

SonicWall[®] SonicOS 6.5 Enterprise Command Line Interface (E-CLI)

Reference Guide

SONICWALL[®]

| | |
|--|--------------|
| Introduction | 3 |
| Text Conventions | 3 |
| CLI Prompt Specification | 4 |
| Input Data Format Specification | 4 |
| Editing and Completion Features | 4 |
| Command Hierarchy | 5 |
| Passwords | 7 |
| Factory Reset to Defaults | 7 |
| Logging into the SonicOS E-CLI | 7 |
| Configuring the SonicWall Network Security Appliance | 7 |
| Configuring Features using the CLI on a Serial Connection via the Console Port | 8 |
| Configuring Features using the CLI in an SSH Management Session via Ethernet | 9 |
| E-CLI-Supported Features | 10 |
| About SafeMode | 10 |
| Example of Configuring a Site-to-Site VPN Using E-CLI | 10 |
| CLI Access | 11 |
| Configuring a Site-to-Site VPN | 11 |
| Viewing a VPN Configuration | 13 |
| Interfaces | 16 |
| User Interfaces | 16 |
| Advantages of CLI | 16 |
| Using a Terminal Emulator or SSH Client | 17 |
| Configuring New SonicWall Appliances With CLI | 17 |
| Routing & OSPF Configuration | 18 |
| To Configure Routing | 18 |
| To Configure OSPF | 18 |
| To Enter ospfv3 | 19 |
| Advanced Routing with ZebOS CLI | 19 |
| Top Level and System Commands | 20 |
| E-CLI Commands | 21 |
| SonicWall Support | .1665 |
| About This Document | 1666 |

Introduction

The SonicWall® SonicOS 6.5 Enterprise Command Line Interface (E-CLI) provides a concise and powerful way to configure SonicWall network security appliances without using the SonicOS web-based management user interface (UI).

You can use the CLI commands individually on the command line, or in scripts for automating configuration tasks. In addition, with SonicWall E-CLI, you can copy the output of a show command and post it back as a CLI command at the prompt. This feature gives the interface even greater speed and flexibility.

This document contains an introduction to E-CLI and a categorized list of the E-CLI commands for the SonicOSfirmware. Each command is described, and where appropriate, an example of usage is included. Some commands, conventions, and connections are different for different SonicWall appliances.

Topics:

- [Text Conventions](#)
- [CLI Prompt Specification](#)
- [Input Data Format Specification](#)
- [Editing and Completion Features](#)
- [Command Hierarchy](#)
- [Passwords](#)
- [Factory Reset to Defaults](#)
- [Logging into the SonicOS E-CLI](#)
- [Configuring the SonicWall Network Security Appliance](#)
- [Example of Configuring a Site-to-Site VPN Using E-CLI](#)

Text Conventions

Bold text indicates a command executed by interacting with the user interface.

Italic text indicates the first occurrence of a new term, as well as a book title, and also emphasized text. In this command summary, items presented in italics represent user-specified information.

Items within angle brackets ("`<`" "`>`") are required information.

Items within square brackets ("`[]`") are optional information.

Items separated by a "pipe" ("`|`") are options. You can select any of them.

NOTE: Though a command string may be displayed on multiple lines in this guide, it must be entered on a single line, with no carriage returns except at the end of the complete command.

CLI Prompt Specification

A user-selected firewall name, chosen through the SonicOS web UI on the **System > Administration** screen, is subsequently used in the prompts throughout the CLI, rather than a generic product name such as NSA3600 or SM9600.


This allows the administrator to more easily identify which firewall is currently being managed, and to identify which firewalls are used for which departments in a business structure. For example, the administrator might name firewalls with names like Marketing, Tech Pubs, Engineering, and Testing.

The format is:

“currentusername@firewallname”.

If no firewall name is configured, the default is the serial number or MAC address of the device, resulting in a prompt such as:

admin@C0EAE45998CC>

 **NOTE:** This document uses NSA3600 as the configured name of the device, and consequently as the prompt in the examples.

Input Data Format Specification

The table below describes the data formats acceptable for most CLI commands. H represents one or more hexadecimal digit (0-9 and A-F). D represents one or more decimal digit.

Input Data Formats

| Data | Data Format |
|----------------|---|
| MAC Address | HH:HH:HH:HH:HH:HH |
| MAC Address | HHHHHHHHHHHH |
| MAC Address | HH-HH-HH-HH-HH-HH |
| IPv4 Address | d.d.d.d |
| IPv6 Address | HHHH:HHHH:HHHH:HHHH: HHHH:HHHH:HHHH:HHHH |
| Integer Values | D |
| Integer Values | 0xHH |

Editing and Completion Features

You can use individual keys and control-key combinations to assist you with the CLI commands in the SonicOS interface. The table below describes the key and control-key combination functions.

NOTE: Some of the functions may be different on the E-CLI for your appliance.

Key Reference

| Key(s) | Function |
|------------------|---|
| Tab with letters | Completes the word, or gives options if there are several |
| Tab alone | Displays possible commands |

Key Reference

| Key(s) | Function |
|-------------|--|
| ? | Displays possible commands with descriptions |
| Ctrl+A | Moves cursor to the beginning of the command line |
| Ctrl+B | Moves cursor to the previous character |
| Ctrl+C | Exits the Quick Start Wizard at any time |
| Ctrl+E | Moves cursor to the end of the command line |
| Ctrl+F | Moves cursor to the next character |
| Ctrl+K | Erases characters from the cursor to the end of the line |
| Ctrl+N | Displays the next command in the command history |
| Ctrl+P | Displays the previous command in the command history |
| Ctrl+W | Erases the previous word |
| Left Arrow | Moves cursor to the previous character |
| Right Arrow | Moves cursor to the next character |
| Up Arrow | Displays the previous command in the command history |
| Down Arrow | Displays the next command in the command history |

The Tab key can also be used to finish a command if the command is uniquely identified by user input.

```
user@devicename ect. > show lo[TAB]
```

displays as:

```
user@devicename ect. > show logs
```

In addition, commands can be abbreviated, as long as the partial commands are unique. The following text:

```
user@devicename ect. > sho inter
```

is an acceptable abbreviation for, and displays as:

```
user@devicename ect. > show interface <interface name>
```

Command Hierarchy

The CLI allows you to control the hardware and firmware of the appliance through a discreet mode and submode system. The commands for the appliance fit into the logical hierarchy of this mode and submode system.

To configure items in a submode, you must activate the submode by entering a command in the mode above it.

For example, to set the default LAN interface speed or duplex, type:

```
configure
```

```
interface x0
```

```
link-speed auto-negotiate.
```

```
exit/end
```

```
commit
```

E-CLI no longer supports “finish” alone. There must be an explicit “commit” command to make the configuration take effect. It is possible to commit within submode, but this only submits the changes within submode. To commit all of the changes, commit from config mode.

Together with the commit and submode concept, there are two other commands that also depend on the mode. These are “show current-config” and “show pending config.”

Access these commands from:

```
(edit-interface[X0])# show
  current-config      Show current configuration.
  pending-config      Show pending configuration.
```

E.g.

```
config(COEAE45998CC)# interface X0
(edit-interface[X0])# show current-config
  ip-assignment LAN static
    ip 192.168.168.168
    netmask 255.255.255.0
    no gateway
    exit

  comment "Default LAN"
...
(edit-interface[X0])# comment test
(edit-interface[X0])# show pending-config
  ip-assignment LAN static
    exit
  comment test
(edit-interface[X0])# commit
% Applying changes...
% Status returned processing command:
  commit
% Changes made.
(edit-interface[X0])# show current-config
  ip-assignment LAN static
    ip 192.168.168.168
    netmask 255.255.255.0
    no gateway
    exit

  comment test
```

Passwords

The SonicOS CLI currently uses the administrator's password to obtain access to the network. SonicWall network security appliances are shipped with a default password. The user should set a secure password for accessing the appliance and configuring it over a network.

In addition to the full admin user, E-CLI also supports limited/readonly admin/guest.

Factory Reset to Defaults

If, at some point, you are unable to connect to your device over the network, follow the steps below during a serial configuration session to reset the device to factory defaults.

- 1 Go to Configure mode.
- 2 Run "restore-defaults".

 **CAUTION:** The "restore" command erases all the settings on the appliance, leaving it in a factory default state.

Logging into the SonicOS E-CLI


When the connection is established, log into the security appliance:

- 1 At the User Name prompt, enter the Admin username. Only the admin user can login from the CLI. The default Admin username is admin. The user should change the username from the default.
- 2 At the Password prompt, enter the Admin password. The CLI prompt specification is admin@my2600NSA>. The format is user@firewallname.
- 3 When an invalid or mismatched username/password are entered, the system returns to the User Name prompt, and an error message states "CLI administrator login denied due to bad credentials". There is no lockout on the CLI.

Configuring the SonicWall Network Security Appliance

You can configure the SonicWall network security appliance using one of the three methods described below. These descriptions are examples of configurations for accessing the Enterprise Command Line Interface. Your equipment may require a different configuration.

- [Configuring Features using the CLI on a Serial Connection via the Console Port](#)
- [Configuring Features using the CLI in an SSH Management Session via Ethernet](#)
- [E-CLI-Supported Features](#)
- [About SafeMode](#)

 **NOTE:** To use the CLI on a serial connection or in an SSH management session, you need to use a terminal emulation application (such as Tera Term) or an SSH Client application (such as PuTTY). You can find a suitable, free, terminal emulator to download from the Internet.

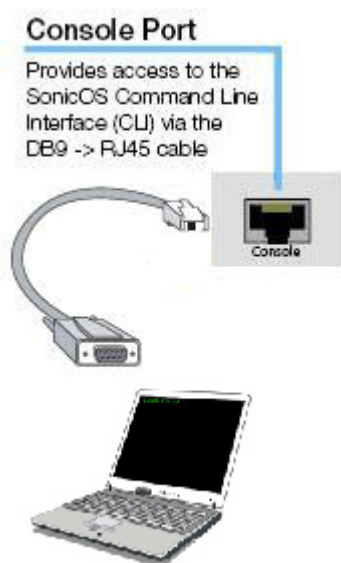
Configuring Features using the CLI on a Serial Connection via the Console Port

You do not need to assign an IP address to the firewall to use the CLI on a serial connection to the Console port.

- NOTE:** The default terminal settings on the firewall are 80 columns by 25 lines. To ensure the best display and reduce the chance of graphic anomalies, use the same settings with the serial terminal software. The device terminal settings can be changed, if necessary. Use the standard ANSI setting on the serial terminal software.

To configure features using the CLI on a serial connection via the console port:

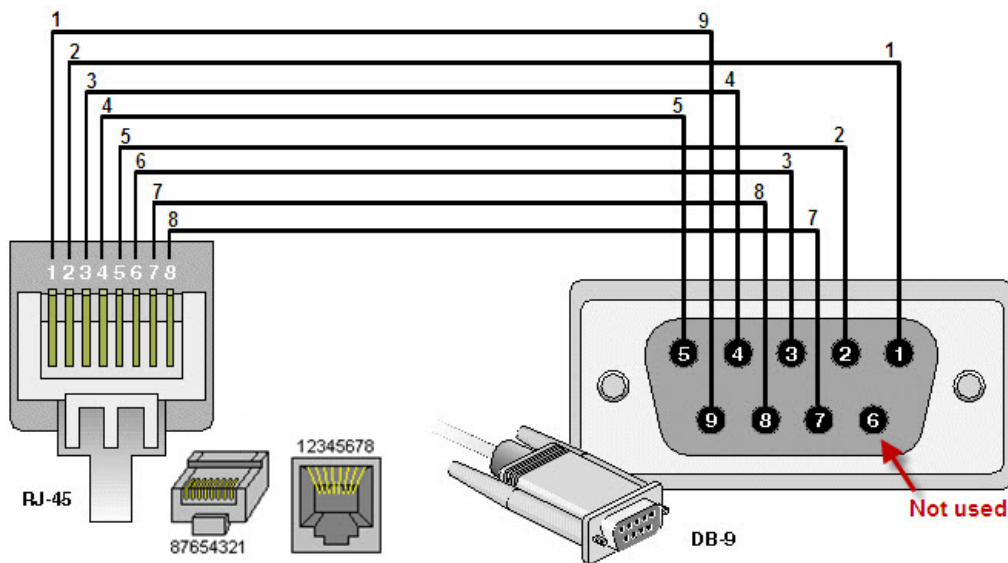
- 1 Attach an RJ-45 to DB-9 serial cable to the appliance port marked CONSOLE. Attach the other end of the cable to a serial port on the configuring computer.



- 2 The RJ-45 to DB-9 serial cable pin assignments are as follows:

| RJ-45 connector | DB-9 connector |
|-----------------|------------------|
| Pin 1 | Pin 9 |
| Pin 2 | Pin 1 |
| Pin 3 | Pin 4 |
| Pin 4 | Pin 5 |
| Pin 5 | Pin 2 |
| Pin 6 | Pin 3 |
| Pin 7 | Pin 8 |
| Pin 8 | Pin 7 |
| Pin 9 | Pin 6 – not used |

The RJ-45 to DB-9 serial cable pin diagram is shown below:



- 3 Launch a terminal emulation application that communicates with the serial port connected to the appliance. Use these settings:
 - 115,200 baud
 - 8 data bits
 - no parity
 - 1 stop bit
 - no flow control
- 4 Press **Enter/Return**. Initial information is displayed followed by a **Device Name> Prompt**.

Configuring Features using the CLI in an SSH Management Session via Ethernet

You can use an SSH client to access the CLI by connecting to the appliance with an Ethernet cable. This option is useful for customers who do not have access to an RJ-45 to DB-9 serial cable for the console port on the firewall.

To use SSH management, you must assign an IP address to X0 (LAN) or X1 (WAN), or use the default LAN IP address of 192.168.168.168.

To configure features using the CLI in an SSH management session via Ethernet:

- 1 Attach an Ethernet cable to the interface port marked X0. Attach the other end of the Ethernet cable to an Ethernet port on the configuring computer.
- 2 Launch a terminal emulation application or SSH client that communicates via Ethernet.
- 3 In the emulation application, enter the IP destination address for the X0 interface, and enter 22 as the port number.
- 4 Select SSH as the connection type and open a connection.

E-CLI-Supported Features

You can manage the appliance securely from your web browser using HTTPS, by connecting to either the LAN or WAN IP address of the appliance directly or over the network. Refer to the *SonicOS Administration Guide* for complete information about the SonicOS management User Interface (web UI).

Many of the same tasks can also be performed using E-CLI. The following features can be configured and managed from the SonicOSCLI interface:


| Category | Features |
|-------------------|--------------|
| Dashboard | All features |
| 3G/4G/Modem | All features |
| System | All features |
| SonicPoint | All features |
| Firewall | All features |
| Firewall Settings | All features |
| DPI-SSL | All features |
| Anti-Spam | All features |
| Users | All features |
| Security Services | All features |
| WAN Acceleration | All features |
| AppFlow | All features |
| Log | All features |

About SafeMode

SafeMode is a limited web management interface that provides a way to upload firmware from your computer and reboot the appliance. The SafeMode feature allows you to recover quickly from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** screen.

There is an E-CLI command “safemode”, which restarts the firewall in safemode.

For more information on SafeMode for your firewall, refer to the *Getting Started Guide* for your appliance.

 **NOTE:** The CLI commands are not available in SafeMode.

Example of Configuring a Site-to-Site VPN Using E-CLI

This section describes how to create a VPN policy using CLI. You can configure all of the parameters using CLI, and enable the VPN without using the web management interface.

 **NOTE:** In this example, the VPN policy on the other end has already been created.

Topics:

- [CLI Access](#)

- [Configuring a Site-to-Site VPN](#)
- [Viewing a VPN Configuration](#)

CLI Access

As in other Command Line Interfaces, such as Unix Shell or Cisco IOS, auto-complete is provided, so you only have to type the first few letters of a command. The rest is automatically completed for you by the system.

- 1 Use a DB9 to RJ45 connector to connect the serial port of your PC to the console port of the firewall.
- 2 Use a terminal emulator program such as PuTTY or Tera Term (downloaded from the Internet) with the following set parameters:
 - 115,200 baud
 - 8 bits
 - No parity
 - 1 stop bit
 - No flow control

- 3 You may need to click return several times to get to a command prompt. In this example, the command prompt is:

```
NSA3600>
```

- 4 When you need to make a configuration change, you must be in configure mode. To enter configure mode, type configure.

```
NSA3600> configure
```

- 5 The command prompt changes and adds the word config to distinguish it from normal mode. In configure mode, you can configure all the settings, enable and disable the VPNs, and configure the firewall.

```
(config[NSA3600])>
```

Configuring a Site-to-Site VPN

This is an example of configuring a Site-to-Site VPN using CLI:

```
config(C0EAE45998CC)# address-object ipv4 "Office LAN"
(add-ipv4-address-object[Office LAN])# zone VPN
(add-ipv4-address-object[Office LAN])# network 192.168.15.0 255.255.255.0
(add-ipv4-address-object[Office LAN])# exit
config(C0EAE45998CC)# commit
% Applying changes...
% Status returned processing command:
  commit
% Changes made.
show address-object ipv4 "Office LAN"
vpn policy site-to-site testS2S
```

```
enable
gateway primary 2.2.2.2

auth-method shared-secret
  shared-secret 11111111
  exit

network local any
network remote name "Office LAN"
proposal ike exchange ikev2
proposal ike encryption aes-128
proposal ike authentication sha-1
proposal ike dh-group 2
proposal ike lifetime 28800
proposal ipsec protocol esp
proposal ipsec encryption aes-128
proposal ipsec authentication sha-1
no proposal ipsec perfect-forward-secrecy
proposal ipsec lifetime 28800
no netbios
anti-replay
no wxa-group
no multicast
no management https
no management ssh
no management snmp
no keep-alive
no allow-sonicpointn-layer3
no user-login http
no user-login https
no default-lan-gateway
bound-to zone WAN
no suppress-trigger-packet
no accept-hash
no send-hash
no suppress-auto-add-rule
no apply-nat
```



```
exit
commit
show vpn policy ipv4 site-to-site testS2S
```

Viewing a VPN Configuration

To view a list of all the configured VPN policies:

- 1 Type the command `show vpn policy`. The output is similar to the following:

```
(config[NSA3600])> show vpn policy
Policy: WAN GroupVPN (Disabled)
Key Mode: Pre-shared
Pre Shared Secret: DE65AD2228EED75A
Proposals:
IKE: Aggressive Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds
Advanced:
Allow NetBIOS OFF, Allow Multicast OFF
Management: HTTP OFF, HTTPS OFF
Lan Default GW: 0.0.0.0
Require XAUTH: ON, User Group: Trusted Users
Client:
Cache XAUTH Settings: Never
Virtual Adapter Settings: None
Allow Connections To: Split Tunnels
Set Default Route OFF, Apply VPN Access Control List OFF
Require GSC OFF
Use Default Key OFF
Policy: OfficeVPN (Enabled)
Key Mode: Pre-shared
Primary GW: 10.50.31.104
Secondary GW: 0.0.0.0
Pre Shared Secret: sonicwall
IKE ID:
Local: IP Address
Peer: IP Address
Network:
Local: LAN Primary Subnet
```

Remote: OfficeLAN

Proposals:

IKE: Main Mode, 3DES SHA, DH Group 2, 28800 seconds

IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds

Advanced:

Keepalive ON, Add Auto-Rule ON, Allow NetBIOS OFF

Allow Multicast OFF

Management: HTTP ON, HTTPS ON

User Login: HTTP ON, HTTPS ON

Lan Default GW: 0.0.0.0

Require XAUTH: OFF

Bound To: Zone WAN

- 2 To view the configuration for a specific policy, specify the policy name in double quotes.

For example:

```
(config[NSA3600])> show vpn policy "OfficeVPN"
```

The output is similar to the following:

Policy: OfficeVPN (Enabled)

Key Mode: Pre-shared

Primary GW: 10.50.31.104

Secondary GW: 0.0.0.0

Pre Shared Secret: sonicwall

IKE ID:

Local: IP Address

Peer: IP Address

Network:

Local: LAN Primary Subnet

Remote: OfficeLAN

Proposals:

IKE: Main Mode, 3DES SHA, DH Group 2, 28800 seconds

IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds

Advanced:

Keepalive ON, Add Auto-Rule ON, Allow NetBIOS OFF

Allow Multicast OFF

Management: HTTP ON, HTTPS ON

User Login: HTTP ON, HTTPS ON

Lan Default GW: 0.0.0.0

Require XAUTH: OFF

Bound To: Zone WAN

- 3 Type the command `show vpn sa [name]` to see the active SA:

```
(config[NSA3600])> show vpn sa "OfficeVPN"
```

Policy: OfficeVPN

IKE SAs

GW: 10.50.31.150:500 --> 10.50.31.104:500

Main Mode, 3DES SHA, DH Group 2, Responder

Cookie: 0x0ac298b6328a670b (I), 0x28d5eec544c63690 (R)

Lifetime: 28800 seconds (28783 seconds remaining)

IPsec SAs

GW: 10.50.31.150:500 --> 10.50.31.104:500

(192.168.61.0 - 192.168.61.255) --> (192.168.15.0 - 192.168.15.255)

ESP, 3DES SHA, In SPI 0xed63174f, Out SPI 0x5092a0b2

Lifetime: 28800 seconds (28783 seconds remaining)

Interfaces

This section discusses the following topics:

Topics:

- [User Interfaces](#)
- [Advantages of CLI](#)
- [Using a Terminal Emulator or SSH Client](#)
- [Configuring New SonicWall Appliances With CLI](#)

User Interfaces

- The Graphic User Interface (GUI) is the one casual computer users are the most familiar with. It consists of moving users through screens in order to accomplish tasks. Users are led through a series of screens with prompts to click in certain boxes or other areas of the screen, usually with a minimum of keyboard work. A GUI is usually user-friendly, and conversational.
- The Application Program Interface (API) is a set of routines, tools, and protocols for building software applications. The API is like a translating tool, allowing two different languages, two different instruction sets, to work together to accomplish tasks. Along with other software components, APIs are used to program GUIs. APIs are intended to be only machine-readable, since they are programmed into the applications.
- The Command Line Interface (CLI), on the other hand, is a direct human interface with the machine, but not through clicking boxes with the mouse. The CLI uses a series of commands with preset meanings, typed on the keyboard by the user at a prompt on the screen. The commands are then translated by the computer into various actions. E-CLI for SonicOS has the added advantage that “show” commands can be copied and pasted at the prompt, to speed up CLI configuration.

Advantages of CLI

Each interface has its advantages and disadvantages. More and more API providers are supporting a set of CLI commands alongside their API. A list of some of the benefits of the CLI is given below:

- A CLI is a human-readable interface that appeals to many developers’ tastes. Most developers work from their favorite editor within the command line anyway, so CLI offers them the ability to stay where they are most comfortable and most productive.
- CLI can automate many tedious UI tasks. It offers powerful scripting capabilities, with the ability to connect many commands into one.
- This leads to a time savings for users. Once CLI commands have been scripted, they can accomplish many tasks with one user action.

- CLI commands can be used for advanced tasks in an interactive mode to debug or control an operating system. If launched from a command line shell, many normal programs allow further manipulation from within the CLI.
- Cloud computing is highly dependent on CLI, for interacting with virtual machines, spinning up instances, running applications in the cloud, arbitrating a virtual data center, and more. CLI is a developer's most effective method for initiating cloud transactions.
- Troubleshooting and testing of vulnerability would be impossible if not done from the command line. All remote access and file manipulation are done from the command line.

Using a Terminal Emulator or SSH Client

To use the CLI on a serial connection or in an SSH management session, you need to use a terminal emulation application (such as Tera Term) or an SSH Client application (such as PuTTY). You can find a suitable, free, terminal emulator to download from the Internet.

Configuring New SonicWall Appliances With CLI

Many of the same tasks that can be done using the Web-based Appliance Management Console (AMC) Maintenance screen, such as configuring a new appliance and backing up and restoring your appliance configuration, are available with expanded functionality from the CLI for administrators who prefer to work on the command line.

Routing & OSPF Configuration

The following section explains the how to configure Routing and OSPF (Open Shortest Path First). OSPF is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm, and therefore operates within a single autonomous system. The following topics are covered in this section:

Topics:

- [To Configure Routing](#)
- [To Configure OSPF](#)
- [To Enter ospfv3](#)
- [Advanced Routing with ZebOS CLI](#)

To Configure Routing

```
admin@my2600NSA> config
config(my2600NSA)# routing
(config-routing)#
```

To Configure OSPF

```
In routing mode,
(config-routing)# mode advanced
(config-routing)# ospf
```

ZebOS version 7.7.0 IPIRouter 7/2009

ARS OSPF>?

Exec commands:

```
clear    Reset functions
configure Enter configuration mode
debug    Debugging functions (see also 'undebug')
exit     End current mode and down to previous mode
faults   Fault management command
help     Description of the interactive help system
no       Negate a command or set its defaults
```

show Show command
terminal Set terminal line parameters
undebug Disable debugging functions (see also 'debug')
who Display who is on vty
write Write running configuration to memory, file or terminal

ARS OSPF>

To Enter ospfv3

```
(config-routing)# ospfv3
```

ZebOS version 7.7.0 IPIRouter 7/2009

```
ARS OSPFv3>?
```

Exec commands:

clear Reset functions
configure Enter configuration mode
debug Debugging functions (see also 'undebug')
exit End current mode and down to previous mode
faults Fault management command
help Description of the interactive help system
no Negate a command or set its defaults
show Show command
terminal Set terminal line parameters
undebug Disable debugging functions (see also 'debug')
who Display who is on vty
write Write running configuration to memory, file or terminal

Advanced Routing with ZebOS CLI

For advanced routing, SonicWall uses a third party product, ZebOS CLI, which is not implemented by us.

E-CLI provides the bridge to enter ZebOS CLI or to get the show result from the ZebOS CLI, as follows:

```
config(C0EAE45998CC)# routing
```

```
(config-routing)# os
```

```
ospf ospfv3
```

```
(config-routing)# ospf
```

ZebOS version 7.7.0 IPIRouter 7/2009

```
ARS OSPF>
```

Top Level and System Commands

This chapter gives some examples of Top Level and System CLI commands in SonicOS. They are entered at the `admin@COEAE45998CC>` prompt or `admin@COEAE45998CC>` [Tab].

```
System Commands:
clear          Reset functions.
cli           CLI configuration.
diag         Diagnostic functions.
exit         Exit the current mode.
export       Export system status or configuration.
help        Display command help.
no          Negate a command or set its defaults.
show        Show system status or configuration.

Top Level Commands:
configure    Enter configuration mode.
geo-botnet-lookup Check GEO location and lookup BOTNET server.
kill-user   Log out users.
log-to-ftp  Log to FTP server.
mxlookup   MX lookup and banner check the specified domain name
          and SMTP port.
network-path Find network path of the specified IP address.
nslookup   DNS lookup of the specified host.
ping       Ping the specified host.
pmtu-discovery Path MTU discovery to the specified host.
rbl-lookup Lookup the specified realtime black list.
restart    Restart SonicOS.
reverse-lookup Resolve the specified reverse name.
safemode  Restart the device and enter safemode.
traceroute Traceroute to the specified host.
unlock    Unlock a locked out IP address.
```

The following are entered with `admin@COEAE45998CC>` `show`.

```
admin@COEAE45998CC> show

System Commands:
cli           current-config    pending-config

Top Level Commands:
access-rule  access-rules
action-objects address-group
address-object address-objects
anti-spyware app-control
appflow     arp
bandwidth-object bandwidth-objects
capture-atp certificate
checksum   client-enforcement
dhcp-server dns
dns-security dpi-ssh
dynamic-dns email-object
failover-lb fips
firmware   gateway-antivirus
high-availability icmp
interfaces intrusion-prevention
license    log
match-object match-objects
nat-policies nat-policy
ndpp      network-monitor
portshield-groups qos-mapping
route-policies route-policy
schedule  schedules
security-services service-group
service-object service-objects
sonicpoint ssh
ssl-vpn   status
tcp       tech-support-report
tunnel-interface tunnel-interfaces
udpvd6   user
virtual-assist vlan-translation
voip     vpn
zone     zones
```


E-CLI Commands

The most recent E-CLI command list is provided in the following pages.

Click the command name to view its syntax and description.

Contents

- ecli/primitive.cdl
 - [clear](#)
 - [export](#)
 - [no](#)
 - [show](#)
 - [cancel](#)
 - [commit](#)
 - [end](#)
 - [end](#)
 - [exit](#)
 - [help](#)
- ecli/top.cdl
 - [configure](#)
- ecli/config.cdl
 - [no pending-config](#)
- ecli/cli.cdl
 - [clear screen](#)
 - [no cli history](#)
 - [cli history](#)
 - [cli format out](#)
 - [cli idle-timeout session](#)
 - [cli idle-timeout default](#)
 - [cli screen width session](#)
 - [cli screen width default](#)
 - [cli screen length session](#)
 - [cli screen length default](#)
 - [cli show-unmodified session](#)
 - [cli show-unmodified default](#)
 - [no cli show-unmodified session](#)
 - [no cli show-unmodified default](#)
 - [cli pager session](#)
 - [no cli pager session](#)
 - [cli pager default](#)
 - [no cli pager default](#)
 - [cli interactive-prompts session](#)
 - [no cli interactive-prompts session](#)
 - [cli interactive-prompts default](#)
 - [no cli interactive-prompts default](#)
 - [cli ftp user session](#)
 - [no cli ftp user session](#)
 - [cli ftp user default](#)
 - [no cli ftp user default](#)
 - [cli ftp password session](#)
 - [no cli ftp password session](#)
 - [cli ftp password default](#)
 - [no cli ftp password default](#)
 - [cli banner](#)
 - [no cli banner](#)
- ecli/config_show.cdl
 - [show current-config](#)
 - [show current-config](#)
 - [show pending-config](#)
 - [show checksum](#)
- ecli/cli_show.cdl
 - [show cli](#)
- ecli/diag.cdl
 - [ping](#)
 - [traceroute](#)
 - [diag network-path](#)
 - [network-path](#)
 - [nslookup](#)
 - [diag reverse-lookup](#)
 - [reverse-lookup](#)
 - [diag rbl-lookup](#)
 - [rbl-lookup](#)
 - [diag mxlookup](#)
 - [mxlookup](#)
 - [diag geo-botnet-lookup](#)
 - [geo-botnet-lookup](#)
 - [pmtu-discovery](#)
 - [diag show abrentries](#)
 - [diag show processes](#)
 - [diag show process](#)
 - [diag show netstat](#)
 - [diag show cores](#)
 - [diag show core](#)
 - [diag show multicore](#)
 - [diag show build-info](#)
 - [diag show cpu](#)
 - [diag show web-server](#)
 - [diag show fpa](#)
 - [diag show mem-pools](#)
 - [diag show memory](#)

- [diag show buf-memzone](#)
- [diag show memzone](#)
- [diag no show memzone](#)
- [diag show tracelog](#)
- [diag clear cp-stats](#)
- [diag show cp-stats](#)
- [diag clear hw-stats](#)
- [diag clear abr-entries](#)
- [diag show hw-stats](#)
- [diag show timer-counters](#)
- [diag show wd-stats](#)
- [diag clear pp-stats](#)
- [diag show pp-stats](#)
- [diag clear active-utm](#)
- [diag show active-utm](#)
- [diag show debug interface](#)
- [diag show alerts](#)
- [diag show log](#)
- [diag show drop-stats](#)
- [diag cli pager-test](#)
- [diag show switch port](#)
- [diag wmi ping-test](#)
- [diag wmi reset](#)
- [diag wmi lsusb](#)
- [diag show wmi status](#)
- [diag show wmi configs](#)
- [diag wmi set-primary-config](#)
- [ecli/diag-advanced.cdl](#)
 - [diag advanced x0-as-mgmt](#)
 - [diag no advanced x0-as-mgmt](#)
 - [diag advanced tracelog](#)
 - [diag advanced arp](#)
 - [bridging](#)
 - [no bridging](#)
 - [open-arp-behavior](#)
 - [no open-arp-behavior](#)
 - [source-ip-validation](#)
 - [no source-ip-validation](#)
 - [only-unicast](#)
 - [no only-unicast](#)
 - [limit-nonresponsive](#)
 - [no limit-nonresponsive](#)
 - [bypass-for-l2bridge](#)
 - [no bypass-for-l2bridge](#)
 - [gratuitous-arp-compatibility](#)
 - [no gratuitous-arp-compatibility](#)
 - [gratuitous-arp-limit](#)
 - [no gratuitous-arp-limit](#)
 - [system-broadcast](#)
 - [no system-broadcast](#)
 - [ignore-arps-with-primary-mac-from-other-if](#)
 - [no ignore-arps-with-primary-mac-from-other-if](#)
 - [display-mac-tracking](#)
 - [no display-mac-tracking](#)
 - [send system-arps](#)
 - [diag advanced network](#)
 - [flush-alternate-path-flows](#)
 - [no flush-alternate-path-flows](#)
 - [update-route-version](#)
 - [no update-route-version](#)
 - [tcp-packet-option-tagging](#)
 - [no tcp-packet-option-tagging](#)
 - [fix-malformed-tcp-headers](#)
 - [no fix-malformed-tcp-headers](#)
 - [sequence-number-randomization](#)
 - [no sequence-number-randomization](#)
 - [syn-validation](#)
 - [no syn-validation](#)
 - [clear ospf](#)
 - [clear dont-fragment-bit](#)
 - [no clear dont-fragment-bit](#)
 - [active-active-clustering-wiremode](#)
 - [no active-active-clustering-wiremode](#)
 - [dmz-icmp-redirect](#)
 - [no dmz-icmp-redirect](#)
 - [learning-bridge-filter](#)
 - [no learning-bridge-filter](#)
 - [diag advanced dns](#)
 - [prefer-arpa](#)
 - [no prefer-arpa](#)
 - [stack-traffic-by-dp](#)
 - [no stack-traffic-by-dp](#)
 - [diag advanced dns-security](#)
 - [dns-tunnel-minimum-packet-number](#)
 - [dns-tunnel-ratio-threshold](#)
 - [dns-tunnel-number-threshold](#)
 - [diag advanced dhcp](#)
 - [network-pre-discovery](#)
 - [no network-pre-discovery](#)
 - [conflict-detect-period](#)
 - [resources-to-discover](#)

- [conflicted-resource-timeout](#)
- [available-resource-timeout](#)
- [save leases](#)
- [dhcpnak](#)
- [no dhcpnak](#)
- [lease-database-refresh-interval](#)
- [lease-database-refresh-number](#)
- [recycle-expired-lease](#)
- [no recycle-expired-lease](#)
- [diag advanced voip](#)
- [max-endpoints](#)
- [no max-endpoints](#)
- [auto-add-sip](#)
- [no auto-add-sip](#)
- [sip-transforms](#)
- [no sip-transforms](#)
- [invite-flush](#)
- [no invite-flush](#)
- [invite-flush-unused](#)
- [no invite-flush-unused](#)
- [reset sip-database](#)
- [diag advanced vpn](#)
- [adjust-tcp-mss](#)
- [no adjust-tcp-mss](#)
- [interoperable-ike-dh-exchange](#)
- [no interoperable-ike-dh-exchange](#)
- [fragment-after-esp](#)
- [no fragment-after-esp](#)
- [spi-cpi-parameter-index](#)
- [no spi-cpi-parameter-index](#)
- [trust-built-in-ca](#)
- [no trust-built-in-ca](#)
- [preserve-ike-port](#)
- [no preserve-ike-port](#)
- [diag advanced encryption](#)
- [hardware-encryption](#)
- [no hardware-encryption](#)
- [dp-stack](#)
- [no dp-stack](#)
- [ssl-v3](#)
- [no ssl-v3](#)
- [tls-v1](#)
- [no tls-v1](#)
- [diag advanced firewall](#)
- [ftp-bounce-attack-protection](#)
- [no ftp-bounce-attack-protection](#)
- [ftp-protocol-anomaly-attack-protection](#)
- [no ftp-protocol-anomaly-attack-protection](#)
- [orphan-data-connection](#)
- [no orphan-data-connection](#)
- [ip-spoof-checking](#)
- [no ip-spoof-checking](#)
- [port-scan-detection](#)
- [no port-scan-detection](#)
- [anticipated-connection-timeout](#)
- [no anticipated-connection-timeout](#)
- [anticipated-connection-parent-termination](#)
- [no anticipated-connection-parent-termination](#)
- [anticipated-media-timeout](#)
- [no anticipated-media-timeout](#)
- [anticipated-media-parent-termination](#)
- [no anticipated-media-parent-termination](#)
- [trace-connections-port](#)
- [no trace-connections-port](#)
- [include-tcp-data-connection](#)
- [no include-tcp-data-connection](#)
- [track-bandwidth-usage](#)
- [no track-bandwidth-usage](#)
- [decrease-connection-count-after-close](#)
- [no decrease-connection-count-after-close](#)
- [tcp-state-manipulation-dos-protection](#)
- [no tcp-state-manipulation-dos-protection](#)
- [sequential-addresses](#)
- [no sequential-addresses](#)
- [default-policy-editable](#)
- [no default-policy-editable](#)
- [udp-icmp-flood-detecting](#)
- [no udp-icmp-flood-detecting](#)
- [clear connections](#)
- [diag advanced support-windows-messenger](#)
- [diag no advanced support-windows-messenger](#)
- [diag advanced security-services](#)
- [dpi-engine](#)
- [no dpi-engine](#)
- [bidirectional-ips](#)
- [no bidirectional-ips](#)
- [dpi-ip-fragment-reassembly](#)
- [no dpi-ip-fragment-reassembly](#)
- [dev-debug](#)
- [no dev-debug](#)
- [smtp-chunking-modification](#)

- [no smtp-chunking-modification](#)
- [pop3-auto-deletion](#)
- [no pop3-auto-deletion](#)
- [pop3-uidl-rewriting](#)
- [no pop3-uidl-rewriting](#)
- [smb-read-write-enforcement](#)
- [no smb-read-write-enforcement](#)
- [keep-http-accept-range-bytes](#)
- [no keep-http-accept-range-bytes](#)
- [log-virus-uri](#)
- [no log-virus-uri](#)
- [offset-qualifier-signature](#)
- [no offset-qualifier-signature](#)
- [minimum-http-header-length](#)
- [no minimum-http-header-length](#)
- [incremental-signature-updates](#)
- [no incremental-signature-updates](#)
- [force-utm-offload](#)
- [no force-utm-offload](#)
- [utm-traffic-offload](#)
- [no utm-traffic-offload](#)
- [limit-dpi-tcp-window-advertisement](#)
- [no limit-dpi-tcp-window-advertisement](#)
- [threshold-limit](#)
- [maximum-regex-automaton-size](#)
- [signature-database-reload](#)
- [no signature-database-reload](#)
- [process-ips-signatures](#)
- [no process-ips-signatures](#)
- [process-gav-signatures](#)
- [no process-gav-signatures](#)
- [process-anti-spyware-signatures](#)
- [no process-anti-spyware-signatures](#)
- [process-app-signatures](#)
- [no process-app-signatures](#)
- [optimal-value](#)
- [no optimal-value](#)
- [limit-ips-cft-scan](#)
- [no limit-ips-cft-scan](#)
- [enforce-cfs-host-tag-search](#)
- [no enforce-cfs-host-tag-search](#)
- [local-cfs-server](#)
- [no local-cfs-server](#)
- [client-anti-virus-timeout](#)
- [reset av-info](#)
- [reset next-gen-av](#)
- [reset licenses](#)
- [reset client-content-filtering](#)
- [reset client-content-filtering](#)
- [reset http-clientless-notification-cache](#)
- [reset cloud-av-cache](#)
- [cloud-av-server](#)
- [no cloud-av-server](#)
- [diag advanced dpi-ssl](#)
- [rewritten-certificate-sn-modifier](#)
- [client-spoofed-certificate-caching](#)
- [no client-spoofed-certificate-caching](#)
- [remove-tcp-timestamp-option](#)
- [no remove-tcp-timestamp-option](#)
- [drop-ssl-on-low-memory](#)
- [no drop-ssl-on-low-memory](#)
- [proxyless-ssl-when-limit-exceeded](#)
- [no proxyless-ssl-when-limit-exceeded](#)
- [endpoint-tcp-window-setup](#)
- [no endpoint-tcp-window-setup](#)
- [server-facing-session-reuse](#)
- [no server-facing-session-reuse](#)
- [block-untrusted-certificate-connections](#)
- [no block-untrusted-certificate-connections](#)
- [max-stream-offset](#)
- [no max-stream-offset](#)
- [tcp-window-multiplier](#)
- [tcp-min-adv-window](#)
- [max-proxied-connections](#)
- [no max-proxied-connections](#)
- [update-security-services-info](#)
- [ssl-version](#)
- [cipher-method](#)
- [diag advanced high-availability](#)
- [idle-monitor](#)
- [no idle-monitor](#)
- [suppress-active-transition-alarm](#)
- [no suppress-active-transition-alarm](#)
- [restart-backup-on-watchdog](#)
- [no restart-backup-on-watchdog](#)
- [interleave-cache](#)
- [no interleave-cache](#)
- [transparent-mode-gratuitous-arp](#)
- [no transparent-mode-gratuitous-arp](#)
- [max-transparent-mode-gratuitous-arps](#)
- [max-gratuitous-arps](#)

- [diag advanced pppoe](#)
- [lcp-requests](#)
- [no lcp-requests](#)
- [log-lcp-echo](#)
- [no log-lcp-echo](#)
- [end-of-list-tag](#)
- [no end-of-list-tag](#)
- [netmask](#)
- [no netmask](#)
- [diag advanced dial-up](#)
- [display-status](#)
- [no display-status](#)
- [max-pppdu-failure](#)
- [reset](#)
- [diag advanced dpi-stateful-firewall-security](#)
- [diag advanced stateful-firewall-security](#)
- [diag advanced management](#)
- [standby-management-sa](#)
- [no standby-management-sa](#)
- [gms-preempts-admin](#)
- [no gms-preempts-admin](#)
- [http-management](#)
- [no http-management](#)
- [classic-view](#)
- [no classic-view](#)
- [online-help-url](#)
- [diag advanced user-authentication](#)
- [post-authentication-redirect-url](#)
- [no post-authentication-redirect-url](#)
- [redirect-http-in-dp](#)
- [no redirect-http-in-dp](#)
- [https-redirect-port](#)
- [flush-cached-redirect-files](#)
- [logout users](#)
- [log-all-sso-attempts](#)
- [no log-all-sso-attempts](#)
- [user-ip](#)
- [include-sso-polling](#)
- [no include-sso-polling](#)
- [include-sso-bypass](#)
- [no include-sso-bypass](#)
- [include-additional-non-initiation](#)
- [no include-additional-non-initiation](#)
- [sso-agent-verison-negotiation](#)
- [no sso-agent-verison-negotiation](#)
- [diag advanced diagnostics](#)
- [setup-tool-server](#)
- [no setup-tool-server](#)
- [trace-message-level](#)
- [auto-restart](#)
- [no auto-restart](#)
- [secured-crash-analysis](#)
- [no secured-crash-analysis](#)
- [show-user-diagnostics](#)
- [no show-user-diagnostics](#)
- [wan-connectivity-test start](#)
- [wan-connectivity-test target-ip](#)
- [no wan-connectivity-test target-ip](#)
- [wan-connectivity-test stop](#)
- [send wan-connectivity-test log](#)
- [dp-jobs-tracked](#)
- [diag advanced watchdog](#)
- [cpu-watchdog](#)
- [no cpu-watchdog](#)
- [restart-for](#)
- [no restart-for](#)
- [quick-restart](#)
- [no quick-restart](#)
- [restart-when-no-packet-rx](#)
- [no restart-when-no-packet-rx](#)
- [wait-for-no-packet-rx](#)
- [diag advanced wireless](#)
- [regulatory-domain](#)
- [no regulatory-domain](#)
- [sonicpoint support-type](#)
- [vap-bssid-local-bit](#)
- [no vap-bssid-local-bit](#)
- [sonicpoint legacy-management](#)
- [no sonicpoint legacy-management](#)
- [sonicpoint update-firmware](#)
- [sonicpoint keepalive-enforcement](#)
- [no sonicpoint keepalive-enforcement](#)
- [sonicpoint profile-tcp-window-size](#)
- [no sonicpoint profile-tcp-window-size](#)
- [sonicpoint default-window-size](#)
- [no sonicpoint default-window-size](#)
- [sonicpointn prefer-channel-1-6-11](#)
- [no sonicpointn prefer-channel-1-6-11](#)
- [sonicpointn ssh-management](#)
- [no sonicpointn ssh-management](#)
- [sonicpointn logging](#)

