Extreme
networks®

ADVANCE WITH US

Customer Release Notes

VSP Operating System Software
Software Release 8.5.1.0
April, 2022

INTRODUCTION:

This document provides specific information for version 8.5.1.0 of agent software for the VSP Operating System Software.

The purpose of this version is to address customer and internally found software issues.

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

> **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:

Please see "New Features in this release" section below for more information.

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.

If upgrading systems running versions prior than 8.5.1.0, refer to the section *SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES* for instructions about the possible need to renumber VRRP instances.

UPGRADE CONSIDERATIONS WHEN UPGRADING TO 8.5.1.0 FROM PREVIOUS RELEASES:

For DVR deployments refer also to Outstanding Issues Section before upgrading.

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 8.5.1.0, 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:

Please see "Release Notes for VSP Operating System Software (VOSS)" for software release 8.5.0 available at https://www.extremenetworks.com/support/release-notes for details regarding supported platforms.

SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES:

I. 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
```

II. 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.

III. 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.

IV. 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). Then upgrade to the desired 7.x+ release (Release 7.1.10.0 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.

V. 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.

VI. 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.

VII. 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 8.5.0 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)
VOSS1400.8.5.1.0_edoc.tar	Logs Reference	63969280
VOSS1400.8.5.1.0.md5	MD5 Checksums	424
VOSS1400.8.5.1.0_mib_sup.txt	MIB - supported object names	1140608
VOSS1400.8.5.1.0_mib.txt	MIB - objects in the OID compile order	8104087
VOSS1400.8.5.1.0_mib.zip	Archive of all MIB files	1212658
VOSS1400.8.5.1.0_oss-notice.html	Open source software - Master copyright file	2781384

File Name	Module or File Type	File Size (bytes)
VOSS1400.8.5.1.0_edoc.tar	Logs Reference	63969280
VOSS1400.8.5.1.0.sha512	SHA512 Checksums	1247
VOSS1400.8.5.1.0.tgz	Release 8.5.1.0 archived software distribution	326339727
VOSSv850_HELP_EDM_gzip.zip	EDM Help file	5066214

Virtual Services Platform 4400 Series

File Name	Module or File Type	File Size (bytes)
restconf_yang.tgz	YANG model	506020
VOSS4400.8.5.1.0_edoc.tar	Logs reference	63969280
VOSS4400.8.5.1.0.md5	MD5 Checksums	476
VOSS4400.8.5.1.0_mib_sup.txt	MIB - supported object names	1482261
VOSS4400.8.5.1.0_mib.txt	MIB - objects in the OID compile order	8104087
VOSS4400.8.5.1.0_mib.zip	Archive of all MIB files	1212658
VOSS4400.8.5.1.0_oss-notice.html	Open source software - Master copyright file	2781384
VOSS4400.8.5.1.0.sha512	SHA512 Checksums	1395
VOSS4400.8.5.1.0.tgz	Release 8.5.1.0 archived software distribution	112813954
VOSSv850_HELP_EDM_gzip.zip	EDM Help file	5066214

Virtual Services Platform 4900 Series

File Name	Module or File Type	File Size (bytes)
FabricIPSecGW_VM_5.1.0.0.ova	Fabric Ipsec Gateway Virtual Machine	4016721920
restconf_yang.tgz	YANG model	506020
TPVM_4900_8.4.0.0.img	Third Party Virtual Machine (TPVM)	1677066240
VOSS4900.8.5.1.0_edoc.tar	Logs reference	63969280
VOSS4900.8.5.1.0.md5	MD5 Checksums	595
VOSS4900.8.5.1.0_mib_sup.txt	MIB - supported object names	1506037
VOSS4900.8.5.1.0_mib.txt	MIB - objects in the OID compile order	8104087
VOSS4900.8.5.1.0_mib.zip	Archive of all MIB files	1212658
VOSS4900.8.5.1.0_oss-notice.html	Open source software - Master copyright file	2781384
VOSS4900.8.5.1.0.sha512	SHA512 Checksums	1706
VOSS4900.8.5.1.0.tgz	Release 8.5.1.0 archived software distribution	259842487
VOSSv850_HELP_EDM_gzip.zip	EDM Help file	5066214

Extreme Switching 5420 Series

File Name	Module or File Type	File Size (bytes)
