



ExtremeCloud OS ONE SD-WAN v30.26.2.0 Command Reference Guide

Command Syntax and Usage

9041213-00 Rev AA
August 2026



Copyright © 2026 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: <https://www.extremenetworks.com/about-extreme-networks/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/>

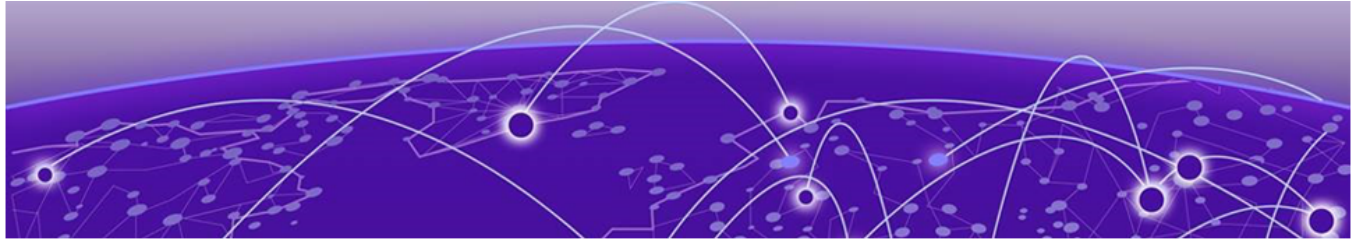
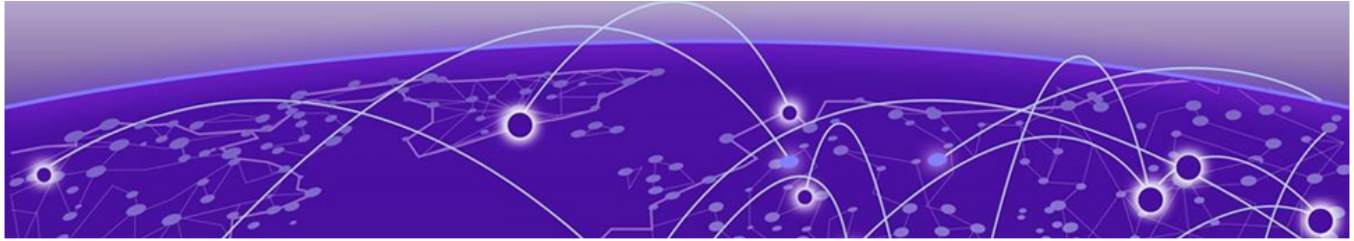


Table of Contents

Abstract.....	vi
Preface.....	7
Text Conventions.....	7
Documentation and Training.....	9
Open Source Declarations.....	9
Training.....	9
Help and Support.....	9
Subscribe to Product Announcements.....	10
Send Feedback.....	10
SD-WAN CLI Overview.....	11
SD-WAN Related Extreme ONE OS Switching Commands.....	12
What's New in This Document.....	17
Supported Platforms.....	17
Using the CLI.....	18
User Accounts.....	18
Accessing the CLI.....	19
Command Modes.....	19
EXEC Mode.....	19
Global Configuration Mode.....	19
Displaying CLI Commands and Command Syntax.....	20
Completing CLI Commands.....	21
CLI Keyboard Shortcuts.....	22
Using CLI Command Output Modifiers.....	22
Unsupported Input Characters.....	23
Debug and System Diagnostic Commands.....	23
Firmware Management Commands.....	24
View Firmware Version Information.....	24
Firmware Upgrade Commands.....	24
Firmware Activation and Rollback Behavior.....	25
AVC Commands.....	26
application.....	27
application-group.....	30
application-performance policy.....	33
capability.....	36
cellular wan-interface	38
dws-method.....	40
security-rule-policy.....	42
sla-profile.....	45
wan-interface.....	49

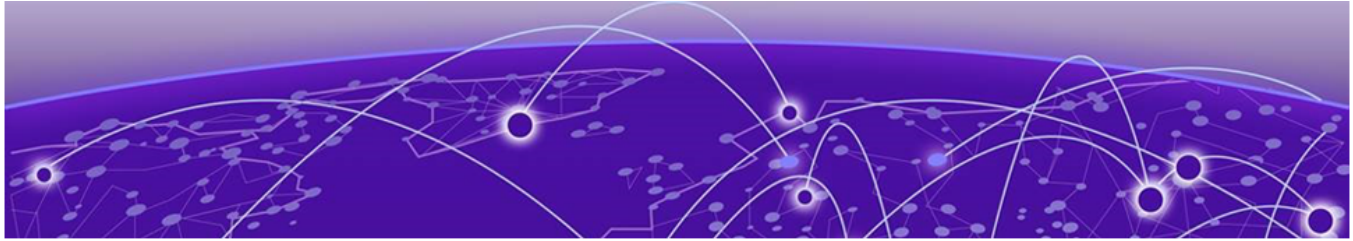
wan-service.....	52
appliance	55
appliance wan-id	57
data-record	59
DTI commands.....	61
dti.....	62
interface.....	63
tracker.....	64
target-ip.....	65
Fabric Extend Commands.....	66
fabric-extend.....	66
Syntax.....	66
Command Default.....	66
Parameters.....	66
Modes.....	66
Example.....	67
show lldp interface.....	68
IPsec Commands.....	70
ipsec.....	71
ipsec-profile.....	73
peer.....	75
sa-policy.....	76
security-policy	78
traffic-selector.....	80
show ipsec peer.....	82
IPsec Tunnel Commands.....	84
show counters ike.....	85
show ipsec tunnel.....	86
type ipsec.....	87
NAT Commands.....	88
nat.....	88
Syntax.....	88
Command Default.....	88
Parameters.....	88
Modes.....	88
Example.....	88
TCP MSS Clamping Commands.....	90
TCP MSS Clamping.....	90
Syntax.....	90
Command Default.....	90
Parameters.....	90
Modes.....	90
Examples.....	90
ZTP Commands.....	92
ZTP.....	92
Syntax.....	92

Command Default.....	92
Parameters.....	92
Examples.....	92
Config Backup Commands.....	93
day1-configuration start	94
day1-configuration stop	95
rm day1-config	96
show day1-config	97
day1-config save.....	99
Config Rollback Commands.....	100
config rollback.....	100
Syntax.....	100
Command Default.....	100
Parameters.....	100
Modes.....	100
Usage Guidelines.....	101
Examples.....	101
Interface Cellular Commands.....	102
interface cellular.....	102
Syntax.....	102
Command Default.....	102
Parameters.....	102
Modes.....	103
Usage Guidelines.....	103
Examples.....	103
show interface cellular	104
show sysinfo modem health.....	107
show sysinfo modem status.....	109



Abstract

This CLI Reference Guide for ExtremeCloud OS ONE SD-WAN version 30.26.2.0 provides comprehensive command syntax and usage documentation for system administrators and advanced network operators. The guide covers SD-WAN-specific configuration and management commands deployed across supported hardware platforms, emphasizing command-line interface operations within the ExtremeCloud ecosystem. Key technical areas include Application Visibility and Control (AVC) commands for managing traffic policies, WAN interfaces, and service definitions; Digital Threat Intelligence (DTI) tracking; Fabric Extend deployment options; IPsec configuration for tunnel establishment, peer management, and security policies; Network Address Translation (NAT) and TCP MSS clamping parameters; and Zero Touch Provisioning (ZTP) for automated device onboarding. The document details firmware management procedures, configuration backup and rollback capabilities, and cellular interface commands for modem health monitoring and status reporting. Command syntax conventions, operational modes (EXEC and Global Configuration), and keyboard shortcuts facilitate user navigation, while keyboard output modifiers enable filtered information retrieval. Critical guidance emphasizes that ExtremeCloud OS ONE SD-WAN is designed for centralized Orchestrator management, with direct CLI configuration reserved for advanced users to prevent system inconsistencies. Supported platforms and interoperability with Extreme OS ONE Switching commands are documented for reference integration.



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches, the product is referred to as *the switch*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
Key names	Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
<i>Words in italicized type</i>	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.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic</i> text	Italic text indicates variable content.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

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 articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the [Open Source Declaration](#) page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the [Extreme Networks Training](#) page.

Help and Support

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 2800. 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 Product Announcements

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

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

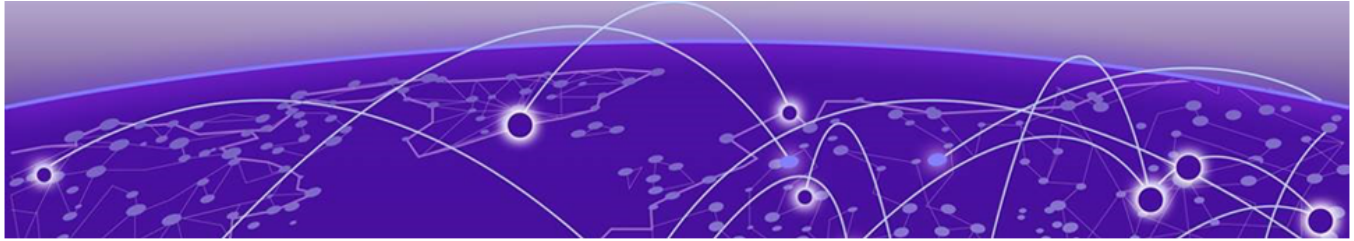
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, 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.
- Broken links or usability issues.

To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



SD-WAN CLI Overview

[SD-WAN Related Extreme ONE OS Switching Commands](#) on page 12

[What's New in This Document](#) on page 17

[Supported Platforms](#) on page 17

The ExtremeCloud SD-WAN OS ONE Command Reference Guide provides comprehensive instructions for working with the Command Line Interface. SD-WAN (Software-Defined Wide Area Networking) enhances network agility, security, and performance by leveraging centralized control and automation.



Note

ExtremeCloud SD-WAN OS ONE is designed to be fully configured and managed through the Orchestrator. Any configuration applied directly through the CLI may be overwritten by the Orchestrator or can cause system inconsistencies. Limit CLI usage to advanced users with sufficient expertise.

Refer to [Extreme ONE OS Switching Command Reference](#) for details about fundamental network commands. Refer to [Table 4](#) on page 12 for a list of Extreme OS Switching commands that are supported in ExtremeCloud OS ONE SD-WAN.

SD-WAN Related Extreme ONE OS Switching Commands

The following commands from Extreme OS ONE Switching are supported in ExtremeCloud SD-WAN OS ONE environments.

Table 4: Extreme OS ONE Switching Commands

Category	Command
Network Management	• <code>interface ethernet</code> • <code>show interface ethernet</code> • <code>interface port-channel</code> • <code>show counters interface port-channel</code> • <code>interface tunnel</code> • <code>show interface tunnel</code> • <code>subinterface (double tagged)</code> • <code>subinterface (untagged)</code> • <code>subinterface vlan (untagged)</code> • <code>show interface subinterface</code> • <code>tunnel-mode</code> • <code>shutdown</code> • <code>speed</code> • <code>duplex</code> • <code>mtu</code> • <code>ipv4 address</code> • <code>ipv4 neighbor</code> • <code>ipv4 neighbor reachable-time</code> • <code>show ipv4 interface</code> • <code>show ipv4 neighbor interface</code> • <code>show ipv4 neighbor vrf</code> • <code>show ipv4 route vrf</code> • <code>clear ipv4 route vrf</code> • <code>ipv4 anycast-gateway</code> • <code>ipv4 anycast-gateway-mac</code> • <code>ipv6 address</code> • <code>ipv6 neighbor</code> • <code>ipv6 neighbor reachable-time</code> • <code>show ipv6 interface</code> • <code>show ipv6 neighbor interface</code> • <code>show ipv6 neighbor vrf</code> • <code>clear ipv6 route vrf</code> • <code>ipv6 anycast-gateway</code> • <code>ipv6 anycast-gateway-mac</code> • <code>static-route enable-bfd</code> • <code>static-route</code> • <code>show access-list</code>

Table 4: Extreme OS ONE Switching Commands (continued)

Category	Command
	• <code>show overlay-networks</code> • <code>show counters link-fault-signaling</code> • <code>show counters interface ethernet</code> • <code>show counters interface port-channel</code> • <code>show counters interface tunnel</code> • <code>show link-fault-signaling</code> • <code>show l2 mac-move-detection</code> • <code>show l2 mac-move-detection shut-list</code> • <code>show mirror</code> • <code>clear bgp vrf routes l2vpn-evpn nvo</code> • <code>clear bgp vrf routes l2vpn-evpn nvo route-distinguisher</code> • <code>clear bgp vrf routes l2vpn-evpn nvo route-distinguisher route-type</code> • <code>clear bgp vrf routes l2vpn-evpn nvo route-type</code> • <code>clear bgp vrf routes l2vpn-evpn nvo route-type arp vlan ipv4-prefix mac</code> • <code>clear bgp vrf routes l2vpn-evpn nvo route-type imr vlan originator</code> • <code>clear bgp vrf routes l2vpn-evpn nvo route-type mac vlan mac</code> • <code>clear bgp vrf routes l2vpn-evpn nvo route-type nd vlan ipv6-prefix mac</code> • <code>clear bgp vrf routes l2vpn-evpn nvo route-type prefix vlan ipv4-prefix</code> • <code>clear bgp vrf routes l2vpn-evpn nvo route-type prefix vlan ipv6-prefix</code> • <code>clear counters access-list</code> • <code>clear counters interface ethernet</code> • <code>clear counters interface cellular</code> • <code>clear counters interface port-channel</code> • <code>clear counters interface tunnel</code> • <code>clear counters lldp</code> • <code>clear ipv4 neighbor interface</code> • <code>clear ipv4 neighbor vrf</code> • <code>clear ipv6 neighbor interface</code> • <code>clear ipv6 neighbor vrf</code> • <code>clear l2 mac-move-detection shut-list</code> • <code>clear ipv4 route vrf</code> • <code>clear ipv6 route vrf</code> • <code>show system redundant-management</code> • <code>show system mac-address-table aging-time</code>

Table 4: Extreme OS ONE Switching Commands (continued)

Category	Command
	• <code>description</code> • <code>type</code> • <code>destination interface</code> • <code>auto-negotiate</code> • <code>link-fault-signaling</code> • <code>show link-fault-signaling</code> • <code>fec</code> (Ethernet interface configuration) • <code>loopback-mode</code> • <code>show interface loopback-mode</code> • <code>mirror</code> • <code>show mirror</code> • <code>load-balance</code> • <code>activate-network</code> • <code>network</code> • <code>overlay-networks</code> • <code>show overlay-networks</code> • <code>neighbor</code>
BGP and Routing	• <code>address-family</code> • <code>activate</code> • <code>activate-network</code> • <code>peer-group</code> • <code>remote-as</code> • <code>local-as-forced</code> • <code>local-as</code> • <code>route-policy</code> • <code>import-policy</code> • <code>export-policy</code> • <code>static-route enable-bfd</code> • <code>show bfd neighbors</code> • <code>show bfd neighbors application</code> • <code>show bfd neighbors dest-ip</code> • <code>show bfd neighbors interface</code> • <code>show mlag peer bfd</code> • <code>clear counters bfd</code> • <code>show bfd neighbors</code> • <code>show bfd neighbors application</code> • <code>show bfd neighbors dest-ip</code> • <code>show bfd neighbors interface</code> • <code>graceful-restart</code> • <code>router bgp</code>

Table 4: Extreme OS ONE Switching Commands (continued)

Category	Command
	• <code>router-id</code> • <code>nexthop-self</code> • <code>ebgp-multihop</code> • <code>update-source</code> • <code>timers</code> • <code>keepalive-interval</code> • <code>keepalive</code> • <code>hold-time</code> • <code>connect-retry</code> • <code>fast-external-failover</code> • <code>cluster-id</code> • <code>route-reflector-client</code> • <code>listen-range</code> • <code>auth-password</code> • <code>use-multiple-paths</code> • <code>add-paths</code> • <code>route-distinguisher</code> • <code>instance-type</code> • <code>restart-time</code> • <code>helper-only</code> • <code>policy-result</code> • <code>policy</code> • <code>conditions</code>

Table 4: Extreme OS ONE Switching Commands (continued)

