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

Customer Release Notes

VSP Operating System

Software Release 8.0.6.0
August 2019

INTRODUCTION:

This document provides specific information for version 8.0.6.0 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 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 or newer.

PLATFORMS SUPPORTED:

Virtual Services Platform 4450 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 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 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:

3. 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.

4. 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.

5. 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 6, 7, and 8 if the ISIS L1 area is **`00.1515.fee1.900d.1515.fee1.900d`**, 00.0000.0000 or all zero's.

6. 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.

7. 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.

8. 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 8.0.x available at https://www.extremenetworks.com/support/release-notes for details regarding Known Limitations.

FILE NAMES FOR THIS RELEASE:

Virtual Services Platform 4450 Series

File Name	Module or File Type	File Size (bytes)
VOSS4K.8.0.6.0.sha512	SHA512 Checksums	1533
VOSS4K.8.0.6.0.md5	MD5 Checksums	573
VOSS4K.8.0.6.0.tgz	Release 8.0.6.0 archived software distribution	123612985
VOSS4K.8.0.6.0_mib.zip	Archive of all MIB files	1145321
VOSS4K.8.0.6.0_mib.txt	MIB file	7593099
VOSS4K.8.0.6.0_mib_sup.txt	MIB file	1528108
VOSSv805_HELP_EDM_gzip.zip	EDM Help file	4108500
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7K.8.0.6.0.sha512	SHA512 Checksums	1533
VOSS7K.8.0.6.0.md5	MD5 Checksums	573
VOSS7K.8.0.6.0.tgz	Release 8.0.6.0 archived software distribution	137734567
VOSS7K.8.0.6.0_mib.zip	Archive of all MIB files	1145321
VOSS7K.8.0.6.0_mib.txt	MIB file	7593099
VOSS7K.8.0.6.0_mib_sup.txt	MIB file	1331178
VOSSv805_HELP_EDM_gzip.zip	EDM Help file	4108500
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 7400 Series

File Name	Module or File Type	File Size (bytes)
VOSS7400.8.0.6.0.sha512	SHA512 Checksums	1859
VOSS7400.8.0.6.0.md5	MD5 Checksums	707
VOSS7400.8.0.6.0.tgz	Release 8.0.6.0 archived software distribution	246570493
VOSS7400.8.0.6.0_mib.zip	Archive of all MIB files	1145321
VOSS7400.8.0.6.0_mib.txt	MIB file	7593099
VOSS7400.8.0.6.0_mib_sup.txt	MIB file	1341187
VOSS7400v800_HELP_EDM_gzip.zip	EDM Help file	4088502
restconf_yang.tgz	YANG model	506020
TPVM_7400_8.0.6.0.img	Third Party Virtual Machine (TPVM)	1677066240
purview_7400_8.0.6.0.ova	Purview Engine Virtual Appliance	1778386432

Virtual Services Platform 8000 Series

File Name	Module or File Type	File Size (bytes)
VOSS8K.8.0.6.0.sha512	SHA512 Checksums	1533
VOSS8K.8.0.6.0.md5	MD5 Checksums	573
VOSS8K.8.0.6.0.tgz	Release 8.0.6.0 archived software distribution	214009762
VOSS8K.8.0.6.0_mib.zip	Archive of all MIB files	1145321
VOSS8K.8.0.6.0_mib.txt	MIB file	7593099
VOSS8K.8.0.6.0_mib_sup.txt	MIB file	1331178
VOSSv805_HELP_EDM_gzip.zip	EDM Help file	4108500
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" 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.8.0.6.0.tgz
software activate VOSS4K.8.0.6.0.GA
```

or

```
software add VOSS7K.8.0.6.0.tgz
software activate VOSS7K.8.0.6.0.GA
```

or

```
software add VOSS7400.8.0.6.0.tgz
software activate VOSS7400.8.0.6.0.GA
```

or

