ExtremeSwitching

Configuring User Interfaces and Operating Systems for VOSS

Release 8.2 (VOSS)
9036547-00 Rev AE
January 2021

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, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

Contents

Chapter 1: About this Document

This section discusses the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

Purpose

This document describes how to use the Command Line Interface (CLI) and Enterprise Device Manager (EDM) interfaces to configure your switch, in addition to other operating systems that run on the switch.

This document provides information on features in VSP Operating System Software (VOSS). VOSS runs on the following product families:

- Extreme Networks VSP 4000 Series (includes VSP 4450 Series)
- Extreme Networks VSP 4900 Series
- Extreme Networks VSP 7200 Series
- Extreme Networks VSP 7400 Series
- Extreme Networks VSP 8000 Series (includes VSP 8200 Series and VSP 8400 Series)
- Extreme Networks VSP 8600 Series
- Extreme Networks XA1400 Series

Note:

VOSS is licensed on the XA1400 Series as a Fabric Connect VPN (FCVPN) application, which includes a subset of VOSS features. FCVPN transparently extends Fabric Connect services over third-party provider networks.

Examples and network illustrations in this document may illustrate only one of the supported platforms. Unless otherwise noted, the concept illustrated applies to all supported platforms.

Related to device management

The following Extreme Networks solutions can be used to manage multiple devices through a single interface on a remote server:

- ExtremeCloud™ IQ
- Extreme Management Center

- Extreme Fabric Orchestrator (EFO)
- Configuration and Orchestration Manager Plus (COM Plus)
- Visualization Performance and Fault Manager Plus (VPFM Plus)

Note:

Solution availability can vary depending on product and release.

For more information on these solutions, see www.extremenetworks.com/documentation/.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notice Icons

Icon	Alerts you to...
Important:	A situation that can cause serious inconvenience.
Note:	Important features or instructions.
Tip:	Helpful tips and notices for using the product.
Danger:	Situations that will result in severe bodily injury; up to and including death.
Warning:	Risk of severe personal injury or critical loss of data.
Caution:	Risk of personal injury, system damage, or loss of data.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can

Table continues…

Convention	Description
	enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon. Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command. For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command. For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed. For example, if the command syntax is `ethernet/2/1 [ <parameter> <value> ]...,` you enter `ethernet/2/1` and as many parameter-value pairs as you need.
Italic Text	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.
`Plain Courier Text`	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages. Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths.

Table continues…

Convention	Description
	For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.
Vertical Line (|)	A vertical line (|) separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. For example, if the command syntax is `access-policy by-mac action { allow | deny }`, you enter either `access-policy by-mac action allow` or `access-policy by-mac action deny`, but not both.

Documentation and Training

Find Extreme Networks product information at the following locations:

- Current Product Documentation
- Release Notes
- Hardware and software compatibility for Extreme Networks products
- Extreme Optics Compatibility
- Other resources such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal — Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub — A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC — For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form (all fields are required).
3. Select the products for which you would like to receive notifications.

   Note:
   You can modify your product selections or unsubscribe at any time.
4. Select **Submit**.

Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Chapter 2: New in this Document

The following sections detail what is new in this document.

Authentication for Privileged EXEC Command Mode

For enhanced security, you can enable user authentication to enter Privileged EXEC command mode. Use the **sys priv-exec-password** command to enable password authentication.

After you enable password authentication for Privileged EXEC command mode, the system prompts you to enter a password to access Privileged EXEC command mode from User EXEC command mode. You must enter the same password that you used to log on to the switch.

For more information, see Authentication for Privileged EXEC Command Mode on page 30.

DEMONSTRATION FEATURE - Extreme Integrated Application Hosting Enhancements

Extreme Integrated Application Hosting (IAH) enhancements are provided for demonstration purposes only on the following platforms:

- VSP4900-24XE
- VSP4900-12MXU-12XE
- VSP 7432CQ
- VSP 7400-48Y

Note:

Demonstration features are provided for testing purposes. Demonstration features are for lab use only, and are not for use in a production environment.

The IAH demonstration feature introduces the following enhancements:

- IAH ports 1/s1 and 1/s2 can be configured to accommodate different connect types.
- VT-d connect type can be configured on either 1/s1 and 1/s2 IAH ports.
- Up to two VT-d connect types can be configured.
- Network Interface Card (NIC) type of the virtual port can be configured.

With current configuration, IAH ports on the VSP 7432CQ platform cannot be configured to support different connect types. IAH port 1/s1 accommodates Single Root I/O Virtualization (SR-IOV) or Open vSwitch (OVS) connect type. IAH port 1/s2 accommodates one Virtualization Technology for Directed I/O (VT-d) connection type only. On the VSP 7400-48Y, the connection type is configured by using the **boot config flags insight-port-connect-type** command in Command Line Interface (CLI).

For **demonstration purposes only**, IAH ports 1/s1 and 1/s2 on supported platforms can be configured to accommodate different connect types. IAH ports 1/s1 and 1/s2 can accommodate

virtual ports of SR-IOV, OVS, or VT-d connect types. Two VT-d connection types are supported on either 1/s1 or 1/s2. Using the **virtual-service** command, you can specify which IAH port is associated with the configured connect type. You can also configure the Network Interface Card (NIC) type of the virtual port using the **virtual-service** command.

Now that you can configure IAH ports to accommodate different connect types in this release, the **boot config flags insight-port-connect-type** is no longer required and has been deprecated.

The following table lists the compatible IAH port connect type configurations available with IAH enhancements demonstration feature.

IAH port 1/s1	IAH port 1/s2
SR-IOV	OVS
SR-IOV	SR-IOV
OVS	SR-IOV
OVS	OVS
VT-d	VT-d

The **show virtual-service statistics** can now display IP address, MAC address, or Guest virtual machine (VM) interface name in CLI.

For more information about IAH enhancements, see Extreme Integrated Application Hosting Ports on page 75.

ExtremeCloud IQ Support for VSP Series

ExtremeCloud IQ provides cloud-managed networking, and delivers unified, full-stack management of wireless access points, switches, and routers. It enables onboarding, configuration, monitoring, troubleshooting, reporting, and more. Using innovative machine learning and artificial intelligence technologies, ExtremeCloud IQ analyzes and interprets millions of network and user data points, from the network edge to the data center, to power actionable business and IT insights, and to deliver new levels of network automation and intelligence.

ExtremeCloud IQ supports the following platforms:

- VSP4900-48P
- VSP 7400 Series
- XA1400 Series

For the most current information on switches supported by ExtremeCloud™ IQ, see ExtremeCloud™ IQ Learning What's New.

VOSS supports a zero touch connection to ExtremeCloud IQ. Zero touch deployment is used to deploy and configure a switch using ExtremeCloud IQ.

VOSS integrates with ExtremeCloud IQ using IQAgent. When you enable IQAgent, you can configure and monitor VOSS devices using ExtremeCloud IQ.

For more information, see the following sections:

- IQAgent on page 124
- Zero Touch Deployment on page 125

- IQAgent Configuration using CLI on page 126
- IQAgent Configuration using EDM on page 132

Fabric IPsec Gateway

The Fabric IPsec Gateway feature introduces a new Virtual Machine that supports aggregation of Fabric Extend Tunnels with fragmentation, reassembly, and Internet Protocol Security (IPsec) encryption functions for VSP 7400 Series switches.

For more information, see:

- Fabric IPsec Gateway Fundamentals on page 78
- Fabric IPsec Gateway Configuration using CLI on page 99

Zero Touch Deployment

Zero Touch Deployment enables a VOSS switch to be deployed automatically with ExtremeCloud IQ but you still must onboard the switch on the ExtremeCloud IQ side. When the switch powers on, the DHCP Client obtains the IP address and gateway from the DHCP Server, and discovers the Domain Name Server, connecting the switch automatically to Extreme Management Center or to ExtremeCloud IQ cloud management applications.

To use zero touch functionality, your switch must be in a Zero Touch Deployment-ready configuration mode, which means the switch cannot have existing primary or secondary configuration files loaded. Factory shipped switches are Zero Touch Deployment ready because they deploy without configuration files. However, existing switches require manual preparation before Zero Touch Deployment can function.

For more information, see Zero Touch Deployment on page 125.

Zero Touch Provisioning Plus

Zero Touch Provisioning Plus (ZTP+) provides Extreme Management Center connectivity to VOSS switches.

With zero touch functionality, VOSS switches are automatically discovered on the network the moment they are connected.

Zero Touch Provisioning Plus (ZTP+) enables you to deploy and configure VOSS switches in Extreme Management Center with minimal server configuration and intervention. ZTP+ enabled switches send information, such as the serial number, software version, MAC, management IP, and port information to Extreme Management Center automatically.

For more information, see the following sections:Zero Touch Provisioning Plus on page 145.

Notice about Feature Support

This document includes content for multiple hardware platforms across different software releases. As a result, the content can include features not supported by your hardware in the current software release.

If a documented command, parameter, tab, or field does not display on your hardware, it is not supported.

For information about physical hardware restrictions, see your hardware documentation.

Chapter 3: Command Line Interface

Table 3: Command Line Interface product support

Feature	Product	Release introduced
For configuration details, see Configuring User Interfaces and Operating Systems for VOSS.		
Command Line Interface (CLI)	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VSP 4200 4.0
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50

Command Line Interface Fundamentals

This section describes the Command Line Interface (CLI).

CLI is an industry standard command line interface that you can use for single-device management.

CLI Command Modes

CLI command modes provide specific sets of CLI commands. When you log onto the switch, you are in User EXEC mode with limited commands. While in a higher mode, you can access most commands from lower modes, except if they conflict with commands of your current mode.

There are two categories of CLI commands: show commands and configuration commands. You can use show commands from multiple command modes with the same results; they show the same configuration information regardless of the command mode. Configuration command results, however, might be dependent on the command mode from which a configuration command is used. For example, an `enable` command used in Global Configuration mode will enable a feature globally for all devices, and the same command used from one of the interface command modes will enable a feature for a specific interface only.

The following figure illustrates the navigation paths for the various command modes:

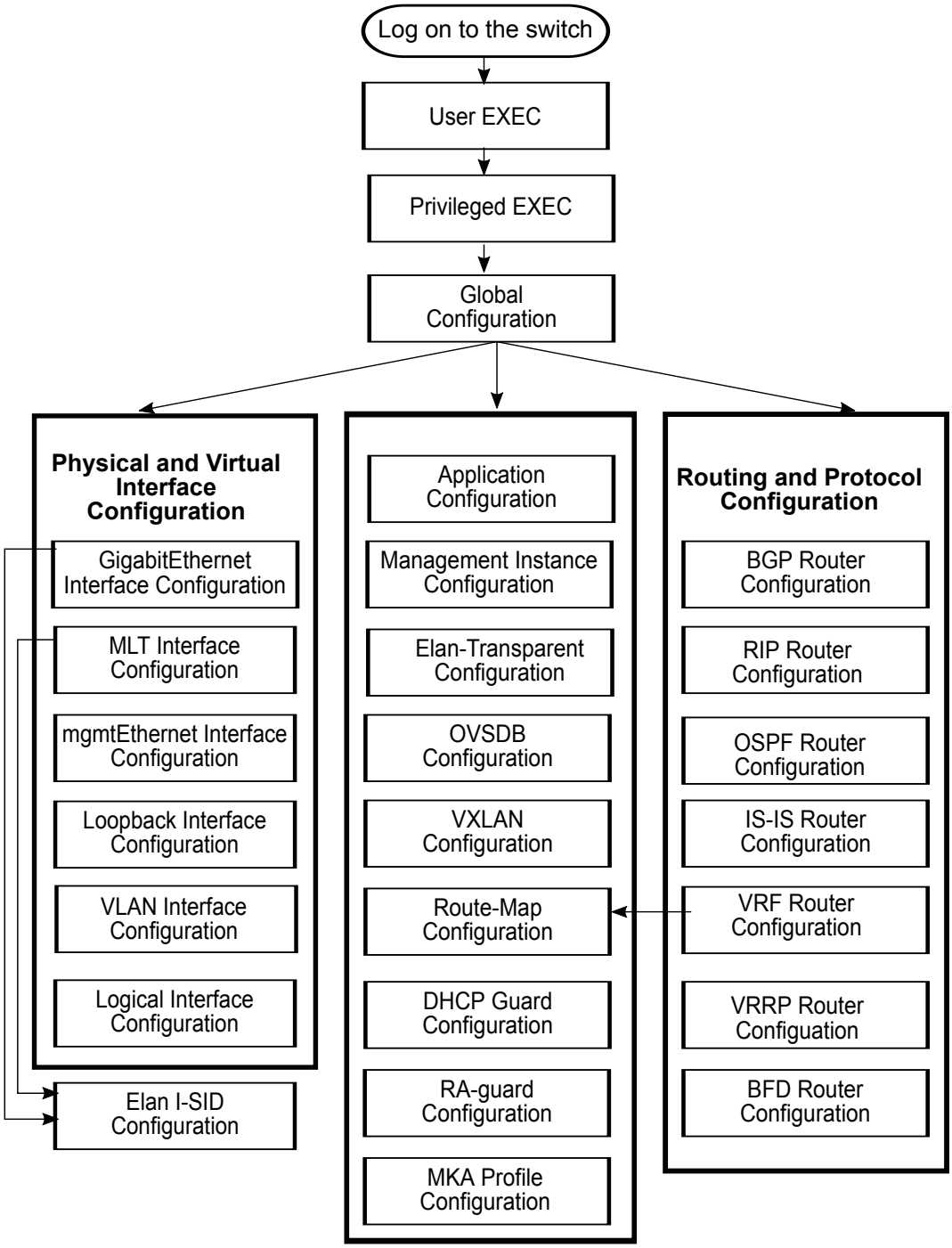


Figure 1: CLI Command Mode Navigation

Your user authorization credentials determine what commands are available to you in Privileged EXEC mode and all higher-level modes. See Administering VOSS for more information.

To navigate from higher-level modes to lower-level modes, use the following commands:

- **exit** to navigate from a higher-level mode to a lower-level mode, down to Privileged EXEC mode
- **end** to navigate from any command mode directly to Privileged EXEC mode
- **disable** to navigate from Privileged EXEC mode to User EXEC mode
- **logout** to terminate the CLI session from any command mode

The following table describes the various command modes, including the CLI command to access each mode, the command prompt that displays in each mode, and a description of the purpose of the mode.

Note:

Some command modes are hardware dependent. If any of the following commands modes do not display on your hardware, they are not supported or applicable.

Table 4: CLI Command Mode Summary

Command mode	Command to access mode	Prompt displayed in mode	Description
User EXEC	None required; default mode	>	View configuration settings and connection status.
	Note: You might be prompted to enter a username and password to access Privileged EXEC mode. For more information, see Authentication for Privileged EXEC Command Mode on page 30.		
Privileged EXEC	`enable`	#	Configure limited device-wide settings.
Global Configuration	`configure {terminal|network}`	`(config)#`	From a terminal or TFTP server, configure device-wide global parameters on a running configuration, or specify the filename of a configuration file.
GigabitEthernet Interface Configuration	`interface GigabitEthernet {slot/port[/sub-port][-slot/port[/subport]][,...]}`	`(config-if)#`	Configure chassis operations and features on a physical port.

Table continues…

Command mode	Command to access mode	Prompt displayed in mode	Description
MLT Interface Configuration	`interface mlt <1-512>`	`(config-mlt)#`	Configure an MLT interface.
mgmtEthernet Interface Configuration	`interface mgmtEthernet <mgmt|mgmt2>`	`(config-if)#`	Configure a dedicated physical management port (if supported on your hardware).
Loopback Interface Configuration	`interface loopback <1-256>`	`(config-if)#`	Configure a loopback CLIP interface.
VLAN Interface Configuration	`interface vlan <1-4059>`	`(config-if)#`	Configure port-based, policy-based, private, or SPBM B-VLANs

Logical Interface Configuration
(Layer 2 or Layer 3)
	Layer 2:
	`logical-intf isis <1-255> vid <list of vids> primary-vid <2-4059> port <slot/port> mlt <1-512> [name WORD<1-16>]`
	Layer 3:
	`logical-intf isis <1-255> dest-ip <A.B.C.D> [name WORD<1-16>]`
		Layer 2:
		`(config-isis-<1-255>)#`
		Layer 3:
		`(config-isis-<1-255>-<A.B.C.D>)#`
			Configure a logical Layer 2 or Layer 3 interface.

BGP Router Configuration	`router bgp`	`(router-bgp)#`	Configure device-wide BGP routing protocol settings.
RIP Router Configuration	`router rip`	`(config-rip)#`	Configure device-wide RIP routing protocol settings.
OSPF Router Configuration	`router ospf`	`(config-ospf)#`	Configure device-wide OSPF routing protocol settings.
IS-IS Router Configuration	`router isis`	`(config-isis)#`	Configure device-wide IS-IS routing protocol settings.
VRF Router Configuration	`router vrf WORD<1-16>`	`(router-vrf)#`	Configure a VRF instance, including the built-in Management VRF (accessed with **`router vrf MgmtRouter`** command).

Table continues…

Command mode	Command to access mode	Prompt displayed in mode	Description
VRRP Router Configuration	`router vrrp`	`(config-vrrp)#`	Configure device-wide VRRP protocol settings.
Application Configuration	`application`	`(config-app)#`	Configure custom applications, such as SLA Monitor or RESTCONF.
Management Instance Configuration	`mgmt <clip | oob | vlan>`	`(mgmt:clip)#` or `(mgmt:oob)#` or `(mgmt:vlan)#`	Configure a segmented management CLIP, Out-of-Band (OOB), or VLAN instance.
Elan I-SID Configuration	`i-sid <1-16777215> [elan]`	`(elan:<1-16777215>)#`	Add ports and traffic to a Switched UNI I-SID on a GigabitEthernet or MLT interface.
Elan-Transparent Configuration	`i-sid <1-16777215> elan-transparent`	`(elan-tp:<1-16777215>)#`	Add ports and MLT interfaces to an Elan-Transparent based service.
OVSDB Configuration	`ovsdb`	`(config-ovsdb)#`	Configure OVSDB protocol support for VXLAN Gateway.
Route-Map Configuration	`route-map WORD<1-64> <1-65535>`	`(route-map)#`	Configure device-wide or VRF instance-specific route map policy settings.
DHCP-guard Configuration	`ipv6 fhs dhcp-guard policy WORD<1-64>`	`(config-dhcpguard)#`	Configure DHCPv6 for advertised address-based, prefix-based, and preference-based filtering.
RA-guard Configuration	`ipv6 fhs ra-guard policy WORD<1-64>`	`(config-raguard)#`	Configure RA Guard for advertised IPv6 and MAC address-based, IPv6 prefix-based, preference-based, hop count limit-based, and default router preference-based filtering.
VXLAN Configuration	`vnid <1-16777215> i-sid <1-16777215>`	`(vxlan:<1-16777215>)#`	Associate port or MLT interface VLANs, configure VXLAN

Table continues…

Command mode	Command to access mode	Prompt displayed in mode	Description
			endpoints and untagged traffic.
MKA Profile Configuration	`macsec mka profile WORD<1-16>`	`(mka-profile)#`	Configure replay protection and confidentiality offset for an MKA profile.
BFD Router Configuration	`router bfd`	`(router-bfd)#`	Configure device-wide BFD settings.

Special CLI Command Modes

A special CLI command mode provides a set of specific CLI commands that are different from the standard CLI command modes and the CLI commands available in them. For example, a set of CLI commands that are specifically introduced to configure services on a Virtual Machine (VM) through a specific CLI command mode.

Note:

Special CLI command modes are hardware dependent. If they do not display on your hardware, they are not supported or applicable.

The following table describes the special command mode.

Table 5: Special CLI Command Mode Summary

Special command mode	Command mode navigation	Command to access mode	Prompt displayed in mode	Description
Fabric IPsec Gateway	Accessible from Privileged EXEC	`virtual-service WORD<1-128> console` **Note:** Type `CTRL+Y` to exit the console.	`FIGW>`	Configure services like IPsec, fragmentation and reassembly, and to manage the Fabric IPsec Gateway VM.

Default user names and passwords

The following table contains the default user names and passwords that you can use to log on to the switch using the command line interface (CLI). For more information about how to change passwords, see Configuring Security for VOSS.

Table 6: CLI default user names and passwords

User name	Password	Description
rwa	rwa	read-write-all
rw	rw	read-write
ro	ro	read-only
l1	l1	layer 1
l2	l2	layer 2
l3	l3	layer 3

If you enable enhanced secure mode, the user names and passwords are different than the default values documented in the preceding table. For more information on enhanced secure mode, see Administering VOSS.

Important:

The default passwords and community strings are documented and well known. It is strongly recommended that you change the default passwords and community strings immediately after you first log on. For more information about how to change user names and passwords, see Configuring Security for VOSS.

Multiple CLI Users for Each Role

Table 7: Multiple CLI Users product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Multiple CLI users per role	VSP 4450 Series	VOSS 7.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 7.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 7.0
	VSP 8400 Series	VOSS 7.0
	VSP 8600 Series	VSP 8600 8.0 demonstration feature
	XA1400 Series	VOSS 8.0.50

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

You can create up to a maximum of 10 CLI users for each role, which includes:

- 3 default users (rwa, rw, and ro)—User Type = default
- 7 user defined users (rwa or rw or ro)—User Type = userDefined

Usernames for default users (rwa, rw, and ro) can be changed; however, usernames for user defined users cannot be changed.

Users require a username and password to connect to the switch. Users can log on through the local serial port, Telnet, SSH, remote login (rlogin), or ftp. When a user is created, authentication is enabled, by default.

Note:

Rlogin is only supported on VSP 8600 Series.

For security reasons, if a login attempt fails, the error feedback does not indicate if the failed login is due to an invalid user name or an invalid password. Response times for invalid user name and invalid user name/password pair are identical to prevent identification of which of the two failed.

Note:

Multiple CLI users for each role does not apply in enhanced secure mode.

Documentation convention for the port variable

Commands that require you to enter one or more port numbers on the switch use the parameter *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}* in the syntax. The following table specifies the rules for using *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*.

Syntax	How to use
{slot/port[/sub-port]}	Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port. For example, 1/1 indicates the first port on slot 1. 1/41/1 indicates the first channel on slot 1, port 41.
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port. For example, 1/1–1/3 indicates ports 1 to 3 on slot 1, or 1/41/1,1/41/3 indicates the first and third channels of slot 1, port 41.

Command completion

The CLI provides potential command completions to the command string. Completions are provided by using a question mark (?) or by using the CLI autocompletion feature.

? command completion

The ? command completion is available for any valid command. By typing a command and using a ? as the last argument in the command, the system returns a list of possible command completions from the point of the ?. A short description is provided with each possible completion.

Example

If you enter the following command:

```
Switch:1(config-isis)#redistribute ?
```

CLI provides a list of completions for the **redistribute ?** command.

```
Switch:1(config-isis)#redistribute ?
    direct     isis redistribute direct command
    ospf        isis redistribute ospf command
    rip          isis redistribute rip command
    static     isis redistribute static command
```

All the parameters listed under redistribute indicate sub-context commands.