Category	Command
Layer 2 and Switching	• <code>bridge-domain</code> • <code>show bridge-domain</code> • <code>show counters bridge-domain</code> • <code>clear counters bridge-domain</code> • <code>clear mac-address-table bridge-domain</code> • <code>mac-address-table aging-time</code> • <code>statistics</code> • <code>arp-proxy</code> • <code>arp-snooping</code> • <code>lacp min-links</code> • <code>lacp port-priority</code> • <code>lacp rate</code> • <code>lacp system-mac</code> • <code>lacp system-priority</code> • <code>protocol lacp</code> • <code>show counters lacp</code> • <code>show lacp interface</code> • <code>show lacp system-identifier</code> • <code>clear counters interface tunnel</code> • <code>channel-group</code> • <code>mld</code> • <code>show counters mld peer</code> • <code>clear counters mld</code> • <code>show mld interfaces</code> • <code>show mld peer bfd</code> • <code>show mld peer</code> • <code>show mld</code> • <code>peer-group</code> • <code>peer</code> • <code>bringup-delay</code> • <code>tunnel-mode</code> • <code>overlay-networks</code> • <code>show overlay-networks</code>
QoS and Security	• <code>qos</code> • <code>show qos interface</code> • <code>show qos nvo</code> • <code>show qos traffic-class-map</code> • <code>show qos remark</code> • <code>show counters qos interface control-plane queue</code>

Table 4: Extreme OS ONE Switching Commands (continued)

Category	Command
	• <code>show counters qos interface ethernet queue</code> • <code>clear counters qos interface control-plane queue</code> • <code>clear counters qos interface ethernet queue</code> • <code>bgp-actions</code> • <code>bgp-conditions</code> • <code>bgp-defined-sets</code> • <code>show bgp vrf l2vpn-evpn</code> • <code>show bgp vrf neighbor</code> • <code>show bgp vrf neighbors</code> • <code>show bgp vrf routes</code> • <code>show bgp vrf summary</code> • <code>clear bgp neighbor</code> • <code>input</code> • <code>access-list</code> • <code>profile</code> • <code>interval</code> • <code>conditions</code> • <code>actions</code> • <code>as-path-set</code> • <code>community-set</code> • <code>ext-community-set</code> • <code>as-notation</code> • <code>protocol</code>

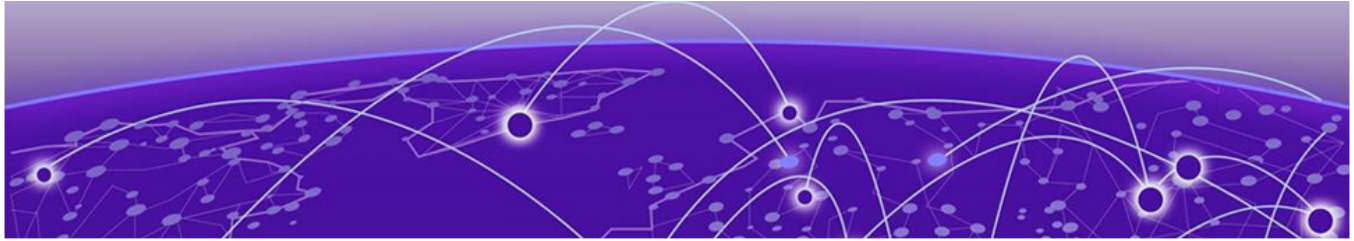
What's New in This Document

This is the initial release of ExtremeCloud OS ONE SD-WAN Command Reference Guide, and all CLI commands in this guide are introduced in this release.

Supported Platforms

This release supports the following hardware platforms:

- lpe 40ax-v2
- lpe 420ax
- lpe 2200ax-F
- lpe 2200ax-T
- XSE 600



Using the CLI

[User Accounts](#) on page 18
[Accessing the CLI](#) on page 19
[Command Modes](#) on page 19
[Displaying CLI Commands and Command Syntax](#) on page 20
[Completing CLI Commands](#) on page 21
[CLI Keyboard Shortcuts](#) on page 22
[Using CLI Command Output Modifiers](#) on page 22
[Unsupported Input Characters](#) on page 23
[Debug and System Diagnostic Commands](#) on page 23

Extreme OS ONE SD-WAN offers Command Line Interface support. The following topics describe how to access system commands to configure, monitor, and troubleshoot network settings efficiently.



Note

ExtremeCloud OS ONE SD-WAN is designed to be fully configured and managed through the Orchestrator. Any configuration applied directly through the CLI may be overwritten by the Orchestrator or can cause system inconsistencies. Limit CLI usage to advanced users with sufficient expertise.

User Accounts

A user account specifies that user's level of access to the SD-WAN CLI.

The software uses role-based access control (RBAC) as the authorization mechanism. A *role* is a container for rules, which specify which commands can be executed and with which permissions. When you create a user account, you need to specify a role for that account. In general, *user* (as opposed to *user-level*) refers to any account to which any role can be assigned user, admin, or a non-default role.

The software includes two default accounts admin and user, each with a corresponding default role:

- **admin:** Accounts with admin permissions can execute all commands supported on the device.

- **user:** Accounts with user-level permissions can execute all **show** commands supported on the device. User-level accounts can also execute the following operational commands: **exit**, **ping**, and **traceroute**.

Accessing the CLI

You can access the CLI through a serial console connection to the serial console connection without a device management IP address assignment. After an IP address is assigned to the device management interface, you can access the CLI through a Telnet or SSH connection using the device management IP address.

The procedure to access the CLI is the same through either the console interface or through a Telnet or SSH session; both access methods bring you to the login prompt. The following example shows the admin role logging into the device:

```
device login: admin
Password:*****
device#
```



Note

Multiple users can open sessions on the device and issue commands. The device supports a maximum of 32 CLI sessions.

Command Modes

The CLI uses an industry-standard hierarchical shell familiar to networking administrators.

EXEC Mode

EXEC mode supports operational commands such as **clear**, **show**, and **debug**. You can also enter configuration mode from EXEC mode to make changes to the system.

To enter configuration mode, use the **configure terminal** command.

```
device# configure terminal
device(config)#
```

Global Configuration Mode

Global configuration mode supports commands that can change the device configuration. The system configuration is restored upon reboot. The global configuration mode provides access to subconfiguration modes for individual interfaces, VLANs, routing protocols, and other configuration areas. The following example shows how you access the interface subconfiguration mode by issuing the **interface** command with a specified interface:

```
device(config)# interface ethernet 0/1
device(config-if-eth-0/1)#
```

Displaying CLI Commands and Command Syntax

You can display commands and syntax information in any mode and from any point in the command hierarchy.

Enter a question mark (?) in any command mode to display the list of commands available in that mode:

```
device# ?
Possible completions:
cat          show information
certificate-manager Certificate Management Operations
clear        Show system information
clock        set switch date and time
configure    Configuration from vty interface
copy         Copy
efa          Extreme Fabric Automation
end          End current mode and change to enable mode
exit         Exit current mode and down to previous mode
factory-reset Update device to factory default settings
iah          Integrated Application Hosting (IAH) operations
list         Print command list
ls           List disk files
measured-boot Measured Boot
monitor      On Monitor session
no           Negate a command or set its defaults
ping         Ping
pwd          Display current mode path
python       Python interpreter shell
quit         Exit current session
reload       Reboot system
rm           delete file
show         Show system information
ssh-server   SSH server
start-shell  Start Bash shell
system       System commands
terminal     Set terminal timeout parameters
traceroute   Traceroute
unlock       Unlock a user account
usb          Enable USB storage access
```

To display a list of commands that start with the same characters, type the characters followed by a question mark (?):

```
device# e?
Possible completions:
show          Show system information
ssh-server    SSH server
start-shell   Start Bash shell
system        System commands
```

To display the keywords and arguments associated with a command, enter the keyword followed by a space and then a question mark (?):

```
device# terminal ?
Possible completions:
length      Set number of lines on a screen
timeout     Sets the interval that command interpreter wait for user input
```

If the question mark (?) is typed within an incomplete keyword, but the keyword matches several keywords, the CLI displays help for all the matching keywords:

```
device# sho s
  sysinfo  Display system components information
  system   Show system information
device#
```

The CLI accepts abbreviated commands, as long as each abbreviated token uniquely identifies a command or subcommand. For example, the following is a valid abbreviation for the **show qos interface** command:

```
device# sh q i
```

If the device does not recognize a command after you press **Enter**, an error message displays:

```
device# hookup
          ^
syntax error: unknown argument.
```

If you enter an incomplete command, an error message displays:

```
S2-IPE1# show
-----^
%Error: Command incomplete: 'show '
S2-IPE1#
```

Completing CLI Commands

To complete the spelling of a command or keyword automatically, begin typing the command or keyword and then press **Tab**. For example, at the CLI command prompt, type `term` and press **Tab**:

```
device# term
```

The CLI displays the following command:

```
device# terminal
```

If there is more than one command or keyword associated with the characters typed, the CLI displays all choices. For example, at the CLI command prompt, type `show l` and press **Tab**:

```
device# show l ?
```

The CLI displays the following command:

```
Possible completions:
S2-IPE1# show l ?
  l2                Layer 2 system information
  lacp              LACP
  link-fault-signaling Display link-fault-signaling
  lldp              Display lldp config information
  load-balance      Load Balance
  logging           Log entries
S2-IPE1#
```

CLI Keyboard Shortcuts

The following table lists CLI keyboard shortcuts.

Table 5: CLI keyboard shortcuts

Keystroke	Description
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+B (or the left arrow key)	Moves the cursor back one character.
Ctrl+C	Escapes and terminates command prompts and ongoing tasks (such as lengthy displays), and displays a fresh command prompt.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+F (or the right arrow key)	Moves the cursor forward one character.
Ctrl+N (or the down arrow key)	Displays commands in the history buffer with the most recent command displayed last.
Ctrl+P (or the up arrow key)	Displays commands in the history buffer with the most recent command displayed first.
Ctrl+U or Ctrl+X	Deletes all characters from the cursor to the beginning of the command line.
Ctrl+W	Deletes the last word you typed.
Ctrl+Z	Returns to privileged EXEC mode. Using Ctrl+Z in privileged EXEC mode executes partial commands.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.



Note

In privileged EXEC mode, use the **show history** command to list the commands most recently entered. The device retains the history of the last 1000 commands entered for the current session.

Using CLI Command Output Modifiers

You can filter the output of the CLI **show** commands by using the output modifiers described below.

Table 6: CLI command output modifiers

Output modifier	Description
append	Appends the output to a file.
redirect	Redirects the command output to the specified file.
include	Displays the command output that includes the specified expression.

Table 6: CLI command output modifiers (continued)

Output modifier	Description
exclude	Displays the command output that excludes the specified expression.
begin	Displays the command output that begins with the specified expression.
last	Displays only the last few lines of the command output.
tee	Redirects the command output to the specified file. Notice that this modifier also displays the command output.
until <i>string</i>	Ends the output when the output text matches the string.
count	Counts the number of lines in the output.
linnum	Enumerates the lines in the output.
more	Paginates the output.
nomore	Suppresses the pagination of the output.
FLASH	Redirects the output to flash memory.

Unsupported Input Characters

Characters dependent on combinations of the **AltGr** key and another key are never supported.

**Note**

The **AltGr** key is the **Alt** key to the right of the spacebar.

Debug and System Diagnostic Commands

Debug and system diagnostic commands, such as debug and show system internal commands, are developed and intended for specialized troubleshooting.

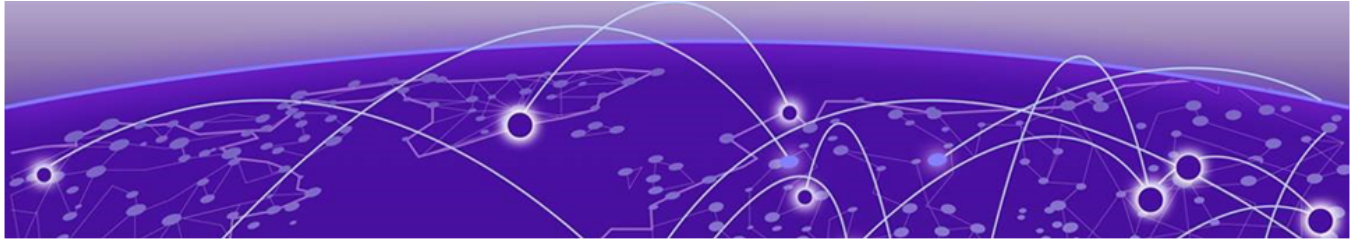
**Note**

ExtremeCloud SD-WAN CLI commands should only be used by advanced users. CLI changes may be overridden by the Orchestrator and can lead to configuration inconsistencies.

Work closely with Extreme Networks technical support in executing such commands and interpreting their results.

**Note**

Not all diagnostic commands are documented.



Firmware Management Commands

Use the following firmware management commands to view firmware version information and upgrade the device firmware.

Refer to [Extreme ONE OS Switching Command Reference](#) for more information on firmware related commands.

View Firmware Version Information

Use the following commands to view firmware version and history details on the device.

View Primary and Secondary Firmware Versions

```
show firmware
```

Displays the firmware images currently installed in the primary and secondary locations.

View Firmware Activation History

```
show firmware history
```

Displays the last five firmware versions that were activated on the device.

View Firmware Audit and Logging Information

```
show logging audit firmware
```

Displays firmware-related audit and logging information.

Firmware Upgrade Commands

The system maintains primary and secondary firmware images. When you install a new firmware image:

1. The system removes the existing secondary image
2. Moves the current primary image to the secondary location
3. Installs the new image in the primary location

Both IPv4 and IPv6 addresses are supported for firmware upgrades. After a successful firmware update, the system automatically reboots to activate the new firmware image. The system sets the reboot reason to **Firmware Upgrade** for both firmware upgrade

and rollback operations and stores this value in the chassis-0 system property, which represents the device chassis state.

Upgrade the firmware using one of the following commands:

- `system firmware update disk://firmware/filename`
- `system firmware update usb://filename`
- `system firmware update scp://username:password@host[:port]/filepath`
- `system firmware update sftp://username:password@host[:port]/filepath`
- `system firmware update http://[username:password@]host[:port]/filepath`
- `system firmware update https://[username:password@]host[:port]/filepath`



Note

To perform a firmware upgrade from a USB device, enable USB access before starting the upgrade:

```
usb enable
```

If the device does not have a dedicated out-of-band management interface and uses an in-band WAN interface for network access, specify the WAN VRF during the firmware upgrade.

```
system firmware update https://[username:password@]host[:port]/filepath vrf <vrf-name>
```

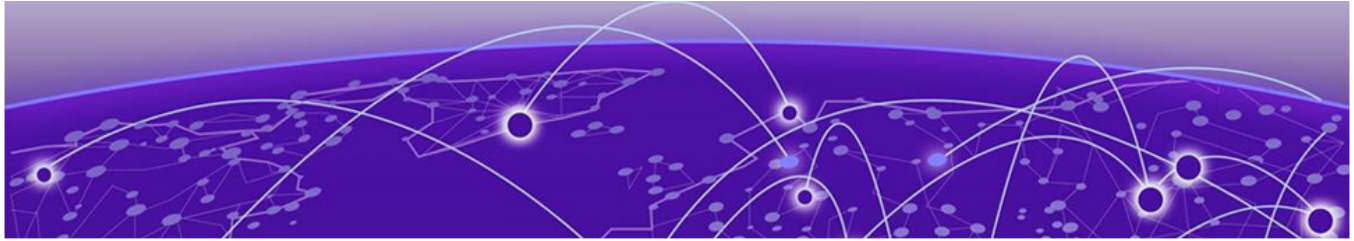
Firmware Activation and Rollback Behavior

After reboot, only specific configurations persist, and the system brings up all microservices. When the microservices start successfully, the system publishes the running firmware version to the **Firmware Rev** property of the **chassis-0** component in the State DB. If any microservice fails to start within the specified time, the system automatically rolls back to the previously installed firmware image.

If the new firmware version is not required, manually revert the device to the previously installed firmware image. Use the following command to roll back the firmware:

```
system firmware rollback
```

After the rollback, the system automatically reboots and activates the previous firmware image.