- [no sonicpointn logging](#)
- [sonicpoint erase-old-crash-log](#)
- [no sonicpoint erase-old-crash-log](#)
- [sonicpointn noise-security-level](#)
- [no sonicpointn noise-security-level](#)
- [sonicpointn noise-safemode-reboot](#)
- [no sonicpointn noise-safemode-reboot](#)
- [sonicpoint retain-ip](#)
- [no sonicpoint retain-ip](#)
- [sonicpoint snap-header](#)
- [no sonicpoint snap-header](#)
- [sonicpoint fragment-icmp](#)
- [no sonicpoint fragment-icmp](#)
- [bonjour-intra-wlan](#)
- [no bonjour-intra-wlan](#)
- [dhcp-arp-enhancement](#)
- [no dhcp-arp-enhancement](#)
- [guest-services-redirect-interval](#)
- [wifisec-enforcement](#)
- [no wifisec-enforcement](#)
- [wlan reply-wifisec-enforcement](#)
- [no wlan reply-wifisec-enforcement](#)
- [wlan dp-core-processing](#)
- [no wlan dp-core-processing](#)
- [wlan broadcast-communication](#)
- [no wlan broadcast-communication](#)
- [wlan bypass-gateway-firewalling](#)
- [no wlan bypass-gateway-firewalling](#)
- [diag advanced tooltip-no-description](#)
- [diag no advanced tooltip-no-description](#)
- [diag advanced preference](#)
- [launching-conversion-control](#)
- [no launching-conversion-control](#)
- [processor-server](#)
- [no processor-server](#)
- [secure-http-to-processor](#)
- [no secure-http-to-processor](#)
- [site-relative-directory](#)
- [no site-relative-directory](#)
- [check-when-importing](#)
- [no check-when-importing](#)
- [diag advanced anti-spam](#)
- [syn-flood-protection](#)
- [no syn-flood-protection](#)
- [check-grid-ip-only](#)
- [no check-grid-ip-only](#)
- [outbound-smtp-grid-ip](#)
- [no outbound-smtp-grid-ip](#)
- [disabling-custom-email](#)
- [no disabling-custom-email](#)
- [limited-admin-configuration](#)
- [no limited-admin-configuration](#)
- [shlo-check](#)
- [no shlo-check](#)
- [auto-generated-cass-acl](#)
- [no auto-generated-cass-acl](#)
- [clear statistics](#)
- [reset grid-name-cache](#)
- [no policies-and-objects](#)
- [cass cloud service addr](#)
- [diag advanced hosted-email-security](#)
- [diag no advanced hosted-email-security](#)
- [diag advanced email-detection](#)
- [diag no advanced email-detection](#)
- [diag advanced remote-assistance](#)
- [diag no advanced remote-assistance](#)
- [diag advanced sslvpn](#)
- [netextender-version](#)
- [no netextender-version](#)
- [diag advanced backend-server](#)
- [enable](#)
- [no enable](#)
- [force-through](#)
- [diag advanced wan-acceleration](#)
- [remote-checking](#)
- [no remote-checking](#)
- [bypass-tcp-acceleration](#)
- [no bypass-tcp-acceleration](#)
- [skip-tcp-acceleration](#)
- [no skip-tcp-acceleration](#)
- [clear debug-status](#)
- [clear tcp-acceleration-database](#)
- [diag advanced geoip-location-service](#)
- [remote-geoip-server](#)
- [clear location-cache](#)
- [use-control-plane](#)
- [no use-control-plane](#)
- [bypass-geoip-blocking](#)
- [no bypass-geoip-blocking](#)
- [bypass-botnet-blocking](#)
- [no bypass-botnet-blocking](#)

- [geoip-botnet-map-file-upload](#)
- [no geoip-botnet-map-file-upload](#)
- [diag advanced flow-reporting](#)
- [clear location-map](#)
- [flow-reporting-and-visualization](#)
- [no flow-reporting-and-visualization](#)
- [report-to-external](#)
- [no report-to-external](#)
- [appflow-monitor-browser-frame-launch](#)
- [no appflow-monitor-browser-frame-launch](#)
- [non-admin-visualization](#)
- [no non-admin-visualization](#)
- [database-busy-timeout](#)
- [no database-busy-timeout](#)
- [hide-appflow-server](#)
- [no hide-appflow-server](#)
- [hide-gmsflow-server](#)
- [no hide-gmsflow-server](#)
- [send-unified-data](#)
- [no send-unified-data](#)
- [gmsflow-server-per-node](#)
- [no gmsflow-server-per-node](#)
- [report-server-addr](#)
- [https-upload](#)
- [no https-upload](#)
- [clear database-tables](#)
- [diag advanced log-reschedule](#)
- [diag no advanced log-reschedule](#)
- [diag advanced ipv6-ready-enforce](#)
- [diag no advanced ipv6-ready-enforce](#)
- [diag advanced icmp drop-unreachable-packet](#)
- [diag no advanced icmp drop-unreachable-packet](#)
- [diag advanced icmp drop-exceeded-packet](#)
- [diag no advanced icmp drop-exceeded-packet](#)
- [diag advanced debug suppress-task-lock](#)
- [diag no advanced debug suppress-task-lock](#)
- [diag advanced debug suppress-task-dead-warning](#)
- [diag no advanced debug suppress-task-dead-warning](#)
- [diag advanced debug suppress-performance-testing-warning](#)
- [diag no advanced debug suppress-performance-testing-warning](#)
- [cli/packet-monitor.cdl](#)
 - [packet-monitor](#)
 - [start capture](#)
 - [stop capture](#)
 - [start mirror](#)
 - [stop mirror](#)
 - [log-to-ftp](#)
 - [export capture](#)
 - [monitor all](#)
 - [monitor default](#)
 - [clear capture](#)
 - [bytes-to-capture](#)
 - [wrap-buffer](#)
 - [no wrap-buffer](#)
 - [exclude encrypted-gms](#)
 - [no exclude encrypted-gms](#)
 - [exclude management](#)
 - [no exclude management](#)
 - [exclude syslog](#)
 - [no exclude syslog](#)
 - [exclude internal-traffic](#)
 - [no exclude internal-traffic](#)
 - [monitor-filter based-on-firewall-rule](#)
 - [no monitor-filter based-on-firewall-rule](#)
 - [monitor-filter interfaces](#)
 - [no monitor-filter interfaces](#)
 - [monitor-filter ether-types](#)
 - [no monitor-filter ether-types](#)
 - [monitor-filter ip-types](#)
 - [no monitor-filter ip-types](#)
 - [monitor-filter source-ips](#)
 - [no monitor-filter source-ips](#)
 - [monitor-filter source-ports](#)
 - [no monitor-filter source-ports](#)
 - [monitor-filter destination-ips](#)
 - [no monitor-filter destination-ips](#)
 - [monitor-filter destination-ports](#)
 - [no monitor-filter destination-ports](#)
 - [monitor-filter bidirectional](#)
 - [no monitor-filter bidirectional](#)
 - [monitor-filter status](#)
 - [no monitor-filter status](#)
 - [display-filter interfaces](#)
 - [no display-filter interfaces](#)
 - [display-filter ether-types](#)
 - [no display-filter ether-types](#)
 - [display-filter ip-types](#)
 - [no display-filter ip-types](#)
 - [display-filter source-ips](#)
 - [no display-filter source-ips](#)
 - [display-filter source-ports](#)

- [no display-filter source-ports](#)
- [display-filter destination-ips](#)
- [no display-filter destination-ips](#)
- [display-filter destination-ports](#)
- [no display-filter destination-ports](#)
- [display-filter bidirectional](#)
- [no display-filter bidirectional](#)
- [display-filter status](#)
- [no display-filter status](#)
- [ftp server](#)
- [no ftp server](#)
- [ftp login](#)
- [no ftp login](#)
- [ftp password](#)
- [no ftp password](#)
- [ftp directory](#)
- [no ftp directory](#)
- [ftp automatic](#)
- [no ftp automatic](#)
- [ftp pcapng](#)
- [no ftp pcapng](#)
- [ftp html](#)
- [no ftp html](#)
- [monitor-filter firewall-generated](#)
- [no monitor-filter firewall-generated](#)
- [monitor-filter intermediate](#)
- [no monitor-filter intermediate](#)
- [mirror max-rate](#)
- [mirror only-ip-packets](#)
- [no mirror only-ip-packets](#)
- [mirror interface](#)
- [no mirror interface](#)
- [mirror ip](#)
- [no mirror ip](#)
- [mirror receive-from-ip](#)
- [no mirror receive-from-ip](#)
- [mirror forward-interface](#)
- [no mirror forward-interface](#)
- [mirror to-capture-buffer](#)
- [no mirror to-capture-buffer](#)
- [mirror encrypt-key](#)
- [mirror decrypt-key](#)
- [ecli/tsr.cdl](#)
 - [send tech-support-report](#)
 - [tech-support-report options](#)
 - [vpn-keys](#)
 - [no vpn-keys](#)
 - [arp-cache](#)
 - [no arp-cache](#)
 - [dhcp-bindings](#)
 - [no dhcp-bindings](#)
 - [ike-info](#)
 - [no ike-info](#)
 - [sonicpointn diagnostics](#)
 - [no sonicpointn diagnostics](#)
 - [users](#)
 - [no users](#)
 - [ip-stack-info](#)
 - [no ip-stack-info](#)
 - [dns-proxy-cache](#)
 - [no dns-proxy-cache](#)
 - [debug-info](#)
 - [no debug-info](#)
 - [user-name](#)
 - [no user-name](#)
 - [ipv6 ndp](#)
 - [no ipv6 ndp](#)
 - [ipv6 dhcp](#)
 - [no ipv6 dhcp](#)
 - [geo-ip-cache](#)
 - [no geo-ip-cache](#)
 - [extra-routing](#)
 - [no extra-routing](#)
 - [atp-cache](#)
 - [no atp-cache](#)
 - [secure-backup](#)
 - [no secure-backup](#)
 - [send-raw-flow-data](#)
 - [no send-raw-flow-data](#)
- [ecli/diag-ipnet.cdl](#)
 - [diag show ipnet](#)
- [ecli/diag-advanced_show.cdl](#)
 - [diag show advanced](#)
- [ecli/packet-monitor_show.cdl](#)
 - [show packet-monitor](#)
- [ecli/tsr_show.cdl](#)
 - [show tech-support-report](#)

- ecli/address-object.cdl
 - [address-object ipv4](#)
 - [no address-object ipv4](#)
 - [address-object ipv6](#)
 - [no address-object ipv6](#)
 - [address-object mac](#)
 - [no address-object mac](#)
 - [address-object fqdn](#)
 - [no address-object fqdn](#)
 - [no address-objects](#)
 - [address-object purge](#)
 - [address-group ipv4](#)
 - [no address-group ipv4](#)
 - [address-group ipv6](#)
 - [no address-group ipv6](#)
 - [no address-groups](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [host](#)
 - [no host](#)
 - [range](#)
 - [no range](#)
 - [network](#)
 - [no network](#)
 - [zone](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [address](#)
 - [no address](#)
 - [zone](#)
 - [multi-homed](#)
 - [no multi-homed](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [domain](#)
 - [no domain](#)
 - [zone](#)
 - [dns-ttl](#)
 - [no dns-ttl](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [host](#)
 - [no host](#)
 - [range](#)
 - [no range](#)
 - [network](#)
 - [no network](#)
 - [zone](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [no address-object ipv4](#)
 - [address-object ipv4](#)
 - [no address-object mac](#)
 - [address-object mac](#)
 - [no address-object fqdn](#)
 - [address-object fqdn](#)
 - [no address-group ipv4](#)
 - [address-group ipv4](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [no address-object ipv6](#)
 - [address-object ipv6](#)
 - [no address-group ipv6](#)
 - [address-group ipv6](#)
- ecli/schedule-object.cdl
 - [schedule](#)
 - [no schedule](#)
 - [no schedules](#)
 - [name](#)
 - [uuid](#)
 - [no uuid](#)
 - [occurs](#)
 - [event](#)
 - [recurring](#)
 - [no recurring](#)
- ecli/service-object.cdl
 - [no service-object](#)
 - [no service-objects](#)
 - [service-object](#)
 - [no service-group](#)
 - [no service-groups](#)
 - [service-group](#)
 - [name](#)
 - [uuid](#)

- [no uuid](#)
- [custom](#)
- [icmp](#)
- [igmp](#)
- [tcp](#)
- [udp](#)
- [6over4](#)
- [gre](#)
- [esp](#)
- [ah](#)
- [icmpv6](#)
- [eigrp](#)
- [ospf](#)
- [pim](#)
- [l2tp](#)
- [ipcomp](#)
- [name](#)
- [uuid](#)
- [no uuid](#)
- [no service-object](#)
- [service-object](#)
- [no service-group](#)
- [service-group](#)
- [ecli/zone-object.cdl](#)
 - [zone](#)
 - [no zone](#)
 - [no zones](#)
 - [guest-services](#)
 - [no guest-services](#)
 - [wireless](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [security-type](#)
 - [no security-type](#)
 - [interface-trust](#)
 - [no interface-trust](#)
 - [auto-generate-access-rules](#)
 - [no auto-generate-access-rules](#)
 - [websense-content-filtering](#)
 - [no websense-content-filtering](#)
 - [client](#)
 - [no client](#)
 - [gateway-anti-virus](#)
 - [no gateway-anti-virus](#)
 - [intrusion-prevention](#)
 - [no intrusion-prevention](#)
 - [app-control](#)
 - [no app-control](#)
 - [anti-spyware](#)
 - [no anti-spyware](#)
 - [create-group-vpn](#)
 - [no create-group-vpn](#)
 - [ssl-control](#)
 - [no ssl-control](#)
 - [dpi-ssl-client](#)
 - [no dpi-ssl-client](#)
 - [dpi-ssl-server](#)
 - [no dpi-ssl-server](#)
 - [sslvpn-access](#)
 - [no sslvpn-access](#)
 - [inter-guest](#)
 - [no inter-guest](#)
 - [bypass client](#)
 - [no bypass client](#)
 - [external-auth](#)
 - [no external-auth](#)
 - [policy-page-non-authentication](#)
 - [no policy-page-non-authentication](#)
 - [client-redirect](#)
 - [web-server-1 protocol](#)
 - [web-server-2 protocol](#)
 - [no web-server-2](#)
 - [web-server timeout](#)
 - [message-auth](#)
 - [no message-auth](#)
 - [social-network](#)
 - [no social-network](#)
 - [wechat-qr-auth](#)
 - [no wechat-qr-auth](#)
 - [only-qr-auth](#)
 - [no only-qr-auth](#)
 - [qr-auth-page](#)
 - [no qr-auth-page](#)
 - [auth-pages web-server-1 login](#)
 - [no auth-pages web-server-1 login](#)
 - [auth-pages web-server-1 expiration](#)
 - [no auth-pages web-server-1 expiration](#)
 - [auth-pages web-server-1 timeout](#)
 - [no auth-pages web-server-1 timeout](#)
 - [auth-pages web-server-1 max-sessions](#)

- [no auth-pages web-server-1 max-sessions](#)
- [auth-pages web-server-1 traffic-exceeded](#)
- [no auth-pages web-server-1 traffic-exceeded](#)
- [auth-pages web-server-2 login](#)
- [no auth-pages web-server-2 login](#)
- [auth-pages web-server-2 expiration](#)
- [no auth-pages web-server-2 expiration](#)
- [auth-pages web-server-2 timeout](#)
- [no auth-pages web-server-2 timeout](#)
- [auth-pages web-server-2 max-sessions](#)
- [no auth-pages web-server-2 max-sessions](#)
- [auth-pages web-server-2 traffic-exceeded](#)
- [no auth-pages web-server-2 traffic-exceeded](#)
- [web-content redirect](#)
- [web-content server-down](#)
- [logout-expired](#)
- [no logout-expired](#)
- [status-check](#)
- [no status-check](#)
- [session-sync](#)
- [no session-sync](#)
- [guest-usage-policy](#)
- [no guest-usage-policy](#)
- [idle-timeout](#)
- [custom-auth-page](#)
- [no custom-auth-page](#)
- [post-auth](#)
- [no post-auth](#)
- [bypass-guest-auth](#)
- [no bypass-guest-auth](#)
- [smtp-redirect](#)
- [no smtp-redirect](#)
- [deny-networks](#)
- [no deny-networks](#)
- [pass-networks](#)
- [no pass-networks](#)
- [max-guests](#)
- [dynamic-address-translation](#)
- [no dynamic-address-translation](#)
- [footer](#)
- [header](#)
- [sslvpn-enforcement](#)
- [no sslvpn-enforcement](#)
- [wifi-sec-enforcement](#)
- [no wifi-sec-enforcement](#)
- [wifi-sec-for-site-to-site-vpn](#)
- [no wifi-sec-for-site-to-site-vpn](#)
- [trust-wpa-traffic-as-wifi-sec](#)
- [no trust-wpa-traffic-as-wifi-sec](#)
- [sonicpoint profile](#)
- [no sonicpoint profile](#)
- [bypass-gateway-firewalling](#)
- [no bypass-gateway-firewalling](#)
- [only-sonicpoint-traffic](#)
- [no only-sonicpoint-traffic](#)
- [auto-channel-limitation](#)
- [no auto-channel-limitation](#)
- [sonicwave-online-registration](#)
- [no sonicwave-online-registration](#)
- [sonicpoint-management](#)
- [no sonicpoint-management](#)
- [local-radius-server](#)
- [no local-radius-server](#)
- [interface-server-numbers](#)
- [port](#)
- [client-password](#)
- [tls-cache](#)
- [no tls-cache](#)
- [tls-cache-lifetime](#)
- [ldap-server](#)
- [no ldap-server](#)
- [server](#)
- [no server](#)
- [base-dn](#)
- [no base-dn](#)
- [identity-dn](#)
- [no identity-dn](#)
- [identity-dn-password](#)
- [no identity-dn-password](#)
- [tls](#)
- [no tls](#)
- [cache](#)
- [no cache](#)
- [cache-lifetime](#)
- [active-directory-server](#)
- [no active-directory-server](#)
- [domain](#)
- [no domain](#)
- [full-name](#)
- [no full-name](#)
- [admin-user-name](#)

- [no admin-user-name](#)
- [admin-user-password](#)
- [no admin-user-password](#)
- ecli/address-object_show.cdl
 - [show address-objects](#)
 - [show address-object ipv4](#)
 - [show address-object ipv6](#)
 - [show address-object mac](#)
 - [show address-object fqdn](#)
 - [show address-groups](#)
 - [show address-group ipv4](#)
 - [show address-group ipv6](#)
- ecli/schedule-object_show.cdl
 - [show schedules](#)
 - [show schedule](#)
- ecli/service-object_show.cdl
 - [show service-objects](#)
 - [show service-object](#)
 - [show service-groups](#)
 - [show service-group](#)
- ecli/zone-object_show.cdl
 - [show zones](#)
 - [show zone](#)
- ecli/interface.cdl
 - [clear interface](#)
 - [interfaces display-all-traffic](#)
 - [no interfaces display-all-traffic](#)
 - [shutdown](#)
 - [no shutdown](#)
 - [interface](#)
 - [no interface](#)
 - [tunnel-interface 4to6](#)
 - [no tunnel-interface 4to6](#)
 - [name](#)
 - [comment](#)
 - [no comment](#)
 - [flow-reporting](#)
 - [no flow-reporting](#)
 - [send-icmp-fragmentation](#)
 - [no send-icmp-fragmentation](#)
 - [fragment-packets](#)
 - [no fragment-packets](#)
 - [ignore-df-bit](#)
 - [no ignore-df-bit](#)
 - [type](#)
 - [bound-to interface](#)
 - [no bound-to](#)
 - [bound-to interface](#)
 - [no bound-to](#)
 - [local](#)
 - [remote](#)
 - [local-ipv4](#)
 - [no local-ipv4](#)
 - [remote ipv6](#)
 - [no remote](#)
 - [local](#)
 - [ip](#)
 - [no ip](#)
 - [tunnel-interface vpn](#)
 - [no tunnel-interface vpn](#)
 - [policy](#)
 - [renew](#)
 - [release](#)
 - [connect](#)
 - [disconnect](#)
 - [link-speed](#)
 - [comment](#)
 - [no comment](#)
 - [bandwidth-management egress](#)
 - [no bandwidth-management egress](#)
 - [bandwidth-management ingress](#)
 - [no bandwidth-management ingress](#)
 - [send-icmp-fragmentation](#)
 - [no send-icmp-fragmentation](#)
 - [fragment-packets](#)
 - [no fragment-packets](#)
 - [ignore-df-bit](#)
 - [no ignore-df-bit](#)
 - [mtu](#)
 - [https-redirect](#)
 - [no https-redirect](#)
 - [management](#)
 - [no management](#)
 - [user-login](#)
 - [no user-login](#)
 - [mac](#)
 - [flow-reporting](#)

- [no flow-reporting](#)
- [multicast](#)
- [no multicast](#)
- [cos-8021p](#)
- [no cos-8021p](#)
- [exclude-route](#)
- [no exclude-route](#)
- [asymmetric-route](#)
- [no asymmetric-route](#)
- [default-8021p-cos](#)
- [no default-8021p-cos](#)
- [shutdown-port](#)
- [no shutdown-port](#)
- [port aggregation aggregate](#)
- [no port aggregation aggregate](#)
- [port aggregation paired-aggregate](#)
- [no port aggregation paired-aggregate](#)
- [port redundancy](#)
- [no port redundancy-aggregation](#)
- [load-balancing-vip](#)
- [no load-balancing-vip](#)
- [routed-mode](#)
- [no routed-mode](#)
- [sonicpoint limit](#)
- [sonicpoint reserve-address](#)
- [ip-assignment](#)
- [no ip-assignment](#)
- [native-bridge](#)
- [no native-bridge](#)
- [firewalling](#)
- [no firewalling](#)
- [type](#)
- [paired-interface](#)
- [no paired-interface](#)
- [paired-interface-zone](#)
- [stateful-inspection](#)
- [no stateful-inspection](#)
- [linkstate-propagation](#)
- [no linkstate-propagation](#)
- [restrict-analysis](#)
- [no restrict-analysis](#)
- [bypass-on-malfunction](#)
- [no bypass-on-malfunction](#)
- [ip](#)
- [no ip](#)
- [virtual-group](#)
- [no virtual-group](#)
- [netmask](#)
- [no netmask](#)
- [backup-ip](#)
- [no backup-ip](#)
- [dns primary](#)
- [dns secondary](#)
- [dns tertiary](#)
- [no dns primary](#)
- [no dns secondary](#)
- [no dns tertiary](#)
- [gateway](#)
- [no gateway](#)
- [hostname](#)
- [no hostname](#)
- [release](#)
- [renew](#)
- [renew-on-startup](#)
- [no renew-on-startup](#)
- [renew-on-link-up](#)
- [no renew-on-link-up](#)
- [initiate-renewals-with-discover](#)
- [no initiate-renewals-with-discover](#)
- [force-discover-interval](#)
- [no force-discover-interval](#)
- [schedule](#)
- [dynamic](#)
- [no dynamic](#)
- [gateway](#)
- [no gateway](#)
- [hostname](#)
- [no hostname](#)
- [inactivity](#)
- [no inactivity](#)
- [ip](#)
- [no ip](#)
- [password](#)
- [no password](#)
- [release](#)
- [renew](#)
- [server](#)
- [no server](#)
- [user-name](#)
- [no user-name](#)
- [schedule](#)

- [dynamic](#)
- [no dynamic](#)
- [gateway](#)
- [no gateway](#)
- [hostname](#)
- [no hostname](#)
- [inactivity](#)
- [no inactivity](#)
- [ip](#)
- [no ip](#)
- [password](#)
- [no password](#)
- [release](#)
- [renew](#)
- [server](#)
- [no server](#)
- [shared-secret](#)
- [no shared-secret](#)
- [user-name](#)
- [no user-name](#)
- [dynamic](#)
- [no dynamic](#)
- [unnumbered](#)
- [no unnumbered](#)
- [inactivity](#)
- [no inactivity](#)
- [ip](#)
- [no ip](#)
- [lcp-echo-packets](#)
- [no lcp-echo-packets](#)
- [password](#)
- [no password](#)
- [service-name](#)
- [no service-name](#)
- [reconnect](#)
- [no reconnect](#)
- [user-name](#)
- [no user-name](#)
- [schedule](#)
- [bridge-to](#)
- [block-non-ip](#)
- [no block-non-ip](#)
- [route-on-bridge-pair](#)
- [no route-on-bridge-pair](#)
- [only-sniff](#)
- [no only-sniff](#)
- [stateful-inspection](#)
- [no stateful-inspection](#)
- [bypass-on-malfunction](#)
- [no bypass-on-malfunction](#)
- [vlan-filtering-mode](#)
- [filtered-vlan](#)
- [no filtered-vlan](#)
- [no filtered-vlans](#)
- [no transparent-range](#)
- [transparent-range](#)
- [gratuitous-arp-wan-forwarding](#)
- [no gratuitous-arp-wan-forwarding](#)
- [gratuitous-arp-wan-generation](#)
- [no gratuitous-arp-wan-generation](#)
- [type](#)
- [dialup](#)
- [type](#)
- [clear_profile](#)
- [clear](#)
- [speaker-volume](#)
- [no speaker-volume](#)
- [initialize](#)
- [connect-on-data](#)
- [no connect-on-data](#)
- [remote-trigger-dialout](#)
- [no remote-trigger-dialout](#)
- [max-hosts](#)
- [no max-hosts](#)
- [bandwidth-management egress](#)
- [no bandwidth-management egress](#)
- [bandwidth-management ingress](#)
- [no bandwidth-management ingress](#)
- [compression-multiplier](#)
- [preferred-profile](#)
- [no preferred-profile](#)
- [connection-profile](#)
- [connection-profile](#)
- [no connection-profile](#)
- [country](#)
- [provider](#)
- [plan-type](#)
- [name](#)
- [service-type](#)
- [no service-type](#)
- [dialed-number](#)

- [primary-dialed-number](#)
- [secondary-dialed-number](#)
- [user-name](#)
- [user-password](#)
- [access-point-name](#)
- [connect-type](#)
- [inactivity-disconnect](#)
- [no inactivity-disconnect](#)
- [max-connection-speed](#)
- [max-connection-time](#)
- [no max-connection-time](#)
- [delay-before-reconnect](#)
- [no delay-before-reconnect](#)
- [call-waiting](#)
- [no call-waiting](#)
- [dial-retries](#)
- [no dial-retries](#)
- [delay-between-retries](#)
- [vpn-when-dialed](#)
- [no vpn-when-dialed](#)
- [force-pap](#)
- [no force-pap](#)
- [ip-assignment](#)
- [dns-assignment](#)
- [schedule](#)
- [no schedule](#)
- [data-usage-limiting](#)
- [no data-usage-limiting](#)
- [chat-script](#)
- [no chat-script](#)
- [ecli/arp.cdl](#)
 - [arp](#)
 - [no entry](#)
 - [no entries](#)
 - [entry](#)
 - [timeout](#)
 - [glean](#)
 - [no glean](#)
 - [ip](#)
 - [mac](#)
 - [interface](#)
 - [publish](#)
 - [no publish](#)
 - [bind-mac](#)
 - [no bind-mac](#)
 - [dynamic](#)
 - [no dynamic](#)
 - [clear arp cache entries](#)
 - [clear arp cache entry](#)
- [ecli/dns.cdl](#)
 - [dns server](#)
 - [no dns server](#)
 - [dns rebinding](#)
 - [no dns rebinding](#)
 - [dns fqdn-binding](#)
 - [no dns fqdn-binding](#)
 - [dns split-servers](#)
 - [no dns split-servers](#)
 - [dns fqdn-over-tcp-dns](#)
 - [no dns fqdn-over-tcp-dns](#)
 - [clear dns cache](#)
- [ecli/ddns.cdl](#)
 - [no dynamic-dns profile](#)
 - [no dynamic-dns profiles](#)
 - [dynamic-dns profile](#)
 - [profile-name](#)
 - [enable](#)
 - [no enable](#)
 - [use-online](#)
 - [no use-online](#)
 - [provider](#)
 - [user-name](#)
 - [no user-name](#)
 - [password](#)
 - [no password](#)
 - [domain](#)
 - [no domain](#)
 - [bound-to](#)
 - [online-settings](#)
 - [offline-settings](#)
 - [service-type](#)
- [ecli/dhcp-server.cdl](#)
 - [dhcp-server](#)
 - [enable](#)
 - [no enable](#)
 - [conflict-detection](#)
 - [no conflict-detection](#)
 - [persistence](#)

- [no_persistence](#)
- [scope](#)
- [scope_dynamic](#)
- [no_scope_dynamic](#)
- [scope_static](#)
- [no_scope_static](#)
- [no_scopes_dynamic](#)
- [no_scopes_static](#)
- [no_scopes](#)
- [clear_lease](#)
- [clear_leases](#)
- [option](#)
- [option_object](#)
- [no_option_object](#)
- [no_option_objects](#)
- [option_group](#)
- [no_option_group](#)
- [no_option_groups](#)
- [trusted-relay-agents](#)
- [no_trusted-relay-agents](#)
- [enable](#)
- [no_enable](#)
- [range](#)
- [lease-time](#)
- [default-gateway](#)
- [netmask](#)
- [comment](#)
- [no_comment](#)
- [allow-bootp](#)
- [no_allow-bootp](#)
- [domain-name](#)
- [no_domain-name](#)
- [dns_server](#)
- [no_dns_server](#)
- [wins](#)
- [no_wins](#)
- [call-manager](#)
- [no_call-manager](#)
- [network-boot](#)
- [no_network-boot](#)
- [no_generic-option](#)
- [generic-option](#)
- [always-send-option](#)
- [no_always-send-option](#)
- [enable](#)
- [no_enable](#)
- [name](#)
- [no_name](#)
- [ip](#)
- [mac](#)
- [lease-time](#)
- [default-gateway](#)
- [netmask](#)
- [comment](#)
- [no_comment](#)
- [domain-name](#)
- [no_domain-name](#)
- [dns_server](#)
- [no_dns_server](#)
- [wins](#)
- [no_wins](#)
- [call-manager](#)
- [no_call-manager](#)
- [network-boot](#)
- [no_network-boot](#)
- [no_generic-option](#)
- [generic-option](#)
- [always-send-option](#)
- [no_always-send-option](#)
- [name](#)
- [number](#)
- [array](#)
- [no_array](#)
- [no_value](#)
- [value](#)
- [name](#)
- [option_object](#)
- [no_option_object](#)
- [option_group](#)
- [no_option_group](#)
- [ecli/failover-load-balancing.cdl](#)
 - [clear_failover-lb](#)
 - [failover-lb](#)
 - [enable](#)
 - [no_enable](#)
 - [respond-to-probes](#)
 - [no_respond-to-probes](#)
 - [group](#)
 - [type](#)
 - [preempt](#)
 - [no_preempt](#)

- [spillover-bandwidth](#)
- [address-binding](#)
- [no address-binding](#)
- [auto-adjust-ratio](#)
- [interface](#)
- [no interface](#)
- [final-backup](#)
- [no final-backup](#)
- [probing](#)
- [health-check](#)
- [missed-intervals](#)
- [successful-intervals](#)
- [global-responder](#)
- [no global-responder](#)
- [rank](#)
- [percent](#)
- [probe-type](#)
- [probe-condition](#)
- [main-target](#)
- [alternate-target](#)
- [default-target](#)
- [no default-target](#)
- [ecli/ip-helper.cdl](#)
 - [ip-helper](#)
 - [enable](#)
 - [no enable](#)
 - [policy](#)
 - [no policy](#)
 - [policy](#)
 - [no policy](#)
 - [no policies](#)
 - [protocol](#)
 - [no protocol](#)
 - [no protocols](#)
 - [enable](#)
 - [no enable](#)
 - [protocol](#)
 - [source](#)
 - [destination](#)
 - [comment](#)
 - [no comment](#)
 - [destination](#)
 - [egressif](#)
 - [name](#)
 - [enable](#)
 - [no enable](#)
 - [no port1](#)
 - [port1](#)
 - [no port2](#)
 - [port2](#)
 - [timeout](#)
 - [source-translation](#)
 - [no source-translation](#)
 - [raw](#)
 - [no raw](#)
- [ecli/mac-ip-anti-spoof.cdl](#)
 - [mac-ip-anti-spoof](#)
 - [interface](#)
 - [interface](#)
 - [cache entry](#)
 - [no cache entry](#)
 - [cache entry](#)
 - [no cache entry](#)
 - [no cache entries](#)
 - [router](#)
 - [no router](#)
 - [blacklisted](#)
 - [no blacklisted](#)
 - [ip](#)
 - [mac](#)
 - [interface](#)
 - [clear cache statistics](#)
 - [clear spoof-detected-list](#)
 - [resolve](#)
 - [router](#)
 - [no router](#)
 - [blacklisted](#)
 - [no blacklisted](#)
 - [ip](#)
 - [mac](#)
 - [interface](#)
 - [clear cache statistics](#)
 - [clear spoof-detected-list](#)
 - [resolve](#)
 - [enable](#)
 - [no enable](#)
 - [static-arp](#)
 - [no static-arp](#)
 - [dhcp-server](#)
 - [no dhcp-server](#)

- [dhcp-relay](#)
- [no dhcp-relay](#)
- [arp-lock](#)
- [no arp-lock](#)
- [arp-watch](#)
- [no arp-watch](#)
- [enforce-ingress](#)
- [no enforce-ingress](#)
- [spoof-detection](#)
- [no spoof-detection](#)
- [allow-management](#)
- [no allow-management](#)
- [enable](#)
- [no enable](#)
- [static-ndp](#)
- [no static-ndp](#)
- [ndp-lock](#)
- [no ndp-lock](#)
- [enforce-ingress](#)
- [no enforce-ingress](#)
- [spoof-detection](#)
- [no spoof-detection](#)
- [allow-management](#)
- [no allow-management](#)
- [ecli/nat.cdl](#)
 - [no nat-policy inbound](#)
 - [no nat-policy ipv6 inbound](#)
 - [no nat-policy uuid](#)
 - [no nat-policy name](#)
 - [no nat-policy ipv6 uuid](#)
 - [no nat-policy ipv6 name](#)
 - [no nat-policies](#)
 - [nat-policy inbound](#)
 - [nat-policy ipv6 inbound](#)
 - [nat-policy uuid](#)
 - [nat-policy name](#)
 - [nat-policy ipv6 uuid](#)
 - [nat-policy ipv6 name](#)
 - [no nat-policy nat64 inbound](#)
 - [no nat-policy nat64 uuid](#)
 - [no nat-policy nat64 name](#)
 - [nat-policy nat64 inbound](#)
 - [nat-policy nat64 uuid](#)
 - [nat-policy nat64 name](#)
 - [uuid](#)
 - [no uuid](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [no name](#)
 - [priority](#)
 - [comment](#)
 - [no comment](#)
 - [enable](#)
 - [no enable](#)
 - [inbound](#)
 - [outbound](#)
 - [destination](#)
 - [source](#)
 - [service](#)
 - [reflexive](#)
 - [no reflexive](#)
 - [translated-destination](#)
 - [translated-source](#)
 - [translated-service](#)
 - [override-mac](#)
 - [source](#)
 - [translated-source](#)
 - [pref64](#)
 - [virtual-group](#)
 - [high-availability](#)
 - [nat-method](#)
 - [source-port-remap](#)
 - [no source-port-remap](#)
 - [probing](#)
 - [no probing](#)
 - [probe-every](#)
 - [probe-type](#)
 - [reply-timeout](#)
 - [deactivate-after](#)
 - [reactivate-after](#)
 - [rst-as-miss](#)
 - [no rst-as-miss](#)
 - [port-probing](#)
 - [no port-probing](#)
- [ecli/network-monitor.cdl](#)
 - [no network-monitor policy](#)
 - [no network-monitor policies](#)

- [clear network-monitor statistics](#)
- [network-monitor policy](#)
- [name](#)
- [no probe target](#)
- [probe target](#)
- [next-hop](#)
- [no next-hop](#)
- [local-ip](#)
- [no local-ip](#)
- [outbound-interface](#)
- [probe type](#)
- [probe interval](#)
- [reply-timeout](#)
- [interval missed](#)
- [interval successful](#)
- [must-respond](#)
- [no must-respond](#)
- [rst-as-miss](#)
- [no rst-as-miss](#)
- [comment](#)
- [no comment](#)
- ecli/routing.cdl
 - [routing](#)
 - [mode](#)
 - [nsm](#)
 - [ospf](#)
 - [rip](#)
 - [ospfv3](#)
 - [ripng](#)
 - [no bgp](#)
 - [bgp](#)
 - [default-route-metric](#)
 - [metric-priority](#)
 - [no metric-priority](#)
 - [no route-policy interface](#)
 - [no route-policy ipv6 interface](#)
 - [no route-policy uuid](#)
 - [no route-policy ipv6 uuid](#)
 - [no route-policies](#)
 - [route-policy interface](#)
 - [route-policy ipv6 interface](#)
 - [route-policy uuid](#)
 - [uuid](#)
 - [no uuid](#)
 - [route-policy ipv6 uuid](#)
 - [uuid](#)
 - [no uuid](#)
 - [source](#)
 - [destination](#)
 - [service](#)
 - [app](#)
 - [gateway](#)
 - [path-selection-profile](#)
 - [no path-selection-profile](#)
 - [interface](#)
 - [gateway2](#)
 - [interface2](#)
 - [gateway3](#)
 - [interface3](#)
 - [gateway4](#)
 - [interface4](#)
 - [nexthop-number](#)
 - [metric](#)
 - [no name](#)
 - [name](#)
 - [no comment](#)
 - [comment](#)
 - [disable-on-interface-down](#)
 - [no disable-on-interface-down](#)
 - [vpn-precedence](#)
 - [no vpn-precedence](#)
 - [tcp-acceleration](#)
 - [no tcp-acceleration](#)
 - [wxa-group](#)
 - [no wxa-group](#)
 - [auto-add-access-rules](#)
 - [no auto-add-access-rules](#)
 - [probe](#)
 - [no probe](#)
 - [disable-when-probes-succeed](#)
 - [no disable-when-probes-succeed](#)
 - [default-probe-state-up](#)
 - [no default-probe-state-up](#)
 - [ipv6 default-route-metric](#)
- ecli/web-proxy.cdl
 - [web-proxy](#)
 - [no server](#)
 - [server](#)
 - [bypass-upon-failure](#)
 - [no bypass-upon-failure](#)

- [forward-public-requests](#)
- [no forward-public-requests](#)
- [user-proxy-server](#)
- [no user-proxy-server](#)
- [no user-proxy-servers](#)
- ecli/neighbor-discovery.cdl
 - [no ndp entry](#)
 - [no ndp entries](#)
 - [ndp reachable-time](#)
 - [no ndp reachable-time](#)
 - [ndp entry](#)
 - [ip](#)
 - [mac](#)
 - [interface](#)
 - [clear ndp cache entries](#)
 - [clear ndp cache entry](#)
- ecli/interface-ipv6.cdl
 - [tunnel-interface ipv6](#)
 - [no tunnel-interface ipv6](#)
 - [name](#)
 - [zone](#)
 - [no zone](#)
 - [type](#)
 - [ip](#)
 - [no ip](#)
 - [prefix-length](#)
 - [comment](#)
 - [no comment](#)
 - [management](#)
 - [no management](#)
 - [user-login](#)
 - [no user-login](#)
 - [https-redirect](#)
 - [no https-redirect](#)
 - [remote ipv4-address](#)
 - [no remote ipv4-address](#)
 - [remote ipv6-network](#)
 - [no remote ipv6-network](#)
 - [bound-to](#)
 - [link-mtu](#)
 - [remote ipv4-address](#)
 - [no remote ipv4-address](#)
 - [remote ipv6-network](#)
 - [no remote ipv6-network](#)
 - [bound-to](#)
 - [link-mtu](#)
 - [bound-to](#)
 - [enable](#)
 - [no enable](#)
 - [link-mtu](#)
 - [bound-to](#)
 - [no bound-to](#)
 - [dynamic](#)
 - [no dynamic](#)
 - [6rd prefix](#)
 - [no 6rd prefix](#)
 - [6rd prefix-length](#)
 - [no 6rd prefix-length](#)
 - [border-relay-ipv4-address](#)
 - [no border-relay-ipv4-address](#)
 - [mask-length](#)
 - [no mask-length](#)
 - [link-mtu](#)
 - [default-route](#)
 - [no default-route](#)
 - [bound-to](#)
 - [no bound-to](#)
 - [prefix](#)
 - [no prefix](#)
 - [link-mtu](#)
 - [ipv6-traffic](#)
 - [no ipv6-traffic](#)
 - [listen-router-advertisement](#)
 - [no listen-router-advertisement](#)
 - [stateless-address-autoconfig](#)
 - [no stateless-address-autoconfig](#)
 - [duplicate-address-detection-transmits](#)
 - [no duplicate-address-detection-transmits](#)
 - [reachable-time](#)
 - [no reachable-time](#)
 - [max ndp-size](#)
 - [no max ndp-size](#)
 - [ip-assignment](#)
 - [no ip-assignment](#)
 - [ip](#)
 - [no ip](#)
 - [prefix-length](#)
 - [dns primary](#)
 - [dns secondary](#)
 - [dns tertiary](#)

- [no dns primary](#)
- [no dns secondary](#)
- [no dns tertiary](#)
- [gateway](#)
- [no gateway](#)
- [advertise subnet-prefix](#)
- [no advertise subnet-prefix](#)
- [extra-ip](#)
- [no extra-ip](#)
- [no extra-ipv6-addresses](#)
- [router-advertisement](#)
- [multicast](#)
- [no multicast](#)
- [type](#)
- [ip](#)
- [prefix-length](#)
- [delegated-prefix](#)
- [no delegated-prefix](#)
- [preferred ip](#)
- [preferred prefix-length](#)
- [no preferred prefix-length](#)
- [advertise subnet-prefix](#)
- [no advertise subnet-prefix](#)
- [enable](#)
- [no enable](#)
- [interval](#)
- [link-mtu](#)
- [no link-mtu](#)
- [reachable-time](#)
- [no reachable-time](#)
- [retransmit-timer](#)
- [no retransmit-timer](#)
- [current-hop-limit](#)
- [no current-hop-limit](#)
- [router lifetime](#)
- [no router lifetime](#)
- [router preference](#)
- [managed](#)
- [no managed](#)
- [other-config](#)
- [no other-config](#)
- [prefix](#)
- [no prefix](#)
- [no prefixes](#)
- [prefix](#)
- [valid-lifetime](#)
- [preferred lifetime](#)
- [on-link](#)
- [no on-link](#)
- [autonomous](#)
- [no autonomous](#)
- [prefix-delegation](#)
- [no prefix-delegation](#)
- [preferred](#)
- [no preferred](#)
- [send-hints](#)
- [no send-hints](#)
- [rapid-commit](#)
- [no rapid-commit](#)
- [send-hints](#)
- [no send-hints](#)
- [aftr-name-option](#)
- [no aftr-name-option](#)
- [mode](#)
- [info-only](#)
- [no info-only](#)
- [release](#)
- [renew](#)
- [mode-assignment](#)
- [reconnect](#)
- [no reconnect](#)
- [schedule](#)
- [inactivity](#)
- [no inactivity](#)
- [lcp-echo-packets](#)
- [no lcp-echo-packets](#)
- [server-keepalive](#)
- [no server-keepalive](#)
- [ecli/dhcp-server-ipv6.cdl](#)
 - [enable](#)
 - [no enable](#)
 - [option](#)
 - [option object](#)
 - [no option object](#)
 - [no option objects](#)
 - [name](#)
 - [number](#)
 - [array](#)
 - [no array](#)
 - [value](#)
 - [no value](#)

- [option_group](#)
- [no_option_group](#)
- [no_option_groups](#)
- [name](#)
- [option_object](#)
- [no_option_object](#)
- [option_group](#)
- [no_option_group](#)
- [scope_dynamic](#)
- [no_scope_dynamic](#)
- [no_scopes_dynamic](#)
- [name](#)
- [enable](#)
- [no_enable](#)
- [prefix](#)
- [no_prefix](#)
- [range](#)
- [no_range](#)
- [lifetime_valid](#)
- [no_lifetime_valid](#)
- [lifetime_preferred](#)
- [no_lifetime_preferred](#)
- [comment](#)
- [no_comment](#)
- [always-send-option](#)
- [no_always-send-option](#)
- [domain-name](#)
- [no_domain-name](#)
- [dns_server](#)
- [no_dns_server](#)
- [generic-option](#)
- [no_generic-option](#)
- [scope_static](#)
- [no_scope_static](#)
- [no_scopes_static](#)
- [enable](#)
- [no_enable](#)
- [name](#)
- [no_name](#)
- [prefix](#)
- [no_prefix](#)
- [ip](#)
- [no_ip](#)
- [iaid](#)
- [no_iaid](#)
- [duid](#)
- [no_duid](#)
- [lifetime](#)
- [no_lifetime](#)
- [comment](#)
- [no_comment](#)
- [always-send-option](#)
- [no_always-send-option](#)
- [domain-name](#)
- [no_domain-name](#)
- [dns_server](#)
- [no_dns_server](#)
- [generic-option](#)
- [no_generic-option](#)
- [clear_lease](#)
- [clear_leases](#)
- [ecli/vlan-translation.cdl](#)
 - [vlan-translation](#)
 - [no_vlan-translation](#)
 - [no_vlan-translations](#)
 - [ingress_interface](#)
 - [ingress_vlan](#)
 - [egress_interface](#)
 - [egress_vlan](#)
 - [reverse](#)
 - [no_reverse](#)
- [ecli/dns-security.cdl](#)
 - [dns-security](#)
 - [dns-sinkhole](#)
 - [enable](#)
 - [no_enable](#)
 - [action-type](#)
 - [no_custom-malicious-entries](#)
 - [no_custom-malicious-entry](#)
 - [custom-malicious-entry](#)
 - [no_white-list-entries](#)
 - [no_white-list-entry](#)
 - [white-list-entry](#)
 - [dns-tunnel](#)
 - [enable](#)
 - [no_enable](#)
 - [block-all](#)
 - [no_block-all](#)
 - [no_white-list-entries](#)
 - [no_white-list-entry](#)