```
software add VOSS8K.8.0.6.0.tgz
software activate VOSS8K.8.0.6.0.GA
```

VERSION OF PREVIOUS RELEASE:

Virtual Services Platform 4000 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 and 8.0.5.1 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 and 8.0.5.1 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 and 8.0.5.1 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 , 8.0.0.0, 8.0.1.0, 8.0.5.0 and 8.0.5.1

Virtual Services Platform 7400 Series

Software Version 8.0.1.0, 8.0.5.0 and 8.0.5.1 for VSP7432CQ platform

Software Version 8.0.5.0 and 8.0.5.1 for VSP-7400-48Y-8C platform

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 , 8.0.0.0, 8.0.1.0, 8.0.5.0 and 8.0.5.1 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 , 8.0.0.0, 8.0.1.0, 8.0.5.0 and 8.0.5.1 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 and 8.0.5.1 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

Configuration Changes

- The `untag-port-default-vlan` setting now allowed for MLT members.
- VLAN ISID mapping to existing ISID now generates warning message.

```
VSP-7254XSQ:1(config)#vlan i-sid 10 20
Error: I-SID is already assigned to a VLAN
```

Remove the mapping before assigning.

```
VSP-7254XSQ:1(config)#no vlan i-sid 10
VSP-7254XSQ:1(config)#vlan i-sid 10 20
VSP-7254XSQ:1(config)#
```

Certificate Enhancements

- Added SAN support.
- Added relaxed mode CSR generation for less restrictive consistency checks and SAN inclusion in the CSR.
- Added relaxed mode offline subject certificate installation for less restrictive consistency checks and new PKCS12 support.
- Added DIGICERT functionality to display the default TLS certificate (self-signed).

New Commands

- `show certificate subject-alternative-name`
- `no/default certificate subject-alternative-name` - Delete all SAN table entries.
- `certificate subject-alternative-name <type> <name>` - Where <type> in {dns, e-mail, ip} and <name> is the actual alternative name to add to SAN table.
- `no certificate subject-alternative-name <type> <name>` - Remove specific entry from SAN table.
- `show certificate cert-type default-tls-certificate`
- `show certificate cert-type offline-subject-cert`

New Features in This Release

Modified Commands

- `certificate generate-csr`
  - Added new `relaxed` option.
- `certificate  install-file offline-subject-filename <cert_name>`
  - Added new `relaxed` option.
- `certificate  install-file offline-subject-filename <cert_name> relaxed`
  - Added new `pkcs12-password` option. It installs a PKCS12 format certificate and secret key in relaxed mode.
- `certificate  install-file offline-subject-filename <cert_name> relaxed pkcs12-password`
  - Added new WORD<1-128> option. It represents the password for extracting the PKCS12 container.
- `show web-server`
  - Added new In use certificate field for providing information about the currently used certificate. Output will either be None, User installed, or Self signed.

MIB Changes

rcDigitalCertGenerateCsr OBJECT-TYPE

SYNTAX INTEGER {

generate (1),

notApplicable (2)

}

MAX-ACCESS read-write

STATUS current

DESCRIPTION "Generates the Certificate Signing Request required to obtain the Offline Subject Certificate

SNMP get for this object will always return notApplicable(2) because it is only meaningful in the context of 'generate-csr' command"

DEFVAL { notApplicable }

::= { rcDigitalCertScalars 12 }

rcDigitalCertRelaxedMode OBJECT-TYPE

SYNTAX INTEGER {

relaxed (1),

notApplicable (2)

}

MAX-ACCESS read-write

STATUS current

DESCRIPTION "Used in conjunction with rcDigitalCertGenerateCsr or rcDigitalCertInstallFile & rcDigitalCertInstallFileName(for offlineSubjectCert only) to:

- allow generation of CSR without setting all certificate subject fields by relaxing consistency checks;

- allow inclusion of Subject Alternative Names(SAN) in CSR

- allow installing certificates(offlineSubjectCert only) not only in DER but PKCS12 format as well with the following minimal restrictions:

- either Subject Common Name or SAN must be configured

- only those Certificate Subject fields(subset of rcDigitalCertScalars 1 -> 7) present in rcDigitalCertInstallFileName(offlineSubjectCert

about to be installed) are matched against their counterparts configured on box

Ignored if used in a different context than the 2 previously mentioned(with rcDigitalCertGenerateCsr or rcDigitalCertInstallFile)