AVC Commands

[application](#) on page 27
[application-group](#) on page 30
[application-performance policy](#) on page 33
[capability](#) on page 36
[cellular wan-interface](#) on page 38
[dws-method](#) on page 40
[security-rule-policy](#) on page 42
[sla-profile](#) on page 45
[wan-interface](#) on page 49
[wan-service](#) on page 52
[appliance](#) on page 55
[appliance wan-id](#) on page 57
[data-record](#) on page 59

application

Use the **application** command to create a named application under AVC and enter the application configuration sub-mode. An application represents a specific network application or protocol that AVC uses for traffic identification, classification, and policy enforcement.

Syntax

application < *NAME* >

Command Default

No application is configured by default.

Parameters

NAME - Name for the identification of the application.

The following sub-commands are available within application configuration mode:

- **ad-hoc-subnets** - Configure ad-hoc subnets for the application. Enters sub-mode with **adhoc prefix**
- **attribute-type** - Configure attribute type parameters for the application. Enters sub-mode with **attribute**
- **id** <*value*> - Unique numeric identifier for the application. Id of the application should be in range of (0-65536)
- **precedence** < *value* > - Precedence of the application. Select the precedence of the application in range of (1-65536)
- **protocol** - Name of the protocol associated with the application
- **protocol-id** < *value* > - Numeric identifier assigned to the protocol. Select ID of the protocol in range of (0-65535)
- **tier** - Defines the tier of the application. This determines the classification of the application as either **CLIENT** or **SERVER**.

The default value is **CLIENT**.

Modes

Entered from: AVC configuration **config-avc**

Enters into: AVC capability configuration **config-avc-application-<NAME>**

Usage Guidelines

Use this command to create a named application and enter its sub-mode, where identification and classification parameters can be configured. Each application is uniquely identified by a numeric ID and can be associated with a protocol, protocol ID, precedence value, and optional attributes for deeper traffic classification.

Use this command in config mode only. Only users with the admin role can use this command.

Examples

The following example configures an application named a1 in the AVC configuration mode.

```
kvm-x86-64(config-avc)# application a1
kvm-x86-64(config-avc-application-a1)#
  precedence      Precedence of the application
kvm-x86-64(config-avc-application-a1)# precedence 1
  protocol        Name of the protocol type of the application
kvm-x86-64(config-avc-application-a1)# protocol http
  protocol-id     ID of the protocol type of the application
kvm-x86-64(config-avc-application-a1)# protocol-id 1
kvm-x86-64(config-avc-application-a1)# tier
  client          Client as the tier
  server          Server as the tier
kvm-x86-64(config-avc-application-a1)# tier client
```

The following output displays the AVC configuration, including the application and its protocol settings:

```
kvm-x86-64# show running-config avc

avc
  application iperf
    id 3
    protocol iperf
    protocol-id 1461
    precedence 1
  !
  application a1
    id 1
    protocol rtp
    protocol-id 175
    precedence 1
    attribute-type Codec
  !
  application-group ag1
    id 1
    application a1
  !
  application-perf-policy ap1
    id 1
    precedence 2
    criticality low
    sla-profile-id 1
    application-group ag1
    dws
    flow-affinity
```

```
last-resort-policy forward
p-to-s-policy preferred
s-to-t-policy backup
primary-wan-service-ids 1 2 3
secondary-wan-service-ids 5
tertiary-wan-service-ids 0
!
!
security-firewall
ip-group ip1
id 1
subnet 1.1.1.0/24 2.2.2.0/24
ip-group ipg3
id 2
policy

!
id 0      type internal
name internall
priority 1
source-ip-group-id ip1
dest-ip-group-id ipg3
app-group ag1
action dti
!
id 1      type internet
name intl
priority 3
source-ip-group-id ip1 ipg3
app-group ag1
action swg
```

application-group

Use the **application-group** command to create a named application group under AVC and enter the application-group configuration sub-mode.

Syntax

application-group *NAME*

Command Default

No application group is configured by default.

Parameters

NAME - Name for the identification of the application group.

Use the following sub-commands are available within application-group configuration mode:

- **id** *<value>* - Unique numeric identifier for the application group. Id of the application group should be in range of (0-65535).
- **application** *<APP_NAME>* - List of Applications associated with application group.

Modes

Entered from: AVC configuration **config-avc**

Enters into: AVC application-group configuration **config-avc-application-group-*<NAME>***

Usage Guidelines

Use this command to create a named application group and enter its sub-mode, where member applications and identification parameters can be configured. Application groups are referenced in security firewall policies and application performance policies to apply rules to a collection of applications as a single entity.

Use this command in config mode only. Only users with the admin role can use this command.

Examples

The following example creates an application group named ag1 and enters its configuration mode:

```
kvm-x86-64 (config-avc) #  
kvm-x86-64 (config-avc-application-group-ag1) #
```

```

id          Unique Id of the application group
kvm-x86-64(config-avc-application-group-ag1)# id 1

```

The following example displays the running configuration with an application group configured:

```

kvm-x86-64# show running-config avc
avc
  application iperf
    id 3
    protocol iperf
    protocol-id 1461
    precedence 1
  !
  application a1
    id 1
    protocol rtp
    protocol-id 175
    precedence 1
    attribute-type Codec
  !
  application-group ag1
    id 1
    application a1
  !
  application-perf-policy ap1
    id 1
    precedence 2
    criticality low
    sla-profile-id 1
    application-group ag1
    dws
    flow-affinity
    last-resort-policy forward
    p-to-s-policy preferred
    s-to-t-policy backup
    primary-wan-service-ids 1 2 3
    secondary-wan-service-ids 5
    tertiary-wan-service-ids 0
  !
!
security-firewall
  ip-group ip1
    id 1
    subnet 1.1.1.0/24 2.2.2.0/24
  ip-group ipg3
    id 2
  policy

  !
  id 0      type internal
    name internal1
    priority 1
    source-ip-group-id ip1
    dest-ip-group-id ipg3
    app-group ag1
    action dti
  !
  id 1      type internet
    name int1
    priority 3
    source-ip-group-id ip1 ipg3

```

```
app-group agl  
action swg
```


application-performance policy

Use the **application-perf-policy** command to create a named application performance policy under AVC and enter the application performance policy configuration sub-mode. An application performance policy defines traffic handling behavior including criticality, SLA profiles, precedence, and dynamic WAN selection (DWS) rules, for one or more applications.

Syntax

application-perf-policy *APP_PERFORM*

Command Default

No application performance policy is configured by default.

Parameters

APP_PERFORM - Name of the application performance policy.

Use the following sub-commands within the application performance policy configuration mode:

- **id** *<value>* - Unique numeric identifier for the policy. Range (0-65535).
- **criticality** *<level>* - List of Applications associated with application group. The criticality is either top or high or medium or low.
- **sla-profile-id** *<value>* - SLA profile identifier associated with the policy. Range (0-4294967295).
- **precedence** *<value>* - Precedence value for policy matching priority. Range (1-65536).
- **application-group** *APP_NAME* - Application group associated with application performance policy.
- **dws** - Enter dynamic WAN selection sub-mode.

The following sub-commands are available within DWS configuration mode:

- **flow-affinity** - Enable flow-based WAN path affinity.
- **last-resort-policy** *< forward | drop >* - Select the last resort policy for traffic handling. Forward packets without any DWS intervention or drop the traffic.
- **p-to-s-policy** *<policy>* - Primary-to-secondary failover policy. Prefer secondary WAN services if primary WAN service quality degrades or if connectivity over primary WAN services is lost.
- **s-to-t-policy** *<policy>* - Secondary-to-tertiary failover policy. Prefer tertiary WAN services when secondary WAN service quality degrades or connectivity over secondary WAN services is lost.
- **primary-wan-service-ids** *<values>* - Primary WAN service IDs.

- **secondary-wan-service-ids** <values> - Secondary WAN service IDs.
- **tertiary-wan-service-ids** <values> - Tertiary WAN service IDs.

The policy name must not be a reserved keyword.

Modes

Entered from: AVC configuration **config-avc**

Enters into: AVC application performance policy configuration **config-avc-application-perf-**<APP_PERFORM>

Usage Guidelines

Use this command to create a named application-performance policy and enter its sub-mode. In the sub-mode, you configure the criticality, SLA profile, precedence, associated applications, and DWS parameters.

Use this command in config mode only. Only users with the admin role can use this command.

Examples

The following example creates an application performance policy, configures all sub-commands including DWS parameters, and shows the resulting running configuration:

```
kvm-x86-64(config-avc)# application-perf-policy apl
kvm-x86-64(config-avc-application-perf-apl)# id 1
kvm-x86-64(config-avc-application-perf-apl)# precedence 2
kvm-x86-64(config-avc-application-perf-apl)# criticality low
kvm-x86-64(config-avc-application-perf-apl)# sla-profile-id 1
kvm-x86-64(config-avc-application-perf-apl)# application-ids 1 2 3
kvm-x86-64(config-avc-application-perf-apl)# dws
kvm-x86-64(config-avc-application-perf-apl-dws)# flow-affinity
kvm-x86-64(config-avc-application-perf-apl-dws)# last-resort-policy forward
kvm-x86-64(config-avc-application-perf-apl-dws)# p-to-s-policy preferred
kvm-x86-64(config-avc-application-perf-apl-dws)# s-to-t-policy backup
kvm-x86-64(config-avc-application-perf-apl-dws)# primary-wan-service-ids 1 2 3
kvm-x86-64(config-avc-application-perf-apl-dws)# secondary-wan-service-ids 5
kvm-x86-64(config-avc-application-perf-apl-dws)# tertiary-wan-service-ids 0
```

The following example shows an error when a reserved keyword is used as the policy name:

```
kvm-x86-64(config-avc)# application-perf-policy app-group
kvm-x86-64(config-avc-application-perf-app-group)# id 3
%Error: application performance policy name must not be reserved keyword "app-group"
```

The following example displays the complete running configuration:

```
kvm-x86-64# show running-config avc

avc
  application iperf
    id 3
    protocol iperf
    protocol-id 1461
    precedence 1
  !
  application a1
    id 1
    protocol rtp
    protocol-id 175
    precedence 1
    attribute-type Codec
  !
  application-group ag1
    id 1
    application a1
  !
  application-perf-policy apl
    id 1
    precedence 2
    criticality low
    sla-profile-id 1
    application-group ag1
    dws
    flow-affinity
    last-resort-policy forward
    p-to-s-policy preferred
    s-to-t-policy backup
    primary-wan-service-ids 1 2 3
    secondary-wan-service-ids 5
    tertiary-wan-service-ids 0
  !
!
security-firewall
  ip-group ip1
    id 1
    subnet 1.1.1.0/24 2.2.2.0/24
    ip-group ipg3
    id 2
    policy

    !
    id 0      type internal
      name internall
      priority 1
      source-ip-group-id ip1
      dest-ip-group-id ipg3
      app-group ag1
      action dti
    !
    id 1      type internet
      name intl
      priority 3
      source-ip-group-id ip1 ipg3
      app-group ag1
      action swg
```

capability

Use the **capability** command to configure AVC capability types that define the functional mode of the Application Visibility and Control engine.

Syntax

```
capability < application-visibility | application-control | application-identification | dws | remote-application-control >
```

Command Default

No AVC capability is configured by default.

Parameters

The following parameters are available for this command:

- *application-visibility* - Enables Application Visibility type. Provides traffic visibility and reporting without enforcement.
- *application-control* - Enables Application Control type. Provides traffic enforcement based on application identification.
- *application-identification* - Enables Application Identification type. Identifies applications in traffic flows.
- *dws* - Enables DWS type. Provides intelligent path selection across WAN links.
- *remote-application-control* - Enables Remote Application Control type. Provides application control for remote/branch deployments.

Modes

Entered from: AVC configuration **config-avc**

Enters into: AVC capability configuration **config-avc-capability-<type>**

Usage Guidelines

Use this command to define which AVC capabilities are active on the device. Each capability type can be independently enabled or disabled. Multiple capability types can be configured simultaneously. After entering capability configuration mode for a specific type, use the **enable** command to activate it.

This command is available only to users with admin role.

Examples

The following example configures a single capability type on the device:

```
device# configure terminal
device(config)# avc
device(config-avc)# capability application-control
device(config-avc-capability-application-control)# enable
device(config-avc-capability-application-control)#
```

The following example configures multiple capability types on the device:

```
device# configure terminal
device(config)# avc
device(config-avc)# capability dws
device(config-avc-capability-dws)# enable
device(config-avc)# capability application-visibility
device(config-avc-capability-application-visibility)# enable
device(config-avc)# capability application-identification
device(config-avc-capability-application-identification)# enable
device(config-avc)# capability remote-application-control
device(config-avc-capability-remote-application-control)# enable
device(config-avc)#
```

The following example displays the running configuration:

```
device# show running-config avc
avc
  capability dws
    enable
  !
  capability application-control
    enable
  !
  capability application-visibility
    enable
  !
  capability application-identification
    enable
  !
  capability remote-application-control
    enable
  !
```

cellular wan-interface

Use the **cellular wan-interface** command to configure a cellular WAN interface for AVC.

Syntax

```
wan-interface cellular WAN_INT
```

Command Default

No cellular WAN interface is configured by default.

Parameters

WAN_INT - Cellular port number. Valid value: 0

The following sub-commands are available within the cellular WAN interface mode:

- **max-egr-bw** *<value>* - Maximum egress (outgoing) bandwidth for this interface, in bits per second. Range 0 - 9223372036854775807.
- **max-ing-bw** *<value>* - Maximum ingress (incoming) bandwidth for this interface, in bits per second.
- **min-egr-bw** *<value>* - Minimum guaranteed egress bandwidth for this interface, in bits per second.
- **min-ing-bw** *<value>* - Minimum guaranteed ingress bandwidth for this interface, in bits per second.
- **wan-service-id** *<value>* - WAN service identifier associated with this interface.

Modes

Entered from: AVC configuration **config-avc**

Enters into: AVC capability configuration **config-avc-wan-interface-cellular-*<WAN_INT>***

Usage Guidelines

Use this command to associate a cellular interface with AVC for WAN traffic management. Once configured, bandwidth parameters and WAN service IDs can be applied to the cellular interface using sub-commands within the WAN interface configuration mode.

This command is available only to users with admin role.

Examples

The following example configures cellular port 0 as a WAN interface under AVC:

```
device# configure terminal
device(config)# avc
device(config-avc)# wan-interface cellular 0
device(config-avc-wan-interface-cellular-0)#
```

The following example configures bandwidth and service parameters on the cellular WAN interface:

```
device# configure terminal
device(config)# avc
device(config-avc)# wan-interface cellular 0
device(config-avc-wan-interface-cellular-0)# wan-service-id 1
device(config-avc-wan-interface-cellular-0)# max-egr-bw 4000
device(config-avc-wan-interface-cellular-0)# max-ing-bw 4000
device(config-avc-wan-interface-cellular-0)# min-egr-bw 2000
device(config-avc-wan-interface-cellular-0)# min-ing-bw 2000
device(config-avc-wan-interface-cellular-0)#
```

The following example displays the running configuration:

```
device# show running-config avc

avc
  wan-interface cellular 0
    wan-service-id 1
    max-egr-bw 4000
    max-ing-bw 4000
    min-egr-bw 2000
    min-ing-bw 2000
```

dws-method

Use the **dws-method** command to select the Dynamic WAN Selection (DWS) method under AVC. The DWS method determines how the device selects WAN paths for application traffic, dynamically based on real-time metrics, via wire, via switch-based selection, or disabled entirely.

Syntax

dws-method < *dynamic* | *wire* | *switch* | *none* >

Command Default

No DWS policy is configured by default.

Parameters

The following parameters are available for this command:

- < *dynamic* > - Selects WAN paths based on real-time performance metrics.
- < *none* > - Disables dynamic WAN selection.
- < *switch* > - Uses switch-based path selection.
- < *wire* > - Uses direct wire path selection.

Modes

AVC configuration mode.

Usage Guidelines

Use this command to define how the device selects WAN paths for traffic subject to application performance policies. The DWS method applies globally to all application performance policies configured under AVC.

The method must be one of: dynamic, wire, switch, or none.

This command is available only to users with admin role.