- [white-list-entry](#)
- [block](#)
- [no block](#)
- ecli/interface_show.cdl
 - [show tunnel-interface 4to6](#)
 - [show tunnel-interfaces 4to6](#)
 - [show interfaces](#)
 - [show interface](#)
 - [show tunnel-interface vpn](#)
 - [show tunnel-interfaces vpn](#)
 - [show dialup](#)
- ecli/arp_show.cdl
 - [show arp](#)
- ecli/dns_show.cdl
 - [show dns](#)
- ecli/ddns_show.cdl
 - [show dynamic-dns profiles](#)
 - [show dynamic-dns profile](#)
- ecli/dhcp-server_show.cdl
 - [show dhcp-server](#)
- ecli/failover-load-balancing_show.cdl
 - [show failover-lb](#)
- ecli/ip-helper_show.cdl
 - [show ip-helper](#)
- ecli/mac-ip-anti-spoof_show.cdl
 - [show mac-ip-anti-spoof](#)
- ecli/nat_show.cdl
 - [show nat-policies](#)
 - [show nat-policy ipv4 inbound](#)
 - [show nat-policy ipv6 inbound](#)
 - [show nat-policy nat64 inbound](#)
 - [show nat-policy ipv4 uuid](#)
 - [show nat-policy ipv6 uuid](#)
 - [show nat-policy nat64 uuid](#)
 - [show nat-policy ipv4 name](#)
 - [show nat-policy ipv6 name](#)
 - [show nat-policy nat64 name](#)
- ecli/network-monitor_show.cdl
 - [show network-monitor policies](#)
 - [show network-monitor policy](#)
- ecli/routing_show.cdl
 - [show routing mode](#)
 - [show route-policies](#)
 - [show route-policy ipv4 interface](#)
 - [show route-policy ipv6 interface](#)
 - [show route-policy ipv4 uuid](#)
 - [show route-policy ipv6 uuid](#)
 - [show route-policy ipv4 name](#)
 - [show route-policy ipv6 name](#)
 - [show routing nsm](#)
 - [show routing rip](#)
 - [show routing ospf](#)
 - [show routing bgp](#)
 - [show routing ripng](#)
 - [show routing ospfv3](#)
- ecli/web-proxy_show.cdl
 - [show web-proxy](#)
- ecli/neighbor-discovery_show.cdl
 - [show ndp](#)
- ecli/interface-ipv6_show.cdl
 - [show tunnel-interface ipv6](#)
 - [show tunnel-interfaces ipv6](#)
- ecli/vlan-translation_show.cdl
 - [show vlan-translation](#)
 - [show vlan-translations](#)
- ecli/dns-security_show.cdl
 - [show dns-security](#)
- ecli/firewall.cdl
 - [firewall](#)
 - [stealth-mode](#)
 - [no stealth-mode](#)
 - [randomize-id](#)
 - [no randomize-id](#)
 - [decrement ttl](#)
 - [no decrement ttl](#)
 - [icmp time-exceeded-packets](#)
 - [no icmp time-exceeded-packets](#)

- [ftp-transforms-in-service-object](#)
- [sqlnet](#)
- [no sqlnet](#)
- [rtsp-transformations](#)
- [no rtsp-transformations](#)
- [drop source-routed](#)
- [no drop source-routed](#)
- [starting-vlan](#)
- [connections](#)
- [force-ftp-data](#)
- [no force-ftp-data](#)
- [apply-rules-for-intra-lan](#)
- [no apply-rules-for-intra-lan](#)
- [issue-rst-for-outgoing-discards](#)
- [no issue-rst-for-outgoing-discards](#)
- [icmp redirect-on-lan](#)
- [no icmp redirect-on-lan](#)
- [ip checksum-enforcement](#)
- [no ip checksum-enforcement](#)
- [udp checksum-enforcement](#)
- [no udp checksum-enforcement](#)
- [jumbo-frame](#)
- [no jumbo-frame](#)
- [ipv6 drop](#)
- [no ipv6 drop](#)
- [ipv6 decrement hop-limit](#)
- [no ipv6 decrement hop-limit](#)
- [ipv6 icmp](#)
- [no ipv6 icmp](#)
- [ipv6 site-local-unicast](#)
- [no ipv6 site-local-unicast](#)
- [ipv6 extension-header-check](#)
- [no ipv6 extension-header-check](#)
- [ipv6 extension-header-order-check](#)
- [no ipv6 extension-header-order-check](#)
- [ipv6 netbios-for-isatap](#)
- [no ipv6 netbios-for-isatap](#)
- [control-plane-flood-protection](#)
- [no control-plane-flood-protection](#)
- ecli/bwm.cdl
 - [bandwidth-management](#)
 - [no type](#)
 - [type](#)
 - [priority](#)
 - [no priority](#)
- ecli/multicast.cdl
 - [no multicast](#)
 - [multicast](#)
 - [require-igmp-membership](#)
 - [no require-igmp-membership](#)
 - [reception](#)
 - [clear multicast state-entries](#)
 - [clear multicast state-entry](#)
- ecli/policy.cdl
 - [no access-rule from](#)
 - [clear access-rule statistics](#)
 - [access-rule from](#)
 - [access-rule uuid](#)
 - [no access-rule uuid](#)
 - [access-rule name](#)
 - [no access-rule name](#)
 - [access-rule restore-defaults](#)
 - [no access-rule ipv6 from](#)
 - [access-rule ipv6 from](#)
 - [no access-rule ipv6 uuid](#)
 - [access-rule ipv6 uuid](#)
 - [access-rule ipv6 name](#)
 - [no access-rule ipv6 name](#)
 - [access-rule ipv6 restore-defaults](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [no name](#)
 - [from](#)
 - [to](#)
 - [action](#)
 - [max-connections](#)
 - [priority](#)
 - [tcp timeout](#)
 - [udp timeout](#)
 - [fragments](#)
 - [no fragments](#)
 - [botnet-filter](#)
 - [no botnet-filter](#)
 - [comment](#)
 - [no comment](#)
 - [connection-limit destination](#)
 - [no connection-limit destination](#)
 - [connection-limit source](#)

- [no connection-limit source](#)
- [tcp urgent](#)
- [no tcp urgent](#)
- [dpi](#)
- [no dpi](#)
- [dpi-ssl](#)
- [no dpi-ssl](#)
- [destination address](#)
- [service](#)
- [enable](#)
- [no enable](#)
- [flow-reporting](#)
- [no flow-reporting](#)
- [geo-ip-filter](#)
- [no geo-ip-filter](#)
- [logging](#)
- [no logging](#)
- [sip](#)
- [no sip](#)
- [h323](#)
- [no h323](#)
- [packet-monitoring](#)
- [no packet-monitoring](#)
- [management](#)
- [no management](#)
- [single-sign-on](#)
- [no single-sign-on](#)
- [quality-of-service class-of-service](#)
- [cos-override](#)
- [no cos-override](#)
- [no quality-of-service](#)
- [quality-of-service dscp](#)
- [reflexive](#)
- [no reflexive](#)
- [schedule](#)
- [source address](#)
- [source port](#)
- [users included](#)
- [users excluded](#)
- [bandwidth-management](#)
- [bandwidth-management](#)
- [egress](#)
- [no egress](#)
- [ingress](#)
- [no ingress](#)
- [usage-tracking](#)
- [no usage-tracking](#)
- [ecli/ssl-control.cdl](#)
 - [ssl-control](#)
 - [enable](#)
 - [no enable](#)
 - [action](#)
 - [blacklist](#)
 - [no blacklist](#)
 - [detect ssl-v2](#)
 - [no detect ssl-v2](#)
 - [detect ssl-v3](#)
 - [no detect ssl-v3](#)
 - [detect weak-ciphers](#)
 - [no detect weak-ciphers](#)
 - [whitelist](#)
 - [no whitelist](#)
 - [detect self-signed](#)
 - [no detect self-signed](#)
 - [detect weak-digest-cert](#)
 - [no detect weak-digest-cert](#)
 - [detect expired](#)
 - [no detect expired](#)
 - [detect untrusted-ca](#)
 - [no detect untrusted-ca](#)
 - [detect tls-v1](#)
 - [no detect tls-v1](#)
 - [blacklist-certificate](#)
 - [no blacklist-certificate](#)
 - [no blacklist-certificates](#)
 - [whitelist-certificate](#)
 - [no whitelist-certificate](#)
 - [no whitelist-certificates](#)
- [ecli/tcp.cdl](#)
 - [tcp](#)
 - [enforce-strict-compliance](#)
 - [no enforce-strict-compliance](#)
 - [handshake-enforcement](#)
 - [no handshake-enforcement](#)
 - [checksum-enforcement](#)
 - [no checksum-enforcement](#)
 - [drop syn-with-data](#)
 - [no drop syn-with-data](#)
 - [handshake-timeout](#)
 - [no handshake-timeout](#)

- [default-connection-timeout](#)
- [maximum-segment-lifetime](#)
- [syn-flood-protection-mode](#)
- [syn-attack-threshold](#)
- [support-tcp-sack](#)
- [no support-tcp-sack](#)
- [limit-mss](#)
- [no limit-mss](#)
- [always-log-syn-packets](#)
- [no always-log-syn-packets](#)
- [proxy-connections](#)
- [no proxy-connections](#)
- [syn-flood-blacklisting](#)
- [no syn-flood-blacklisting](#)
- [blacklist-threshold](#)
- [never-blacklist-wan](#)
- [no never-blacklist-wan](#)
- [always-allow-management](#)
- [no always-allow-management](#)
- [ddos on-wan-interfaces](#)
- [no ddos on-wan-interfaces](#)
- [ddos threshold](#)
- [no ddos threshold](#)
- [ddos filter-bypass-rate](#)
- [no ddos filter-bypass-rate](#)
- [ddos allow-list-timeout](#)
- [no ddos allow-list-timeout](#)
- [ddos always-allow-management](#)
- [no ddos always-allow-management](#)
- [ddos always-allow-negotiation](#)
- [no ddos always-allow-negotiation](#)
- [clear tcp statistics](#)
- ecli/bandwidth-object.cdl
 - [no bandwidth-object](#)
 - [no bandwidth-objects](#)
 - [bandwidth-object](#)
 - [name](#)
 - [guaranteed](#)
 - [maximum](#)
 - [priority](#)
 - [action](#)
 - [comment](#)
 - [no comment](#)
 - [per-ip-management](#)
 - [no per-ip-management](#)
- ecli/udp.cdl
 - [udp](#)
 - [default-connection-timeout](#)
 - [flood protection](#)
 - [no flood protection](#)
 - [flood attack-threshold](#)
 - [flood block-timeout](#)
 - [flood protected-dest-list](#)
 - [clear udp statistics](#)
- ecli/icmp.cdl
 - [icmp](#)
 - [flood protection](#)
 - [no flood protection](#)
 - [flood attack-threshold](#)
 - [flood block-timeout](#)
 - [flood protected-dest-list](#)
 - [clear icmp statistics](#)
- ecli/qos-mapping.cdl
 - [qos-mapping cos](#)
 - [qos-mapping reset](#)
- ecli/firewall_show.cdl
 - [show firewall](#)
- ecli/bwm_show.cdl
 - [show bandwidth-management](#)
- ecli/multicast_show.cdl
 - [show multicast](#)
- ecli/policy_show.cdl
 - [show access-rule ipv4 from](#)
 - [show access-rule ipv4 uuid](#)
 - [show access-rule ipv4 name](#)
 - [show access-rules](#)
 - [show access-rule ipv6 from](#)
 - [show access-rule ipv6 uuid](#)
 - [show access-rule ipv6 name](#)
- ecli/ssl-control_show.cdl
 - [show ssl-control](#)
- ecli/tcp_show.cdl
 - [show tcp](#)

- ecli/bandwidth-object_show.cdl
 - [show bandwidth-objects](#)
 - [show bandwidth-object](#)
- ecli/udp_show.cdl
 - [show udp](#)
- ecli/icmp_show.cdl
 - [show icmp](#)
- ecli/qos-mapping_show.cdl
 - [show qos-mapping](#)
- ecli/administration.cdl
 - [administration](#)
 - [firewall-name](#)
 - [no firewall-name](#)
 - [firewall-domain-name](#)
 - [no firewall-domain-name](#)
 - [language-override](#)
 - [no language-override](#)
 - [admin name](#)
 - [admin password](#)
 - [admin one-time-password totp](#)
 - [no admin one-time-password](#)
 - [admin unbind-totp-key](#)
 - [wireless-lan](#)
 - [no wireless-lan](#)
 - [ipv6](#)
 - [no ipv6](#)
 - [password aging](#)
 - [no password aging](#)
 - [password uniqueness](#)
 - [no password uniqueness](#)
 - [password enforce-character-difference](#)
 - [no password enforce-character-difference](#)
 - [password minimum-length](#)
 - [password complexity alpha-and-numeric-and-symbols](#)
 - [password complexity alpha-and-numeric](#)
 - [password complexity type](#)
 - [password complexity upper-case](#)
 - [password complexity lower-case](#)
 - [password complexity digital](#)
 - [password complexity symbolic](#)
 - [no password complexity](#)
 - [password constraints-apply-to](#)
 - [no password constraints-apply-to](#)
 - [idle-logout-time](#)
 - [user-lockout](#)
 - [no user-lockout](#)
 - [local-user-lockout](#)
 - [no local-user-lockout](#)
 - [log-without-lockout](#)
 - [no log-without-lockout](#)
 - [admin preempt-action](#)
 - [admin preempt-inactivity-timeout](#)
 - [inter-admin-messaging](#)
 - [no inter-admin-messaging](#)
 - [multiple-admin](#)
 - [no multiple-admin](#)
 - [enhanced-audit-logging](#)
 - [no enhanced-audit-logging](#)
 - [wireless-controller-mode](#)
 - [web-management allow-http](#)
 - [no web-management allow-http](#)
 - [http-port](#)
 - [https-port](#)
 - [web-management certificate](#)
 - [web-management cert-common-name](#)
 - [no web-management cert-common-name](#)
 - [web-management client-certificate-check](#)
 - [no web-management client-certificate-check](#)
 - [web-management client-certificate-issuer](#)
 - [web-management oosp-check](#)
 - [no web-management oosp-check](#)
 - [web-management default-table-size](#)
 - [web-management refresh-interval](#)
 - [web-management tooltip](#)
 - [no web-management tooltip](#)
 - [dashboard-as-starting-page](#)
 - [no dashboard-as-starting-page](#)
 - [tls-and-above](#)
 - [no tls-and-above](#)
 - [out-of-band-management](#)
 - [no out-of-band-management](#)
 - [override-download-url sonicpoint n](#)
 - [no override-download-url sonicpoint n](#)
 - [override-download-url sonicpoint nv](#)
 - [no override-download-url sonicpoint nv](#)
 - [override-download-url sonicpoint ndr](#)
 - [no override-download-url sonicpoint ndr](#)
 - [override-download-url sonicpoint ac](#)

- [no override-download-url sonicpoint ac](#)
- [gms-management](#)
- [no gms-management](#)
- [host-name](#)
- [syslog-server-port](#)
- [no syslog-server-port](#)
- [heartbeat-status-only](#)
- [no heartbeat-status-only](#)
- [behind-nat-device](#)
- [no behind-nat-device](#)
- [spi](#)
- [encryption-type](#)
- [encryption-key](#)
- [authentication-key](#)
- [reporting-server](#)
- [no reporting-server](#)
- [sonicos-api](#)
- [no sonicos-api](#)
- [digest](#)
- [no digest](#)
- [sha256-digest](#)
- [no sha256-digest](#)
- [md5-digest](#)
- [no md5-digest](#)
- [integrity-protection](#)
- [no integrity-protection](#)
- [chap](#)
- [no chap](#)
- [basic](#)
- [no basic](#)
- [public-key](#)
- [no public-key](#)
- [rsa-key-size](#)
- [rsa-padding-type](#)
- [session-security](#)
- [no session-security](#)
- [hold-password](#)
- [no hold-password](#)
- [max-nonce](#)
- [two-factor-bearer-token](#)
- [no two-factor-bearer-token](#)
- [ecli/snmp.cdl](#)
 - [snmp](#)
 - [no snmp](#)
 - [system-name](#)
 - [no system-name](#)
 - [system-contact](#)
 - [no system-contact](#)
 - [system-location](#)
 - [no system-location](#)
 - [asset-number](#)
 - [no asset-number](#)
 - [get-community-name](#)
 - [no get-community-name](#)
 - [trap-community-name](#)
 - [no trap-community-name](#)
 - [host](#)
 - [no host](#)
 - [snmp3 mandatory](#)
 - [no snmp3 mandatory](#)
 - [snmp3 engine-id](#)
 - [snmp3 increase-subsystem-priority](#)
 - [no snmp3 increase-subsystem-priority](#)
 - [view](#)
 - [no view](#)
 - [group](#)
 - [no group](#)
 - [user](#)
 - [no user](#)
 - [name](#)
 - [security-level](#)
 - [no security-level](#)
 - [authentication](#)
 - [encryption](#)
 - [group](#)
 - [no group](#)
 - [access](#)
 - [no access](#)
 - [name](#)
 - [read-view](#)
 - [master-group](#)
 - [security-level](#)
 - [no security-level](#)
- [ecli/export.cdl](#)
 - [export current-config](#)
 - [export pending-config](#)
 - [export firmware](#)
 - [export tech-support-report](#)
- [ecli/firmware.cdl](#)

- [firmware auto](#)
- [no firmware auto](#)
- [firmware diagnostics](#)
- [no firmware diagnostics](#)
- [firmware backup](#)
- ecli/import.cdl
 - [import firmware](#)
 - [import cli](#)
- ecli/system.cdl
 - [restart](#)
 - [safemode](#)
 - [restore-defaults](#)
 - [boot](#)
- ecli/time.cdl
 - [time](#)
 - [time](#)
 - [date](#)
 - [time-zone](#)
 - [use-ntp](#)
 - [no use-ntp](#)
 - [daylight-savings](#)
 - [no daylight-savings](#)
 - [universal](#)
 - [no universal](#)
 - [international-format](#)
 - [no international-format](#)
 - [only-custom-ntp](#)
 - [no only-custom-ntp](#)
 - [ntp-server](#)
 - [no ntp-server](#)
 - [no ntp-servers](#)
 - [ntp-update-interval](#)
- ecli/license.cdl
 - [license](#)
 - [synchronize](#)
 - [upgrade](#)
- ecli/ssh-server.cdl
 - [ssh server](#)
 - [port](#)
 - [keygen](#)
 - [restart](#)
 - [enable](#)
 - [terminate](#)
 - [kill session](#)
 - [kill sessions](#)
- ecli/ssh.cdl
 - [ssh client](#)
 - [server-key](#)
 - [no server-key](#)
 - [no server-keys](#)
- ecli/fips.cdl
 - [fips](#)
 - [no fips](#)
- ecli/ndpp.cdl
 - [ndpp](#)
 - [no ndpp](#)
- ecli/administration_show.cdl
 - [show administration](#)
- ecli/snmp_show.cdl
 - [show snmp](#)
- ecli/firmware_show.cdl
 - [show firmware](#)
- ecli/status_show.cdl
 - [show status](#)
- ecli/time_show.cdl
 - [show time](#)
- ecli/version_show.cdl
 - [show version](#)
- ecli/license_show.cdl
 - [show license](#)
- ecli/ssh-server_show.cdl
 - [show ssh server](#)
- ecli/ssh_show.cdl
 - [show ssh client](#)
- ecli/fips_show.cdl
 - [show fips](#)

- ecli/ndpp_show.cdl
 - [show ndpp](#)
- ecli/user-auth.cdl
 - [user authentication](#)
 - [method](#)
 - [sso-method](#)
 - [no sso-method](#)
 - [case-sensitive-names](#)
 - [no case-sensitive-names](#)
 - [login-uniqueness](#)
 - [no login-uniqueness](#)
 - [relogin-after-password-change](#)
 - [no relogin-after-password-change](#)
 - [one-time-password format](#)
 - [one-time-password length](#)
 - [one-time-password email-format](#)
 - [auth-page-timeout](#)
 - [no auth-page-timeout](#)
 - [browser-redirect-via](#)
 - [http-redirect-after-login](#)
 - [no http-redirect-after-login](#)
 - [policy-banner](#)
 - [no policy-banner](#)
 - [radius-chap-http-login](#)
 - [no radius-chap-http-login](#)
 - [inactivity-timeout](#)
 - [prevent-inactivity-logout service](#)
 - [no prevent-inactivity-logout service](#)
 - [log-user-name](#)
 - [no log-user-name](#)
 - [user-connections-logout](#)
 - [inactive-user](#)
 - [no inactive-user](#)
 - [age-out](#)
 - [web-login-session-limit](#)
 - [no web-login-session-limit](#)
 - [show-user-status-window](#)
 - [no show-user-status-window](#)
 - [status-window-heartbeat](#)
 - [disconnected-user-detect](#)
 - [no disconnected-user-detect](#)
 - [open-in-same-window](#)
 - [no open-in-same-window](#)
 - [rule-auth-bypass-http-url](#)
 - [no rule-auth-bypass-http-url](#)
 - [acceptable-use-policy](#)
 - [window-size](#)
 - [scroll-bars](#)
 - [no scroll-bars](#)
 - [content](#)
 - [no content](#)
 - [aup-on-zones](#)
 - [no aup-on-zones](#)
 - [customize-login-page](#)
 - [no customize-login-page](#)
- ecli/user-local.cdl
 - [user local](#)
 - [apply-password-constraints](#)
 - [no apply-password-constraints](#)
 - [prune-on-expiry](#)
 - [no prune-on-expiry](#)
 - [user](#)
 - [no user](#)
 - [no users](#)
 - [group](#)
 - [no group](#)
 - [no groups](#)
 - [name](#)
 - [uuid](#)
 - [no uuid](#)
 - [domain](#)
 - [no domain](#)
 - [comment](#)
 - [no comment](#)
 - [password](#)
 - [no password](#)
 - [force-password-change](#)
 - [no force-password-change](#)
 - [expiration](#)
 - [account-lifetime](#)
 - [no account-lifetime](#)
 - [prune-on-expiry](#)
 - [no prune-on-expiry](#)
 - [one-time-password](#)
 - [no one-time-password](#)
 - [unbind-totp-key](#)
 - [email-address](#)
 - [no email-address](#)
 - [vpn-client-access](#)
 - [no vpn-client-access](#)

- [guest-login-uniqueness](#)
- [no guest-login-uniqueness](#)
- [guest-idle-timeout](#)
- [no guest-idle-timeout](#)
- [no quota-cycle](#)
- [quota-cycle](#)
- [session-lifetime](#)
- [no session-lifetime](#)
- [limit](#)
- [no limit](#)
- [member-of](#)
- [no member-of](#)
- [name](#)
- [domain](#)
- [no domain](#)
- [comment](#)
- [no comment](#)
- [ldap-location](#)
- [no ldap-location](#)
- [memberships-by-ldap-location](#)
- [no memberships-by-ldap-location](#)
- [refresh-from-ldap-server](#)
- [one-time-password](#)
- [no one-time-password](#)
- [to-management-on-login](#)
- [no to-management-on-login](#)
- [vpn-client-access](#)
- [no vpn-client-access](#)
- [member](#)
- [no member](#)
- [uuid](#)
- [no uuid](#)
- [bookmark](#)
- [no bookmark](#)
- [no bookmarks](#)
- [name](#)
- [host](#)
- [no host](#)
- [service](#)
- [screen-size](#)
- [colors](#)
- [application-path](#)
- [no application-path](#)
- [start-in-folder](#)
- [no start-in-folder](#)
- [automatic-login](#)
- [no automatic-login](#)
- [plugin-dlls](#)
- [no plugin-dlls](#)
- [redirect-clipboard](#)
- [no redirect-clipboard](#)
- [redirect-audio](#)
- [no redirect-audio](#)
- [auto-reconnection](#)
- [no auto-reconnection](#)
- [desktop-background](#)
- [no desktop-background](#)
- [window-drag](#)
- [no window-drag](#)
- [animation](#)
- [no animation](#)
- [view-only](#)
- [no view-only](#)
- [share-desktop](#)
- [no share-desktop](#)
- [automatic-accept-host-key](#)
- [no automatic-accept-host-key](#)
- [display-on-mobile](#)
- [no display-on-mobile](#)
- [bookmark](#)
- [no bookmark](#)
- [no bookmarks](#)
- [name](#)
- [host](#)
- [no host](#)
- [service](#)
- [screen-size](#)
- [colors](#)
- [application-path](#)
- [no application-path](#)
- [start-in-folder](#)
- [no start-in-folder](#)
- [automatic-login](#)
- [no automatic-login](#)
- [plugin-dlls](#)
- [no plugin-dlls](#)
- [redirect-clipboard](#)
- [no redirect-clipboard](#)
- [redirect-audio](#)
- [no redirect-audio](#)
- [auto-reconnection](#)

- [no auto-reconnection](#)
- [desktop-background](#)
- [no desktop-back-ground](#)
- [window-drag](#)
- [no window-drag](#)
- [animation](#)
- [no animation](#)
- [view-only](#)
- [no view-only](#)
- [share-desktop](#)
- [no share-desktop](#)
- [automatic-accept-host-key](#)
- [no automatic-accept-host-key](#)
- [display-on-mobile](#)
- [no display-on-mobile](#)
- [ecli/user-mgmt.cdl](#)
 - [kill-user name](#)
 - [kill-user at](#)
 - [unlock](#)
 - [user management](#)
 - [include](#)
 - [no include](#)
- [ecli/user-radius.cdl](#)
 - [user radius](#)
 - [clear user radius statistics](#)
 - [local-users-only](#)
 - [no local-users-only](#)
 - [default-user-group](#)
 - [no default-user-group](#)
 - [timeout](#)
 - [retries](#)
 - [user-group-mechanism](#)
 - [server](#)
 - [no server](#)
 - [no servers](#)
 - [enable](#)
 - [no enable](#)
 - [host](#)
 - [port](#)
 - [partition](#)
 - [no partition](#)
 - [shared-secret](#)
 - [no shared-secret](#)
 - [send-through-vpn-tunnel](#)
 - [no send-through-vpn-tunnel](#)
 - [user-name-format](#)
 - [test](#)
 - [accounting](#)
 - [server](#)
 - [no server](#)
 - [no servers](#)
 - [enable](#)
 - [no enable](#)
 - [host](#)
 - [port](#)
 - [partition](#)
 - [no partition](#)
 - [shared-secret](#)
 - [no shared-secret](#)
 - [user-name-format](#)
 - [test](#)
 - [timeout](#)
 - [retries](#)
 - [data](#)
 - [no data](#)
 - [include](#)
 - [no include](#)
 - [interim-updates](#)
 - [no interim-updates](#)
- [ecli/user-ldap.cdl](#)
 - [user ldap](#)
 - [clear user ldap statistics](#)
 - [protocol-version](#)
 - [require-valid-certificate](#)
 - [no require-valid-certificate](#)
 - [local-tls-certificate](#)
 - [no local-tls-certificate](#)
 - [allow-referrals](#)
 - [no allow-referrals](#)
 - [allow-references](#)
 - [no allow-references](#)
 - [local-users-only](#)
 - [no local-users-only](#)
 - [default-user-group](#)
 - [no default-user-group](#)
 - [mirror-user-groups](#)
 - [no mirror-user-groups](#)
 - [exclude-tree](#)
 - [no exclude-tree](#)

- [relay](#)
- [enable](#)
- [no enable](#)
- [clients-connect](#)
- [no clients-connect](#)
- [shared-secret](#)
- [no shared-secret](#)
- [legacy-user-group](#)
- [no legacy-user-group](#)
- [server](#)
- [no server](#)
- [no servers](#)
- [save dynamic-secondary](#)
- [enable](#)
- [no enable](#)
- [host](#)
- [role](#)
- [port](#)
- [partition](#)
- [timeout](#)
- [use-tls](#)
- [no use-tls](#)
- [send-start-tls-request](#)
- [no send-start-tls-request](#)
- [backup-for](#)
- [no backup-for](#)
- [same-bind-credentials](#)
- [no same-bind-credentials](#)
- [schema](#)
- [read-from-server auto-configure](#)
- [read-from-server display](#)
- [user-class](#)
- [user-attribute](#)
- [no user-attribute](#)
- [user-group-class](#)
- [user-group-attribute](#)
- [no user-group-attribute](#)
- [directory](#)
- [read-trees-from-server](#)
- [primary-domain](#)
- [no primary-domain](#)
- [users-tree](#)
- [no users-tree](#)
- [user-groups-tree](#)
- [no user-groups-tree](#)
- [bind](#)
- [bind-password](#)
- [no bind-password](#)
- [referred-bind-with-account](#)
- [test](#)
- [ecli/user-partition.cdl](#)
 - [user partitioning](#)
 - [enable](#)
 - [no enable](#)
 - [partition](#)
 - [no partition](#)
 - [no partitions](#)
 - [name](#)
 - [parent-partition](#)
 - [no parent-partition](#)
 - [domain](#)
 - [no domain](#)
 - [no domains](#)
 - [comment](#)
 - [no comment](#)
 - [no policy](#)
 - [no policies](#)
 - [policy](#)
 - [zone](#)
 - [interface](#)
 - [address-object](#)
 - [partition](#)
 - [comment](#)
 - [no comment](#)
 - [auto-assign](#)
- [ecli/user-sso.cdl](#)
 - [user sso](#)
 - [clear user sso statistics](#)
 - [method](#)
 - [no method](#)
 - [next-agent-on-no-name](#)
 - [no next-agent-on-no-name](#)
 - [block-traffic](#)
 - [no block-traffic](#)
 - [including-for-access-rules](#)
 - [no including-for-access-rules](#)
 - [local-users-only](#)
 - [no local-users-only](#)
 - [non-domain-limited-access](#)
 - [no non-domain-limited-access](#)

- [probe](#)
- [no_probe](#)
- [user-group-mechanism](#)
- [poll_rate](#)
- [poll_same-agent](#)
- [no_poll_same-agent](#)
- [hold-time after-failure](#)
- [hold-time after-no-user](#)
- [windows-service-user-name](#)
- [no_windows-service-user-name](#)
- [security-service-bypass address](#)
- [no_security-service-bypass address](#)
- [security-service-bypass service](#)
- [no_security-service-bypass service](#)
- [address](#)
- [service](#)
- [type](#)
- [dummy-user](#)
- [no_dummy-user](#)
- [enforce-on-zone](#)
- [no_enforce-on-zone](#)
- [tsa-services-bypass](#)
- [no_tsa-services-bypass](#)
- [authentication-domain](#)
- [redirect-browser](#)
- [retries-on-failure](#)
- [poll_users](#)
- [forward-lanman](#)
- [no_forward-lanman](#)
- [radius-accounting.port](#)
- [agent](#)
- [no_agent](#)
- [no_agents](#)
- [host](#)
- [port](#)
- [enable](#)
- [no_enable](#)
- [timeout](#)
- [retries](#)
- [no_shared-key](#)
- [shared-key](#)
- [max-requests](#)
- [partition](#)
- [no_partition](#)
- [terminal-services-agent](#)
- [no_terminal-services-agent](#)
- [no_terminal-services-agents](#)
- [host](#)
- [port](#)
- [enable](#)
- [no_enable](#)
- [no_shared-key](#)
- [shared-key](#)
- [partition](#)
- [no_partition](#)
- [radius-accounting-client](#)
- [no_radius-accounting-client](#)
- [no_radius-accounting-clients](#)
- [host](#)
- [shared-secret](#)
- [no_shared-secret](#)
- [user-name-format](#)
- [missing-domain](#)
- [log-user-out](#)
- [no_log-user-out](#)
- [server](#)
- [no_server](#)
- [proxy-forward timeout](#)
- [proxy-forward retries](#)
- [proxy-forward type](#)
- [partition](#)
- [no_partition](#)
- [test](#)
- [ecli/user-guest.cdl](#)
 - [user.guest](#)
 - [profile](#)
 - [no_profile](#)
 - [user](#)
 - [generate](#)
 - [no_user](#)
 - [no_users](#)
 - [show-guest-status-window](#)
 - [no_show-guest-status-window](#)
 - [export.guest-accounts](#)
 - [logout.user](#)
 - [logout.users](#)
 - [name](#)
 - [generate](#)
 - [no_generate](#)
 - [name.prefix](#)
 - [comment](#)

- [no comment](#)
- [enable](#)
- [no enable](#)
- [activate-on-login](#)
- [no activate-on-login](#)
- [login-uniqueness](#)
- [no login-uniqueness](#)
- [prune-on-expiry](#)
- [no prune-on-expiry](#)
- [account-lifetime](#)
- [no quota-cycle](#)
- [quota-cycle](#)
- [session-lifetime](#)
- [idle-timeout](#)
- [limit](#)
- [no limit](#)
- [name](#)
- [uuid](#)
- [no uuid](#)
- [generate](#)
- [profile](#)
- [comment](#)
- [no comment](#)
- [password](#)
- [no password](#)
- [enable](#)
- [no enable](#)
- [activate-on-login](#)
- [no activate-on-login](#)
- [login-uniqueness](#)
- [no login-uniqueness](#)
- [prune-on-expiry](#)
- [no prune-on-expiry](#)
- [account-lifetime](#)
- [no quota-cycle](#)
- [quota-cycle](#)
- [session-lifetime](#)
- [no session-lifetime](#)
- [idle-timeout](#)
- [limit](#)
- [no limit](#)
- [ecli/user-auth_show.cdl](#)
 - [show user authentication](#)
- [ecli/user-local_show.cdl](#)
 - [show user local](#)
- [ecli/user-mgmt_show.cdl](#)
 - [show user status](#)
 - [show user statistics](#)
 - [show user management](#)
- [ecli/user-radius_show.cdl](#)
 - [show user radius](#)
- [ecli/user-ldap_show.cdl](#)
 - [show user ldap](#)
- [ecli/user-partition_show.cdl](#)
 - [show user partitioning](#)
- [ecli/user-sso_show.cdl](#)
 - [show user sso](#)
- [ecli/user-guest_show.cdl](#)
 - [show user guest](#)
- [ecli/appflow.cdl](#)
 - [appflow](#)
 - [clear flow-reporting statistics](#)
 - [default](#)
 - [report connections](#)
 - [real-time data-collection](#)
 - [no real-time data-collection](#)
 - [real-time collect-for](#)
 - [no real-time collect-for](#)
 - [aggregate data-collection](#)
 - [no aggregate data-collection](#)
 - [aggregate collect-for](#)
 - [no aggregate collect-for](#)
 - [flows-to local-collector](#)
 - [no flows-to local-collector](#)
 - [report dropped](#)
 - [no report dropped](#)
 - [report stack](#)
 - [no report stack](#)
 - [include-url-types](#)
 - [no include-url-types](#)
 - [geo-ip-resolution](#)
 - [no geo-ip-resolution](#)
 - [report ipv6-flows](#)
 - [no report ipv6-flows](#)

- [report upload-timeout](#)
- [gmsflow-server](#)
- [flows](#)
- [no flows](#)
- [real-time](#)
- [no real-time](#)
- [report open](#)
- [no report open](#)
- [report close](#)
- [no report close](#)
- [report update](#)
- [no report update](#)
- [dynamic-flows](#)
- [no dynamic-flows](#)
- [server-ip](#)
- [ip](#)
- [vpn-source-ip](#)
- [communication-timeout](#)
- [auto-synchronize](#)
- [no auto-synchronize](#)
- [synchronize](#)
- [test-connectivity](#)
- [appflow-server](#)
- [flows](#)
- [no flows](#)
- [real-time](#)
- [no real-time](#)
- [report open](#)
- [no report open](#)
- [report close](#)
- [no report close](#)
- [report update](#)
- [no report update](#)
- [dynamic-flows](#)
- [no dynamic-flows](#)
- [server-ip](#)
- [keep-alive](#)
- [no keep-alive](#)
- [ip](#)
- [vpn-source-ip](#)
- [max-flows](#)
- [communication-timeout](#)
- [firewall-name](#)
- [passphrase](#)
- [no passphrase](#)
- [auto-synchronize](#)
- [no auto-synchronize](#)
- [synchronize](#)
- [test-connectivity](#)
- [flush server](#)
- [flush servers](#)
- [discover](#)
- [external-collector](#)
- [flows](#)
- [no flows](#)
- [reporting-format](#)
- [ip](#)
- [vpn-source-ip](#)
- [port](#)
- [send templates](#)
- [no send templates](#)
- [send static-flows](#)
- [no send static-flows](#)
- [static-flows](#)
- [no static-flows](#)
- [dynamic-flows](#)
- [no dynamic-flows](#)
- [ipfix-reports](#)
- [no ipfix-reports](#)
- [report open](#)
- [no report open](#)
- [report close](#)
- [no report close](#)
- [report active-timeout](#)
- [no report active-timeout](#)
- [report kilobytes-exchanged](#)
- [no report kilobytes-exchanged](#)
- [report update](#)
- [no report update](#)
- [generate all-templates](#)
- [generate static-appflow-data](#)
- [ecli/appflow_show.cdl](#)
 - [show appflow](#)
- [ecli/certificate.cdl](#)
 - [certificates](#)
 - [export signing-request](#)
 - [export cert-key-pair](#)
 - [import cert-key-pair](#)
 - [import ca-cert](#)
 - [import signed-cert](#)

- [import crt](#)
- [no certificate](#)
- [no certificates](#)
- [generate-signing-request](#)
- [no enrollment](#)
- [scep](#)
- [alias](#)
- [distinguished-name element1](#)
- [distinguished-name element2](#)
- [distinguished-name element3](#)
- [distinguished-name element4](#)
- [distinguished-name element5](#)
- [distinguished-name element6](#)
- [distinguished-name element7](#)
- [distinguished-name element8](#)
- [alternate-name](#)
- [signature-algorithm](#)
- [key.type](#)
- [key.size](#)
- [generate](#)
- [signing-request](#)
- [ca-url](#)
- [challenge-password](#)
- [request-count](#)
- [polling-interval](#)
- [max-polling-time](#)
- [scep](#)
- [ecli/certificate_show.cdl](#)
 - [show certificates](#)
 - [show certificate](#)
- [ecli/ha.cdl](#)
 - [high-availability](#)
 - [heartbeat-interval](#)
 - [failover-trigger-level](#)
 - [probe interval](#)
 - [probe count](#)
 - [election-delay-time](#)
 - [route-hold-down-time](#)
 - [no route-hold-down-time](#)
 - [failover-when-aggregate-down](#)
 - [no failover-when-aggregate-down](#)
 - [enable node](#)
 - [no enable node](#)
 - [include-certificates-keys](#)
 - [no include-certificates-keys](#)
 - [synchronize settings](#)
 - [synchronize firmware](#)
 - [force-failover](#)
 - [no mode](#)
 - [mode](#)
 - [primary-serial](#)
 - [secondary-serial](#)
 - [no secondary-serial](#)
 - [node-num](#)
 - [rank node](#)
 - [serial node](#)
 - [no serial node](#)
 - [stateful-synchronization](#)
 - [no stateful-synchronization](#)
 - [dpi-interface](#)
 - [no dpi-interface](#)
 - [control-interface](#)
 - [no control-interface](#)
 - [data-interface](#)
 - [no data-interface](#)
 - [switched-link](#)
 - [no switched-link](#)
 - [active-active-cluster-link](#)
 - [no active-active-cluster-link](#)
 - [preempt](#)
 - [no preempt](#)
 - [encryption](#)
 - [no encryption](#)
 - [generate-backup-firmware](#)
 - [no generate-backup-firmware](#)
 - [enable-encryption](#)
 - [no enable-encryption](#)
 - [virtual-mac](#)
 - [no virtual-mac](#)
 - [monitoring](#)
 - [monitoring interface](#)
 - [svrrp](#)
 - [svrrp monitoring node](#)
 - [link-monitoring](#)
 - [no link-monitoring](#)
 - [no primary](#)
 - [primary](#)
 - [no secondary](#)
 - [secondary](#)
 - [allow-management](#)

- [no allow-management](#)
- [logical-probe](#)
- [no logical-probe](#)
- [override-virtual-mac](#)
- [no override-virtual-mac](#)
- [link-monitoring](#)
- [no link-monitoring](#)
- [no primary](#)
- [primary](#)
- [no secondary](#)
- [secondary](#)
- [allow-management](#)
- [no allow-management](#)
- [logical-probe](#)
- [no logical-probe](#)
- [ecli/ha_show.cdl](#)
 - [show high-availability](#)
- [ecli/log.cdl](#)
 - [export log](#)
 - [clear log](#)
 - [email log](#)
 - [log display](#)
 - [log event-id](#)
 - [log category](#)
 - [log categories](#)
 - [log syslog](#)
 - [log automation](#)
 - [log name-resolution](#)
 - [log reports](#)
 - [log viewpoint](#)
 - [log analyzer](#)
 - [save-template](#)
 - [import-template](#)
 - [reset event-count](#)
 - [logging-level](#)
 - [alert-level](#)
 - [global-category-attribute](#)
 - [priority-level](#)
 - [log-monitor](#)
 - [no log-monitor](#)
 - [email-alert](#)
 - [no email-alert](#)
 - [syslog](#)
 - [no syslog](#)
 - [event-profile](#)
 - [ipfix](#)
 - [no ipfix](#)
 - [log-digest](#)
 - [no log-digest](#)
 - [color](#)
 - [log-email](#)
 - [no log-email](#)
 - [alert-email](#)
 - [no alert-email](#)
 - [priority-level](#)
 - [log-monitor](#)
 - [no log-monitor](#)
 - [email-alert](#)
 - [no email-alert](#)
 - [syslog](#)
 - [no syslog](#)
 - [event-profile](#)
 - [ipfix](#)
 - [no ipfix](#)
 - [log-digest](#)
 - [no log-digest](#)
 - [color](#)
 - [log-email](#)
 - [no log-email](#)
 - [alert-email](#)
 - [no alert-email](#)
 - [priority-level](#)
 - [log-monitor](#)
 - [no log-monitor](#)
 - [email-alert](#)
 - [no email-alert](#)
 - [syslog](#)
 - [no syslog](#)
 - [event-profile](#)
 - [ipfix](#)
 - [no ipfix](#)
 - [log-digest](#)
 - [no log-digest](#)
 - [color](#)
 - [alert-email](#)
 - [no alert-email](#)
 - [priority-level](#)
 - [log-monitor](#)
 - [no log-monitor](#)
 - [email-alert](#)

- [no email-alert](#)
 - [syslog](#)
 - [no syslog](#)
 - [event-profile syslog-server-profile](#)
 - [ipfix](#)
 - [no ipfix](#)
 - [log-digest](#)
 - [no log-digest](#)
 - [color](#)
 - [alert-email](#)
 - [no alert-email](#)
 - [facility](#)
 - [format](#)
 - [id](#)
 - [event-rate-limiting](#)
 - [data-rate-limiting](#)
 - [type](#)
 - [facility](#)
 - [format](#)
 - [id](#)
 - [event-rate-limiting](#)
 - [no event-rate-limiting](#)
 - [data-rate-limiting](#)
 - [no data-rate-limiting](#)
 - [enabled](#)
 - [no enabled](#)
 - [ndpp](#)
 - [no ndpp](#)
 - [syslog-server server](#)
 - [no syslog-server server](#)
 - [no servers](#)
 - [profile](#)
 - [server](#)
 - [port](#)
 - [outbound-interface](#)
 - [no outbound-interface](#)
 - [local-interface](#)
 - [no local-interface](#)
 - [email-address](#)
 - [no email-address](#)
 - [send-log](#)
 - [email-format](#)
 - [include-all-log-information](#)
 - [no include-all-log-information](#)
 - [health-check-email](#)
 - [no health-check-email](#)
 - [mail-server](#)
 - [no mail-server](#)
 - [mail-from](#)
 - [no mail-from](#)
 - [authentication-method](#)
 - [pop3-server](#)
 - [no pop3-server](#)
 - [pop3-user-name](#)
 - [no pop3-user-name](#)
 - [pop3-password](#)
 - [no pop3-password](#)
 - [test](#)
 - [mail-server-advanced](#)
 - [smtp-port](#)
 - [connection-security-method](#)
 - [no connection-security-method](#)
 - [smtp-authentication](#)
 - [no smtp-authentication](#)
 - [user-name](#)
 - [no user-name](#)
 - [password](#)
 - [no password](#)
 - [solera server](#)
 - [no solera](#)
 - [protocol](#)
 - [port](#)
 - [user](#)
 - [password](#)
 - [deepsee-base-url](#)
 - [pcap-base-url](#)
 - [address-to-link](#)
 - [method](#)
 - [dns](#)
 - [no dns](#)
 - [start](#)
 - [stop](#)
 - [report-view](#)
 - [show](#)
 - [enable](#)
 - [no enable](#)
 - [enable](#)
 - [no enable](#)
- [ecli/config-audit.cdl](#)
 - [log audit](#)
 - [enable](#)

- [no enable](#)
- [debug](#)
- [no debug](#)
- [audit-all](#)
- [no audit-all](#)
- [send audit](#)
- [ecli/log_show.cdl](#)
 - [show log](#)
- [ecli/voip.cdl](#)
 - [voip](#)
 - [flush-all](#)
 - [consistent-nat](#)
 - [no consistent-nat](#)
 - [sip](#)
 - [no sip](#)
 - [h323](#)
 - [no h323](#)
 - [non-sip-packets](#)
 - [no non-sip-packets](#)
 - [b2bua-support](#)
 - [no b2bua-support](#)
 - [signaling-timeout](#)
 - [media-timeout](#)
 - [no signaling-port](#)
 - [signaling-port](#)
 - [endpoint-registration-anomaly-tracking](#)
 - [no endpoint-registration-anomaly-tracking](#)
 - [registration-tracking-interval](#)
 - [failed-registration-threshold](#)
 - [endpoint-block-interval](#)
 - [only-gatekeeper-calls](#)
 - [no only-gatekeeper-calls](#)
 - [inactivity-timeout](#)
 - [no gatekeeper-ip](#)
 - [gatekeeper-ip](#)
- [ecli/voip_show.cdl](#)
 - [show voip](#)
- [ecli/security-services.cdl](#)
 - [security-services](#)
 - [synchronize](#)
 - [security](#)
 - [reduce-isdn-antivirus-traffic](#)
 - [no reduce-isdn-antivirus-traffic](#)
 - [drop-packets-at-reload](#)
 - [no drop-packets-at-reload](#)
 - [http-clientless-notification-timeout](#)
 - [proxy-server](#)
 - [no proxy-server](#)
 - [host](#)
 - [no host](#)
 - [port](#)
 - [no port](#)
 - [authentication](#)
 - [no authentication](#)
 - [portal](#)
 - [no portal](#)
- [ecli/dpi-ssh.cdl](#)
 - [dpi-ssh](#)
 - [enable](#)
 - [no enable](#)
 - [intrusion-prevention](#)
 - [no intrusion-prevention](#)
 - [gateway](#)
 - [no gateway](#)
 - [application-firewall](#)
 - [no application-firewall](#)
 - [block-port-forwarding](#)
 - [no block-port-forwarding](#)
 - [include address](#)
 - [exclude address](#)
 - [no exclude address](#)
 - [include service](#)
 - [exclude service](#)
 - [no exclude service](#)
 - [include user](#)
 - [exclude user](#)
 - [no exclude user](#)
- [ecli/content-filter.cdl](#)
 - [content-filter](#)
 - [filter-type](#)
- [ecli/content-filter-cfs.cdl](#)
 - [max-url-caches](#)
 - [enable](#)
 - [no enable](#)
 - [block-if-server-unavailable](#)