5420.8.5.1.0_edoc.tar	Logs reference	63969280
5420.8.5.1.0.md5	MD5 Checksums	453
5420.8.5.1.0_mib_sup.txt	MIB - supported object names	1501278

File Name	Module or File Type	File Size (bytes)
5420.8.5.1.0_mib.txt	MIB - objects in the OID compile order	8104087
5420.8.5.1.0_mib.zip	Archive of all MIB files	1212658
5420.8.5.1.0_oss-notice.html	Open source software - Master copyright file	2781384
5420.8.5.1.0.sha512	SHA512 Checksums	1368
5420.8.5.1.0.voss	Release 8.5.1.0 archived software distribution	97700649
restconf_yang.tgz	YANG model	506020
VOSSv850_HELP_EDM_gzip.zip	EDM Help file	5066214

Extreme Switching 5520 Series

File Name	Module or File Type	File Size (bytes)
5520.8.5.1.0_edoc.tar	Logs reference	63969280
5520.8.5.1.0.md5	MD5 Checksums	453
5520.8.5.1.0_mib_sup.txt	MIB - supported object names	1501835
5520.8.5.1.0_mib.txt	MIB - objects in the OID compile order	8104087
5520.8.5.1.0_mib.zip	Archive of all MIB files	1212658
5520.8.5.1.0_oss-notice.html	Open source software - Master copyright file	2781384
5520.8.5.1.0.sha512	SHA512 Checksums	1368
5520.8.5.1.0.voss	Release 8.5.1.0 archived software distribution	101180255
restconf_yang.tgz	YANG model	506020
VOSSv850_HELP_EDM_gzip.zip	EDM Help file	5066214

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
restconf_yang.tgz	YANG model	506020
VOSS7200.8.5.1.0_edoc.tar	Logs reference	63969280
VOSS7200.8.5.1.0.md5	MD5 Checksums	476
VOSS7200.8.5.1.0_mib_sup.txt	MIB - supported object names	1446753
VOSS7200.8.5.1.0_mib.txt	MIB - objects in the OID compile order	8104087
VOSS7200.8.5.1.0_mib.zip	Archive of all MIB files	1212658
VOSS7200.8.5.1.0_oss-notice.html	Open source software - Master copyright file	2781237
VOSS7200.8.5.1.0.sha512	SHA512 Checksums	1395
VOSS7200.8.5.1.0.tgz	Release 8.5.1.0 archived software distribution	127576871
VOSSv850_HELP_EDM_gzip.zip	EDM Help file	5066214

Virtual Services Platform 7400 Series

File Name	Module or File Type	File Size (bytes)
FabricIPSecGW_VM_5.1.0.0.ova	Fabric Ipsec Gateway Virtual Machine	4016721920
restconf_yang.tgz	YANG model	506020

File Name	Module or File Type	File Size (bytes)
TPVM_7400_8.4.0.0.img	Third Party Virtual Machine (TPVM)	1677066240
VOSS7400.8.5.1.0_edoc.tar	Logs reference	63969280
VOSS7400.8.5.1.0.md5	MD5 Checksums	595
VOSS7400.8.5.1.0_mib_sup.txt	MIB - supported object names	1499439
VOSS7400.8.5.1.0_mib.txt	MIB - objects in the OID compile order	8104087
VOSS7400.8.5.1.0_mib.zip	Archive of all MIB files	1212658
VOSS7400.8.5.1.0_oss-notice.html	Open source software - Master copyright file	2781384
VOSS7400.8.5.1.0.sha512	SHA512 Checksums	1706
VOSS7400.8.5.1.0.tgz	Release 8.5.1.0 archived software distribution	259534102
VOSSv850_HELP_EDM_gzip.zip	EDM Help file	5066214

Virtual Services Platform 8200 Series

File Name	Module or File Type	File Size (bytes)
restconf_yang.tgz	YANG model	506020
VOSS8200.8.5.1.0_edoc.tar	Logs reference	63969280
VOSS8200.8.5.1.0.md5	MD5 Checksums	476
VOSS8200.8.5.1.0_mib_sup.txt	MIB - supported object names	1446753
VOSS8200.8.5.1.0_mib.txt	MIB - objects in the OID compile order	8104087
VOSS8200.8.5.1.0_mib.zip	Archive of all MIB files	1212658
VOSS8200.8.5.1.0_oss-notice.html	Open source software - Master copyright file	2781384
VOSS8200.8.5.1.0.sha512	SHA512 Checksums	1395
VOSS8200.8.5.1.0.tgz	Release 8.5.1.0 archived software distribution	127578864
VOSSv850_HELP_EDM_gzip.zip	EDM Help file	5066214

Virtual Services Platform 8400 Series

File Name	Module or File Type	File Size (bytes)
restconf_yang.tgz	YANG model	506020
VOSS8400.8.5.1.0_edoc.tar	Logs reference	63969280
VOSS8400.8.5.1.0.md5	MD5 Checksums	476
VOSS8400.8.5.1.0_mib_sup.txt	MIB - supported object names	1446753
VOSS8400.8.5.1.0_mib.txt	MIB - objects in the OID compile order	8104087
VOSS8400.8.5.1.0_mib.zip	Archive of all MIB files	1212658
VOSS8400.8.5.1.0_oss-notice.html	Open source software - Master copyright file	2781384
VOSS8400.8.5.1.0.sha512	SHA512 Checksums	1395
VOSS8400.8.5.1.0.tgz	Release 8.5.1.0 archived software distribution	190283365
VOSSv850_HELP_EDM_gzip.zip	EDM Help file	5066214

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 VOSS1400.8.5.1.0.tgz
software activate 8.5.1.0.GA
```