You must use one of the available completions, and if necessary, use the command completion help again to find the next completion.

```
Switch:1(config-isis)#redistribute direct ?
  enable       Enable isis redistribute direct command
  metric       Isis route redistribute metric
  metric-type  Set isis redistribute metric type
  route-map    Set isis redistribute direct route-policy
  subnets      Set isis redistribute subnets
<cr>
```

When you see <cr> (Carriage Return/Enter Key) in the list with the additional choices, this means that no additional parameters are required to execute the CLI command. However, the additional choices listed could be peer commands or sub-context commands.

For example, the parameters listed under **redistribute direct ?** are peer commands. You can enter these peer commands on the same line as the root command, for example **redistribute direct enable**. However, the <cr> indicates that you can also enter the **redistribute direct** command only and this command does not require any additional parameters at this level.

CLI autocompletion

CLI autocompletion is a feature that you can use to automatically fill in the unique parts of a command string rather than typing the entire command. Autcompletion makes the CLI experience easier and prevents mistakes in spelling that force you to re-enter the command.

Autocompletion completes the token in the command as soon as it becomes unique.

The Tab key autocompletes the command without executing the command, and places the cursor immediately after the last character. The Enter key autocompletes the command and executes it.

Example

To enable redistribution of ISIS direct routes,

```
Switch:1(config-isis)#redistribute direct
```

When you use `redistribute ?`, you see four possible sub-context commands.

```
direct
static
ospf
rip
```

If you type the following without pressing `Enter`:

```
Switch:1(config-isis)#redistribute direct m
```

and press the `Tab` key, the system completes the command to the following point:

```
redistribute direct metric
```

Two possible completions exist. You can type `-t`, and then press `Tab` to finish the command:

```
Switch:1(config-isis)#redistribute direct metric-type
```

default command operator

You can reset the modified configuration of a command to the default configuration by using the default operator. For more information about the default value for each command, see Command Line Interface Commands Reference for VOSS.

Use the ? command completion along with the default keyword in each configuration mode, to view the list of commands that support the default operator. For more information, see Command completion on page 25.

Example

Configure **`csnp-interval`** to its default value. The default value of **`csnp-interval`** is 10 seconds.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#router isis
Switch:1(config-isis)#show isis

================================================================================
                              ISIS General Info
================================================================================
                            AdminState : disabled
                            RouterType : Level 1
                             System ID : e45d.523c.6484
                  Max LSP Gen Interval : 900
                                Metric : wide
                 Overload-on-startup : 20
                              Overload : false
                        Csnp Interval : 200
                        PSNP Interval : 2
                    Rxmt LSP Interval : 5
                              spf-delay : 100
                           Router Name :
```

```
                    ip source-address :
                ipv6 source-address :
            ip tunnel source-address :
                         Tunnel vrf :
                      ip tunnel mtu :
                Num of Interfaces : 1
             Num of Area Addresses : 0

                    inband-mgmt-ip :
                          backbone : disabled
            Dynamically Learned Area : 00.0000.0000
                         FAN Member : Yes

Switch:1(config-isis)#default csnp-interval
Switch:1(config-isis)#show isis

================================================================================
                              ISIS General Info
================================================================================
                            AdminState : disabled
                            RouterType : Level 1
                             System ID : e45d.523c.6484
                Max LSP Gen Interval : 900
                               Metric : wide
                 Overload-on-startup : 20
                            Overload : false
                       Csnp Interval : 10
                       PSNP Interval : 2
                  Rxmt LSP Interval : 5
                           spf-delay : 100
                         Router Name :
                    ip source-address :
                ipv6 source-address :
            ip tunnel source-address :
                         Tunnel vrf :
                      ip tunnel mtu :
                Num of Interfaces : 1
             Num of Area Addresses : 0

                    inband-mgmt-ip :
                          backbone : disabled
            Dynamically Learned Area : 00.0000.0000
                         FAN Member : Yes
```

Example

View the IP configuration commands for an MLT interface that support the default operator.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#interface mlt 1
Switch:1(config-mlt)#default ?
Default settings
fa                  Set Fabric Attach configuration to default on mlt
flex-uni            Set flex-uni to default on mlt interface
ip                  Default IP configurations on MTL interface
isis                Set interface level isis parameters to default value
lacp                Set lacp for specific mlt to default
smlt                Create default smlt on a specific mlt
svlan-prototype  Set vlan port type to default
virtual-ist      Create virtual-ist on MLT with default value
Switch:1(config-mlt)#default ip ?
Default IP configurations on MLT interface
```

```
  arp-inspection   Default arp inspection configuration
  dhcp-snooping    Default dhcp snooping configuration
Switch:1(config-mlt)#default ip arp-inspection ?
  <cr>
```

no command operator

You can use the no operator in a command to negate a configuration. Based on the functionality of the command, you can perform negations, such as disable, delete, remove, or reset to the default configuration. For more information about the no operator for each command, see Command Line Interface Commands Reference for VOSS.

Use the ? command completion along with the no keyword to view the list of commands that support the no operator in each configuration mode. For more information, see Command completion on page 25.

Example

Negate the automatic virtual link that provides automatic dynamic backup link for OSPF traffic.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#router ospf
Switch:1(config-ospf)#no auto-vlink
```

Example

Remove an IP address configuration from VLAN.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#interface vlan 3
Switch:1(config-if)#no ip address 192.0.2.4
```

Example

View the commands that can negate a configuration in RIP router configuration mode.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#router rip
Switch:1(config-rip)#no ?
Negate a command or set its defaults
ipv6          Disable ipv6 configurations
network       Disable rip on an ip network
redistribute  To disable/delete redistribute golbally
Switch:1(config-rip)#no network ?
  {A.B.C.D}  Network ip address
Switch:1(config-rip)#no network 192.0.2.4 ?
  <cr>
```

GREP with CLI show command

You can use Global Regular Expression Print (GREP) with **show** commands to filter the output based on match criteria.

Enter the **show** command followed by the pipe (|) character, followed by the GREP filter command. The **show** command output contains only the lines that match the GREP filter pattern.

Note:

The **show fulltech** command does not support GREP filters.

The following GREP filter commands are supported.

GREP filter function	Description
begin	Displays the output of a command starting from the first line, which matches the given pattern.
count	Counts the number of lines in the output of a command.
exclude	Displays only the output lines which do not match the given pattern. The lines matching the pattern are discarded.
head	Limits the output of a command to the first few lines. If a number is not specified then only the first 10 lines display.
include	Displays only the output lines which match the given pattern.
no-more	Temporarily disables pagination for the output of an CLI command. When the lines of output exceed the terminal length, you are not prompted to continue or quit but the entire output of the command continues to be displayed. The effect is similar to setting terminal length 0 but only for the current command.
tail	Limits the output of a command to the last few lines. If a number is not specified then only the last 10 lines display.

Timestamp in show command outputs

The output for all CLI show commands includes a timestamp header to indicate when the command output was generated. This information can be helpful when communicating with Support.

The following command output shows a timestamp example.

```
Switch:1#show alarm statistics
********************************************************************************
                Command Execution Time: Wed Nov 07 19:55:15 2018 UTC
********************************************************************************
```

```
================================================================================================
                                    ALARM STATISTICS
================================================================================================
PERSISTENT PERSISTENT PERSISTENT  PERSISTENT  DYNAMIC   DYNAMIC  DYNAMIC DYNAMIC
  ALARM      ACTIVE    CLEARED      WRPRD      ALARM    ACTIVE   CLEARED  WRPRD
    0          0          0           0         11        8         3       0
```

Authentication for Privileged EXEC Command Mode

For enhanced security, you can enable user authentication to enter Privileged EXEC command mode. Use the **sys priv-exec-password** command to enable password authentication.

After you enable password authentication for Privileged EXEC command mode, the system prompts you to enter a password to access Privileged EXEC command mode from User EXEC command mode. You must enter the same password that you used to log on to the switch.

For more information about configuring Privileged EXEC authentication, see Configuring Security for VOSS.

CLI procedures

This chapter contains information about common CLI tasks. You can access CLI during runtime to manage the switch.

Logging on to the software

Before you begin

- The first time you connect to the switch, you must log on to CLI using the direct console port.

About this task

After you first connect to CLI you can log on to the software using the default user name and password. For more information about the default user names and passwords, see Default user names and passwords on page 22.

Procedure

1. At the login prompt, enter the user name.
2. At the password prompt, enter the password.

Viewing configurations

You can view the running configuration using the show command.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View running configuration:

   ```
   show running-config
   ```

Example

```
VSP-8284XSQ:1#show running-config
Preparing to Display Configuration...
#
#
# Thu Feb 05 18:38:02 2015 UTC
# box type             : VSP-8284XSQ
# software version     : 4.2.0.0_B004 (PRIVATE)
# cli mode             : CLI
#
#

#
#!end

#
config terminal
#
#
#BOOT CONFIGURATION
#

boot config flags ftpd
boot config flags telnetd
# end boot flags
auto-recover-delay 10

#CLI CONFIGURATION
#

telnet-access sessions 3
password password-history 3

#
#SYSTEM CONFIGURATION
#

ip name-server primary 198.51.100.0
sys msg-control control-interval 30
sys msg-control

#
#
```

Saving the configuration

After you change the configuration, you must save the changes to the module. Save the configuration to a file to retain the configuration settings.

About this task

File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Save the running configuration:

   ```
   save config [backup WORD<1-99>] [file WORD<1-99>] [verbose]
   ```

Example

Save the configuration to the default location:

```
Switch:1#save config
```

Identify the file as a backup file and designate a location to save the file:

```
Switch:1#save config backup 198.51.100.1/configs/backup.cfg
```

Variable definitions

Use the data in the following table to use the **`save config`** command.

Variable	Value
backup *WORD<1–99>*	Saves the specified file name and identifies the file as a backup file. *WORD<1–99>* uses one of the following formats: • a.b.c.d:<file> • /intflash/<file> The file name, including the directory structure, up to 1 to 99 characters.
file *WORD<1–99>*	Specifies the file name in one of the following formats: • /intflash/<file> • a.b.c.d:<file> The file name, including the directory structure, up to 1 to 99 characters.
verbose	Saves the default and current configuration. If you omit this parameter, the command saves only parameters you change.
standby *WORD<1-99>*	Specifies the standby file name in the following format: • `/intflash/<file>`

Table continues…

Variable	Value
	The file name, including the directory structure, up to 1 to 99 characters.

Configure the Web Server

Note:

DEMO FEATURE - Read Only User for EDM is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information, see VOSS Feature Support Matrix.

Perform this procedure to enable and manage the web server using the Command Line Interface (CLI). After you enable the web server, you can connect to EDM.

HTTP and FTP support both IPv4 and IPv6 addresses, with no difference in functionality or configuration. The TFTP server supports both IPv4 and IPv6 addresses. The TFTP client is not supported, only the server.

About this task

This procedure assumes that you use the default port assignments. You can change the port number used for HTTP and HTTPS.

Important:

If you want to allow HTTP access to the device, you must disable the web server secure-only option. If you want to allow HTTPS access to the device, the web server secure-only option is enabled by default.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable the web server:

   ```
   web-server enable
   ```

3. Disable the secure-only option (for HTTP access) :

   ```
   no web-server secure-only
   ```

4. Enable the secure-only option (for HTTPs access) :

   ```
   web-server secure-only
   ```

5. Enable read-only user:

   ```
   web-server read-only-user enable
   ```

6. Display the web server status:

   ```
   show web-server
   ```

Example

Enable the secure-only web-server. Configure the Read-Write-All access level username to smith2 and the password to 90Go2437. Enable read-only-user for the web server. Configure the read-only-user username to jones6 and the password to G69s8672.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#web-server enable
Switch:1(config)#web-server secure-only
Switch:1(config)#web-server read-only-user enable
Switch:1(config)#web-server password ro jones6 G69s8672
SSwitch:1(config)#web-server password rwa smith2 90Go2437
Switch:1(config)#show web-server

Web Server Info :

        Status                    : on
        Secure-only               : enabled
        TLS-minimum-version       : tlsv12
        RO Username Status        : enabled
        RO Username               : jones6
        RO Password               : ********
        RWA Username              : smith2
        RWA Password              : ********
        Def-display-rows          : 30
        Inactivity timeout        : 900 sec
        Html help tftp source-dir :
        HttpPort                  : 80
        HttpsPort                 : 443
        NumHits                   : 0
        NumAccessChecks           : 0
        NumAccessBlocks           : 0
        NumRxErrors               : 0
        NumTxErrors               : 0
        NumSetRequest             : 0
        Minimum password length   : 8
        Last Host Access Blocked  : 0.0.0.0
        In use certificate        : Self signed
```

Variable Definitions

Use the data in the following table to use the **`web-server`** command.

Variable	Value
def-display-rows <*10-100*>	Configures the number of rows each page displays, between 10 and 100.
enable	Enables the Web interface. To disable the web server, use the no form of this command: `no web-server [enable]`
help-tftp <*WORD/0-256*>	Configures the TFTP or FTP directory for Help files, in one of the following formats: a.b.c.d:/| peer:/

Table continues…

Variable	Value
	[<dir>]. The path can use 0–256 characters. The following example paths illustrate the correct format: • 192.0.2.1:/help • 192.0.2.1:/
http-port *<80-49151>*	Configures the web server HTTP port. The default port is 80.
https-port *<443-49151>*	Configure the web server HTTPS port. The default port is 443.
inactivity-timeout*<30–65535>*	Configures the web-server session inactivity timeout. The default is 900 seconds (15 minutes).
password {ro | rwa} *WORD<1-20> WORD<1-32>*	Configures the logon and password for the web interface, where the first *WORD<1-20>* is the new logon and the second *WORD<1-32>* is the new password.
password min-passwd-len*<1–32>*	Configures the minimum password length. By default, the minimum password length is 8 characters.
read-only-user	Enables read-only user for the web server. **Note:** **`read-only-user enable`** is available for demonstration purposes on some products. For more information, see VOSS Feature Support Matrix.
secure-only	Enables secure-only access for the web server.
tls-min-ver*<tlsv10|tlsv11|tlsv12>*	Configures the minimum version of the TLS protocol supported by the web-server. You can select among the following: • tlsv10 – Configures the version to TLS 1.0. • tlsv11 – Configures the version to TLS 1.1. • tlsv12 – Configures the version to TLS 1.2 The default is tlsv12.

Enable the Web Server RO User

About this task

Note:

DEMO FEATURE - Read Only User for EDM is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab

use only and are not for use in a production environment. For more information, see VOSS Feature Support Matrix.

Perform this procedure to enable the web server RO user, which is disabled by default after a software upgrade.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enable the read-only user:

   ```
   web-server read-only-user enable
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
```

Enable the default ro username:

```
Switch1:(config)#web-server read-only-user enable
```

Display the output of the **`show web-server command`** with the ro username enabled:

```
Switch:1(config)#show web-server
Web Server Info :

        Status                     : on
        Secure-only                : enabled
        TLS-minimum-version        : tlsv12
        RO Username Status         : enabled
        RO Username                : jones6
        RO Password                : ********
        RWA Username               : smith2
        RWA Password               : ********
        Def-display-rows           : 30
        Inactivity timeout         : 900 sec
        Html help tftp source-dir  :
        HttpPort                   : 80
        HttpsPort                  : 443
        NumHits                    : 87
        NumAccessChecks            : 4
        NumAccessBlocks            : 0
        NumRxErrors                : 73
        NumTxErrors                : 0
        NumSetRequest              : 0
        Minimum password length    : 8
        Last Host Access Blocked   : 0.0.0.0
        In use certificate         : Self signed
```

Setting the TLS protocol version

The switch by default supports version TLS 1.2 and above. You can explicitly configure TLS 1.0 and TLS 1.1 version support using CLI.

About this task

Disable the web server before changing the TLS version. By disabling the web server, other existing users with a connection to the web server are not affected from changing to a different version after you run the **tls-min-ver** command.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable the Web server:

   ```
   no web-server enable
   ```

3. Set the TLS protocol version:

   ```
   web-server tls-min-ver [tlsv10 | tlsv11 | tlsv12]
   ```

4. Enable the Web server:

   ```
   web-server enable
   ```

5. Verify the protocol version:

   ```
   show web-server
   ```

Example

```
Switch> enable
Switch# configure terminal
Switch(config)# web-server tls-min-ver tlsv11
```

Verify the protocol version.

```
Switch> show web-server

Web Server Info :

        Status                    : on
        Secure-only               : disabled
        TLS-minimum-version       : tlsv11
        RWA Username              : admin
        RWA Password              : ********
        Def-display-rows          : 30
        Inactivity timeout        : 900 sec
        Html help tftp source-dir :
        HttpPort                  : 80
        HttpsPort                 : 443
        NumHits                   : 198
        NumAccessChecks           : 8
        NumAccessBlocks           : 0
        NumRxErrors               : 198
        NumTxErrors               : 0
        NumSetRequest             : 0
        Minimum password length   : 8
        Last Host Access Blocked  : 0.0.0.0
        In use certificate        : Self signed
```

Variable Definitions

Use the data in the following table to use the **web-server** command.

Variable	Value
def-display-rows *<10-100>*	Configures the number of rows each page displays, between 10 and 100.
enable	Enables the Web interface. To disable the web server, use the no form of this command: `no web-server [enable]`
help-tftp *<WORD/0-256>*	Configures the TFTP or FTP directory for Help files, in one of the following formats: a.b.c.d:/| peer:/[<dir>]. The path can use 0–256 characters. The following example paths illustrate the correct format: • 192.0.2.1:/help • 192.0.2.1:/
http-port *<80-49151>*	Configures the web server HTTP port. The default port is 80.
https-port *<443-49151>*	Configure the web server HTTPS port. The default port is 443.
inactivity-timeout*<30–65535>*	Configures the web-server session inactivity timeout. The default is 900 seconds (15 minutes).
password {ro | rwa} *WORD<1-20> WORD<1-32>*	Configures the logon and password for the web interface, where the first *WORD<1-20>* is the new logon and the second *WORD<1-32>* is the new password.
password min-passwd-len*<1–32>*	Configures the minimum password length. By default, the minimum password length is 8 characters.
read-only-user	Enables read-only user for the web server. **Note:** **read-only-user enable** is available for demonstration purposes on some products. For more information, see VOSS Feature Support Matrix.
secure-only	Enables secure-only access for the web server.
tls-min-ver*<tlsv10|tlsv11|tlsv12>*	Configures the minimum version of the TLS protocol supported by the web-server. You can select among the following: • tlsv10 – Configures the version to TLS 1.0. • tlsv11 – Configures the version to TLS 1.1. • tlsv12 – Configures the version to TLS 1.2

Table continues…

Variable	Value
	The default is tlsv12.

Multiple users per role configuration using CLI

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

The following section provides procedures to configure multiple users per role.

Creating multiple CLI users

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

You can create up to seven new CLI users on the switch, in addition to the three default CLI users. The username must be unique. If you enable the hsecure flag, password complexity rules apply to all users.

Before you begin

You must use an account with read-write-all privileges to create new CLI users.

About this task

Note:

When a new CLI user is created, the specified username and access level cannot be changed later.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create a new CLI user:

   ```
   username add {<WORD 1-20> level [ro|rw|rwa] enable}
   ```

3. Enter a password.
4. Enter the password a second time.

Example

Create a new CLI user:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#username add smith level rwa enable
Enter password : *******
Re-enter password : *******
Switch:1(config)#
```

Variable Definitions

The following table defines parameters for the **username** command.

Variable	Value
add *WORD<1–20>*	Specifies the username to create.
enable	Enables the new CLI user.
level *<ro | rw | rwa>*	Specifies the level assigned to the new CLI user: • ro: Read-only level • rw: Read-write level • rwa: Read-write-all level

Disabling a user

About this task

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Use this task to disable a user.

Before you begin

You must use an account with read-write-all privileges to disable a user.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable the username:

   ```
   no username <WORD 1-20> enable
   ```

Example

Disable a user:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#no username smith enable
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#show cli username smith

============================================================
UserName              AccessLevel    State        Type
============================================================
ro                    ro             enable       default
rw                    rw             enable       default
rwa                   rwa            NA           default
smith                 rw             disable      userDefined
```

Deleting a username

About this task

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Use this task to delete a username. Default ro, rw, and rwa users cannot be deleted.