- [no block-if-server-unavailable](#)
- [server-timeout](#)
- [local-server](#)
- [no local-server](#)
- [exclude administrator](#)
- [no exclude administrator](#)
- [exclude address](#)
- [no exclude address](#)
- [clear policies statistics](#)
- [no policies](#)
- [no policy](#)
- [policy](#)
- [name](#)
- [source zone](#)
- [destination zone](#)
- [source address included](#)
- [source address excluded](#)
- [user included](#)
- [user excluded](#)
- [schedule](#)
- [profile](#)
- [action](#)
- [enable](#)
- [no enable](#)
- [priority](#)
- [custom-category](#)
- [enable](#)
- [no enable](#)
- [no category-entries](#)
- [no category-entry](#)
- [category-entry](#)
- [domain](#)
- [no ratings](#)
- [rating](#)
- [no rating](#)
- [ecli/content-filter-objects.cdl](#)
 - [no uri-list-objects](#)
 - [no uri-list-groups](#)
 - [no uri-list-object](#)
 - [no uri-list-group](#)
 - [uri-list-object](#)
 - [uri-list-group](#)
 - [name](#)
 - [name](#)
 - [uri](#)
 - [no uri](#)
 - [no uris](#)
 - [keyword](#)
 - [no keyword](#)
 - [no keywords](#)
 - [uri-list-object](#)
 - [no uri-list-object](#)
 - [uri-list-group](#)
 - [no uri-list-group](#)
 - [no actions](#)
 - [no action](#)
 - [action](#)
 - [name](#)
 - [wipe-cookies](#)
 - [no wipe-cookies](#)
 - [flow-reporting](#)
 - [no flow-reporting](#)
 - [block page](#)
 - [passphrase page](#)
 - [passphrase password](#)
 - [no passphrase password](#)
 - [passphrase active-time](#)
 - [confirm page](#)
 - [confirm active-time](#)
 - [bandwidth-management aggregation-method](#)
 - [bandwidth-management egress](#)
 - [no bandwidth-management egress](#)
 - [bandwidth-management ingress](#)
 - [no bandwidth-management ingress](#)
 - [bandwidth-management usage-tracking](#)
 - [no bandwidth-management usage-tracking](#)
 - [no profiles](#)
 - [no profile](#)
 - [profile](#)
 - [name](#)
 - [uri-list allowed](#)
 - [no uri-list allowed](#)
 - [uri-list forbidden](#)
 - [no uri-list forbidden](#)
 - [uri-list search-order](#)
 - [uri-list forbidden-operation](#)
 - [category](#)
 - [categories](#)
 - [https-filtering](#)
 - [no https-filtering](#)
 - [smart-filter](#)

- [no smart-filter](#)
 - [safe-search](#)
 - [no safe-search](#)
 - [google-force-safe-search](#)
 - [no google-force-safe-search](#)
 - [youtube-restrict-mode](#)
 - [no youtube-restrict-mode](#)
 - [bing-force-safe-search](#)
 - [no bing-force-safe-search](#)
 - [consent required](#)
 - [no consent required](#)
 - [consent user-idle-timeout](#)
 - [consent optional page-url](#)
 - [no consent optional page-url](#)
 - [consent mandatory page-url](#)
 - [no consent mandatory page-url](#)
 - [consent mandatory address](#)
 - [no consent mandatory address](#)
 - [custom-header insertion](#)
 - [no custom-header insertion](#)
 - [custom-header entry](#)
 - [no custom-header entry](#)
 - [no custom-header entries](#)
- [ecli/content-filter-websense.cdl](#)
 - [server](#)
 - [no server](#)
 - [port](#)
 - [user-name](#)
 - [no user-name](#)
 - [max-url-caches](#)
 - [https-content-filtering](#)
 - [no https-content-filtering](#)
 - [probe monitoring](#)
 - [no probe monitoring](#)
 - [probe interval](#)
 - [probe deactivate-after](#)
 - [probe reactivate-after](#)
 - [block-if-server-unavailable](#)
 - [no block-if-server-unavailable](#)
 - [server-timeout](#)
 - [blockactivex](#)
 - [no blockactivex](#)
 - [block java](#)
 - [no block java](#)
 - [block flash](#)
 - [no block flash](#)
 - [block cookies](#)
 - [no block cookies](#)
 - [block http-proxy-access](#)
 - [no block http-proxy-access](#)
 - [exclude web-features-domains](#)
 - [no exclude web-features-domains](#)
 - [exclude administrator](#)
 - [no exclude administrator](#)
 - [exclude address](#)
 - [no exclude address](#)
 - [blocking-page](#)
- [ecli/anti-spam.cdl](#)
 - [anti-spam](#)
 - [start capture](#)
 - [stop capture](#)
 - [clear capture](#)
 - [export capture](#)
 - [grid-ip-check](#)
 - [enable](#)
 - [destination-mail-server public](#)
 - [no enable](#)
 - [action likely-spam](#)
 - [action definite-spam](#)
 - [action likely-phishing](#)
 - [action definite-phishing](#)
 - [action likely-virus](#)
 - [action definite-virus](#)
 - [allow-list](#)
 - [no allow-list](#)
 - [reject-list](#)
 - [no reject-list](#)
 - [service-down](#)
 - [junk-box down](#)
 - [junk-box secure-http](#)
 - [no junk-box secure-http](#)
 - [junk-box port](#)
 - [no junk-box port](#)
 - [probe interval](#)
 - [probe timeout](#)
 - [success-threshold](#)
 - [failure-threshold](#)
 - [mail-server](#)
 - [no mail-server](#)
 - [destination-mail-address-as-junk-store](#)

- [no destination-mail-address-as-junk-store](#)
- [junk-store-ip](#)
- [system-detection](#)
- [no system-detection](#)
- ecli/ips.cdl
 - [intrusion-prevention](#)
 - [update-signatures](#)
 - [enable](#)
 - [no enable](#)
 - [signature-group high-priority](#)
 - [signature-group medium-priority](#)
 - [signature-group low-priority](#)
 - [no signature-group high-priority](#)
 - [no signature-group medium-priority](#)
 - [no signature-group low-priority](#)
 - [reset](#)
 - [category](#)
 - [exclusion](#)
 - [no exclusion](#)
 - [name](#)
 - [id](#)
 - [prevention](#)
 - [no prevention](#)
 - [detection](#)
 - [no detection](#)
 - [included users](#)
 - [excluded users](#)
 - [included ip](#)
 - [excluded ip](#)
 - [no excluded](#)
 - [schedule](#)
 - [log-redundancy](#)
 - [category](#)
 - [prevention](#)
 - [no prevention](#)
 - [detection](#)
 - [no detection](#)
 - [included users](#)
 - [excluded users](#)
 - [included ip](#)
 - [excluded ip](#)
 - [no excluded](#)
 - [schedule](#)
 - [log-redundancy](#)
 - [priority](#)
 - [direction](#)
- ecli/gav.cdl
 - [gateway-antivirus](#)
 - [update-signatures](#)
 - [enable](#)
 - [no enable](#)
 - [signature](#)
 - [no signature](#)
 - [inbound-inspection](#)
 - [no inbound-inspection](#)
 - [outbound-inspection](#)
 - [no outbound-inspection](#)
 - [restrict password-protected-zip](#)
 - [no restrict password-protected-zip](#)
 - [restrict ms-office-macros](#)
 - [no restrict ms-office-macros](#)
 - [restrict packed-executables](#)
 - [no restrict packed-executables](#)
 - [exclusion-object http](#)
 - [exclusion-object ftp](#)
 - [exclusion-object imap](#)
 - [exclusion-object smtp](#)
 - [exclusion-object pop3](#)
 - [exclusion-object cifs-netbios](#)
 - [no exclusion-object](#)
 - [reset-settings](#)
 - [cloud anti-virus-database](#)
 - [no cloud anti-virus-database](#)
 - [cloud exclusion](#)
 - [no cloud exclusion](#)
 - [no cloud exclusions](#)
 - [smtp-responses](#)
 - [no smtp-responses](#)
 - [eicar-detection](#)
 - [no eicar-detection](#)
 - [http-byte-range](#)
 - [no http-byte-range](#)
 - [ftp-rest](#)
 - [no ftp-rest](#)
 - [scan-high-compression](#)
 - [no scan-high-compression](#)
 - [block-multiple-compress-files](#)
 - [no block-multiple-compress-files](#)
 - [detection-only](#)
 - [no detection-only](#)

- [http-clientless-notification](#)
- [no http-clientless-notification](#)
- [no notification-message](#)
- [notification-message](#)
- [exclusion](#)
- [no exclusion](#)
- [ecli/capture-atp.cdl](#)
 - [capture-atp](#)
 - [enable](#)
 - [no enable](#)
 - [file-type](#)
 - [no file-type](#)
 - [file-size](#)
 - [exclude address for-capture-atp](#)
 - [no exclude address for-capture-atp](#)
 - [exclude md5-entry](#)
 - [no exclude md5-entry](#)
 - [no exclude md5-entries](#)
 - [await-verdict](#)
 - [exclude address for-block-until-verdict](#)
 - [no exclude address for-block-until-verdict](#)
 - [exclude file-type](#)
 - [no exclude file-type](#)
- [ecli/match-object.cdl](#)
 - [no match-object](#)
 - [no match-objects](#)
 - [match-object](#)
 - [no type](#)
 - [type](#)
 - [name](#)
 - [match-type](#)
 - [no match-type](#)
 - [enable](#)
 - [no enable](#)
 - [offset](#)
 - [no offset](#)
 - [depth](#)
 - [no depth](#)
 - [min-size](#)
 - [no min-size](#)
 - [max-size](#)
 - [no max-size](#)
 - [negative-matching](#)
 - [no negative-matching](#)
 - [no input-representation](#)
 - [input-representation](#)
 - [content-entry](#)
 - [no content-entry](#)
 - [no content-entries](#)
 - [pre-defined-regex](#)
 - [no pre-defined-regex](#)
 - [browser](#)
 - [no browser](#)
 - [no browsers](#)
 - [custom-header](#)
 - [no custom-header](#)
 - [email-size](#)
 - [no email-size](#)
 - [ftp-command](#)
 - [no ftp-command](#)
 - [no ftp-commands](#)
 - [argument](#)
 - [no argument](#)
 - [no arguments](#)
 - [ips category](#)
 - [no ips category](#)
 - [no ips categories](#)
 - [ips policy](#)
 - [no ips policy](#)
 - [no ips policies](#)
 - [category](#)
 - [no category](#)
 - [no categories](#)
 - [application](#)
 - [no application](#)
 - [no applications](#)
 - [signature](#)
 - [no signature](#)
 - [no signatures](#)
- [ecli/action-object.cdl](#)
 - [action-object](#)
 - [no action-object](#)
 - [no action-objects](#)
 - [name](#)
 - [action](#)
 - [no content](#)
 - [content](#)
 - [no color](#)
 - [color](#)

- [bandwidth-management](#)
- [aggregation-method](#)
- [no egress](#)
- [egress priority](#)
- [egress bandwidth-object](#)
- [no ingress](#)
- [ingress priority](#)
- [ingress bandwidth-object](#)
- [usage-tracking](#)
- [no usage-tracking](#)
- ecli/email-object.cdl
 - [no email-object](#)
 - [no email-objects](#)
 - [email-object](#)
 - [name](#)
 - [no match-type](#)
 - [match-type](#)
 - [content-entry](#)
 - [no content-entry](#)
 - [no content-entries](#)
- ecli/app-rules.cdl
 - [app-rules](#)
 - [enable](#)
 - [no enable](#)
 - [log-redundancy](#)
 - [no log-redundancy](#)
 - [no policy](#)
 - [no policies](#)
 - [policy](#)
 - [name](#)
 - [type](#)
 - [source address](#)
 - [destination address](#)
 - [address](#)
 - [exclusion address](#)
 - [no exclusion address](#)
 - [source service](#)
 - [destination service](#)
 - [match-object](#)
 - [action-object](#)
 - [users](#)
 - [no users](#)
 - [mail-from included](#)
 - [mail-from excluded](#)
 - [no mail-from](#)
 - [rcpt-to included](#)
 - [rcpt-to excluded](#)
 - [no rcpt-to](#)
 - [schedule](#)
 - [flow-reporting](#)
 - [no flow-reporting](#)
 - [logging](#)
 - [no logging](#)
 - [log individual](#)
 - [no log individual](#)
 - [ips-message-format](#)
 - [no ips-message-format](#)
 - [app-control-message-format](#)
 - [no app-control-message-format](#)
 - [cfs-message-format](#)
 - [no cfs-message-format](#)
 - [log redundancy](#)
 - [connection-side](#)
 - [direction](#)
 - [zone](#)
 - [cfs-list allow](#)
 - [no cfs-list allow](#)
 - [cfs-list forbidden](#)
 - [no cfs-list forbidden](#)
 - [safe-search](#)
 - [no safe-search](#)
 - [youtube-for-schools](#)
 - [no youtube-for-schools](#)
 - [school-id](#)
 - [no school-id](#)
- ecli/app-control.cdl
 - [app-control](#)
 - [update-signatures](#)
 - [enable](#)
 - [no enable](#)
 - [log-all](#)
 - [no log-all](#)
 - [log-filename](#)
 - [no log-filename](#)
 - [log-redundancy filter](#)
 - [reset](#)
 - [category](#)
 - [exclusion list](#)
 - [no exclusion list](#)

- [name](#)
- [id](#)
- [block](#)
- [no block](#)
- [log](#)
- [no log](#)
- [included users](#)
- [excluded users](#)
- [included ip](#)
- [excluded ip](#)
- [no excluded](#)
- [schedule](#)
- [log-redundancy](#)
- [block](#)
- [no block](#)
- [log](#)
- [no log](#)
- [included users](#)
- [excluded users](#)
- [included ip](#)
- [excluded ip](#)
- [no excluded](#)
- [schedule](#)
- [log-redundancy](#)
- [category](#)
- [application](#)
- [block](#)
- [no block](#)
- [log](#)
- [no log](#)
- [included users](#)
- [excluded users](#)
- [included ip](#)
- [excluded ip](#)
- [no excluded](#)
- [schedule](#)
- [log-redundancy](#)
- [ecli/rbl.cdl](#)
 - [rbl](#)
 - [enable](#)
 - [no enable](#)
 - [dns](#)
 - [no dns](#)
 - [service](#)
 - [no service](#)
 - [no services](#)
 - [clear statistics](#)
 - [blacklist](#)
 - [no blacklist](#)
 - [whitelist](#)
 - [no whitelist](#)
 - [enable](#)
 - [no enable](#)
 - [domain](#)
 - [blocked-responses](#)
 - [no blocked-responses](#)
- [ecli/dpi-ssl.cdl](#)
 - [dpi-ssl](#)
 - [enable](#)
 - [no enable](#)
 - [intrusion-prevention](#)
 - [no intrusion-prevention](#)
 - [gateway](#)
 - [no gateway](#)
 - [application-firewall](#)
 - [no application-firewall](#)
 - [content-filter](#)
 - [no content-filter](#)
 - [authenticate-server-for-decrypted-connections](#)
 - [no authenticate-server-for-decrypted-connections](#)
 - [expired-ca](#)
 - [no expired-ca](#)
 - [deployment-server-domains](#)
 - [no deployment-server-domains](#)
 - [bypass-decryption](#)
 - [no bypass-decryption](#)
 - [audit-built-in-exclusion](#)
 - [no audit-built-in-exclusion](#)
 - [authenticate-server](#)
 - [no authenticate-server](#)
 - [open-failed-connections](#)
 - [no open-failed-connections](#)
 - [resigning-authority](#)
 - [include address](#)
 - [exclude address](#)
 - [no exclude address](#)
 - [include service](#)
 - [exclude service](#)
 - [no exclude service](#)
 - [include user](#)

- [exclude user](#)
- [no exclude user](#)
- [reject](#)
- [accept](#)
- [no common-name](#)
- [no common-names](#)
- [common-name](#)
- [cfs-categories](#)
- [no cfs-categories](#)
- [exclude cfs-category-unavailable](#)
- [no exclude cfs-category-unavailable](#)
- [enable](#)
- [no enable](#)
- [intrusion-prevention](#)
- [no intrusion-prevention](#)
- [gateway](#)
- [no gateway](#)
- [application-firewall](#)
- [no application-firewall](#)
- [include address](#)
- [exclude address](#)
- [include user](#)
- [exclude user](#)
- [no exclude](#)
- [ssl-server](#)
- [no ssl-server](#)
- [no ssl-servers](#)
- [ecli/client-av-enforcement.cdl](#)
 - [client-enforcement anti-virus](#)
 - [policing](#)
 - [no policing](#)
 - [force interval](#)
 - [no force interval](#)
 - [force update](#)
 - [no force update](#)
 - [enforcement-list](#)
 - [no enforcement-list](#)
- [ecli/client-cfs-enforcement.cdl](#)
 - [client-enforcement content-filtering](#)
 - [grace-period](#)
 - [no grace-period](#)
 - [enforcement-list](#)
 - [no enforcement-list](#)
 - [default-enforcement](#)
 - [no default-enforcement](#)
- [ecli/geo-ip.cdl](#)
 - [geo-ip](#)
 - [custom-list](#)
 - [enable](#)
 - [no enable](#)
 - [override-countries](#)
 - [no override-countries](#)
 - [address](#)
 - [no address](#)
 - [no addresses](#)
 - [country](#)
 - [comment](#)
 - [no comment](#)
 - [block connections](#)
 - [no block connections](#)
 - [block database-not-downloaded](#)
 - [no block database-not-downloaded](#)
 - [logging](#)
 - [no logging](#)
 - [block country](#)
 - [no block country](#)
 - [block countries](#)
 - [no block countries](#)
 - [no exclude](#)
 - [exclude](#)
 - [include block-details](#)
 - [no include block-details](#)
 - [alert-text](#)
 - [no alert-text](#)
 - [logo-icon](#)
 - [default blocked-page](#)
- [ecli/botnet.cdl](#)
 - [botnet](#)
 - [custom-list](#)
 - [dynamic-list](#)
 - [block connections](#)
 - [no block connections](#)
 - [block database-not-downloaded](#)
 - [no block database-not-downloaded](#)
 - [enable](#)
 - [no enable](#)
 - [address](#)
 - [no address](#)

- [no addresses](#)
 - [name](#)
 - [group](#)
 - [enable](#)
 - [no enable](#)
 - [comment](#)
 - [no comment](#)
 - [enable](#)
 - [no enable](#)
 - [flush](#)
 - [download](#)
 - [periodical-download](#)
 - [no periodical-download](#)
 - [download-interval](#)
 - [protocol](#)
 - [server-ip-address](#)
 - [no server-ip-address](#)
 - [login](#)
 - [no login](#)
 - [password](#)
 - [no password](#)
 - [directory-path](#)
 - [no directory-path](#)
 - [file-name](#)
 - [no file-name](#)
 - [url-name](#)
 - [no url-name](#)
 - [logging](#)
 - [no logging](#)
 - [exclude](#)
 - [no exclude](#)
 - [include block-details](#)
 - [no include block-details](#)
 - [alert-text](#)
 - [no alert-text](#)
 - [logo-icon](#)
 - [default blocked-page](#)
- [ecli/anti-spyware.cdl](#)
 - [anti-spyware](#)
 - [update-signatures](#)
 - [enable](#)
 - [no enable](#)
 - [signature-group](#)
 - [no signature-group](#)
 - [reset](#)
 - [inspection inbound](#)
 - [no inspection inbound](#)
 - [inspection outbound](#)
 - [no inspection outbound](#)
 - [smtp-responses](#)
 - [no smtp-responses](#)
 - [http-clientless-notification](#)
 - [no http-clientless-notification](#)
 - [message](#)
 - [no message](#)
 - [exclusion](#)
 - [no exclusion list](#)
 - [no exclusion entry](#)
 - [no exclusion entries](#)
 - [product](#)
 - [name](#)
 - [id](#)
 - [prevention](#)
 - [no prevention](#)
 - [detection](#)
 - [no detection](#)
 - [included](#)
 - [excluded](#)
 - [no excluded](#)
 - [schedule](#)
 - [log-redundancy](#)
 - [product](#)
 - [danger-level](#)
 - [prevention](#)
 - [no prevention](#)
 - [detection](#)
 - [no detection](#)
 - [included](#)
 - [excluded](#)
 - [no excluded](#)
 - [schedule](#)
 - [log-redundancy](#)
- [ecli/security-services_show.cdl](#)
 - [show security-services](#)
- [ecli/dpi-ssh_show.cdl](#)
 - [show dpi-ssh](#)
- [ecli/content-filter_show.cdl](#)
 - [show content-filter](#)

- ecli/anti-spam_show.cd
 - [show anti-spam](#)
- ecli/ips_show.cd
 - [show intrusion-prevention](#)
- ecli/gav_show.cd
 - [show gateway-antivirus](#)
- ecli/capture-atp_show.cd
 - [show capture-atp](#)
- ecli/match-object_show.cd
 - [show match-objects](#)
 - [show match-object](#)
- ecli/action-object_show.cd
 - [show action-objects](#)
 - [show action-object](#)
- ecli/email-object_show.cd
 - [show email-objects](#)
 - [show email-object](#)
- ecli/app-rules_show.cd
 - [show app-rules](#)
- ecli/app-control_show.cd
 - [show app-control](#)
- ecli/rbl_show.cd
 - [show rbl](#)
- ecli/dpi-ssl_show.cd
 - [show dpi-ssl](#)
- ecli/client-av-enforcement_show.cd
 - [show client-enforcement anti-virus](#)
- ecli/client-efs-enforcement_show.cd
 - [show client-enforcement content-filtering](#)
- ecli/geo-ip_show.cd
 - [show geo-ip](#)
- ecli/botnet_show.cd
 - [show botnet](#)
- ecli/anti-spyware_show.cd
 - [show anti-spyware](#)
- ecli/sonicpoint.cd
 - [sonicpoint](#)
 - [synchronize](#)
 - [reboot](#)
 - [no sonicpoint](#)
 - [no profile](#)
 - [no sonicpoints](#)
 - [no profiles](#)
 - [sonicpoint](#)
 - [profile](#)
 - [enable](#)
 - [no enable](#)
 - [rf-monitoring](#)
 - [no rf-monitoring](#)
 - [poe-out](#)
 - [no poe-out](#)
 - [low-power](#)
 - [no low-power](#)
 - [retain](#)
 - [no retain](#)
 - [led](#)
 - [no led](#)
 - [name-prefix](#)
 - [name](#)
 - [country-code](#)
 - [eapol-version](#)
 - [band-steering](#)
 - [no band-steering](#)
 - [sslvpn](#)
 - [no sslvpn](#)
 - [radius](#)
 - [no radius](#)
 - [administrator](#)
 - [no administrator](#)
 - [widp-sensor](#)
 - [no widp-sensor](#)
 - [wwan](#)
 - [no wwan](#)
 - [mesh](#)
 - [no mesh](#)
 - [ble](#)
 - [no ble](#)

- [packet-capture](#)
- [mode](#)
- [band](#)
- [channel](#)
- [capture](#)
- [no capture](#)
- [ssid](#)
- [no ssid](#)
- [bssid](#)
- [no bssid](#)
- [mac](#)
- [no mac](#)
- [radio](#)
- [radio-2400mhz](#)
- [radio-5000mhz](#)
- [virtual-access-point_group](#)
- [no virtual-access-point_group](#)
- [dynamic-vlan](#)
- [no dynamic-vlan](#)
- [vlan](#)
- [no vlan](#)
- [no vlans](#)
- [enable](#)
- [no enable](#)
- [schedule](#)
- [mode](#)
- [dfs-channel](#)
- [no dfs-channel](#)
- [ssid](#)
- [no ssid](#)
- [channel](#)
- [band](#)
- [short-guard-interval](#)
- [no short-guard-interval](#)
- [aggregation](#)
- [no aggregation](#)
- [mimo](#)
- [no mimo](#)
- [no access-list](#)
- [access-list](#)
- [mic-failure acl-blacklist](#)
- [no mic-failure acl-blacklist](#)
- [mic-failure frequency](#)
- [virtual-access-point_wep-key](#)
- [no virtual-access-point_wep-key](#)
- [authentication-type](#)
- [no wep-key](#)
- [wep-key](#)
- [wpa_auth-balance-method](#)
- [wpa_cipher-type](#)
- [wpa_group-key-interval](#)
- [wpa_passphrase](#)
- [no_wpa_passphrase](#)
- [wpa_pmf](#)
- [no_wpa_pmf](#)
- [remote-mac-access-control](#)
- [no_remote-mac-access-control](#)
- [hide-ssid](#)
- [no_hide-ssid](#)
- [ids-scan schedule](#)
- [no_ids-scan schedule](#)
- [data-rate](#)
- [transmit-power](#)
- [antennae-diversity](#)
- [interval](#)
- [threshold](#)
- [max-clients](#)
- [station-inactivity-timeout](#)
- [preamble-length](#)
- [protection mode](#)
- [no_protection mode](#)
- [protection rate](#)
- [protection type](#)
- [short-slot-time](#)
- [no_short-slot-time](#)
- [deny-b](#)
- [no deny-b](#)
- [wds-ap](#)
- [no wds-ap](#)
- [wmm](#)
- [no wmm](#)
- [green-ap](#)
- [no_green-ap](#)
- [rssi](#)
- [no_rssi](#)
- [airtime-fairness](#)
- [no airtime-fairness](#)
- [80211r](#)
- [no_80211r](#)
- [80211k neighbour-report](#)
- [no_80211k neighbour-report](#)

- [80211v](#)
- [no 80211v](#)
- [ids](#)
- [scan sonicpoint](#)
- [scan all](#)
- [authorizing-access-point](#)
- [widp](#)
- [no widp](#)
- [authorized-access-point](#)
- [rogue-access-point](#)
- [unauthorized-access-point](#)
- [no unauthorized-access-point](#)
- [arp-cache-lookup](#)
- [no arp-cache-lookup](#)
- [active-probe](#)
- [no active-probe](#)
- [evil-twin](#)
- [no evil-twin](#)
- [block-traffic](#)
- [no block-traffic](#)
- [disassociate rogue](#)
- [no disassociate rogue](#)
- [disassociate krack](#)
- [no disassociate krack](#)
- [rf-monitoring](#)
- [measurement-interval](#)
- [management-frame-flood](#)
- [no management-frame-flood](#)
- [null-probe-response](#)
- [no null-probe-response](#)
- [broadcasting-deauthentication](#)
- [no broadcasting-deauthentication](#)
- [station-with-invalid-ssid](#)
- [no station-with-invalid-ssid](#)
- [wellenreiter](#)
- [no wellenreiter](#)
- [ad-hoc-station](#)
- [no ad-hoc-station](#)
- [long-duration](#)
- [no long-duration](#)
- [unassociated-station](#)
- [no unassociated-station](#)
- [netstumbler](#)
- [no netstumbler](#)
- [eapol-packet-flood](#)
- [no eapol-packet-flood](#)
- [weak-wep-iv](#)
- [no weak-wep-iv](#)
- [watch station](#)
- [no watch station](#)
- [clear rf-monitoring statistics](#)
- [fairnet enable](#)
- [no fairnet enable](#)
- [fairnet policy](#)
- [no fairnet policy](#)
- [no fairnet policies](#)
- [enable](#)
- [no enable](#)
- [direction](#)
- [range](#)
- [interface](#)
- [rate min](#)
- [ecli/wifi-multimedia.cdl](#)
 - [wmm profile](#)
 - [no wmm profile](#)
 - [no wmm profiles](#)
 - [name](#)
 - [no access-point](#)
 - [access-point](#)
 - [no station](#)
 - [station](#)
 - [no mapping](#)
 - [mapping](#)
- [ecli/virtual-access-point.cdl](#)
 - [virtual-access-point group](#)
 - [virtual-access-point profile](#)
 - [virtual-access-point object](#)
 - [no virtual-access-point](#)
 - [name](#)
 - [virtual-access-point](#)
 - [group](#)
 - [no virtual-access-point](#)
 - [no group](#)
 - [name](#)
 - [schedule](#)
 - [access-list](#)
 - [no access-list](#)
 - [radio-type](#)
 - [max-clients](#)
 - [wep-key](#)

- [authentication-type](#)
- [wpa auth-balance-method](#)
- [cipher-type](#)
- [no cipher-type](#)
- [wpa passphrase](#)
- [no wpa passphrase](#)
- [wpa group-key-interval](#)
- [wpa pmf](#)
- [no wpa pmf](#)
- [radius](#)
- [no radius](#)
- [remote-mac-access-control](#)
- [no remote-mac-access-control](#)
- [wds](#)
- [no wds](#)
- [radio-type](#)
- [ssid](#)
- [no ssid](#)
- [no vlan-id](#)
- [vlan-id](#)
- [suppress-ssid](#)
- [no suppress-ssid](#)
- [enable](#)
- [no enable](#)
- [dynamic-vlan](#)
- [no dynamic-vlan](#)
- [vlan](#)
- [no vlan](#)
- [no vlans](#)
- [profile](#)
- [no profile](#)
- [80211r](#)
- [no 80211r](#)
- [80211k neighbour-report](#)
- [no 80211k neighbour-report](#)
- [80211v](#)
- [no 80211v](#)
- [ecli/sonicpoint_show.cdl](#)
 - [show sonicpoint](#)
- [ecli/virtual-assist.cdl](#)
 - [virtual-assist](#)
 - [logout](#)
 - [assistance-code](#)
 - [no assistance-code](#)
 - [support-without-invitation](#)
 - [no support-without-invitation](#)
 - [disclaimer](#)
 - [no disclaimer](#)
 - [customer-access-link](#)
 - [no customer-access-link](#)
 - [link-on-portal-login](#)
 - [no link-on-portal-login](#)
 - [technician-email-list](#)
 - [no technician-email-list](#)
 - [invitation-subject](#)
 - [no invitation-subject](#)
 - [invitation-message](#)
 - [no invitation-message](#)
 - [max-requests](#)
 - [limit-message](#)
 - [no limit-message](#)
 - [max-requests-one-ip](#)
 - [no max-requests-one-ip](#)
 - [pending-request-expiration](#)
 - [no pending-request-expiration](#)
 - [deny-requests](#)
 - [no deny-requests](#)
- [ecli/virtual-assist_show.cdl](#)
 - [show virtual-assist](#)
- [ecli/vpn.cdl](#)
 - [vpn](#)
 - [no vpn policy](#)
 - [no vpn policies](#)
 - [enable](#)
 - [no enable](#)
 - [firewall-identifier](#)
 - [no ike-dpd](#)
 - [ike-dpd](#)
 - [interval](#)
 - [trigger](#)
 - [idle-dpd](#)
 - [no idle-dpd](#)
 - [frag-packets](#)
 - [no frag-packets](#)
 - [ignore-df-bit](#)
 - [no ignore-df-bit](#)
 - [nat-traversal](#)
 - [no nat-traversal](#)

- [cleanup-tunnels](#)
- [no cleanup-tunnels](#)
- [preserve-ike-port](#)
- [no preserve-ike-port](#)
- [no ocsdp-checking](#)
- [ocsdp-checking](#)
- [responder-url](#)
- [no responder-url](#)
- [traps-on-change](#)
- [no traps-on-change](#)
- [use-radius](#)
- [no use-radius](#)
- [dns server](#)
- [no dns server](#)
- [wins](#)
- [no wins](#)
- [ikev2](#)
- [send-cookie](#)
- [no send-cookie](#)
- [send-invalid-spi](#)
- [no send-invalid-spi](#)
- [proposal dh-group](#)
- [proposal encryption](#)
- [proposal authentication](#)
- [policy](#)
- [no policy](#)
- [no policies](#)
- [name](#)
- [name](#)
- [enable](#)
- [no enable](#)
- [gateway primary](#)
- [no gateway primary](#)
- [gateway secondary](#)
- [no gateway secondary](#)
- [auth-method](#)
- [auth-method](#)
- [export group-vpn](#)
- [shared-secret](#)
- [no shared-secret](#)
- [ike-id local](#)
- [no ike-id local](#)
- [ike-id peer](#)
- [no ike-id peer](#)
- [certificate](#)
- [no certificate](#)
- [ike-id local](#)
- [ike-id peer](#)
- [no ike-id peer](#)
- [peer id](#)
- [peer match-issuer](#)
- [no peer match-issuer](#)
- [network local](#)
- [no network local](#)
- [network remote](#)
- [no network remote](#)
- [proposal ike](#)
- [proposal ipsec](#)
- [no proposal ipsec](#)
- [client cache-xauth](#)
- [client virtual-adaptor](#)
- [client allow-connections-to](#)
- [client default-route](#)
- [no client default-route](#)
- [client simple-provisioning](#)
- [no client simple-provisioning](#)
- [keep-alive](#)
- [no keep-alive](#)
- [suppress-auto-add-rule](#)
- [no suppress-auto-add-rule](#)
- [require-xauth](#)
- [no require-xauth](#)
- [anti-replay](#)
- [no anti-replay](#)
- [advanced-routing](#)
- [no advanced-routing](#)
- [transport-mode](#)
- [no transport-mode](#)
- [netbios](#)
- [no netbios](#)
- [multicast](#)
- [no multicast](#)
- [permit-acceleration](#)
- [no permit-acceleration](#)
- [wxa-group](#)
- [no wxa-group](#)
- [apply-nat](#)
- [no apply-nat](#)
- [no ocsdp-checking](#)
- [ocsdp-checking](#)
- [responder-url](#)

- [no responder-url](#)
 - [management](#)
 - [no management](#)
 - [user-login](#)
 - [no user-login](#)
 - [default-lan-gateway](#)
 - [no default-lan-gateway](#)
 - [bound-to](#)
 - [local-ip](#)
 - [group](#)
 - [preempt-secondary-gateway](#)
 - [no preempt-secondary-gateway](#)
 - [client-authentication](#)
 - [suppress-trigger-packet](#)
 - [no suppress-trigger-packet](#)
 - [accept-hash](#)
 - [no accept-hash](#)
 - [send-hash](#)
 - [no send-hash](#)
 - [accept-multiple-proposals](#)
 - [no accept-multiple-proposals](#)
 - [ike-mode-configuration](#)
 - [no ike-mode-configuration](#)
 - [allow-sonicpointn-layer3](#)
 - [no allow-sonicpointn-layer3](#)
- [ecli/l2tp-server.cdl](#)
 - [l2tp-server](#)
 - [no l2tp-server](#)
 - [keep-alive](#)
 - [dns](#)
 - [no dns](#)
 - [wins](#)
 - [no wins](#)
 - [ip-pool](#)
 - [no user-group](#)
 - [user-group](#)
- [ecli/dhcp-over-vpn.cdl](#)
 - [dhcp-over-vpn](#)
 - [internal-dhcp](#)
 - [no internal-dhcp](#)
 - [global-vpn](#)
 - [no global-vpn](#)
 - [remote](#)
 - [no remote](#)
 - [send-requests](#)
 - [no send-requests](#)
 - [dhcp-server](#)
 - [no dhcp-server](#)
 - [no dhcp-servers](#)
 - [no relay-ip](#)
 - [relay-ip](#)
 - [bound-to](#)
 - [accept-bridged-wlan-request](#)
 - [no accept-bridged-wlan-request](#)
 - [no relay-ip](#)
 - [relay-ip](#)
 - [no management-ip](#)
 - [management-ip](#)
 - [block-spoof](#)
 - [no block-spoof](#)
 - [temp-lease](#)
 - [no temp-lease](#)
 - [lease-time](#)
 - [static-device](#)
 - [no static-device](#)
 - [no static-devices](#)
 - [excluded-device](#)
 - [no excluded-device](#)
 - [no excluded-devices](#)
- [ecli/vpn_show.cdl](#)
 - [show vpn](#)
- [ecli/ssl-vpn.cdl](#)
 - [ssl-vpn server](#)
 - [logout](#)
 - [access](#)
 - [no access](#)
 - [port](#)
 - [certificate](#)
 - [use-radius](#)
 - [no use-radius](#)
 - [user-domain](#)
 - [no user-domain](#)
 - [management web](#)
 - [no management web](#)
 - [management ssh](#)
 - [no management ssh](#)
 - [session-timeout](#)
 - [download-url](#)

- [ssl-vpn portal](#)
- [site-title](#)
- [banner-title](#)
- [home-page-message](#)
- [login-message](#)
- [auto-launch](#)
- [no auto-launch](#)
- [cache-control](#)
- [no cache-control](#)
- [display-link](#)
- [no display-link](#)
- [logo](#)
- [ssl-vpn epc-profile](#)
- [ssl-vpn profile](#)
- [enable-epc](#)
- [no enable-epc](#)
- [fallback-options](#)
- [device-profile](#)
- [device-profile](#)
- [no device-profile](#)
- [no device-profiles](#)
- [name](#)
- [description](#)
- [no description](#)
- [enable](#)
- [no enable](#)
- [action](#)
- [network-address](#)
- [no network-address](#)
- [deny-message](#)
- [no deny-message](#)
- [quarantine-message](#)
- [no quarantine-message](#)
- [wlan-tunnel-interface](#)
- [no wlan-tunnel-interface](#)
- [security](#)
- [routes](#)
- [client](#)
- [no all-attributes](#)
- [type](#)
- [no type](#)
- [firewall](#)
- [no firewall](#)
- [certification](#)
- [no certification](#)
- [application](#)
- [no application](#)
- [directory](#)
- [no directory](#)
- [equipment](#)
- [no equipment](#)
- [domain](#)
- [no domain](#)
- [file](#)
- [no file](#)
- [registry](#)
- [no registry](#)
- [os-version](#)
- [no os-version](#)
- [dns inherit](#)
- [dns primary](#)
- [no dns primary](#)
- [dns secondary](#)
- [no dns secondary](#)
- [dns search-list](#)
- [no dns search-list](#)
- [no dns search-lists](#)
- [wins primary](#)
- [no wins primary](#)
- [wins secondary](#)
- [no wins secondary](#)
- [auto-update](#)
- [no auto-update](#)
- [exit-after-disconnect](#)
- [no exit-after-disconnect](#)
- [netbios-over-sslvpn](#)
- [no netbios-over-sslvpn](#)
- [touch-id-authentication](#)
- [no touch-id-authentication](#)
- [fingerprint-authentication](#)
- [no fingerprint-authentication](#)
- [uninstall-after-exit](#)
- [no uninstall-after-exit](#)
- [create-connection-profile](#)
- [no create-connection-profile](#)
- [cache](#)
- [no cache](#)
- [tunnel-all](#)
- [no tunnel-all](#)
- [route](#)
- [no route](#)

- [no routes](#)
 - [ssl-vpn virtual-office](#)
 - [ssl-vpn logout](#)
 - [bookmark](#)
 - [no bookmark](#)
 - [no bookmarks](#)
 - [name](#)
 - [host](#)
 - [no host](#)
 - [service](#)
 - [screen-size](#)
 - [colors](#)
 - [application-path](#)
 - [no application-path](#)
 - [start-in-folder](#)
 - [no start-in-folder](#)
 - [automatic-login](#)
 - [no automatic-login](#)
 - [plugin-dlls](#)
 - [no plugin-dlls](#)
 - [redirect-clipboard](#)
 - [no redirect-clipboard](#)
 - [redirect-audio](#)
 - [no redirect-audio](#)
 - [auto-reconnection](#)
 - [no auto-reconnection](#)
 - [desktop-background](#)
 - [no desktop-background](#)
 - [window-drag](#)
 - [no window-drag](#)
 - [animation](#)
 - [no animation](#)
 - [view-only](#)
 - [no view-only](#)
 - [share-desktop](#)
 - [no share-desktop](#)
 - [automatic-accept-host-key](#)
 - [no automatic-accept-host-key](#)
 - [display-on-mobile](#)
 - [no display-on-mobile](#)
- [ecli/ssl-vpn_show.cdl](#)
 - [show ssl-vpn](#)
- [ecli/switching.cdl](#)
 - [switch](#)
 - [trunk](#)
 - [vlan](#)
 - [no vlan](#)
 - [no trunk port](#)
 - [no trunk ports](#)
 - [portshield](#)
 - [vlan](#)
 - [no vlan](#)
 - [trunked](#)
 - [no trunked](#)
 - [refresh l2-discovery](#)
 - [link-aggregation](#)
 - [key](#)
 - [member](#)
 - [no member](#)
 - [lACP](#)
 - [no lACP](#)
 - [load-balance-type source ip](#)
 - [load-balance-type source mac](#)
 - [load-balance-type source destination](#)
 - [load-balance-type destination](#)
 - [no link-aggregation](#)
 - [port mirror](#)
 - [name](#)
 - [direction](#)
 - [enable](#)
 - [no enable](#)
 - [mirror-port](#)
 - [no mirror-port](#)
 - [mirrored-port](#)
 - [no mirrored-port](#)
 - [no port mirror](#)
 - [no port mirrors](#)
 - [rapid-spanning-tree](#)
 - [version](#)
 - [bridge-priority](#)
 - [no bridge-priority](#)
 - [hello-time](#)
 - [forward-delay](#)
 - [interface](#)
 - [enable](#)
 - [no enable](#)
 - [cost](#)
 - [priority](#)
 - [no priority](#)
 - [dscp-remap value](#)

- [dscp-remap restore-defaults](#)
- [qos output-scheduling](#)
- [qos interface](#)
- [fixed-priority](#)
- [no fixed-priority](#)
- [trust cos](#)
- [no trust cos](#)
- [trust dscp](#)
- [no trust dscp](#)
- [prefer cos](#)
- [no prefer cos](#)
- [default-priority](#)
- [rate-control interface](#)
- [flow-control](#)
- [no flow-control](#)
- [ingress limit](#)
- [ingress rate](#)
- [no ingress rate](#)
- [egress rate](#)
- [no egress rate](#)
- [rate-control restore-defaults](#)
- [port security](#)
- [discard](#)
- [no discard](#)
- [mac-address](#)
- [no mac-address](#)
- [no mac-addresses](#)
- [ecli/switching_show.cdl](#)
 - [show switch](#)
- [ecli/sdwan-perf-class-obj.cdl](#)
 - [performance-class-object](#)
 - [no performance-class-object](#)
 - [no performance-class-objects](#)
 - [name](#)
 - [include](#)
 - [no include](#)
 - [latency](#)
 - [no latency](#)
 - [jitter](#)
 - [no jitter](#)
 - [packet-loss](#)
 - [no packet-loss](#)
 - [comment](#)
 - [no comment](#)
- [ecli/sdwan-probe.cdl](#)
 - [performance-probe](#)
 - [no performance-probe](#)
 - [no performance-probes](#)
 - [name](#)
 - [sdwan-group](#)
 - [no probe target](#)
 - [probe target](#)
 - [probe type](#)
 - [probe interval](#)
 - [reply-timeout](#)
 - [interval missed](#)
 - [interval successful](#)
 - [rst-as-miss](#)
 - [no rst-as-miss](#)
 - [comment](#)
 - [no comment](#)
- [ecli/sdwan-group.cdl](#)
 - [sdwan](#)
 - [no group](#)
 - [no groups](#)
 - [group](#)
 - [name](#)
 - [interface](#)
 - [no interface](#)
 - [priority](#)
- [ecli/sdwan-path-selection-profile.cdl](#)
 - [path-selection-profile](#)
 - [no path-selection-profile](#)
 - [no path-selection-profiles](#)
 - [name](#)
 - [sdwan-group](#)
 - [no sdwan-group](#)
 - [performance-probe](#)
 - [no performance-probe](#)
 - [performance-class](#)
 - [no performance-class](#)
 - [backup-interface](#)
 - [no backup-interface](#)
 - [probe-default-up](#)
 - [no probe-default-up](#)
 - [reset-connections](#)
 - [no reset-connections](#)

- ecli/sdwan-perf-class-obj_show.cdl
 - [show sdwan performance-class-objects](#)
 - [show sdwan performance-class-object](#)
 - ecli/sdwan-probe_show.cdl
 - [show sdwan performance-probes](#)
 - [show sdwan performance-probe](#)
 - ecli/sdwan-group_show.cdl
 - [show sdwan group](#)
 - [show sdwan groups](#)
 - ecli/sdwan-path-selection-profile_show.cdl
 - [show sdwan path-selection-profiles](#)
 - [show sdwan path-selection-profile](#)
-

Syntax

clear

Mode

All Modes

Description

Reset functions.

Syntax

export

Mode

All Modes

Description

Export system status or configuration.

Syntax

no

Mode

All Modes

Description

Negate a command or set its defaults.

Syntax

show

Mode

All Modes

Description

Show system status or configuration.

Syntax

cancel

Mode

All Modes
Top Level

Description

Cancel current changes and return to the previous mode.

Example

cancel

Syntax

commit [best-effort]

Mode

All Modes
Top Level

Description

Commits configuration changes.

Options

best-effort Commits only valid configuration (best effort).

Example

commit

Syntax

end

Mode

Config

Description

End configuration mode.

Example

end

Syntax

end

Mode

All Modes
Top Level
Config

Description

Exits current mode and returns to global configuration mode.

Example

end

Syntax

exit

Mode

All Modes

Description

Exit the current mode.

Example

exit

Syntax

help

Mode

All Modes

Description

Display command help.

Example

help

Syntax

configure [terminal]

Mode

Top Level

Description

Enter configuration mode.

Options

terminal Terminal.

Example

configure

Syntax

no pending-config

Mode

Config

Syntax

```
clear screen
```

Mode

All Modes

Description

Disable command history for the current CLI session.

Example

```
clear screen
```

Syntax

```
no cli history
```

Mode

All Modes

Description

Disable command history for the current CLI session.

Example

```
no cli history
```

Syntax

```
cli history [ size <UINT32> ]
```

Mode

All Modes

Description

Enable command history for the current CLI session.

