Extreme *networks*

ADVANCE WITH US

Customer Release Notes

VSP Operating System Software

Software Release 8.1.6.0
June 2020

INTRODUCTION:

This document provides specific information for version 8.1.6.0 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/

NEW IN THIS RELEASE:

A consistency check was added to prevent configuration of VRRP VRID 37 or 38 when DVR is enabled and vice versa.

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 release.

UPGRADE CONSIDERATION WHEN UPGRADING TO 8.1.6.0 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 8.1.6.0 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.

F0615-O

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 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).

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.

F0615-O

    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)
VOSS4400.8.1.6.0.sha512	SHA512 Checksums	1549
VOSS4400.8.1.6.0.md5	MD5 Checksums	589
VOSS4400.8.1.6.0.tgz	Release 8.1.6.0 archived software distribution	110234518
VOSS4400.8.1.6.0_mib.zip	Archive of all MIB files	1160409
VOSS4400.8.1.6.0_mib.txt	MIB file	7699369
VOSS4400.8.1.6.0_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)
VOSS4900.8.1.6.0.sha512	SHA512 Checksums	1701
VOSS4900.8.1.6.0.md5	MD5 Checksums	645
VOSS4900.8.1.6.0.tgz	Release 8.1.6.0 archived software distribution	237281524
VOSS4900.8.1.6.0_mib.zip	Archive of all MIB files	1160409
VOSS4900.8.1.6.0_mib.txt	MIB file	7699369
VOSS4900.8.1.6.0_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)
VOSS7200.8.1.6.0.sha512	SHA512 Checksums	1549
VOSS7200.8.1.6.0.md5	MD5 Checksums	589
VOSS7200.8.1.6.0.tgz	Release 8.1.6.0 archived software distribution	124576368
VOSS7200.8.1.6.0_mib.zip	Archive of all MIB files	1160409
VOSS7200.8.1.6.0_mib.txt	MIB file	7699369
VOSS7200.8.1.6.0_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)
VOSS7400.8.1.6.0.sha512	SHA512 Checksums	1701
VOSS7400.8.1.6.0.md5	MD5 Checksums	645
VOSS7400.8.1.6.0.tgz	Release 8.1.6.0 archived software distribution	236929137
VOSS7400.8.1.6.0_mib.zip	Archive of all MIB files	1160409
VOSS7400.8.1.6.0_mib.txt	MIB file	7699369
VOSS7400.8.1.6.0_mib_sup.txt	MIB file	1380078
VOSS7400v815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020
TPVM_7400_8.1.6.0.img	Third Party Virtual Machine (TPVM)	1677066240

Virtual Services Platform 8200 Series

File Name	Module or File Type	File Size (bytes)
VOSS8200.8.1.6.0.sha512	SHA512 Checksums	1549
VOSS8200.8.1.6.0.md5	MD5 Checksums	589
VOSS8200.8.1.6.0.tgz	Release 8.1.6.0 archived software distribution	124579569
VOSS8200.8.1.6.0_mib.zip	Archive of all MIB files	1160409
VOSS8200.8.1.6.0_mib.txt	MIB file	7699369
VOSS8200.8.1.6.0_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)
VOSS8400.8.1.6.0.sha512	SHA512 Checksums	1549
VOSS8400.8.1.6.0.md5	MD5 Checksums	589
VOSS8400.8.1.6.0.tgz	Release 8.1.6.0 archived software distribution	185773637
VOSS8400.8.1.6.0_mib.zip	Archive of all MIB files	1160409
VOSS8400.8.1.6.0_mib.txt	MIB file	7699369
VOSS8400.8.1.6.0_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)
VOSS1400.8.1.6.0.sha512	SHA512 Checksums	1401
VOSS1400.8.1.6.0.md5	MD5 Checksums	537
VOSS1400.8.1.6.0.tgz	Release 8.1.6.0 archived software distribution	320519565
VOSS1400.8.1.6.0_mib.zip	Archive of all MIB files	1160409
VOSS1400.8.1.6.0_mib.txt	MIB file	7699369
VOSS1400.8.1.6.0_mib_sup.txt	MIB file	1045164
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669

F0615-O

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 VOSS4400.8.1.6.0.tgz
software activate 8.1.6.0.GA
```

or