Before you begin

You must use an account with read-write-all privileges to delete a user.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Delete the username:

   ```
   no username <WORD 1-20>
   ```

Example

Delete a user:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#no username smith
The specified username will be deleted! Contiune (y/n) ? Y
Switch:1(config)#show cli username smith
Username does not exit
```

Variable Definitions

The following table defines parameters for the **`no username`** command.

Variable	Value
WORD <1–20>	Specifies the username to delete.
enable	Disables the username.

Displaying CLI usernames and roles

About this task

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Use this task to display CLI usernames and roles.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display CLI usernames and roles:

   ```
   show cli username
   ```

Example

```
Switch:1>show cli username

============================================================
UserName              AccessLevel    State        Type
============================================================
ro                    ro             enable       default
rw                    rw             enable       default
rwa                   rwa            NA           default
smith                 rw             enable       userDefined
```

Using GREP CLI show command filters

Use the following GREP filters to output only the command lines specified by the filter.

Procedure

1. Count the number of lines in the output:

   ```
   <CLI command> | count
   ```

2. Display the output of a command starting from the first line that matches the given pattern:

   ```
   <CLI command> | begin WORD<0-255> [field <number>] [ignore-case]
   [header <number>]
   ```

3. Display only the output lines that match the given pattern:

```
<CLI command> | include <pattern> [field <number>] [ignore-case]
[header <number>]
```

4. Display only the output lines that do not match the given pattern:

   ```
   <CLI command> | exclude <pattern> [field <number>] [ignore-case]
   [header <number>]
   ```

5. Temporarily disable pagination for the output of a CLI command:

   ```
   <CLI command> | no-more
   ```

   There is no prompt to continue or to quit when the lines of output exceed the terminal length.

6. Limit the output of a command to the first few lines:

   ```
   <CLI command> | head [<number>]
   ```

   If a number is not specified, the first 10 lines display.

7. Limit the output of a command to the last few lines:

   ```
   <CLI command> | tail [<number>] [from-line <number>] [header
   <number>]
   ```

   If a number is not specified, the last 10 lines display.

Example

```
Switch:1>enable
Siwtch:1#configure terminal
```

Count the number of lines in the output:

```
Switch1:#show vlan basic | count
Count: 17 lines
```

Display only the output lines that match the given pattern:

```
Switch:1(config)#show vlan basic | include byPort field 3 header 6

================================================================================================
                                        Vlan Basic
================================================================================================
VLAN                                MSTP
ID    NAME              TYPE        INST_ID PROTOCOLID   SUBNETADDR      SUBNETMASK      VRFID
------------------------------------------------------------------------------------------------
1     Default           byPort      0       none         N/A             N/A             0
3     VLAN3             byPort      3       none         N/A             N/A             0
4     VLAN4             byPort      4       none         N/A             N/A             0
5     VLAN5             byPort      5       none         N/A             N/A             0
8     VLAN-8            byPort      8       none         N/A             N/A             0
9     VLAN-9            byPort      9       none         N/A             N/A             0
11    VLAN-11           byPort      11      none         N/A             N/A             0
12    VLAN-12           byPort      12      none         N/A             N/A             0
20    VLAN-20           byPort      0       none         N/A             N/A             0
```

```
Switch:1(config)#show vlan basic | include private field 3 header 6

================================================================================================
                                        Vlan Basic
================================================================================================
VLAN                                MSTP
ID    NAME              TYPE        INST_ID PROTOCOLID   SUBNETADDR      SUBNETMASK      VRFID
6     VLAN6             private     40      none         N/A             N/A             0
7     VLAN7             private     41      none         N/A             N/A             0
```

Display only the output lines that do not match the given pattern:

```
Switch:1(config)#show vlan basic | exclude private field 3 header 6
================================================================================================
                                        Vlan Basic
================================================================================================
VLAN                                MSTP
ID    NAME              TYPE        INST_ID PROTOCOLID   SUBNETADDR      SUBNETMASK      VRFID
------------------------------------------------------------------------------------------------
1     Default           byPort      0       none         N/A             N/A             0
3     VLAN3             byPort      3       none         N/A             N/A             0
4     VLAN4             byPort      4       none         N/A             N/A             0
5     VLAN5             byPort      5       none         N/A             N/A             0
8     VLAN-8            byPort      8       none         N/A             N/A             0
9     VLAN-9            byPort      9       none         N/A             N/A             0
11    VLAN-11           byPort      11      none         N/A             N/A             0
12    VLAN-12           byPort      12      none         N/A             N/A             0
20    VLAN-20           byPort      0       none         N/A             N/A             0
```

```
Switch:1(config)#show vlan basic | exclude byPort field 3 header 6

================================================================================================
                                        Vlan Basic
================================================================================================
VLAN                                MSTP
ID    NAME              TYPE        INST_ID PROTOCOLID   SUBNETADDR      SUBNETMASK      VRFID
------------------------------------------------------------------------------------------------
6     VLAN6             private     40      none         N/A             N/A             0
7     VLAN7             private     41      none         N/A             N/A             0
```

Display the output of a command starting from the first line that matches the given pattern:

```
Switch:1(config)#show vlan basic | begin 8 header 6

================================================================================================
                                        Vlan Basic
================================================================================================
VLAN                                MSTP
ID    NAME              TYPE        INST_ID PROTOCOLID   SUBNETADDR      SUBNETMASK      VRFID
8     VLAN-8            byPort      8       none         N/A             N/A             0
9     VLAN-9            byPort      9       none         N/A             N/A             0
11    VLAN-11           byPort      11      none         N/A             N/A             0
12    VLAN-12           byPort      12      none         N/A             N/A             0
20    VLAN-20           byPort      0       none         N/A             N/A             0
```

Display the entire output of the command:

```
Switch:1(config)#show vlan basic | no-more

================================================================================================
                                        Vlan Basic
================================================================================================
VLAN                                MSTP
ID    NAME              TYPE        INST_ID PROTOCOLID   SUBNETADDR      SUBNETMASK      VRFID
------------------------------------------------------------------------------------------------
1     Default           byPort      0       none         N/A             N/A             0
3     VLAN3             byPort      3       none         N/A             N/A             0
4     VLAN4             byPort      4       none         N/A             N/A             0
5     VLAN5             byPort      5       none         N/A             N/A             0
6     VLAN6             private     40      none         N/A             N/A             0
7     VLAN7             private     41      none         N/A             N/A             0
8     VLAN-8            byPort      8       none         N/A             N/A             0
9     VLAN-9            byPort      9       none         N/A             N/A             0
11    VLAN-11           byPort      11      none         N/A             N/A             0
12    VLAN-12           byPort      12      none         N/A             N/A             0
20    VLAN-20           byPort      0       none         N/A             N/A             0
```

Display only the first few lines of output:

```
Switch:1(config)#show vlan basic | head 9

================================================================================================
```

```
                                        Vlan Basic
================================================================================================
VLAN                                MSTP
ID    NAME              TYPE        INST_ID PROTOCOLID   SUBNETADDR      SUBNETMASK      VRFID
------------------------------------------------------------------------------------------------
1     Default           byPort      0       none         N/A             N/A             0
3     VLAN3             byPort      3       none         N/A             N/A             0
```

Display only the last few lines of output:

```
Switch:1(config)#show vlan basic | tail 8 header 6

================================================================================================
                                        Vlan Basic
================================================================================================
VLAN                                MSTP
ID    NAME              TYPE        INST_ID PROTOCOLID   SUBNETADDR      SUBNETMASK      VRFID
8     VLAN-8            byPort      8       none         N/A             N/A             0
9     VLAN-9            byPort      9       none         N/A             N/A             0
11    VLAN-11           byPort      11      none         N/A             N/A             0
12    VLAN-12           byPort      12      none         N/A             N/A             0
20    VLAN-20           byPort      0       none         N/A             N/A             0
```

```
Switch:1(config)#show vlan basic | tail from-line 15 header 6

================================================================================================
                                        Vlan Basic
================================================================================================
VLAN                                MSTP
ID    NAME              TYPE        INST_ID PROTOCOLID   SUBNETADDR      SUBNETMASK      VRFID
9     VLAN-9            byPort      9       none         N/A             N/A             0
11    VLAN-11           byPort      11      none         N/A             N/A             0
12    VLAN-12           byPort      12      none         N/A             N/A             0
20    VLAN-20           byPort      0       none         N/A             N/A             0
```

Variable definitions

The GREP filters use the following parameters:

Parameter	Description
field<*number*>	Specifies the field in each line to match against the pattern. Fields are separated by white spaces and are counted starting with 1 for the left-most field. If the output is formatted as a table, whitespaces are not counted as fields.
from-line <*number*>	Specifies the remaining output starting with a given line.
head<*number*>	Specifies the number of lines to keep from the beginning of the output.
header<*number*>	Specifies a number of lines from the start of the output to display unchanged before trying to match the pattern. This parameter is useful to keep the header of a table intact. This filter skips the header lines.
ignore-case	Specifies letters to match in the pattern regardless of case.
<number>	Specifies the number of lines of output to keep, either from the beginning of the output or from the end of the output.

Table continues…

Parameter	Description
<pattern>	Specifies the regular expression to match against each line of output. Use quotations if the parameter contains spaces.

Chapter 4: Enterprise Device Manager

Table 8: Enterprise Device Manager product support

Feature	Product	Release introduced
For configuration details, see Configuring User Interfaces and Operating Systems for VOSS.		
Enterprise Device Manager (EDM)	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VSP 8200 4.0
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50
Read-Only user for EDM	VSP 4450 Series	VOSS 7.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 7.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 7.0
	VSP 8400 Series	VOSS 7.0
	VSP 8600 Series	VSP 8600 8.0 demo feature
	XA1400 Series	VOSS 8.0.50

Enterprise Device Manager Fundamentals

This section details Enterprise Device Manager (EDM).

EDM is a web-based graphical user interface (GUI) you can use to configure a single switch. EDM runs from the switch and you can access it from a web browser. You do not need to install additional client software, and you can access it with all operating systems.

Supported Browsers

Use the following browser versions to access Enterprise Device Manager (EDM):

- EdgeHTML 18+
- Microsoft Internet Explorer 11.+
- Mozilla Firefox 72+
- Google Chrome 80+
- Safari 13+

For optimal performance, use Mozilla Firefox or Google Chrome.

Enterprise Device Manager Access

To access EDM, open *http://<deviceip>/login.html* or *https://<deviceip>/login.html* from Microsoft Edge, Microsoft Internet Explorer, Google Chrome, or Mozilla Firefox. Ensure you use a supported browser version.

Important:

- You must enable the web server from CLI (see Configuring the Web server using CLI on page 33) to enable HTTP access to the EDM. If you want HTTP access to the device, you must also disable the web server secure-only option. The web server secure-only option, allowing for HTTPS access to the device, is enabled by default. It is recommended that you take the appropriate security precautions within the network if you use HTTP
- EDM access is available to read-write users only

If you experience issues while connecting to the EDM, check the proxy settings. Proxy settings can affect EDM connectivity to the switch. Clear the browser cache and do not use proxy when connecting to the device.

Default user name and password

The following table contains the default user name and password that you can use to log on to the switch using EDM. For more information about changing the passwords, see Configuring Security for VOSS.

Table 9: EDM default username and password

Username	Password
admin	password

Important:

The default passwords and community strings are documented and well known. It is strongly recommended that you change the default passwords and community strings immediately after you first log on. For more information about changing user names and passwords, see Configuring Security for VOSS.

Device Physical View

After you access EDM, the system displays a real-time physical view of the front panel of the device. From the front panel view, you can view fault, configuration, and performance information for the device or a single port. You can open this tab by clicking the Device Physical View tab above the device view.

You can use the device view to determine the operating status of the various ports in your hardware configuration. You can also use the device view to perform management tasks on specific objects. In the device view, you can select a port or the entire chassis. To select an object, click the object. EDM outlines the selected object in yellow, indicating your selection.

The conventions on the device view are similar to the actual device appearance. The port LEDs and the ports are color-coded to provide status. Green indicates the module or port is up and running, red indicates the module or port is disabled, dark pink indicates a protocol is down, and amber indicates an enabled port that is not connected to anything. For information about LED behavior, see your hardware documentation.

EDM Window

The following list identifies the different sections of the EDM window:

- Navigation pane—Located on the left side of the window, the navigation pane displays all the available command tabs in a tree format. A row of buttons at the top of the navigation pane provides a quick method to perform common functions.
- Content pane—Located on the right side of the window, the content pane displays the tabs and dialog boxes where you can view or configure parameters on the switch.
- Menu bar—Located at the top of the content pane, the menu bar shows the most recently accessed primary tabs and their respective secondary tabs.
- Toolbar—Located just below the menu bar, the toolbar provides quick access to the most common operational commands such as Apply, Refresh, and Help.

The following figure shows an example of the Device Physical View tab within the EDM window.

Note:

The Device Physical View tab on your hardware can appear differently than the following example.

Figure 2: EDM window

Navigation Pane

You can use the navigation pane to see what commands are available and to quickly browse through the command hierarchy. A row of buttons at the top of the navigation pane provides a quick method to perform common functions.

Note:

For module-based chassis, menu options related to a specific module are activated only after you install and select the required module.

The following table describes the buttons that appear at the top of the navigation pane.

Table 10: Navigation pane buttons

Button	Name	Description
	Save Config	Saves the running configuration.
	Refresh Status	Refreshes the Device Physical View.
	Edit	Edits the selected item in the Device Physical View.
	Graph	Opens the graph options for the selected item in the Device Physical View.
	Help Setup Guide	Opens instructions about how to install the Help files and configure EDM to use the Help files.

Expand a folder by clicking it. Some folders have subfolders such as the Edit folder, which has the Port, Diagnostics, and other subfolders.

Within each folder and subfolder menu, there are numerous options, which provide access to tabs. To open an option, click it. The selected tab appears in the menu bar and opens in the content pane. The following table describes the main folders in the navigation pane.

Table 11: Navigation Pane Folders

Menu	Description
Device	Use the Device menu to refresh and update device information or enable polling. • Preference Setting — Enable polling or hot swap detection. Configure the frequency to poll the device. • Refresh Status — Use this option to refresh the device view. • Rediscover Device — Use this to trigger a rediscovery to update all of the device information.
VRF Context view	Use the VRF Context view to switch to another VRF context when you use the embedded EDM. GlobalRouter is the default view at log in. You can configure both Global Router (GRT) and Virtual Routing and Forwarding (VRF) instances when you launch a VRF context view. You can open only five tabs for each EDM session.
Edit	Use the Edit menu to view and configure parameters for the chassis hardware or for the currently selected object. The selected object can be a port. You can also use the Edit menu to perform the following tasks: • check and configure ports, including the internal Extreme Integrated Application Hosting ports, on the device • run diagnostic tests • change the configuration of many features, including but not limited to, the file system, NTP, OVSDB, SMTP, Link-state tracking, service delivery, Fabric Attach, VTEP, DvR, Management Instance, Endpoint Tracking, and SNMPv3 settings for the device
Graph	Use the Graph menu to view and configure EDM statistics and to produce graphs of the chassis or port statistics.

Table continues…

Menu	Description
Power Management	Use the Power Management menu to view and configure Energy Saver.
VLAN	Use the VLAN menu to view and configure VLANs, spanning tree groups (STG), MultiLink Trunks/LACP, SMLT, and SLPP.
IS-IS	Use the IS-IS menu to view and configure IS-IS, Shortest Path Bridging MAC (SPBM), statistics, and I-SIDs.
VRF	Use the VRF menu to view and create VRFs.
IP	Use the IP menu to view and configure IP routing functions for the system, including the following: • IP-VPN • IP-MVPN • IP • TCP/UDP • OSPF • RIP • VRRP • RSMLT • BGP • Multicast • MSDP • IGMP • IPFIX • PIM • SPB-PIM-GW • DHCP Relay • DHCP Snooping • ARP Inspection • Source Guard • UDP Forwarding • IS-IS • Policies • BFD

Table continues…

Menu	Description
IPv6	Use the IPv6 menu to view and configure IPv6 routing functions, including the following: • IPv6 • IPv6 - VPN • TCP/UDP • Tunnel • OSPFv3 • VRRP • BGP+ • RSMLT • DHCP Relay • Policy • FHS • IS-IS • RIPng • IPv6 PIM • IPv6 MLD • IPv6 Mroute • IPv6 BFD
Security	Use the Security menu to view and configure access policies, ACL filters, certificates, and features such as RADIUS, RADIUS CoA, SSH, IPSec, TACACS+, and EAPoL.
QOS	Use the QOS menu to view and configure mapping tables, QoS port states, CoS Queue Stats, and Queue Profiles.
Serviceability	Use the Serviceability menu to enable, configure, or view: • RMON • sFlow • Application Telemetry • SLA Monitor • RESTCONF • Virtual services

Menu Bar

The menu bar is above the content pane and consists of two rows of tabs.

- The top row displays the tabs you can open through the navigation pane. These primary tabs appear in the sequence in which you open them.
- After you click a primary tab, the secondary tabs associated with it appear in the bottom row. Click a secondary tab to display it in the content pane.

In both the top and bottom rows of the menu bar, if the number of tabs exceeds the viewable space, the system displays left- and right-pointing arrows. Click an arrow to scroll to the required tab.

To reduce the number of tabs on the top row, you can click the X on the right corner of a tab to remove it from the row. The following figure shows a sample menu bar.

Figure 3: Menu bar

Toolbar

The toolbar buttons provide quick access to commonly used operational commands. The buttons that appear vary depending on the tab you select. However, the Apply, Refresh, and Help buttons are on almost every screen. Other common buttons are Insert and Delete. The following list detail the common toolbar buttons.

- Apply—Use this button to execute all edits that you make.
- Refresh—Use this button to refresh all data on the screen.
- Help—Use this button to display online help that is context sensitive to the current dialog box.
- Insert—Use this button to display a secondary dialog box related to the selected tab. After you edit the configurable parameters, click the Insert button in the dialog box. This causes a new entry to appear in the dialog box of the selected tab.
- Delete—Use this button to delete a selected entry.

The following figure shows a sample toolbar.

Figure 4: Toolbar

Content Pane

The content pane is the main area on the right side of the window that displays the configuration tabs and dialog boxes. Use the content pane to view or configure parameters on the switch.

Note:

You can view valid ranges for all configurable parameters on EDM tabs.

The following figure is a sample that shows the content pane for the Port 1/3 General, Interface tab. If you want to compare the information in two tabs, you can undock one, then open another tab. For more information about undocking a tab, see Undocking and docking tabs on page 64.

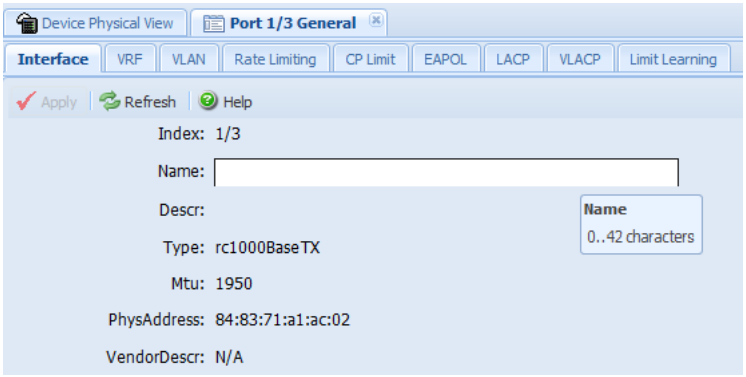


Figure 5: Content pane

EDM user session extension

If the EDM user session remains unused for a duration of ten minutes, the system displays the following message:

```
Your session will expire in about 5 minute(s). Would you like to extend the session?
```

If you do not respond, EDM automatically ends the session with the following message: `Your session has expired`.

You can log on again if you want to continue to use EDM.

TLS server for secure HTTPS

Table 12: TLS server for secure HTTPS product support

Feature	Product	Release introduced
For configuration details, see Configuring User Interfaces and Operating Systems for VOSS.		
TLS server for secure HTTPS **Note:** VOSS Releases 6.0 and 6.0.1 do not support this feature.	VSP 4450 Series	VOSS 5.1.2
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 5.1.2
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 5.1.2
	VSP 8400 Series	VOSS 5.1.2
	VSP 8600 Series	VSP 8600 6.1
	XA1400 Series	VOSS 8.0.50

This feature enhances communications security by implementing Mocana NanoSSL to secure HTTPS server using Transport Layer Security (TLS) cryptographic protocol.

The following are the key properties of Secure Web server with TLS:

- This feature can be implemented on a maximum of only 10 concurrent client connections.
- The switch supports version TLS 1.2 and above by default. You can explicitly configure TLS 1.0 and TLS 1.1 version support using CLI or EDM.
- This feature replaces SSL 3.0 with TLS. SSL 3.0 is not supported.
- TLS server does not support RC4, DES, TDES, and MD5 based cipher suites.
- The minimum password length for the web server is 8 characters, by default. You can change this using CLI or EDM.

Certificate Order Priority

Table 13: Certificate order priority product support

Feature	Product	Release introduced
For configuration details, see Configuring Security for VOSS.		
Certificate order priority **Note:** VOSS Releases 6.0 and 6.0.1 do not support this feature.	VSP 4450 Series	VOSS 5.1.2
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 5.1.2
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 5.1.2
	VSP 8400 Series	VOSS 5.1.2

Table continues…

Feature	Product	Release introduced
	VSP 8600 Series	Not Supported
	XA1400 Series	VOSS 8.0.50

Use the following information to understand the certificate order priority when the Transport Layer Security (TLS) server and switch connect.

The TLS server selects the server certificate in the following order:

1. A certification authority (CA)-signed certificate if the certificate is already present in the `/intflash/.cert/` folder on the switch.
2. A self-signed certificate if the certificate is already present in the `/intflash/.cert/` folder on the switch.

If the server certificates are not available, the TLS server generates a new self-signed certificate at startup and uses that by default. The self-signed certificate is available in `/.intflash/.cert/.ssl`. You can choose to use an online or offline CA-signed certificate, which will take precedence over the self-signed certificate.

SSL-Based Self-Signed Certificate

Some earlier releases use the default certificate available in the `/intflash/.ssh` folder, which is the open SSL-based self-signed certificate that is named host.cert.

To use the Mocana stack-based self-signed certificate, delete the open SSL self-signed certificate prior to upgrading your software release. The Mocana certificate offers better and stronger encryption than open SSL-based certificates.

If you do not delete the host.cert file in the `/intflash/.ssh` folder used in earlier releases, you must generate a self-signed certificate automatically during upgrade or post upgrade using the command **`config ssl certificate`**.

If you have a subscribed CA-signed certificate renamed as host.cert in folder `/intflash/.ssh` in a previous release, it cannot be reused.

To use your subscribed CA-signed certificate, upgrade with the Mocana-based self-signed certificate, and then use the digital certificates feature to install a CA-signed certificate through the online or offline method.

You cannot obtain a CA-signed certificate and rename the certificate as host.cert. You must use the online or offline method to obtain a certificate.

EDM interface procedures

This section contains procedures for starting and using Enterprise Device Manager (EDM). The software is built-in to the switch, and you do not need to install additional software.

Connecting to EDM

Before you begin

- Ensure that the switch is running.
- Note the IP address of the switch.
- Ensure that you use a supported browser version.
- Ensure that you enable the web server using CLI.

About this task

Perform this procedure to connect to EDM to configure and maintain your network through a graphical user interface.

Procedure

1. In the address field, enter the IP address of the system using the following formats: **https://<IP_address>** (default) or **http://<IP_address>**.

   Note:

   By default the Web server is configured with the secure-only option, which requires you to use HTTPS to access EDM. To access EDM using HTTP, you must disable the secure-only option.

2. In the **User Name** field, type the user name. The default is admin.
3. In the **Password** field, type a password. The default is password.
4. Click **Log On**.

   For information about how to change the Log On credentials, see Configuring Security for VOSS.

Configure the Web Management Interface

Note:

DEMO FEATURE - Read Only User for EDM is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information, see VOSS Feature Support Matrix.

Before you begin

- Enable the web server.
- For VSP 8600 Series, enable the web server RO user in CLI.

About this task

Configure the web management interface to change the user names and passwords for management access to the switch using a web browser.

HTTP, FTP, and TFTP server supports both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

You can also use the CLI interface for creating users.

Procedure

1. In the navigation pane, open the **Configuration** > **Security** > **Control Path** folders.
2. Select **General**.
3. Select the **Web** tab.
4. Complete the **WebRWAUserName** and **WebRWAUserPassword** fields to specify the user name and password for access to the web interface.

   This user will have full permission.
5. To enable the RO user for the web server, select **WebROEnable**.

   Note:

   This step does not apply to VSP 8600 Series.
6. Complete the **WebROUserName** and **WebROUserPassword** fields to specify the user name and password for access to the web interface.

   This user will have read only permission.
7. Select **Apply**.

Web Field Descriptions

Use the data in the following table to use the Web tab.

Name	Description
WebRWAUserName	Specifies the RWA username from 1–20 characters. The default is admin.
WebRWAUserPassword	Specifies the password from 1–32 characters. The default is 12345678.
WebROEnable **Note:** Exception: not supported on VSP 8600 Series.	Enables the web server read-only (RO) user, which is disabled by default after a software upgrade.
WebROUserName	Specifies the RO username from 1–20 characters. The default is user. **Note:** Product Notice: For VSP 8600 Series the web server RO username must be enabled in CLI.
WebROUserPassword	Specifies the password from 1–32 characters. The default is password.

Table continues…

Name	Description
MinimumPasswordLength	Configures the minimum password length. By default, the minimum password length is 8 characters.
HttpPort	Specifies the HTTP port for web access. The default value is 80.
HttpsPort	Specifies the HTTPS port for web access. The default value is 443.
SecureOnly	Controls whether the secure-only option is enabled. The default is enabled.
InactivityTimeout	Specifies the idle time (in seconds) to wait before the EDM login session expires. The default value is 900 seconds (15 minutes).
TlsMinimumVersion	Configures the minimum version of the TLS protocol supported by the web-server. You can select from the following options: • tlsv10 – Configures the version to TLS 1.0. • tlsv11 – Configures the version to TLS 1.1. • tlsv12 – Configures the version to TLS 1.2 The default is tlsv12.
HelpTftp/Ftp_SourceDir	Configures the TFTP or FTP directory for Help files, in one of the following formats: a.b.c.d:/| peer:/ [<dir>]. The path can use 0–256 characters. The following example paths illustrate the correct format: • 192.0.2.1:/Help • 192.0.2.1:/
DefaultDisplayRows	Configures the web server display row width between 10–100. The default is 30.
LastChange	Shows the last web-browser initiated configuration change.
NumHits	Shows the number of hits to the web server.
NumAccessChecks	Shows the number of access checks performed by the web server.
NumAccessBlocks	Shows the number of access attempts blocked by the web server.
LastHostAccessBlockedAddressType	Shows the address type, either IPv4 or IPv6, of the last host access blocked by the web server.
LastHostAccessBlockedAddress	Shows the IP address of the last host access blocked by the web server.
NumRxErrors	Shows the number of receive errors the web server encounters.

Table continues…

Name	Description
NumTxErrors	Shows the number of transmit errors the web server encounters.
NumSetRequest	Shows the number of set-requests sent to the web server.

Using the chassis shortcut menu

About this task

Perform the following procedure to display the chassis shortcut menu.

Procedure

1. In the Device Physical View, select the chassis.
2. Right-click the chassis.

Chassis shortcut menu field descriptions

Use the data in the following table to use the Chassis shortcut menu.

Name	Description
Edit	Edits chassis parameters.
Graph	Graphs chassis statistics.
Refresh Status	Refreshes the status of the chassis and MDAs.
Refresh Port Tooltips	Refreshes the port tooltip data of the system. The port tooltip data contains the following variables: Slot/Port, PortName, and PortOperSpeed.

Using the port shortcut menu

About this task

Perform this procedure to display the port shortcut menu.

Procedure

1. In the Device Physical View, select a port.
2. Right-click the selected port.

Port shortcut menu field descriptions

Use the data in the following table to use the port shortcut menu.

Name	Description
Edit General	Configures the general options for the port.
Edit IP	Configures the IP options for the port.
Edit IPv6	Configures the IPv6 options for the port.
Channelization Enable	Enables channelization for the port.
Channelization Disable	Disables channelization for the port.
Graph	Displays the statistics for the port.
Enable	Enables the port.
Disable	Disables the port.

Using a table-based tab

About this task

Change an existing configuration using a table-based tab. You cannot edit grey-shaded fields in the table. The following procedure is an illustration on how to use a table-based tab.

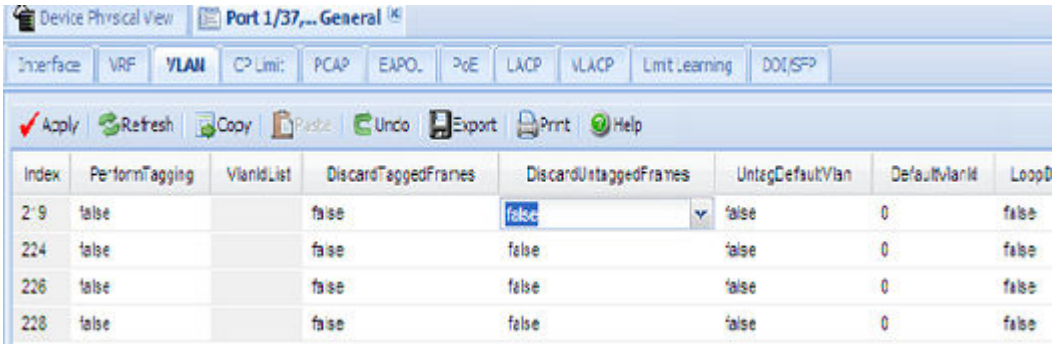
Note:

You can expand the appropriate folders for any feature you configure and select a table-based tab.

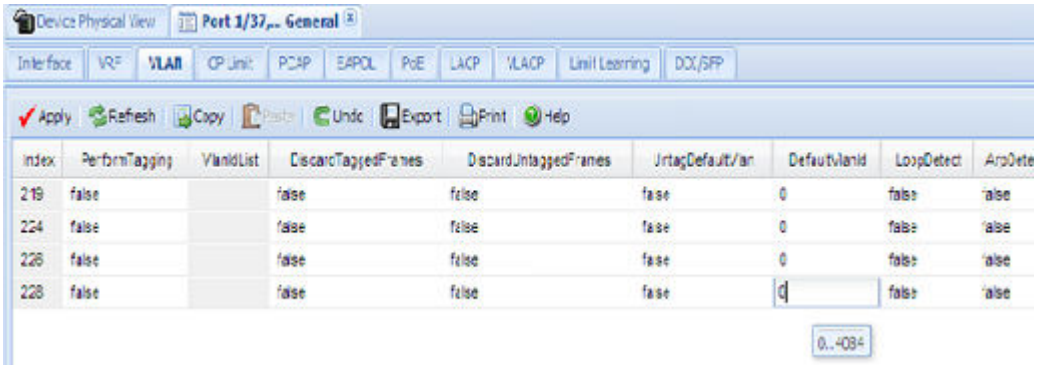
Procedure

1. In the Device Physical View, select multiple ports.
2. In the navigation pane, expand the **Configuration** > **Edit** > **Port** > **General** folders.
3. Click the **VLAN** tab.

   The system displays a table-based tab with the VLAN information.
4. Select a table-based tab.
5. Double-click a white-shaded field to edit the value.
6. Click the arrow in the list field to view the options, and then select the appropriate value.



7. In a text-entry field, double-click, and then edit the value.



8. Click **Apply** to save the configuration changes.

Monitor Multiple Ports and Configuration Support

About this task

You can monitor or apply the same configuration changes to more than one port by using the multiple port selection function. You can use the standard menu or the shortcut menu to edit the configuration settings for multiple ports.

Tip:

A selected port shows a yellow outline around the port.

Procedure

1. Click the **Device Physical View** tab.
2. To select multiple ports, press the `Control` key, and then click the required ports.

   Note:

   When you use the Enterprise Device Manager (EDM) embedded in the software, you can select a maximum of 24 ports.

   No port limitation exists for COM users.

Open Folders and Tabs

About this task

Perform this procedure to navigate in EDM.

Procedure

1. In the navigation pane, expand the **Configuration** folder.
2. Click a subfolder to expand the subfolder and see the list of menu options, for example, the **VLAN** folder.

3. In a folder or subfolder menu, click an option to open the related tabs.

Undocking and docking tabs

About this task

Perform this procedure to undock a tab. You can undock tabs to have more than one tab visible at a time.

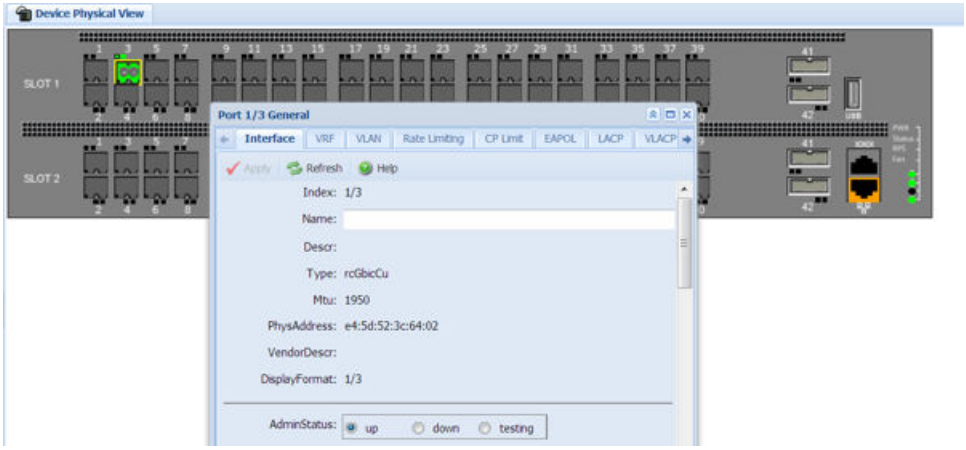
Procedure

1. In the navigation pane, click a tab.
2. In the menu bar, click and drag a tab to undock it.
3. In the top right corner of the tab, click **pages** to dock the tab.

Example of undocking and docking tabs

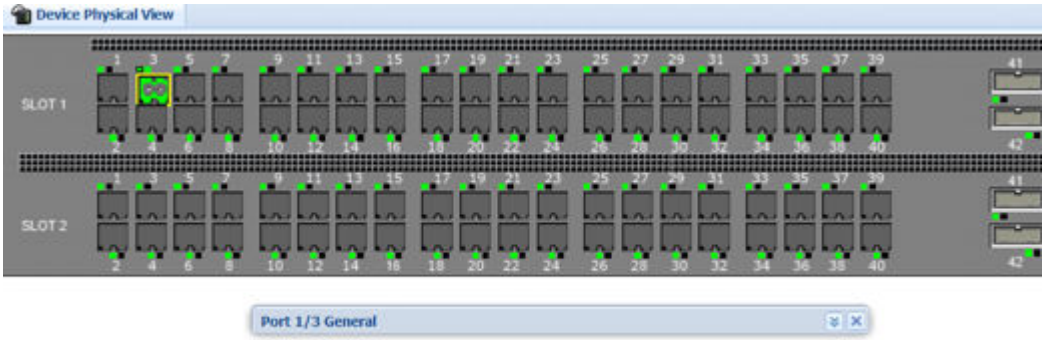
Procedure

1. Click the **Device Physical View** tab.
2. In the Device Physical View, select a port. In this example, right-click port 3.
3. In the Port shortcut menu, click **Edit General**.
4. Click and drag the Port 1/3 General tab wherever you want on the screen as shown in the following figure.



5. To reposition the tab anywhere on the screen, click and drag the title bar.
6. To manipulate the tab, click on the buttons in the top-right of the dialog box.

7. Click the up arrowhead to minimize the tab as shown in the following figure.



8. Click the down arrowhead to restore the tab to its original size.
9. Click the pages to dock the tab back into the menu bar.
10. Click the X to close the tab.

Installing EDM help files

While the EDM GUI is bundled with the switch software, the associated EDM help files are not. To access the help files from the EDM GUI, you must install the EDM help files on a TFTP or FTP server in your network.

Use the following procedure to install the EDM help files on a TFTP or FTP server, and configure EDM to use the help files

Before you begin

If you use an FTP server to store the help files, ensure that you configure the switch with the host user name and password.

Procedure

1. Download the EDM help file.
2. On a TFTP or FTP server reachable from the switch, create a directory called **Help**.

   Tip:

   You can name the directory anything that will help you remember its purpose.
3. Unzip the EDM help zip file into the directory created in the preceding step.
4. In the EDM navigation pane, expand the **Configuration** > **Security** > **Control Path** folders.
5. Click **General**.
6. Click **Web**.
7. In the **HelpTftp/Ftp_SourceDir** field, enter the IP address of the file server and the path to the help files, for example, 192.0.2.15:/home/Help/.

Multiple users per role configuration using EDM

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

The following section provides procedures to configure multiple users per role.

Creating Multiple Users

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

You can create up to seven new CLI user roles on the switch, in addition to the three default CLI user roles. The username must be unique. If you enable the hsecure flag, password complexity rules apply to all users.

Before you begin

You must use an EDM account with read-write-all privileges to create new CLI users.

About this task

Use this task to create multiple CLI users on the switch using EDM.

Procedure

1. In the navigation pane, expand **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Multiple Users** tab.
4. Click **Insert**.
5. Type the ID.
6. Type a unique user name.
7. Type a password.
8. Select the access level.
9. Select **Enable** to activate the user account.
10. Click **Insert**.

Multiple Users field descriptions

Use the data in the following table to the use the Multiple Users tab.

Name	Description
Id	Specifies the unique ID.
Name	Specifies the username.
Password	Specifies the password.
Level	Specifies the user access level. • ro • rw • rwa
Enable	Enables the user access on the switch.
Type	Specifies the user type.

Modify User Passwords

About this task

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Use this task to modify user account passwords using EDM.

Procedure

1. In the navigation pane, expand **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Multiple Users** tab.
4. To change the user account password, double-click the **Password** field.
5. Click **Apply**.

Disable a User Account

About this task

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Use this task to disable a user account using EDM.

Note:

Users with rwa access rights cannot be disabled. Only users with ro and rw access rights can be disabled.

Procedure

1. In the navigation pane, expand **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Multiple Users** tab.
4. View whether the user account is enabled. To modify, double-click on the cell and select false from the list.
5. Click **Apply**.

Delete a User Account

About this task

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Use this task to delete a user account using EDM. You cannot delete default ro, rw, and rwa users.

Procedure

1. In the navigation pane, expand **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Multiple Users** tab.
4. Select the row with the user account to delete and click **Delete**.
5. Click **Yes** to confirm.

Enable Authentication for Privileged EXEC Command Mode

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Chassis**.
3. Select the **System Control** tab.
4. Select **PrivExecPasswordEnable**.

System Control Field Descriptions

Use the data in the following table to use the System Control tab.

Name	Description
TcpTimestamp	Enables or disables the TCP timestamp. The timestamp is enabled by default. The system displays the following warning message when a new configuration is applied: `Warning: Existing TCP connections won't be affected. A config save and reboot is required to apply this configuration for all TCP connections.`
PrivExecPasswordEnable	Enables authentication for Privileged EXEC CLI command mode. Authentication is disabled by default.
KeepaliveTime **Note:** Exception: Not supported on VSP 8600 Series.	Specify the TCP keepalive time in seconds. Range is 5 to 65535 and default is 60.
KeepaliveInterval **Note:** Exception: Not supported on VSP 8600 Series.	Specify the TCP keepalive interval an seconds. Range is 1 to 3600 and the default is 10.
KeepaliveProbes **Note:** Exception: Not supported on VSP 8600 Series.	Specify the TCP keepalive probes. Range is 1 to 50 and the default is 5.

File Management in EDM

This setion contains procedures for managing files with Enterprise Device Manager (EDM).

Use the File System tab to perform the following tasks:

- Copy a file.
- Check the amount of memory used and the number of files stored in the internal flash memory.
- Verify the name, size, and storage date of each file present in the internal flash memory.
- Display USB file information.

Copy a File

About this task

Copy files on the internal flash.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **Copy File** tab.
4. Edit the fields as required.
5. Click **Apply**.

Copy File Field Descriptions

Use the data in the following table to use the **Copy File** tab.

Name	Description
Source	Identifies the device and file name to copy. You must specify the full path and filename, for example, `<deviceip-ftp server>:/<filename>`
Destination	Identifies the location to which to copy the source file with the filename, for example, `/intflash/<filename>`
Action	Starts or stops the copy process.
Result	Specifies the result of the copy process: • none • inProgress • success • fail • invalidSource • invalidDestination • outOfMemory • outOfSpace • fileNotFound

Display Storage Use

About this task

Display the amount of memory used, memory available, and the number of files for internal flash memory.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **Storage usage** tab

Storage Usage Field Descriptions

Use the data in the following table to use the Storage Usage tab.

Name	Description
IntflashBytesUsed	Specifies the number of bytes used in internal flash memory.
IntflashBytesFree	Specifies the number of bytes available for use in internal flash memory.
IntflashNumFiles	Specifies the number of files in internal flash memory.
UsbBytesUsed	Specifies the number of bytes used in USB device.
UsbBytesFree	Specifies the number of bytes available for use in USB device.
UsbNumFiles	Specifies the number of files in USB device.

Display Internal Flash File Information

About this task

Display information about the files in internal flash memory on this device.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **Flash Files** tab.

Flash Files field descriptions

Use the data in the following table to use the Flash Files tab.

Name	Description
Slot	Specifies the slot number.
Name	Specifies the directory name of the file.
Date	Specifies the creation or modification date of the file.
Size	Specifies the size of the file.

Display USB File Information

About this task

Display information about the files on a USB device to view general file information.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **USB Files** tab.

USB Files field descriptions

Use the data in the following table to use the **USB Files** tab.

Name	Description
Slot	Specifies the slot number of the device.
Name	Specifies the directory name of the file.
Date	Specifies the creation or modification date of the file.
Size	Specifies the size of the file.

Chapter 5: Extreme Integrated Application Hosting

Table 14: Extreme Integrated Application Hosting product support

Feature	Product	Release introduced
For configuration details, see Configuring User Interfaces and Operating Systems for VOSS.		
Extreme Integrated Application Hosting (IAH)	VSP 4450 Series	Not Supported
	VSP 4900 Series	VOSS 8.1.5 VSP4900-12MXU-12XE and VSP4900-24XE only
	VSP 7200 Series	Not Supported
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	Not Supported
	VSP 8400 Series	Not Supported
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported
Fabric IPsec Gateway	VSP 4450 Series	Not Supported
	VSP 4900 Series	Not Supported
	VSP 7200 Series	Not Supported
	VSP 7400 Series	VOSS 8.2
	VSP 8200 Series	Not Supported
	VSP 8400 Series	Not Supported
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported

Extreme Integrated Application Hosting

Extreme Integrated Application Hosting (IAH) architecture provides a flexible and open solution that enables organizations to deploy high-performance and flexible visibility applications pervasively throughout their network for improved monitoring and troubleshooting. Enabled by VOSS, this

preconfigured Quick Emulator (QEMU) Kernel-based Virtual Machine (KVM) environment leverages high performance x86 CPUs to host these applications, extending visibility customized to the business and operational needs of the organization across the entire network.

The QEMU KVM environment supports several pretested and well-known packet capture applications in a Linux virtual machine, including Wireshark and tcpdump. There are a wide variety of additional applications, tools, and utilities that organizations are able to run in this environment, such as data analytics applications, packet generators, monitoring tools, troubleshooting utilities, and many others. While the QEMU KVM environment is open and can host any application, it is designed and ideally suited for networking applications, tools, and utilities.

IAH architecture supports the creation and use of virtualization domains, such as virtual machines, and Docker containers. This design creates a common-use host, which coordinates and automates multiple guest-networking functions into chains. The hardware boots into the virtual Linux OS, providing the ability to run additional applications or services within a specific virtual machine or a Docker container, and simultaneously supporting the regular functionality of the switch.

Yet Another Next Generation (YANG) model is used to manage configuration and retrieve operational data. You access the YANG model through Representational State Transfer Configuration Protocol (RESTCONF) using a northbound interface, namely Extreme Management Center, that provides an additional way to configure and monitor the switch. For more information on RESTCONF, see Representational State Transfer Configuration Protocol (RESTCONF) Fundamentals on page 134.

Virtual Services Resources

The virtual services resources are isolated from each other, as well as from the Network Operating System (NOS) running the switch.

The resources available for all virtual services on VSP 7400 Series switches are as follows:

- - Six Central Processing Unit (CPU) cores
  - 12 GB Random Access Memory (RAM)
  - 100 GB Solid State Drive (SSD) flash memory

The resources available for all virtual services on VSP 4900 Series switches are as follows:

Note:

You must install a modular SSD unit to use virtual services on VSP 4900 Series switches.

- - Two CPU cores
  - 4 GB RAM
  - 120 GB SSD flash memory (separately available modular SSD unit), with 104 GB dedicated for IAH storage.

The switch OS uses the following resources on VSP 7400 Series and VSP 4900 Series:

- Two CPU cores
- 4 GB RAM
- 8 GB internal flash memory storage

Extreme Integrated Application Hosting Ports

Extreme Integrated Application Hosting (IAH) ports are labeled as Insight ports, which are internal ports used to support Ethernet connectivity by the virtual services configured on the switch. ports operate at 10 Gigabits per second (Gbps). The following features support IAH ports on the switch:

- VLANs
- Filters
- Port Statistics
- Basic Interface Configuration
- Mirroring
- Switched UNI - Demonstration purposes only
- Transparent Port UNI - Demonstration purposes only

Note:

Network-to-network (NNI) interface support is not available for IAH ports. IS-IS adjacencies cannot be estabilised on IAH ports.

Note:

Support for Switched UNI and Transparent Port UNI is available with the IAH enhancements demonstration feature.

Demonstration features are provided for testing purposes. Demonstration features are for lab use only, and are not for use in a production environment.

For information about how to configure IAH ports, see the following tasks:

- Configure a Virtual Service on page 81
- Configure Virtual Ports on page 96

Connection Types

The VM and Docker virtual ports map to a physical Extreme Integrated Application Hosting port using the following connection types:

- Open vSwitch (OVS)
- Single Root I/O Virtualization (SR-IOV).
- Virtualization Technology for Directed I/O (VT-d)

Note:

You must enable trunking on the Extreme Integrated Application Hosting port when you use SR-IOV and OVS connection types. For more information about enabling trunking, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.

With Integrated Application Hosting enhancements, Extreme Integrated Application Hosting ports 1/s1 and 1/s2 can be configured to accommodate different connect types. Extreme Integrated Application Hosting ports 1/s1 and 1/s2 can accommodate virtual ports of SR-IOV, OVS, or VT-d connect types. Two VT-d connetion types are supported on either 1/s1 or 1/s2 Extreme Integrated Application Hosting ports. Using the **`virtual-service`** command, you can specify which Extreme Integrated Application Hosting port is associated with the configured connect type. You can also configure the Network Interface Card (NIC) type of the virtual port using the **`virtual-service`** command.

Note:

Product Notice: Integrated Application Hosting enhancements are available for demonstration purposes only on VSP4900-24XE, VSP4900-12MXU-12XE, VSP 7432CQ, and VSP 7400-48Y platforms.

Demonstration features are provided for testing purposes. Demonstration features are for lab use only, and are not for use in a production environment.

The following table lists the compatible Extreme Integrated Application Hosting port connect type configurations.

Note:

Two virtual services with conflicting connect types or two virtual services with VT-d connect type cannot be configured on the same Extreme Integrated Application Hosting port.

Extreme Integrated Application Hosting port 1/s1	Extreme Integrated Application Hosting port 1/s2
SR-IOV	OVS
SR-IOV	SR-IOV
OVS	SR-IOV
OVS	OVS
VT-d	VT-d

Link Flapping

When the switch initializes, the Extreme Integrated Application Hosting ports connect to the underlying Linux hypervisor. When a virtual port of connection type OVS or SR-IOV is configured on the switch, the Linux hypervisor saves this connection, and the link state of the Extreme Integrated Application Hosting port does not change. However, when a virtual port of connection type VT-d is configured on the switch, control of the Extreme Integrated Application Hosting port is passed from the Linux hypervisor to the configured Virtual Machine (VM). The Extreme Integrated Application Hosting port flaps due to this transition, and the switch reports it in the system log. The Extreme Integrated Application Hosting port flaps twice during the transition:

1. when the Extreme Integrated Application Hosting port is removed from the Linux hypervisor.
2. when the Extreme Integrated Application Hosting port is added to the VM.

A similar link flap sequence takes place on the Extreme Integrated Application Hosting port when the associated VM is disabled on the switch, and the control of the Extreme Integrated Application Hosting port is passed from the VM back to the Linux hypervisor.

Third Party Virtual Machine

The Extreme Integrated Application Hosting (IAH) feature supports the pre-installed Third Party Virtual Machine (TPVM). For switches that use a modular Solid State Drive (SSD) for IAH , the virtual machine is pre-installed on the modular SSD. For switches that do not use a modular Solid State Drive (SSD) for IAH , the virtual machine is pre-installed on the switch.

You can use the **`show virtual-service config`** command to view the information about the pre-installed virtual machine on the switch. For more information, see Display Virtual Service Configuration on page 88.

Important:

You must upgrade virtual services independently of a VOSS upgrade; separate images for virtual services are available. For more information, see Upgrade a Virtual Service on page 91.

For more information about how to configure virtual services, see Virtual Services Configuration using CLI on page 80 and Virtual Services Configuration using EDM on page 93.

Third Party Virtual Machine (TPVM) provides a set of troubleshooting tools on the switch. The following installed packages are available on TPVM:

- build-essential
- checkinstall
- iperf
- mtools
- netperf
- qemu-guest-agent
- tshark
- valgrind
- vim-gnome
- wireshark
- xterm

Important:

TPVM includes an administrator account with a default username and password. To ensure security, you must change the default password when you access TPVM for the first time, before enabling the IAH ports using the **`no shutdown`** command. The software automatically prompts you to change this password at first boot; no action can be taken with the VM until you change the password.

The following user applications are available on TPVM:

- Dynamic Host Configuration Protocol (DHCP) server
- Domain Name Server (DNS)
- Authentication, authorization, and accounting (AAA) server for Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control Service Plus (TACACS+).
- Syslog server
- Simple Network Management Protocol (SNMP) trap receiver
- Surricata - a free and open-source robust network threat detection engine that provides real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM), and offline packet capture (pcap) processing.
- Wireshark – a protocol analyzer that provides packet capturing and analysis.
- Ostinato - provides packet crafting, network traffic generation, and analysis with a user-friendly Graphical User Interface (GUI).

Note:

If you start the console for TPVM without network connectivity to a DHCP server, the VM remains in a retry loop for approximately 5 minutes while it tries to obtain a DHCP address. The system displays the following message: `[FAILED] Failed to start Raise network interfaces`, and then the VM continues to boot. The VM does start but with the virtual port, eth0, in the administratively down state.

The following are the recommended virtual services resources for TPVM:

- Two CPU cores
- 4 GB RAM
- One virtual port of VT-d connection type
- 1.8 GB up to 32 GB SSD

Important:

To enable SR-IOV and VT-d, the guest OS must have Ethernet drivers (ixgbe) that support these Intel technologies. These drivers are not available by default in many OS distribution versions. The TPVM version based on Ubuntu 16.04 is enhanced to include updated driver versions to support SR-IOV and VT-d. If you upgrade the TPVM guest OS kernel, you override these drivers and the VM does not support SR-IOV or VT-d vport connection types.

Do not perform a kernel upgrade from within the TPVM. If necessary, you can upgrade individual packages. You can upgrade to Ubuntu 18.04, which includes support for these new driver versions by default.

Fabric IPsec Gateway Fundamentals

The Fabric IPsec Gateway feature introduces a new Virtual Machine (VM) that supports aggregation of Fabric Extend Tunnels with fragmentation, reassembly, and Internet Protocol Security (IPsec) encryption functions for VSP 7400 Series switches.

The minimum configuration requirements for the Fabric IPsec Gateway VM are as follows:

- Two Central Processing Unit (CPU) cores
- 4 GB Random Access Memory (RAM)
- One Virtualization Technology for Directed I/O (VT-d) vport (eth0)

To configure IPsec on a VSP 7400 Series switch through the Fabric IPsec Gateway VM, see Fabric IPsec Gateway Configuration using CLI on page 99.

Fabric IPsec Gateway supports the following services through the VM:

- IPsec with fragmentation and reassembly - for the VXLAN traffic that needs IPsec, the network routes the packets through the Fabric IPsec Gateway VM that provides IPsec encryption and decryption for VXLAN packets. The system also supports fragmentation and reassembly for IPsec tunnels that you configure on the VM, and a minimum of 1300 bytes of Maximum Transmission Unit (MTU) value.
- Fragmentation and reassembly - the Fabric IPsec Gateway VM performs fragmentation and reassembly for VXLAN and IPsec tunnels, for which the network routes the packets through the VM. The system supports a minimum of 750 bytes of Maximum Transmission Unit (MTU) value.

IPsec Coupled and Decoupled Mode

A device is in IPsec decoupled mode when IPsec and Fabric Extend (FE) termination takes place on two different IP addresses. And, it is in IPsec coupled mode when IPsec and Fabric Extend (FE) termination takes place on the same IP address.

The XA1400 Series devices support both IPsec decoupled and coupled modes. But, the VSP 7400 Series devices support IPsec in decoupled mode only. You must configure IPsec tunnel in decoupled mode to enable IPsec termination in the Fabric IPsec Gateway VM. For more information about configuring IPsec tunnels on the VM, see Configure IPsec Tunnels on Fabric IPsec Gateway VM on page 106.

Operational Considerations and Restrictions

Consider the following when deploying Extreme Integrated Application Hosting (IAH) on various switches:

Table 15: Operational Considerations

	VSP 7400 Series	VSP 4900 Series
Number of IAH ports	VSP 7432CQ: 2 VSP 7400-48Y: 1	2
Multiple simultaneous VMs	Supported	Not supported
Pre-installed VM	Third Party Virtual Machine	Third Party Virtual Machine

Table continues…

	VSP 7400 Series	VSP 4900 Series
	Extreme Encryption Engine (EEE) (for demonstration purposes only)	
Additional components required	None	Modular Solid State Drive (SSD)

Note:

Extreme Encryption Engine is introduced with Fabric IPsec Gateway. Fabric IPsec Gateway is a demonstration feature.

Demonstration features are provided for testing purposes. Demonstration features are for lab use only, and are not for use in a production environment.

Virtual Services Configuration using CLI

Perform the procedures in this section to configure Extreme Integrated Application Hosting (IAH) virtual services on the switch using the command line interface (CLI).

Access a Virtual Service Console

The virtual services running on a Virtual Machine (VM) require a console for configuration and monitoring purposes.

About this task

Perform this procedure to access the virtual service console port for the specific VM.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Enter the following command to access the virtual service console:

   ```
   virtual-service WORD<1-80> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