Options

size Command history buffer size.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
cli history
```

Syntax

```
cli format out { json | plain-text }
```

Mode

All Modes

Description

Set the CLI format.

Options

json Render all CLI output as JSON.

plain-text Render all CLI output as plain-text.

Example

```
cli format out plain-text
```

Syntax

```
cli idle-timeout session <CLI_IDLE_TIMEOUT>
```

Mode

All Modes

Description

Set the maximum time that a session can be idle before being logged off.

Options

<CLI_IDLE_TIMEOUT> Integer in the form: D OR 0xHH.
Max: 60
Example: 5

Example

```
cli idle-timeout session 5
```

Syntax

```
cli idle-timeout default <CLI_IDLE_TIMEOUT>
```

Mode

Config

Description

Set the maximum time that a session can be idle before being logged off.

Options

<CLI_IDLE_TIMEOUT> Integer in the form: D OR 0xHH.
Max: 60
Example: 5

Example

```
cli idle-timeout default 5
```

Syntax

```
cli screen width session <CLI_SCREEN_WIDTH>
```

Mode

All Modes

Description

Set the number of characters on a line.

Options

<CLI_SCREEN_WIDTH> Integer in the form: D OR 0xHHHH.
Min: 80

Max: 2560
Example: 80

Example

```
cli screen width session 80
```

Syntax

```
cli screen width default <CLI_SCREEN_WIDTH>
```

Mode

Config

Description

Set the number of characters on a line.

Options

<CLI_SCREEN_WIDTH> Integer in the form: D OR 0xHHHH.
Min: 80
Max: 2560
Example: 80

Example

```
cli screen width default 80
```

Syntax

```
cli screen length session <CLI_SCREEN_LENGTH>
```

Mode

All Modes

Description

Set the number of lines on screen.

Options

<CLI_SCREEN_LENGTH> Integer in the form: D OR 0xHHHH.
Min: 24
Max: 1600
Example: 24

Example

```
cli screen-length session 24
```

Syntax

```
cli screen length default <CLI_SCREEN_LENGTH>
```

Mode

Config

Description

Set the number of lines on screen.

Options

<CLI_SCREEN_LENGTH> Integer in the form: D OR 0xHHHH.
Min: 24

Max: 1600
Example: 24

Example

```
cli screen length default 24
```

Syntax

```
cli show-unmodified session
```

Mode

Config

Description

Show unmodified pending configuration changes.

Example

```
cli show-unmodified session
```

Syntax

```
cli show-unmodified default
```

Mode

Config

Description

Show unmodified pending configuration changes.

Example

```
cli show-unmodified default
```

Syntax

```
no cli show-unmodified session
```

Mode

Config

Description

Hide unmodified pending configuration changes.

Example

```
no cli show-unmodified session
```

Syntax

```
no cli show-unmodified default
```

Mode

Config

Description

Hide unmodified pending configuration changes.

Example

```
no cli show-unmodified default
```

Syntax

```
cli pager session
```

Mode

All Modes

Description

Enable cli pager.

Example

```
cli pager session
```

Syntax

```
no cli pager session
```

Mode

All Modes

Description

Disable cli pager.

Example

```
no cli pager session
```

Syntax

```
cli pager default
```

Mode

Config

Description

Enable cli pager.

Example

```
cli pager default
```

Syntax

```
no cli pager default
```

Mode

Config

Description

Disable cli pager.

Example

no cli pager default

Syntax

cli interactive-prompts session

Mode

All Modes

Description

Enable cli interactive prompts.

Example

cli interactive-prompts session

Syntax

no cli interactive-prompts session

Mode

All Modes

Description

Disable cli interactive prompts.

Example

no cli interactive-prompts session

Syntax

cli interactive-prompts default

Mode

Config

Description

Enable cli interactive prompts.

Example

cli interactive-prompts default

Syntax

no cli interactive-prompts default

Mode

Config

Description

Disable cli interactive prompts.

Example

no cli interactive-prompts default

Syntax

```
cli ftp user session <WORD>
```

Mode

All Modes

Description

Configure the username for File Transfer Protocol (FTP) connections.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
cli ftp user session Administrator
```

Syntax

```
no cli ftp user session
```

Mode

All Modes

Description

Configure anonymous username for File Transfer Protocol (FTP) connections.

Example

```
cli ftp user session
```

Syntax

```
cli ftp user default <WORD>
```

Mode

Config

Description

Configure the username for File Transfer Protocol (FTP) connections.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
cli ftp user default Administrator
```

Syntax

```
no cli ftp user default
```

Mode

Config

Description

Configure anonymous username for File Transfer Protocol (FTP) connections.

Example

```
cli ftp user default
```

Syntax

```
cli ftp password session <ENC_PASSWORD>
```

Mode

All Modes

Description

Configure the password for File Transfer Protocol (FTP) connections.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
cli ftp password session mysecret
```

Syntax

```
no cli ftp password session
```

Mode

All Modes

Description

Clear password for File Transfer Protocol (FTP) connections.

Example

```
no cli ftp password session
```

Syntax

```
cli ftp password default <ENC_PASSWORD>
```

Mode

Config

Description

Configure the password for File Transfer Protocol (FTP) connections.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
cli ftp password default mysecret
```

Syntax

```
no cli ftp password default
```

Mode

Config

Description

Clear password for File Transfer Protocol (FTP) connections.

Example

```
no cli ftp password default
```

Syntax

```
cli banner { connection | login | logout } <WORD>
```

Mode

Config

Description

CLI banner configuration.

Options

connection Configure connection banner

login Configure login banner

logout Configure logout banner

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
cli banner connection "You have connected to System 88.\nLog in using a valid username and password combination."\ncli banner login "You are now logged into System 88.\nPlease do not make modifications without proper authorization."\ncli banner logout "Thank you for visiting System 88.\nLogin is now terminated."
```

Syntax

```
no cli banner { connection | login | logout }
```

Mode

Config

Description

Clear CLI banner message.

Options

connection Clear connection banner

login Clear login banner

logout Clear logout banner

Example

```
no cli banner connection
no cli banner login
no cli banner logout
```

Syntax

```
show current-config [ with-pending-config ]
```

Mode

All Modes
Top Level
Config

Description

Show current configuration.

Options

with-pending-config View current configuration with pending changes included in the output.

Example

```
show current-config
```

Syntax

```
show current-config [ { custom | default } ] [ with-pending-config ]
```

Mode

Top Level
Config

Description

Show current configuration.

Options

custom Show custom configuration.

default Show system/factory default configuration.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show current-config
```

Syntax

```
show pending-config
```

Mode

All Modes
Top Level

Description

Show pending configuration.

Example

```
show pending-config
```

Syntax

```
show checksum [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show checksum
```

Syntax

```
show cli [ banner | data-model [ { group <INT32> | tag <WORD> } ] | data-store [ group <INT32> ] | debug | ftp | history [ top <UINT16> ] | idle-timeout | interactive-prompts | pager | screen | show-api | show-unmodified | staging-area [ { command-hash | current-mode } ] | token-types ]
```

Mode

All Modes

Description

Show a list of recent commands issued.

Options

| | |
|--|---|
| banner | Show CLI Banner. |
| data-model | Display data model debug information. |
| group <INT32> | Group ID. Integer in the form: D OR 0xHHHHHHHH. Example: 123 |
| tag <WORD> | CGI tag name. Word in the form: WORD or \"QUOTED STRING\". Example: abc |
| data-store group <INT32> | Display data store debug information. Group ID. Integer in the form: D OR 0xHHHHHHHH. Example: 123 |
| debug | Display CLI debug information. |
| ftp | Display CLI FTP configuration. |
| history top <UINT16> | Show a list of recent keywords issued. Show the specified number of recent keywords issued. Integer in the form: D OR 0xHHHH. Example: 123 |
| idle-timeout | Show idle timeout. |
| interactive-prompts | show cli interactive prompts. |
| pager | Show tty pager. |
| screen | Show screen settings. |

| | |
|------------------------|---|
| show-api | Display Show command API debug information. |
| show-unmodified | Show unmodified settings. |
| staging-area | Display staging area debug information. |
| command-hash | Display only the command hash. |
| current-mode | Display only the current mode. |
| token-types | Display token type debug information. |

Example

```
show cli history
```

Syntax

```
ping <HOSTNAME_MIXED> [ interface <WAN_MGMT_INTERFACE> ] [ ipv6-preferred ]
```

Mode

Top Level
Config

Description

Ping the specified host.

Options

| | |
|-----------------------------------|--|
| <HOSTNAME_MIXED> | IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n |
| interface | Route ping request through the specified interface. |
| <WAN_MGMT_INTERFACE> | WAN interface name. Example: X1 |
| ipv6-preferred | Prefer to use IPv6 network. |

Example

```
ping 10.10.10.1
ping fe00::1 ipv6-preferred
ping 10.10.10.1 interface X1
```

Syntax

```
traceroute <HOSTNAME_MIXED> [ interface <WAN_MGMT_INTERFACE> ] [ ipv6-preferred ]
```

Mode

Top Level
Config

Description

Traceroute to the specified host.

Options

| | |
|-----------------------------------|--|
| <HOSTNAME_MIXED> | IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n |
| interface | Route traceroute request through the specified interface. |
| <WAN_MGMT_INTERFACE> | WAN interface name. Example: X1 |
| ipv6-preferred | Prefer to use IPv6 network. |

Example

```
traceroute 10.10.10.1
traceroute fe00::1
```

```
traceroute www.sonicwall.com
traceroute 10.10.10.1 interface X1
```

Syntax

```
diag network-path <IP_V4V6_HOST>
```

Mode

Top Level
Config

Description

Find network path of the specified IP address.

Options

<IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
diag network-path 10.10.10.1
diag network-path fe00::1
```

Syntax

```
network-path <IP_V4V6_HOST>
```

Mode

Top Level
Config

Description

Find network path of the specified IP address.

Options

<IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
network-path 10.10.10.1
network-path fe00::1
```

Syntax

```
nslookup <HOSTNAME> [ ipv6 [ ipv4-dns <IPV4_HOST> ] [ ipv6-dns <IPV6_HOST> ] ]
```

Mode

Top Level
Config

Description

DNS lookup of the specified host.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: example.com

ipv6 DNS lookup IPv6 host.

ipv4-dns IPv4 DNS server.

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.

Example: 192.168.168.168

ipv6-dns IPv6 DNS server.
<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
nslookup 1001::1001 ipv6 ipv4-dns 10.10.10.1
nslookup ipv6.baidu.com ipv6 ipv6-dns 1001::1001
nslookup 10.10.10.1
nslookup www.sonicwall.com
```

Syntax

```
diag reverse-lookup <IP_V4V6_HOST> [ ipv6 [ ipv4-dns <IPV4_HOST> ] [ ipv6-dns <IPV6_HOST> ] ]
```

Mode

Top Level
Config

Description

Resolve the specified reverse name.

Options

<IP_V4V6_HOST> IPV4: address in the form: D.D.D.D\nIPV6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

ipv6 DNS lookup IPv6 host.

ipv4-dns IPv4 DNS server.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

ipv6-dns IPv6 DNS server.

<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
diag reverse-lookup 1001::1001 ipv6 ipv4-dns 10.10.10.1
diag reverse-lookup 10.10.10.1
```

Syntax

```
reverse-lookup <IP_V4V6_HOST> [ ipv6 [ ipv4-dns <IPV4_HOST> ] [ ipv6-dns <IPV6_HOST> ] ]
```

Mode

Top Level
Config

Description

Resolve the specified reverse name.

Options

<IP_V4V6_HOST> IPV4: address in the form: D.D.D.D\nIPV6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

ipv6 DNS lookup IPv6 host.

ipv4-dns IPv4 DNS server.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

ipv6-dns IPv6 DNS server.

<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
reverse-lookup 1001::1001 ipv6 ipv4-dns 10.10.10.1
reverse-lookup 10.10.10.1
```

Syntax

```
diag rbl-lookup ip <IPV4_HOST> domain <HOSTNAME> dns-server <IPV4_HOST>
```

Mode

Top Level
Config

Description

Lookup the specified realtime black list.

Options

ip RBL IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*
domain RBL domain name.
<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*
dns-server RBL DNS server.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
diag rbl-lookup ip 10.10.10.1 domain domainName dns-server 10.10.10.22
```

Syntax

```
rbl-lookup ip <IPV4_HOST> domain <HOSTNAME> dns-server <IPV4_HOST>
```

Mode

Top Level
Config

Description

Lookup the specified realtime black list.

Options

ip RBL IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*
domain RBL domain name.
<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*
dns-server RBL DNS server.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
rbl-lookup ip 10.10.10.1 domain domainName dns-server 10.10.10.22
```

Syntax

```
diag mxlookup <HOSTNAME_MIXED> [ port <IPV4_PORT> ]
```

Mode

Top Level
Config

Description

MX lookup and banner check the specified domain name and SMTP port.

Options

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

port Specified the SMTP port.

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
diag mxlookup 10.10.10.1 port 25
diag mxlookup fe00::1
diag mxlookup www.sonicwall.com
```

Syntax

```
mxlookup <HOSTNAME_MIXED> [ port <IPV4_PORT> ]
```

Mode

Top Level
Config
Anti-Spam

Description

MX lookup and banner check the specified domain name and SMTP port.

Options

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

port Specified the SMTP port.

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
mxlookup 10.10.10.1 port 25
mxlookup fe00::1
mxlookup www.sonicwall.com
```

Syntax

```
diag geo-botnet-lookup <IP_V4V6_HOST>
```

Mode

Top Level
Config

Description

Check GEO location and lookup BOTNET server.

Options

<IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
diag geo-botnet-lookup 10.10.10.1
```

Syntax

```
geo-botnet-lookup <IP_V4V6_HOST>
```

Mode

Top Level
Config
Geo-IP
Botnet

Description

Check GEO location and lookup BOTNET server.

Options

<IP_V4V6_HOST> IPV4: address in the form: D.D.D.D\nIPV6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
geo-botnet-lookup 10.10.10.1
```

Syntax

```
pmtu-discovery <HOSTNAME_MIXED> [ interface <WAN_MGMT_INTERFACE> ]
```

Mode

Top Level
Config

Description

Path MTU discovery to the specified host.

Options

<HOSTNAME_MIXED> IPV4: hostname in the form: D.D.D.D or hostname\nIPV6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

interface Path MTU discovery request through the specified interface.

<WAN_MGMT_INTERFACE> WAN interface name.
Example: X1

Example

```
pmtu-discovery 10.10.10.1  
pmtu-discovery 1001::1001  
pmtu-discovery 10.10.10.1 interface X1
```

Syntax

```
diag show abrentries <IP_V4V6_HOST>
```

Mode

All Modes

Description

Look Up ABR Entries By Destination IP.

Options

<IP_V4V6_HOST> IPV4: address in the form: D.D.D.D\nIPV6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
diag show abrentries 10.10.10.1  
diag show abrentries 1001::1001
```

Syntax

```
diag show processes
```

Mode

All Modes

Description

Show all system processes.

Example

```
diag show processes
```

Syntax

```
diag show process <WORD>
```

Mode

All Modes

Description

Show a system process.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
diag show process tNtp
```

Syntax

```
diag show netstat
```

Mode

All Modes

Description

Show all active connections for Internet protocol sockets.

Example

```
diag show netstat
```

Syntax

```
diag show cores
```

Mode

All Modes

Description

Show all CPU core status information.

Example

```
diag show cores
```

Syntax

diag show core <UINT8>

Mode

All Modes

Description

Show CPU core status information.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

diag show core 1

Syntax

diag show multicore

Mode

All Modes

Description

Show multicore utilization information.

Example

diag show multicore

Syntax

diag show build-info

Mode

All Modes

Description

Show build information.

Example

diag show build-info

Syntax

diag show cpu

Mode

All Modes

Description

Show all cpu information.

Example

diag show cpu

Syntax

diag show web-server

Mode

All Modes

Description

Show all web server information.

Example

diag show web-server

Syntax

diag show fpa

Mode

All Modes

Description

Show fpa information.

Example

diag show fpa

Syntax

diag show mem-pools

Mode

All Modes

Description

Show mem-pools information.

Example

diag show mem-pools

Syntax

diag show memory

Mode

All Modes

Description

Show memory information.

Example

diag show memory

Syntax

```
diag show buf-memzone
```

Mode

All Modes

Description

Show buf-memzone information.

Example

```
diag show buf-memzone
```

Syntax

```
diag show memzone [ summary | verbose ] [ period <UINT32> [ repeat-forever | repeats <UINT32> ] [ on-console ] ]
```

Mode

All Modes

Description

Show memzone information.

Options

| | |
|-----------------------|--|
| summary | Show just a short memory usage summary. |
| verbose | Show verbose output including top memory usage reports. |
| period | Keep showing the information periodically. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: 123 |
| repeat-forever | Repeat forever (or until canceled by 'diag no show memzone period'). |
| repeats | Stop after a number of periodic showings. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: 123 |
| on-console | Print the periodic output on the console port. Note this will not be terminated on logout. |

Example

```
diag show memzone
diag show memzone summary
diag show memzone summary period 2 repeats 10
diag show memzone summary period 2 repeat-forever on-console
```

Syntax

```
diag no show memzone period
```

Mode

All Modes

Description

Stop periodic printing of memzone information.

Options

period Period.

Example

```
diag no show memzone period
```

Syntax

```
diag show tracelog [ current | last ]
```

Mode

All Modes

Description

Show tracelog information.

Options

current Current tracelog.

last Last tracelog.

Example

```
diag show tracelog current
```

Syntax

```
diag clear cp-stats
```

Mode

All Modes

Description

Clear cp-related network driver counters.

Example

```
diag clear cp-stats
```

Syntax

```
diag show cp-stats
```

Mode

All Modes

Description

Show cp-related network driver counters.

Example

```
diag show cp-stats
```

Syntax

```
diag clear hw-stats
```

Mode

All Modes

Description

Clear octeon hardware statistics.

Example

```
diag clear hw-stats
```

Syntax

```
diag clear abr-entries
```

Mode

All Modes

Description

Clear APP route entries.

Example

```
diag clear abr-entries
```

Syntax

```
diag show hw-stats
```

Mode

All Modes

Description

Show octeon hardware statistics.

Example

```
diag show hw-stats
```

Syntax

```
diag show timer-counters
```

Mode

All Modes

Description

Show timer counters.

Example

```
diag show timer-counters
```

Syntax

```
diag show wd-stats
```

Mode

All Modes

Description

Show watchdog statistics.

Example

```
diag show wd-stats
```

Syntax

```
diag clear pp-stats
```

Mode

All Modes

Description

Clear packet processing statistics.

Example

```
diag clear pp-stats
```

Syntax

```
diag show pp-stats
```

Mode

All Modes

Description

Show packet processing statistics.

Example

```
diag show pp-stats
```

Syntax

```
diag clear active-utm
```

Mode

All Modes

Description

Clear active UTM statistics.

Example

```
diag clear active-utm
```

Syntax

```
diag show active-utm
```

Mode

All Modes

Description

Show active UTM statistics.

Example

```
diag show active-utm
```

Syntax

```
diag show debug interface <INTERFACE_NAME>
```

Mode

All Modes

Description

Show interface debug information.

Options

<INTERFACE_NAME> Interface name.
Example: *X0*

Example

```
diag show debug interface "X1"
```

Syntax

```
diag show alerts [ top <UINT32> ]
```

Mode

All Modes

Description

Show alerts.

Options

top Maximum alerts to display.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
diag show alerts  
diag show alerts top 100
```

Syntax

```
diag show log [ top <UINT32> ]
```

Mode

All Modes

Description

Show log entries.

Options

top Maximum entries to display.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
diag show log
diag show log top 100
```

Syntax

```
diag show drop-stats
```

Mode

All Modes

Description

Show packet drop statistics.

Example

```
diag show drop-stats
```

Syntax

```
diag cli pager-test
```

Mode

All Modes

Description

CLI pager test.

Example

```
diag cli pager-test
```

Syntax

```
diag show switch port { counters | status } [ interface <PHYS_INTERFACE> ]
```

Mode

All Modes

Description

Show switch diagnostics information.

Options

| | |
|-------------------------------|--|
| counters | Show port counters information. |
| status | Show port status information. |
| interface | Show switch diagnostics information for the specified interface. |
| <PHYS_INTERFACE> | Physical interface name. Example: X0 |

Example

```
diag show switch port status
diag show switch port status interface "X1"
diag show switch port counters
diag show switch port counters interface "X1"
```

Syntax

```
diag wmi ping-test [ ip <IPV4_HOST> | log | stop ]
```

Mode

All Modes

Description

Ping test.

Options

ip Start ping test at specified host IP.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

log Log ping test.

stop Stop ping test.

Example

```
diag wmi ping-test log
```

Syntax

```
diag wmi reset
```

Mode

All Modes

Description

WMI reset.

Example

```
diag wmi reset
```

Syntax

```
diag wmi lsusb <UINT32>
```

Mode

All Modes

Description

WMI lsusb.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
diag wmi lsusb 4
```

Syntax

```
diag show wmi status
```


Mode

All Modes

Description

Show Wan Modem Interface (WMI) status.

Example

```
diag show wmi status
```

Syntax

```
diag show wmi configs
```

Mode

All Modes

Description

Show Wan Modem Interface Configurations.

Example

```
diag show wmi configs
```

Syntax

```
diag wmi set-primary-config <UINT32>
```

Mode

All Modes

Description

Set the primary Wan Modem configuration.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
diag wmi set-primary-config 2
```

Syntax

```
diag advanced x0-as-mgmt
```

Mode

Config

Description

Default to X0 instead of MGMT for safemode.

Example

```
diag advanced x0-as-mgmt
```

Syntax

diag no advanced x0-as-mgmt

Mode

Config

Description

Disable default to X0 instead of MGMT for safemode.

Example

diag no advanced x0-as-mgmt

Syntax

diag advanced tracelog { all | current | last }

Mode

Config

Description

Set tracelog.

Options

all All.

current Current.

last Last.

Example

tracelog current

Syntax

diag advanced arp

Mode

Config

Description

Configure advanced diag ARP settings.

Example

diag advanced arp

Syntax

bridging

Mode

Diag Advanced ARP Settings

Description

Enable ARP bridging.

Example

bridging

Syntax

no bridging

Mode

Diag Advanced ARP Settings

Description

Disable ARP bridging.

Example

no bridging

Syntax

open-arp-behavior

Mode

Diag Advanced ARP Settings

Description

Enable open ARP behavior (WARNING: Insecure!!).

Example

open-arp-behavior

Syntax

no open-arp-behavior

Mode

Diag Advanced ARP Settings

Description

Disable open ARP behavior.

Example

no open-arp-behavior

Syntax

source-ip-validation

Mode

Diag Advanced ARP Settings

Description

Enable source IP address validation for being directly connected.

Example

source-ip-validation

Syntax

no source-ip-validation

Mode

Diag Advanced ARP Settings

Description

Disable source IP address validation for being directly connected.

Example

no source-ip-validation

Syntax

only-unicast

Mode

Diag Advanced ARP Settings

Description

Enable only allowing ARP entries with unicast addresses.

Example

only-unicast

Syntax

no only-unicast

Mode

Diag Advanced ARP Settings

Description

Disable only allowing ARP entries with unicast addresses.

Example

no only-unicast

Syntax

limit-nonresponsive

Mode

Diag Advanced ARP Settings

Description

Enable limiting ARPs of non-responsive IPs.

Example

limit-nonresponsive

Syntax

no limit-nonresponsive

Mode

Diag Advanced ARP Settings

Description

Disable limiting ARPs of non-responsive IPs.

Example

no limit-nonresponsive

Syntax

bypass-for-l2bridge

Mode

Diag Advanced ARP Settings

Description

Enable bypassing ARP processing on L2 bridge interfaces.

Example

bypass-for-l2bridge

Syntax

no bypass-for-l2bridge

Mode

Diag Advanced ARP Settings

Description

Disable bypassing ARP processing on L2 bridge interfaces.

Example

no bypass-for-l2bridge

Syntax

gratuitous-arp-compatibility

Mode

Diag Advanced ARP Settings

Description

Enable gratuitous ARP compatibility mode.

Example

gratuitous-arp-compatibility

Syntax

no gratuitous-arp-compatibility

Mode

Diag Advanced ARP Settings

Description

Disable gratuitous ARP compatibility mode.

Example

no gratuitous-arp-compatibility

Syntax

gratuitous-arp-limit [amount <UINT32>]

Mode

Diag Advanced ARP Settings

Description

Enable gratuitous ARP limiting and never broadcast more than set number gratuitous ARPs in any 60 second period.

Options

amount Set limit of gratuitous ARPs in any 60 second period.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

gratuitous-arp-limit amount 100

Syntax

no gratuitous-arp-limit

Mode

Diag Advanced ARP Settings

Description

Disable gratuitous ARP limiting.

Example

no gratuitous-arp-limit

Syntax

system-broadcast [interval <UINT32>]

Mode

Diag Advanced ARP Settings

Description

Enable periodically broadcast system ARPs and set the interval.

Options

interval Set the interval for periodically broadcast system ARPs in minutes.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
system-broadcast interval 60
```

Syntax

```
no system-broadcast
```

Mode

Diag Advanced ARP Settings

Description

Disable periodically broadcast system ARPs.

Example

```
no system-broadcast
```

Syntax

```
ignore-arps-with-primary-mac-from-other-if
```

Mode

Diag Advanced ARP Settings

Description

Enable ignore ARPs with primary-gateway's MAC received on other interfaces.

Example

```
ignore-arps-with-primary-mac-from-other-if
```

Syntax

```
no ignore-arps-with-primary-mac-from-other-if
```

Mode

Diag Advanced ARP Settings

Description

Disable ignore ARPs with primary-gateway's MAC received on other interfaces.

Example

```
no ignore-arps-with-primary-mac-from-other-if
```

Syntax

```
display-mac-tracking
```

Mode

Diag Advanced ARP Settings

Description

Enable displaying of MAC tracking information.

Example

display-mac-tracking

Syntax

no display-mac-tracking

Mode

Diag Advanced ARP Settings

Description

Disable displaying of MAC tracking information.

Example

no display-mac-tracking

Syntax

send system-arps

Mode

Diag Advanced ARP Settings

Description

Send system ARPs.

Example

send system-arps

Syntax

diag advanced network

Mode

Config

Description

Configure advanced diag Network and Routing settings.

Example

diag advanced network

Syntax

flush-alternate-path-flows

Mode

Diag Advanced Network Settings

Description

Enable flushing flows on alternate path when normal route path is enabled (affects existing connections).

Example

flush-alternate-path-flows

Syntax

no flush-alternate-path-flows

Mode

Diag Advanced Network Settings

Description

Disable flushing flows on alternate path when normal route path is enabled (affects existing connections).

Example

no flush-alternate-path-flows

Syntax

update-route-version

Mode

Diag Advanced Network Settings

Description

Enable updating route version when route is enabled/disabled (affects existing connections).

Example

update-route-version

Syntax

no update-route-version

Mode

Diag Advanced Network Settings

Description

Disable updating route version when route is enabled/disabled (affects existing connections).

Example

no update-route-version

Syntax

tcp-packet-option-tagging

Mode

Diag Advanced Network Settings

Description

Enable TCP packet option tagging.

Example

tcp-packet-option-tagging

Syntax

no tcp-packet-option-tagging

Mode

Diag Advanced Network Settings

Description

Disable TCP packet option tagging.

Example

no tcp-packet-option-tagging

Syntax

fix-malformed-tcp-headers

Mode

Diag Advanced Network Settings

Description

Enable fix/ignore malformed TCP headers.

Example

fix-malformed-tcp-headers

Syntax

no fix-malformed-tcp-headers

Mode

Diag Advanced Network Settings

Description

Disable fix/ignore malformed TCP headers.

Example

no fix-malformed-tcp-headers

Syntax

sequence-number-randomization

Mode

Diag Advanced Network Settings

Description

Enable TCP sequence number randomization.

Example

sequence-number-randomization

Syntax

no sequence-number-randomization

Mode

Diag Advanced Network Settings

Description

Disable TCP sequence number randomization.

Example

no sequence-number-randomization

Syntax

syn-validation

Mode

Diag Advanced Network Settings

Description

Enable performing SYN validation when not operating in strict TCP compliance mode.

Example

syn-validation

Syntax

no syn-validation

Mode

Diag Advanced Network Settings

Description

Disable performing SYN validation when not operating in strict TCP compliance mode.

Example

no syn-validation

Syntax

clear ospf

Mode

Diag Advanced Network Settings

Description

Clear OSPF process.

Example

clear ospf

Syntax

clear dont-fragment-bit

Mode

Diag Advanced Network Settings

Description

Enable clear DF (don't fragment) bit.

Example

```
clear dont-fragment-bit
```

Syntax

```
no clear dont-fragment-bit
```

Mode

Diag Advanced Network Settings

Description

Disable clear DF (don't fragment) bit.

Example

```
no clear dont-fragment-bit
```

Syntax

```
active-active-clustering-wiremode
```

Mode

Diag Advanced Network Settings

Description

Allow wiremode in Active/Active clustering.

Example

```
active-active-clustering-wiremode
```

Syntax

```
no active-active-clustering-wiremode
```

Mode

Diag Advanced Network Settings

Description

Disable allow wiremode in Active / Active clustering.

Example

```
no active-active-clustering-wiremode
```

Syntax

```
dmz-icmp-redirect
```

Mode

Diag Advanced Network Settings

Description

Enable ICMP redirect on DMZ zone.

Example

```
dmz-icmp-redirect
```

Syntax

```
no dmz-icmp-redirect
```

Mode

Diag Advanced Network Settings

Description

Disable ICMP redirect on DMZ zone.

Example

```
no dmz-icmp-redirect
```

Syntax

```
learning-bridge-filter
```

Mode

Diag Advanced Network Settings

Description

Enable learning-bridge filtering on L2 bridge interfaces.

Example

```
learning-bridge-filter
```

Syntax

```
no learning-bridge-filter
```

Mode

Diag Advanced Network Settings

Description

Disable learning-bridge filtering on L2 bridge interfaces.

Example

```
no learning-bridge-filter
```

Syntax

```
diag advanced dns
```

Mode

Config

Description

Configure advanced diag DNS settings.

Example

```
diag advanced dns
```

Syntax

```
prefer-arpa
```

Mode

Diag Advanced DNS Settings

Description

Enable prefer arpa as suffix when commit ipv6 DNS reverse name resolution.

Example

```
prefer-arpa
```

Syntax

```
no prefer-arpa
```

Mode

Diag Advanced DNS Settings

Description

Disable prefer arpa as suffix when commit ipv6 DNS reverse name resolution.

Example

```
no prefer-arpa
```

Syntax

```
stack-traffic-by-dp
```

Mode

Diag Advanced DNS Settings

Description

Enable stack traffic sending by DP core.

Example

```
stack-traffic-by-dp
```

Syntax

```
no stack-traffic-by-dp
```

Mode

Diag Advanced DNS Settings

Description

Disable stack traffic sending by DP core.

Example

```
no stack-traffic-by-dp
```

Syntax

```
diag advanced dns-security
```

Mode

Config

Description

Configure advanced diag DNS security settings.

Example

```
diag advanced dns-security
```

Syntax

```
dns-tunnel-minimum-packet-number <UINT32>
```

Mode

Diag Advanced DNS Security Settings

Description

Configure the minimum DNS packet number for DNS tunnel detection.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
dns-tunnel-minimum-packet-number 100
```

Syntax

```
dns-tunnel-ratio-threshold <UINT32>
```

Mode

Diag Advanced DNS Security Settings

Description

Configure the ratio threshold for corner DNS types.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
dns-tunnel-ratio-threshold 10
```

Syntax

dns-tunnel-number-threshold <UINT32>

Mode

Diag Advanced DNS Security Settings

Description

Configure the number threshold for normal DNS types.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

dns-tunnel-number-threshold 1000

Syntax

diag advanced dhcp

Mode

Config

Description

Configure advanced diag DHCP settings.

Example

diag advanced dhcp

Syntax

network-pre-discovery

Mode

Diag Advanced DHCP Settings

Description

Enable DHCP server network pre-discovery.

Example

network-pre-discovery

Syntax

no network-pre-discovery

Mode

Diag Advanced DHCP Settings

Description

Disable DHCP server network pre-discovery.

Example

no network-pre-discovery

Syntax

```
conflict-detect-period <UINT16>
```

Mode

Diag Advanced DHCP Settings

Description

Set the DHCP server conflict detect period in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
conflict-detect-period 300
```

Syntax

```
resources-to-discover <UINT8>
```

Mode

Diag Advanced DHCP Settings

Description

Set number of DHCP resources to discover.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
resources-to-discover 10
```

Syntax

```
conflicted-resource-timeout <UINT16>
```

Mode

Diag Advanced DHCP Settings

Description

Set the timeout for conflicted resource to be rechecked in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
conflicted-resource-timeout 1800
```

Syntax

```
available-resource-timeout <UINT16>
```

Mode

Diag Advanced DHCP Settings

Description

Set the timeout for available resource to be rechecked in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
available-resource-timeout 600
```

Syntax

```
save leases
```

Mode

Diag Advanced DHCP Settings

Description

Save DHCP leases to flash.

Example

```
save leases
```

Syntax

```
dhcpnak
```

Mode

Diag Advanced DHCP Settings

Description

Enable sending DHCPNAK if the 'requested IP address' is on the wrong network.

Example

```
dhcpnak
```

Syntax

```
no dhcpnak
```

Mode

Diag Advanced DHCP Settings

Description

Disable sending DHCPNAK if the 'requested IP address' is on the wrong network.

Example

```
no dhcpnak
```

Syntax

```
lease-database-refresh-interval <UINT16>
```

Mode

Diag Advanced DHCP Settings

Description

Set time interval of DHCP lease database to be refreshed in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
lease_database_refresh_interval 600
```

Syntax

```
lease-database-refresh-number <UINT16>
```

Mode

Diag Advanced DHCP Settings

Description

Set number of DHCP leases in database to be refreshed.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
lease_database_refresh_number 10
```

Syntax

```
recycle-expired-lease
```

Mode

Diag Advanced DHCP Settings

Description

Enable aggressively recycle expired DHCP leases in advance.

Example

```
recycle-expired-lease
```

Syntax

```
no recycle-expired-lease
```

Mode

Diag Advanced DHCP Settings

Description

Disable aggressively recycle expired DHCP leases in advance.

Example

```
no recycle-expired-lease
```

Syntax

diag advanced voip

Mode

Config

Description

Configure advanced diag VoIP settings.

Example

diag advanced voip

Syntax

max-endpoints <UINT16>

Mode

Diag Advanced VoIP Settings

Description

Set the maximum 'public' VoIP endpoints.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

max-endpoints 2048

Syntax

no max-endpoints

Mode

Diag Advanced VoIP Settings

Description

Clear the maximum 'public' VoIP endpoints.

Example

no max-endpoints

Syntax

auto-add-sip

Mode

Diag Advanced VoIP Settings

Description

Enable auto-add SIP endpoints.

Example

```
auto-add-sip
```

Syntax

```
no auto-add-sip
```

Mode

Diag Advanced VoIP Settings

Description

Disable auto-add SIP endpoints.

Example

```
no auto-add-sip
```

Syntax

```
sip-transforms
```

Mode

Diag Advanced VoIP Settings

Description

Enable transforming SIP URIs to have an explicit port.

Example

```
sip-transforms
```

Syntax

```
no sip-transforms
```

Mode

Diag Advanced VoIP Settings

Description

Disable transforming SIP URIs to have an explicit port.

Example

```
no sip-transforms
```

Syntax

```
invite-flush
```

Mode

Diag Advanced VoIP Settings

Description

Enable flush active media for SIP INVITES without SDP.

Example

flush-active-media

Syntax

no invite-flush

Mode

Diag Advanced VoIP Settings

Description

Disable flush active media for SIP INVITEs without SDP.

Example

no invite-flush

Syntax

invite-flush-unused

Mode

Diag Advanced VoIP Settings

Description

Enable flush unused media for SIP INVITEs without SDP.

Example

invite-flush-unused

Syntax

no invite-flush-unused

Mode

Diag Advanced VoIP Settings

Description

Disable flush unused media for SIP INVITEs without SDP.

Example

no invite-flush-unused

Syntax

reset sip-database

Mode

Diag Advanced VoIP Settings

Description

Reset sip database.

Example

reset sip-database

Syntax

diag advanced vpn

Mode

Config

Description

Configure advanced diag VPN settings.

Example

diag advanced vpn

Syntax

adjust-tcp-mss

Mode

Diag Advanced VPN Settings

Description

Enable adjusting TCP MSS option for VPN traffic.

Example

adjust-tcp-mss

Syntax

no adjust-tcp-mss

Mode

Diag Advanced VPN Settings

Description

Do not adjusting TCP MSS option for VPN traffic.

Example

no adjust-tcp-mss

Syntax

interoperable-ike-dh-exchange

Mode

Diag Advanced VPN Settings

Description

Enable using interoperable IKE DH exchange .

Example

interoperable-ike-dh-exchange

Syntax

no interoperable-ike-dh-exchange

Mode

Diag Advanced VPN Settings

Description

Disable using interoperable IKE DH exchange .

Example

no interoperable-ike-dh-exchange

Syntax

fragment-after-esp

Mode

Diag Advanced VPN Settings

Description

Enable fragmenting VPN packets after applying ESP.

Example

fragment-after-esp

Syntax

no fragment-after-esp

Mode

Diag Advanced VPN Settings

Description

Disable fragmenting VPN packets after applying ESP.

Example

no fragment-after-esp

Syntax

spi-cpi-parameter-index

Mode

Diag Advanced VPN Settings

Description

Enable using SPI/CPI parameter index for IPsec/IPcomp passthru connections.

Example

spi-cpi-parameter-index

Syntax

no spi-cpi-parameter-index

Mode

Diag Advanced VPN Settings

Description

Disable using SPI/CPI parameter index for IPsec/IPcomp passthru connections.

Example

no spi-cpi-parameter-index

Syntax

trust-built-in-ca

Mode

Diag Advanced VPN Settings

Description

Enable trust built-in CA certificates for IKE authentication and local certificate import.

Example

trust-built-in-ca

Syntax

no trust-built-in-ca

Mode

Diag Advanced VPN Settings

Description

Disable trust built-in CA certificates for IKE authentication and local certificate import.

Example

no trust-built-in-ca

Syntax

preserve-ike-port

Mode

Diag Advanced VPN Settings

Description

Enable preserve IKE port for pass through connections.

Example

preserve-ike-port

Syntax

no preserve-ike-port

Mode

Diag Advanced VPN Settings

Description

Disable preserve IKE port for pass through connections.

Example

```
no preserve-ike-port
```

Syntax

```
diag advanced encryption
```

Mode

Config

Description

Configure advanced diag encryption settings.

Example

```
diag advanced encryption
```

Syntax

```
hardware-encryption
```

Mode

Diag Advanced Encryption

Description

Enable hardware encryption.

Example

```
hardware-encryption
```

Syntax

```
no hardware-encryption
```

Mode

Diag Advanced Encryption

Description

Disable hardware encryption.

Example

```
no hardware-encryption
```

Syntax

```
dp-stack
```

Mode

Diag Advanced Encryption

Description

Enable DP stack processing.

Example

```
dp-stack
```

Syntax

```
no dp-stack
```

Mode

Diag Advanced Encryption

Description

Disable DP stack processing.

Example

```
no dp-stack
```

Syntax

```
ssl-v3
```

Mode

Diag Advanced Encryption

Description

Enable SSLv3.

Example

```
ssl-v3
```

Syntax

```
no ssl-v3
```

Mode

Diag Advanced Encryption

Description

Disable SSLv3.

Example

```
no ssl-v3
```

Syntax

```
tls-v1
```

Mode

Diag Advanced Encryption

Description

Enable TLSv1.

Example

```
tls-v1
```

Syntax

```
no tls-v1
```

Mode

Diag Advanced Encryption

Description

Disable TLSv1.

Example

```
no tls-v1
```

Syntax

```
diag advanced firewall
```

Mode

Config

Description

Configure advanced diag firewall settings.

Example

```
diag advanced firewall
```

Syntax

```
ftp-bounce-attack-protection
```

Mode

All Modes

Description

Enable FTP bounce attack protection.

Example

```
ftp-bounce-attack-protection
```

Syntax

```
no ftp-bounce-attack-protection
```

Mode

All Modes

Description

Disable FTP bounce attack protection.

Example

```
no ftp-bounce-attack-protection
```

Syntax

```
ftp-protocol-anomaly-attack-protection
```

Mode

All Modes

Description

Enable FTP protocol anomaly attack protection.

Example

```
ftp-protocol-anomaly-attack-protection
```

Syntax

```
no ftp-protocol-anomaly-attack-protection
```

Mode

All Modes

Description

Disable FTP protocol anomaly attack protection.

Example

```
no ftp-protocol-anomaly-attack-protection
```

Syntax

```
orphan-data-connection
```

Mode

All Modes

Description

Enable allow orphan data connections.

Example

```
orphan-data-connection
```

Syntax

```
no orphan-data-connection
```

Mode

All Modes

Description

Disable allow orphan data connections.

Example

no orphan-data-connection

Syntax

ip-spoof-checking

Mode

All Modes

Description

Enable IP spoof checking.

Example

ip-spoof-checking

Syntax

no ip-spoof-checking

Mode

All Modes

Description

Disable IP spoof checking.

Example

no ip-spoof-checking

Syntax

port-scan-detection

Mode

All Modes

Description

Enable port scan detection.

Example

port-scan-detection

Syntax

no port-scan-detection

Mode

All Modes

Description

Disable port scan detection.

Example

no port-scan-detection

Syntax

anticipated-connection-timeout <UINT32>

Mode

All Modes

Description

Set timeout for anticipated TCP/UDP connections (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

anticipated-connection-timeout 10

Syntax

no anticipated-connection-timeout

Mode

All Modes

Description

Clear timeout for anticipated TCP/UDP connections (seconds).

Example

no anticipated-connection-timeout

Syntax

anticipated-connection-parent-termination

Mode

All Modes

Description

Enable termination of parent on timeout of anticipated TCP/UDP connections.

Example

anticipated-connection-parent-termination

Syntax

no anticipated-connection-parent-termination

Mode

All Modes

Description

Disable termination of parent on timeout of anticipated TCP/UDP connections.

Example

```
no anticipated-connection-parent-termination
```

Syntax

```
anticipated-media-timeout <UINT32>
```

Mode

All Modes

Description

Set timeout for anticipated media connections(seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
anticipated-media-timeout 60
```

Syntax

```
no anticipated-media-timeout
```

Mode

All Modes

Description

Clear timeout for anticipated media connections(seconds).

Example

```
no anticipated-media-timeout
```

Syntax

```
anticipated-media-parent-termination
```

Mode

All Modes

Description

Enable termination of parent on timeout of anticipated media connections.

Example

```
anticipated-media-parent-termination
```

Syntax

```
no anticipated-media-parent-termination
```

Mode

All Modes

Description

Disable termination of parent on timeout of anticipated media connections.