```
software add VOSS4900.8.1.6.0.tgz
software activate 8.1.6.0.GA
```

or

```
software add VOSS7200.8.1.6.0.tgz
software activate 8.1.6.0.GA
```

or

```
software add VOSS7400.8.1.6.0.tgz
software activate 8.1.6.0.GA
```

or

```
software add VOSS8200.8.1.6.0.tgz
software activate 8.1.6.0.GA
```

or

```
software add VOSS8400.8.1.6.0.tgz
software activate 8.1.6.0.GA
```

or

```
software add VOSS1400.8.1.6.0.tgz
software activate 8.1.6.0.GA
```

F0615-O

VERSION OF PREVIOUS RELEASE:

Virtual Services Platform 4400 Series

Software version 4.0.0.0, 4.0.0.1, 4.0.0.2, 4.0.0.3, 4.1.0.0, 4.1.0.1, 4.2.0.0, 4.2.0.1, 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.1.0.0, 6.1.1.0, 6.1.2.0, 6.1.2.1, 6.1.3.0, 6.1.3.1, 6.1.3.2, 6.1.4.0, 6.1.5.0, 6.1.6.0, 7.1.0.0, 7.1.0.1, 7.1.1.0, 7.1.2.0 , 8.0.0.0, 8.0.1.0, 8.0.5.0, 8.0.5.1, 8.0.6.0, 8.0.6.1, 8.0.7.0, 8.0.7.2, 8.1.0.0, 8.1.1.0, 8.0.8.0, 8.0.9.0, 8.1.2.0 and 8.1.5.0 for VSP 4450GSX platform

Software Version 4.0.50.0 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.1.0.0, 6.1.1.0, 6.1.2.0, 6.1.2.1, 6.1.3.0, 6.1.3.1, 6.1.3.2, 6.1.4.0, 6.1.5.0, 6.1.6.0, 7.1.0.0, 7.1.0.1, 7.1.1.0, 7.1.2.0 , 8.0.0.0, 8.0.1.0, 8.0.5.0, 8.0.5.1, 8.0.6.0, 8.0.6.1, 8.0.7.0, 8.0.7.2, 8.1.0.0, 8.1.1.0, 8.0.8.0, 8.0.9.0, 8.1.2.0 and 8.1.5.0 for VSP 4450GSX DC and VSP 4450GTS DC platforms

Software Version 4.0.40.0**,** 4.1.0.0, 4.1.0.1, 4.2.0.0, 4.2.0.1, 4.2.1.0 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.1.0.0, 6.1.1.0, 6.1.2.0, 6.1.2.1, 6.1.3.0, 6.1.3.1, 6.1.3.2, 6.1.4.0, 6.1.5.0, 6.1.6.0, 7.1.0.0 , 7.1.0.1, 7.1.1.0, 7.1.2.0 , 8.0.0.0, 8.0.1.0, 8.0.5.0, 8.0.5.1, 8.0.6.0, 8.0.6.1, 8.0.7.0, 8.0.7.2, 8.1.0.0, 8.1.1.0, 8.0.8.0, 8.0.9.0, 8.1.2.0 and 8.1.5.0 for VSP 4450GTX-HT-PWR+ platform

Virtual Services Platform 4900 Series
Software version 8.1.0.0, 8.1.1.0, 8.1.2.0 and 8.1.5.0 for VSP 4900-48P platrform

Virtual Services Platform 7200 Series

Software Version 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.1.0.0**,** 6.1.1.0, 6.1.2.0, 6.1.2.1, 6.1.3.0, 6.1.3.1, 6.1.3.2, 6.1.4.0, 6.1.5.0, 6.1.6.0, 7.1.0.0, 7.1.0.1, 7.1.1.0, 7.1.2.0 , 8.0.0.0, 8.0.1.0, 8.0.5.0, 8.0.5.1, 8.0.6.0, 8.0.6.1, 8.0.7.0, 8.0.7.2, 8.1.0.0, 8.1.1.0, 8.0.8.0, 8.0.9.0, 8.1.2.0 and 8.1.5.0 for VSP 7254XSQ and VSP 7254XTQ platforms

Virtual Services Platform 7400 Series

Software Version 8.0.1.0, 8.0.5.0, 8.0.5.1, 8.0.6.0, 8.0.6.1, 8.0.7.0, 8.0.7.2, 8.1.0.0, 8.1.1.0, 8.0.8.0, 8.0.9.0, 8.1.2.0 and 8.1.5.0 for VSP7432CQ platform

Software Version 8.0.5.0, 8.0.5.1, 8.0.6.0, 8.0.6.1, 8.0.7.0, 8.0.7.2, 8.1.0.0, 8.1.1.0, 8.0.8.0, 8.0.9.0, 8.1.2.0 and 8.1.5.0 for VSP-7400-48Y-8C platform

Virtual Services Platform 8200 Series