Examples

The following example sets the DWS method to dynamic in AVC configuration mode:

```
kvm-x86-64(config-avc)# dws-method
dynamic    Dynamic DWS method
none       No DWS
switch     Switch DWS method
wire       Wire DWS method

kvm-x86-64(config-avc)# dws-method dynamic
```


The following output shows the **dws-method** setting along with other AVC configuration details:

```
kvm-x86-64# show running-config avc

avc
  application iperf
    id 3
    protocol iperf
    protocol-id 1461
    precedence 1
  !
  application a1
    id 1
    protocol rtp
    protocol-id 175
    precedence 1
    attribute-type Codec
  !
  application-group ag1
    id 1
    application a1
  !
  application-perf-policy ap1
    id 1
    precedence 2
    criticality low
    sla-profile-id 1
    application-group ag1
    dws
      flow-affinity
      last-resort-policy forward
      p-to-s-policy preferred
      s-to-t-policy backup
      primary-wan-service-ids 1 2 3
      secondary-wan-service-ids 5
      tertiary-wan-service-ids 0
    !
  !
  security-firewall
    ip-group ip1
      id 1
      subnet 1.1.1.0/24 2.2.2.0/24
    ip-group ipg3
      id 2
    policy

      !
      id 0      type internal
        name internal1
        priority 1
        source-ip-group-id ip1
        dest-ip-group-id ipg3
        app-group ag1
        action dti
      !
      id 1      type internet
        name int1
        priority 3
        source-ip-group-id ip1 ipg3
        app-group ag1
        action swg
```

security-rule-policy

Use the **policy** command to the security firewall policy configuration sub-mode under AVC. A security rule policy defines traffic filtering and enforcement behavior, including source or destination IP groups, application groups, URL filtering, reputation scoring, and actions for internet, internal, or URL-filter security rules.

Syntax

policy

Command Default

NA

Parameters

policy - Internet/internal-security policy config mode for the IP groups.

The following are the commands to configure settings in the security rule policy:

Security Firewall Configuration

- **ip-group** *NAME* - Create an IP group under the security firewall.

The following sub-command is available after entering an IP group

- **subnet** *A.B.C.D/M* - Configure subnets in the IP group.

Policy Rule Creation

- **id** *<0-65535>* **type** *<internet \|| internal \|| url-filter>* - Create a security rule and enter rule configuration mode.

Rule Configuration

The following sub-commands are available after entering a rule with id *<value>* type *<type>*

- **app-group** *APP_NAME* - List of application groups in the rule.
- **dest-ip-group-id** *<value>* - List of destination IP group IDs.
- **action** *<deny | dti | swg>* - Action to be performed on the rule. deny: deny traffic. dti: direct traffic to internet. swg: traffic through secure web gateway.
- **name** *<NAME>* - Name of the security firewall policy.
- **priority** *<value>* - Priority of the policy in range of (0-65535).
- **source-ip-group-id** *<value>* - List of source IP group IDs.

Modes

Entered from: AVC security firewall configuration **config-avc-security-firewall**

Enters into: AVC security firewall policy configuration **config-avc-security-firewall-policy**

Usage Guidelines

Use this command to enter policy configuration mode under the security firewall. When in policy mode, create individual security rules using the id and type combination to enter a rule-specific sub-mode. Then configure match criteria and actions.

Use this command in config mode only. Only users with the admin role can use this command.

Examples

The following example configures settings in the security rule policy:

```
kvm-x86-64 (config-avc-security-firewall) #

ip-group      Ip group name

kvm-x86-64 (config-avc-security-firewall-ip-group1) # ip-group ip1
kvm-x86-64 (config-avc-security-firewall-ip1) #
    id          ip-group id

kvm-x86-64 (config-avc-security-firewall-ip1) # id 1
kvm-x86-64 (config-avc-security-firewall-ip1) #
    subnet      List of subnets under ip-group
kvm-x86-64 (config-avc-security-firewall-ip1) # subnet 1.1.1.0/24

kvm-x86-64 (config-avc-security-firewall-ip1) # subnet 1.1.1.0/24 2.2.2.0/24
kvm-x86-64 (config-avc-security-firewall-policy) # id 0 type internet

kvm-x86-64 (config-avc-security-firewall-policy-internet) #

dest-ip-group-id      List of destination ip group ids

kvm-x86-64 (config-avc-security-firewall-policy-internet) # dest-ip-group-id ipg3

kvm-x86-64 (config-avc-security-firewall-policy-internet) #
    action          Action to be performed on the rule
kvm-x86-64 (config-avc-security-firewall-policy-internet) # action dti
kvm-x86-64 (config-avc-security-firewall-policy-internet) #
    name            name of the security firewall policy
kvm-x86-64 (config-avc-security-firewall-policy-internet) # name intrule
kvm-x86-64 (config-avc-security-firewall-policy-internet) #
    priority        Priority of the policy configured
kvm-x86-64 (config-avc-security-firewall-policy-internet) # priority 1

kvm-x86-64 (config-avc-security-firewall-policy-internet) #

source-ip-group-id      List of source ip group ids

kvm-x86-64 (config-avc-security-firewall-policy-internet) # source-ip-group-id ip1
```

The following example displays the complete running configuration showing all security firewall components together:

```
kvm-x86-64# show running-config avc

avc
  application iperf
    id 3
    protocol iperf
    protocol-id 1461
    precedence 1
  !
  application a1
    id 1
    protocol rtp
    protocol-id 175
    precedence 1
    attribute-type Codec
  !
  application-group ag1
    id 1
    application a1
  !
  application-perf-policy ap1
    id 1
    precedence 2
    criticality low
    sla-profile-id 1
    application-group ag1
    dws
    flow-affinity
    last-resort-policy forward
    p-to-s-policy preferred
    s-to-t-policy backup
    primary-wan-service-ids 1 2 3
    secondary-wan-service-ids 5
    tertiary-wan-service-ids 0
  !
!
security-firewall
  ip-group ip1
    id 1
    subnet 1.1.1.0/24 2.2.2.0/24
  ip-group ipg3
    id 2
  policy

    !
    id 0      type internal
    name internal1
    priority 1
    source-ip-group-id ip1
    dest-ip-group-id ipg3
    app-group ag1
    action dti
    !
    id 1      type internet
    name int1
    priority 3
    source-ip-group-id ip1 ipg3
    app-group ag1
    action swg
```

sla-profile

Use the **sla-profile** command to create a named SLA (Service Level Agreement) profile under AVC and enter the SLA profile configuration sub-mode. An SLA profile defines performance thresholds and objectives including bandwidth, delay, jitter, loss, and TCP metrics against which WAN path quality is measured for Dynamic WAN Selection (DWS) decisions.

Syntax

sla-profile <PROFILE>

Command Default

No SLA profile is configured by default.

Parameters

PROFILE - Name of the SLA profile.

Use the following commands to configure settings in an SLA profile:

- **max-bandwidth** <0-9223372036854775807> - Specifies the maximum bandwidth allowed for a single session, in bps.
- **max-jitter** <0-4294967295> - Maximum jitter value in milliseconds.
- **max-loss** <(0-4294967295)> - Defines the maximum packet loss.
- **max-tcp-srt** <(0-4294967295)> - Specifies the maximum TCP session response time (SRT) in milliseconds.
- **max-tcp-retransmission** <(0-4294967295)> - Maximum number of TCP retransmissions allowed.
- **max-tcp-rtt** <(0-4294967295)> - Specifies the maximum allowable TCP round-trip time (RTT), in milliseconds.
- **max-delay** <0-4294967295> - Specifies the delay threshold (in milliseconds) beyond which service degradation is considered severe.
- **objective-bandwidth** <(0-9223372036854775807)> - Defines the desired or target bandwidth for a single session, in bits per second (bps).
- **objective-delay** <(0-4294967295)> - Specifies the target end-to-end delay for the session, measured in milliseconds.
- **objective-jitter** <(0-4294967295)> - Specifies the acceptable jitter threshold for the session, in milliseconds.
- **objective-loss** <(0-4294967295)> - Indicates the acceptable packet loss threshold, expressed in tenths of a percent.
- **objective-tcp-srt** <(0-4294967295)> - Defines the desired TCP session response time (SRT), measured in milliseconds.

- **objective-tcp-retransmission** *<(0-4294967295)>* - Specifies the acceptable number of TCP retransmissions before the connection is considered degraded.
- **objective-tcp-rtt** *<(0-4294967295)>* - Defines the target TCP round-trip time (RTT), in milliseconds.
- **id** *<(0-4294967295)>* - Unique identifier for the SLA profile. Used to associate traffic with the defined SLA objectives.
- **traffic-type** *<realtime | transactional | other>* - Specifies the type of traffic the SLA profile applies to.

Modes

Entered from: AVC configuration **config-avc**

Enters into: AVC SLA profile configuration **config-avc-*<PROFILE>***

Usage Guidelines

Use this command to create a named SLA profile and enter its sub-mode, where performance thresholds (maximum tolerable values) and objectives (desired target values) can be configured for various network metrics. The SLA profile is referenced by application performance policies via **sla-profile-id** to determine when a WAN path is considered degraded and DWS should trigger a path change.

Each metric supports two values:

- **max** - The maximum tolerable threshold. If exceeded, the WAN path is considered failed for that metric.
- **objective** - The desired target. If exceeded but still below max, the path is considered degraded.

Use this command in config mode only. Only users with the admin role can use this command.

Examples

The following example configures an SLA profile named **qos1** in AVC configuration mode. The SLA profile defines acceptable thresholds and objectives for network performance metrics such as bandwidth, delay, jitter, loss, and TCP characteristics.

```
kvm-x86-64(config-avc)# sla-profile qos1
kvm-x86-64(config-avc-qos1)#
kvm-x86-64(config-avc-qos1)#
    max-bandwidth                Maximum Bandwidth for a single session in bits per second

kvm-x86-64(config-avc-qos1)# max-bandwidth 100
kvm-x86-64(config-avc-qos1)# max-delay
    (0-4294967295) Delay threshold in milliseconds should be in range (0-4294967295)
kvm-x86-64(config-avc-qos1)# max-delay 1000
kvm-x86-64(config-avc-qos1)# max-jitter
```

```

(0-4294967295) Maximum jitter in milliseconds should be in range (0-4294967295)
kvm-x86-64(config-avc-qos1)# max-jitter 100
kvm-x86-64(config-avc-qos1)# max-loss
(0-4294967295) Maximum packet loss should be in range (0-4294967295) since value is
tenth of percent
kvm-x86-64(config-avc-qos1)# max-loss 15
kvm-x86-64(config-avc-qos1)# max-tcp-srt
(0-4294967295) Maximum TCP server response time in milliseconds should be in range
(0-4294967295)
kvm-x86-64(config-avc-qos1)# max-tcp-srt 100
kvm-x86-64(config-avc-qos1)# max-tcp-retransmission
(0-4294967295) Maximum TCP retransmissions should be in range (0-4294967295) since
value is tenth of percent
kvm-x86-64(config-avc-qos1)# max-tcp-retransmission 20
kvm-x86-64(config-avc-qos1)# max-tcp-rtt
(0-4294967295) Maximum TCP round-trip time in milliseconds should be in range
(0-4294967295)
kvm-x86-64(config-avc-qos1)# max-tcp-rtt 100
kvm-x86-64(config-avc-qos1)# objective-bandwidth
(0-9223372036854775807) Objective bandwidth should be in range (0-9223372036854775807)
kvm-x86-64(config-avc-qos1)# objective-bandwidth 0
kvm-x86-64(config-avc-qos1)# objective-delay
(0-4294967295) Delay in milliseconds should be in range (0-4294967295)
kvm-x86-64(config-avc-qos1)# objective-delay 10
kvm-x86-64(config-avc-qos1)# objective-jitter
(0-4294967295) Objective jitter in milliseconds should be in range (0-4294967295)
kvm-x86-64(config-avc-qos1)# objective-jitter 10
kvm-x86-64(config-avc-qos1)# objective-loss
(0-4294967295) Objective packet loss should be in range (0-4294967295) since value is
tenth of percent
kvm-x86-64(config-avc-qos1)# objective-loss 10
kvm-x86-64(config-avc-qos1)# objective-tcp-srt
(0-4294967295) Objective TCP session response time in milliseconds should be in range
(0-4294967295)
kvm-x86-64(config-avc-qos1)# objective-tcp-srt 10
kvm-x86-64(config-avc-qos1)# objective-tcp-retransmission
(0-4294967295) Objective TCP retransmissions should be in range (0-4294967295) since
value is tenth of percent
kvm-x86-64(config-avc-qos1)# objective-tcp-retransmission 10
kvm-x86-64(config-avc-qos1)# objective-tcp-rtt
(0-4294967295) Objective TCP round-trip time in milliseconds should be in range
(0-4294967295)
kvm-x86-64(config-avc-qos1)# objective-tcp-rtt 100
kvm-x86-64(config-avc-qos1)# id
(0-4294967295) Id of the Sla profile should be in range of (0-4294967295)
kvm-x86-64(config-avc-qos1)# id 0
kvm-x86-64(config-avc-qos1)# traffic-type
other          Other traffic
realtime       Real time traffic
transactional  Transactional traffic
kvm-x86-64(config-avc-qos1)# traffic-type transactional

```

The following output displays the SLA profile configuration:

```

kvm-x86-64# show running-config avc
avc
sla-profile qos1
profile-id 0
traffic-type realtime
max-bandwidth 100
objective-bandwidth 1

```

```
max-delay 200
objective-delay 2
max-jitter 300
objective-jitter 3
max-loss 10
objective-loss 1
max-tcp-rtt 600
objective-tcp-rtt 5
max-tcp-response-time 700
objective-tcp-response-time 6
max-tcp-retransmission 50
objective-tcp-retransmission 5
!
```


wan-interface

Use **wan-interface** command to configure a WAN interface under AVC. A WAN interface associates a physical Ethernet interface with WAN service parameters including bandwidth limits and WAN service IDs for use in DWS and application performance policies.

Syntax

```
wan-interface <ethernet> <WAN_INT>
```

Command Default

No WAN interface is configured by default.

Parameters

WAN_INT - WAN interface identifier

Use the following commands to configure settings in an WAN interface:

- **max-egr-bw** <0-9223372036854775807> - Maximum egress (outgoing) bandwidth in bits per second.
- **max-ing-bw** <0-9223372036854775807> - Maximum ingress (incoming) bandwidth in bits per second.
- **min-egr-bw** <0-9223372036854775807> - Minimum egress bandwidth in bits per second.
- **min-ing-bw** <0-9223372036854775807> - Minimum guaranteed ingress bandwidth in bits per second.
- **wan-service-ids** <0-65536> - Identifier for WAN services associated with this interface.

Modes

Entered from: AVC configuration **config-avc**

Enters into: AVC WAN interface configuration **config-avc-wan-interface**

Usage Guidelines

Use this command to associate an Ethernet interface as a WAN interface under AVC. Once in WAN interface sub-mode, bandwidth parameters and WAN service IDs can be configured. These settings are used by DWS to determine available bandwidth and map traffic to the correct WAN service.

Use this command in config mode only. Only users with the admin role can use this command.

Examples

The following example configures a WAN interface **ethernet 0/2** in AVC configuration mode. It specifies ingress/egress bandwidth values and associates the interface with a WAN service ID.

```
kvm-x86-64(config-avc)# wan-interface
    ethernet Ethernet
kvm-x86-64(config-avc)# wan-interface ethernet
    WAN_INT Wan interface
kvm-x86-64(config-avc)# wan-interface ethernet 0/2
kvm-x86-64(config-avc-eth-0/1)# max-egr-bw
    (0-9223372036854775807) Maximum egress bandwidth should be in range
    (0-9223372036854775807)
kvm-x86-64(config-avc-eth-0/1)# max-egr-bw 100000

    max-ing-bw          Maximum ingress bandwidth for this interface in bits per second

kvm-x86-64(config-avc-eth-0/1)# max-ing-bw
    (0-9223372036854775807) Maximum ingress bandwidth should be in range
    (0-9223372036854775807)
kvm-x86-64(config-avc-eth-0/2)# min-egr-bw
    (0-9223372036854775807) Minimum egress bandwidth should be in range
    (0-9223372036854775807)
kvm-x86-64(config-avc-eth-0/2)# min-egr-bw 100
kvm-x86-64(config-avc-eth-0/1)# min-egr-bw
    (0-9223372036854775807) Minimum egress bandwidth should be in range
    (0-9223372036854775807)
kvm-x86-64(config-avc-eth-0/1)# min-egr-bw 100
kvm-x86-64(config-avc-eth-0/1)# wan-service-ids
    (0-65536) IDs of the WAN service should be in range (0-65536)
kvm-x86-64(config-avc-eth-0/1)# wan-service-ids 1
```

The following example configures WAN interfaces:

```
kvm-x86-64(config)# show running-con dws
avc
    wan-service Social
        id 0
    !
    wan-interface ethernet 0/2
        wan-service-ids 0 max-egr-bw 100 max-ing-bw 200 min-egr-bw 1 min-ing-bw 2 !
    dws-method dynamic
    application-group ag1
        id 0
        precedence 1
        type application-performance
        applications
            app-id 0 1
        !
        criticality top
        sla-profile-id 0
    dws
        sticky-choice
        last-resort-policy forward
        p-to-s-policy preferred
```

```
s-to-t-policy preferred
primary-wan-service-ids 0
secondary-wan-service-ids 1
tertiary-wan-service-ids 2
!
!
sla-profile qos1
id 0
max-delay 200
objective-delay 2
max-bandwidth 100
objective-bandwidth 1
max-jitter 300
objective-jitter 3
max-tcp-rtt 600
objective-tcp-rtt 5
max-tcp-srt 700
objective-tcp-srt 6
traffic-type realtime
!
!
```

wan-service

Use the **wan-service** command to create a named WAN service under AVC and enter the WAN service configuration sub-mode. A WAN service represents a logical WAN connection that can be referenced by WAN interfaces (via **wan-service-ids**) and application performance policies (via **primary-wan-service-ids**, **secondary-wan-service-ids**, **tertiary-wan-service-ids**) for DWS.