Example

```
no anticipated-media-parent-termination
```

Syntax

```
trace-connections-port <IPV4_PORT>
```

Mode

All Modes

Description

Set TCP port to trace connections to.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
trace-connections-port 8080
```

Syntax

```
no trace-connections-port
```

Mode

All Modes

Description

Clear TCP port to trace connections to.

Example

```
no trace-connections-port
```

Syntax

```
include-tcp-data-connection
```

Mode

All Modes

Description

Enable include TCP data connections in traces.

Example

```
include-tcp-data-connection
```

Syntax

```
no include-tcp-data-connection
```

Mode

All Modes

Description

Disable include TCP data connections in traces.

Example

```
no include-tcp-data-connection
```

Syntax

```
track-bandwidth-usage
```

Mode

All Modes

Description

Enable tracking bandwidth usage for default traffic.

Example

```
track-bandwidth-usage
```

Syntax

```
no track-bandwidth-usage
```

Mode

All Modes

Description

Disable tracking bandwidth usage for default traffic.

Example

```
no track-bandwidth-usage
```

Syntax

```
decrease-connection-count-after-close
```

Mode

All Modes

Description

Enable decreasing connection count immediately after TCP connection close.

Example

```
decrease-connection-count-after-close
```

Syntax

```
no decrease-connection-count-after-close
```

Mode

All Modes

Description

Disable decreasing connection count immediately after TCP connection close.

Example

```
no decrease-connection-count-after-close
```

Syntax

```
tcp-state-manipulation-dos-protection
```

Mode

All Modes

Description

Enable protection against TCP state manipulation DoS.

Example

```
tcp-state-manipulation-dos-protection
```

Syntax

```
no tcp-state-manipulation-dos-protection
```

Mode

All Modes

Description

Disable protection against TCP state manipulation DoS.

Example

```
no tcp-state-manipulation-dos-protection
```

Syntax

```
sequential-addresses
```

Mode

All Modes

Description

Enable allocation of sequential addresses when performing many-to-few NAT.

Example

```
sequential-addresses
```

Syntax

```
no sequential-addresses
```

Mode

All Modes

Description

Disable allocation of sequential addresses when performing many-to-few NAT.

Example

no sequential-addresses

Syntax

default-policy-editable

Mode

All Modes

Description

Enable the ability to remove and fully edit auto-added access rules and NATs.

Example

default-policy-editable

Syntax

no default-policy-editable

Mode

All Modes

Description

Disable the ability to remove and fully edit auto-added access rules and NATs.

Example

no default-policy-editable

Syntax

udp-icmp-flood-detecting

Mode

All Modes

Description

Enable aggressive UDP/ICMP flood detecting.

Example

udp-icmp-flood-detecting

Syntax

no udp-icmp-flood-detecting

Mode

All Modes

Description

Disable aggressive UDP/ICMP flood detecting.

Example

no udp-icmp-flood-detecting

Syntax

clear connections

Mode

All Modes

Description

Clear connections.

Example

flush connections

Syntax

diag advanced support-windows-messenger

Mode

Config

Description

Enable support for windows messenger.

Example

diag advanced support-windows-messenger

Syntax

diag no advanced support-windows-messenger

Mode

Config

Description

Disable support for windows messenger.

Example

diag no advanced support-windows-messenger

Syntax

diag advanced security-services

Mode

Config

Description

Configure advanced diag security services settings.

Example

diag advanced security-services

Syntax

dpi-engine

Mode

Diag Advanced Security Services Settings

Description

Enable DPI engine.

Example

dpi-engine

Syntax

no dpi-engine

Mode

Diag Advanced Security Services Settings

Description

Disable DPI engine.

Example

no dpi-engine

Syntax

bidirectional-ips

Mode

Diag Advanced Security Services Settings

Description

Enable applying IPS signatures bidirectionally.

Example

bidirectional-ips

Syntax

no bidirectional-ips

Mode

Diag Advanced Security Services Settings

Description

Disable applying IPS signatures bidirectionally.

Example

no bidirectional-ips

Syntax

dpi-ip-fragment-reassembly

Mode

Diag Advanced Security Services Settings

Description

Enable IP fragment reassembly in DPI.

Example

dpi-ip-fragment-reassembly

Syntax

no dpi-ip-fragment-reassembly

Mode

Diag Advanced Security Services Settings

Description

Disable IP fragment reassembly in DPI.

Example

no dpi-ip-fragment-reassembly

Syntax

dev-debug

Mode

Diag Advanced Security Services Settings

Description

Enable extra dev debug info.

Example

dev-debug

Syntax

no dev-debug

Mode

Diag Advanced Security Services Settings

Description

Disable extra dev debug info.

Example

no dev-debug

Syntax

smtp-chunking-modification

Mode

Diag Advanced Security Services Settings

Description

Enable App-Firewall SMTP CHUNKING modification.

Example

smtp-chunking-modification

Syntax

no smtp-chunking-modification

Mode

Diag Advanced Security Services Settings

Description

Disable App-Firewall SMTP CHUNKING modification.

Example

no smtp-chunking-modification

Syntax

pop3-auto-deletion

Mode

Diag Advanced Security Services Settings

Description

Enable gateway AV POP3 auto deletion.

Example

pop3-auto-deletion

Syntax

no pop3-auto-deletion

Mode

Diag Advanced Security Services Settings

Description

Disable gateway AV POP3 auto deletion.

Example

no pop3-auto-deletion

Syntax

pop3-uidl-rewriting

Mode

Diag Advanced Security Services Settings

Description

Enable gateway AV POP3 UIDL rewriting.

Example

```
pop3-uidl-rewriting
```

Syntax

```
no pop3-uidl-rewriting
```

Mode

Diag Advanced Security Services Settings

Description

Disable gateway AV POP3 UIDL rewriting.

Example

```
no pop3-uidl-rewriting
```

Syntax

```
smb-read-write-enforcement
```

Mode

Diag Advanced Security Services Settings

Description

Enable gateway AV SMB read/write ordering enforcement.

Example

```
smb-read-write-enforcement
```

Syntax

```
no smb-read-write-enforcement
```

Mode

Diag Advanced Security Services Settings

Description

Disable gateway AV SMB read/write ordering enforcement.

Example

```
no smb-read-write-enforcement
```

Syntax

```
keep-http-accept-range-bytes
```

Mode

Diag Advanced Security Services Settings

Description

Keep HTTP header Accept-range: bytes.

Example

```
keep-http-accept-range-bytes
```

Syntax

```
no keep-http-accept-range-bytes
```

Mode

Diag Advanced Security Services Settings

Description

Don't keep HTTP header Accept-range: bytes.

Example

```
no keep-http-accept-range-bytes
```

Syntax

```
log-virus-uri
```

Mode

Diag Advanced Security Services Settings

Description

Enable log virus URI.

Example

```
log-virus-uri
```

Syntax

```
no log-virus-uri
```

Mode

Diag Advanced Security Services Settings

Description

Disable log virus URI.

Example

```
no log_virus_uri
```

Syntax

```
offset-qualifier-signature
```

Mode

Diag Advanced Security Services Settings

Description

Enable apply signatures containing file offset qualifiers
 that trigger on TCP streams with unidentified protocols.

Example

```
offset-qualifier-signature
```

Syntax

```
no offset-qualifier-signature
```

Mode

Diag Advanced Security Services Settings

Description

Disable apply signatures containing file offset qualifiers
 that trigger on TCP streams with unidentified protocols.

Example

```
no offset-qualifier-signature
```

Syntax

```
minimum-http-header-length <UINT16>
```

Mode

Diag Advanced Security Services Settings

Description

Set minimum HTTP header length (0 to disable).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
minimum-http-header-length 0
```

Syntax

```
no minimum-http-header-length
```

Mode

Diag Advanced Security Services Settings

Description

Clear minimum HTTP header length (0 to disable).

Example

```
no minimum-http-header-length
```

Syntax

```
incremental-signature-updates
```

Mode

Diag Advanced Security Services Settings

Description

Enable incremental updates to IDP, GAV and SPY signature databases.

Example

```
incremental-signature-updates
```

Syntax

```
no incremental-signature-updates
```

Mode

Diag Advanced Security Services Settings

Description

Disable incremental updates to IDP, GAV and SPY signature databases.

Example

```
no incremental-signature-updates
```

Syntax

```
force-utm-offload
```

Mode

Diag Advanced Security Services Settings

Description

Enable force UTM offload.

Example

```
force-utm-offload
```

Syntax

```
no force-utm-offload
```

Mode

Diag Advanced Security Services Settings

Description

Disable force UTM offload.

Example

```
no force-utm-offload
```

Syntax

```
utm-traffic-offload <UINT8>
```

Mode

Diag Advanced Security Services Settings

Description

Set Active/Active UTM traffic Offload percentage.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
utm-traffic-offload 60
```

Syntax

```
no utm-traffic-offload
```

Mode

Diag Advanced Security Services Settings

Description

Clear Active/Active UTM traffic Offload percentage.

Example

```
no utm-traffic-offload
```

Syntax

```
limit-dpi-tcp-window-advertisement [ maximum <UINT16> ]
```

Mode

Diag Advanced Security Services Settings

Description

Enable enforcement of a limit on maximum allowed advertised TCP window with any DPI-based service enabled and set the maximum allowed.

Options

maximum Set the maximum allowed advertised TCP window with any DPI-based service enabled.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
limit-dpi-tcp-window-advertisement maximum 256
```

Syntax

```
no limit-dpi-tcp-window-advertisement
```

Mode

Diag Advanced Security Services Settings

Description

Disable enforcement of a limit on maximum allowed advertised TCP window with any DPI-based service enabled.

Example

```
no limit-dpi-tcp-window-advertisement
```

Syntax

```
threshold-limit <UINT32>
```

Mode

Diag Advanced Security Services Settings

Description

Threshold above which size limits are enforced on regex automaton.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
threshold-limit 5000
```

Syntax

```
maximum-regex-automaton-size <UINT32>
```

Mode

Diag Advanced Security Services Settings

Description

Maximum allowed size for regex automaton.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
maximum-regex-automaton-size 10000
```

Syntax

```
signature-database-reload
```

Mode

Diag Advanced Security Services Settings

Description

Enable signature database reload.

Example

```
signature-database-reload
```

Syntax

```
no signature-database-reload
```

Mode

Diag Advanced Security Services Settings

Description

Disable signature database reload.

Example

```
no signature-database-reload
```

Syntax

```
process-ips-signatures
```

Mode

Diag Advanced Security Services Settings

Description

Enable processing of IPS signatures.

Example

```
process-ips-signatures
```

Syntax

```
no process-ips-signatures
```

Mode

Diag Advanced Security Services Settings

Description

Disable processing of IPS signatures.

Example

```
no process-ips-signatures
```

Syntax

```
process-gav-signatures
```

Mode

Diag Advanced Security Services Settings

Description

Enable processing of GAV signatures.

Example

```
process-gav-signatures
```

Syntax

```
no process-gav-signatures
```

Mode

Diag Advanced Security Services Settings

Description

Disable processing of GAV signatures.

Example

no process-gav-signatures

Syntax

process-anti-spyware-signatures

Mode

Diag Advanced Security Services Settings

Description

Enable processing of Anti-Spyware signatures.

Example

process-anti-spyware-signatures

Syntax

no process-anti-spyware-signatures

Mode

Diag Advanced Security Services Settings

Description

Disable processing of Anti-Spyware signatures.

Example

no process-anti-spyware-signatures

Syntax

process-app-signatures

Mode

Diag Advanced Security Services Settings

Description

Enable processing of App signatures.

Example

process-app-signatures

Syntax

no process-app-signatures

Mode

Diag Advanced Security Services Settings

Description

Disable processing of App signatures.

Example

no process-app-signatures

Syntax

optimal-value [val <UINT32>]

Mode

Diag Advanced Security Services Settings

Description

Enable optimal value and set the value.

Options

val Set the optimal value.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

optimal-value 10240

Syntax

no optimal-value

Mode

Diag Advanced Security Services Settings

Description

Disable optimal value and set the value.

Example

no optimal-value

Syntax

limit-ips-cft-scan

Mode

Diag Advanced Security Services Settings

Description

Eable limit IPS CFT scan.

Example

limit-ips-cft-scan

Syntax

no limit-ips-cft-scan

Mode

Diag Advanced Security Services Settings

Description

Disable limit IPS CFT scan.

Example

```
no limit-ips-cft-scan
```

Syntax

```
enforce-cfs-host-tag-search
```

Mode

Diag Advanced Security Services Settings

Description

Enable enforcement of host tag search for CFS.

Example

```
enforce-cfs-host-tag-search
```

Syntax

```
no enforce-cfs-host-tag-search
```

Mode

Diag Advanced Security Services Settings

Description

Disable enforcement of host tag search for CFS.

Example

```
no enforce-cfs-host-tag-search
```

Syntax

```
local-cfs-server [ primary <HOSTNAME_MIXED> ] [ secondary <HOSTNAME_MIXED> ]
```

Mode

Diag Advanced Security Services Settings

Description

Enable local CFS server and set the IP addresses.

Options

| | |
|-------------------------------|--|
| primary | Primary local CFS server. |
| <HOSTNAME_MIXED> | IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: 2001:cdba:0000:0000:0000:0000:3257:9652\n |
| secondary | Secondary local CFS server. |
| <HOSTNAME_MIXED> | IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: 2001:cdba:0000:0000:0000:0000:3257:9652\n |

Example

```
local-cfs-server
local-cfs-server primary 10.10.10.10
local-cfs-server secondary 10.10.10.11
```

Syntax

```
no local-cfs-server
```

Mode

Diag Advanced Security Services Settings

Description

Disable local CFS server.

Example

```
no local-cfs-server
```

Syntax

```
client-anti-virus-timeout <UINT32>
```

Mode

Diag Advanced Security Services Settings

Description

Set client AV cache timeout (minutes).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
client-anti-virus-timeout 5
```

Syntax

```
reset av-info
```

Mode

Diag Advanced Security Services Settings

Description

Reset AV info.

Example

```
reset av-info
```

Syntax

```
reset next-gen-av cache
```

Mode

Diag Advanced Security Services Settings

Description

Reset Next-Gen AV client status cache.

Options

cache Reset Next-Gen AV client status cache.

Example

```
reset next-gen-av cache
```

Syntax

reset licenses

Mode

Diag Advanced Security Services Settings

Description

Reset licenses and security services info.

Example

reset licenses

Syntax

reset client-content-filtering info

Mode

Diag Advanced Security Services Settings

Description

Reset client CF enforcement info.

Options

info Reset client CF enforcement info.

Example

reset client-content-filtering info

Syntax

reset client-content-filtering cache

Mode

Diag Advanced Security Services Settings

Description

Reset client CF enforcement cache.

Options

cache Reset client CF enforcement cache.

Example

reset client-content-filtering cache

Syntax

reset http-clientless-notification-cache

Mode

Diag Advanced Security Services Settings

Description

Reset HTTP clientless notification cache.

Example

```
reset http-clientless-notification-cache
```

Syntax

```
reset cloud-av-cache
```

Mode

Diag Advanced Security Services Settings

Description

Reset cloud AV cache.

Example

```
reset cloud-av-cache
```

Syntax

```
cloud-av-server [ host <HOSTNAME> ]
```

Mode

Diag Advanced Security Services Settings

Description

Enable private cloud AV server and set the IP address.

Options

| | |
|-------------------------|---|
| host | Private cloud AV server IP or name. |
| <HOSTNAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i> |

Example

```
cloud-av-server  
cloud-av-server host 10.10.10.12
```

Syntax

```
no cloud-av-server
```

Mode

Diag Advanced Security Services Settings

Description

Disable private cloud AV server.

Example

```
no cloud-av-server
```

Syntax

```
diag advanced dpi-ssl
```

Mode

Config

Description

Configure advanced diag DPI-SSL settings.

Example

```
diag advanced dpi-ssl
```

Syntax

```
rewritten-certificate-sn-modifier <UINT16>
```

Mode

Diag Advanced DPI-SSL Settings

Description

Set rewritten certificate SN modifier.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
rewritten-certificate-sn-modifier 1
```

Syntax

```
client-spoofed-certificate-caching
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable client spoofed certificate caching.

Example

```
client-spoofed-certificate-caching
```

Syntax

```
no client-spoofed-certificate-caching
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable client spoofed certificate caching.

Example

```
no client-spoofed-certificate-caching
```

Syntax

```
remove-tcp-timestamp-option
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable removing TCP timestamp option.

Example

```
remove-tcp-timestamp-option
```

Syntax

```
no remove-tcp-timestamp-option
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable removing TCP timestamp option.

Example

```
no remove-tcp-timestamp-option
```

Syntax

```
drop-ssl-on-low-memory
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable dropping SSL packets when memory low.

Example

```
drop-ssl-on-low-memory
```

Syntax

```
no drop-ssl-on-low-memory
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable dropping SSL packets when memory low.

Example

```
no drop-ssl-on-low-memory
```

Syntax

```
proxyless-ssl-when-limit-exceeded
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable allowing SSL without proxy when connection limit exceeded.

Example

```
proxyless-ssl-when-limit-exceeded
```

Syntax

```
no proxyless-ssl-when-limit-exceeded
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable allowing SSL without proxy when connection limit exceeded.

Example

```
no proxyless-ssl-when-limit-exceeded
```

Syntax

```
endpoint-tcp-window-setup
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable endpoint TCP window setup.

Example

```
endpoint-tcp-window-setup
```

Syntax

```
no endpoint-tcp-window-setup
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable endpoint TCP window setup.

Example

```
no endpoint-tcp-window-setup
```

Syntax

```
server-facing-session-reuse
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable server facing session reuse.

Example

```
server-facing-session-reuse
```

Syntax

```
no server-facing-session-reuse
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable server facing session reuse.

Example

```
no server-facing-session-reuse
```

Syntax

```
block-untrusted-certificate-connections
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable blocking connections to sites with untrusted certificates.

Example

```
block-untrusted-certificate-connections
```

Syntax

```
no block-untrusted-certificate-connections
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable blocking connections to sites with untrusted certificates.

Example

```
no block-untrusted-certificate-connections
```

Syntax

```
max-stream-offset <UINT16>
```

Mode

Diag Advanced DPI-SSL Settings

Description

Set max stream offset to check for SSL client-hello resemblance.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
max-stream-offset 512
```

Syntax

```
no max-stream-offset
```

Mode

Diag Advanced DPI-SSL Settings

Description

Clear max stream offset to check for SSL client-hello resemblance.

Example

```
no max-stream-offset
```

Syntax

```
tcp-window-multiplier <UINT8>
```

Mode

Diag Advanced DPI-SSL Settings

Description

Set TCP window multiplier (N *64k).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
tcp-window-multiplier 8
```

Syntax

```
tcp-min-adv-window <UINT8>
```

Mode

Diag Advanced DPI-SSL Settings

Description

Set TCP Min Advertised window (N * 1k).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
tcp-min-adv-window 16
```

Syntax

max-proxied-connections <UINT16>

Mode

Diag Advanced DPI-SSL Settings

Description

Set the override for max proxied SSL connections.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

max-proxied-connections 0

Syntax

no max-proxied-connections

Mode

Diag Advanced DPI-SSL Settings

Description

Clear the override for max proxied SSL connections.

Example

no max-proxied-connections

Syntax

update-security-services-info

Mode

Diag Advanced DPI-SSL Settings

Description

Update licenses and security services info.

Example

update-security-services-info

Syntax

ssl-version { *ssl-v23* | *ssl-v3* | *tls-v1* }

Mode

Diag Advanced DPI-SSL Settings

Description

Set ssl version.

Options

ssl-v23 ssl version23.

ssl-v3 ssl version3.0.

tls-v1 tls version1.0.

Example

```
ssl-version ssl-v3
```

Syntax

```
cipher-method { compatible | secure }
```

Mode

Diag Advanced DPI-SSL Settings

Description

Set ssl cipher method.

Options

compatible Compatible ciphers method.

secure Secure ciphers method.

Example

```
cipher-method secure
```

Syntax

```
diag advanced high-availability
```

Mode

Config

Description

Configure advanced diag High Availability settings.

Example

```
diag advanced high-availability
```

Syntax

```
idle-monitor
```

Mode

Diag Advanced High Availability Settings

Description

Enable network monitor probing on idle unit.

Example

```
idle-monitor
```

Syntax

no idle-monitor

Mode

Diag Advanced High Availability Settings

Description

Disable network monitor probing on idle unit.

Example

no idle-monitor

Syntax

suppress-active-transition-alarm

Mode

Diag Advanced High Availability Settings

Description

Enable suppressing alarm on HA transition to active.

Example

suppress-active-transition-alarm

Syntax

no suppress-active-transition-alarm

Mode

Diag Advanced High Availability Settings

Description

Disable suppressing alarm on HA transition to active.

Example

no suppress-active-transition-alarm

Syntax

restart-backup-on-watchdog

Mode

Diag Advanced High Availability Settings

Description

Enable always restarting HA backup for watchdog task.

Example

restart-backup-on-watchdog

Syntax

no restart-backup-on-watchdog

Mode

Diag Advanced High Availability Settings

Description

Disable always restarting HA backup for watchdog task .

Example

no restart-backup-on-watchdog

Syntax

interleave-cache

Mode

Diag Advanced High Availability Settings

Description

Enable interleave connection cache state synchronization messages.

Example

interleave-cache

Syntax

no interleave-cache

Mode

Diag Advanced High Availability Settings

Description

Disable interleave connection cache state synchronization messages.

Example

no interleave-cache

Syntax

transparent-mode-gratuitous-arp

Mode

Diag Advanced High Availability Settings

Description

Enable sending gratuitous ARP to DMZ or LAN on transparent mode while HA failover.

Example

transparent-mode-gratuitous-arp

Syntax

no transparent-mode-gratuitous-arp

Mode

Diag Advanced High Availability Settings

Description

Disable sending gratuitous ARP to DMZ or LAN on transparent mode while HA failover.

Example

```
no transparent-mode-gratuitous-arp
```

Syntax

```
max-transparent-mode-gratuitous-arps <UINT32>
```

Mode

Diag Advanced High Availability Settings

Description

Set maximum number of gratuitous ARP of transparent mode per interface while HA failover.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
max-transparent-mode-gratuitous-arps 256
```

Syntax

```
max-gratuitous-arps <UINT32>
```

Mode

Diag Advanced High Availability Settings

Description

Set maximum number of gratuitous ARP while HA failover.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
max-gratuitous-arps 1
```

Syntax

```
diag advanced pppoe
```

Mode

Config

Description

Configure advanced diag PPPoE settings.

Example

```
diag advanced pppoe
```

Syntax

lcp-requests

Mode

Diag Advanced PPPoE Settings

Description

Enable allowing LCP requests to PPPoE server.

Example

lcp-requests

Syntax

no lcp-requests

Mode

Diag Advanced PPPoE Settings

Description

Disable allowing LCP requests to PPPoE server.

Example

no lcp-requests

Syntax

log-lcp-echo

Mode

Diag Advanced PPPoE Settings

Description

Enable logging LCP echo requests and replies between client and server.

Example

log-lcp-echo

Syntax

no log-lcp-echo

Mode

Diag Advanced PPPoE Settings

Description

Disable logging LCP echo requests and replies between client and server.

Example

no log-lcp-echo

Syntax

end-of-list-tag

Mode

Diag Advanced PPPoE Settings

Description

Enable PPPoE End-Of-List tag.

Example

end-of-list-tag

Syntax

no end-of-list-tag

Mode

Diag Advanced PPPoE Settings

Description

Disable PPPoE End-Of-List tag.

Example

no end-of-list-tag

Syntax

netmask <HOST_IP>

Mode

Diag Advanced PPPoE Settings

Description

Set PPPoE netmask.

Options

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

netmask 255.255.255.252

Syntax

no netmask

Mode

Diag Advanced PPPoE Settings

Description

Clear PPPoE netmask.

Example

no netmask

Syntax

diag advanced dial-up

Mode

Config

Description

Configure advanced diag dial-up settings.

Example

diag advanced dial-up

Syntax

display-status

Mode

Diag Advanced Dial-Up Settings

Description

Enable display dialup status on console.

Example

display-status

Syntax

no display-status

Mode

Diag Advanced Dial-Up Settings

Description

Disable display dialup status on console.

Example

no display-status

Syntax

max-pppdu-failure <UINT16>

Mode

Diag Advanced Dial-Up Settings

Description

Set PPPDU max configuration failure number.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

Syntax

reset

Mode

Diag Advanced Dial-Up Settings

Description

Restart dial-up devices.

Example

reset

Syntax

diag advanced dpi-stateful-firewall-security

Mode

Config

Description

DPI and stateful firewall security.

Example

diag advanced dpi-stateful-firewall-security

Syntax

diag advanced stateful-firewall-security

Mode

Config

Description

Stateful firewall security.

Example

diag advanced stateful-firewall-security

Syntax

diag advanced management

Mode

Config

Description

Configure advanced diag management settings.

Example

diag advanced management

Syntax

standby-management-sa

Mode

Diag Advanced Management Settings

Description

Enable using standby management SA.

Example

standby-management-sa

Syntax

no standby-management-sa

Mode

Diag Advanced Management Settings

Description

Disable using standby management SA.

Example

no standby-management-sa

Syntax

gms-preempts-admin

Mode

Diag Advanced Management Settings

Description

Enable allowing SGMS to preempt a logged in administrator.

Example

gms-preempts-admin

Syntax

no gms-preempts-admin

Mode

Diag Advanced Management Settings

Description

Disable allowing SGMS to preempt a logged in administrator.

Example

no gms-preempts-admin

Syntax

http-management

Mode

Diag Advanced Management Settings

Description

Allow management via HTTP.

Example

http-management

Syntax

no http-management

Mode

Diag Advanced Management Settings

Description

Disable allow management via HTTP.

Example

no http-management

Syntax

classic-view

Mode

Diag Advanced Management Settings

Description

Show classic address Objects, services and NAT policies view pages.

Example

classic-view

Syntax

no classic-view

Mode

Diag Advanced Management Settings

Description

Disable show classic address objects, services and NAT policies view pages.

Example

no classic-view

Syntax

```
online-help-url { default | override [ url <WORD> ] }
```

Mode

Diag Advanced Management Settings

Description

Set the online help URL.

Options

default Use the default global help system URL.

override Override the default using the configured value.

url Set URL.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
online-help-url url "help.mysonicwall.com/help.asp"
```

Syntax

```
diag advanced user-authentication
```

Mode

Config

Description

Configure advanced diag user authentication settings.

Example

```
diag advanced user-authentication
```

Syntax

```
post-authentication-redirect-url <URL>
```

Mode

Diag Advanced User Authentication Settings

Description

Set post authentication user redirect URL.

Options

<URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

```
post-authentication-redirect-url "10.10.10.10/welcome.asp"
```

Syntax

```
no post-authentication-redirect-url
```

Mode

Diag Advanced User Authentication Settings

Description

Clear post authentication user redirect URL.

Example

```
no post-authentication-redirect-url
```

Syntax

```
redirect-http-in-dp
```

Mode

Diag Advanced User Authentication Settings

Description

Enable redirecting unauthenticated HTTP connections to the login page in the data plane.

Example

```
redirect-http-in-dp
```

Syntax

```
no redirect-http-in-dp
```

Mode

Diag Advanced User Authentication Settings

Description

Disable redirecting unauthenticated HTTP connections to the login page in the data plane.

Example

```
no redirect-http-in-dp
```

Syntax

```
https-redirect-port <UINT32>
```

Mode

Diag Advanced User Authentication Settings

Description

Set the internal NAT TCP port number for HTTPS redirect.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
https-redirect-port 3443
```

Syntax

```
flush-cached-redirect-files
```

Mode

Diag Advanced User Authentication Settings

Description

Flush all files (redirect pages etc.) cached for redirecting.

Example

```
flush-cached-redirect-files
```

Syntax

```
logout users
```

Mode

Diag Advanced User Authentication Settings

Description

Logout all users.

Example

```
logout users
```

Syntax

```
log-all-sso-attempts [ { sso-auth-log [ buffer-full { stop | wrap } | max-buffer <UINT32> ] } | event-log ]
```

Mode

Diag Advanced User Authentication Settings

Description

Enable logging an audit trail of all SSO attempts in the event log.

Options

sso-auth-log Log in in memory to download as ssoAuthLog.wri.

buffer-full When buffer is full.

stop When buffer is full, stop logging.

wrap Enable including SSO polling, wrap logging.

max-buffer Max buffer size.

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

event-log Log in the event log.

Example

```
log-all-sso-attempts
```

Syntax

```
no log-all-sso-attempts
```

Mode

Diag Advanced User Authentication Settings

Description

Disable logging an audit trail of all SSO attempts in the event log.

Example

```
no log-all-sso-attempts
```

Syntax

```
user-ip { all | group <ADDR_GROUP_NAME> | name <ADDR_NAME> }
```

Mode

Diag Advanced User Authentication Settings

Description

Set user ip address object name or group name.

Options

| | |
|--------------------------------|---|
| all | All. |
| group | Address group name. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |

Example

```
user-ip group "ALL XI Managemetn IP"
```

Syntax

```
include-sso-polling
```

Mode

Diag Advanced User Authentication Settings

Description

Enable inclusion of polling events in the SSO audit trail log.

Example

```
include-sso-polling
```

Syntax

```
no include-sso-polling
```

Mode

Diag Advanced User Authentication Settings

Description

Disable inclusion of polling events in the SSO audit trail log.

Example

```
no include-sso-polling
```

Syntax

include-ss0-bypass

Mode

Diag Advanced User Authentication Settings

Description

Enable inclusion of SSO bypass events in the SSO audit trail log.

Example

include-ss0-bypass

Syntax

no include-ss0-bypass

Mode

Diag Advanced User Authentication Settings

Description

Disable inclusion of SSO bypass events in the SSO audit trail log.

Example

no include-ss0-bypass

Syntax

include-additional-non-initiation

Mode

Diag Advanced User Authentication Settings

Description

Enable inclusion of additional non-initiation of SSO in the SSO audit trail log.

Example

include-additional-non-initiation

Syntax

no include-additional-non-initiation

Mode

Diag Advanced User Authentication Settings

Description

Disable inclusion of additional non-initiation of SSO in the SSO audit trail log.

Example

no include-additional-non-initiation

Syntax

```
sso-agent-verison-negotiation <UINT32>
```

Mode

Diag Advanced User Authentication Settings

Description

Set version try to negotiate SSO agent protocol to(default version 5).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
sso-agent-verison-negotiation 5
```

Syntax

```
no sso-agent-verison-negotiation
```

Mode

Diag Advanced User Authentication Settings

Description

Disable to negotiate SSO agent protocol version.

Example

```
no sso-agent-verison-negotiation
```

Syntax

```
diag advanced diagnostics
```

Mode

Config

Description

Configure advanced diag diagnostics settings.

Example

```
diag advanced diagnostics
```

Syntax

```
setup-tool-server
```

Mode

Diag Advanced Diagnostics Settings

Description

Enable SonicSetup/Setuptool server.

Example

```
setup-tool-server
```

Syntax

```
no setup-tool-server
```

Mode

Diag Advanced Diagnostics Settings

Description

Disable SonicSetup/Setuptools server.

Example

```
no setup-tool-server
```

Syntax

```
trace-message-level { error | fatal | info | verbose | warning }
```

Mode

Diag Advanced Diagnostics Settings

Description

Set the trace message level.

Options

error Error.

fatal Fatal.

info Info.

verbose Verbose.

warning Warning.

Example

```
trace-message-level
```

Syntax

```
auto-restart [ every <UINT32> ]
```

Mode

Diag Advanced Diagnostics Settings

Description

Enable (for diagnostic testing purposes) auto-restarting system every set amount of minutes.

Options

every Set number of minutes to auto-restart system.

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
auto-restart every 60
```

Syntax

no auto-restart

Mode

Diag Advanced Diagnostics Settings

Description

Disable (for diagnostic testing purposes) auto-restarting system every set amount of minutes.

Example

no auto-restart

Syntax

secured-crash-analysis

Mode

Diag Advanced Diagnostics Settings

Description

Enable secured www.mysonicwall.com crash analysis.

Example

secured-crash-analysis

Syntax

no secured-crash-analysis

Mode

Diag Advanced Diagnostics Settings

Description

Disable secured www.mysonicwall.com crash analysis.

Example

no secured-crash-analysis

Syntax

show-user-diagnostics

Mode

Diag Advanced Diagnostics Settings

Description

Enable to show user diagnostics on web block by CFS.

Example

show-user-diagnostics

Syntax

no show-user-diagnostics

Mode

Diag Advanced Diagnostics Settings

Description

Disable to show user diagnostics on web block by CFS.

Example

no show-user-diagnostics

Syntax

wan-connectivity-test start

Mode

Diag Advanced Diagnostics Settings

Description

WAN connectivity test.

Example

wan-connectivity-test start

Syntax

wan-connectivity-test target-ip <IPV4_HOST>

Mode

Diag Advanced Diagnostics Settings

Description

Set WAN connectivity test target IP.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

wan-connectivity-test target-ip 10.10.10.10

Syntax

no wan-connectivity-test target-ip

Mode

Diag Advanced Diagnostics Settings

Description

Clear WAN connectivity test target IP.

Example

no wan-connectivity target-ip

Syntax

```
wan-connectivity-test stop
```

Mode

Diag Advanced Diagnostics Settings

Description

WAN connectivity test.

Example

```
wan-connectivity-test stop
```

Syntax

```
send wan-connectivity-test log
```

Mode

Diag Advanced Diagnostics Settings

Description

Send WAN connectivity state log.

Example

```
send wan-connectivity-test log
```

Syntax

```
dp-jobs-tracked <UINT8>
```

Mode

Diag Advanced Diagnostics Settings

Description

Set number of jobs executed by data plane task to be tracked.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
dp-jobs-tracked 10
```

Syntax

```
diag advanced watchdog
```

Mode

Config

Description

Configure advanced diag watchdog settings.

Example

```
diag advanced watchdog
```

Syntax

cpu-watchdog

Mode

Diag Advanced Watchdog Settings

Description

Enable CPU watchdog.

Example

cpu-watchdog

Syntax

no cpu-watchdog

Mode

Diag Advanced Watchdog Settings

Description

Disable CPU watchdog.

Example

no cpu-watchdog

Syntax

restart-for

Mode

Diag Advanced Watchdog Settings

Description

Enable restarting for watchdog task.

Example

restart-for

Syntax

no restart-for

Mode

Diag Advanced Watchdog Settings

Description

Disable restarting for watchdog task.

Example

no restart-for

Syntax

quick-restart

Mode

Diag Advanced Watchdog Settings

Description

Enable restarting quickly after an exception.

Example

quick-restart

Syntax

no quick-restart

Mode

Diag Advanced Watchdog Settings

Description

Disable restarting quickly after an exception.

Example

no quick-restart

Syntax

restart-when-no-packet-rx

Mode

Diag Advanced Watchdog Settings

Description

Enable restart when no packet Rx activity is detected.

Example

restart-when-no-packet-rx

Syntax

no restart-when-no-packet-rx

Mode

Diag Advanced Watchdog Settings

Description

Disable restart when no packet Rx activity is detected.

Example

no restart-when-no-packet-rx

Syntax

```
wait-for-no-packet-rx <UINT16>
```

Mode

Diag Advanced Watchdog Settings

Description

Set no packet Rx activity wait time in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
wait-for-no-packet-rx 60
```

Syntax

```
diag advanced wireless
```

Mode

Config

Description

Configure advanced diag wireless settings.

Example

```
diag advanced wireless
```

Syntax

```
regulatory-domain
```

Mode

Diag Advanced Wireless Settings

Description

Enable wireless regulatory domain.

Example

```
regulatory-domain
```

Syntax

```
no regulatory-domain
```

Mode

Diag Advanced Wireless Settings

Description

Disbale wireless regulatory domain.

Example

```
no regulatory-domain
```

Syntax

```
sonicpoint support-type { all | sonicpoint-only | sonicpointn-only }
```

Mode

Diag Advanced Wireless Settings

Description

Set supported sonicPoint type.

Options

all All types.

sonicpoint-only Only support sonicpoint.

sonicpointn-only Only support sonicpointn.

Example

```
sonicpoint support-type all
```

Syntax

```
vap-bssid-local-bit
```

Mode

Diag Advanced Wireless Settings

Description

Set local bit for virtual access point BSSID MAC address.

Example

```
vap-bssid-local-bit
```

Syntax

```
no vap-bssid-local-bit
```

Mode

Diag Advanced Wireless Settings

Description

Disable to set local bit for virtual access point BSSID MAC address.

Example

```
no vap-bssid-local-bit
```

Syntax

```
sonicpoint legacy-management
```

Mode

Diag Advanced Wireless Settings

Description

Enforce legacy SonicPoint-A/B/G and SonicPoint-G Only to be managed.

Example

```
sonicpoint legacy-management
```

Syntax

```
no sonicpoint legacy-management
```

Mode

Diag Advanced Wireless Settings

Description

Disable enforce legacy SonicPoint-A/B/G and SonicPoint-G Only to be managed.

Example

```
no sonicpoint legacy-management
```

Syntax

```
sonicpoint update-firmware
```

Mode

Diag Advanced Wireless Settings

Description

Update all sonicPoint firmware.

Example

```
sonicpoint update-firmware
```

Syntax

```
sonicpoint keepalive-enforcement
```

Mode

Diag Advanced Wireless Settings

Description

Enable sonicPoint keepalive enforcement.

Example

```
sonicpoint keepalive-enforcement
```

Syntax

```
no sonicpoint keepalive-enforcement
```

Mode

Diag Advanced Wireless Settings

Description

Disable sonicPoint keepalive enforcement.

Example

no sonicpoint keepalive-enforcement

Syntax

sonicpoint profile-tcp-window-size <UINT16>

Mode

Diag Advanced Wireless Settings

Description

Set sonicPoint provisioning profile TCP window size.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

sonicpoint profile-tcp-window-size 1400

Syntax

no sonicpoint profile-tcp-window-size

Mode

Diag Advanced Wireless Settings

Description

Clear sonicPoint provisioning profile TCP window size.

Example

sonicpoint profile-tcp-window-size 1400

Syntax

sonicpoint default-window-size

Mode

Diag Advanced Wireless Settings

Description

Use default TCP window size for sonicpointn provisioning protocol.

Example

sonicpoint default-window-size

Syntax

no sonicpoint default-window-size

Mode

Diag Advanced Wireless Settings

Description

Disable to use default TCP window size for sonicpointn provisioning protocol.

Example

```
no sonicpoint default-window-size
```

Syntax

```
sonicpointn prefer-channel-1-6-11
```

Mode

Diag Advanced Wireless Settings

Description

Prefer sonicpointn 2.4GHz Auto channel selection to be 1, 6 and 11 only.

Example

```
sonicpointn prefer-channel-1-6-11
```

Syntax

```
no sonicpointn prefer-channel-1-6-11
```

Mode

Diag Advanced Wireless Settings

Description

Disable to prefer sonicpointn 2.4GHz Auto channel selection to be 1, 6 and 11 only.

Example

```
no sonicpointn prefer-channel-1-6-11
```

Syntax

```
sonicpointn ssh-management
```

Mode

Diag Advanced Wireless Settings

Description

Enable SonicPointN SSH management.

Example

```
sonicpointn ssh-management
```

Syntax

```
no sonicpointn ssh-management
```

Mode

Diag Advanced Wireless Settings

Description

Disable SonicPointN SSH management.

Example

no sonicpointn ssh-management

Syntax

sonicpointn logging

Mode

Diag Advanced Wireless Settings

Description

Enable SonicPointN logging.

Example

sonicpointn logging

Syntax

no sonicpointn logging

Mode

Diag Advanced Wireless Settings

Description

Disable SonicPointN logging.

Example

no sonicpointn logging

Syntax

sonicpoint erase-old-crash-log

Mode

Diag Advanced Wireless Settings

Description

Erase SonicPoint crash log generated by previous firmware image when SonicPoint image is updated.

Example

sonicpoint erase-old-crash-log

Syntax

no sonicpoint erase-old-crash-log

Mode

Diag Advanced Wireless Settings

Description

Disable to erase SonicPoint crash log generated by previous firmware image.

Example

no sonicpoint erase-old-crash-log

Syntax

```
sonicpointn noise-security-level { extremely-high | extremely-low | high | low | medium }
```

Mode

Diag Advanced Diagnostics Settings

Description

Set SonicPoint-Ni/Ne noise sensitivity level:
 (The higher noise sensitivity level should be selected when RF environment is getting noiser).

Options

extremely-high Extremely high.

extremely-low Extremely low.

high High.

low Low.

medium Medium.

Example

```
sonicpointn noise-security-level medium
```

Syntax

```
no sonicpointn noise-security-level
```

Mode

Diag Advanced Wireless Settings

Description

Disable SonicPoint-Ni/Ne noise sensitivity.

Example

```
no sonicpointn noise-security-level
```

Syntax

```
sonicpointn noise-safemode-reboot
```

Mode

Diag Advanced Wireless Settings

Description

Reboot SonicPointN when noise safe mode detected.

Example

```
sonicpointn noise-safemode-reboot
```

Syntax

```
no sonicpointn noise-safemode-reboot
```


Mode

Diag Advanced Wireless Settings

Description

Disable to reboot SonicPointN when noise safe mode detected.

Example

```
no sonicpoint noise-safemode-reboot
```

Syntax

```
sonicpoint retain-ip
```

Mode

Diag Advanced Wireless Settings

Description

Enable SonicPoint(N) IP address retaining.

Example

```
sonicpoint retain-ip
```

Syntax

```
no sonicpoint retain-ip
```

Mode

Diag Advanced Wireless Settings

Description

Disable SonicPoint(N) IP address retaining.

Example

```
no sonicpoint retain-ip
```

Syntax

```
sonicpoint snap-header
```

Mode

Diag Advanced Wireless Settings

Description

Use SNAP packet between SonicPoint / SonicPointN and gateway.

Example

```
sonicpoint snap-header
```

Syntax

```
no sonicpoint snap-header
```

Mode

Diag Advanced Wireless Settings

Description

Disable to use SNAP packet between SonicPoint / SonicPointN and gateway.

Example

```
no sonicpoint snap-header
```

Syntax

```
sonicpoint fragment-icmp
```

Mode

Diag Advanced Wireless Settings

Description

Send need fragment ICMP packet to SonicPoint / SonicPointN client.

Example

```
sonicpoint fragment-icmp
```

Syntax

```
no sonicpoint fragment-icmp
```

Mode

Diag Advanced Wireless Settings

Description

Disable to send need fragment ICMP packet to SonicPoint / SonicPointN client.

Example

```
no sonicpoint fragment-icmp
```

Syntax

```
bonjour-intra-wlan
```

Mode

Diag Advanced Wireless Settings

Description

Enable intra-WLAN zone communication for bonjour packet.

Example

```
bonjour-intra-wlan
```

Syntax

```
no bonjour-intra-wlan
```

Mode

Diag Advanced Wireless Settings

Description

Disable intra-WLAN zone communication for Bonjour packet.

Example

```
no Bonjour-intra-wlan
```

Syntax

```
dhcp-arp-enhancement
```

Mode

Diag Advanced Wireless Settings

Description

WLAN DHCP lease / ARP delivery success rate enhancement.

Example

```
dhcp-arp-enhancement
```

Syntax

```
no dhcp-arp-enhancement
```

Mode

Diag Advanced Wireless Settings

Description

Disable WLAN DHCP lease / ARP delivery success rate enhancement.

Example

```
no dhcp-arp-enhancement
```

Syntax

```
guest-services-redirect-interval <UINT8>
```

Mode

Diag Advanced Wireless Settings

Description

Set wireless guest services redirect interval in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
guest-services-redirect-interval 15
```

Syntax

```
wifisec-enforcement
```

Mode

Diag Advanced Wireless Settings

Description

Enable legacy WiFiSec enforcement support.

Example

```
wifisec-enforcement
```

Syntax

```
no wifisec-enforcement
```

Mode

Diag Advanced Wireless Settings

Description

Disable legacy WiFiSec enforcement support.

Example

```
no wifisec-enforcement
```

Syntax

```
wlan reply-wifisec-enforcement
```

Mode

Diag Advanced Wireless Settings

Description

Enable applying WiFi security enforcement on reply traffic from WLAN to any other zone.

Example

```
wlan reply-wifisec-enforcement
```

Syntax

```
no wlan reply-wifisec-enforcement
```

Mode

Diag Advanced Wireless Settings

Description

Disable applying WiFi security enforcement on reply traffic from WLAN to any other zone.

Example

```
no wlan reply-wifisec-enforcement
```

Syntax

```
wlan dp-core-processing
```

Mode

Diag Advanced Wireless Settings

Description

Enable WLAN traffic DP core processing capability.

Example

```
wlan dp-core-processing
```

Syntax

```
no wlan dp-core-processing
```

Mode

Diag Advanced Wireless Settings

Description

Disable WLAN traffic DP core processing capability.

Example

```
no wlan dp-core-processing
```

Syntax

```
wlan broadcast-communication
```

Mode

Diag Advanced Wireless Settings

Description

Enable intra-WLAN zone communication for broadcast packet.

Example

```
wlan broadcast-communication
```

Syntax

```
no wlan broadcast-communication
```

Mode

Diag Advanced Wireless Settings

Description

Disable intra-WLAN Zone communication for broadcast packet.

Example

```
no wlan broadcast-communication
```

Syntax

```
wlan bypass-gateway-firewalling
```

Mode

Diag Advanced Wireless Settings

Description

Enable local wireless zone traffic to bypass gateway firewalling.

Example

```
wlan bypass-gateway-firewalling
```

Syntax

```
no wlan bypass-gateway-firewalling
```

Mode

Diag Advanced Wireless Settings

Description

Disable local wireless zone traffic to bypass gateway firewalling.

Example

```
no wlan bypass-gateway-firewalling
```

Syntax

```
diag advanced tooltip-no-description
```

Mode

Config

Description

Enable tooltip with no descriptions.

Example

```
diag advanced tooltip-no-description
```

Syntax

```
diag no advanced tooltip-no-description
```

Mode

Config

Description

Disable tooltip with no descriptions.

Example

```
diag no advanced tooltip-no-description
```

Syntax

```
diag advanced preference
```

Mode

Config

Description

Configure advanced diag preference conversion.

Example

diag advanced preference

Syntax

launching-conversion-control

Mode

Diag Advanced Preference Conversion

Description

Enable showing control for launching preference conversion window.

Example

launching-conversion-control

Syntax

no launching-conversion-control

Mode

Diag Advanced Preference Conversion

Description

Disable showing control for launching preference conversion window.

Example

no launching-conversion-control

Syntax

processor-server <HOSTNAME>

Mode

Diag Advanced Preference Conversion

Description

Set preference processor server.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

processor-server convert.global.sonicwall.com

Syntax

no processor-server

Mode

Diag Advanced Preference Conversion

Description

Clear preference processor server.

Example

```
no processor-server
```

Syntax

```
secure-http-to-processor
```

Mode

Diag Advanced Preference Conversion

Description

Enable using secure HTTP to connect to preference processor server.

Example

```
secure-http-to-processor
```

Syntax

```
no secure-http-to-processor
```

Mode

Diag Advanced Preference Conversion

Description

Disable using secure HTTP to connect to preference processor server.

