Extreme networks
ADVANCE WITH US

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

# Customer Release Notes

## VSP Operating System Software

Software Release 8.2.6.0
Dec 11, 2020

## INTRODUCTION:

This document provides specific information for version 8.2.6.0 of agent software for the VSP Operating System Software.

The purpose of this version is to address customer and internally found software issues. This release also includes a couple of minor feature enhancements as indicated in the New in this Release section of this document.

Newly Purchased Switches Require Software Upgrade. You should promptly upgrade the VOSS software to the latest version available by visiting the Extreme Portal.

**IMPORTANT NOTE**: If you are using Distributed Virtual Routing (DvR) in your network, we recommend that you stay on your current software release until VOSS 8.2.7.0 is available.

**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:

1. Mask password for SNMPv3 user and web passwords in CLI.

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

3. Logging has been updated to accurately notify the user when maximum number of ECMP groups (125) is being reached on 5520. The log messages are:

- “GlobalRouter COP-SW INFO 85% of ECMP group limit reached: 106” when the 106th ECMP group is created (85% of 125 groups)

and

- “GlobalRouter COP-SW WARNING Total ECMP group limit reached: 125” when the maximum number of 5520 supported ECMP groups is reached (100% of 125 groups)

## 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 8.2.6.0 FROM PREVIOUS RELEASE:

If you have a VLAN with VRRP instance of 37 provisioned and functional on a node running with several other VLANs with DvR enabled, upon upgrade to 8.2.6.0, VRRP configuration for instance 37 is removed from that VLAN. This would result in  traffic loss for members of that VLAN. Recommend renumbering the VRRP instance IDs to values 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 VSP 4900-12MXU-12XE
- Virtual Services Platform VSP 4900-24S
- Virtual Services Platform VSP 4900-24XE

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 Platform 1440
- ExtremeAccess Platform 1480

Extreme Switching 5520 Series
- 5520-24T
- 5520-24W
- 5520-48T
- 5520-48W
- 5520-12MW-36W
- 5520-24X
- 5520-48SE

## 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.
   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 8.2.5 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) |
|---|---|---:|
| VOSS4400.8.2.6.0.sha512 | SHA512 Checksums | 1549 |
| VOSS4400.8.2.6.0.md5 | MD5 Checksums | 589 |
| VOSS4400.8.2.6.0.tgz | Release 8.2.6.0 archived software distribution | 112244078 |
| VOSS4400.8.2.6.0_mib.zip | Archive of all MIB files | 1172896 |
| VOSS4400.8.2.6.0_mib.txt | MIB file | 7793520 |
| VOSS4400.8.2.6.0_mib_sup.txt | MIB file | 1413418 |
| VOSSv820_HELP_EDM_gzip.zip | EDM Help file | 4414827 |
| restconf_yang.tgz | YANG model | 506020 |

Virtual Services Platform 4900 Series

| File Name | Module or File Type | File Size (bytes) |
|---|---|---:|
| VOSS4900.8.2.6.0.sha512 | SHA512 Checksums | 1701 |
| VOSS4900.8.2.6.0.md5 | MD5 Checksums | 645 |
| VOSS4900.8.2.6.0.tgz | Release 8.2.6.0 archived software distribution | 244678957 |
| VOSS4900.8.2.6.0_mib.zip | Archive of all MIB files | 1172896 |
| VOSS4900.8.2.6.0_mib.txt | MIB file | 7793520 |

| File Name | Module or File Type | File Size (bytes) |
|---|---|---|
| VOSS4900.8.2.6.0_mib_sup.txt | MIB file | 1436064 |
| VOSSv820_HELP_EDM_gzip.zip | EDM Help file | 4414827 |
| restconf_yang.tgz | YANG model | 506020 |
| TPVM_7400_8.2.6.0.img | Third Party Virtual Machine (TPVM) | 1677066240 |

Virtual Services Platform 7200 Series

| File Name | Module or File Type | File Size (bytes) |
|---|---|---|
| VOSS7200.8.2.6.0.sha512 | SHA512 Checksums | 1549 |
| VOSS7200.8.2.6.0.md5 | MD5 Checksums | 589 |
| VOSS7200.8.2.6.0.tgz | Release 8.2.6.0 archived software distribution | 126622603 |
| VOSS7200.8.2.6.0_mib.zip | Archive of all MIB files | 1172896 |
| VOSS7200.8.2.6.0_mib.txt | MIB file | 7793520 |
| VOSS7200.8.2.6.0_mib_sup.txt | MIB file | 1379657 |
| VOSSv820_HELP_EDM_gzip.zip | EDM Help file | 4414827 |
| restconf_yang.tgz | YANG model | 506020 |

Virtual Services Platform 7400 Series

| File Name | Module or File Type | File Size (bytes) |
|---|---|---|
| VOSS7400.8.2.6.0.sha512 | SHA512 Checksums | 1857 |
| VOSS7400.8.2.6.0.md5 | MD5 Checksums | 705 |
| VOSS7400.8.2.6.0.tgz | Release 8.2.6.0 archived software distribution | 244342438 |
| VOSS7400.8.2.6.0_mib.zip | Archive of all MIB files | 1172896 |
| VOSS7400.8.2.6.0_mib.txt | MIB file | 7793520 |
| VOSS7400.8.2.6.0_mib_sup.txt | MIB file | 1430261 |
| VOSSv820_HELP_EDM_gzip.zip | EDM Help file | 4414827 |
| restconf_yang.tgz | YANG model | 506020 |
| TPVM_7400_8.2.6.0.img | Third Party Virtual Machine (TPVM) | 1677066240 |
| FIGWVM_7400_8.2.6.0.qcow2 | Fabric Ipsec Gateway Virtual Machine | 1970339840 |

