSP4900 platform being unresponsive for 3 hours
VOSS-20778	ACL redirect-next-hop filter doesn't work
VOSS-20805	DVR ECMP: ref count 0 multipath objects when hosts are moving and remain a few seconds in 2 places
VOSS-20839	Memory utilization has slowly continued to increase since upgrading VSP8284s to v8.1.5.0.
VOSS-20873	Session lock when commands issued - Show full and Show int gig
VOSS-20966	Switch crashed during show fulltech command
VOSS-21038	High CPU utilization at 75 – 80% for long periods if the IP more-specific-non-local-route feature is enabled
VOSS-21066	VSP7400-48Y-8C: Displaying pluggable details for the 40Gb AA1404005-E6 SKU, we were seeing a checksum error
VOSS-21109	VSP-7254XTQ: After upgrading to 8.1.9.0, odd numbered ports (2/1,2/3,2/5) in slot 2 are not detecting the GBIC
VOSS-21147	OOM crashes & MIIM crashes driven by rapid MAC address movement
VOSS-21192	DVR Route redist to OSPF/host route redistributed by both domains
VOSS-21193	Both switches in cluster crashed when LACP enabled on port that was previous member of vIST
VOSS-21194	EDM: Export button does not respond
VOSS-21259	XA 1400 - CLI "show io ipsec logs " delays around 20 to 30 min to display latest log
VOSS-21334	Not able to use compare function for the md5 checksum
VOSS-21376	Missing L3 HW Records for ARP and DVR host routes
VOSS-21394	Command “banner custom” does not remove the default banner on SSH session
VOSS-21398	VSP 8400: ARP refreshing for devices on single home MLTs generating DVR TLV messages
VOSS-21402	"DYNAMIC CLEAR GlobalRouter P2IP ERROR Cleared the condition for PORT Flapping detected" log not displaying correctly the port when sending ARP reqs besides traffic
VOSS-21412	Duplication of IP address of IP VLAN interface on multiple DVR controllers leads to stale backbone entries that cannot be removed
VOSS-21562	Unable to read SMP log files in non-JITC and JITC mode on the same switch
VOSS-21636	VSP7400 does not route to an ISIS accept entry
VOSS-21827	IST, SMLT, VRRP down briefly after enabling access policy config

Fixes from Previous Releases
VOSS 8.1.10.0 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.

VOSS-19471	DVR: Backbone host entry may be incorrectly removed from other DVR domains when a DVR controller in the local domain is taken down. The host entries will be repopulated when the down controller is recovered. Workaround: Clear DVR host entries in the remaining DVR controller in the local domain using this command: *clear dvr host-entries ipv4 <IP> l3isid <I-SID>* or *clear dvr host-entries l3isid <I-SID>* - this could be disruptive in the local domain
VOSS-20030	An interaction between DVR host learning and wireless solutions configured with proxy-ARP and bridging at the AP may create instability within the DVR domain due to specific combinations of roaming events and topology factors. This interaction is exposed when a client roams between AP's connected to different BEB's and both AP's momentarily respond for the client IP on both BEB's (host duplication). These interactions can be avoided by using VRRP instead of DVR for wireless segments.
VOSS-21087	After duplicates hosts are resolved a traffic loss for some hosts may occur Workaround: Clear the DVR host for each impacted individual host entry using this command in the domain in which the host resides: *clear dvr host-entries ipv4 <IP> l3isid <I-SID>*

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.