Example

```
Switch:1>enable
Switch:1#virtual-service tpvm console
```

Variable Definitions

Use data in the following table to use the **`virtual-service`** command.

Variable	Value
WORD<1-80>	Specifies the virtual service name.
console	Accesses the console for the specific virtual service.

Install a Virtual Service

A virtual service provides the ability to support additional applications or services and simultaneously support the regular switching functionality. Each virtual service provides an Open Virtual Appliance (OVA) image, which is installed on Extreme Integrated Application Hosting (IAH) through Extreme Management Center.

Before you begin

- Use FTP or SFTP to transfer the OVA image to the `/var/lib/insight/packages/` directory on the switch.

About this task

Perform this procedure to install a package file to a specific location indicated by a virtual service name. This procedure also verifies if the package is in OVA format, and if a certificate is provided in the package.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Install the virtual service package:

   ```
   virtual-service WORD<1-80> install package WORD<1-512>
   ```

Variable Definitions

The following table defines parameters for the **`virtual-service`** command.

Variable	Value
WORD<1-80>	Specifies the virtual service name.
install	Installs the virtual service package.
package *WORD<1-512>*	Specifies the package name and path.

Configure a Virtual Service

About this task

Perform this procedure to configure a virtual service on the switch.

Note:

- Following procedure lists the general sequence to configure a virtual service.

- The names of Ethernet ports appearing in a specific Virtual Machine (VM) are not correlated to the configured virtual port names. Each VM renames the Ethernet ports as per its requirements, after they are discovered during the VM initialization.
- By default, all virtual ports of OVS connection type appear first in the alphabetical order of their configured names, followed by the virtual ports of SR-IOV and VT-d connection types.

Before you begin

- You must enable trunking on the Extreme Integrated Application Hosting (IAH) port when you use SR-IOV and OVS connection types. For more information about enabling trunking, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.
- Ensure the switch has the Ethernet drivers installed as per the SR-IOV standard, to support the VT-d and the SR-IOV connection type for the configured virtual ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create a VLAN:

   Note:

   Virtual service configuration supports port based VLANs only.

   ```
   vlan create <2-4059> name WORD<0-64> type {port-mstprstp <0-63>}
   [color <0-32>]
   ```

3. Add the IAH and faceplate port to the VLAN:

   ```
   vlan members add <1-4059> {slot/port[/sub-port][-slot/port[/sub-
   port]][,...]}
   ```

4. Enter GigabitEthernet Interface Configuration mode:

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-
   port]][,...]}
   ```

   Note:

   If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

5. Enable the IAH and faceplate ports:

   ```
   no shutdown
   ```

6. Exit to Global Configuration mode:

   ```
   exit
   ```

7. **(Optional)** Create a virtual service:

   ```
   virtual-service WORD<1-80>
   ```

Note:

IAH supports pre-installed virtual machines. For more information, see Third Party Virtual Machine on page 77.

8. **(Optional)** Configure the number of CPU cores to be assigned to the virtual service created:

```
virtual-service WORD<1-80> num-cores <1-6>
```

9. **(Optional)** Configure the memory size to be assigned to the virtual service created:

```
virtual-service WORD<1-80> mem-size <1-50000>
```

10. **(Optional)** Configure the disk to be assigned to the virtual service created:

```
virtual-service WORD<1-80> disk WORD<1-32> size <1-30>
```

11. Configure the virtual port connection type:

Note:

Ensure the connection type you configure for the virtual port matches the connection type supported by the IAH port.

```
virtual-service WORD<1-80> vport WORD<1-32> connect-type {ovs |
sriov | vtd}
```

12. Configure the IAH port to associate with the connection type:

Note:

Demonstration feature- Extreme Integrated Application Hosting enhancements: This step is available for demonstration purposes only.

Demonstration features are provided for testing purposes. Demonstration features are for lab use only, and are not for use in a production environment.

```
virtual-service WORD<1-80> vport WORD<1-32> port WORD<1-32>
```

Important:

Two virtual services with conflicting connect types cannot be configured on the same IAH port. You cannot configure two virtual services with VT-d connect type on the same IAH port.

13. Configure the NIC type of the IAH port.

Note:

Demonstration feature- Extreme Integrated Application Hosting enhancements: This step is available for demonstration purposes only.

Demonstration features are provided for testing purposes. Demonstration features are for lab use only, and are not for use in a production environment.

```
virtual-service WORD<1-80> vport WORD<1-32> port WORD<1-32> nic-type
{virtio | e1000}
```

14. Add the virtual port to the VLAN created:

    ```
    virtual-service WORD<1-80> vport WORD<1-32> vlan <1-4096>
    ```

15. Enable the virtual service:

    ```
    virtual-service WORD<1-80> enable
    ```

Example

Configuring the TPVM virtual service using IAH port 1/s1 with an SR-IOV connection type:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 1/s1
Switch:1(config-if)#encapsulation dot1q
Switch:1(config-if)#exit
Switch:1(config)#vlan create 10 name tpvm-lan-vlan type port-mstprstp 0
Switch:1(config)#vlan members add 10 1/s1,1/6/2
Switch:1(config)#interface GigabitEthernet 1/s1,1/6/2
Switch:1(config-if)#no shutdown
Switch:1(config-if)#exit
Switch:1(config)#virtual-service tpvm vport eth0 connect-type sriov
Switch:1(config)#virtual-service tpvm vport eth0 vlan 10
Switch:1(config)#virtual-service tpvm enable
```

Configuring the TPVM virtual service on IAH port 1/s2 with a VT-d connection type:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#vlan create 10 type port-mstprstp 0
Switch:1(config)#vlan member add 10 1/1,1/s2
Switch:1(config)#interface GigabitEthernet 1/s2,1/1
Switch:1(config-if)#no shutdown
Switch:1(config-if)#exit
Switch:1(config-if)virtual-service tpvm vport eth0 port 1/s2
Switch:1(config)#virtual-service tpvm enable
```

Variable Definitions

Use data in the following table to use the **`vlan create`** command:

Variable	Value
<2-4059>	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.
color*<0–32>*	Specifies the color of the VLAN.
name*WORD<0-64>*	Specifies a name for the VLAN to be created.
type {port-mstprstp*<0-63>*}	Creates a VLAN by port, with the STP instance ID ranging from 0 to 63.

Table continues…

Variable	Value
	Note: MSTI instance 62 is reserved for SPBM if SPBM is enabled on the switch.

Use data in the following table to use the **`vlan members`** command:

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
add	Adds ports to a specified VLAN ID.

Use data in the following table to use the **`virtual-service`** command:

Variable	Value
WORD<1-80>	Specifies a name for virtual service.
connect-type *{ovs | sriov | vtd}*	Specifies the connection type for the virtual port created. The default is VT-d. The switch supports the following maximums for virtual ports: • OVS - 16 • SR-IOV - 16 • VT-d - 1 **Note:** Demonstration feature- With Extreme Integrated Application Hosting (IAH) enhancements, the switch can support the maximum value of two VT-d virtual port connect types.
disk *WORD<1-32>*	Specifies the disk assigned to the virtual service.
mem-size *<1-50000>*	Specifies the memory size in Megabytes assigned to the virtual service. The default value is 1024 Megabytes.
nic-type *[virtio | e1000]*	Specifies the Virtual Port NIC type. The default is virtio.

Table continues…

Variable	Value
Note: Demonstration feature- This command option is available for demonstration purposes only with Extreme Integrated Application Hosting enhancements. This command does not apply to all hardware platforms.	
num-cores *<1-6>*	Specifies the number of cores assigned to the virtual service. The default value is 1.
port *WORD<1-32>* **Note:** Demonstration feature- This command option is available for demonstration purposes only with Extreme Integrated Application Hosting enhancements. This command does not apply to all hardware platforms.	Specifies the name of the Extreme Integrated Application Hosting (IAH) port associated with the virtual port. The switch supports the following IAH ports: • 1/s1 • 1/s2
size *<1-30>*	Specifies the size of the disk in Gigabytes.
vlan *<1–4096>*	Specifies the VLAN ID used by the virtual port.
vport *WORD<1-32>*	Specifies the name of the virtual port.

Note:

Demonstration features are provided for testing purposes. Demonstration features are for lab use only, and are not for use in a production environment.

Shut Down a Virtual Service

About this task

Perform this procedure to disable the virtual service.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable the virtual service:

   ```
   no virtual-service WORD<1-80> enable
   ```

Example

Disable the virtual service.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#no virtual-service tpvm enable
```

Delete Virtual Service Resources

About this task

Perform this procedure to delete the virtual service resource allocation.

Note:

If a corresponding virtual machine is running, it is stopped, and then the virtual service configuration is deleted.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Delete the virtual service resource allocation:

   ```
   no virtual-service WORD<1-80> [disk WORD<1-32>] [vport WORD<1-32>]
   ```

Example

Delete all virtual service resource allocation.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#no virtual-service tpvm
```

Uninstall a Virtual Service

About this task

Perform this procedure to uninstall a configured virtual service.

Note:

If a virtual machine is running, it is stopped, and then the service directory is uninstalled.

Before you begin

You must disable the virtual service before you uninstall it.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Uninstall a specific virtual service:

   ```
   virtual-service WORD<1-80> uninstall
   ```

Example

```
Switch:1>enable
Switch:1#virtual-service tpvm uninstall
```

Variable Definitions

Use data in the following table to use the **`virtual-service`** command.

Variable	Value
WORD<1-80>	Specifies the virtual service name.
uninstall	Uninstalls the specified virtual service name.

Display Virtual Service Configuration

About this task

Perform this procedure to display the virtual service configuration on the switch.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display the virtual-service configuration:

   ```
   show virtual-service config [WORD<1-80>]
   ```

Example

Display the configuration of a specific virtual service:

Note:

`Name` displayed in the following show output is the Virtual Machine (VM) image name and not the version of the application within the VM. You can see the version of the application by logging in to the console. For more information, see Access a Virtual Service Console on page 80.

```
Switch:1>show virtual-service config tpvm
================================================================================
                            Virtual Services Config
================================================================================

Virtual Service :tpvm
Additional Disk Assigned:
   Name           Size(GB)
   vdb               2
```

```
  VPort Information:
  Name            Vlan      Connect Type
  eth0            100       sriov

Management Status :         Enabled
-------------------------------------------------------------------------
```

The following sample output shows the Extreme Integrated Application Hosting (IAH) enhancements available for demonstration purposes only.

Note:

Demonstration features are provided for testing purposes. Demonstration features are for lab use only, and are not for use in a production environment.

```
Switch:1>show virtual-service config tpvm
=========================================================================
                           Virtual Services Config
=========================================================================

Virtual Service :tpvm
Additional Disk Assigned:
   Name           Size(GB)
   vdb               2


  VPort Information:
  Name            Vlan      Connect Type    Insight Port    NIC Type
  InsightPort                   vtd             1/s1
  eth0                          ovs             1/s1         VIRTIO

Management Status :         Enabled
-------------------------------------------------------------------------
```

Display Virtual Service Installation Status

About this task

Perform this procedure to display the installation status for the specific virtual service. This procedure indicates if the installation finished successfully or failed to complete.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display installation status for a specific virtual service:

   ```
   show virtual-service install WORD<1-80>
   ```

Example

Display installation status for a specific virtual service:

```
Switch:1>show virtual-service install tpvm
        Stage:   Convert
        Status:  In Progress
```

Display Virtual Services Resources

About this task

Perform the following procedure to display the number of remaining virtual services resources on the switch.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display statistics for all virtual services configured on the switch or a specific virtual service:

   ```
   show virtual-service statistics [WORD<1-80>]
   ```

Example

Note:

```
Switch:1>show virtual-service statistics
================================================================================
                          Virtual Services
================================================================================
Virtual Service :     tpvm

Memory Utilization (Mega Bytes)
  Allocated     Used    Available
   1024         726       298

CPU Utilization
  Allocated(# cores)     CPU Utilization (Total %)
           1               0

Disk Utilization
  Primary Disk Size  :     10G


VPort Information:

  Name      Vlan        Connect Type    Insight Port      NIC Type
  eth0       20           ovs           1/s1           VIRTIO
    Guest Intf Name : eth0
    MAC Address     : 3e:19:9b:00:01:00
    IPv4 Address    : 192.0.2.1
    IPv6 Address    : 2001:0db8:3c4d:0015:0000:0000:1a2f:1aaa

Management Status   :     Enabled
Operational Status  :     Running
Uptime  :         2 day(s), 01:43:37
--------------------------------------------------------------------------------

================================================================================
                          Hypervisor Remaining Resources
================================================================================
    Number of Cores Remaining:  5
    Total Memory Remaining(M):  11411
    Total Disk Remaining(GB):  13
```

The following sample output shows the Extreme Integrated Application Hosting (IAH) enhancements available for demonstration purposes only.

Note:

Demonstration features are provided for testing purposes. Demonstration features are for lab use only, and are not for use in a production environment.

```
Switch:1>show virtual-service statistics
================================================================================
                          Virtual Services
================================================================================

Virtual Service :     tpvm

Memory Utilization (Mega Bytes)
  Allocated     Used    Available
   0             0          0

CPU Utilization
  Allocated(# cores)     CPU Utilization (Total %)
           0              0

Disk Utilization
 Addtional Disk Name:     vdc
  Allocated(M)          Used(M)     Available(M)
       4975              9           4693


VPort Information :
  Name                    Vlan      Connect Type    Insight Port    NIC Type
  InsightPort                           vtd             1/s1


Management Status   :     Not Enabled
Operational Status  :     Not Running
Uptime  :                 0 day(s), 00:00:00
--------------------------------------------------------------------------------

