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

Customer Release Notes

VSP Operating System

Software Release 7.1.4.0
August 2019

INTRODUCTION:

This document provides specific information for version 7.1.4.0 of agent software for the VSP Operating System.

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 release.

PLATFORMS SUPPORTED:

Virtual Services Platform 4000 Series
- Virtual Services Platform VSP 4850GTS
- Virtual Services Platform VSP 4850GTS-PWR+
- 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 7200 Series
- Virtual Services Platform VSP 7254XSQ
- Virtual Services Platform VSP 7254XTQ

Virtual Services Platform 8000 Series
- Virtual Services Platform 8200
- Virtual Services Platform 8400

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 your networks have Zero Touch Fabric (ZTF) enabled or the ISIS L1 area is **`00.1515.fee1.900d.1515.fee1.900d`**.

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 steo 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 Future 8.x
   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 steo 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

   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:

      - Check the ISIS manual area (`show isis manual-area`).
      - 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 7.1.3.0, 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 to 7.1.3.0, 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” for software release 7.1.0, available at https://www.extremenetworks.com/support/release-notes for details regarding Known Limitations.

FILE NAMES FOR THIS RELEASE:

Virtual Services Platform 4000 Series

File Name	Module or File Type	File Size (bytes)
VOSS4K.7.1.4.0.tgz	Release 7.1.4.0 archived software distribution	143874558
VOSS4K.7.1.4.0_mib.zip	Archive of all MIB files	1118428
VOSS4K.7.1.4.0_mib.txt	MIB file	7414108
VOSS4K.7.1.4.0_mib_sup.txt	MIB file	1271682
VSP4000v711_HELP_EDM_gzip.zip	EDM Help file	3960940
VSP4000v7.1.1.0.zip	EDM plug-in for COM	5578143
VOSS4K.7.1.4.0.md5	MD5 Checksums	578
VOSS4K.7.1.4.0.sha512	SHA512 Checksums	1538

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7K.7.1.4.0.tgz	Release 7.1.4.0 archived software distribution	104520512
VOSS7K.7.1.4.0_mib.zip	Archive of all MIB files	1118428
VOSS7K.7.1.4.0_mib.txt	MIB file	7414108
VOSS7K.7.1.4.0_mib_sup.txt	MIB file	1274282
VOSSv711_HELP_EDM_gzip.zip	EDM Help file	3960940
VOSSv7.1.1.0.zip	EDM plug-in for COM	5904477
VSP7K.7.1.4.0.md5	MD5 Checksums	572
VOSS7K.7.1.4.0.sha512	SHA512 Checksums	1532

Virtual Services Platform 8000 Series

File Name	Module or File Type	File Size (bytes)
VOSS8K.7.1.4.0.tgz	Release 7.1.4.0 archived software distribution	160014558
VOSS8K.7.1.4.0_mib.zip	Archive of all MIB files	1118428
VOSS8K_7.1.4.0_mib.txt	MIB file	7414108
VOSS8K.7.1.4.0_mib_sup.txt	MIB file	1274282
VOSSv711_HELP_EDM_gzip.zip	EDM Help file	3960940
VOSSv7.1.1.0.zip	EDM plug-in for COM	5904477
VSP8K.7.1.4.0.md5	MD5 Checksums	572
VOSS8K.7.1.4.0.sha512	SHA512 Checksums	1532

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 VOSS4K.7.1.4.0.tgz
software activate VOSS4K.7.1.4.0.GA
```

or

```
software add VOSS7K.7.1.4.0.tgz
software activate VOSS7K.7.1.4.0.GA
```

or

```
software add VOSS8K.7.1.4.0.tgz
software activate VOSS8K.7.1.4.0.GA
```

VERSION OF PREVIOUS RELEASE:

Virtual Services Platform 4000 Series

Software Version 3.0.0.0, 3.0.1.0, 3.1.0.0, 3.1.0.2, 3.1.0.3, 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 and 7.1.3.0 for VSP 4850GTS platforms

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 and 7.1.3.0 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 and 7.1.3.0 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 and 7.1.3.0 for VSP 4450GTX-HT-PWR+ platform

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 and 7.1.3.0

Virtual Services Platform 8000 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 and 7.1.3.0 for VSP8200 platform

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 and 7.1.3.0 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 and 7.1.3.0 for VSP8404c platform

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

DIGICERT functionality to display default TLS certificate (self-signed):

```
show certificate cert-type default-tls-certificate

show certificate cert-type offline-subject-cert
```

Added a new field to the `show web-server` command that provides information regarding the in use certificate. The **`In use certificate field`** displays either **`None`**, **`User installed`**, or **`Self signed`**.

Old Features Removed From This Release
None.

Problems Resolved in This Release	
VOSS-13537	Attempting to redistribute a BGP route into ISIS as an external route with a route-map containing a 'match community xyz' clause, then that route is getting redistributed into ISIS to the peer device even if the match fails.
VOSS-13825	"show isis logical interface" output repeats forever.
VOSS-14029	Limit SFTP access to same as FTP according to access permissions.
VOSS-14030	Reports incorrect port num in the log when mac is corrected to point to vIST after learned on non IST port due to loop on the edge

Problems Resolved in This Release	
VOSS-14042	LLDP pdu with a TLV length greater than 32 bytes caused chassis reset. System truncates string to 32 bytes if length exceeded.
VOSS-14089	VIST Peer MAC movement log support for MLT
VOSS-14210	BGP log messages missing when BGP session goes down
VOSS-14211	For configurations using brouter interfaces as the FE tunnel endpoints: if the node learns about a non-direct route (say a default route) that encompasses the tunnel endpoint prior to the direct interface coming up the logical ISIS adjacency will fail to establish.
VOSS-14216	Unexpected error when trying to install PKCS12 file but the file does not exist in flash
VOSS-14217	Cannot install PKCS12 file if a public/private key does not already exist on the switch
VOSS-14218	A CSR can be generated with relax option when CN or SAN is configured, the error shown when neither CN nor SAN are configured should be more clear (just one of the parameters are required)
VOSS-14220	User should not be allowed to configure invalid values for the certificate SAN
VOSS-14276	Chassis reset for no reason. Fixed thread death handling.
VOSS-14278	Use of single quote in regular expression caused chassis reset.
VOSS-14315	Chassis reset after entering ‘clear telnet 0’ while logged in via telnet.
VOSS-14478	Configuration loss after reboot when MSTP-Fabric Connect Multi Homing is enabled on the SPBM instance
VOSS-14496	SSH is disabled after reboot.
VOSS-14508	ipv6 dhcp-relay fwd-path configuration lost on reboot
VOSS-14604	Add autopology nmm-table support for devices: "VSP7432CQ" "VSP7400-48Y-8C" "VSP1100" "VSP4900-24P" "VSP4900-48P" "XA1440" "XA1480"
VOSS-14719	When port is configured as tagged and Egress-VLANID is used alongside Tunnel-Private-Group-ID attribute, the tagging is taken from port level. Egress-VLANID is overwriting port level tagging only to tagged value not otherwise.

OUTSTANDING ISSUES:

Please see “Release Notes for VSP Operating System” for software release 7.1.0 available at https://www.extremenetworks.com/support/release-notes for details regarding Known Issues.

KNOWN LIMITATIONS:

Please see “Release Notes for VSP Operating System” for software release 7.1.0 available at https://www.extremenetworks.com/support/release-notes for details regarding Known Limitations.

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.

Copyright © 2019 Extreme Networks, Inc. - All Rights Reserved.

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