Syntax

```
wan-service <NAME>
```

Command Default

No WAN services are configured by default.

Parameters

The following parameters are available for this command:

- **<NAME>** - Name of the WAN service instance.
- **id** <0-4294967295> - Unique identifier for the WAN service.

Modes

Entered from: AVC configuration **config-avc**

Enters into: AVC WAN service configuration **config-avc-<NAME>**

Usage Guidelines

Use this command to create a named WAN service and enter its sub-mode, where an identifier can be assigned. The WAN service ID is referenced by WAN interfaces and application performance policies to associate physical links and traffic handling with a logical WAN service.

Use this command in config mode only. Only users with the admin role can use this command.

Examples

The following example creates a WAN service named *Social* and configures its ID:

```
kvm-x86-64(config-avc)# wan-service Social
kvm-x86-64(config-avc-Social)#
kvm-x86-64(config-avc-Social)# id
(0-4294967295) Id of the Wan service should be in range of (0-4294967295)
kvm-x86-64(config-avc-Social)# id 0
```

The following example displays the running configuration showing the WAN service in context with WAN interface and other AVC components:

```
kvm-x86-64(config)# show running-con avc
avc
  wan-service Social
    id 0
  !
  wan-interface ethernet 0/2
    wan-service-ids 0
    max-egr-bw 100
    max-egr-bw 200
    min-egr-bw 1
    min-ing-bw 2
  !
  dws-method dynamic
  sla-profile qos1
    id 0
    max-delay 200
    objective-delay 2
    max-bandwidth 100
    objective-bandwidth 1
    max-jitter 300
    objective-jitter 3
    max-tcp-rtt 600
    objective-tcp-rtt 5
    max-tcp-srt 700
    objective-tcp-srt 6
    traffic-type realtime
  application a1
    id 1
    protocol rtp
    protocol-id 175
    precedence 1
    attribute-type Codec
  !
  application iperf
    id 3
    protocol iperf
    protocol-id 1461
    precedence 1
  !
  application-group ag1
    id 1
    application a1
  !
  application-perf-policy ap1
    id 1
    precedence 2
    criticality low
    sla-profile-id 1
    dws
      sticky-choice
      last-resort-policy forward
      p-to-s-policy preferred
      s-to-t-policy backup
      primary-wan-service-ids 1 2 3
      secondary-wan-service-ids 5
      tertiary-wan-service-ids 0
  !
```

```
!
security-firewall
  ip-group ip1
  id 1
  subnet 1.1.1.0/24 2.2.2.0/24
  ip-group ipg3
  id 2
  policy

  !
  id 0      type internal
  name internal1
  priority 1
  source-ip-group-id ip1
  dest-ip-group-id ipg3
  app-group agl
  bidirectional
  action dti
  !
  id 1      type internet
  name int1
  priority 3
  source-ip-group-id ip1 ipg3
  app-group agl
  bidirectional
  action swg
```

appliance

Use the **appliance** command to create an appliance under AVC and enter the appliance configuration sub-mode for configuring relevant parameters.

Syntax

appliance *APPLIANCE*

Command Default

No appliance is configured by default.

Parameters

APPLIANCE - Name of the appliance.

The following sub-commands are available within appliance configuration mode:

- **id** *<value>* - Unique numeric identifier for the appliance. The appliance id should be in range between 0-65536.
- **appliance-type** *<local | internet>* - Defines the role of the appliance. Appliance type is either local or internet.

Modes

Entered from: AVC configuration **config-avc**

Enters into: AVC capability configuration **config-avc-*<APPLIANCE>***

Usage Guidelines

Use this command to create a named appliance and enter its sub-mode, where identification and classification parameters can be configured. Each appliance is uniquely identified by a numeric ID and can be assigned a type that defines its role in the AVC traffic flow

Use this command in config mode only. Only users with the admin role can use this command.

Examples

The following example creates an appliance named ap1 and enters its configuration mode:

```
kvm-x86-64(config-avc)# appliance ap1
kvm-x86-64(config-avc-ap1)#
```

The following example displays the running configuration with an appliance configured:

```
kvm-x86-64# show running-config avc
avc
  appliance A1
    id 1
    appliance-type internet
```


appliance wan-id

Use the **appliance wan-id** command to associate a WAN interface ID with an appliance and enter the WAN-ID sub-mode. Once in this mode, tunnel configurations can be applied as child configuration under the selected WAN ID.

Syntax

```
wan-id WAN_ID
```

Command Default

No WAN ID is configured by default.

Parameters

WAN_ID - WAN Interface ID. Type: integer. Valid range: 0 - 65535.

The following sub-command is available within WAN-ID configuration mode:

tunnel *<name>* - Tunnel name(s) associated with this WAN ID (comma-separated for multiple tunnels).

The WAN ID value must be in the range 0 - 65535.

Modes

Entered from: AVC configuration **config-avc-appliance**

Enters into: AVC capability configuration **config-avc-appliance-wan-id**

Usage Guidelines

Use this command to assign a WAN interface ID to an appliance. Each appliance can have multiple WAN IDs configured. Once in WAN-ID sub-mode, tunnel names can be associated with the WAN interface.

Use this command in appliance configuration mode. Only users with the admin role can use this command.

Examples

The following example configures WAN ID 1 under an appliance:

```
kvm-x86-64(config-avc-appliance)# wan-id 1
kvm-x86-64(config-avc-appliance-wan-id)#
```

The following example displays the running configuration with WAN IDs and tunnels configured:

```
kvm-x86-64# show running-config avc
avc
  appliance a1
    id 1
    appliance-type remote
    wan-id 1
      tunnel t1,t2,t3
    !
  wan-id 2
    tunnel tunnell1,tunnel2,tunnel
```

data-record

Use the **data-record** command to configure the type of data record for Application Visibility and Control (AVC) flow reporting.

Syntax

```
data-record < flow_dr | application_dr | application_flow_dr >
```

Command Default

No data record type is configured by default.

Parameters

The following parameters are available for this command:

- *flow_dr* - Flow data record.
- *application_dr* - Application data record.
- *application_flow_dr* - Application flow data record.

The following sub-command is available within data record configuration mode:

period <*value*> - Reporting period in seconds for this data record type. Period should be in range of (0-65536).

Data record type must be one of: *flow_dr*, *application_dr* and *application_flow_dr*.

Modes

Entered from: AVC configuration **config-avc**

Enters into: AVC capability configuration **config-avc-*<type>***

Usage Guidelines

Use this command to configure a data record type under AVC. Each data record type can be independently configured with its own reporting period. Multiple data record types can be configured simultaneously.

This command is available only to users with admin role.

Examples

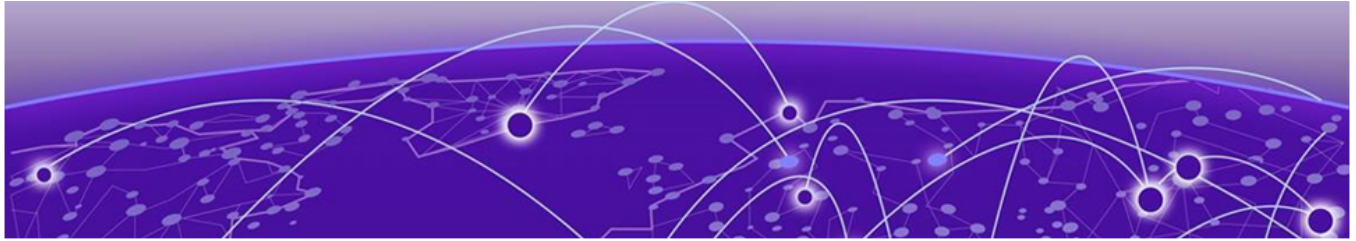
The following example configures a flow data record with a reporting period:

```
device# configure terminal
device(config)# avc
device(config-avc)# data-record flow_dr
```

```
device(config-avc-flow_dr)# period 30
device(config-avc-flow_dr)#
```

The following example displays the running configuration with multiple data record types:

```
device# show running-config avc
avc
  data-record flow_dr
    period 30
  !
  data-record application_dr
    period 10
  !
  data-record application_flow_dr
    period 20
  !
```



DTI commands

[dti](#) on page 62

[interface](#) on page 63

[tracker](#) on page 64

[target-ip](#) on page 65

dti

Use the **dti** command to switch from the global configuration to Direct to Internet (DTI) configuration mode.

Syntax

dti

Command Default

DTI is disabled by default.

Modes

dti configuration mode.

Examples

Configuration

```
# configure terminal
(config)# dti
(config-dti)#
```

interface

Use the **interface** command to configure a DTI interface.

Syntax

```
interface <IFNAME>
```

Command Default

No DTI interface is configured by default.

Parameters

enable - Use this command to enable DTI on an interface.

Modes

interface configuration mode

Examples

Configuration

```
kvm-x86-64(config-dti)# interface ethernet 0/5
kvm-x86-64(config-dti-eth-0/5)#
kvm-x86-64(config-dti-eth-0/5)# enable
kvm-x86-64(config-dti-eth-0/5)#
```

Running Configuration Output

```
kvm-x86-64(config)# do show running-config dti
dti
  interface ethernet 0/5
    enable
  !
!
kvm-x86-64(config)#
```

tracker

Use the **tracker** command to switch from the DTI configuration mode to tracker configuration mode.

Syntax

tracker

Command Default

No tracker IP is configured by default.

Parameters

This command has no keywords or variables.

Modes

tracker configuration mode

Examples

```
#configure terminal
kvm-x86-64(config)# dti
kvm-x86-64(config-dti)# tracker
kvm-x86-64(config-dti-tracker)#
```


target-ip

Use the **target-ip** command to create target IP

Syntax

target-ip IPV4

Command Default

No target IP is configured by default.

Parameters

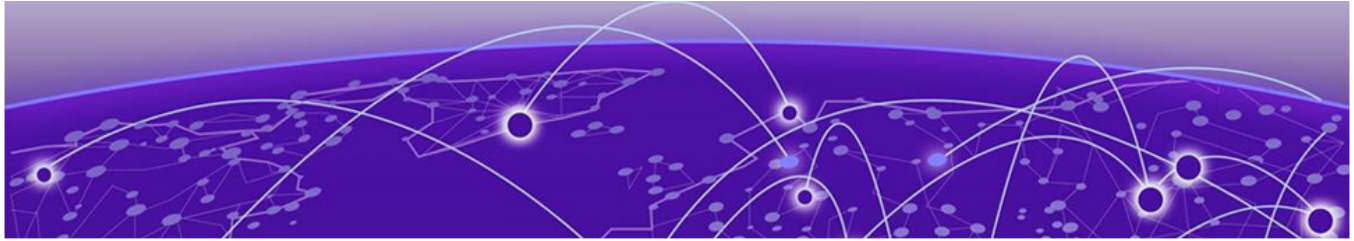
- *interval* - Interval between icmp packets to target IP. Interval should be between 1 and 300 seconds. Default interval is 10 sec.
- *retry* - Retry-count of ping/icmp to the target IP. Number of entries should be between 1 and 10. Default retry value is 3

Modes

Target IP configuration mode

Examples

```
kvm-x86-64(config-dti-tracker)#  
  target-ip  IPv4 Target IP address to check the Internet reachability  
kvm-x86-64(config-dti-tracker)# target-ip  
  IPV4  A.B.C.D  
kvm-x86-64(config-dti-tracker)# target-ip 1.1.1.1  
kvm-x86-64(config-dti-tracker-1.1.1.1)#  
  interval  Interval between ICMP packets  
kvm-x86-64(config-dti-tracker-1.1.1.1)# interval  
  (1-300)  interval should be between 1 and 300 seconds.Default interval is 10 sec  
kvm-x86-64(config-dti-tracker-1.1.1.1)# interval 14  
kvm-x86-64(config-dti-tracker-1.1.1.1)# retry  
  (1-10)  Number of entries should be between 1 and 10.Default retry value is 3  
kvm-x86-64(config-dti-tracker-1.1.1.1)# retry 4
```



Fabric Extend Commands

[fabric-extend](#) on page 66

[show lldp interface](#) on page 68

fabric-extend

Use the **fabric-extend** command to configure LLDP settings on the LAN port of the SD-WAN appliance.

Syntax

fabric-extend

Command Default

Fabric Extend is disabled by default.

Parameters

- **advertise-fabric-ip** *<A.B.C.D/M>* - This IP address is included as an entry in the LLDP Organization Defined TLV Subtype 5. The Fabric Engine on the peer side learns this IP address and assigns it to its receiving interface.
- **mtu** - Maximum Transmission Unit (MTU) is encoded in LLDP Organization Defined TLV Subtype 5. When an LLDP PDU is received, the Fabric on the peer side applies this MTU to its port.
If the user does not configure an MTU, the default value of 1500 is used.
- **remote-neighbor** - Use this command to configure a remote neighbor for fabric extension.
 - **ip** *<A.B.C.D>*: Specifies the remote neighbor's IP address.
 - **isis-metric** *<value>*: Sets the ISIS metric for the remote neighbor.

Modes

Interface LLDP fabric-extend mode

Example

```
(config-if-eth-0/1-ldp)# fabric-extend
(config-if-eth-0/1-ldp-fe)# advertise-fabric-ip 10.1.1.1/24
(config-if-eth-0/1-ldp-fe)# mtu 1280
(config-if-eth-0/1-ldp-fe)# remote-neighbor hub1
(config-if-eth-0/1-ldp-fe-hub1)# ip 10.1.1.2
(config-if-eth-0/1-ldp-fe-hub1)# isis-metric 12000
```

show lldp interface

Use the **show lldp interface** command to view the LLDP information for the specified interface.