Example

```
no secure-http-to-processor
```

Syntax

```
site-relative-directory <WORD>
```

Mode

Diag Advanced Preference Conversion

Description

Set site relative directory.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
site-relative-directory \"/popup\"
```

Syntax

```
no site-relative-directory
```

Mode

Diag Advanced Preference Conversion

Description

Clear site relative directory.

Example

```
no site-relative-directory
```

Syntax

```
check-when-importing
```

Mode

Diag Advanced Preference Conversion

Description

Enable checking when importing settings.

Example

```
check-when-importing
```

Syntax

```
no check-when-importing
```

Mode

Diag Advanced Preference Conversion

Description

Disable checking when importing settings.

Example

```
no check-when-importing
```

Syntax

```
diag advanced anti-spam
```

Mode

Config

Description

Configure advanced diag Anti-Spam.

Example

```
diag advanced anti-spam
```

Syntax

```
syn-flood-protection
```

Mode

Diag Advanced Anti-Spam

Description

Enable SYN flood protection for Anti-Spam-related connections.

Example

```
syn-flood-protection
```

Syntax

```
no syn-flood-protection
```

Mode

Diag Advanced Anti-Spam

Description

Disable SYN flood protection for Anti-Spam-related connections.

Example

```
no syn-flood-protection
```

Syntax

```
check-grid-ip-only
```

Mode

Diag Advanced Anti-Spam

Description

Use GRID IP reputation check only.

Example

```
check-grid-ip-only
```

Syntax

```
no check-grid-ip-only
```

Mode

Diag Advanced Anti-Spam

Description

Disable to use GRID IP reputation check only.

Example

```
no check-grid-ip-only
```

Syntax

```
outbound-smtp-grid-ip
```

Mode

Diag Advanced Anti-Spam

Description

Enable GRID IP reputation checking for outbound SMTP connections.

Example

```
outbound-smtp-grid-ip
```

Syntax

```
no outbound-smtp-grid-ip
```

Mode

Diag Advanced Anti-Spam

Description

Disable GRID IP reputation checking for outbound SMTP connections.

Example

```
no outbound-smtp-grid-ip
```

Syntax

```
disabling-custom-email
```

Mode

Diag Advanced Anti-Spam

Description

Enable disabling of custom user e-mail policies when Anti-spam is enabled.

Example

```
disabling-custom-email
```

Syntax

```
no disabling-custom-email
```

Mode

Diag Advanced Anti-Spam

Description

Disable disabling of custom user e-mail policies when Anti-Spam is enabled.

Example

```
no disabling-custom-email
```

Syntax

```
limited-admin-configuration
```

Mode

Diag Advanced Anti-Spam

Description

Enable allowing limited admin users to configure Anti-Spam service.

Example

limited-admin-configuration

Syntax

no limited-admin-configuration

Mode

Diag Advanced Anti-Spam

Description

Disable allowing limited admin users to configure Anti-Spam service.

Example

no limited-admin-configuration

Syntax

shlo-check

Mode

Diag Advanced Anti-Spam

Description

Enable SHLO check when Junk Store is unavailable (while E-mail Security is operational).

Example

shlo-check

Syntax

no shlo-check

Mode

Diag Advanced Anti-Spam

Description

Disable SHLO check when Junk Store is unavailable (while E-mail Security is operational).

Example

no shlo-check

Syntax

auto-generated-cass-acl

Mode

Diag Advanced Anti-Spam

Description

Enable editing of auto-generated CASS access rules.

Example

auto-generated-cass-acl

Syntax

```
no auto-generated-cass-acl
```

Mode

Diag Advanced Anti-Spam

Description

Disable editing of auto-generated CASS access rules.

Example

```
no auto-generated-cass-acl
```

Syntax

```
clear statistics
```

Mode

Diag Advanced Anti-Spam

Description

Clear statistics.

Example

```
clear statistics
```

Syntax

```
reset grid-name-cache
```

Mode

Diag Advanced Anti-Spam

Description

Reset GRID name cache.

Example

```
reset grid-name-cache
```

Syntax

```
no policies-and-objects
```

Mode

Diag Advanced Anti-Spam

Description

Deletes policies and objects.

Example

```
no policies-and-objects
```

Syntax

```
cass_cloud_service_addr { auto-resolve | static-ip <IPV4_HOST> }
```

Mode

Diag Advanced Anti-Spam

Description

Set CASS cloud service address.

Options

auto-resolve Resolve automatically.

static-ip Use this static IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
cass_cloud_service_addr static-ip 204.212.170.13
```

Syntax

```
diag advanced hosted-email-security
```

Mode

Config

Description

Enable hosted e-mail security.

Example

```
diag advanced hosted-email-security
```

Syntax

```
diag no advanced hosted-email-security
```

Mode

Config

Description

Disable hosted e-mail security.

Example

```
diag no advanced hosted-email-security
```

Syntax

```
diag advanced email-detection
```

Mode

Config

Description

Enable e-mail system detection.

Example

```
diag advanced email-detection
```

Syntax

```
diag no advanced email-detection
```

Mode

Config

Description

Disable e-mail system detection.

Example

```
diag no advanced email-detection
```

Syntax

```
diag advanced remote-assistance
```

Mode

Config

Description

Enable remote assistance.

Example

```
diag advanced remote-assistance
```

Syntax

```
diag no advanced remote-assistance
```

Mode

Config

Description

Disable remote assistance.

Example

```
diag no advanced remote-assistance
```

Syntax

```
diag advanced sslvpn
```

Mode

Config

Description

Configure advanced diag SSL-VPN settings.

Example

diag advanced sslvpn

Syntax

netextender-version <WORD>

Mode

Diag Advanced SSL-VPN Settings

Description

Set NetExtender(for Windows) version.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

netextender-version TBD

Syntax

no netextender-version

Mode

Diag Advanced SSL-VPN Settings

Description

Clear NetExtender(for Windows) version.

Example

no netextender-version

Syntax

diag advanced backend-server

Mode

Config

Description

Configure advanced diag backend servers settings.

Example

diag advanced backend-server

Syntax

enable

Mode

Diag Advanced Backend Server Settings

Description

Enable communication with SonicWall backend servers.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Diag Advanced Backend Server Settings

Description

Disable communication with SonicWall backend servers.

Example

```
no enable
```

Syntax

```
force-through { any | interface <ASSIGNED_INTERFACE> }
```

Mode

Diag Advanced Backend Server Settings

Description

Set interface to force communication with SonicWall backend servers going through.

Options

| | |
|-----------------------------------|--------------------------------|
| any | Any interface. |
| interface | Set interface. |
| <ASSIGNED_INTERFACE> | Interface name. Example: X0 |

Example

```
force-through interface X1
```

Syntax

```
diag advanced wan-acceleration
```

Mode

Config

Description

Configure advanced diag WAN acceleration.

Example

```
diag advanced wan-acceleration
```

Syntax

```
remote-checking
```

Mode

Diag Advanced Wan Acceleration

Description

Enable checking of connection responses by remote WAN acceleration device.

Example

```
remote-dev-connection-checking
```

Syntax

```
no remote-checking
```

Mode

Diag Advanced Wan Acceleration

Description

Disable checking of connection responses by remote WAN acceleration device.

Example

```
no remote-dev-connection-checking
```

Syntax

```
bypass-tcp-acceleration { failed-proxied-connection <UINT32> | short-lived-proxied-connection <UINT32> }
```

Mode

Diag Advanced Wan Acceleration

Description

Enable temporarily bypass TCP acceleration.

Options

| | |
|--|---|
| <i>failed-proxied-connection</i> <UINT32> | Set temporarily bypass TCP acceleration for failed proxied connections (minutes). Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |
|--|---|

| | |
|---|--|
| <i>short-lived-proxied-connection</i> <UINT32> | Set temporarily bypass TCP acceleration for short-lived proxied connections (minutes). Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |
|---|--|

Example

```
bypass-tcp-acceleration failed-proxied-connection 15
```

Syntax

```
no bypass-tcp-acceleration { failed-proxied-connection | short-lived-proxied-connection }
```

Mode

Diag Advanced Wan Acceleration

Description

Disable temporarily bypass TCP acceleration.

Options

failed-proxied-connection Set temporarily bypass TCP acceleration for failed proxied connections (minutes).

short-lived-proxied-connection Set temporarily bypass TCP acceleration for short-lived proxied connections (minutes).

Example

```
no bypass-tcp-acceleration failed-proxied-connection
```

Syntax

```
skip-tcp-acceleration
```

Mode

Diag Advanced Wan Acceleration

Description

Skip TCP acceleration for stateful control channels (but accelerate data channels).

Example

```
skip-tcp-acceleration
```

Syntax

```
no skip-tcp-acceleration
```

Mode

Diag Advanced Wan Acceleration

Description

Disable skip TCP acceleration for stateful control channels (but accelerate data channels).

Example

```
no skip-tcp-acceleration
```

Syntax

```
clear debug-status
```

Mode

Diag Advanced Wan Acceleration

Description

Clear debug status.

Example

```
clear debug-status
```

Syntax

```
clear tcp-acceleration-database
```

Mode

Diag Advanced Wan Acceleration

Description

Clear TCP acceleration database.

Example

```
clear tcp-acceleration-database
```

Syntax

```
diag advanced geoip-location-service
```

Mode

Config

Description

Configure advanced diag GeoIP/Location service.

Example

```
diag advanced geoip-location-service
```

Syntax

```
remote-geoip-server { always | failed-resolution } [ default | ip <IPV4_HOST> ]
```

Mode

Diag Advanced GeoIP/Location Service

Description

Set location of remote GeoIP server address.

Options

always Always use this IP for geoipdata.global.sonicwall.com.

failed-resolution Use if geoipdata.global.sonicwall.com does not resolve.

default Set the IP address to the default setting.

ip Specify the IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
remote-geoip-server failed-resolution 204.212.170.189
```

Syntax

```
clear location-cache
```

Mode

Diag Advanced GeoIP/Location Service

Description

Clear location cache.

Example

```
clear location-cache
```

Syntax

use-control-plane

Mode

Diag Advanced GeoIP/Location Service

Description

Use control plane for GeoIP database lookups.

Example

use-control-plane

Syntax

no use-control-plane

Mode

Diag Advanced GeoIP/Location Service

Description

Disable to use control plane for GeoIP database lookups.

Example

no use-control-plane

Syntax

bypass-geoip-blocking

Mode

Diag Advanced GeoIP/Location Service

Description

Bypass GeoIp blocking for stack initiated connections.

Example

bypass-geoip-blocking

Syntax

no bypass-geoip-blocking

Mode

Diag Advanced GeoIP/Location Service

Description

Disable to bypass GeoIp blocking for stack initiated connections.

Example

no bypass-geoip-blocking

Syntax

bypass-botnet-blocking

Mode

Diag Advanced GeoIP/Location Service

Description

Bypass BOTNET blocking for stack initiated connections.

Example

bypass-botnet-blocking

Syntax

no bypass-botnet-blocking

Mode

Diag Advanced GeoIP/Location Service

Description

Disable to bypass BOTNET blocking for stack initiated connections.

Example

no bypass-botnet-blocking

Syntax

geoup-botnet-map-file-upload

Mode

Diag Advanced GeoIP/Location Service

Description

Allow Geo-IP/Botnet filter map database file upload.

Example

geoup-botnet-map-file-upload

Syntax

no geoup-botnet-map-file-upload

Mode

Diag Advanced GeoIP/Location Service

Description

Disable to upload Geo-IP/Botnet filter map database file.

Example

no geoup-botnet-map-file-upload

Syntax

diag advanced flow-reporting

Mode

Config

Description

Configure advanced diag Flow Reporting.

Example

diag advanced flow-reporting

Syntax

clear location-map

Mode

Diag Advanced Flow Reporting

Description

Clear location map database.

Example

clear location-map

Syntax

flow-reporting-and-visualization

Mode

Diag Advanced Flow Reporting

Description

Enable flow reporting and visualization.

Example

flow-reporting-and-visualization

Syntax

no flow-reporting-and-visualization

Mode

Diag Advanced Flow Reporting

Description

Disable flow reporting and visualization.

Example

no flow-reporting-and-visualization

Syntax

report-to-external

Mode

Diag Advanced Flow Reporting

Description

Report to external flow collector.

Example

```
report-to-external
```

Syntax

```
no report-to-external
```

Mode

Diag Advanced Flow Reporting

Description

Disable to report to external flow collector.

Example

```
no report-to-external
```

Syntax

```
appflow-monitor-browser-frame-launch
```

Mode

Diag Advanced Flow Reporting

Description

Enable launching of AppFlow monitor in a stand-alone browser frame.

Example

```
appflow-monitor-browser-frame-launch
```

Syntax

```
no appflow-monitor-browser-frame-launch
```

Mode

Diag Advanced Flow Reporting

Description

Disable launching of AppFlow monitor in a stand-alone browser frame.

Example

```
no appflow-monitor-browser-frame-launch
```

Syntax

```
non-admin-visualization
```

Mode

Diag Advanced Flow Reporting

Description

Enable visualization UI for Non-Admin/Config users.

Example

```
non-admin-visualization
```

Syntax

```
no non-admin-visualization
```

Mode

Diag Advanced Flow Reporting

Description

Disable visualization UI for Non-Admin/Config users.

Example

```
no non-admin-visualization
```

Syntax

```
database-busy-timeout <UINT32>
```

Mode

Diag Advanced Flow Reporting

Description

Set database busy timeout in msec.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
database-busy-timeout 3000
```

Syntax

```
no database-busy-timeout
```

Mode

Diag Advanced Flow Reporting

Description

Clear database busy timeout in msec.

Example

```
no database-busy-timeout
```

Syntax

```
hide-appflow-server
```

Mode

Diag Advanced Flow Reporting

Description

Hide AppFlow server feature.

Example

```
hide-appflow-server
```

Syntax

```
no hide-appflow-server
```

Mode

Diag Advanced Flow Reporting

Description

Disable to hide AppFlow server feature.

Example

```
no hide-appflow-server
```

Syntax

```
hide-gmsflow-server
```

Mode

Diag Advanced Flow Reporting

Description

Hide GmsFlow server feature.

Example

```
hide-gmsflow-server
```

Syntax

```
no hide-gmsflow-server
```

Mode

Diag Advanced Flow Reporting

Description

Disable to hide GmsFlow server feature.

Example

```
no hide-appflow-server
```

Syntax

```
send-unified-data
```

Mode

Description

Send unified AppFlow and RTM data to GMSFlow server.

Example

```
send-unified-data
```

Syntax

```
no send-unified-data
```

Mode

Diag Advanced Flow Reporting

Description

Disable to send unified AppFlow and RTM data to GMSFlow server.

Example

```
no send-unified-data
```

Syntax

```
gmsflow-server-per-node node <UINT8> ip-addr <IPV4_HOST>
```

Mode

Diag Advanced Flow Reporting

Description

Enable per node GMSFlow server.

Options

| | |
|--------------------------|--|
| node | Per node GMSFlow server. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| ip-addr | GMSFlow server address for each node. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |

Example

```
gmsflow-server-per-node  
gmsflow-server-per-node node 4 ip-addr 10.10.10.10
```

Syntax

```
no gmsflow-server-per-node [ node <UINT8> ip-addr ]
```

Mode

Diag Advanced Flow Reporting

Description

Clear per node GMSFlow server ip address.

Options

| | |
|----------------------|---|
| node | Per node GMSFlow server. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |

ip-addr GMSFlow server address for each node.

Example

```
no gmsflow-server-per-node node 4 ip-addr
```

Syntax

```
report-server-addr { ip <IPV4_HOST> | sonicwall }
```

Mode

Diag Advanced Flow Reporting

Description

Set appFlow reports server address.

Options

ip Use this IP address for App reports upload.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

sonicwall Connect to appreports.global.sonicwall.com.

Example

```
report-server-addr ip 173.240.209.223
```

Syntax

```
https-upload
```

Mode

Diag Advanced Flow Reporting

Description

Use secure HTTP for AppFlow report upload.

Example

```
https-upload
```

Syntax

```
no https-upload
```

Mode

Diag Advanced Flow Reporting

Description

Disable to use secure HTTP for AppFlow report upload.

Example

```
no https-upload
```

Syntax

```
clear database-tables
```

Mode

Diag Advanced Flow Reporting

Description

Clear appflow database tables.

Example

```
clear database-tables
```

Syntax

```
diag advanced log-reschedule [ interval <UINT16> ]
```

Mode

Config

Description

Enable main log process reschedule and set interval.

Options

- interval** Main log process reschedule interval.
- <UINT16>** Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
diag advanced log-reschedule-interval 100
```

Syntax

```
diag no advanced log-reschedule
```

Mode

Config

Description

Disable main log process reschedule.

Example

```
diag no advanced log-reschedule
```

Syntax

```
diag advanced ipv6-ready-enforce
```

Mode

Config

Description

Enable enforcement of IPv6 ready logo requirement.

Example

```
diag advanced ipv6-ready-enforce
```

Syntax

diag no advanced ipv6-ready-enforce

Mode

Config

Description

Disable enforcement of IPv6 ready logo requirement.

Example

diag no advanced ipv6-ready-enforce

Syntax

diag advanced icmp drop-unreachable-packet

Mode

Config

Description

Enable enforcement of dropping unreachable ICMP packet.

Example

diag advanced icmp drop-unreachable-packet

Syntax

diag no advanced icmp drop-unreachable-packet

Mode

Config

Description

Disable enforcement of dropping unreachable ICMP packet.

Example

diag no advanced icmp drop-unreachable-packet

Syntax

diag advanced icmp drop-exceeded-packet

Mode

Config

Description

Enable enforcement of dropping time exceed ICMP packet.

Example

diag advanced icmp drop-exceeded-packet

Syntax

diag no advanced icmp drop-exceeded-packet

Mode

Config

Description

Disable enforcement of dropping time exceed ICMP packet.

Example

diag no advanced icmp drop-exceeded-packet

Syntax

diag advanced debug suppress-task-lock

Mode

Config

Description

Suppress potential task lock warning message.

Example

diag advanced debug suppress-task-lock

Syntax

diag no advanced debug suppress-task-lock

Mode

Config

Description

Disable to suppress potential task lock message.

Example

diag no advanced debug suppress-task-lock

Syntax

diag advanced debug suppress-task-dead-warning

Mode

Config

Description

Suppress potential task dead loop warning message.

Example

diag advanced debug suppress-task-dead-warning

Syntax

diag no advanced debug suppress-task-dead-warning

Mode

Config

Description

Disable to suppress potential task dead loop warning message.

Example

```
diag no advanced debug suppress-task-dead-warning
```

Syntax

```
diag advanced debug suppress-performance-testing-warning
```

Mode

Config

Description

Suppress performance testing warning message.

Example

```
diag advanced debug suppress-performance-testing-warning
```

Syntax

```
diag no advanced debug suppress-performance-testing-warning
```

Mode

Config

Description

Disable to suppress performance testing warning message.

Example

```
diag no advanced debug suppress-performance-testing-warning
```

Syntax

```
packet-monitor
```

Mode

Config

Description

Configure packet monitor settings.

Example

```
packet-monitor
```

Syntax

```
start capture
```

Mode

Packet Monitor
Top Level

Description

Start packet capture.

Example

```
start capture
```

Syntax

```
stop capture
```

Mode

Packet Monitor
Top Level

Description

Stop packet capture.

Example

```
stop capture
```

Syntax

```
start mirror
```

Mode

Packet Monitor
Top Level

Description

Start mirror.

Example

```
start mirror
```

Syntax

```
stop mirror
```

Mode

Packet Monitor
Top Level

Description

Stop mirror.

Example

```
stop mirror
```

Syntax

```
log-to-ftp
```

Mode

Packet Monitor
Top Level

Description

Log to FTP server.

Example

```
log-to-ftp
```

Syntax

```
export capture { app-data | html | libpcap | pcapng | text } { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

Top Level
Packet Monitor

Description

Export capture from the device using ftp.

Options

app-data App data.

html HTML.

libpcap LibPcap.

pcapng PcapNG.

text Text.

ftp Export using the FTP protocol.

<FTP_URL> FTP URL in the form: ftp://username:password@hostname/ Escape character: '!' -> '\\!', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: ftp://username:password@hostname/ nftp://username@hostname/ nftp://hostname/

scp Export using the SCP protocol.

<SCP_URL> SCP URL in the form: scp://username@host/ Escape character: '!' -> '\\!', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: scp://username@host/ nscp://host/

Example

```
export capture libpcap ftp ftp://user:password@ftp.myserver.local/capture.cap  
export capture libpcap scp scp://user@server/capture.cap
```

Syntax

```
monitor all
```

Mode

Packet Monitor
Top Level

Description

Monitor all packets.

Example

```
monitor all
```

Syntax

monitor default

Mode

Packet Monitor
Top Level

Description

Set packet monitor settings to default.

Example

monitor default

Syntax

clear capture

Mode

Packet Monitor
Top Level

Description

Clear the packet capture buffer.

Example

clear capture

Syntax

bytes-to-capture <UINT16>

Mode

Packet Monitor

Description

Specify number of bytes to capture (per packet).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

bytes-to-capture 1520

Syntax

wrap-buffer

Mode

Packet Monitor

Description

Enable wrapping of capture buffer once full.

Example

wrap-buffer

Syntax

no wrap-buffer

Mode

Packet Monitor

Description

Disable wrapping of capture buffer once full.

Example

no wrap-buffer

Syntax

exclude encrypted-gms

Mode

Packet Monitor

Description

Enable exclusion of encrypted GMS traffic.

Example

exclude encrypted-gms

Syntax

no exclude encrypted-gms

Mode

Packet Monitor

Description

Disable exclusion of encrypted GMS traffic.

Example

no exclude encrypted-gms

Syntax

exclude management { http | snmp | ssh }

Mode

Packet Monitor

Description

Enable exclusion of specified management.

Options

http HTTP/HTTPS.

snmp SNMP.

ssh SSH.

Example

```
exclude management http ssh
```

Syntax

```
no exclude management { http | snmp | ssh }
```

Mode

Packet Monitor

Description

Disable exclusion of specified management.

Options

http HTTP/HTTPS.

snmp SNMP.

ssh SSH.

Example

```
no exclude management http ssh
```

Syntax

```
exclude syslog { gms-server | syslog-servers }
```

Mode

Packet Monitor

Description

Enable exclusion of syslog traffic to specified server(s).

Options

gms-server GMS server.

syslog-servers Sylog servers.

Example

```
exclude syslog syslog-servers
```

Syntax

```
no exclude syslog { gms-server | syslog-servers }
```

Mode

Packet Monitor

Description

Disable exclusion of syslog traffic to specified server(s).

Options

gms-server GMS server.

syslog-servers Sylog servers.

Example

```
no exclude syslog syslog-servers
```

Syntax

```
exclude internal-traffic { ha | sonicpoint }
```

Mode

Packet Monitor

Description

Enable exclusion of internal traffic.

Options

ha High availability.

sonicpoint SonicPoint.

Example

```
exclude internal-traffic ha
```

Syntax

```
no exclude internal-traffic { ha | sonicpoint }
```

Mode

Packet Monitor

Description

Disable exclusion of internal traffic.

Options

ha High availability.

sonicpoint SonicPoint.

Example

```
no exclude internal-traffic internal-servers
```

Syntax

```
monitor-filter based-on-firewall-rule
```

Mode

Packet Monitor

Description

Enable packet monitor filter based on the firewall access/app rules.

Example

```
monitor-filter based-on-firewall-rule
```

Syntax

```
no monitor-filter based-on-firewall-rule
```

Mode

Packet Monitor

Description

Disable packet monitor filter based on the firewall access/app rules.

Example

```
no monitor-filter based-on-firewall-rule
```

Syntax

```
monitor-filter interfaces <WORD>
```

Mode

Packet Monitor

Description

Specify name of interface(s) on which packet capture needs to be performed (maximum 10).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
monitor-filter interfaces "X0,X1,X2:V100"  
monitor-filter interfaces "!X0,!X1"
```

Syntax

```
no monitor-filter interfaces
```

Mode

Packet Monitor

Description

Clear name of interface(s) on which packet capture needs to be performed.

Example

```
no monitor-filter interfaces
```

Syntax

```
monitor-filter ether-types <WORD>
```

Mode

Packet Monitor

Description

Specify name of ether type(s) on which packet capture needs to be performed. Currently ARP(arp), IP(ip), PPPoE-SES, PPPoE-DIS or you can specify the value directly in hex format like 0x800.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
monitor-filter ether-types "ARP,ip,0x800"  
monitor-filter ether-types "!ARP,!0x800"
```

Syntax

```
no monitor-filter ether-types
```

Mode

Packet Monitor

Description

Clear name of ether type(s) on which packet capture needs to be performed.

Example

```
no monitor-filter ether-types
```

Syntax

```
monitor-filter ip-types <WORD>
```

Mode

Packet Monitor

Description

Specify name of ip type(s) on which packet capture needs to be performed. Currently TCP, UDP, ICMP, GRE, IGMP, AH, ESP or you can specify the value directly in hex format like 0x6.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
monitor-filter ip-types "TCP,UDP,0x6"  
monitor-filter ip-types "!TCP,!0x6"
```

Syntax

```
no monitor-filter ip-types
```

Mode

Packet Monitor

Description

Clear name of ip type(s) on which packet capture needs to be performed.

Example

```
no monitor-filter ip-types
```

Syntax

monitor-filter source-ips <WORD>

Mode

Packet Monitor

Description

Specify source IP addresses on which packet capture needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
monitor-filter source-ips "10.10.10.1,10.10.10.3,10.10.10.7"  
monitor-filter source-ips "!10.10.10.1,!10.10.10.3"
```

Syntax

no monitor-filter source-ips

Mode

Packet Monitor

Description

Clear source IP addresses on which packet capture needs to be performed.

Example

```
no monitor-filter source-ips
```

Syntax

monitor-filter source-ports <WORD>

Mode

Packet Monitor

Description

Specify source TCP/UDP ports on which packet capture needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
monitor-filter source-ports "20,75,80"
```

Syntax

no monitor-filter source-ports

Mode

Packet Monitor

Description

Clear source TCP/UDP ports on which packet capture needs to be performed.

Example

```
no monitor-filter source-ports
```

Syntax

```
monitor-filter destination-ips <WORD>
```

Mode

Packet Monitor

Description

Specify destination IP addresses on which packet capture needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
monitor-filter destination-ips "10.10.10.1,10.10.10.7"  
monitor-filter destination-ips "!10.10.10.1,!10.10.10.3"
```

Syntax

```
no monitor-filter destination-ips
```

Mode

Packet Monitor

Description

Clear destination IP addresses on which packet capture needs to be performed.

Example

```
no monitor-filter destination-ips
```

Syntax

```
monitor-filter destination-ports <WORD>
```

Mode

Packet Monitor

Description

Specify destination TCP/UDP ports on which packet capture needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
monitor-filter destination-ports "20,75,80"  
monitor-filter destination-ports "!20,!80"
```

Syntax

```
no monitor-filter destination-ports
```

Mode

Packet Monitor

Description

Clear destination TCP/UDP ports on which packet capture needs to be performed.

Example

```
no monitor-filter destination-ports
```

Syntax

```
monitor-filter bidirectional
```

Mode

Packet Monitor

Description

Enable bidirectional address and port matching.

Example

```
monitor-filter bidirectional
```

Syntax

```
no monitor-filter bidirectional
```

Mode

Packet Monitor

Description

Disable bidirectional address and port matching.

Example

```
no monitor-filter bidirectional
```

Syntax

```
monitor-filter status { consumed | dropped | forwarded }
```

Mode

Packet Monitor

Description

Enable monitor filtering for the specified status.

Options

consumed Consumed.

dropped Dropped.

forwarded Forwarded.

Example

```
monitor-filter status forwarded
```

Syntax

```
no monitor-filter status { consumed | dropped | forwarded }
```

Mode

Packet Monitor

Description

Disable monitor filtering for the specified status.

Options

consumed Consumed.

dropped Dropped.

forwarded Forwarded.

Example

```
no monitor-filter status forwarded
```

Syntax

```
display-filter interfaces <WORD>
```

Mode

Packet Monitor

Description

Specify name of interface(s) on which packet filter needs to be performed (maximum 10).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
display-filter interfaces "X0,X1,X2:V100"  
display-filter interfaces "!X0,!X1"
```

Syntax

```
no display-filter interfaces
```

Mode

Packet Monitor

Description

Clear name of interface(s) on which packet filter needs to be performed.

Example

```
no display-filter interfaces
```

Syntax

```
display-filter ether-types <WORD>
```

Mode

Packet Monitor

Description

Specify name of ether type(s) on which packet filter needs to be performed. Currently ARP(arp), IP(ip), PPPoE-SES, PPPoE-DIS or you can specify the value directly in hex format like 0x800.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
display-filter ether-types "ARP,ip,0x800"  
display-filter ether-types "!ARP,!0x800"
```

Syntax

```
no display-filter ether-types
```

Mode

Packet Monitor

Description

Clear name of ether type(s) on which packet filter needs to be performed.

Example

```
no display-filter ether-types
```

Syntax

```
display-filter ip-types <WORD>
```

Mode

Packet Monitor

Description

Specify name of ip type(s) on which packet filter needs to be performed. Currently TCP, UDP, ICMP, GRE, IGMP, AH, ESP or you can specify the value directly in hex format like 0x6.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
display-filter ip-types "TCP,UDP,0x6"  
display-filter ip-types "!TCP,!0x6"
```

Syntax

```
no display-filter ip-types
```

Mode

Packet Monitor

Description

Clear name of ip type(s) on which packet filter needs to be performed.

Example

```
no display-filter ip-types
```

Syntax

```
display-filter source-ips <WORD>
```

Mode

Packet Monitor

Description

Specify source IP addresses on which packet filter needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
display-filter source-ips "10.10.10.1,10.10.10.7"  
display-filter source-ips "!10.10.10.1,!10.10.10.3"
```

Syntax

```
no display-filter source-ips
```

Mode

Packet Monitor

Description

Clear source IP addresses on which packet filter needs to be performed.

Example

```
no display-filter source-ips
```

Syntax

```
display-filter source-ports <WORD>
```

Mode

Packet Monitor

Description

Specify source TCP/UDP ports on which packet filter needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
display-filter source-ports "20,75,80"  
display-filter source-ports "!20,!80"
```

Syntax

```
no display-filter source-ports
```

Mode

Packet Monitor

Description

Clear source TCP/UDP ports on which packet filter needs to be performed.

Example

```
no display-filter source-ports
```

Syntax

```
display-filter destination-ips <WORD>
```

Mode

Packet Monitor

Description

Specify destination IP addresses on which packet filter needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
display-filter destination-ips "10.10.10.1,10.10.10.7"  
display-filter destination-ips "!10.10.10.1,!10.10.10.3"
```

Syntax

```
no display-filter destination-ips
```

Mode

Packet Monitor

Description

Clear destination IP addresses on which packet filter needs to be performed.

Example

```
no display-filter destination-ips
```

Syntax

```
display-filter destination-ports <WORD>
```

Mode

Packet Monitor

Description

Specify destination TCP/UDP ports on which packet filter needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
display-filter destination-ports "20,75,80"  
display-filter destination-ports "!20,!80"
```

Syntax

```
no display-filter destination-ports
```

Mode

Packet Monitor

Description

Clear destination TCP/UDP ports on which packet filter needs to be performed.

Example

```
no display-filter destination-ports
```

Syntax

```
display-filter bidirectional
```

Mode

Packet Monitor

Description

Enable bidirectional address and port matching.

Example

```
display-filter bidirectional
```

Syntax

```
no display-filter bidirectional
```

Mode

Packet Monitor

Description

Disable bidirectional address and port matching.

Example

```
no display-filter bidirectional
```

Syntax

```
display-filter status { consumed | dropped | forwarded | generated }
```

Mode

Packet Monitor

Description

Enable display filtering for the specified status.

Options

consumed Consumed.

dropped Dropped.

forwarded Forwarded.

generated Generated.

Example

```
display-filter status forwarded generated
```

Syntax

```
no display-filter status { consumed | dropped | forwarded | generated }
```

Mode

Packet Monitor

Description

Disable display filtering for the specified status.

Options

consumed Consumed.

dropped Dropped.

forwarded Forwarded.

generated Generated.

Example

```
no display-filter status forwarded generated
```

Syntax

```
ftp server <IPV4_HOST>
```

Mode

Packet Monitor

Description

Specify the FTP server's IP address to send the packet capture to.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
ftp server 192.168.168.75
```

Syntax

```
no ftp server
```

Mode

Packet Monitor

Description

Clear the FTP server's IP address.

Example

```
no ftp server
```

Syntax

```
ftp login <WORD>
```

Mode

Packet Monitor

Description

Specify the FTP server's login name to send the packet capture.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ftp login admin@testing.local
```

Syntax

```
no ftp login
```

Mode

Packet Monitor

Description

Clear the FTP server's login name.

Example

```
no ftp login
```

Syntax

```
ftp password <WORD>
```

Mode

Packet Monitor

Description

Specify the FTP server's login password to send the packet capture.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ftp password myftppassword
```

Syntax

no ftp password

Mode

Packet Monitor

Description

Clear the FTP server's login password.

Example

no ftp password

Syntax

ftp directory <WORD>

Mode

Packet Monitor

Description

Specify the FTP server's directory to place the packet capture in.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

ftp directory captures/firewall/

Syntax

no ftp directory

Mode

Packet Monitor

Description

Clear the FTP server's directory.

Example

no ftp directory

Syntax

ftp automatic

Mode

Packet Monitor

Description

Enable automatically log captures to the FTP server.

Example

```
ftp automatic
```

Syntax

```
no ftp automatic
```

Mode

Packet Monitor

Description

Disable automatically log captures to the FTP server.

Example

```
no ftp automatic
```

Syntax

```
ftp pcapng
```

Mode

Packet Monitor

Description

Enable logging of PCAPNG file.

Example

```
ftp pcapng
```

Syntax

```
no ftp pcapng
```

Mode

Packet Monitor

Description

Disable logging of PCAPNG file.

Example

```
no ftp pcapng
```

Syntax

```
ftp html
```

Mode

Packet Monitor

Description

Enable logging of HTML file along with .cap file.

Example

ftp html

Syntax

no ftp html

Mode

Packet Monitor

Description

Disable logging of HTML file along with .cap file.

Example

no ftp html

Syntax

monitor-filter firewall-generated

Mode

Packet Monitor

Description

Enable monitoring of firewall generated packets. (This will bypass interface filter).

Example

monitor-filter firewall-generated

Syntax

no monitor-filter firewall-generated

Mode

Packet Monitor

Description

Disable monitoring of firewall generated packets. (This will bypass interface filter).

Example

no monitor-filter firewall-generated

Syntax

monitor-filter intermediate [fragmented | intermediate-packets | iphelper | ipsec | ldap-over-tls | multicast | reassembled | remote-mirrored | restore-ports-ssl | ssl | sso-agent]

Mode

Packet Monitor

Description

Enable monitoring of intermediate packet.

Options

| | |
|-----------------------------|--|
| <i>fragmented</i> | Enable monitoring of intermediate fragmented traffic. |
| <i>intermediate-packets</i> | Enable monitoring of intermediate multicast traffic. |
| <i>iphelper</i> | Enable monitoring of intermediate IP helper traffic. |
| <i>ipsec</i> | Enable monitoring of intermediate IPSEC traffic. |
| <i>ldap-over-tls</i> | Enable monitoring of intermediate decrypted LDAP over TLS traffic. |
| <i>multicast</i> | Enable monitoring of intermediate multicast traffic. |
| <i>reassembled</i> | Enable monitoring of intermediate reassembled traffic. |
| <i>remote-mirrored</i> | Enable monitoring of intermediate remote mirrored traffic. |
| <i>restore-ports-ssl</i> | Enable restore original ports on SSL decrypted traffic. |
| <i>ssl</i> | Enable monitoring of intermediate SSL decrypted traffic. |
| <i>sso-agent</i> | Enable monitoring of intermediate decrypted Single Sign On agent messages. |

Example

```
monitor-filter intermediate ipsec
```

Syntax

```
no monitor-filter intermediate [ fragmented | intermediate-packets | iphelper | ipsec | ldap-over-tls | multicast | reassembled | remote-mirrored | restore-ports-ssl | ssl | sso-agent ]
```

Mode

Packet Monitor

Description

Disable monitoring of intermediate packet.

Options

| | |
|-----------------------------|---|
| <i>fragmented</i> | Disable monitoring of intermediate fragmented traffic. |
| <i>intermediate-packets</i> | Enable monitoring of intermediate multicast traffic. |
| <i>iphelper</i> | Disable monitoring of intermediate IP helper traffic. |
| <i>ipsec</i> | Disable monitoring of intermediate IPSEC traffic. |
| <i>ldap-over-tls</i> | Disable monitoring of intermediate decrypted LDAP over TLS traffic. |
| <i>multicast</i> | Disable monitoring of intermediate multicast traffic. |
| <i>reassembled</i> | Disable monitoring of intermediate reassembled traffic. |
| <i>remote-mirrored</i> | Disable monitoring of intermediate remote mirrored traffic. |
| <i>restore-ports-ssl</i> | Disable restore original ports on SSL decrypted traffic. |
| <i>ssl</i> | Disable monitoring of intermediate SSL decrypted traffic. |
| <i>sso-agent</i> | Disable monitoring of intermediate decrypted Single Sign On agent messages. |

Example

```
no monitor-filter intermediate ipsec
```

Syntax

mirror max-rate <UINT32>

Mode

Packet Monitor

Description

Set maximum mirror rate (in kilobits per second).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

mirror max-rate 100

Syntax

mirror only-ip-packets

Mode

Packet Monitor

Description

Enable mirror only IP packets.

Example

mirror only-ip-packets

Syntax

no mirror only-ip-packets

Mode

Packet Monitor

Description

Disable mirror only IP packets.

Example

no mirror only-ip-packets

Syntax

mirror interface <CONFIGURABLE_INTERFACE>

Mode

Packet Monitor

Description

Mirror filtered packets to interface.

Options

<CONFIGURABLE_INTERFACE> Interface name.
Example: X0

Example

```
mirror interface X3
```

Syntax

```
no mirror interface
```

Mode

Packet Monitor

Description

Disable mirror filtered packets to interface (NSA platforms only).

Example

```
no mirror interface
```

Syntax

```
mirror ip <IPV4_HOST>
```

Mode

Packet Monitor

Description

Mirror filtered packets to remote SonicWall firewall (IP address).

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
mirror ip 10.11.10.10
```

Syntax

```
no mirror ip
```

Mode

Packet Monitor

Description

Disable mirror filtered packets to remote SonicWall firewall (IP address).

Example

```
no mirror ip
```

Syntax

```
mirror receive-from-ip <IPV4_HOST>
```

Mode

Packet Monitor

Description

Receive mirrored packets from remote SonicWall firewall (IP address).

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
mirror receive-from-ip 10.11.10.10
```

Syntax

```
no mirror receive-from-ip
```

Mode

Packet Monitor

Description

Disable receive mirrored packets from remote SonicWall firewall (IP address).

Example

```
no mirror receive-from-ip
```

Syntax

```
mirror forward-interface <CONFIGURABLE_INTERFACE>
```

Mode

Packet Monitor

Description

Send received remote mirrored packets to interface.

Options

<CONFIGURABLE_INTERFACE> Interface name.
Example: *X0*

Example

```
mirror forward-interface X2
```

Syntax

```
no mirror forward-interface
```

Mode

Packet Monitor

Description

Mirror filtered packets to interface.

Example

```
no mirror forward-interface
```

Syntax

```
mirror to-capture-buffer
```

Mode

Packet Monitor

Description

Enable sending received remote mirrored packets to capture buffer.

Example

```
mirror to-capture-buffer
```

Syntax

```
no mirror to-capture-buffer
```

Mode

Packet Monitor

Description

Disable sending received remote mirrored packets to capture buffer.

Example

```
no mirror to-capture-buffer
```

Syntax

```
mirror encrypt-key <WORD>
```

Mode

Packet Monitor

Description

Encrypt remote mirrored packets via IPSec (preshared key-IKE).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
mirror encrypt-key
```

Syntax

```
mirror decrypt-key <WORD>
```

Mode

Packet Monitor

Description

Decrypt remote mirrored packets via IPSec (preshared key-IKE).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
mirror encrypt-key
```

Syntax

```
send tech-support-report
```

Mode

Config

Description

Send tech support report to MySonicwall.

Example

```
send tech-support-report
```

Syntax

```
tech-support-report options
```

Mode

Config

Description

Configure tech support report options.

Example

```
tech-support-report options
```

Syntax

```
vpn-keys
```

Mode

TSR options

Description

Enable display of VPN keys in tech support report.

Example

```
vpn-keys
```

Syntax

```
no vpn-keys
```

Mode

TSR options

Description

Disable display of VPN keys in tech support report.

Example

no vpn-keys

Syntax

arp-cache

Mode

TSR options

Description

Enable display of ARP cache in tech support report.

Example

arp-cache

Syntax

no arp-cache

Mode

TSR options

Description

Disable display of ARP cache in tech support report.

Example

no arp-cache

Syntax

dhcp-bindings

Mode

TSR options

Description

Enable display of DHCP bindings in tech support report.

Example

dhcp-bindings

Syntax

no dhcp-bindings

Mode

TSR options

Description

Disable display of DHCP bindings in tech support report.

Example

no dhcp-bindings

Syntax

ike-info

Mode

TSR options

Description

Enable display of IKE information in tech support report.

Example

ike-info

Syntax

no ike-info

Mode

TSR options

Description

Disable display of IKE information in tech support report.

Example

no ike-info

Syntax

sonicpointn diagnostics

Mode

TSR options

Description

Enable display of SonicPointN diagnostics in tech support report.

Example

sonicpointn diagnostics

Syntax

no sonicpointn diagnostics

Mode

TSR options

Description

Disable display of SonicPointN diagnostics in tech support report.

Example

no sonicpointn diagnostics

Syntax

```
users { current | detail | inactive }
```

Mode

TSR options

Description

Enable display of users in tech support report.

Options

current Current users.

detail Detail of users.

inactive Include inactive of users.

Example

```
users current
```

Syntax

```
no users { current | detail | inactive }
```

Mode

TSR options

Description

Disable display of users in tech support report.

Options

current Current users.

detail Detail of users.

inactive Include inactive of users.

Example

```
no users current
```

Syntax

```
ip-stack-info
```

Mode

TSR options

Description

Enable display of IP stack info in tech support report.

Example

```
ip-stack-info
```

Syntax

no ip-stack-info

Mode

TSR options

Description

Disable display of IP stack info in tech support report.

Example

no ip-stack-info

Syntax

dns-proxy-cache

Mode

TSR options

Description

Enable display of DNS proxy cache info in tech support report.

Example

dns-proxy-cache

Syntax

no dns-proxy-cache

Mode

TSR options

Description

Disable display of DNS proxy cache info in tech support report.

Example

no dns-proxy-cache

Syntax

debug-info

Mode

TSR options

Description

Enable display of debug info in tech support report.

Example

debug-info

Syntax

no debug-info

Mode

TSR options

Description

Disable display of debug info in tech support report.

Example

```
no debug-info
```

Syntax

```
user-name
```

Mode

TSR options

Description

Enable display of user name in tech support report.

Example

```
user-name
```

Syntax

```
no user-name
```

Mode

TSR options

Description

Disable display of user name in tech support report.

Example

```
no user-name
```

Syntax

```
ipv6 ndp
```

Mode

TSR options

Description

Enable display of IPv6 NDP in tech support report.

Example

```
ipv6 ndp
```

Syntax

```
no ipv6 ndp
```

Mode

TSR options

Description

Disable display of IPv6 NDP in tech support report.

Example

```
no ipv6 ndp
```

Syntax

```
ipv6 dhcp
```

Mode

TSR options

Description

Enable display of IPv6 DHCP in tech support report.

Example

```
ipv6 dhcp
```

Syntax

```
no ipv6 dhcp
```

Mode

TSR options

Description

Disable display of IPv6 DHCP in tech support report.

Example

```
no ipv6 dhcp
```

Syntax

```
geo-ip-cache
```

Mode

TSR options

Description

Enable display of geo-ip/botnet cache in report in tech support report.

Example

```
geo-ip-cache
```

Syntax

```
no geo-ip-cache
```

Mode

TSR options

Description

Disable display of geo-ip/botnet cache in report in tech support report.

Example

```
no geo-ip-cache
```

Syntax

```
extra-routing
```

Mode

TSR options

Description

Enable display of additional routing commands output in tech support report.

Example

```
extra-routing
```

Syntax

```
no extra-routing
```

Mode

TSR options

Description

Disable display of additional routing commands output in tech support report.

Example

```
no extra-routing
```

Syntax

```
atp-cache
```

Mode

TSR options

Description

Enable display of Capture ATP cache in tech support report.

Example

```
atp-cache
```

Syntax

```
no atp-cache
```

Mode

TSR options

Description

Disable display of Capture ATP cache in tech support report.

Example

```
no atp-cache
```

Syntax

```
secure-backup [ interval <UINT32> ]
```

Mode

TSR options

Description

Enable periodic secure backup of diagnostics report to MySonicwall.

Options

- interval** Specify backup interval.
- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
secure-backup
```

Syntax

```
no secure-backup
```

Mode

TSR options

Description

Disable periodic secure backup of diagnostics report to MySonicwall.

Example

```
no secure-backup
```

Syntax

```
send-raw-flow-data
```

Mode

TSR options

Description

Enable include raw flow table data entries when sending diagnostic report.

Example

```
send-raw-flow-data
```

Syntax

```
no send-raw-flow-data
```

Mode

TSR options

Description

Disable include raw flow table data entries when sending diagnostic report.

Example

```
no send-raw-flow-data
```

Syntax

```
diag show ipnet { interfaces | ndp | route | sockets | statistic | tcp-statistic }
```

Mode

All Modes

Description

Show IPNET status and configuration.