```
                SNMP get for this object will always return notApplicable(2) because it is only meaningful in the
context of 'generate-csr' or
                'install-file offline-subject-filename' commands
                "
        DEFVAL      { notApplicable }
        ::= { rcDigitalCertScalars 13 }

rcDigitalCertPkcs12Password  OBJECT-TYPE
        SYNTAX      DisplayString   (SIZE(1..128))
        MAX-ACCESS    read-write
        STATUS      current
        DESCRIPTION   "Password to be used for PKCS12 container extraction; a SNMP get will always return
'******' for this object (security reasons)
                Used in conjunction with rcDigitalCertRelaxedMode & rcDigitalCertInstallFile &
rcDigitalCertInstallFileName(for offlineSubjectCert only)
                otherwise it is ignored.
                Allows installing offlineSubjectCert and private key in the form of a PKCS12 container"
        DEFVAL      { "******" }
        ::= { rcDigitalCertScalars 14 }
--
-- Digital certificate SAN section
--
rcDigitalCertSanTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF RcDigitalCertSanEntry
        MAX-ACCESS    not-accessible
        STATUS      current
        DESCRIPTION   "table containing Subject Alternative Names used in csr generation"
        ::= { rcDigitalCertObjects 6 }

rcDigitalCertSanEntry OBJECT-TYPE
        SYNTAX        RcDigitalCertSanEntry
        MAX-ACCESS      not-accessible
        STATUS        current
        DESCRIPTION     "Subject Alternative Names table entry"
        INDEX         { rcDigitalCertSanType, rcDigitalCertSanName }
        ::= { rcDigitalCertSanTable 1 }
```

```
RcDigitalCertSanEntry ::=
    SEQUENCE {
        rcDigitalCertSanType       INTEGER,
        rcDigitalCertSanName       DisplayString,
        rcDigitalCertSanRowStatus  RowStatus
    }

rcDigitalCertSanType OBJECT-TYPE
    SYNTAX        INTEGER {
                  -- otherName(0),
                  -- x400Address(3),
                  -- directoryName(4),
                  -- ediPartyName(5),
                  -- uniformResourceIdentifier(6),
                  -- registeredID(8),
                  rfc822Name(1),
                  dNSName(2),
                  iPAddress(7)
                 }
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION   "Type of current Alternative Name as per RFC 5280"
    ::= { rcDigitalCertSanEntry 1 }

rcDigitalCertSanName OBJECT-TYPE
    SYNTAX        DisplayString (SIZE (1..255))
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION   "Alternative name; combination rcDigitalCertSanType + rcDigitalCertSanName is
unique"
    ::= { rcDigitalCertSanEntry 2 }