Syntax

```
show lldp interface ethernet 0/1
```

Parameters

- **ethernet** - Use this command to display LLDP information of ethernet interface.
- *<IFNAME>* - Interface name in slot/port format,
Example: 0/1, Range Example: 0/1-3,5,7-9

Modes

exec mode

Examples

```
# show lldp interface ethernet 0/1

LLDP Interface Information:
-----

Interface: ethernet 0/1
Status: Enabled
Transmit: On
Receive: On
Static Mgmtip: Disabled
Suppressed Tlvs:
Fabric Extend
  MTU: 2000
Advertise Fabric IP: 172.16.0.42/29
  Remote Neighbor: Appl-R1-Spoke2
    Status: UP
    IP Address: 172.16.0.10
    ISIS Metric: 20000
  Remote Neighbor: Appl-DC-Core2
    Status: UP
    IP Address: 172.16.0.50
    ISIS Metric: 20000
  Remote Neighbor: Appl-R1-Spoke3
    Status: UP
    IP Address: 172.16.0.18
    ISIS Metric: 20000
  Remote Neighbor: Appl-R1-Spoke1
    Status: UP
    IP Address: 172.16.0.58
    ISIS Metric: 20000
  Remote Neighbor: Appl-DC-Core1
    Status: UP
    IP Address: 172.16.0.2
    ISIS Metric: 20000
```

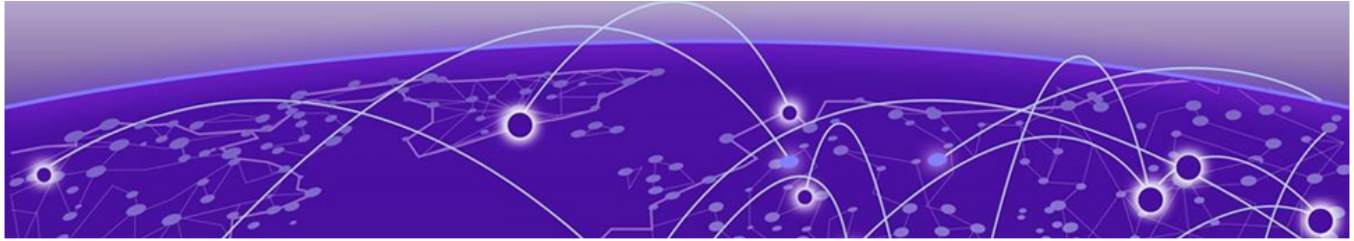
```
# show lldp interface ethernet all
LLDP Interface Information:
-----

Interface: ethernet 0/1
Status: Enabled
Transmit: On
Receive: On
Static Mgmtip: Disabled
Suppressed Tlvs:
Fabric Extend
  MTU: 2000
Advertise Fabric IP: 172.16.0.42/29
  Remote Neighbor: Appl-R1-Spoke2
    Status: UP
    IP Address: 172.16.0.10
    ISIS Metric: 20000
  Remote Neighbor: Appl-DC-Core2
    Status: UP
    IP Address: 172.16.0.50
    ISIS Metric: 20000
  Remote Neighbor: Appl-R1-Spoke3
    Status: UP
    IP Address: 172.16.0.18
    ISIS Metric: 20000
  Remote Neighbor: Appl-R1-Spoke1
    Status: UP
    IP Address: 172.16.0.58
    ISIS Metric: 20000
  Remote Neighbor: Appl-DC-Core1
    Status: UP
    IP Address: 172.16.0.2
    ISIS Metric: 20000

Interface: ethernet 0/2
Status: Enabled
Transmit: On
Receive: On
Static Mgmtip: Disabled
Suppressed Tlvs:

Interface: ethernet 0/4
Status: Enabled
Transmit: On
Receive: On
Static Mgmtip: Disabled
Suppressed Tlvs:

Interface: ethernet 0/5
Status: Enabled
Transmit: On
Receive: On
Static Mgmtip: Disabled
Suppressed Tlvs:
```



IPsec Commands

[Ipsec](#) on page 71
[ipsec-profile](#) on page 73
[peer](#) on page 75
[sa-policy](#) on page 76
[security-policy](#) on page 78
[traffic-selector](#) on page 80
[show ipsec peer](#) on page 82

Ipsec

Use the **ipsec** command to switch from the global configuration mode to ipsec configuration mode.

Syntax

ipsec

Command Default

IPsec is disabled by default.

Parameters

This command has no keywords or variables.

Modes

IPsec configuration mode.

Examples

Configuration

```
# configure terminal
(config)# ipsec
(config-ipsec)#
```

Running Configuration Output

```
kvm-x86-64(config-ipsec)# do show running-config ipsec
ipsec
  ike-policy test
    encryption aes128_cbc
    integrity hmac_md5
    dh-group dh_group_1
    rekeytime 10000
  !
  sa-policy test
    encryption aes128_cbc
    integrity hmac_md5
    dh-group dh_group_1
    rekeytime 10000
  !
  ipsec-profile test
    ike-policy test
    sa-policy test
    role initiator
    shared-key-hashed
2I3N9QamNZGYE0Qr5Ka+RdMSPxy1tvOeA+EI3AF0ekxg4WXVthCiIcAmbjyS0k1LZrNitLsZUNzpln9E+FetEw==
  !
```

```
peer test
  ipsec-profile test
  primary-destination 10.10.10.2
  local-identity router1
  remote-identity router2
  source-interface ethernet 0/2
  security-policy test
!
security-policy test
  priority 200
  action protect
  sa-policy test
  local-traffic-selector lts
  remote-traffic-selector rts
!
traffic-selector lts
  traffic-list any 20.20.1.0/24
!
!
traffic-selector rts
  traffic-list any 30.30.1.0/24
!
!
!
```


ipsec-profile

Use the **ipsec-profile** command to create an IPsec profile.

Syntax

```
ipsec-profile <name>
```

Command Default

No IPsec profiles are configured by default.

Parameters

- **ike-policy** - Map ike-policy with IPsec profile.
- **role** <initiator|responder> - Define the role of the host machine for IPsec profile.
- **sa-policy** <name> - Map sa-policy with IPsec profile.
- **shared-key** <value> - Configure the shared-key for IPsec profile.

Modes

ipsec-profile configuration mode

Examples

Configuration

```
kvm-x86-64(config-ipsec)# ipsec-profile test
kvm-x86-64(config-ipsec-ipsec-profile-test)#
kvm-x86-64(config-ipsec)# ipsec-profile ip
kvm-x86-64(config-ipsec-ipsec-profile-ip)# ike-policy test
kvm-x86-64(config-ipsec-ipsec-profile-ip)#
role          IPSEC role defines the role of the host machine. Default connection type is
responder
kvm-x86-64(config-ipsec-ipsec-profile-ip)# role initiator
kvm-x86-64(config-ipsec-ipsec-profile-ip)#
kvm-x86-64(config-ipsec-ipsec-profile-ip)# sa-policy test
kvm-x86-64(config-ipsec-ipsec-profile-ip)#
kvm-x86-64(config-ipsec-ipsec-profile-ip)# shared-key mysharedkey
kvm-x86-64(config-ipsec-ipsec-profile-ip)#
```

Running Configuration Output

```
kvm-x86-64(config-ip-security-ike-policy-test)# do show running-config ipsec
ipsec
ike-policy test
    encryption aes128_gcm
```

```
    integrity hmac_md5
    dh-group dh_group_1
    rekeytime 5600
!
sa-policy test
  encryption aes128_gcm
  integrity hmac_md5
  dh-group dh_group_1
  rekeytime 5600
!
ipsec-profile test
  ike-policy test
  sa-policy test
  role initiator
  shared-key-hashed
v+t43b0va4hWFsRw13BN8w7QfLXXYr1MKsbuYpNerT9+nvNYYCk0GEsVJC1OOYFWf5CLPbuXLT9C1+PP5sZDCw==
!
```

peer

Use the **peer** command to create an ipsec peer.

Syntax

peer <name>

Command Default

No peers are configured by default.

Parameters

- **ipsec-profile** <name> - Map ipsec profile with peer.
- **local-identity** <identity> - Create a local-identity for an IKE peer.
- **primary-destination** <A.B.C.D> - Map primary-destination with peer.
- **remote-identity** <identity> - Create a remote-identity for a remote IKE peer.
- **secondary-destination** <A.B.C.D> - Map secondary-destination with peer.
- **security-policy** <name> - Map security-policy with peer.
- **source-interface ethernet** <IFNAME> - Specifies the source interface for the IPsec tunnel type.

Modes

IPsec profile configuration mode

Examples

```
kvm-x86-64(config-ipsec)# peer test
kvm-x86-64(config-ipsec-peer-test)#
kvm-x86-64(config-ipsec-peer-test)# ipsec-profile test
kvm-x86-64(config-ipsec-peer-test)# local-identity router1
kvm-x86-64(config-ipsec-peer-test)#
kvm-x86-64(config-ipsec-peer-test)# primary-destination 10.10.10.2
kvm-x86-64(config-ipsec)# peer test
kvm-x86-64(config-ipsec-peer-test)# remote-identity router2
kvm-x86-64(config-ipsec-peer-test)#
kvm-x86-64(config-ipsec-peer-test)# security-policy test
kvm-x86-64(config-ipsec-peer-test)#
kvm-x86-64(config-ipsec-peer-test)# source-interface
    ethernet Peer destination ethernet port
kvm-x86-64(config-ipsec-peer-test)# source-interface ethernet 0/1
kvm-x86-64(config-ipsec-peer-test)# secondary-destination A.B.C.D IP Address config
```

sa-policy

Use the **sa-policy** command to create a IPsec Security Association (SA) policy.

Syntax

```
sa-policy <name>
```

Command Default

No SA policy is configured by default.

Parameters

- **dh-group** <value> - DH group in the IKE policy.
- **encryption** <value> - ESP encryption algorithm for the SA policy.
- **integrity** <value> - ESP integrity algorithm for the SA policy.
- **sa-rekeytime** <time> - Rekey interval (in seconds) for each child SA.

Modes

SA policy configuration mode.

Examples

Configuration

```
kvm-x86-64(config-ipsec)# sa-policy test
kvm-x86-64(config-ipsec-sa-policy-test)#

kvm-x86-64(config-ipsec-ike-policy-test)# dh-group dh_group_1
kvm-x86-64(config-ipsec-ike-policy-test)#
kvm-x86-64(config-ipsec-sa-policy-test)# encryption aes_128_cbc
kvm-x86-64(config-ipsec-ike-policy-test)#
kvm-x86-64(config-ipsec-sa-policy-test)# integrity md5
kvm-x86-64(config-ipsec-sa-policy-test)#
kvm-x86-64(config-ipsec-sa-policy-test)# rekeytime 5600
```

Running Configuration Output

```
kvm-x86-64(config-ip-security-ike-policy-test)# do show running-config ipsec
ipsec
  ike-policy test
    encryption aes128_gcm
    integrity hmac_md5
    dh-group dh_group_1
    rekeytime 5600
  !
  sa-policy test
```

```
    encryption aes128_gcm
    integrity hmac_md5
    dh-group dh_group_1
    rekeytime 5600
!
ipsec-profile test
    ike-policy test
    sa-policy test
    role initiator
    shared-key-hashed
v+t43b0va4hWFsRw13BN8w7QfLXXYr1MKsbuYpNerT9+nvNYYCk0GEsVJC1OOYFWf5CLPbuXLT9C1+PP5sZDCw==
!
```

security-policy

Use the **security-policy** command to create an ipsec security policy.

Syntax

security-policy <name>

Command Default

No security policies are configured by default.

Parameters

- **action** <protect | bypass | discard> - Action with security policy.
- **local-traffic-selector** <name> - Local traffic selector with security policy.
- **priority** - Priority with security policy.
- **remote-traffic-selector** <name> - Remote traffic selector with security policy.
- **sa-policy** <name> - SA policy with security policy.

Modes

Security policy configuration mode

Examples

Configuration

```
kvm-x86-64 (config-ipsec)# security-policy test
kvm-x86-64 (config-ipsec-security-policy-test)#
kvm-x86-64 (config-ipsec-security-policy-test)# action protect
kvm-x86-64 (config-ipsec-security-policy-test)#
kvm-x86-64 (config-ipsec-security-policy-test)# local-traffic-selector lts
kvm-x86-64 (config-ipsec-security-policy-test)#

kvm-x86-64 (config-ipsec-security-policy-test)# priority 200
kvm-x86-64 (config-ipsec-security-policy-test)#
kvm-x86-64 (config-ipsec-security-policy-test)# remote-traffic-selector rts
kvm-x86-64 (config-ipsec-security-policy-test)#
kvm-x86-64 (config-ipsec-security-policy-test)# sa-policy test
kvm-x86-64 (config-ipsec-security-policy-test)#
```

Running Configuration Output

```
kvm-x86-64 (config-ipsec)# do show running-config ipsec
ipsec
  ike-policy test
  encryption aes128_cbc
  integrity hmac_md5
  dh-group dh_group_1
  rekeytime 10000
!
```

```
sa-policy test
  encryption aes128_cbc
  integrity hmac_md5
  dh-group dh_group_1
  rekeytime 10000
!
ipsec-profile test
  ike-policy test
  sa-policy test
  role initiator
  shared-key-hashed
2I3N9QamNZGYE0Qr5Ka+RdMSPxy1tvOeA+EI3AF0ekxg4WXVthCiIcAmbjyS0k1LZrNitLsZUNzpln9E+FetEw==
!
peer test
  ipsec-profile test
  primary-destination 10.10.10.2
  local-identity router1
  remote-identity router2
  source-interface ethernet 0/2
  security-policy test
!
security-policy test
  priority 200
  action protect
  sa-policy test
  local-traffic-selector lts
  remote-traffic-selector rts
!
traffic-selector lts
  traffic-list any 20.20.1.0/24
!
!
traffic-selector rts
  traffic-list any 30.30.1.0/24
!
!
!
```

traffic-selector

Use the **traffic-selector** command to switch from configuration IPsec to traffic selector configuration mode.

Syntax

traffic-selector <name>

Command Default

No traffic selectors are configured by default.

Parameters

- **traffic-list** <protocol> [ip-prefix] - Traffic list with the traffic selector.
- *l4-port* (0-65535) - l4-port with the traffic list.
- *l4-port-end* (0-65535) - l4-port with the traffic list.

Modes

Traffic selector configuration mode

Examples

Configuration

```
kvm-x86-64(config-ipsec)#traffic-selector test
kvm-x86-64(config-ipsec-traffic-selector-test)#
kvm-x86-64(config-ipsec)# traffic-selector lts
kvm-x86-64(config-ipsec-traffic-selector-lts)# traffic-list udp 10.10.10.20/24
kvm-x86-64(config-ipsec-traffic-selector-lts-traffic-list-udp-10.10.10.20/24)#
kvm-x86-64(config-ipsec)# traffic-selector lts
kvm-x86-64(config-ipsec-traffic-selector-lts)# traffic-list udp 10.10.10.20/24
kvm-x86-64(config-ipsec-traffic-selector-lts-traffic-list-udp-10.10.10.20/24)# l4-portend
200
```

Running Configuration Output

```
kvm-x86-64(config-ipsec)# do show running-config ipsec
ipsec
  ike-policy test
    encryption aes128_cbc
    integrity hmac_md5
    dh-group dh_group_1
    rekeytime 10000
  !
  sa-policy test
    encryption aes128_cbc
    integrity hmac_md5
    dh-group dh_group_1
    rekeytime 10000
  !
```



```
ipsec-profile test
  ike-policy test
  sa-policy test
  role initiator
  shared-key-hashed
2I3N9QamNZGYE0Qr5Ka+RdMSPxy1tvOeA+EI3AF0ekxg4WXVthCiIcAmbjyS0k1LZrNitLsZUNzpln9E+FetEw==
!
peer test
  ipsec-profile test
  primary-destination 10.10.10.2
  local-identity router1
  remote-identity router2
  source-interface ethernet 0/2
  security-policy test
!
security-policy test
  priority 200
  action protect
  sa-policy test
  local-traffic-selector test
!
traffic-selector test
  traffic-list any 20.20.1.0/24
!
!
```

show ipsec peer

Use the **show ipsec peer** command to display the detailed IPsec information for the specified peer.

Syntax

```
show ipsec peer <all | NAME> [detail]
```

Command Default

No ipsec peers are configured by default.

Parameters

This command has no keywords or variables.