================================================================================
                          Hypervisor Remaining Resources
================================================================================
    Number of Cores Remaining:  6
    Total Memory Remaining(M):  12435
    Total Disk Remaining(GB):   85
```

Upgrade a Virtual Service

If Extreme Networks makes a new version of the virtual service available, uninstall the original virtual service and install the newer virtual service.

Important:

You can perform an upgrade of Linux inside the virtual service by standard Linux upgrade procedures. For example, TPVM is Ubuntu based, so you can use **`sudo apt-get update`** and **`sudo apt-get upgrade`**. If you complete such an upgrade, Extreme Networks is not responsible for the behavior of the VM; it has not been tested with that version on the OS.

Before you begin

- If you installed applications in the Third Party Virtual Machine (TPVM), you must migrate important data for those applications before you perform this procedure.

- If you created new users in the TPVM, follow standard Linux procedures to back up user names and passwords.
- For Fabric IPsec Gateway, back up the configuration files (*.cfg) and the `shadov.txt` file, which is an encrypted file that contains the authentication keys for the IPsec tunnels. You can use the **`ls`** command within the VM to see the file list. Use FTP within the VM to transfer the files for backup.
- Use FTP or SFTP to transfer the new OVA image to the `/var/lib/insight/packages/` directory on the switch.

About this task

When you uninstall the original virtual service, the system removes the complete virtual service configuration from the configuration file.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable the virtual service:

   ```
   no virtual-service WORD<1-80> enable
   ```

3. Return to Privileged EXEC mode:

   ```
   end
   ```

4. Uninstall the virtual service:

   ```
   virtual-service WORD<1-80> uninstall
   ```

5. Install the virtual service package using the new OVA image:

   ```
   virtual-service WORD<1-80> install package WORD<1-512>
   ```

6. Reconfigure the virtual service; for more information, see Configure a Virtual Service on page 81.

7. Remove the original OVA image from the `/var/lib/insight/packages/` directory on the switch.

   ```
   remove WORD<1-255>
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#no virtual-service tpvm enable
Switch:1(config)#end
Switch:1#virtual-service tpvm uninstall
Switch:1#virtual service tpvm install package var/lib/insight/packages/
TPVM_4900_8.2.0.0.img
Switch:1#configure terminal
Switch:1(config)#virtual-service tpvm vport eth0 connect-type sriov
Switch:1(config)#virtual-service tpvm vport eth0 vlan 10
Switch:1(config)#virtual-service tpvm enable
Switch:1(config)#remove /intflash/var/lib/insight/packages/TPVM_4900_8.1.5.0.img
```

Virtual Services Configuration using EDM

Perform the procedures in this section to configure Extreme Integrated Application Hosting (IAH) virtual services on the switch using the Enterprise Device Manager (EDM).

Viewing Virtual Services Resources

About this task

Perform the following procedure to view the number of remaining virtual services resources on the switch.

Procedure

1. In the navigation pane, expand the **Configuration** > **Serviceability** folders.
2. Click **Virtual Service**.
3. Click the **Globals** tab.

Globals Field Descriptions

Use data in the following table to use the Globals tab.

Name	Description
DiskRemain	Shows the remaining disk space available, in Gigabytes (GB).
NumCoresRemain	Shows the remaining number of CPU cores available.
MemSizeRemain	Shows the remaining amount of memory size available, in Megabytes (MB).

Configure a Virtual Service

About this task

Perform this procedure to configure a virtual service on the switch.

Before you begin

You must configure at least one virtual port to enable the virtual service. For more information, see Configure Virtual Ports on page 96.

Procedure

1. In the navigation pane, expand the **Configuration** > **Serviceability** folders.
2. Select **Virtual Service**.
3. Select the **Virtual Service** tab.

4. Select **Insert**.
5. In the **Name** field, enter a unique name.
6. **(Optional)** In the **NumCores** field, enter a value.
7. **(Optional)** In the **MemSize** field, enter a value.
8. Select **Insert**.
9. In the **Enable** field for the newly inserted row, change the value to true.
10. Select **Apply**.

Virtual Service Field Descriptions

Use data in the following table to use the Virtual Service tab.

Name	Description
Name	Specifies the name of the virtual service. Every virtual service must have a unique name.
NumCores	Specifies the number of CPU cores assigned to the virtual service. The default is 1.
MemSize	Specifies the memory size (in Megabytes) assigned to the virtual service. The default value is 1024 Megabytes.
Enable	Enables the virtual service. **Note:** You must configure at least one virtual port to enable the virtual service.
UtilCpuAllot	Specifies the number of CPUs allocated to the virtual service.
UtilCpuUtil	Specifies the average percentage of CPU utilization over the past 30 seconds.
UtilMemAllot	Specifies the memory (in Megabytes) allocated to the virtual service.
UtilMemUsed	Specifies the memory used (in Megabytes) by the virtual service.
UtilMemAvailable	Specifies the memory available (in Megabytes) for the virtual service.
State	Specifies the operational state of the virtual service.
UpTime	Specifies the operational time of the virtual service.

Configuring Disks to be used by the Virtual Service

About this task

Perform the following procedure to configure the number of disks to be used by the virtual service configured on the switch.

Procedure

1. In the navigation pane, expand the **Configuration** > **Serviceability** folders.
2. Click **Virtual Service**.
3. Click the **Disks** tab.
4. Click **Insert**.
5. In the **ServName** field, enter the virtual service name.
6. In the **Name** field, enter the disk name.
7. **(Optional)** In the **Size** field, enter a value.
8. Click **Insert**.

Disks Field Descriptions

Use data in the following table to use the Disks tab.

Name	Description
ServName	Specifies the virtual service name. **Note:** The specified name must match the virtual service name configured on the switch.
Name	Specifies the name of the disk used by the virtual service.
Size	Specifies the disk size (in Gigabytes). The default is 10 Gigabytes.
SizeAllot	Shows the disk size (in Megabytes) allocated to the virtual service.
SizeAvailable	Shows the available disk storage space (in Megabytes).
SizeUsed	Shows the amount of disk storage space (in Megabytes) used by the virtual service.

Configure Virtual Ports

About this task

Perform the following procedure to configure virtual ports to be used by the virtual service configured on the switch.

Note:

The names of Ethernet ports appearing in a specific Virtual Machine (VM) are not correlated to the configured virtual port names. Each VM renames the Ethernet ports as per its requirements, after they are discovered during the VM initialization.

By default, all virtual ports of OVS connection type appear first in the alphabetical order of their configured names, followed by the virtual ports of SR-IOV and VT-d connection types.

Before you begin

- You must enable trunking on the Extreme Integrated Application Hosting (IAH) port when you use SR-IOV and OVS connection types. For more information about enabling trunking, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.
- Ensure the switch has the Ethernet drivers installed as per the SR-IOV standard, to support the VT-d and the SR-IOV connection type for the configured virtual ports.

Procedure

1. In the navigation pane, expand the **Configuration** > **Serviceability** folders.
2. Select **Virtual Service**.
3. Select the **VPorts** tab.
4. Select **Insert**.
5. In the **Virtual Service Name** field, enter the virtual service name.
6. In the **Interface Name** field, enter a name for the virtual port.
7. **(Optional)** In the **VlanIdList** field, enter a VLAN ID.
8. **(Optional)** In the **ConnectType** field, select a connection type.

   Note:

   Ensure the connection type you configure for the virtual port matches the connection type supported by the IAH port.
9. Select **Insert**.

VPorts Field Descriptions

Use data in the following table to use the VPorts tab.

Name	Description
Virtual Service Name	Specifies the virtual service name. **Note:** The specified name must match the virtual service name configured on the switch.
Interface Name	Specifies the virtual port.
VlanIdList	Specifies the VLAN ID to which the virtual port is assigned.
ConnectType	Specifies the virtual port connect type. The default is VT-d. The switch supports the following maximums for virtual ports: • OVS - 16 • SR-IOV - 16 • VT-d - 1 **Note:** Demonstration feature- Extreme Integrated Application Hosting enhancements. The switch can support the maximum value of 2 for VT-d virtual port connect type.
Port **Note:** Demonstration feature- Extreme Integrated Application Hosting enhancements. This field option is available for demonstration purposes only.	Specifies the name of the Extreme Integrated Application Hosting port associated with the virtual port. The switch supports the following Extreme Integrated Application Hosting ports: • 1/s1 • 1/s2
NicType **Note:** Demonstration feature- Extreme Integrated Application Hosting enhancements. This field option is available for demonstration purposes only.	Specifies the Virtual Port NIC type. The default is virtio. • virtio • e1000

Demonstration features are provided for testing purposes. Demonstration features are for lab use only, and are not for use in a production environment.

Installing a Virtual Service

About this task

Perform the following procedure to configure the package information to be used by the virtual service.

Procedure

1. In the navigation pane, expand the **Configuration** > **Serviceability** folders.
2. Click **Virtual Service**.
3. Click the **Application** tab.
4. Click **Insert**.
5. In the **Name** field, enter the virtual service name.
6. Next to the **PackageName** field, click the ellipsis, select the package to install, and then click Ok.
7. Click **Insert**.

Application Field Descriptions

Use data in the following table to use the Application tab.

Name	Description
Name	Specifies the name of the virtual service.
PackageName	Specifies the name and location of the package.
InstallResult	Shows the status of the virtual service installation.
InstallStage	Shows the stages of a package installation.

Viewing Virtual Services Package File Information

About this task

Perform the following procedure to view information about the package files available in the `/var/lib/insight/packages` directory, which you can use to install a new virtual service.

Procedure

1. In the navigation pane, expand the **Configuration** > **Serviceability** folders.
2. Click **Virtual Service**.
3. Click the **PackageFile** tab.

PackageFile Field Descriptions

Use data in the following table to use the PackageFile tab.

Name	Description
Name	Shows the name and absolute path information for package files available in the `/var/lib/insight/packages` directory.

Table continues…

Name	Description
Date	Shows the date and time when the package file was added to the directory.
Size	Shows the size (in bytes) of the package file.

View Modular SSD Information

About this task

Perform this procedure to display information about an installed Solid State Drive (SSD) on a switch.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Chassis**.
3. Select the **SSD** tab.

SSD Field Descriptions

Use the data in the following table to use the SSD tab.

Name	Description
ProductName	Specifies Solid State Drive (SSD) product name.
VendorName	Specifies the SSD vendor.
ManufactureDate	Specifies the date on which the SSD was manufactured.
SerialNum	Specifies the SSD serial number.
PartNum	Specifies the SSD part number.
DeviceVersion	Specifies the version of the SSD.
TotalSize	Specifies the total memory size of the SSD.

Fabric IPsec Gateway Configuration using CLI

Perform the procedures in this section to configure services like IPsec, fragmentation and reassembly, and to manage the Fabric IPsec Gateway Virtual Machine using the command line interface (CLI).

Configure FTP Connection to an IP Address

Fabric IPsec Gateway Virtual Machine (VM) provides a File Transfer Protocol (FTP) CLI to copy the configuration files to the VM.

About this task

Perform this procedure to configure an FTP connection to a specific IP Address.

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Configure FTP connection:

   ```
   ftp {A.B.C.D}
   ```

Example

Configuring FTP connection to 192.0.2.50:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> ftp 192.0.2.50
```

Variable Definitions

The following table defines the variable for **`ftp`** command.

Variable	Value
{A.B.C.D}	Specifies the IP Address to establish the FTP connection with.

Display the Default Directory on Fabric IPsec Gateway VM

About this task

Perform this procedure to display content in the default directory on the Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

```
enable
virtual-service WORD<1-128> console
```

Note:

Type `CTRL+Y` to exit the console.

2. Display the configured directory:

```
ls
```

Example

Displaying the configured directory on the VM.

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> ls
coupled.cfg
```

Load Configuration File to Fabric IPsec Gateway VM

About this task

Perform this procedure to load a configuration file to the Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

```
enable
virtual-service WORD<1-128> console
```

Note:

Type `CTRL+Y` to exit the console.

2. Load a specific configuration file to the VM :

```
load WORD <1-255>
```

Example

Loading a configuration file to the VM.

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> load coupled.cfg
```

Variable Definitions

The following table defines the variable for **load** command.

Variable	Value
WORD <1-255>	Specifies the configuration file name.

Ping an IP Address on Fabric IPsec Gateway VM

About this task

Perform this procedure to ping an IP Address on the Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Ping an IP Address:

   ```
   ping {A.B.C.D}
   ```

Example

Pinging an IP Address on the VM.

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> ping 192.0.2.35
```

Variable Definitions

The following table defines parameters for the **ping** command.

Variable	Value
{A.B.C.D}	Specifies the IP address.

Configure Global Parameters on Fabric IPsec Gateway VM

About this task

Perform this procedure to configure IPsec source IP address, Local Area Network (LAN) interface IP and gateway IP address, maximum transmission unit (MTU) value, and so on globally, on the Fabric IPsec Gateway Virtual Machine (VM).

Note:

You must perform this procedure only after the VM boots up.

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Configure IPsec source IP address for a Fabric Extend (FE) tunnel for IPsec in decoupled mode:

   ```
   set global ipsec-tunnel-src-ip {A.B.C.D/X}
   ```

3. Assign VLAN ID to the configured IPsec source IP address:

   ```
   set global ipsec-tunnel-src-vlan <2-4059>
   ```

4. Configure the LAN interface IP address on the first Ethernet interface (eth0) of Fabric IPsec Gateway VM:

   ```
   set global lan-intf-ip {A.B.C.D/X}
   ```

5. Assign VLAN ID to the configured LAN interface IP address:

   ```
   set global lan-intf-vlan <2-4059>
   ```

6. Configure the LAN interface gateway IP address on the VOSS switch:

   ```
   set global lan-intf-gw-ip {A.B.C.D}
   ```

7. Configure the logical interface gateway IP address, to add routes for FE tunnels that need Fragmentation:

   ```
   set global fe-tunnel-gw-ip {A.B.C.D}
   ```

8. Configure the logical interface source IP address for the FE tunnel:

   ```
   set global fe-tunnel-src-ip {A.B.C.D}
   ```

Note:

The logical interface source IP address must be same as the source IP address configured on the VOSS switch.

9. Configure the global MTU value:

   ```
   set global mtu <mtu-value>
   ```

   Note:

   - The switch applies the global MTU value, if you do not configure MTU during the IPsec tunnel configuration.
   - If an IPsec tunnel is not using the fragmentation and reassembly capabilities, the default MTU value is 1950.

10. Configure the Wide Area Network (WAN) interface gateway IP address, which is the next hop for IPsec tunnels.

    ```
    set global wan-intf-gw-ip {A.B.C.D}
    ```

11. Configure the virtual reassembly interface IP address:

    ```
    set global virtual-reassembly-intf-ip {A.B.C.D/X}
    ```

    Note:

    You must configure the virtual reassembly interface IP address to use the fragmentation and reassembly service.

12. Assign VLAN ID to the configured virtual reassembly interface IP address:

    ```
    set global virtual-reassembly-intf-vlan <2-4059>
    ```

13. Disable IPsec on all configured tunnels:

    ```
    set global ipsec-disable
    ```

14. Set IPsec log level:

    ```
    set global ipsec-log-level <-1-5>
    ```

Example

Configuring global parameters on Fabric IPsec Gateway VM to configure an IPsec tunnel between two switches:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> set global ipsec-tunnel-src-ip 192.0.2.10/24
FIGW> set global ipsec-tunnel-src-vlan 101
FIGW> set global lan-intf-ip 192.0.2.20/24
FIGW> set global lan-intf-vlan 30
FIGW> set global lan-intf-gw-ip 192.0.2.30
FIGW> set global fe-tunnel-src-ip 192.0.2.40
```

```
FIGW> set global wan-intf-gw-ip 192.0.2.50
FIGW> set global mtu 1950
```

Variable Definitions

The following table defines parameters for the **`set global`** command.

Variable	Value
ipsec-tunnel-src-ip *{A.B.C.D/X}*	Specifies the source IP address and subnet mask for IPsec tunnel.
ipsec-tunnel-src-vlan *<2-4059>*	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.
lan-intf-ip *{A.B.C.D/X}*	Specifies the IP address and subnet mask for Local Area Network (LAN) interface.
lan-intf-vlan *<2-4059>*	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.
lan-intf-gw-ip *{A.B.C.D}*	Specifies the gateway IP address for LAN interface.
fe-tunnel-gw-ip *{A.B.C.D}*	Specifies the gateway IP address for Fabric Extend (FE) tunnel.
fe-tunnel-src-ip *{A.B.C.D}*	Specifies the source IP address for FE tunnel.
mtu *<750-9000>*	Specifies the Maximum Transmission Unit (MTU) value. **Note:** If an IPsec tunnel is not using the fragmentation and reassembly capabilities, the default MTU value is 1950.
wan-intf-gw-ip *{A.B.C.D}*	Specifies the Wide Area Network (WAN) interface gateway IP address.
virtual-reassembly-intf-ip *{A.B.C.D/X}*	Specifies the virtual-reassembly interface IP address and subnet mask on the Fabric IPsec Gateway (VM). **Note:** You must configure the virtual reassembly interface IP address to use the fragmentation and reassembly service.
virtual-reassembly-intf-vlan *<2-4059>*	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.
ipsec-disable	Disables IPsec operationally on all tunnels in the Fabric IPsec Gateway VM.

Table continues…

Variable	Value
ipsec-log-level <*-1-5*>	Specifies the IPsec log levels on Fabric IPsec Gateway VM. Following are the three levels: • -1: Absolutely Silent • 0-4: Log levels • 5: Clear Logs

Configure IPsec Tunnels on Fabric IPsec Gateway VM

About this task

Perform this procedure to configure IPsec tunnels on Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Configure the Maximum Transmission Unit (MTU) value for the specific IPsec tunnel:

   ```
   set ipsec <1-255> mtu <1300 - 9000>
   ```

   Note:

   The MTU range <1300-9000> is applicable for FE tunnels with IPsec and fragmentation and reassembly capabilities.

3. Configure the encryption key length for IPsec Tunnel:

   ```
   set ipsec <1-255> encryption-key-length <128 | 256>
   ```

   Note:

   By default, the encryption key length is 128 bytes.

4. Configure the authentication key for specific IPsec tunnel:

   ```
   set ipsec <1-255> auth-key WORD <1-32>
   ```

   Note:

   You must not use special characters ?, \, &, <, >, #.

5. Configure VXLAN destination IP address for IPsec tunnel:

   ```
   set ipsec <1-255> fe-tunnel-dest-ip {A.B.C.D}
   ```

Note:

The VXLAN destination IP address for IPsec tunnel must be the same as the VXLAN destination IP address for FE tunnel.

6. Configure the IPsec destination IP address for the specific tunnel deployed in decoupled mode:

   ```
   set ipsec <1-255> ipsec-dest-ip {A.B.C.D}
   ```

7. Configure a name for the IPsec tunnel:

   ```
   set ipsec <1-255> tunnel-name WORD <1-64>
   ```

8. Identify if the specific tunnel is a responder or initiator in Network Address Translation (NAT) cases:

   ```
   set ipsec <1-255> responder-only <true | False>
   ```

9. Enable or disable IPsec on a specific tunnel:

   ```
   set ipsec <1-255> <enable | disable>
   ```

Example

Configuring parameters for IPsec tunnel on Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> set ipsec 1 ipsec-dest-ip 192.0.2.5
FIGW> set ipsec 1 mtu 1950
FIGW> set ipsec 1 auth-key abcd
FIGW> set ipsec 1 tunnel-name Tunnel-to-BEB2
FIGW> set ipsec 1 fe-tunnel-dest-ip 192.0.2.15
FIGW> set ipsec 1 encryption-key-length 128
FIGW> set ipsec 1 admin-state enable
```

Variable Definitions

The following table defines parameters for the **`set ipsec`** command.

Variable	Value
<1-255>	Specifies the unique ID for the IPsec tunnel.
admin-state <*enable* | *disable*>	Enables or disables IPsec on the specific IPsec tunnel.
auth-key *WORD <1-32>*	Specifies the pre-shared authentication key. **Note:** You must not use special characters ?, \, &, <, >, #.
encryption-key-length *<128 | 256>*	Specifies the encryption key length for the IPsec tunnel. The default encryption key length is 128.

Table continues…

Variable	Value
fe-tunnel-dest-ip *{A.B.C.D}*	Specifies the destination IP address for Fabric Extend (FE) tunnel.
ipsec-dest-ip *{A.B.C.D}*	Specifies the destination IP address for IPsec tunnel.
mtu *<1300-9000*	Specifies the Maximum Transmission Unit (MTU) value for the FE tunnel with both IPsec and fragmentation and assembly capabilities.
responder-only *<true | false>*	Specifies if the IPsec session in the FE tunnel will be in responder only mode or initiator mode. When in responder mode the FE tunnel will only respond to the incoming request and not initiate the IPsec connection. By default both sides of IPSec connection will be initiators in the FE tunnel. Configure the IPsec tunnel to be in responder only mode when there is Network Address Translation (NAT) between the IPsec connection. For more information about NAT, see Configuring Security for VOSS.
tunnel-name *WORD <1-64>*	Specifies a name for the IPsec tunnel.

Configure Logical Interface Tunnel on Fabric IPsec Gateway VM

About this task

Perform this procedure to configure a Fabric Extend (FE) tunnel with only fragmentation and reassembly capabilities, on the Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Configure the logical interface destination IP address for the specific tunnel:

   ```
   set logical-intf-tunnel <1-255> fe-tunnel-dest-ip {A.B.C.D}
   ```

3. Configure the Maximum Transmission Unit (MTU) value for the specific tunnel:

   ```
   set logical-intf-tunnel <1-255> mtu <750-9000>
   ```

   Note:

   The MTU range <750-9000> is applicable for FE tunnels with only fragmentation and reassembly capabilities.

4. Configure tunnel name:

   ```
   set logical-intf-tunnel <1-255> tunnel-name WORD <1-64>
   ```

Example

Configuring logical interface tunnel on Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> set logical-intf-tunnel 2 fe-tunnel-dest-ip 192.0.2.50
FIGW> set logical-intf-tunnel 2 mtu 1300
FIGW> set logical-intf-tunnel 2 tunnel-name Tunnel-to-BEB2
```

Variable Definitions

The following table defines parameters for the **`set logical-intf-tunnel`** command.

Variable	Value
<1-255>	Specifies the unique ID for the logical interface tunnel.
fe-tunnel-dest-ip *{A.B.C.D}*	Specifies the FE tunnel destination IP address for the logical interface.
mtu *<750-9000>*	Specifies the Maximum Transmission Unit (MTU) value for the FE tunnel with only fragmentation and assembly capabilities.
tunnel-name *WORD <1-64>*	Specifies a name for the the logical interface tunnel.

Save Running Configuration to a File

About this task

Perform this procedure to save the current configuration on Fabric IPsec Gateway Virtual Machine (VM) to a specific file.

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Save configuration to the default configuration file:

   ```
   save config
   ```

3. Save configuration to a specific file in the Fabric IPsec Gateway VM.

   ```
   save config file WORD <1-255>
   ```

Example

Saving configuration of Fabric IPsec Gateway VM to file "test":

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> save config file test
```

Variable Definitions

The following table defines parameters for the **`save config`** command.

Variable	Value
file *WORD <1-255>*	Specifies the name of file to save the configuration of the Fabric IPsec Gateway VM.

Remove Configuration File from Fabric IPsec Gateway VM

About this task

Perform this procedure to remove a specific configuration file from Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   ```

   ```
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Remove the configuration file:

   ```
   remove WORD <1-255>
   ```

Example

Remove configuration file "test" from Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> remove test
```

Variable Definitions

The following table defines parameters for the **remove** command.

Variable	Value
WORD <1-255>	Specifies the configuration file name that the system removes from Fabric IPsec Gateway VM.

Delete Global Configuration on Fabric IPsec Gateway VM

About this task

Perform this procedure to delete the global parameters that you configure on Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Delete configuration of specific global parameters:

   ```
   delete global <fe-tunnel-gw-ip | fe-tunnel-src-ip | ipsec-disable |
   ipsec-tunnel-src-ip | ipsec-tunnel-src-vlan | lan-intf-gw-ip | lan-
   intf-ip | lan-intf-vlan | mtu | virtual-reassembly-intf-ip |
   virtual-reassembly-intf-vlan | wan-intf-gw-ip>
   ```

Example

Deleting the global Maximum Transmission Unit (MTU) configuration on Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> delete global mtu
```

Variable Definitions

The following table defines parameters for the **delete global** command.

Variable	Value
fe-tunnel-gw-ip	Deletes the global gateway IP address for Fabric Extend (FE) tunnel.

Table continues…

Variable	Value
fe-tunnel-src-ip	Deletes the global source IP address for FE tunnel.
ipsec-disable	Deletes the global IPsec configuration.
ipsec-tunnel-src-ip	Deletes the global source IP address and subnet mask for IPsec tunnel.
ipsec-tunnel-src-vlan	Deletes the global source VLAN configuration for IPsec tunnel.
lan-intf-gw-ip	Deletes the global gateway IP address on the Local Area Network (LAN) interface.
lan-intf-ip	Deletes the global IP address and subnet mask on LAN interface.
lan-intf-vlan	Deletes the global VLAN configuration on LAN interface.
mtu	Resets the Maximum Transmission Unit (MTU) value to its default, that is 1950 bytes.
virtual-reassembly-intf-ip	Deletes the global virtual-reassembly interface IP address and subnet mask.
virtual-reassembly-intf-vlan	Deletes the global virtual-reassembly interface VLAN configuration.
wan-intf-gw-ip	Deletes the global gateway IP address on the Wide Area Network (WAN) interface.

Delete IPsec Tunnel Configuration on Fabric IPsec Gateway VM

About this task

Perform this procedure to delete the configuration of specific IPsec tunnel on Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Delete the configuration of specific IPsec tunnel:

   ```
   delete ipsec <1-255> <admin-state enable | auth-key | encryption-
   key-length | fe-tunnel-dest-ip | ipsec-dest-ip | mtu | responder-
   only | tunnel-name>
   ```

Example

Deleting the authentication key and tunnel name configured on IPsec tunnel with ID 2:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y
```

```
  <cr>
FIGW> delete ipsec 2 auth-key
FIGW> delete ipsec 2 tunnel-name
```

Variable Definitions

The following table defines parameters for the **`delete ipsec`** command.

Variable	Value
<1-255>	Specifies the unique ID of the configured IPsec tunnel.
admin-state *enable*	Disables the IPsec status on the specific IPsec tunnel.
auth-key	Deletes the authentication key that you configure on the specific IPsec tunnel.
encryption-key-length	Resets the encryption key length for the specific IPsec tunnel to its default value, that is 128 bit.
fe-tunnel-dest-ip	Deletes the destination IP address that you configure on the Fabric Extend (FE) tunnel.
ipsec-dest-ip	Deletes the destination IP address that you configure on the IPsec tunnel.
mtu	Resets the Maximum Transmission Unit (MTU) value for the specific IPsec tunnel to the MTU value configured globally.
responder-only	Deletes the mode that you configure for the IPsec session in FE tunnel.
tunnel-name	Deletes the name that you configure for the IPsec tunnel.

Delete Logical Interface Tunnel Configuration on Fabric IPsec Gateway VM

About this task

Perform this procedure to delete configuration of a specific logical interface tunnel on Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Delete configuration of specific logical interface tunnel:

   ```
   delete logical-intf-tunnel <1-255> < fe-tunnel-dest-ip | mtu>
   ```

Example

Deleting the destination IP address for Fabric Extend (FE) tunnel configured on the logical interface tunnel with ID 3.

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> delete logical-intf-tunnel 3 fe-tunnel-dest-ip
```

Variable Definitions

The following table defines parameters for the **`delete logical-intf-tunnel`** command.

Variable	Value
<1-255>	Specifies the unique ID of the logical interface tunnel.
fe-tunnel-dest-ip	Deletes the destination IP address that you configure on the logical interface tunnel.
mtu	Resets the Maximum Transmission Unit (MTU) value for the specific logical interface tunnel to the MTU value configured globally.