Software Version 4.0.0.0, 4.0.1.0, 4.0.1.1, 4.0.1.2, 4.0.1.3, 4.0.1.4, 4.1.0.0, 4.1.0.1, 4.2.0.0, 4.2.0.1, 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0**,** 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.1.0.0, 6.1.1.0, 6.1.2.0, 6.1.2.1, 6.1.3.0, 6.1.3.1, 6.1.3.2, 6.1.4.0, 6.1.5.0, 6.1.6.0, 7.1.0.0, 7.1.0.1, 7.1.1.0, 7.1.2.0 , 8.0.0.0, 8.0.1.0, 8.0.5.0, 8.0.5.1, 8.0.6.0, 8.0.6.1, 8.0.7.0, 8.0.7.2, 8.1.0.0, 8.1.1.0, 8.0.8.0, 8.0.9.0, 8.1.2.0 and 8.1.5.0 for VSP8200 platform

Virtual Services Platform 8400 Series

Software Version, 4.2.0.0, 4.2.0.1, 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.1.0.0, 6.1.1.0, 6.1.2.0**,** 6.1.2.1, 6.1.3.0, 6.1.3.1, 6.1.3.2, 6.1.4.0, 6.1.5.0, 6.1.6.0, 7.1.0.0, 7.1.0.1, 7.1.1.0, 7.1.2.0 , 8.0.0.0, 8.0.1.0, 8.0.5.0, 8.0.5.1, 8.0.6.0, 8.0.6.1, 8.0.7.0, 8.0.7.2, 8.1.0.0, 8.1.1.0, 8.0.8.0, 8.0.9.0, 8.1.2.0 and 8.1.5.0 for VSP8404 platform

Software Version, 5.3.0.0, 6.1.0.0, 6.1.1.0, 6.1.2.0, 6.1.2.1, 6.1.3.0, 6.1.3.1, 6.1.3.2, 6.1.4.0, 6.1.5.0, 6.1.6.0, 7.1.0.0, 7.1.0.1, 7.1.1.0, 7.1.2.0 , 8.0.0.0, 8.0.1.0, 8.0.5.0, 8.0.5.1, 8.0.6.0, 8.0.6.1, 8.0.7.0, 8.0.7.2, 8.1.0.0, 8.1.1.0, 8.0.8.0, 8.0.9.0, 8.1.2.0 and 8.1.5.0 for VSP8404c platform

ExtremeAccess 1400 Series
Software Version 8.1.0.0, 8.1.1.0, 8.1.50.0 and 8.1.5.0 for XA 1440 and XA 1480 platforms

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

Addition of the `sys control virtual-ist mac-move-protection` and `no sys control virtual-ist mac-move-protection` commands.

Old Features Removed From This Release
None.

Problems Resolved in This Release	
VOSS-15698	Unable to access CLI through SSH or console.
VOSS-16891	Port statistics stop incrementing after a random period of time.
VOSS-17284	EDM shows incorrect interface cost metric
VOSS-17331	Allow disabling MAC move protection.
VOSS-17487	L2VSN traffic was incorrectly filtered by inVlan ACL in 8.0+ release.
VOSS-17599	ARP spoof detect not working correctly with VRRPv3.
VOSS-17757	Node reset on exit from SSH. Some SSH clients bundle together the 'exit' command with ^Z causing exception in some scenarios.
VOSS-17781	For DVR controllers and VIST, ARP HW Records failed to be deleted and resulted in bad records.
VOSS-17791	VOSS rejects SSH connection from Dropbear SSH client.
VOSS-17815	LACP packet leak on untagged I-SIDs can lead to frequent LACP link flaps.
VOSS-17920	ISID Mirror of untagged packets on a VIST node is incorrectly flooded into BVLAN.
VOSS-17928	Fixed "show qos queue-profile 1 queue all" output on bootup.

Problems Resolved in This Release	
VOSS-18075	Memory leaks when polling an XA device for port statistics.
VOSS-18112	Setting RWAUserName in EDM does not work without setting also a new RWAPassword

Fixes from Previous Releases
VOSS 8.1.6.0 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.