VSP Operating System Software Release 7.1.2.0

1. Release Summary

Release Date: April 2019
Purpose: Software release to address customer found software issues.

2. 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 section (4) below in order to avoid potential network connectivity loss.

If upgrading systems running 4.1.X releases which also have TACACS+ enabled, refer to section 4 for upgrade instructions.

If upgrading systems running 6.0.x releases or older, refer to section 4 for instruction about the need to step-through a 6.1.x release prior to going to 7.1.x release.

3. 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

4. Special Instructions for Upgrade 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).

5. Notes for Upgrade

Please see “Release Notes for VSP Operating System” for software release 6.1.0 available at https://www.extremenetworks.com/support/documentation for details on how to upgrade your Switch.

File Names For This Release

Virtual Services Platform 4000 Series

File Name	Module or File Type	File Size (bytes)
VOSS4K.7.1.2.0.tgz	Release 7.1.2.0 archived software distribution	143833696
VOSS4K.7.1.2.0_mib.zip	Archive of all MIB files	1117245
VOSS4K.7.1.2.0_mib.txt	MIB file	7408227
VOSS4K.7.1.2.0_mib_sup.txt	MIB file	1270792
VSP4000v711_HELP_EDM_gzip.zip	EDM Help file	3960940
VSP4000v7.1.1.0.zip	EDM plug-in for COM	5578143
VOSS4K.7.1.2.0.md5	MD5 Checksums	578
VOSS4K.7.1.2.0.sha512	SHA512 Checksums	1538

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7K.7.1.2.0.tgz	Release 7.1.2.0 archived software distribution	104503150
VOSS7K.7.1.2.0_mib.zip	Archive of all MIB files	1117245
VOSS7K.7.1.2.0_mib.txt	MIB file	7408227
VOSS7K.7.1.2.0_mib_sup.txt	MIB file	1274420
VOSSv711_HELP_EDM_gzip.zip	EDM Help file	3960940
VOSSv7.1.1.0.zip	EDM plug-in for COM	5904477
VSP7K.7.1.2.0.md5	MD5 Checksums	572
VOSS7K.7.1.2.0.sha512	SHA512 Checksums	1532

Virtual Services Platform 8000 Series

File Name	Module or File Type	File Size (bytes)
VOSS8K.7.1.2.0.tgz	Release 7.1.2.0 archived software distribution	159956579
VOSS8K.7.1.2.0_mib.zip	Archive of all MIB files	1117245
VOSS8K_7.1.2.0_mib.txt	MIB file	7408227
VOSS8K.7.1.2.0_mib_sup.txt	MIB file	1274420
VOSSv711_HELP_EDM_gzip.zip	EDM Help file	3960940
VOSSv7.1.1.0.zip	EDM plug-in for COM	5904477
VSP8K.7.1.2.0.md5	MD5 Checksums	572
VOSS8K.7.1.2.0.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.7.1.2.0.tgz
software activate VOSS4K.7.1.2.0.GA

or

software add VOSS7K.7.1.2.0.tgz
software activate VOSS7K.7.1.2.0.GA

or

software add VOSS8K.7.1.2.0.tgz
software activate VOSS8K.7.1.2.0.GA

6. 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 and 7.1.1.0 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 and 7.1.1.0 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 and 7.1.1.0 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 and 7.1.1.0 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 and 7.1.1.0

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 and 7.1.1.0 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 and 7.1.1.0 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 and 7.1.1.0 for VSP8404c platform

7. Compatibility

8. Changes in 7.1.2.0

New Features in This Release

New operational CLI command to remove MAC entries that are marked as Remote true on both VIST peers.

"clear mac-address-table remote"

Old Features Removed From This Release

Problems Resolved in This Release

ID	Description
VOSS-11672	NTP auth passwords that contain the quotation mark (") symbol are not accepted.
VOSS-11841	Add timestamp display with show command outputs.
VOSS-11976	DIGICERT generate-csr subject Allows Country Value Greater Than Two Characters.
VOSS-12029	PIMGW - IGMPv3 - traffic not forwarded to remote PIM v3 rcvr after bounce spb sender port.
VOSS-12155	Intermittently, EDM is stuck on blank page after providing the credentials in the EDM login page.
VOSS-12342	"Insufficient VFI/VPN resources to create McoSpb source" messages are observed after the upgrade.
VOSS-12372	Polling MIB lldpXMedRemSerialNum can cause node reset.
VOSS-12404	LACP key config at port interface lost after reboot when used with LST.
VOSS-12434	FE Adjacency stuck in "init" state when tunnel endpoint is reachable via default route.
VOSS-12487	Remove warning when no Certificate Subject country is required.
VOSS-12517	Crash seen while executing 'isis apply redistribute' command.
VOSS-12539	Upgrade issue from 7.1.0.0 or 7.1.1.0 to 8.0 in VSPSim.
VOSS-12582	Password containing 22 characters cores switch.
VOSS-12606	Crash in rcip_route_notify_app while system shutting down coincides with SPF calculation.
VOSS-12769	Outbound RADIUS Access-Request Does Not Include NAS-Port-Type.
VOSS-12787	Invalid slowProtocolRx: PDUs with Dest Mac 01:80:c2:00:00:02 and Version = 0 trigger backtraces. Disable backtrace but keep log message.
VOSS-12806	Network disruption due to network security scan.
VOSS-12835	Not learning ARP of NLB cluster VIP when in NLB-Multicast mode. Introduced in 7.0.0.0.
VOSS-13008	EDM session is not accessible when logged out from different browser on the same PC
VSP4000-245	SMLT Remote True condition on both the vIST peers. New command added to remove MAC entries that are marked as Remote true on both VIST peers "clear mac-address-table remote".

VSP7200-73	"GlobalRouter ISIS ERROR isisCheckAndSlide: TLV overflow del tlv 186 error" due to heavy multicast stream thrashing.
VSP8000-350	TACACS+ receiving unsupported frame causes node reset.
VSP8000-363	Lifecycle Crash Reporter: Process Name: cbcp-main.x, Thread Name: tTacacspTask, Signal 6, Slot: 1, PID 4876, LWP: 5071.
VSP8000-370	ssio process crash due to socket error handling.
VSP8000-373	IGMP Static Group configuration lost after VOSS upgrade from 6.0.1.2 -> 6.1.0.0 -> 7.1.

9. 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.

10. 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.

Regular cleanup of unneeded files on USB drives is recommended to minimize possibility of USB corruption when a system is reset, shutdown or power is lost.

11. Documentation Corrections

For other known issues, please refer to the product release notes and technical documentation available at: https://www.extremenetworks.com/support/documentation.