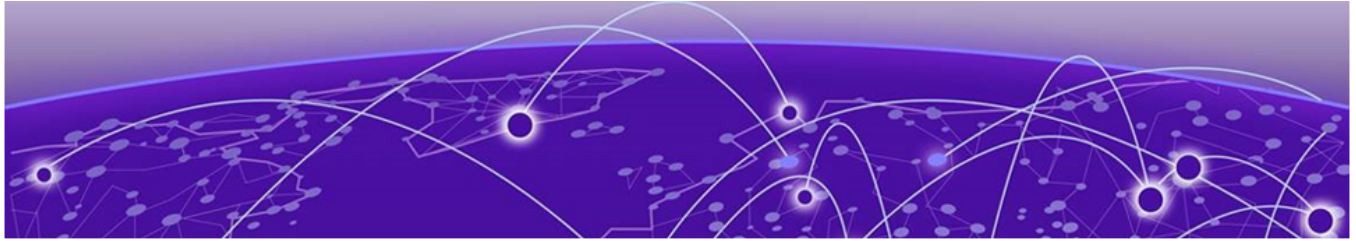
Modes

exec mode

Examples

```
420ax# show ipsec peer all detail
PEER: router2_sdwan
=====
      Source: 10.10.10.1
      Destination: 10.10.10.2
source-interface: ethernet 0/5
  local-identity: router1
  remote-identity: router2
IKE SA:
      IKE State: ESTABLISHED
      Encryption: AES128_CBC
      Integrity: HMAC_MD5
      DH Group: DH_GROUP_1
      NAT Local: false
      NAT Remote: true
      Initiator: true
      Initiator-SPI: baa4003c23f3ab74
      Responder-SPI: 901aab1bda45a015
      Uptime: 2h10m19.398008845s
      Rekey: 28m17.601990001s
Security-Policies:
      security-policy: protect1
      action: PROTECT
priority: 200
Child SA:
      Name: protect1
      SA State: INSTALLED
      local-traffic-selector: 192.168.1.0/24
      remote-traffic-selector: 192.168.2.0/24
      Encryption: AES128_CBC
      Integrity: HMAC_MD5
      DH Group: DH_GROUP_1
      In-SA-SPI: cf538e79
```

```
Out-SA-SPI: c282391e
  Uptime: 2h13m42.398643025s
    Rekey: 22m36.601373375s
  Lifetime: 49m37.601377412s
    Rx Pkts: 1
  Rx Bytes: 132
    Tx Pkts: 1
  Tx Bytes: 108
-----
1 out of 1 Peers are Established
```



IPsec Tunnel Commands

[show counters ike](#) on page 85

[show ipsec tunnel](#) on page 86

[type ipsec](#) on page 87

show counters ike

Use the **show counters ike** command to display the IKE counters for the specified tunnel.

Syntax

```
show counters ike <all | IFNAME>
```

Command Default

Displays all IKE counters.

Parameters

This command has no keywords or variables.

Modes

exec mode

Examples

```
kvm-x86-64# show counters ike t1

Tunnel Name: tunnel t1
    ike-rekey-init: 0
    ike-rekey-resp: 0
        child-rekey: 0
            invalid: 0
                invalid-spi: 0
    ike-init-in-req: 0
    ike-init-in-resp: 0
    ike-init-out-req: 0
    ike-init-out-resp: 0
    ike-auth-in-req: 0
    ike-auth-in-resp: 0
    ike-auth-out-req: 0
    ike-auth-out-resp: 1
    create-child-in-req: 0
    create-child-in-resp: 0
    create-child-out-req: 0
    create-child-out-resp: 0
        info-in-req: 1
        info-in-resp: 2
        info-out-req: 2
        info-out-resp: 1
```

show ipsec tunnel

Use the **show ipsec tunnel** command to display the detailed ipsec information for the specified tunnel.

Syntax

```
show ipsec tunnel <all | IFNAME> [detail]
```

Command Default

No IPsec tunnel is configured by default.

Parameters

This command has no keywords or variables.

Modes

exec mode

Examples

```
kvm-x86-64# show ipsec tunnel all detail
TUNNEL: t3
=====
      Destination: 192.168.10.1
      Source: 192.168.10.2
Source Interface: ethernet 0/3
  IPSEC Profile: tnl3
  Local Identity: t2resp
  Remote Identity: t2init
      IP Address: 10.254.0.7/31
IKE SA:
      IKE State: ESTABLISHED
      Encryption: AES128_GCM
      DH Group: DH_GROUP_19
      Remote: true
Initiator-SPI: 1ad2de58585777e
Responder-SPI: 344d9d80fd2be31c
      Uptime: 1h9m24.812555146s
      Rekey: 22h42m32.187447074s
Child SA:
      SA State: INSTALLED
      Encryption: AES128_GCM
      DH Group: DH_GROUP_19
      In-SA-SPI: cfd90264
      Out-SA-SPI: cab2bd16
      Uptime: 1h29m50.812520296s
      Rekey: 20h9m36.187474408s
      Lifetime: 24h54m9.187477928s
      Rx Pkts: 5
      Rx Bytes: 620
      Tx Pkts: 5
      Tx Bytes: 760
```

type ipsec

Use the **type ipsec** command to configure type as ipsec for interface tunnel.

Syntax

type ipsec

Command Default

Displays the IPsec type configuration.

Parameters

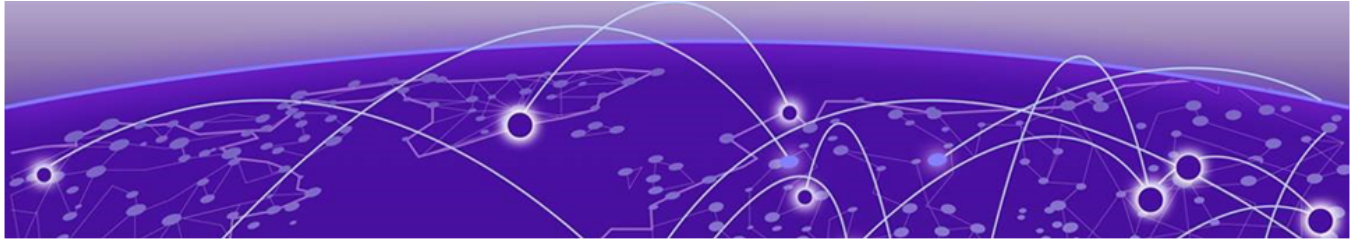
- **ipsec-profile** *<name>* - Map ipsec profile with ipsec tunnel.
- **destination** *<A.B.C.D | X:X::X:X>* - Set the tunnel destination. This can be either IPv4 address or IPv6 address.
- **local-identity** *<identity>* - Create a local identity for a local IKE peer.
- **reassemble** - Enable or disable full reassembly feature on IPSEC tunnel.
- **remote-identity** - Create a remote identity for a remote IKE peer.
- **source-interface ethernet** - Specify the ipsec tunnel type source interface.
- **ip address** *<A.B.C.D/M>* - Set the IP address for the tunnel interface.

Modes

IPSEC tunnel configuration mode

Examples

```
kvm-x86-64(config-tunnel-rtest)#  
kvm-x86-64(config-tunnel-rtest)# type ipsec  
kvm-x86-64(config-tunnel-ipsec)#  
kvm-x86-64(config-tunnel-ipsec)# ipsec-profile test  
kvm-x86-64(config-tunnel-ipsec)#  
kvm-x86-64(config-tunnel-ipsec)# destination 20.20.10.30  
  
kvm-x86-64(config-tunnel-ipsec)#  
kvm-x86-64(config-tunnel-ipsec)# local-identity t1init  
kvm-x86-64(config-tunnel-ipsec)#  
kvm-x86-64(config-tunnel-ipsec)# reassembly  
kvm-x86-64(config-tunnel-ipsec)#  
kvm-x86-64(config-tunnel-ipsec)# remote-identity t1resp  
kvm-x86-64(config-tunnel-ipsec)#  
kvm-x86-64(config-tunnel-ipsec)# source-interface ethernet 0/2  
kvm-x86-64(config-tunnel-ipsec)#  
kvm-x86-64(config-tunnel-ipsec)# ip address
```



NAT Commands

[nat](#) on page 88

nat

Use the **nat** command to switch from global configuration to nat configuration mode.

Syntax

nat

Command Default

By default NAT is enabled on LAN interfaces with direction as inside.

Parameters

- **Interface** < *IFNAME*> - Create a NAT interface.
- **Direction** - Specify whether the NAT interface direction is inbound or outbound.

Modes

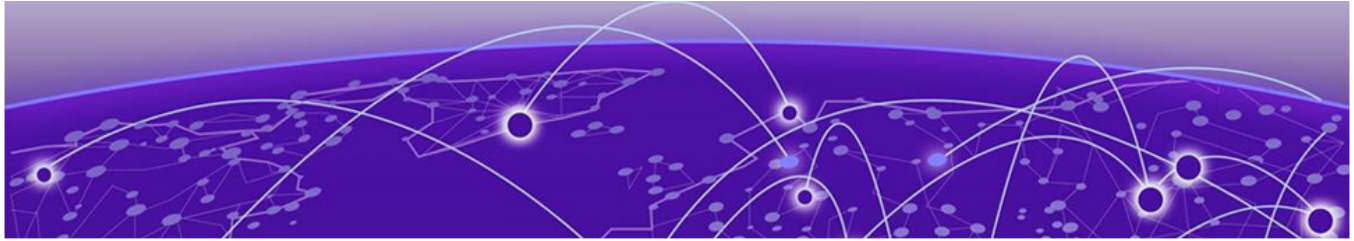
Nat configuration mode

Example

```
# configure terminal
(config)# nat
(config-nat)#
kvm-x86-64(config-nat)# interface ethernet 0/5
kvm-x86-64(config-nat-eth-0/5)#
kvm-x86-64(config-nat-eth-0/5)# direction outside
kvm-x86-64(config-nat-eth-0/5)#
```


The following example displays the running configuration

```
Spoke2-BN-IPE1# show running-config nat
nat
  interface ethernet 0/5
    direction outside
  !
  interface ethernet 0/1
    direction inside
  !
  interface ethernet 0/2
    direction outside
  !
  interface ethernet 0/3
    direction inside
  !
  interface ethernet 0/4
    direction outside
  !
!
Spoke2-BN-IPE1#
```



TCP MSS Clamping Commands

[TCP MSS Clamping](#) on page 90

TCP MSS Clamping

Use the **mss-clamping** command to switch from the global configuration to MSS clamping configuration mode. TCP MSS Clamping specifies the maximum segment size (MSS) for TCP packets to prevent fragmentation in networks with varying MTU sizes. This feature ensures reliable transmission by adjusting the MSS value in TCP SYN packets during connection setup.

Syntax

```
mss-clamping
```

Command Default

No mss-clamping is configured by default.

Parameters

Use the following commands to configure MSS clamping settings:

- **interface** *<IFNAME>* - Creates an MSS clamping interface and allows further configuration for the interface.
- **enable** - Enables MSS clamping on the specified interface.
- **tcp-mss** *<Value>* - Sets the TCP MSS clamp size for the interface.

Modes

Interface configuration mode

Examples

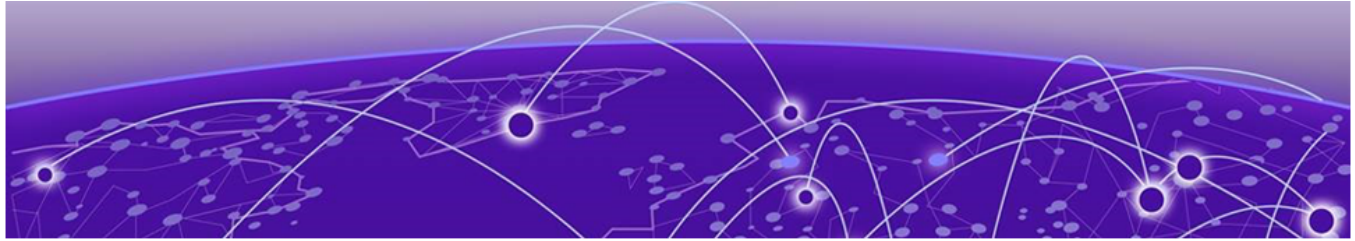
The following example configures MSS clamping on an interface.

```
# configure terminal
(config)# mss-clamping
```

```
(config-mss-clamping)#  
kvm-x86-64(config-mss-clamping)# interface ethernet 0/5  
kvm-x86-64(config-mss-clamping-eth-0/5)#  
kvm-x86-64(config-mss-clamping-eth-0/5)# enable  
kvm-x86-64(config-mss-clamping-eth-0/5)#  
kvm-x86-64(config-mss-clamping-eth-0/5)# tcp-mss 1280
```

The following output displays the MSS clamping configuration and its protocol settings:

```
kvm-x86-64(config)# do show running-config mss-clamping  
mss-clamping  
  interface ethernet 0/5  
    enable  
    tcp-mss 1280  
  !  
!  
kvm-x86-64(config)#
```



ZTP Commands

[ZTP](#) on page 92

ZTP

Use the **ztp** command to create a sub-mode for configuring ZTP parameters. The ZTP command is available at below mode.

```
SPOKE1-IPE2# con t
SPOKE1-IPE2(config)# system
SPOKE1-IPE2(config-system)# ztp
SPOKE1-IPE2(config-system-ztp)#
SPOKE1-IPE2(config-system-ztp)# pwd
Current submode path:
    system \ zt
```

Syntax

ztp

Command Default

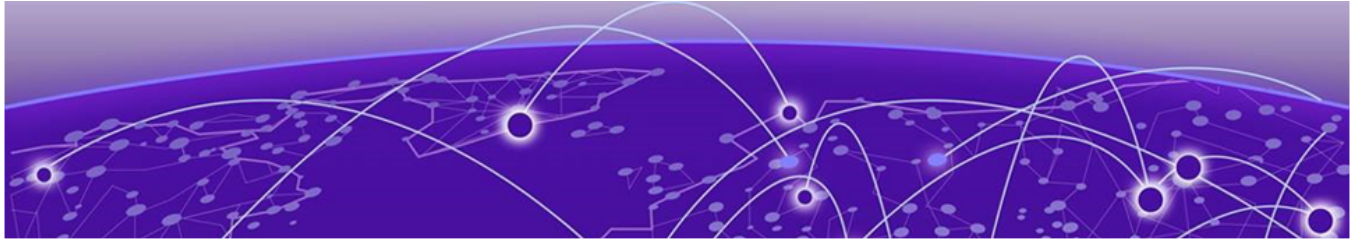
Displays the current Zero-Touch Provisioning (ZTP) status.

Parameters

- **url** <name> - Specify the complete ZTP server URL, including the port and schema.
- **show ztp status** - Display the ZTP process status, indicating whether it is completed or in progress. It also provides details such as the org-id, owner-id, communicator URL, shows inlets-endpoint and certificates received during the ZTP process with the configured ZTP server.

Examples

```
IPE1-BR4# show ztp status
ztpServerUrl:https://ztp01.extremecloudiq.com:443/api
status:completed
owner-id:508931
org-id:0
communicator:https://jp-sdwan-comm.extremecloudiq.com:9670/api
inlets-endpoint:wss://sdwan-jp-inlets-endpoint.extremecloudiq.com:443
```



Config Backup Commands

[day1-configuration start](#) on page 94

[day1-configuration stop](#) on page 95

[rm day1-config](#) on page 96

[show day1-config](#) on page 97

[day1-config save](#) on page 99

day1-configuration start

Use the **day1-configuration start** command to clear existing configuration and prepare the device for Day-1 configuration. This command sets an internal marker and reboots the device to restore default configuration.

Syntax

day1-configuration start

Command Default

No Day-1 configuration mode is active by default

Parameters

This command has no keywords or variables

Modes

EXEC mode

Usage Guidelines

Use this command to initiate Day-1 configuration. The device will reboot to restore default configuration. After reboot, make the required configurations and save them using `day1-configuration stop` to complete the process.

If Day-1 configuration creation is already in progress, the system will display a message to `day1-configuration stop` run to complete it first.

A confirmation prompt will appear before the reboot. Entering `n` aborts the operation.

Examples

The following example initiates Day-1 configuration with user confirmation:

```
MGMT-SVC-420ax# day1-configuration start
WARN: system will be rebooted to restore default configuration!
Make required configurations after reboot and save using 'day1-configuration stop'.
Do you want to continue? [y/n]: y
```

The following example shows the operation aborted by the user:

```
MGMT-SVC-420ax# day1-configuration start
WARN: system will be rebooted to restore default configuration!
Make required configurations after reboot and save using 'day1-configuration stop'.
Do you want to continue? [y/n]: n
Day1 configuration start operation aborted by user
```

day1-configuration stop

Use the **day1-configuration stop** command to mark the completion of Day-1 configuration, clear the internal marker, and save the current running configuration as the Day-1 configuration.

Syntax

day1-configuration stop

Command Default

No Day-1 configuration mode is active by default

Parameters

This command has no keywords or variables

Modes

EXEC mode

Usage Guidelines

Use this command after the device has rebooted from a day1-configuration start command and the required configurations have been applied. This command marks the completion of the Day-1 configuration process, clears the marker, and saves the Day-1 configuration.

If Day-1 configuration creation is not in progress, the system will display an error message.

This command is available only to users with admin role.