or
```
software add VOSS4400.8.5.1.0.tgz
software activate 8.5.1.0.GA
```

or
```
software add VOSS4900.8.5.1.0.tgz
software activate 8.5.1.0.GA
```

or
```
software add 5420.8.5.1.0.voss
software activate 8.5.1.0.GA
```

or
```
software add 5520.8.5.1.0.voss
software activate 8.5.1.0.GA
```

or
```
software add VOSS7200.8.5.1.0.tgz
software activate 8.5.1.0.GA
```

or
```
software add VOSS7400.8.5.1.0.tgz
software activate 8.5.1.0.GA
```

or
```
software add VOSS8200.8.5.1.0.tgz
software activate 8.5.1.0.GA
```

or
```
software add VOSS8400.8.5.1.0.tgz
software activate 8.5.1.0.GA
```

COMPATIBILITY:

This software release is managed with Enterprise Device Manager (EDM), which is integrated into the agent software.

CHANGES IN THIS RELEASE:

F0615-O

New Features in This Release
None.

Old Features Removed From This Release
None.

Problems Resolved in This Release	
VOSS-22909	Filter ACL get applied to wrong I-SID (lowest) on DVR leaf
VOSS-22992	VSP7400: IPsec channel stability issues on the FIGW when oversubscription from a branch XA1400 is present on one channel that affects other channels on the FIGW *Note: the fix for this issue is included in FabricIPSecGW_VM_5.1.0.0.ova*
VOSS-23103	After 497 days, uptime counter rollover, CPU utilization rises and switch loses connection to devices
VOSS-23367	Intermittent incorrect ARP learning after initial vIST sync
VOSS-24852	ProxyDHCP requests are dropped when DHCP snooping is enabled
VOSS-24856	DVR leaf: Default route is programmed incorrectly for a new VRF
VOSS-24945	SFLOW and App Telemetry packets processed by CP causes slow SNMP responses when 32-bit static route is used for SFLOW collector
VOSS-24959	Added an instrumentation code for an unexpected reboot of VSPs
VOSS-24999	The switch crashed when an SSH session is "challenged" by Radius and the user does not enter any input
VOSS-25081	A port configured as a switched UNI, passes traffic even when not EAP-authenticated
VOSS-25094	Removing VRRP configuration does not clean up "ip vrrp version 2" from switch configuration
VOSS-25180	When a loopback interface is configured with a name, all subsequent interfaces inherit that loopback interface name
VOSS-25194	Enhanced the output for "show khi performance rx-queue" with new counters for queues and packet types; enhanced the log stating that 60 percent of fbufs are in use by outlining the packet types in the most utilized queue
VOSS-25196	XA1480 Aggregation box rebooted
VOSS-25197	XA1400 - slow memory depletion caused by the IPSEC/Charon process
VOSS-25198	Connectivity loss in user vlan when user vlan co-exists with mgmt vlan with no ip assigned to mgmt vlan manually or via mgmt dhcp-client
VOSS-25199	Printer cannot access network when directly connected to auto-sense onboarding vsp setup port
VOSS-25200	Inconsistent Auto-Negotiation values on 10G SFP+ connected VIM Ports