Display Data in a File on Fabric IPsec Gateway VM

About this task

Perform this procedure to display the data in a specific file on Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Display data in a file:

   ```
   more WORD <1-255>
   ```

Example

Display the data from coupled.cfg file:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y
```

```
  <cr>
FIGW> more coupled.cfg
set global ipsec-tunnel-src-vlan 125
set global ipsec-tunnel-src-ip 192.0.2.10/24
set global lan-intf-vlan 30
set global lan-intf-ip 192.0.2.20/24
set global lan-intf-gw-ip 192.0.2.25
set global fe-tunnel-src-ip 192.0.2.45
set global wan-intf-gw-ip 192.0.2.11
set global mtu 1950
set ipsec 1 auth-key ******
set ipsec 1 fe-tunnel-dest-ip 192.0.2.50
set ipsec 1 encryption-key-length 128
set ipsec 1 admin-state enable
```

Reboot Fabric IPsec Gateway VM

About this task

Perform this procedure to reboot the Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   ```

   ```
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Reboot the VM:

   ```
   reboot
   ```

Example

Rebooting Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> reboot
```

Reset Current Configuration on Fabric IPsec Gateway VM

About this task

Perform this procedure to reset the current configuration on Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Reset current configuration:

   ```
   reset-config
   ```

   Note:

   Reboot the Fabric IPsec Gateway VM after you reset the configuration.

Example

Resetting current configuration on Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> reset-config
```

Traceroute to an IP address on Fabric IPsec Gateway VM

About this task

Perform this procedure to traceroute to an IP address on Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Traceroute to an IP address:

   ```
   traceroute {A.B.C.D}
   ```

Example

Traceroute to IP address.

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> traceroute 192.0.2.100
```

Variable Definitions

The following table defines parameters for the **`traceroute`** command.

Variable	Value
{A.B.C.D}	Specifies the IP address to initiate traceroute to.

Display the Default Configuration File on Fabric IPsec Gateway VM

About this task

Perform this procedure to display the default configuration file on the Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   ```

   ```
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Display default configuration file:

   ```
   show default-config-file
   ```

Example

Displaying default configuration file on Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> show default-config-file
coupled.cfg
```

Display IPsec Logs on Fabric IPsec Gateway

About this task

Perform this procedure to display IPsec session logs on the Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Display IPsec session logs:

   ```
   show ipsec-logs
   ```

Example

Displaying IPsec session logs on Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> show ipsec-logs
<<Month dd>> <<hh:mm:ss>> 15[IKE] <ipsec0-192.0.2.10|29> sending DPD request
<<Month dd>> <<hh:mm:ss>> 15[ENC] <ipsec0-192.0.2.10|29> generating INFORMATIONAL request
11832 [ ]
<<Month dd>> <<hh:mm:ss>> 15[NET] <ipsec0-192.0.2.10|29> sending packet: from
192.0.2.30[500] to 192.0.2.10[500] (76 bytes)
<<Month dd>> <<hh:mm:ss>> 13[NET] <ipsec0-192.0.2.10|29> received packet: from
192.0.2.10[500] to 192.0.2.30[500] (76 bytes)
<<Month dd>> <<hh:mm:ss>> 13[ENC] <ipsec0-192.0.2.10|29> parsed INFORMATIONAL response
11832 [ ]
<<Month dd>> <<hh:mm:ss>> 11[NET] <ipsec0-192.0.2.10|29> received packet: from
192.0.2.10[500] to 192.0.2.30[500] (76 bytes)
<<Month dd>> <<hh:mm:ss>> 11[ENC] <ipsec0-192.0.2.10|29> parsed INFORMATIONAL request
12924 [ ]
<<Month dd>> <<hh:mm:ss>> 11[ENC] <ipsec0-192.0.2.10|29> generating INFORMATIONAL
response 12924 [ ]
<<Month dd>> <<hh:mm:ss>> 11[NET] <ipsec0-192.0.2.10|29> sending packet: from
192.0.2.30[500] to 192.0.2.10[500] (76 bytes)
<<Month dd>> <<hh:mm:ss>> 06[IKE] <ipsec0-192.0.2.10|29> sending DPD request
<<Month dd>> <<hh:mm:ss>> 06[ENC] <ipsec0-192.0.2.10|29> generating INFORMATIONAL request
11833 [ ]
<<Month dd>> <<hh:mm:ss>> 06[NET] <ipsec0-192.0.2.10|29> sending packet: from
192.0.2.30[500] to 192.0.2.10[500] (76 bytes)
--More-- (q = quit)
```

Display IPsec Routes on Fabric IPsec Gateway VM

About this task

Perform this procedure to display the IPsec routes configured on the Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Display IPsec routes installed:

   ```
   show ipsec-routes
   ```

Example

Displaying the IPsec routes configured on Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> show ipsec-routes
192.0.2.30 via 192.0.2.20 dev eth0.125  mtu lock 1950
192.0.2.1/24 dev eth0.30  proto kernel  scope link  src 192.0.2.2
192.0.2.10 via 192.0.2.45 dev eth0.30
192.0.2.100/24 dev eth0.125  proto kernel  scope link  src 192.0.2.60
192.0.2.11/16 dev docker0  proto kernel  scope link  src 192.0.2.12 linkdown
```

Display IPsec Encryption Statistics on Fabric IPsec Gateway VM

About this task

Perform this procedure to display the IPsec encryption statistics on the Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

Note:

Type `CTRL+Y` to exit the console.

2. Display IPsec encryption statistics:

   ```
   show ipsec-stats
   ```

Example

Displaying IPsec encryption statistics on Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> show ipsec-stats
src 192.0.2.30 dst 192.0.2.40
        proto esp spi 0xc0c2d9cd(3233995213) reqid 1(0x00000001) mode tunnel
        replay-window 32 seq 0x00000000 flag af-unspec (0x00100000)
        aead rfc4106(gcm(aes)) 0xa9c1923a4b4c5618ea2f3596de821261218bdea2 (160 bits) 128
        anti-replay context: seq 0x0, oseq 0x138, bitmap 0x00000000
        lifetime config:
          limit: soft (INF)(bytes), hard (INF)(bytes)
          limit: soft (INF)(packets), hard (INF)(packets)
          expire add: soft 3268(sec), hard 3600(sec)
          expire use: soft 0(sec), hard 0(sec)
        lifetime current:
          475650(bytes), 312(packets)
          add <<yyyy-mm-dd>> <<hh:mm:ss>> use <<yyyy-mm-dd>> <<hh:mm:ss>>
        stats:
          replay-window 0 replay 0 failed 0
src 192.0.2.40 dst 192.0.2.30
        proto esp spi 0xc92b08e5(3375040741) reqid 1(0x00000001) mode tunnel
        replay-window 32 seq 0x00000000 flag af-unspec (0x00100000)
        aead rfc4106(gcm(aes)) 0x9ca3568095298cefaaa709b9b932eb5141bd252c (160 bits) 128
        anti-replay context: seq 0x135, oseq 0x0, bitmap 0xffffffff
        lifetime config:
          limit: soft (INF)(bytes), hard (INF)(bytes)
          limit: soft (INF)(packets), hard (INF)(packets)
          expire add: soft 3341(sec), hard 3600(sec)
          expire use: soft 0(sec), hard 0(sec)
        lifetime current:
          470953(bytes), 309(packets)
          add <<yyyy-mm-dd>> <<hh:mm:ss>> use <<yyyy-mm-dd>> <<hh:mm:ss>>
        stats:
          replay-window 0 replay 0 failed 0
```

Display the Status of IPsec Tunnels on Fabric IPsec Gateway VM

About this task

Perform this procedure to display the status of configured IPsec tunnel on the Fabric IPsec Gateway Virtual Machine (VM):

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

```
enable
virtual-service WORD<1-128> console
```

Note:

Type `CTRL+Y` to exit the console.

2. Display the status of IPsec tunnels configured on the VM:

```
show ipsec-status
```

Example

Displaying the status of configured IPsec tunnel on Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> show ipsec-status
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-128-generic, x86_64):
  uptime: 13 days, since <<month, day hh:mm:ss year>>
  malloc: sbrk 2433024, mmap 0, used 369408, free 2063616
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509
revocation constraints
  pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc
hmac gcm attr
  kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.0.2.40
  192.0.2.20
Connections:
ipsec0-192.0.2.5:  192.0.2.40...192.0.2.5  IKEv2, dpddelay=3s
ipsec0-192.0.2.5:   local:  [192.0.2.60] uses pre-shared key authentication
ipsec0-192.0.2.5:   remote: [192.0.2.5] uses pre-shared key authentication
ipsec0-192.0.2.5:   child:  192.0.2.60/32 === 192.0.2.5/32 TUNNEL, dpdaction=restart
Security Associations (1 up, 0 connecting):
ipsec0-192.0.2.5[29]: ESTABLISHED 21 hours ago, 192.0.2.40[192.0.2.60]...
192.0.2.5[192.0.2.5]
ipsec0-192.0.2.5[29]: IKEv2 SPIs: dcf0a2d545d40679_i 55006e07252b9934_r*, pre-shared key
reauthentication in 2 hours
ipsec0-192.0.2.5[29]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
ipsec0-192.0.2.5{377}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c92b08e5_i c0c2d9cd_o
ipsec0-192.0.2.5{377}:  AES_GCM_16_128, 291247 bytes_i (190 pkts, 6s ago), 297523 bytes_o
(194 pkts, 1s ago), rekeying in 30 minutes
ipsec0-192.0.2.5{377}:   192.0.2.60/32 === 192.0.2.5/32
```

Display Current Configuration on Fabric IPsec Gateway VM

About this task

Perform this procedure to display the parameters configured currently on the Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

```
enable
virtual-service WORD<1-128> console
```

Note:

Type `CTRL+Y` to exit the console.

2. Display the parameters currently configured on the VM:

```
show running-config
```

Example

Displaying the parameters configured on Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> show running-config
set global ipsec-tunnel-src-vlan 125
set global ipsec-tunnel-src-ip 192.0.2.1/24
set global lan-intf-vlan 30
set global lan-intf-ip 192.0.2.10/24
set global lan-intf-gw-ip 192.0.2.25
set global fe-tunnel-src-ip 192.0.2.55
set global wan-intf-gw-ip 192.0.2.11
set global mtu 1950
set ipsec 1 auth-key ******
set ipsec 1 fe-tunnel-dest-ip 192.0.2.70
set ipsec 1 encryption-key-length 128
set ipsec 1 admin-state enable
```

Display Current Version of Fabric IPsec Gateway VM

About this task

Display current version of the Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

```
enable
virtual-service WORD<1-128> console
```

Note:

Type `CTRL+Y` to exit the console.

2. Display current version of the VM:

```
show version
```

Example

Displaying current version of the Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> show version
FabricIPSecGW_VM_1.0
```

Log Out of Fabric IPsec Gateway VM

About this task

Perform this procedure to log out of the Fabric IPsec Gateway Virtual Machine (VM).

Procedure

1. Enter Fabric IPsec Gateway Configuration mode:

   ```
   enable
   virtual-service WORD<1-128> console
   ```

   Note:

   Type `CTRL+Y` to exit the console.

2. Log out of VM:

   ```
   exit
   ```

Example

Logging out of the Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

  <cr>
FIGW> exit
```

Chapter 6: IQAgent

Table 16: IQAgent product support

Feature	Product	Release introduced
For configuration details, see Configuring User Interfaces and Operating Systems for VOSS.		
IQAgent	VSP 4450 Series	Not supported
	VSP 4900 Series	VOSS 8.2 VIMs: VIM5-4YE, VIM5-4X, VIM5-4XE, and VIM5-2Y only
	VSP 7200 Series	Not supported
	VSP 7400 Series	VOSS 8.2
	VSP 8200 Series	Not supported
	VSP 8400 Series	Not supported
	VSP 8600 Series	Not supported
	XA1400 Series	VOSS 8.2

For the most current information on switches supported by ExtremeCloud™ IQ, see ExtremeCloud™ IQ Learning What's New.

ExtremeCloud IQ provides cloud-managed networking, and delivers unified, full-stack management of wireless access points, switches, and routers. It enables onboarding, configuration, monitoring, troubleshooting, reporting, and more. Using innovative machine learning and artificial intelligence technologies, ExtremeCloud IQ analyzes and interprets millions of network and user data points, from the network edge to the data center, to power actionable business and IT insights, and to deliver new levels of network automation and intelligence.

VOSS supports a zero touch connection to ExtremeCloud IQ. Zero touch deployment is used to deploy and configure a switch using ExtremeCloud IQ.

VOSS integrates with ExtremeCloud IQ using IQAgent. When you enable IQAgent, you can configure and monitor VOSS devices using ExtremeCloud IQ.

ExtremeCloud IQ supports the following features for VOSS:

- Firmware upgrade
- IQAgent upgrade
- Supplemental CLI

You can configure the following features using the ExtremeCloud IQ interface:

- Hostname configuration
- SNMP location
- Device-level MTU
- Flow control
- Port state, usage type, and settings
- VLAN configuration
- DNS, NTP, SNMP, and Syslog servers

For more information about ExtremeCloud IQ, see https://www.extremenetworks.com/support/documentation/extremecloud-iq/.

IQAgent Configuration Considerations

The following configuration considerations apply to IQAgent:

- SSH and SSH password authenticaton is required. **`boot config flag ssh`** is enabled when IQAgent is enabled. **`boot config flag ssh`** cannot be disabled while IQAqent is enabled.
- SNMP is required. **`boot config flag block-snmp`** is disabled when IQAgent is enabled. **`boot config flag block-snmp`** cannot be enabled while IQAgent is enabled.
- High Secure mode disables IQAgent automatically. IQAgent must be enabled manually when this mode is enabled.
- IQAgent is not supported in Enhanced Secure mode.

Note:

You must configure a Segmented Management Instance to use IQAgent. For more information, see Administering VOSS.

For information about onboarding switches, see https://www.extremenetworks.com/support/documentation/extremecloud-iq/.

Zero Touch Deployment

Zero Touch Deployment enables a VOSS switch to be deployed automatically with ExtremeCloud IQ but you still must onboard the switch on the ExtremeCloud IQ side. When the switch powers on, the DHCP Client obtains the IP address and gateway from the DHCP Server, and discovers the Domain Name Server, connecting the switch automatically to Extreme Management Center or to ExtremeCloud IQ cloud management applications.

With Zero Touch Deployment, IQAgent is enabled by default.

To use zero touch functionality, your switch must be in a Zero Touch Deployment-ready configuration mode, which means the switch cannot have existing primary or secondary configuration files loaded. Factory shipped switches are Zero Touch Deployment ready because they deploy without configuration files. However, existing switches require manual preparation before Zero Touch Deployment can function.

For more information about preparing your switch for Zero Touch Deployment, see Administering VOSS.

DHCP Option 43 Support

With the support of DHCP option 43, DHCP can dynamically configure the IP address of a private/non-public ExtremeCloud IQ server for zero touch deployments when the default ExtremeCloud IQ server (hac.extremecloudiq.com) is not desired.

To use this functionality, DHCP Client must be enabled. For information about DHCP Client for a Segmented Management Instance, see Administering VOSS.

Considerations

The following considerations apply with DHCP option 43:

- A dynamic IP address overwrites the default value (hac.extremecloudiq.com) or 0.0.0.0.
- A static server IP address overwrites a dynamic server IP address.
- A dynamic server IP address does not overwrite an existing static server IP address.

  If a static server IP address is already configured and a new value is received from the DHCP server, the following warning displays on the console: *WARNING Dynamic Cloud IQ Server Address x.x.x.x provided by DHCP option 43 could not be set. Static configured server address y.y.y.y cannot be overwritten by a dynamic address.*
- The default value (hac.extremecloudiq.com) replaces the dynamic server IP address if the DHCP Client is disabled on the switch.
- The dynamic server IP address is not saved in the running-config.

IQAgent Configuration using CLI

After your VOSS device is onboarded (that is, the serial number for the device is associated with your ExtremeCloud IQ account), you are only required to enable IQAgent. Other feature configuration, such as configuring proxy parameters and configuring access to ExtremeCloud IQ is optional.

Note:

You must configure a Segmented Management Instance to use IQAgent. For more information, see Administering VOSS.

For information about onboarding switches, see https://www.extremenetworks.com/support/documentation/extremecloud-iq/.

Configure IQAgent

You must first onboard the VOSS device. When zero touch connection establishes, IQAgent is enabled, by default. Before IQAgent is operational, you must first disable IQAgent, configure the ExtremeCloud IQ IPv4 address or DNS name, and then reneable IQAgent.

Before you begin

You must first onboard the VOSS device.

Procedure

1. Enter Application Configuration mode:

   ```
   enable
   configure terminal
   application
   ```

2. Disable IQAgent:

   ```
   no iqagent enable
   ```

3. Configure the ExtremeCloud IQ IPv4 address or DNS name:

   ```
   iqagent server address WORD<1-255>
   ```

4. Enable IQAgent:

   ```
   iqagent enable
   ```

Example

Configure IQAgent:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#application
Switch:1(config-app)#no iqagent enable
Switch:1(config-app)#iqagent server address hac.extremecloudiq.com
Switch:1(config-app)#iqagent enable
```

Display default IQAgent configuration:

```
Switch:1>show application iqagent

================================================================================
                                IQAgent Info
================================================================================
Agent Admin State       : true
```

```
Agent Version           : 0.2.7
Agent Oper State        : disconnected
Server Address          : hac.extremecloudiq.com
Server Address Origin   : None
Proxy Address           : 0.0.0.0
Proxy TCP Port          : 0
Proxy Username          :
```

Configure Access to ExtremeCloud IQ

Use this task to configure IQAgent parameters to access ExtremeCloud IQ.

Before you begin

You must onboard the VOSS device and configure any optional IQAgent parameters on the supported VOSS device before you enable IQAgent.

You can configure the IQAgent parameters on the supported VOSS devices first, and then onboard the devices (that is, add the serial numbers for the devices in the ExtremeCloud IQ GUI) or vice versa.

For information about onboarding switches, see https://www.extremenetworks.com/support.

Procedure

1. Enter Application Configuration mode:

   ```
   enable

   configure terminal

   application
   ```

2. Configure the ExtremeCloud IQ IPv4 address or DNS name:

   ```
   iqagent server address WORD<1-255>
   ```

Example

Configure access to ExtremeCloud IQ using an IPv4 address:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#application
Switch:1(config-app)#iqagent server address 192.0.2.1
```

Configure access to ExtremeCloud IQ using a DNS name:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#application
Switch:1(config-app)#iqagent server address extremecloudiq.com
```

Variable Definitions

The following table defines parameters for the **`iqagent server`** command.

Variable	Value
address <*WORD 1-255*>	Specifies the ExtremeCloud IQ IPv4 address or DNS name.

Configure Proxy Parameters

If you use a proxy https server in your network, you must configure proxy parameters so that the IQAgent on the device can communicate with ExtremeCloud IQ through the proxy.

Use this task to configure the proxy parameters for ExtremeCloud IQ on the IQAgent.

Note:

You must onboard the VOSS device and configure any optional IQAgent parameters on the supported VOSS device before you enable IQAgent.

You can configure the IQAgent parameters on the supported VOSS devices first, and then onboard the devices (that is, add the serial numbers for the devices in the ExtremeCloud IQ GUI) or vice versa.

For information about onboarding switches, see https://www.extremenetworks.com/support.

Procedure

1. Enter Application Configuration mode:

   ```
   enable

   configure terminal

   application
   ```

2. Configure the proxy IPv4 address or DNS name:

   ```
   iqagent proxy address <WORD 1-255> tcp-port <1-49151>
   ```

3. Configure the proxy username and password for the ExtremeCloud IQ account:

   ```
   iqagent proxy username <WORD 1-64> password <WORD 1-128>
   ```

Example

Configure proxy parameters using an IPv4 address:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#application
Switch:1(config-app)#iqagent proxy address 192.0.2.254 tcp-port 21
Switch:1(config-app)#iqagent proxy username admin password ****
```

Configure proxy parameters using a DNS name:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#application
Switch:1(config-app)#iqagent proxy address hac.extremecouldiq.com tcp-port 21
Switch:1(config-app)#iqagent proxy username admin password ****
```

Variable Definitions

The following table defines parameters for the **`iqagent proxy`** command.

Variable	Value
address <*WORD 1-255*>	Specifies the proxy IPv4 address or DNS name.
tcp-port <*1-49151*>	Specifies the TCP port.
username <*WORD 1-64*>	Specifies the proxy server username.
password <*WORD 1-128*>	Specifies the proxy server password.

Display IQAgent Information

About this task

Use this task to display IQAgent configuration information and status.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display IAQgent configuration information and status:

   ```
   show application iqagent
   ```

Example

Display IQAgent configuration information and status when IQAgent is enabled using the default ExtremeCloud IQ server:

```
Switch:1>show application iqagent

================================================================================
                                IQAgent Info
================================================================================
Agent Admin State       : true
Agent Version           : 0.2.7
Agent Oper State        : connected
Server Address          : hac.extremecloudiq.com
Server Address Origin   : None
Proxy Address           : extremeiq.com
Proxy TCP Port          : 21
Proxy Username          : admin
```

Display IQAgent disabled state:

```
Switch:1>show application iqagent

================================================================================
                                IQAgent Info
================================================================================
Agent Admin State       : false
Agent Version           : 0.2.7
Agent Oper State        : disconnected
Server Address          : 0.0.0.0
Server Address Origin   : None
Proxy Address           : 0.0.0.0
Proxy TCP Port          : 0
Proxy Username          :
```

Display IQAgent configuration information and status when DHCP provides a dynamic server IP address:

```
Switch:1>show application iqagent

================================================================================
                                IQAgent Info
================================================================================
Agent Admin State       : true
Agent Version           : 0.2.7
Agent Oper State        : disconnected
Server Address          : 192.0.2.1
Server Address Origin   : DHCP
Proxy Address           : 0.0.0.0
Proxy TCP Port          : 0
Proxy Username          :
```

Display IQAgent configuration information and status when DHCP Client is disabled on the switch:

```
Switch:1>show application iqagent

================================================================================
                                IQAgent Info
================================================================================
Agent Admin State       : false
Agent Version           : 0.2.7
Agent Oper State        : disconnected
Server Address          : hac.extremecloudiq.com
Server Address Origin   : None
Proxy Address           : 0.0.0.0
Proxy TCP Port          : 0
Proxy Username          :
```

Job Aid

The following sections describe the fields in the output for the **`show application iqagent`** command.

Table 17:

Output	Description
Agent Admin State	Specifies the administrative state of the IQAgent.
Agent Version	Specifies the IQAgent version that runs on the device.
Agent Oper State	Specifies the operational status of the IQAgent, whether IQAgent is connected to ExtremeCloud IQ.
Server Address	Specifies the default ExtremeCloud IQ server.
Server Address Origin	Specifies the origin of the server IP address. • None - displays the default value (hac.extremecloudiq.com) or 0.0.0.0 • Configured - displays the static server IP address configured using CLI or EDM. • DHCP - displays the dynamic server IP address configured by the DHCP server.

Table continues…

Output	Description
Proxy Address	Specifies the proxy address.
Proxy TCP Port	Specifies the proxy TCP port.
Proxy Username	Specifies the proxy server username.
Proxy Password	Specifies the proxy server password.

Display IQAgent Status

About this task

Use this task to display IQAgent status information.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display IQAgent status information:

   ```
   show application iqagent status
   ```

Example