Examples

The following example completes the Day-1 configuration process after reboot:

```
Device# day1-configuration stop
Day1 configuration created successfully
```

rm day1-config

Use the **rm day1-config** command to delete the Day-1 backup configuration file from the device.

Syntax

```
rm day1-config
```

Command Default

NA

Parameters

This command has no keywords or variables

Modes

EXEC mode

Usage Guidelines

Use this command to delete the Day-1 backup configuration file. Once deleted, the device will no longer have a stored Day-1 configuration to restore from.

If the Day-1 configuration file does not exist on the device, an error message is displayed.

This command is available only to users with admin role.

Examples

The following example lists files before and after removing the Day-1 configuration:

```
MGMT-SVC-420ax# ls
config-file :
-rw-r--r--  31800  2026-02-26 11:42:26  day1config
-rw-r--r--  8728   2026-02-26 11:42:40  comm.day1config.tgz
tech-support :
firmware :
coredumps :
MGMT-SVC-420ax# rm day1-config
Warning: Day1-config will be deleted.
MGMT-SVC-420ax# ls
config-file :
tech-support :
firmware :
coredumps :
```


show day1-config

Use the **show day1-config** command to display the content of the Day-1 configuration file.

Syntax

```
show day1-config <running>
```

Command Default

NA

Parameters

<running> - Display day1-config renderable from the running-config instead of the saved file.

Modes

EXEC mode

Usage Guidelines

Use this command to view the stored Day-1 configuration. When the optional running parameter is specified, it displays the day1-config renderable from the current running-config instead of the saved file.

If the Day-1 configuration file does not exist on the device, an error message is displayed.

This command is available only to users with admin role.

Examples

The following example displays the saved Day-1 configuration:

```
MGMT-SVC-420ax# show day1-config
system
  grub
    username root password-hashed
  grub.pbkdf2.sha512.10000.AA8C315154428264D5474C322A7F187F120BFB57EDBACB78CBC130B9915E0E9EC
  CB615D045F3CD05C39DF7767C7645A279A195928ABD9BE5422E096563435D0C.AFBFB72FC886A16C850D22181
  913B7E9A100EA71A45583EABA0E7C8A41904A3B553B42363AFABB919621093C1B46AA0E54133F47E60729C2426
  49F2B8074880
  !
  aaa
    authentication
      admin-user admin password-hashed
$6$D5Bb9D3t8sKdxflb$rZIwfTkhh33dEvbiMSyqff.zAk.Z2xSYz3dmaA.GQooCbBeDU4Iy0CXZMaXwflyTpKlQ.M
GHmUz.F1/IjdHa..
  !
```

```
!  
grpc-server DEFAULT  
ssh-server DEFAULT  
  key rsa 4096  
  vrf mgmt-vrf  
  enable  
!  
!  
interface management 0  
  ipv4 address dhcp  
  no shutdown  
!  
vrf mgmt-vrf  
  member management 0  
!
```

The following example displays the Day-1 configuration from running-config:

```
MGMT-SVC-420ax# show day1-config running
```

day1-config save

Use the **day1-config save** command to save the Day-1 related configuration from the running configuration to a file.

Syntax

day1-config save

Command Default

No Day-1 configuration mode is active by default

Parameters

This command has no keywords or variables

Modes

EXEC mode

Usage Guidelines

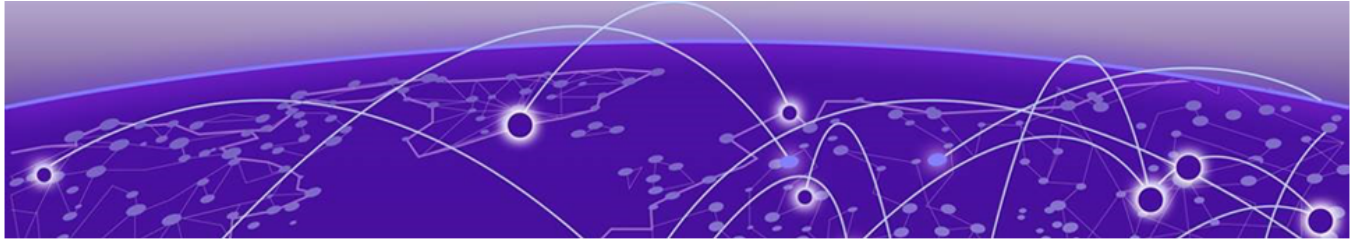
Use this command to capture the current Day-1 related configuration from the running configuration and save it to a file. This is useful for preserving Day-1 configuration after making changes, without requiring a full day1-configuration stop workflow.

This command is available only to users with admin role.

Examples

The following example saves the Day-1 configuration from running config to file:

```
Device# day1-config save
Device#
```



Config Rollback Commands

[config rollback](#) on page 100

config rollback

Use the **config-rollback** command to enter configuration rollback settings mode. This feature provides automatic rollback of configuration changes if connectivity is lost after a configuration change.

Syntax

config-rollback

Command Default

Configuration rollback is not configured by default.

Parameters

The following sub-commands are available within configuration rollback mode:

auto-mode - Enters automatic configuration rollback mode for enabling and configuring rollback parameters.

Within **auto-mode**, the following sub-commands are available:

- **enable** - Enables or disables the auto configuration rollback feature. Range: true or false.
- **monitor-period** *<INTERVAL>* - Interval in seconds at which polling for connection status is performed. Range: Minimum 60 seconds.

Modes

Entered from: Global configuration **config**

Enters into: Configuration rollback mode **config-rollback**

Usage Guidelines

Use this command to enter configuration rollback mode, and configure automatic rollback behavior. The auto-mode sub-command enables automatic rollback and defines the monitoring interval for connectivity checks.

This command is available only to users with admin role.

Examples

The following example enters configuration rollback mode:

```
device# configure terminal
device(config)# config-rollback
device(config-rollback)#
```

The following example enables auto-mode and configures the monitor period:

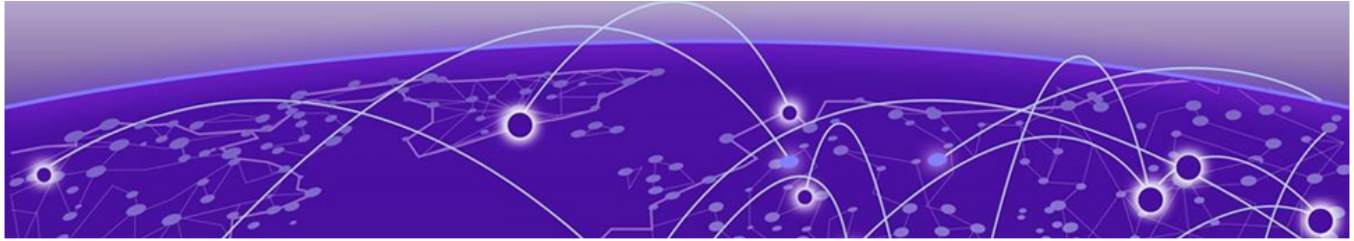
```
device# configure terminal
device(config)# config-rollback
device(config-rollback)# auto-mode
device(config-rollback-auto-mode)# enable
device(config-rollback-auto-mode)# monitor-period 300
device(config-rollback-auto-mode)#
```

The following example displays the error message:

```
device(config-rollback-auto-mode)# monitor-period 30
%Error: monitor-period must be at least 60 seconds
```

The following example displays the running configuration:

```
device(config-rollback-auto-mode)# do show running-config config-rollback
config-rollback
  auto-mode
    enable true
    monitor-period 62
  !
!
```



Interface Cellular Commands

[interface cellular](#) on page 102
[show interface cellular](#) on page 104
[show sysinfo modem health](#) on page 107
[show sysinfo modem status](#) on page 109

interface cellular

Use the **interface cellular** command to enter cellular interface configuration mode. This command changes the config mode to the cellular interface configuration mode where interface-specific parameters can be configured.

Syntax

```
interface cellular IFNAME
```

Command Default

NA

Parameters

IFNAME - Interface name in slot/port format. Valid value: 0

Use this command to enter cellular interface configuration mode. Once in this mode, the following sub-commands are available:

- **ip** - The Internet Protocol information
- **ipv4** - The Internet Protocol version 4 (IPv4) information
- **ipv6** - The Internet Protocol version 6 (IPv6) information
- **mtu** - MTU value
- **preemptive-disconnect** - Configure preemptive disconnect
- **shutdown** - Shut down the interface
- **sim-reset-cycle** - Configure SIM reset cycle
- **sim-reset-time** - Configure SIM reset time and timezone

Modes

Entered from: Global configuration **config**

Enters into: Cellular interface configuration **config-if-cell**-<*IFNAME*>

Usage Guidelines

This command is allowed in config mode only.

This command is available only to users with admin role.

The **no** form of this command is not supported.

Examples

The following example enters cellular interface configuration mode for port 0:

```
40axv2(config)# interface cellular 0
40axv2(config-if-cell-0)#
```

The following example displays the running configuration for cellular interface 0:

```
40axv2# show running-config interface cellular 0
interface cellular 0
  ipv6 address auto-config
  no shutdown
!
```

show interface cellular

Use the **show interface cellular** command to display the details of a cellular interface, including admin/operational state, counters, and rate information.

Syntax

```
show interface cellular IFNAME
```

Command Default

NA

Parameters

IFNAME - Interface name in slot/port format. Valid value: 0

Modes

EXEC mode

Usage Guidelines

Use this command to display detailed information about the cellular interface including admin state, operational state, MTU, MAC address, speed, FEC mode, carrier transitions, input/output packet counters, and rate information.

For SD-WAN platforms, FCS/CRC error information is not displayed as part of this command.

Examples

The following example displays the cellular interface details:

```
40axv2# show interface brief
Flags:  M - Redundant Management  P - Performance-Path
Number of interfaces 7
Port      Mtu      Admin-State Oper-State Speed   Ifindex  Description
-----
Cell 0    2048     UP          UP       1G      0x61000000 Cellular 0
Eth 0/1   2048     UP          DOWN     1G      0x1000020 Ethernet 0/1
Eth 0/2   2048     UP          UP       1G      0x1000040 Ethernet 0/2
Eth 0/3   2048     DOWN       DOWN     1G      0x1000060 Ethernet 0/3
Eth 0/4   2048     UP          UP       1G      0x1000080 Ethernet 0/4
Eth 0/5   2048     UP          DOWN     1G      0x10000a0 Ethernet 0/5
Mgmt 0    1514     UP          UP       1G      0x6000001 Management 0

40axv2# show interface cellular 0
cellular 0 Admin state UP, Oper state UP
Interface index is 1627389952 (0x61000000)
Hardware is Cellular (QMI RAW IP)
Description: Cellular 0
Carrier Transitions: 13
```



```

LastClear: 0s
Input:
    Total pkts: 75
    Discard pkts: 0
    Errors pkts: 0
    Octets: 30628
    UCast pkts: 75
Out:
    Total pkts: 96
    Discard pkts: 0
    Errors pkts: 0
    Octets: 14206
    UCast pkts: 96
Rate Info:
    Input: 0.000000 Mbits/sec, 0 pkts/sec
    Output: 0.000000 Mbits/sec, 0 pkts/sec
40axv2# show running-config vrf
vrf wan1vrf
    member ethernet 0/2
vrf wan2vrf
    member ethernet 0/4
vrf wan3vrf
    member ethernet 0/5
vrf wan4vrf
    member cellular 0
vrf mgmt-vrf
    member management 0
    static-route 0.0.0.0/0 10.133.240.1
!
vrf default-vrf
    member ethernet 0/1
!
40axv2# show running-config interface cellular 0
interface cellular 0
    ipv6 address auto-config
    no shutdown
!
40axv2# show vrf brief
VrfName      Vrf ID  V4-Ucast V6-Ucast
=====
wan1vrf      3       Enabled Enabled
wan2vrf      4       Enabled Enabled
wan3vrf      5       Enabled Enabled
wan4vrf      6       Enabled Enabled
mgmt-vrf     1       Enabled Enabled
default-vrf  2       Enabled Enabled
40axv2# show vrf wan4vrf
VrfName: wan4vrf
VrfID: 6
Address family:  IPv4 Unicast  IPv6 Unicast
Interfaces: Count 1
40axv2# show counters interface cellular brief
Packets
Errors      Discards      CRC
Port        rx      tx      tx      rx      tx
=====
Cell 0      75      96      0      0
0            0      0
40axv2# show counters interface cellular 0
Interface Statistics: cellular 0
Carrier Transitions: 13
LastClear: 0s

```

```
Input:
    Total pkts: 75
    Discard pkts: 0
    Errors pkts: 0
    Octets: 30628
    UCast pkts: 75
Out:
    Total pkts: 96
    Discard pkts: 0
    Errors pkts: 0
    Octets: 14206
    UCast pkts: 96
Rate Info:
    Input: 0.000000 Mbits/sec, 0 pkts/sec
    Output: 0.000000 Mbits/sec, 0 pkts/sec
40axv2# clear counters interface cellular 0
40axv2# show counters interface cellular brief
      Packets
Errors          Discards          CRC
Port            rx            tx            rx            tx
=====
Cell 0           0             0             0             0
0                0             0             0             0
```

The following example shows an error when an invalid interface is specified:

```
Device# show interface cellular 1
Error: Invalid interface cellular 1
%Error: validation of cellular port name/format failed
```

show sysinfo modem health

Use the **show sysinfo modem health** command to display detailed LTE modem diagnostic information including device identity, SIM status, network registration, radio signal quality, and APN profile details.

Syntax

```
show sysinfo modem health
```

Command Default

NA

Parameters

This command has no keywords or variables.

Modes

EXEC mode

Usage Guidelines

Use this command to view low-level LTE radio and modem information for troubleshooting connectivity and signal quality issues. The output includes device identity (vendor, product, firmware, IMEI), SIM state (presence, lock, registration, ICCID), network details (operator, RAT, band), signal strength metrics (RSRP, RSRQ, RSSI, SINR, SNR with bar representation), and the active APN profile configuration.

This command is read-only and does not modify any configuration.

When no USB LTE modem is detected, this command may display empty status or indicate that the modem is not present.

Examples

The following example displays modem health information:

```
40axv2# show sysinfo modem health
Modem Health
=====
Device Information:
-----
Vendor ID       : QUALCOMM INCORPORATED
Product ID      : FS040U
Firmware Version : LWDJCO2.1.0_M132
IMEI            : 867826033210022
SIM Information:
-----
SIM Present     : present
SIM Lock        : disabled
```

```
Registration      : registered
ICCID            : 8991000924293681709
```

Network Information:

```
-----
Operator          : airtel
Network Type (RAT) : LTE
Band              : 8
```

Signal Strength:

```
-----
Signal Bars       : (2/5)
RSRP              : -108 dBm (Poor)
RSRQ              : -14 dB
RSSI              : -80 dBm
SINR              : 9 dB
SNR               : 3 dB
```

APN Profile:

```
-----
Profile ID        : 15
Profile Name      : profile15
APN               : airtelgprs.com
PDP Type          : ipv6
PDP Context Number : 15
Username          : N/A
Password          : N/A
Auth Type         : none
No Roaming        : no
APN Disabled      : no
```

show sysinfo modem status

Use the **show sysinfo modem status** command to display the operational and connection status of the LTE modem, including connection state, uptime, and basic network information.

Syntax

```
show sysinfo modem status
```

Command Default

NA

Parameters

This command has no keywords or variables.

Modes

EXEC mode

Usage Guidelines

Use this command to quickly determine whether the LTE session is established, how long the current connection has been active, and basic network details. This is the primary command for verifying LTE operational state.

This command is read-only and does not modify any configuration.

When no USB LTE modem is detected, this command may display empty status or indicate that the modem is not present

Examples

The following example displays modem status when connected:

```
40axv2# show sysinfo modem status
Modem Status
=====
Connection Status:
-----
State           : Connected
Uptime          : 1h 14m 23s
Network:
-----
Operator        : Jio
Network Type    : LTE
```

The following example displays modem status when disconnected:

```
40axv2# show sysinfo modem status
Modem Status
=====
Connection Status:
-----
State           : Disconnected
Uptime          : -
Network:
-----
Operator        : -
Network Type    : -
```

The following example displays modem status when no modem is present:

```
40axv2# show sysinfo modem status
Modem Status
=====
Connection Status:
-----
State           : Not Detected
Uptime          : -
Network:
-----
Operator        : -
Network Type    : -
```