rcDigitalCertSanRowStatus OBJECT-TYPE
    SYNTAX        RowStatus
```

New Features in This Release

MAX-ACCESS read-create

STATUS current

DESCRIPTION "Used to create/delete entries in rcDigitalCertSanTable"

::= { rcDigitalCertSanEntry 3 }

--

-- end of Digital certificate SAN section

--

Zero Touch Fabric (ZTF) Changes

Changed the ZTF area from `00.0000.0000` to `00.1515.fee1.900d.1515.fee1.900d.`

- Manual area can be changed dynamically (without disabling ISIS) only when the area is ZTF.
- The last manual area cannot be deleted when ISIS is enabled.

Old Features Removed From This Release

None.

Problems Resolved in This Release	
VOSS-13158	Certificate Enhancements - relax consistency checks for CSR generation by introducing a new 'relaxed' mode for installing them via 'certificate generate-csr relaxed' command; - Relaxed mode also allows for adding SANs (Subject Alternative Names) to CSR - support for PKCS12
VOSS-13185	VIST staying up on VSP8600 even when VIST peer is rebooted or powered off.
VOSS-13193	MPLS packets with EtherType 0x8847 are not passing over a T-UNI, other EtherTypes work.
VOSS-13194	ISIS adjacency not coming up for manual-area “00.0000”
VOSS-13754	Chassis may reset during ARP cleanup.
VOSS-13792	VIST may not come up after deleting and reconfiguring DVR leaf VIST.
VOSS-13713	"show isis spbm ip-multicast detail" for long egress port list may cause chassis to reset. If list exceeds the length of the buffer, "..." is appended to the output display.
VOSS-13731	LLDP neighbor content is not displayed for back to back port connections.
VOSS-13797	Changed traces that were using VERY_TERSE level to TERSE level in PLSB FIB.
VOSS-13783	DVR leaf reports DVR ERROR L3_ENTRY table limit reached. Error counting resources.
VOSS-13825	"show isis logical interface" output repeats forever.

Problems Resolved in This Release	
VOSS-13835	GlobalRouter IPMC ERROR Insufficient VFI/VPN resources to create McoSpb source
VOSS-13860	Chassis reset during ARP age out.
VOSS-13893	VLAN I-SID mapping can be overwritten without warning message
VOSS-13944	stp-multi-homing generates error messages and messages about unknown port
VOSS-13945	stp-multi-homing shows unknown port in "show spanning-tree config"
VOSS-13977	Chassis reset during ARP deletion
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
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-14056	Resource manager leak when VRF is deleted. Seen when enabling/disabling DVR controller Following logs maybe seen: CP1 [05/24/19 02:57:19.973:EDT] 0x001087d7 00000000 GlobalRouter RCIP6 INFO 85% of route limit reached for combined ipv4/v6 routes: total(13383), ipv4(3), ipv6 <=64 prefix length(6690)
VOSS-14064	“clear dvr host-entries” command may cause chassis reset.
VOSS-14068	Allow untag-port-default-vlan for MLT/LACP trunks
VOSS-14107	“no ssh encryption” configuration truncated in saved config
VOSS-14148	Missing GRT default route when DVR Controller Leaf Link bounce.
VOSS-14200	After rebooting VSP7254XSQ a QSFP+ card won’t come up without re-plugging.
VOSS-14210	BGP log messages missing when BGP session goes down
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

Problems Resolved in This Release	
VOSS-14267	Two DVR controllers reset following 95% memory utilization. Excessive control messages cause memory leak. Log messages added to indicate state of DBsync Message queue: EventCode: 0x00390606 AlarmId: <0x00000000> AlarmStatus: <ALARM_NONE> ModuleName: <MOD_DBSYNC> Severity: <S_WARNING> TerseMsg: <"Message queue length from DB Sync to tMain reached warning threshold"> ProbableCause: <"CPU utilization is high"> Remedy: <"Check alarm status and network configuration"> EventCode: 0x00390607 AlarmId: <0x00000000> AlarmStatus: <ALARM_NONE> ModuleName: <MOD_DBSYNC> Severity: <S_WARNING> TerseMsg: <"Message queue length from DB Sync to tMain threshold cleared "> ProbableCause: <"This message indicates that the queue length has returned to normal operating range"> Remedy: <"No action required">
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. Use of single quote caused reset.
VOSS-14366	Sunon fans generate many fault on VSP7432 and VSP7448 platforms.
VOSS-14373	DVR dbsync queue full messages when flapping same IP with 2 MACs
VOSS-14396	Unable to provision more than 24 VRFs with Genlic license.
VOSS-14444	100gigER4-Lite optic support.
VOSS-14484	Not all DVR host-entries are relearned by all BEBs when “clear dvr host-entries” command is issued.
VOSS-14496	SSH is disabled after reboot.
VOSS-14508	ipv6 dhcp-relay fwd-path configuration lost on reboot
VOSS-14585	VSP7K platforms may not automatically reset after a core dump.
VOSS-14587	Starting multiple VMs results in CPU usage overlap with VOSS and other VMs. VOSS processes affected by VMs
VOSS-14608	VSP7432, VSP7448 Fan tray unit2 operational message and alarm message missing
VOSS-14679	Add one alarm per DVR arp/mac flapping detected.
VOSS-14712	SMLT high/low memory wrong alarm detection
VOSS-14765	Add certificate enhancement MIB support for vsp7400
VOSS-14794	Forwarding records point to vIST on DVR leaf node instead of client port after reboot of leaf node
VSP4000-248	ISIS adjacency over FE Tunnel not coming up

OUTSTANDING ISSUES:

Please see “Release Notes for VSP Operating System Software (VOSS)” for software release 8.0.x available at https://www.extremenetworks.com/support/release-notes for details regarding Known Limitations.

KNOWN LIMITATIONS:

Please see “Release Notes for VSP Operating System Software (VOSS)” for software release 8.0.x 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.

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