VOSS-25201	Port goes to TRUSTED by using the UNTRUSTED command
VOSS-25202	Multicast over FE over multi-area not working consistently
VOSS-25203	Unable to login to 5520-VOSS after power outage
VOSS-25204	Fulltech does not complete due to "show debug-files" error
VOSS-25205	TACACS authentication using Single connection mode option fails with VSP switches. Authentication is successful when using TACACS Multiple connection mode
VOSS-25206	An OSPF SPF-run in a VRF requires enabling OSPF in GRT
VOSS-25213	DVR controller: cluster pair rebooted with core dump due to high memory utilization
VOSS-25215	VMem reached critical level of 90% utilization and crashed without DVR WARNING messages when receiving the same ARP on a different port of an MLT where it had been previously learned
VOSS-25216	Around 1/3rd of ISID RSPAN mirrored traffic not reaching monitoring server
VOSS-25218	Core file is generated when a BFD packet is allocated multiple times - "VMem reached critical level of 90% utilization"

Problems Resolved in This Release	
VOSS-25243	OOM crash "90% utilization on x86 for process cbcp-main.x" in Multi-Area L2 Mac Sync
VOSS-25252	On Board Extreme Device Manager is not displaying routes for ISIS Remote Areas
VOSS-25298	MACsec MKA profile 1 is not shown with "show macsec mka profile" command
VOSS-25489	Traps are not sent when a non-powered PSU is inserted, or when the power supply is faulty
VOSS-25512	SPB MultiArea: IPMC: not working due to out of range I-SID
VOSS-25536	Core file is generated when UdpPortFwdTbl is accessed from a show operation.
VOSS-25558	CLI command "show isis spbm multicast-fib summary" gives wrong output

Fixes from Previous Releases
VOSS 8.5.1.0 incorporates all fixes from prior releases, up to and including VOSS 7.1.10.0, VOSS 8.0.9.0, VOSS 8.1.10.0, VOSS 8.2.8.0, VOSS 8.3.1, VOSS 8.4.3.0 and VOSS 8.5.0.

OUTSTANDING ISSUES:

Please see "Release Notes for VSP Operating System Software (VOSS)" for software release 8.5.0 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>*
VOSS-21358	Extended presence of a duplicate host may lead to a DP-CP discrepancy on controllers in other domains after the duplicate is resolved. This may impact traffic originating in the other domains towards the impacted host

KNOWN LIMITATIONS:

Please see "Release Notes for VSP Operating System Software (VOSS)" for software release 8.5.0 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, shut down, or power is lost.

VOSS-22530	Certain VOIP phone models may send tagged LLDP frames, or once the MED is sent by VOSS, the phone will begin transmitting tagged LLDP frames. VOSS only supports untagged LLDP frames. For proper LLDP/Auto-sense functionality, the phone must be configured to send untagged LLDP frames only."

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.