```
Switch:1>show application iqagent status
================================================================================
                                IQAgent Status
================================================================================
Connection Status               : Connected
Last Onboard Time               : 18:54:23 11 27 2019 UTC
Agent Version                   : 0.2.7
Association URL                 : https://10.16.231.98/hac-webapp/rest/v1/association
Poll URL                        : https://10.16.231.98/hac-webapp/rest/v1/poll/1904Q-20028
Monitor Frequency               : 600
Poll Frequency                  : 30
Last Poll Status                : SUCCESS
Last Poll Success Time          : 14:39:16 11 28 2019 UTC
Last Health Status              : SUCCESS
Last Health Success Time        : 14:38:35 11 28 2019 UTC
Last Monitor Status             : SUCCESS
Last Monitor Success Time       : 14:38:35 11 28 2019 UTC
```

IQAgent Configuration using EDM

Perform the procedures in this section to configure ExtremeCloud IQ Agent on the switch using the Enterprise Device Manager (EDM).

Configure ExtremeCloud IQ Agent

Before you begin

You must first onboard the VOSS device and configure any optional IQAgent parameters before you enable IQAgent.

About this task

Procedure

1. In the navigation pane, expand **Configuration** > **Serviceability.**
2. Select **IQAgent**.
3. Select the **Globals** tab.
4. Select the **GlobalEnable** check box to enable the server.
5. Configure optional parameters as required.
6. Select **Apply**.

CloudIQ Field Descriptions

Use the data in the following table to use the CloudIQ tab and to configure the CloudIQ Agent.

Name	Description
Address	Specifies the proxy IPv4 address or DNS name.
Enable	Specifies whether IQAgent is enabled. The default is enabled.
Server/Address	Specifies the ExtremeCloud IQ DNS name. The default is hac.extremcloudiq.com.
Password	Specifies the proxy server username.
TcpPort	Specifies the TCP port.
UserName	Specifies the proxy server password.

Chapter 7: Representational State Transfer Configuration Protocol (RESTCONF)

Table 18: Representational State Transfer Configuration Protocol (RESTCONF) product support

Feature	Product	Release introduced
For configuration details, see Configuring User Interfaces and Operating Systems for VOSS.		
Representational State Transfer Configuration Protocol (RESTCONF)	VSP 4450 Series	VOSS 8.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 8.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 8.0
	VSP 8400 Series	VOSS 8.0
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported

Note:

Product Notice: Using RESTCONF on VSP4900-48P or VSP4900-24S reduces the number of supported port-based VLANs on those platforms. For known issues, see Release Notes for VOSS.

Representational State Transfer Configuration Protocol (RESTCONF) Fundamentals

Representational State Transfer Configuration Protocol (RESTCONF) is a next generation northbound interface that provides an additional way to configure and monitor the switch. RESTCONF is an HTTP-based protocol that provides a programmatic interface to access data defined in a YANG model using the datastore concepts defined in NETCONF. RESTCONF uses a client-server model. The server acts as an entry point to a datastore, a conceptual place to store

and access information. Clients use HTTP or HTTPS to interface with the server to configure and monitor devices.

RESTCONF Client and Server

A typical RESTCONF interaction consists of an HTTP/HTTPS request sent by a RESTCONF client and an HTTP/HTTPS response sent by the server. The HTTP/HTTPS request and response contain a required set of expected HTTP headers and may contain a request or response message body. The message body is encoded in JSON.

An HTTP request consists of the HTTP method (such as GET or POST) identifier, resource identifier, HTTP protocol version, HTTP headers, and HTTP body. The HTTP resource identifier is the string that identifies a service or resource that the server makes available to the client. The RESTCONF request contains the Universal Resource Identifier or URI which starts with /rest/restconf/data/ or /rest/restconf/operations/.

YANG Model

YANG is the data modeling language used for modeling configuration and state data for manipulation by using remote procedure calls (RPCs). The RESTCONF interface is generated with YANG Data Model. The YANG model is based on Open config model, which is a non vendor specific model that captures the key components found in multiple vendor solutions.RESTCONF is described by the Internet Engineering Task Force (IETF) in RFC 8040.

RESTCONF Authentication

RESTCONF uses the CLI user account and supports both local and remote authentication. Local authentication uses the local CLI user account while remote authentication can use either a RADIUS or TACACS+ server.

You can only use a CLI account with the RWA access level.

With RADIUS or TACACS+ enabled, if the remote server is not available, authentication falls back to local authentication and uses the local CLI user on the switch.

When the RESTCONF client posts for authentication, the HTTP server validates the login username and password if you have not enabled CLI remote authentication. If the remote server is not reachable, the HTTP server uses the local user for login validation.

For HTTPs access to the RESTCONF server, you must enable TLS and install a certificate.

RESTCONF APIs

You can access the RESTCONF API documentation on your switch using the following URL:

http(s)://<IP>:<tcp-port>/apps/restconfdoc/

Replace <IP> with the management IP address of your switch and <tcp-port> with the TCP port configured for RESTCONF. For example, http://192.0.2.16:8080/apps/restconfdoc/.

The on-switch URL works only if the RESTCONF feature is enabled on the switch.

You can also access the RESTCONF API documentation online at www.extremenetworks.com/support/documentation-api/.

VOSS Support

VOSS RESTCONF server supports the following actions:

HTTP Action	VOSS Instrumentation
GET	Corresponds to SHOW
POST	Corresponds to SET for creation
PATCH	Corresponds to SET for modification
DELETE	Maps to SET for deletion

VOSS RESTCONF supports the following features:

- System (authorization, authentication, and accounting)
- Link Layer Discovery Protocol (LLDP)
- Interfaces (IPv4, Ethernet, and LAG)
- VLAN (under network instance)
- Virtual Service (Extreme YANG model)

The RESTCONF feature is disabled by default. The RESTCONF server uses the same management IP address as the other applications and TCP port. The default TCP port that RESTCONF server listens to is port 8080. The TCP port delivers the message to the HTTP server for RESTCONF.

RESTCONF configuration using CLI

Enable the RESTCONF Server

About this task

Use the following procedure to enable the RESTCONF server.

Before you begin

Run the **`show application restconf conflict-ifname`** command to see if any conflict in interface names exist. To enable RESTCONF, the interface names (VLAN name, MLT name, and Port interface name) must be unique.

Run the **`show application restconf invalid-name mlt`** and **`show application restconf invalid-name vlan`** commands to see if any MLT or VLAN names contain special characters. To enable RESTCONF, VLAN and MLT names cannot contain special characters other than underscore (_) and en dash (-).

Procedure

1. Enter Application Configuration mode:

   ```
   enable
   configure terminal
   application
   ```

2. Enable the RESTCONF server:

   ```
   restconf enable
   ```

   Note:

   If the interface names (VLAN, MLT, and Port) are not unique, or if VLAN or MLT names contain prohibited special characters, an error occurs indicating that you cannot enable RESTCONF. You must change the interface names before you enable RESTCONF.

Example

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line. End with CTRL/Z.
Switch:1(config)#application
Switch:1(config-app)#restconf enable
```

Configuring HTTPS Access to the RESTCONF Server

About this task

By default, the RESTCONF server uses HTTP. If you need to use HTTPS, generate a certificate file and transfer the certificate file to the `/intflash` directory on the switch.

For more information on generating certificate files, see *SSL certificate* in Administering VOSS.

Before you begin

Ensure that you have the certificate file in the `/intflash` directory on the switch.

Procedure

1. Enter Application Configuration mode:

   ```
   enable
   configure terminal
   application
   ```

2. If RESTCONF is enabled, disable RESTCONF:

   ```
   no restconf enable
   ```

3. Install the certificate file for the RESTCONF server:

   ```
   restconf install-cert-file WORD<1-128>
   ```

4. Enable HTTPS:

   ```
   restconf tls
   ```

5. Enable RESTCONF:

   ```
   restconf enable
   ```

Example

```
Switch:1>enable
Switch:1# configure terminal
Enter configuration commands, one per line. End with CTRL/Z.
Switch:1(config)#application
Switch:1(config-app)#no restconf enable
Switch:1(config-app)#restconf install-cert-file /intflash/.cert/restconf-cert.pem
Switch:1(config-app)#restconf tls
Switch:1(config-app)#restconf enable
```

Variable Definitions

Use the data in the following table to use the **restconf** command.

Variable	Value
enable	Enables the RESTCONF Server.
install-cert-file WORD<1-128>	Installs the certificate file for the RESTCONF server.
tcp-port <1-49151>	Set RESTCONF Server TCP port number.
tls	Enables TLS for the RESTCONF server. The default is disabled.
trap-notification	Enables trap notification.

Modifying the RESTCONF Server Settings

About this task

Use this procedure to modify the RESTCONF server settings.

Note:

These steps are considered optional and RESTCONF can operate with the default configuration of these values.

Procedure

1. Enter Application Configuration mode:

   ```
   enable
   configure terminal
   application
   ```

2. Disable trap notification when the RESTCONF server is not available:

   ```
   no restconf trap-notification
   ```

3. Modify the TCP port number for the RESTCONF server:
   a. Disable RESTCONF: `no restconf enable`
   b. Change the value of the TCP port: `restconf tcp-port <1-49151>`
   c. Enable RESTCONF: `restconf enable`

4. Disable TLS for the RESTCONF server:
   a. Disable RESTCONF: `no restconf enable`
   b. Disable TLS: `no restconf tls`
   c. Enable RESTCONF: `restconf enable`

Variable Definitions

Use the data in the following table to modify the RESTCONF server settings.

Variable	Value
enable	Enables or disables the RESTCONF server. The default is disabled.
tcp-port <1-49151>	Specifies the TCP port to use for the RESTCONF server. The default is 8080.
trap-notification	Enables or disables trap notification when the RESTCONF server is not available. The default is enabled.

Showing the RESTCONF Configuration Information

About this task

Use this procedure to show the RESTCONF configuration information and operation status.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Show the RESTCONF configuration:

   ```
   show application restconf
   ```

Example

```
Switch:1>show application restconf
================================================================================
                                    RESTCONF Info
================================================================================
Admin State             : true
TCP Port                : 8080
Certificate File Status : install
TLS Enable              : false
Trap Notification       : true
Oper State              : up
Web Server Version      : 1.0.1.11
RESTCONF Server Version : 1.0.1.39
================================================================================
```

Showing Conflicting Interface Name Information

About this task

To enable RESTCONF, the interface name (VLAN name, MLT name, and Port interface name) must be unique. Use this procedure to display conflicting interface name information.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Show the RESTCONF conflicting interface name information:

   ```
   show application restconf conflict-ifname
   ```

Example

```
Switch:1>show application restconf conflict-ifname
-------------------------------------------------------------------------------------------
 Conflicting Interface IfName - Port, VLAN Name and MLT Name
-------------------------------------------------------------------------------------------
 Mlt 1 name is same as Vlan 1001 name - "Interface-1"
 Mlt 2 name is same as Vlan 1002 name - "VLAN-1002"
 Vlan 1003 name is Mlt 1 Default Name - "MLT-1"
-------------------------------------------------------------------------------------------
Total Conflict Count: 3
```

Next steps

If a conflict exists, change the conflicting interface name to a unique name.

Show Special Characters in VLAN or MLT Names

About this task

To enable RESTCONF, VLAN and MLT names cannot contain special characters other than underscore (_) and en dash (-). Use this procedure to display VLAN or MLT names that contain prohibited special characters.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Show the RESTCONF VLAN or MLT names that contain prohibited special characters:

   ```
   show application restconf invalid-name vlan
   ```

   ```
   show application restconf invalid-name mlt
   ```

Example

```
Switch:1>show application restconf invalid-name mlt
-------------------------------------------------------------------------------------------
 Invalid MLT names - Only "-" and "_" special characters are allowed
-------------------------------------------------------------------------------------------
 Mlt 3 name has special characters - "gigi#g"
 Mlt 4 name has special characters - "my%mlt"
 Mlt 5 name has special characters - "isa.text"
```

```
--------------------------------------------------------------------------------
Total Invalid Names Count: 3
```

Next steps

If any of the names contain prohibited special characters, change the names to remove the special characters.

RESTCONF Configuration using EDM

This section contains procedures for configuring RESTCONF with Enterprise Device Manager (EDM).

Configuring the RESTCONF Server

About this task

To configure the server, you must enable RESTCONF. RESTCONF is disabled by default.

After RESTCONF is enabled, you must disable RESTCONF to modify some of the RESTCONF parameters.

Procedure

1. In the navigation pane, expand **Configuration** > **Serviceability.**
2. Click **RESTCONF**.
3. Click the **RESTCONF** tab.
4. Select the **GlobalEnable** check box to enable the RESTCONFserver.
5. Configure optional parameters as required.
6. Click **Apply**.

RESTCONF Field Descriptions

Use the data in the following table to use the RESTCONF tab.

Name	Description
GlobalEnable	Enables or disables the RESTCONF server. The default is disabled (cleared).
TcpPort	Specifies the TCP port to use for the RESTCONF server. The default is 8080. The RESTCONF status must be disabled before you can modify this field.
TlsEnable	Enables or disables TLS/SSL if you require HTTPS access to the RESTCONF server. The default is

Table continues…

Name	Description
	disabled. The RESTCONF status must be disabled before you can modify this field.
CertificateFilename	If HTTPS access is required, specifies the file name and path of the TLS/SSL certificate. The certificate file must be in the `/intflash` directory on the switch.
CertificateAction	Installs or uninstalls the TLS/SSL certificate file. It also shows the current status of the certificate installation.
NotificationEnable	Enables or disables trap notification when the RESTCONF server is not available. The default is enabled.
OperStatus	Shows the operational status of the RESTCONF server.
WebServerVersion	Shows the RESTCONF web server version that is running on the server.
RestConfServerVersion	Shows the RESTCONF server version that is running on the server.

Use Representational State Transfer Configuration Protocol (RESTCONF) to Configure a Switch

The documentation does not include information about how to use RESTCONF clients. This example documents some common tasks using Python.

Before you begin

Configure the RESTCONF server on the switch.

Procedure

1. Import classes, define variables, and prepare the session object:

```
#!/usr/bin/env python
import sys
import json
import requests
from requests import Request, Session
from requests.auth import HTTPBasicAuth
from requests.packages.urllib3.exceptions import InsecureRequestWarning
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
#####################################################################
Host     = '192.0.2.1'
TcpPort  = '8080'
UserName = 'rwa'
PassWord = 'rwa'
LoginUrl = 'https://%s:%s/auth/token' % (Host, TcpPort)QueryUrl = 'https://%s:%s/
rest/restconf/data/' % (Host, TcpPort)
```

```
vlan     = 123
##############################################################################
session         = Session()
session.verify  = False
session.timeout = 5

session.headers.update({    'Accept':       'application/json',
                            'Accept-Encoding': 'gzip, deflate, br',
                            'Connection':      'keep-alive',
                            'Cache-Control':   'no-cache',
                            'Pragma':       'no-cache', })
```

2. Learn the authentication token:

Note:

The token expires after 24 hours.

```
body = '{"username": "%s", "password" : "%s" }' % (UserName,PassWord)


response = session.put( LoginUrl, body )

if response.status_code != 200:
    print "ERROR: Login failed"
    sys.exit(1)
else:    session.headers.update({
            'X-Auth-Token': response.headers['X-Auth-Token']
    })
    print "INFO: login passed"
```

3. Query all VLANs:

```
response = session.get( QueryUrl + 'openconfig-vlan:vlans' )
if response.status_code != 200:
    print 'ERROR: can't fetch VLANs'
```

4. Query specific VLANs:

```
response = session.get( QueryUrl + 'openconfig-vlan:vlans/vlan=%s' % vlan )

if response.status_code != 200:
    print 'INFO: VLAN %s doesn't exists' % vlan
else:
    print 'INFO: VLAN %s exists' % vlan
```

5. Access data:

```
inbound_data = json.loads( response.text )

for vlan in inbound_data['openconfig-vlan:vlans' ]['vlan']:
     print 'VLAN: %s [%s]' % ( vlan['state']['name'], vlan['vlan-id'] )
```

6. Present data:

```
inbound_data = json.loads( response.text )

for dataVlan in inbound_data[ dataObject ]['vlan']:
    print ''
    print 'VLAN: ' + dataVlan['state']['name'] + '[' + dataVlan['vlan-id'] + ']'
    interfaces = ' '
    if 'members' in dataVlan :
        for interface in dataVlan['members']['member ']:
            interfaces = interfaces + interface['interface-ref']['state']
['interface'] + ','
```

```
        print interfaces
```

7. Add a VLAN:

```
dataObject = 'openconfig-vlan:vlans’

data = { "openconfig-vlan:vlan": [
                                    { "config":
                                { "name":    "Test-VLAN",
                                  "extreme-mod-oc-vlan:stg-id": 1,
                                  "vlan-id": vlan
                                }
                               }
                                    ]
       }

response = session.post( QueryUrl + dataObject, json=data )

if response.status_code != 201:
    print "ERROR: add VLAN %s failed" % vlan
else:
    print "INFO: VLAN %s added " % vlan
```

8. Update a VLAN:

```
dataObject = 'openconfig-vlan:vlans/vlan=%s/config' % vlan

data = { "openconfig-vlan:config":
               { "name":    "New-VLAN-Name" }
        }

response = session.patch( QueryUrl + dataObject )

if response.status_code != 204:
    print "ERROR: update VLAN %s fails" % vlan
else:
    print "INFO: VLAN %s updated" % vlan
```

9. Delete a VLAN:

```
dataObject = 'openconfig-vlan:vlans/vlan=%s' % vlan

response = session.delete( QueryUrl + dataObject )

if response.status_code != 204:
    print "ERROR: delete VLAN %s fails" % vlan
else:
    print "INFO: VLAN %s deleted" % vlan
```

Chapter 8: Zero Touch Provisioning Plus

Table 19: Zero Touch Provisioning Plus product support

Feature	Product	Release introduced
For configuration details, see Configuring User Interfaces and Operating Systems for VOSS.		
Zero Touch Provisioning Plus	VSP 4450 Series	VOSS 8.2
	VSP 4900 Series	VOSS 8.2
	VSP 7200 Series	VOSS 8.2
	VSP 7400 Series	VOSS 8.2
	VSP 8200 Series	VOSS 8.2
	VSP 8400 Series	VOSS 8.2
	VSP 8600 Series	Not Supported
	XA1400 Series	VOSS 8.2

Note:

Demonstration features are provided for testing purposes. Demonstration features are for lab use only, and are not for use in a production environment.

With zero touch functionality, VOSS switches are automatically discovered on the network the moment they are connected.

Zero Touch Provisioning Plus (ZTP+) enables you to deploy and configure VOSS switches in Extreme Management Center with minimal server configuration and intervention. ZTP+ enabled switches send information, such as the serial number, software version, MAC, management IP, and port information to Extreme Management Center automatically.

When the switch powers on, the DHCP Client obtains the IP address and gateway from the DHCP server, discovers the Domain Name Server, and connects the switch to Extreme Management Center.

ZTP+ uses HTTPS for communication between the switch and the Extreme Management Center server. The switch discovers the Extreme Management Center server by resolving the DNS name *extremecontrol.<domain-name>*.

Important:
This feature requires a Zero Touch Deployment-ready configuration. For more information, see Administering VOSS.

ZTP+ Phases of Operation

ZTP+ auto-provisioning occurs in phases after you connect the switch to the network, if the switch is in factory ship state with no valid configuration saved on the device.

Connect

The Connect phase is the first phase of ZTP+ during which the switch connects to the Extreme Management Center server on the network. The Extreme Management Center server is discovered by resolving the DNS name *extremecontrol.<domain-name>*.

If the attempt is successful, the Extreme Management Center server responds with an **Accept** message. When connectivity is established, the switch communicates with the Extreme Management Center server securely and transmits information, such as its serial number, model number. The switch then progresses to the next phase of ZTP+.

Upgrade

After a successful connect to the Extreme Management Center server, the next phase of ZTP+ is the Upgrade phase. This phase verifies that the switch is running the image file version that is currently selected as the reference version on the Extreme Management Center server.

Image file validation is initiated by the switch. After a successful connect, the switch sends an image file upgrade request to the Extreme Management Center server with details on the current image file version. If the image file versions on the switch and the Extreme Management Center server match, no upgrade is initiated, and the switch moves to the next phase of ZTP+. If the Extreme Management Center server detects a different image file version, ZTP+ initiates the .tgz image file download from a specified URL location.

After a successful image upgrade, the switch reboots and reconnects to the Extreme Management Center server. If there are errors in the image upgrade process, an event is added to the server log. The switch then retries the image upgrade.

Configuration

The next phase after the image upgrade is ZTP+ Configuration phase. During this phase, the switch queries the Extreme Management Center server for configuration updates, and initiates auto-provisioning by transmitting information, such as the image version, model name, and serial number. The switch then attempts to apply the configuration that is pushed from the Extreme Management Center server.

If the switch can still communicate with the Extreme Management Center server after the configuration is applied, the new configuration is automatically saved on the switch. The switch can be managed through the Extreme Management Center using SNMP. However, if the configuration that is pushed from the Extreme Management Center server breaks switch connectivity to the Extreme Management Center server, the switch reboots without saving the configuration. After the switch reboots, the ZTP+ onboarding restarts.

Note:

Any configurations pushed from the Extreme Management Center server to VOSS devices using the initial ZTP+ configuration push are not displayed in the **`show log file detail`** command output. The logs associated with the Cloud connector are logged internally to state_machine.txt and ztp_plus.txt files located in `/intflash/cc/cc_logs/`.

ZTP+ Considerations

The following considerations apply to ZTP+:

- Only SNMP, Login, VLANs, and Ports configuration are supported for Extreme Management Center registration.
- Only LLDP neighbor discovery is supported. Based on the LLDP discovery, port templates can be used on the Extreme Management Center server. Enabling or disabling LLDP is not supported.
- Fabric configurations are not supported with ZTP+. After ZTP+ is configured, Extreme Management Center server can use Simple Network Management Protocol (SNMP) to remotely configure Fabric-related configurations on the switch using SNMP MIBs.
- Only the OOB port or the Management VLAN interface are used to connect the Extreme Management Center server.

Configuring ZTP+ using the CLI

This section provides procedures to configure and manage ZTP+ using the Command Line Interface (CLI).

After your VOSS device is onboarded, you have access to Extreme Management Center.

Note:

You must configure a Segmented Management Instance to use ZTP+. For more information, see Administering VOSS.

For information about onboarding switches, see https://www.extremenetworks.com/support.

View ZTP+ Status

About this task

Use this procedure to verify the status of ZTP+ on the switch.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Verify that ZTP+ is enabled:

   ```
   show application auto-provision
   ```

Example

The following is an example output of the **`show application auto-provision`** command:

```
Switch:1>show application auto-provision
```

```
Admin state          : Enabled
Operational state    : Running
```

Glossary

command line interface (CLI)	A textual user interface. When you use CLI, you respond to a prompt by typing a command. After you enter the command, you receive a system response.
Configuration and Orchestration Manager (COM)	A management system in the network, which manages multiple network devices by offering Web-based user-interfaces to the user. You must purchase and install COM separately from the individual product.
Enterprise Device Manager (EDM)	A web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.
graphical user interface (GUI)	A graphical (rather than textual) computer interface.
Trivial File Transfer Protocol (TFTP)	A protocol that governs transferring files between nodes without protection against packet loss.