Virtual Services Platform 8200 Series

| File Name | Module or File Type | File Size (bytes) |
|---|---|---|
| VOSS8200.8.2.6.0.sha512 | SHA512 Checksums | 1549 |
| VOSS8200.8.2.6.0.md5 | MD5 Checksums | 589 |
| VOSS8200.8.2.6.0.tgz | Release 8.2.6.0 archived software distribution | 126626986 |
| VOSS8200.8.2.6.0_mib.zip | Archive of all MIB files | 1172896 |
| VOSS8200.8.2.6.0_mib.txt | MIB file | 7793520 |
| VOSS8200.8.2.6.0_mib_sup.txt | MIB file | 1379657 |

| File Name | Module or File Type | File Size (bytes) |
|---|---|---|
| VOSSv820_HELP_EDM_gzip.zip | EDM Help file | 4414827 |
| restconf_yang.tgz | YANG model | 506020 |

Virtual Services Platform 8400 Series

| File Name | Module or File Type | File Size (bytes) |
|---|---|---|
| VOSS8400.8.2.6.0.sha512 | SHA512 Checksums | 1549 |
| VOSS8400.8.2.6.0.md5 | MD5 Checksums | 589 |
| VOSS8400.8.2.6.0.tgz | Release 8.2.6.0 archived software distribution | 188114534 |
| VOSS8400.8.2.6.0_mib.zip | Archive of all MIB files | 1172896 |
| VOSS8400.8.2.6.0_mib.txt | MIB file | 7793520 |
| VOSS8400.8.2.6.0_mib_sup.txt | MIB file | 1379657 |
| VOSSv820_HELP_EDM_gzip.zip | EDM Help file | 4414827 |
| restconf_yang.tgz | YANG model | 506020 |

ExtremeAccess 1400 Series

| File Name | Module or File Type | File Size (bytes) |
|---|---|---|
| VOSS1400.8.2.6.0.sha512 | SHA512 Checksums | 1401 |
| VOSS1400.8.2.6.0.md5 | MD5 Checksums | 537 |
| VOSS1400.8.2.6.0.tgz | Release 8.2.6.0 archived software distribution | 322544170 |
| VOSS1400.8.2.6.0_mib.zip | Archive of all MIB files | 1172896 |
| VOSS1400.8.2.6.0_mib.txt | MIB file | 7793520 |
| VOSS1400.8.2.6.0_mib_sup.txt | MIB file | 1086794 |
| VOSSv820_HELP_EDM_gzip.zip | EDM Help file | 4414827 |

Extreme Switching 5520 Series

| File Name | Module or File Type | File Size (bytes) |
|---|---|---|
| 5520.8.2.6.0.sha512 | SHA512 Checksums | 1669 |
| 5520.8.2.6.0.md5 | MD5 Checksums | 558 |
| 5520.8.2.6.0.voss | Release 8.2.6.0 archived software distribution | 99131019 |
| 5520.8.2.6.0_mib.zip | Archive of all MIB files | 1172896 |
| 5520.8.2.6.0_mib.txt | MIB file | 7793520 |
| 5520.8.2.6.0_mib_sup.txt | MIB file | 1435203 |
| VOSSv820_HELP_EDM_gzip.zip | EDM Help file | 4414827 |
| 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" or ".voss" 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 5520.8.2.6.0.voss
software activate 8.2.6.0.GA
```

**or**

```
software add VOSS4400.8.2.6.0.tgz
software activate 8.2.6.0.GA
```

**or**

```
software add VOSS4900.8.2.6.0.tgz
software activate 8.2.6.0.GA
```

**or**

```
software add VOSS7200.8.2.6.0.tgz
software activate 8.2.6.0.GA
```

**or**

```
software add VOSS7400.8.2.6.0.tgz
software activate 8.2.6.0.GA
```

**or**

```
software add VOSS8200.8.2.6.0.tgz
software activate 8.2.6.0.GA
```

**or**

```
software add VOSS8400.8.2.6.0.tgz
software activate 8.2.6.0.GA
```

**or**

```
software add VOSS1400.8.2.6.0.tgz
software activate 8.2.6.0.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 |
|---|
| 1. Mask password for SNMPv3 user and web passwords in CLI.<br>2. A consistency check was added to prevent configuration of VRRP VRID 37 or 38 when DvR is enabled.<br>3. Logging has been updated to accurately notify the user when maximum number of ECMP groups (125) is being reached on 5520 |

| Old Features Removed From This Release |
|---|
| None. |

| Problems Resolved in This Release | |
|---|---|
| VOSS-19135 | Cisco IP Phone 7821 does not negotiate to 100M when connected some models of 5520. |
| VOSS-19253 | On 5520 switches, an EAP request packet using 802.1X-2010 Version 3 is not accepted on a port with EAP enabled. |
| VOSS-19255 | For 5520 switches, the output of the show software command displays an incorrect release name for VOSS 8.2.5. |
| VOSS-19261 | For 5520 switches, low is the only valid value for the command boot config flags advanced-featurebandwidth-reservation. (This command enables the switch to support advanced features by reserving ports as loopback ports.) In EDM, both options, low and high, are selectable. However, low is the only valid value. |
| VOSS-19303 | Can't create a static route in GRT with next hop leaked from ISIS. |
| VOSS-19385 | Incorrect handling of certain ARP requests will lead to incorrect programming of the default route on all DVR leaves and DVR controllers. |

| Fixes from Previous Releases |
|---|
| VOSS 8.2.6.0 incorporates all fixes from prior releases, up to and including VOSS 7.1.7.0, VOSS 8.0.9.0 and VOSS 8.1.7.0. |

## OUTSTANDING ISSUES:

Please see "Release Notes for VSP Operating System Software (VOSS)" for software release 8.2.5 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 8.2.5 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.

### 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