Options

| | |
|----------------------|--------------------------------------|
| interfaces | Show IPNET interfaces status. |
| ndp | Show IPNET NDP table. |
| route | Show IPNET routing table. |
| sockets | Show the state of all IPNET sockets. |
| statistic | Show IPNET statistic. |
| tcp-statistic | Show IPNET tcp statistic. |

Example

```
diag show ipnet interfaces
diag show ipnet sockets
diag show ipnet route
diag show ipnet ndp
diag show ipnet statistic
diag show ipnet tcp-statistic
```

Syntax

```
diag show advanced [ anti-spam | arp | backend | control-plane | dhcp | diagnostics | dial-up | dns | dns-security | dpi-ssl |
encryption | firewall | flow-reporting | geoip-location-service | high-availability | management | network | pppoe | preference |
security-service | ssl-vpn | user-authentication | voip | vpn | watchdog | wireless ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show advanced diag configuration.

Options

| | |
|----------------------|--|
| anti-spam | Anti-Spam settings. |
| arp | ARP settings. |
| backend | Backend Server settings. |
| control-plane | Control Plane Master/Slaves Monitoring and Diagnostics settings. |

| | |
|-------------------------------------|---|
| <i>dhcp</i> | DHCP settings. |
| <i>diagnostics</i> | Diagnostics settings. |
| <i>dial-up</i> | Dial-up settings. |
| <i>dns</i> | DNS settings. |
| <i>dns-security</i> | DNS Security settings. |
| <i>dpi-ssl</i> | DPI-SSL settings. |
| <i>encryption</i> | Encryption settings. |
| <i>firewall</i> | Firewall settings. |
| <i>flow-reporting</i> | Flow Reporting settings. |
| <i>geop-location-service</i> | GeoIP/Location Service settings. |
| <i>high-availability</i> | High Availability settings. |
| <i>management</i> | Management settings. |
| <i>network</i> | Network settings. |
| <i>pppoe</i> | PPPoE settings. |
| <i>preference</i> | Preference Conversion settings. |
| <i>security-service</i> | Security Services settings. |
| <i>ssl-vpn</i> | SSL-VPN settings. |
| <i>user-authentication</i> | User Authentication settings. |
| <i>voip</i> | VoIP settings. |
| <i>vpn</i> | VPN settings. |
| <i>watchdog</i> | Watchdog settings. |
| <i>wireless</i> | Wireless settings. |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |

Example

```
diag show advanced arp
```

Syntax

```
show packet-monitor [ packet <UINT32> | packets | statistics ]
```

Mode

All Modes

Description

Show packet monitor configuration.

Options

packet Show one captured packet with detail.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

packets Show all captured packets in list.

statistics Show packet monitor statistics.

Example

```
show packet-monitor
```

Syntax

```
show tech-support-report [ access-rules | active-utm | address-objects | anti-spam | anti-virus | arp-cache | cache-check | content-filtering | data-plane-task-jobs | db-trace | dhcp-client | dhcp-network-disc | dhcp-persistence | dhcp-relay | dhcp-server | dhcp-serverstat | diag | dns-proxy-cache | dpi-ssl { { client | server } } | dynamic-dns | ethernet | flight-data-recorder | gateway-anti-virus | guest-profile-objects | h323 | high-availability | hypervisor | interfaces | intrusion-detection-prevention | ip-helper | ip-reassembly | ipsec | l2tp-client | l2tp-server | ldap | license | management | mirror-state | msn | multicast | nat-policies | network | objects | options | pki | port-counters | port-status | pppoe-client | pptp-client | pref-stats | product | qos | radius | redirector-status [ list | statistics | summary | verbose ] | route-policies | routes | rtsp | schedule-objects | sd-wan | service-objects | single-sign-on [ full | statistics | status | summary ] | sip | snmp | sonicpoint | ssl-control | stateful-stats | stateful-sync | status | svrrp | time | timers | update | user-authentication-partitioning | user-objects | users-guest-users | users-local-groups | users-local-users | users-settings [ debug ] | users-status [ full | list | summary ] [ inactive ] [ debug ] | vx-net-stats | wan-load-balancing | wire-mode | wlan-zone | zone-objects ]
```

Mode

All Modes

Description

Display basic system status and information.

Options

| | |
|-----------------------------|--|
| access-rules | Access rules technical support report. |
| active-utm | Active-active UTM technical support report. |
| address-objects | Address object table technical support report. |
| anti-spam | Anti-spam technical support report. |
| anti-virus | AV technical support report. |
| arp-cache | ARP cache technical support report. |
| cache-check | Cache check technical support report. |
| content-filtering | CFL technical support report. |
| data-plane-task-jobs | Data plane task jobs technical support report. |
| db-trace | DB trace dump technical support report. |
| dhcp-client | DHCP client technical support report. |
| dhcp-network-disc | DHCP network discovery technical support report. |
| dhcp-persistence | DHCP persistence technical support report. |
| dhcp-relay | DHCP relay technical support report. |
| dhcp-server | DHCP server technical support report. |
| dhcp-serverstat | DHCP server stats technical support report. |

| | |
|---------------------------------------|--|
| <i>diag</i> | Diagnostics technical support report. |
| <i>dns-proxy-cache</i> | DNS Proxy Cache Technical Support Report. |
| <i>dpi-ssl</i> | DPI SSL technical support report. |
| <i>client</i> | DPI SSL client technical support report. |
| <i>server</i> | DPI SSL server technical support report. |
| <i>dynamic-dns</i> | Dynamic dns technical support report. |
| <i>ethernet</i> | Ethernet technical support report. |
| <i>flight-data-recorder</i> | Flight data recorder technical support report. |
| <i>gateway-anti-virus</i> | Global anti-virus technical support report. |
| <i>guest-profile-objects</i> | Guest profile objects technical support report. |
| <i>h323</i> | H.323 technical support report. |
| <i>high-availability</i> | HA technical support report. |
| <i>hypervisor</i> | Hypervisor technical support report. |
| <i>interfaces</i> | Interfaces technical support report. |
| <i>intrusion-detection-prevention</i> | IDP technical support report. |
| <i>ip-helper</i> | IP helper technical support report. |
| <i>ip-reassembly</i> | IP fragment reassembly technical support report. |
| <i>ipsec</i> | IPSec technical support report. |
| <i>l2tp-client</i> | L2tp client technical support report. |
| <i>l2tp-server</i> | L2tp server technical support report. |
| <i>ldap</i> | LDAP technical support report. |
| <i>license</i> | License technical support report. |
| <i>management</i> | Management technical support report. |
| <i>mirror-state</i> | Flash prefs mirror state technical support report. |
| <i>msn</i> | MSN technical support report. |
| <i>multicast</i> | Mcast igmp config technical support report. |
| <i>nat-policies</i> | NAT policies technical support report. |
| <i>network</i> | Network technical support report. |
| <i>objects</i> | Network objects technical support report. |
| <i>options</i> | Options of technical support report. |
| <i>pki</i> | PKI technical support report. |
| <i>port-counters</i> | Port counters technical support report. |
| <i>port-status</i> | Port status technical support report. |
| <i>pppoe-client</i> | PPPoE client technical support report. |

| | |
|---|--|
| <i>pptp-client</i> | PPTP client technical support report. |
| <i>pref-stats</i> | Flash prefs load/save technical support report. |
| <i>product</i> | Product technical support report. |
| <i>qos</i> | QOS technical support report. |
| <i>radius</i> | Radius technical support report. |
| <i>redirector-status</i> | HTTP/HTTPS redirector status technical support report. |
| <i>list</i> | Include a list of redirected users. |
| <i>statistics</i> | Show statistics counters only. |
| <i>summary</i> | Show an overall summary only. |
| <i>verbose</i> | Show detailed information. |
| <i>route-policies</i> | Detailed route policy table technical support report. |
| <i>routes</i> | Routing table. |
| <i>rtsp</i> | RTSP technical support report. |
| <i>schedule-objects</i> | Service object table technical support report. |
| <i>sd-wan</i> | SD-WAN technical support report. |
| <i>service-objects</i> | Service object table technical support report. |
| <i>single-sign-on</i> | Single sign on technical support report. |
| <i>full</i> | Show full information including a (possibly lengthy) list of SSO failures. |
| <i>statistics</i> | Show only the SSO statistics. |
| <i>status</i> | Show only the SSO status information. |
| <i>summary</i> | Show an overall summary only. |
| <i>sip</i> | SIP technical support report. |
| <i>snmp</i> | Snmp technical support report. |
| <i>sonicpoint</i> | Sonicpoint technical support report. |
| <i>ssl-control</i> | SSL control technical support report. |
| <i>stateful-stats</i> | Stateful stats technical support report. |
| <i>stateful-sync</i> | Stateful sync technical support report. |
| <i>status</i> | Status technical support report. |
| <i>svrrp</i> | SVRRP technical support report. |
| <i>time</i> | Time technical support report. |
| <i>timers</i> | Timers technical support report. |
| <i>update</i> | Update technical support report. |
| <i>user-authentication-partitioning</i> | User Authentication Partitioning Technical Support Report. |

| | |
|---------------------------|--|
| user-objects | User object table technical support report. |
| users-guest-users | Guest User Accounts Technical Support Report. |
| users-local-groups | Local User Groups Technical Support Report. |
| users-local-users | Local User Accounts Technical Support Report. |
| users-settings | Users Settings Technical Support Report. |
| debug | Include additional debug information. |
| users-status | Users Status Technical Support Report. |
| full | Show full detail of each user. |
| list | Include a terse list of connected users. |
| summary | Show an overall summary only. |
| inactive | Include a list of inactive users. |
| debug | Include additional debug information. |
| vx-net-stats | Vxworks network status technical support report. |
| wan-load-balancing | WLB technical support report. |
| wire-mode | Wire mode technical support report. |
| wlan-zone | Wlan zone technical support report. |
| zone-objects | Zone object table technical support report. |

Example

```
show tech-support-report
```

Syntax

```
address-object ipv4 [ uuid ] <ADDR_HOST_NETWORK_RANGE_NAME> [ host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> ] [ zone <ZONE_NAME> ]
```

Mode

Config

Description

Add/edit IPv4 address object.

Options

| | |
|---|--|
| uuid | Edit an address object by UUID. |
| <ADDR_HOST_NETWORK_RANGE_NAME> | Host/network/range address object name. Example: <i>Web Server</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n |

```

      HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
      Example: IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n
<ADDR_END> IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form:
      HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
      Example: IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n
zone Address object zone.
<ZONE_NAME> Zone object name.
      Example: DMZ

```

Example

```

address-object ipv4 "Mail Server" host 192.168.168.33 zone DMZ
address-object ipv4 "Web Servers" range 192.168.100.50 192.168.100.60
address-object ipv4 "HR Network" network 192.168.100.0 /24
address-object ipv4 "HR Network" network 192.168.100.0 255.255.255.0

```

Syntax

```
no address-object ipv4 [ uuid ] <ADDR_HOST_NETWORK_RANGE_NAME>
```

Mode

Config

Description

Delete an address object.

Options

```

uuid Delete an IPv4 address object by UUID.
<ADDR_HOST_NETWORK_RANGE_NAME> Host/network/range address object name.
      Example: Web Server

```

Example

```
no address-object ipv4 "Web Server"
```

Syntax

```
address-object ipv6 [ uuid ] <ADDR_HOST_NETWORK_RANGE_NAME> [ host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range
<ADDR_BEGIN> <ADDR_END> ] [ zone <ZONE_NAME> ]
```

Mode

Config

Description

Add/edit IPv6 address object.

Options

```

uuid Edit an IPv6 address object by UUID.
<ADDR_HOST_NETWORK_RANGE_NAME> Host/network/range address object name.
      Example: Web Server

host Address object host.
<ADDR_HOST> IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form:
      HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
      Example: IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n

network Address object network.
<ADDR_NETWORK> IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form:
      HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
      Example: IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n

<ADDR_MASK> IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n
      Example: IPV4: 255.255.255.0\nIPV6: /64\n

range Address object range.
<ADDR_BEGIN> IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form:

```

```

      HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
      Example: IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n
<ADDR_END> IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form:
      HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
      Example: IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n
zone Address object zone.
<ZONE_NAME> Zone object name.
      Example: DMZ

```

Example

```

address-object ipv6 "Mail Server" host fe80::217:c5ff:fecl zone DMZ
address-object ipv6 "Web Servers" range fe80::217:c5ff:fecl fe80::217:c5ff:ffff
address-object ipv6 "HR Network" network fe80::217:c5ff:fecl /64

```

Syntax

```
no address-object ipv6 [ uuid ] <ADDR_HOST_NETWORK_RANGE_NAME>
```

Mode

Config

Description

Delete an address object.

Options

```

uuid Delete an IPv6 address object by UUID.
<ADDR_HOST_NETWORK_RANGE_NAME> Host/network/range address object name.
      Example: Web Server

```

Example

```
no address-object ipv6 "Web Server"
```

Syntax

```
address-object mac [ uuid ] <ADDR_MAC_NAME> [ address <ADDR_MAC> ] [ zone <ZONE_NAME> ]
```

Mode

Config

Description

Add/edit MAC address object.

Options

```

uuid Edit a MAC address object by UUID.
<ADDR_MAC_NAME> MAC address object name.
      Example: Sales Network Access Point
address MAC address.
<ADDR_MAC> Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
zone Address object zone.
<ZONE_NAME> Zone object name.
      Example: DMZ

```

Example

```
address-object mac "WAP MAC" address 00:09:5B:BD:93:DB
```

Syntax

```
no address-object mac [ uuid ] <ADDR_MAC_NAME>
```

Mode

Config

Description

Delete an address object.

Options

uuid Delete a MAC address object by UUID.
<ADDR_MAC_NAME> MAC address object name.
Example: *Sales Network Access Point*

Example

```
no address-object mac "Sales Network Access Point"
```

Syntax

```
address-object fqdn [ uuid ] <ADDR_FQDN_NAME> [ domain <ADDR_FQDN> ] [ zone <ZONE_NAME> ]
```

Mode

Config

Description

Add/edit FQDN address object.

Options

uuid Edit an FQDN address object by UUID.
<ADDR_FQDN_NAME> FQDN address object name.
Example: *www.example.com*
domain Address object full qualified domain name.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*
zone Address object zone.
<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
address-object fqdn Whitelist domain *.google.com
```

Syntax

```
no address-object fqdn [ uuid ] <ADDR_FQDN_NAME>
```

Mode

Config

Description

Delete an address object.

Options

uuid Delete an FQDN address object by UUID.
<ADDR_FQDN_NAME> FQDN address object name.
Example: *www.example.com*

Example

```
no address-object fqdn "*.example.com"
```

Syntax

```
no address-objects [ fqdn | host | mac | network | range ]
```

Mode

Config

Description

Delete all custom address objects.

Options

fqdn Delete all custom FQDN address objects.

host Delete all custom host address objects.

mac Delete all custom MAC address objects.

network Delete all custom network address objects.

range Delete all custom range address objects.

Example

```
no address-objects
```

Syntax

```
address-object purge [ fqdn <ADDR_FQDN_NAME> | mac <ADDR_MAC_NAME> ]
```

Mode

Config

Description

Purge a specified MAC/FQDN address object or all address objects.

Options

fqdn Purge a FQDN address object.
<ADDR_FQDN_NAME> FQDN address object name.
Example: *www.example.com*

mac Purge a MAC address object.
<ADDR_MAC_NAME> MAC address object name.
Example: *Sales Network Access Point*

Example

```
address-object purge mac "WAP MAC"  
address-object purge fqdn "*.example.com"  
address-object purge
```

Syntax

```
address-group ipv4 [ uuid ] <ADDR_GROUP_NAME>
```

Mode

Config

Description

Add/edit IPv4 address group.

Options

uuid Edit an IPv4 address group by UUID.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

```
address-group ipv4 "Corp Web Servers"
```

Syntax

```
no address-group ipv4 [ uuid ] <ADDR_GROUP_NAME>
```

Mode

Config

Description

Delete an IPv4 address group.

Options

uuid Delete an IPv4 address group by UUID.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

```
no address-group ipv4 "Corp Web Servers"
```

Syntax

```
address-group ipv6 [ uuid ] <ADDR_GROUP_NAME>
```

Mode

Config

Description

Add/edit IPv6 address group.

Options

uuid Delete an IPv6 address group by UUID.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

```
address-group ipv6 "Corp Web Servers"
```

Syntax

```
no address-group ipv6 [ uuid ] <ADDR_GROUP_NAME>
```

Mode

Config

Description

Delete an IPv4 address group.

Options

uuid Delete an IPv6 address group by UUID.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

```
no address-group ipv6 "Corp Web Servers"
```

Syntax

```
no address-groups [ ipv4 | ipv6 ]
```

Mode

Config

Description

Delete all custom address groups.

Options

ipv4 Delete all IPv4 address groups.

ipv6 Delete all IPv6 address groups.

Example

```
no address-groups
```

Syntax

```
uuid <UUID>
```

Mode

Address Object

Description

Set address object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

Address Object

Description

Clear address object UUID.

Example

no uuid

Syntax

name <ADDR_HOST_NETWORK_RANGE_NAME>

Mode

Address Object

Description

Set address object name.

Options

<ADDR_HOST_NETWORK_RANGE_NAME> Host/network/range address object name.
Example: *Web Server*

Example

name "Corp E-mail Server"

Syntax

host <ADDR_HOST>

Mode

Address Object

Description

Set address object host.

Options

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

host 10.10.10.10

Syntax

no host

Mode

Address Object

Description

Clear address object host.

Example

no host

Syntax

range <ADDR_BEGIN> <ADDR_END>

Mode

Address Object

Description

Set address object range.

Options

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
range 10.10.10.1 10.10.10.10
```

Syntax

```
no range
```

Mode

Address Object

Description

Clear address object range.

Example

```
no range
```

Syntax

```
network <ADDR_NETWORK> <ADDR_MASK>
```

Mode

Address Object

Description

Set address object network.

Options

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

Example

```
network 10.10.10.0 255.255.255.0
```

Syntax

```
no network
```

Mode

Address Object

Description

Clear address object network.

Example

```
no network
```

Syntax

```
zone <ZONE_NAME>
```

Mode

Address Object

Description

Set address object zone.

Options

<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
zone WAN
```

Syntax

```
uuid <UUID>
```

Mode

MAC Address Object

Description

Set address object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

MAC Address Object

Description

Clear address object UUID.

Example

```
no uuid
```

Syntax

name <ADDR_MAC_NAME>

Mode

MAC Address Object

Description

Set address object name.

Options

<ADDR_MAC_NAME> MAC address object name.
Example: *Sales Network Access Point*

Example

name "Corp E-mail Server"

Syntax

address <ADDR_MAC>

Mode

MAC Address Object

Description

Set address object MAC.

Options

<ADDR_MAC> Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.

Example

address 00:D0:68:09:4B:2A

Syntax

no address

Mode

MAC Address Object

Description

Clear address object MAC.

Example

no address

Syntax

zone <ZONE_NAME>

Mode

MAC Address Object

Description

Set address object zone.

Options

<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

zone WAN

Syntax

multi-homed

Mode

MAC Address Object

Description

Enable multi-homed host.

Example

multi-homed

Syntax

no multi-homed

Mode

MAC Address Object

Description

Disable multi-homed host.

Example

no multi-homed

Syntax

uuid <UUID>

Mode

FQDN Address Object

Description

Set address object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

FQDN Address Object

Description

Clear address object UUID.

Example

no uuid

Syntax

name <ADDR_FQDN_NAME>

Mode

FQDN Address Object

Description

Set address object name.

Options

<ADDR_FQDN_NAME> FQDN address object name.
Example: *www.example.com*

Example

name "Corp E-mail Server"

Syntax

domain <ADDR_FQDN>

Mode

FQDN Address Object

Description

Set address object fully qualified domain name (FQDN).

Options

<ADDR_FQDN> FQDN in the form: *example.com* or **.example.com*.
Example: *example.com*

Example

domain www.sonicwall.com

Syntax

no domain

Mode

FQDN Address Object

Description

Clear address object fully qualified domain name (FQDN).

Example

no domain

Syntax

zone <ZONE_NAME>

Mode

FQDN Address Object

Description

Set address object zone.

Options

<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

zone WAN

Syntax

dns-ttl <UINT16>

Mode

FQDN Address Object

Description

Manually set DNS entries' TTL.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

dns-ttl 120

Syntax

no dns-ttl

Mode

FQDN Address Object

Description

Disable manually set DNS entries' TTL.

Example

no dns-ttl

Syntax

uuid <UUID>

Mode

IPV6 Address Object

Description

Set address object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

IPV6 Address Object

Description

Clear address object UUID.

Example

```
no uuid
```

Syntax

```
name <ADDR_HOST_NETWORK_RANGE_NAME>
```

Mode

IPV6 Address Object

Description

Set address object name.

Options

<ADDR_HOST_NETWORK_RANGE_NAME> Host/network/range address object name.
Example: *Web Server*

Example

```
name "Corp E-mail Server"
```

Syntax

```
host <ADDR_HOST>
```

Mode

IPV6 Address Object

Description

Set address object host IP.

Options

<ADDR_HOST> IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

```
host fe80::217:c5ff:fec2
```

Syntax

```
no host
```

Mode

IPv6 Address Object

Description

Clear address object host IP.

Example

```
no host
```

Syntax

```
range <ADDR_BEGIN> <ADDR_END>
```

Mode

IPv6 Address Object

Description

Set address object range.

Options

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n

Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n

Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
range fe80::217:c5ff:fec1 fe80::217:c5ff:ffff
```

Syntax

```
no range
```

Mode

IPv6 Address Object

Description

Clear address object range.

Example

```
no range
```

Syntax


```
network <ADDR_NETWORK> <ADDR_PREFIX_LEN>
```

Mode

IPv6 Address Object

Description

Set address object network.

Options

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_PREFIX_LEN> Network prefix length in decimal or CIDR form: D OR /D.
Max: 128
Example: *128*

Example

```
network fe80::217:c5ff:fecl /64
```

Syntax

```
no network
```

Mode

IPv6 Address Object

Description

Clear address object network.

Example

```
no network
```

Syntax

```
zone <ZONE_NAME>
```

Mode

IPv6 Address Object

Description

Set address object zone.

Options

<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
zone WAN
```

Syntax

```
uuid <UUID>
```

Mode

IPv4 Address Group

Description

Set address group UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

IPv4 Address Group

Description

Clear address group UUID.

Example

```
no uuid
```

Syntax

```
name <ADDR_GROUP_NAME>
```

Mode

IPv4 Address Group

Description

Set address group name.

Options

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

```
name "Corporate Servers "
```

Syntax

```
no address-object ipv4 <ADDR_HOST_NETWORK_RANGE_NAME>
```

Mode

IPv4 Address Group

IPv6 Address Group

Description

Remove an IPv4 address object from group.

Options

<ADDR_HOST_NETWORK_RANGE_NAME> Host/network/range address object name.
Example: *Web Server*

Example

```
no address-object ipv4 "Corp E-mail Server"
```

Syntax

```
address-object ipv4 <ADDR_HOST_NETWORK_RANGE_NAME>
```

Mode

IPV4 Address Group
IPV6 Address Group

Description

Assign an IPv4 address object to group.

Options

<ADDR_HOST_NETWORK_RANGE_NAME> Host/network/range address object name.
Example: *Web Server*

Example

```
address-object ipv4 "Corp E-mail Server"
```

Syntax

```
no address-object mac <ADDR_MAC_NAME>
```

Mode

IPV4 Address Group
IPV6 Address Group

Description

Remove a MAC address object from group.

Options

<ADDR_MAC_NAME> MAC address object name.
Example: *Sales Network Access Point*

Example

```
no address-object mac "Corp E-mail Server"
```

Syntax

```
address-object mac <ADDR_MAC_NAME>
```

Mode

IPV4 Address Group
IPV6 Address Group

Description

Assign an MAC address object to group.

Options

<ADDR_MAC_NAME> MAC address object name.
Example: *Sales Network Access Point*

Example

```
address-object mac "Corp E-mail Server"
```

Syntax

```
no address-object fqdn <ADDR_FQDN_NAME>
```

Mode

IPv4 Address Group
IPv6 Address Group

Description

Remove a FQDN address object from group.

Options

<ADDR_FQDN_NAME> FQDN address object name.
Example: *www.example.com*

Example

```
no address-object fqdn "Corp E-mail Server"
```

Syntax

```
address-object fqdn <ADDR_FQDN_NAME>
```

Mode

IPv4 Address Group
IPv6 Address Group

Description

Assign an FQDN address object to group.

Options

<ADDR_FQDN_NAME> FQDN address object name.
Example: *www.example.com*

Example

```
address-object fqdn "Corp E-mail Server"
```

Syntax

```
no address-group ipv4 <ADDR_GROUP_NAME>
```

Mode

IPv4 Address Group
IPv6 Address Group

Description

Remove an IPv4 address group from group.

Options

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

```
no address-group ipv4 "Corp Web Servers"
```

Syntax

```
address-group ipv4 <ADDR_GROUP_NAME>
```

Mode

IPV4 Address Group
IPV6 Address Group

Description

Assign an IPv4 address group to group.

Options

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

```
address-group ipv4 "Corp Web Servers"
```

Syntax

```
uuid <UUID>
```

Mode

IPV6 Address Group

Description

Set address group UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

IPV6 Address Group

Description

Clear address group UUID.

Example

```
no uuid
```

Syntax

```
name <ADDR_GROUP_NAME>
```

Mode

IPV6 Address Group

Options

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

```
name "Corporate Servers "
```

Syntax

```
no address-object ipv6 <ADDR_NAME>
```

Mode

IPv6 Address Group

Description

Remove an IPv6 address object from group.

Options

<ADDR_NAME> Address object name.
Example: *Web Server*

Example

```
no address-object ipv6 "Corp E-mail Server"
```

Syntax

```
address-object ipv6 <ADDR_NAME>
```

Mode

IPv6 Address Group

Description

Assign an IPv6 address object to group.

Options

<ADDR_NAME> Address object name.
Example: *Web Server*

Example

```
address-object ipv6 "Corp E-mail Server"
```

Syntax

```
no address-group ipv6 <ADDR_GROUP_NAME>
```

Mode

IPv6 Address Group

Description

Remove an IPv6 address group from group.

Options

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

```
no address-group ipv6 "Corp Web Servers"
```

Syntax

```
address-group ipv6 <ADDR_GROUP_NAME>
```

Mode

IPv6 Address Group

Description

Assign an IPv6 address group to group.

Options

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

```
address-group ipv6 "Corp Web Servers"
```

Syntax

```
schedule [ uuid ] <SCHED_NAME>
```

Mode

Config

Description

Add/Edit a Schedule.

Options

uuid Edit a schedule object by UUID.
<SCHED_NAME> Schedule object name.
Example: *Work Hours*

Example

```
schedule "Contract Schedule"
```

Syntax

```
no schedule [ uuid ] <SCHED_NAME>
```

Mode

Config

Description

Delete a schedule.

Options

uuid Delete a schedule object by UUID.
<SCHED_NAME> Schedule object name.
Example: *Work Hours*

Example

```
no schedule "Maintenance Schedule"
```

Syntax

```
no schedules
```

Mode

Config

Description

Delete all custom schedules.

Example

```
no schedules
```

Syntax

```
name <WORD>
```

Mode

Schedule

Description

Schedule object name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name "Contract Schedule"
```

Syntax

```
uuid <UUID>
```

Mode

Schedule

Description

Set schedule object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid f40b27d6-b8b9-a4fc-0b00-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

Schedule

Description

Clear schedule object UUID.

Example

no uuid

Syntax

```
occurs { mixed | once | recurring }
```

Mode

Schedule

Description

Set schedule occurrence.

Options

mixed Set for both recurring schedule and single occurrence.

once Set for single occurrence.

recurring Set for recurring schedule.

Example

```
occurs recurring
```

Syntax

```
event <TIME_YYYYMMDDHHMM> <TIME_YYYYMMDDHHMM>
```

Mode

One Time Schedule
Mixed Schedule

Description

Enter the start and end date and time of a one time event.

Options

<TIME_YYYYMMDDHHMM> Timestamp in the form: YYYY:MM:DD:HH:MM.
Example: 2010:06:30:23:30

<TIME_YYYYMMDDHHMM> Timestamp in the form: YYYY:MM:DD:HH:MM.
Example: 2010:06:30:23:30

Example

```
event 2010:06:01:00:00 2010:06:02:00:00
```

Syntax

```
recurring <TIME_HHMM> <TIME_HHMM> { { [ sun ] [ mon ] [ tue ] [ wed ] [ thu ] [ fri ] [ sat ] } | all }
```

Mode

Mixed Schedule
Recurring Schedule

Description

Add to the list of applicable days and start and stop time of the schedule.

Options

<TIME_HHMM> Time in the form: DD:DD.
Example: 12:00

<TIME_HHMM> Time in the form: DD:DD.
Example: 12:00

sun Day of the week.
mon Day of the week.
tue Day of the week.
wed Day of the week.
thu Day of the week.
fri Day of the week.
sat Day of the week.

all Everyday.

Example

```
recurring 12:00 18:00 mon tue wed thu fri
```

Syntax

```
no recurring <TIME_HHMM> <TIME_HHMM> { { [ sun ] [ mon ] [ tue ] [ wed ] [ thu ] [ fri ] [ sat ] } | all }
```

Mode

Mixed Schedule
Recurring Schedule

Description

Remove from the schedule an entry by specifying applicable days and start and stop time.

Options

<TIME_HHMM> Time in the form: DD:DD.
Example: 12:00

<TIME_HHMM> Time in the form: DD:DD.
Example: 12:00

sun Day of the week.
mon Day of the week.
tue Day of the week.
wed Day of the week.
thu Day of the week.
fri Day of the week.
sat Day of the week.

all Everyday.

Example

```
no recurring 12:00 18:00 mon tue wed thu fri
```

Syntax

```
no service-object [ uuid ] <SVC_NAME>
```

Mode

Config

Description

Delete a service object.

Options

uuid Delete a service object by UUID.

<SVC_NAME> Service object name.
Example: *HTTPS*

Example

```
no service-object "Corp E-mail Server"
```

Syntax

```
no service-objects
```

Mode

Config

Description

Delete all custom service objects.

Example

```
no service-objects
```

Syntax

```
service-object [ uuid ] <SVC_NAME> [ 6over4 | ah | custom <UINT8> | eigrp | esp | gre | icmp { { { address-mask-reply | address-mask-request | alternative-host | datagram-error | destination-unreachable | domain-name | domain-name-reply | echo-reply | echo-request | info-reply | info-request | mobile-host-redirect | mobile-registration-reply | mobile-registration-request | none | parameter-problem | redirect | router-advertise | router-solicit | source-quench | time-exceeded | timestamp | timestamp-reply | traceroute } } } | icmpv6 { { { certification-path-advertisement | certification-path-solicitation | destination-unreachable | echo-reply | echo-request | fmipv6 | home-discover-reply | home-discover-request | inverse-nd-advertisement | inverse-nd-solicitation | mobile-prefix-advertisement | mobile-prefix-solicitation | multicast-listener-done | multicast-listener-query | multicast-listener-report | multicast-router-advertisement | multicast-router-solicitation | multicast-router-termination | neighbour-advertisement | neighbour-solicitation | node-query | node-response | none | packet-too-big | parameter-problem | redirect | router-advertisement | router-renumbering | router-solicitation | rpl-control | time-exceeded | v2-multicast-listener-report } } } | igmp { { { leave-group | member-query | none | v1-member-report | v2-member-report | v3-member-report } } } | ipcomp | l2tp | ospf { { { database-description | hello | link-state-acknowledge | link-state-request | link-state-update | none } } } | pim { { { assert | bootstrap | candidate-rp | graft | graft-acknowledge | hello | join-prune | none | register | register-stop | state-refresh } } } | tcp <SVC_PORT_BEGIN> <SVC_PORT_END> | udp <SVC_PORT_BEGIN> <SVC_PORT_END> ]
```

Mode

Config

Description

Add/edit firewall and service object and enter configuration mode.

Options

| | |
|-----------------------------|--|
| uuid | Edit a service object by UUID. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| 6over4 | Service object 6over4. |
| ah | Service object AH. |
| custom | Custom service object. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| eigrp | Service object EIGRP. |
| esp | Service object ESP. |
| gre | Service object GRE. |
| icmp | Service object ICMP. |
| address-mask-reply | ICMP with sub-type of address mask reply. |
| address-mask-request | ICMP with sub-type of address mask request. |

| | |
|---|---|
| <i>alternative-host</i> | ICMP with sub-type of alternative address for host. |
| <i>datagram-error</i> | ICMP with sub-type of datagram error. |
| <i>destination-unreachable</i> | ICMP with sub-type of destination unreachable. |
| <i>domain-name</i> | ICMP with sub-type of domain name. |
| <i>domain-name-reply</i> | ICMP with sub-type of domain name reply. |
| <i>echo-reply</i> | ICMP with sub-type of echo reply. |
| <i>echo-request</i> | ICMP with sub-type of echo request. |
| <i>info-reply</i> | ICMP with sub-type of info reply. |
| <i>info-request</i> | ICMP with sub-type of info request. |
| <i>mobile-host-redirect</i> | ICMP with sub-type of mobile host redirect. |
| <i>mobile-registration-reply</i> | ICMP with sub-type of mobile registration reply. |
| <i>mobile-registration-request</i> | ICMP with sub-type of mobile registration request. |
| <i>none</i> | ICMP with sub-type of none. |
| <i>parameter-problem</i> | ICMP with sub-type of parameter problem. |
| <i>redirect</i> | ICMP with sub-type of redirect. |
| <i>router-advertise</i> | ICMP with sub-type of router advertise. |
| <i>router-solicit</i> | ICMP with sub-type of router solicit. |
| <i>source-quench</i> | ICMP with sub-type of source quench. |
| <i>time-exceeded</i> | ICMP with sub-type of time exceeded. |
| <i>timestamp</i> | ICMP with sub-type of timestamp. |
| <i>timestamp-reply</i> | ICMP with sub-type of timestamp reply. |
| <i>traceroute</i> | ICMP with sub-type of traceroute. |
| <i>icmpv6</i> | Service object ICMPV6/ND. |
| <i>certification-path-advertisement</i> | ICMPV6 with sub-type of certification path advertisement message. |
| <i>certification-path-solicitation</i> | ICMPV6 with sub-type of certification path solicitation message. |
| <i>destination-unreachable</i> | ICMPV6 with sub-type of destination unreachable. |
| <i>echo-reply</i> | ICMPV6 with sub-type of echo reply. |
| <i>echo-request</i> | ICMPV6 with sub-type of echo request. |
| <i>fmipv6</i> | ICMPV6 with sub-type of FMIPv6 messages. |
| <i>home-discover-reply</i> | ICMPV6 with sub-type of home agent address discovery reply message. |
| <i>home-discover-request</i> | ICMPV6 with sub-type of home agent address discovery request message. |
| <i>inverse-nd-advertisement</i> | ICMPV6 with sub-type of inverse ND advertisement message. |
| <i>inverse-nd-solicitation</i> | ICMPV6 with sub-type of inverse ND solicitation message. |

| | |
|---------------------------------------|--|
| <i>mobile-prefix-advertisement</i> | ICMPV6 with sub-type of mobile prefix advertisement. |
| <i>mobile-prefix-solicitation</i> | ICMPV6 with sub-type of mobile prefix solicitation. |
| <i>multicast-listener-done</i> | ICMPV6 with sub-type of multicast listener done. |
| <i>multicast-listener-query</i> | ICMPV6 with sub-type of multicast listener query. |
| <i>multicast-listener-report</i> | ICMPV6 with sub-type of multicast listener report. |
| <i>multicast-router-advertisement</i> | ICMPV6 with sub-type of multicast router advertisement. |
| <i>multicast-router-solicitation</i> | ICMPV6 with sub-type of multicast router solicitation. |
| <i>multicast-router-termination</i> | ICMPV6 with sub-type of multicast router termination. |
| <i>neighbour-advertisement</i> | ICMPV6 with sub-type of neighbour advertisement. |
| <i>neighbour-solicitation</i> | ND with sub-type of neighbour solicitation. |
| <i>node-query</i> | ICMPV6 with sub-type of ICMP node information query. |
| <i>node-response</i> | ICMPV6 with sub-type of ICMP node information response. |
| <i>none</i> | ICMPV6 with sub-type of none. |
| <i>packet-too-big</i> | ICMPV6 with sub-type of packet too big. |
| <i>parameter-problem</i> | ICMPV6 with sub-type of parameter problem. |
| <i>redirect</i> | ND with sub-type of redirect. |
| <i>router-advertisement</i> | ND with sub-type of router advertisement. |
| <i>router-renumbering</i> | ICMPV6 with sub-type of router renumbering. |
| <i>router-solicitation</i> | ND with sub-type of router solicitation. |
| <i>rpl-control</i> | ICMPV6 with sub-type of RPL control message. |
| <i>time-exceeded</i> | ICMPV6 with sub-type of time exceeded. |
| <i>v2-multicast-listener-report</i> | ICMPV6 with sub-type of version 2 multicast listener report. |
| <i>igmp</i> | Service object IGMP. |
| <i>leave-group</i> | IGMP with sub-type of leave group. |
| <i>member-query</i> | IGMP with sub-type of member query. |
| <i>none</i> | IGMP with sub-type of none. |
| <i>v1-member-report</i> | IGMP with sub-type of v1 member report. |
| <i>v2-member-report</i> | IGMP with sub-type of v2 member report. |
| <i>v3-member-report</i> | IGMP with sub-type of v3 member report. |
| <i>ipcomp</i> | Service object IPCOMP. |
| <i>l2tp</i> | Service object l2tp. |
| <i>ospf</i> | Service object OSPF. |
| <i>database-description</i> | OSPF with sub-type of database description. |
| <i>hello</i> | OSPF with sub-type of hello. |

| | |
|-------------------------------|--|
| <i>link-state-acknowledge</i> | OSPF with sub-type of link state acknowledge. |
| <i>link-state-request</i> | OSPF with sub-type of link state request. |
| <i>link-state-update</i> | OSPF with sub-type of link state update. |
| <i>none</i> | OSPF with sub-type of none. |
| <i>pim</i> | Service object PIM. |
| <i>assert</i> | PIM with sub-type of assert. |
| <i>bootstrap</i> | PIM with sub-type of bootstrap. |
| <i>candidate-rp</i> | PIM with sub-type of candidate rp. |
| <i>graft</i> | PIM with sub-type of graft. |
| <i>graft-acknowledge</i> | PIM with sub-type of graft acknowledge. |
| <i>hello</i> | PIM with sub-type of hello. |
| <i>join-prune</i> | PIM with sub-type of join/prune. |
| <i>none</i> | PIM with sub-type of none. |
| <i>register</i> | PIM with sub-type of register. |
| <i>register-stop</i> | PIM with sub-type of register stop. |
| <i>state-refresh</i> | PIM with sub-type of state refresh. |
| <i>tcp</i> | Service object TCP. |
| <i><SVC_PORT_BEGIN></i> | Integer in the form: D OR 0xHHHH. Example: 80 |
| <i><SVC_PORT_END></i> | Integer in the form: D OR 0xHHHH. Example: 80 |
| <i>udp</i> | Service object UDP. |
| <i><SVC_PORT_BEGIN></i> | Integer in the form: D OR 0xHHHH. Example: 80 |
| <i><SVC_PORT_END></i> | Integer in the form: D OR 0xHHHH. Example: 80 |

Example

```
service-object "Web Server" TCP 80 80
```

Syntax

```
no service-group [ uuid ] <SVC_GROUP_NAME>
```

Mode

Config

Description

Delete a service group.

Options

| | |
|-------------------------------|--|
| <i>uuid</i> | Delete a service group by UUID. |
| <i><SVC_GROUP_NAME></i> | Service object group name. Example: <i>VOIP</i> |

Example

```
no service-group "Corporate Servers"
```

Syntax

```
no service-groups
```

Mode

Config

Description

Delete all custom service groups.

Example

```
no service-groups
```

Syntax

```
service-group [ uuid ] <SVC_GROUP_NAME>
```

Mode

Config

Description

Add/edit service group and enter configuration mode.

Options

| | |
|-------------------------------|--|
| uuid | Edit a service group by UUID. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |

Example

```
service-group "Corporate Servers"
```

Syntax

```
name <SVC_NAME>
```

Mode

Service Object

Description

Set service object name.

Options

| | |
|-------------------------|---|
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
|-------------------------|---|

Example

```
name "Corp E-mail Server "
```

Syntax

```
uuid <UUID>
```

Mode

Service Object

Description

Set service object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

Service Object

Description

Clear service object UUID.

Example

```
no uuid
```

Syntax

```
custom <UINT8>
```

Mode

Service Object

Description

Set service object as custom and specify.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
custom 123
```

Syntax

```
icmp { { { address-mask-reply | address-mask-request | alternative-host | datagram-error | destination-unreachable | domain-name | domain-name-reply | echo-reply | echo-request | info-reply | info-request | mobile-host-redirect | mobile-registration-reply | mobile-registration-request | none | parameter-problem | redirect | router-advertise | router-solicit | source-quench | time-exceeded | timestamp | timestamp-reply | traceroute } } }
```

Mode

Service Object

Description

Set service object as ICMP and specify sub type.

Options

| | |
|------------------------------------|---|
| <i>address-mask-reply</i> | ICMP with sub-type of address mask reply. |
| <i>address-mask-request</i> | ICMP with sub-type of address mask request. |
| <i>alternative-host</i> | ICMP with sub-type of alternative address for host. |
| <i>datagram-error</i> | ICMP with sub-type of datagram error. |
| <i>destination-unreachable</i> | ICMP with sub-type of destination unreachable. |
| <i>domain-name</i> | ICMP with sub-type of domain name. |
| <i>domain-name-reply</i> | ICMP with sub-type of domain name reply. |
| <i>echo-reply</i> | ICMP with sub-type of echo reply. |
| <i>echo-request</i> | ICMP with sub-type of echo request. |
| <i>info-reply</i> | ICMP with sub-type of info reply. |
| <i>info-request</i> | ICMP with sub-type of info request. |
| <i>mobile-host-redirect</i> | ICMP with sub-type of mobile host redirect. |
| <i>mobile-registration-reply</i> | ICMP with sub-type of mobile registration reply. |
| <i>mobile-registration-request</i> | ICMP with sub-type of mobile registration request. |
| <i>none</i> | ICMP with sub-type of none. |
| <i>parameter-problem</i> | ICMP with sub-type of parameter problem. |
| <i>redirect</i> | ICMP with sub-type of redirect. |
| <i>router-advertise</i> | ICMP with sub-type of router advertise. |
| <i>router-solicit</i> | ICMP with sub-type of router solicit. |
| <i>source-quench</i> | ICMP with sub-type of source quench. |
| <i>time-exceeded</i> | ICMP with sub-type of time exceeded. |
| <i>timestamp</i> | ICMP with sub-type of timestamp. |
| <i>timestamp-reply</i> | ICMP with sub-type of timestamp reply. |
| <i>traceroute</i> | ICMP with sub-type of traceroute. |

Example

```
icmp echo-reply
```

Syntax

```
igmp { { { leave-group | member-query | none | v1-member-report | v2-member-report | v3-member-report } } }
```

Mode

Service Object

Description

Set service object as IGMP and specify sub type.

Options

| | |
|-------------------------|---|
| leave-group | IGMP with sub-type of leave group. |
| member-query | IGMP with sub-type of member query. |
| none | IGMP with sub-type of none. |
| v1-member-report | IGMP with sub-type of v1 member report. |
| v2-member-report | IGMP with sub-type of v2 member report. |
| v3-member-report | IGMP with sub-type of v3 member report. |

Example

```
igmp member-query
```

Syntax

```
tcp <SVC_PORT_BEGIN> <SVC_PORT_END>
```

Mode

Service Object

Description

Set service object as TCP.

Options

| | |
|-------------------------------|--|
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: 80 |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: 80 |

Example

```
tcp 1 80
```

Syntax

```
udp <SVC_PORT_BEGIN> <SVC_PORT_END>
```

Mode

Service Object

Description

Set service object as UDP.

Options

| | |
|-------------------------------|--|
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: 80 |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: 80 |

Example

```
udp 1 80
```

Syntax

6over4

Mode

Service Object

Description

Set service object as 6over4.

Example

6over4

Syntax

gre

Mode

Service Object

Description

Set service object as GRE.

Example

gre

Syntax

esp

Mode

Service Object

Description

Set service object as ESP.

Example

esp

Syntax

ah

Mode

Service Object

Description

Set service object as AH.

Example

ah

Syntax

icmpv6 { { certification-path-advertisement | certification-path-solicitation | destination-unreachable | echo-reply | echo-request | fmipv6 | home-discover-reply | home-discover-request | inverse-nd-advertisement | inverse-nd-solicitation | mobile-prefix-advertisement | mobile-prefix-solicitation | multicast-listener-done | multicast-listener-report | service-unavailable | source-quarantine-report

```
| multicast-router-advertisement | multicast-router-solicitation | multicast-router-termination | neighbour-advertisement |  
neighbour-solicitation | node-query | node-response | none | packet-too-big | parameter-problem | redirect | router-advertisement  
| router-renumbering | router-solicitation | rpl-control | time-exceeded | v2-multicast-listener-report } } }
```

Mode

Service Object

Description

Set service object as ICMPV6.

Options

| | |
|--|---|
| <i>certification-path-advertisement</i> | ICMPV6 with sub-type of certification path advertisement message. |
| <i>certification-path-solicitation</i> | ICMPV6 with sub-type of certification path solicitation message. |
| <i>destination-unreachable</i> | ICMPV6 with sub-type of destination unreachable. |
| <i>echo-reply</i> | ICMPV6 with sub-type of echo reply. |
| <i>echo-request</i> | ICMPV6 with sub-type of echo request. |
| <i>fmipv6</i> | ICMPV6 with sub-type of FMIPv6 messages. |
| <i>home-discover-reply</i> | ICMPV6 with sub-type of home agent address discovery reply message. |
| <i>home-discover-request</i> | ICMPV6 with sub-type of home agent address discovery request message. |
| <i>inverse-nd-advertisement</i> | ICMPV6 with sub-type of inverse ND advertisement message. |
| <i>inverse-nd-solicitation</i> | ICMPV6 with sub-type of inverse ND solicitation message. |
| <i>mobile-prefix-advertisement</i> | ICMPV6 with sub-type of mobile prefix advertisement. |
| <i>mobile-prefix-solicitation</i> | ICMPV6 with sub-type of mobile prefix solicitation. |
| <i>multicast-listener-done</i> | ICMPV6 with sub-type of multicast listener done. |
| <i>multicast-listener-query</i> | ICMPV6 with sub-type of multicast listener query. |
| <i>multicast-listener-report</i> | ICMPV6 with sub-type of multicast listener report. |
| <i>multicast-router-advertisement</i> | ICMPV6 with sub-type of multicast router advertisement. |
| <i>multicast-router-solicitation</i> | ICMPV6 with sub-type of multicast router solicitation. |
| <i>multicast-router-termination</i> | ICMPV6 with sub-type of multicast router termination. |
| <i>neighbour-advertisement</i> | ICMPV6 with sub-type of neighbour advertisement. |
| <i>neighbour-solicitation</i> | ND with sub-type of neighbour solicitation. |
| <i>node-query</i> | ICMPV6 with sub-type of ICMP node information query. |
| <i>node-response</i> | ICMPV6 with sub-type of ICMP node information response. |
| <i>none</i> | ICMPV6 with sub-type of none. |
| <i>packet-too-big</i> | ICMPV6 with sub-type of packet too big. |
| <i>parameter-problem</i> | ICMPV6 with sub-type of parameter problem. |
| <i>redirect</i> | ND with sub-type of redirect. |
| <i>router-advertisement</i> | ND with sub-type of router advertisement. |

| | |
|-------------------------------------|--|
| <i>router-renumbering</i> | ICMPV6 with sub-type of router renumbering. |
| <i>router-solicitation</i> | ND with sub-type of router solicitation. |
| <i>rpl-control</i> | ICMPV6 with sub-type of RPL control message. |
| <i>time-exceeded</i> | ICMPV6 with sub-type of time exceeded. |
| <i>v2-multicast-listener-report</i> | ICMPV6 with sub-type of version 2 multicast listener report. |

Example

```
icmpv6 echo-reply
```

Syntax

```
eigrp
```

Mode

Service Object

Description

Set service object as EIGRP.

Example

```
eigrp
```

Syntax

```
ospf { { { database-description | hello | link-state-acknowledge | link-state-request | link-state-update | none } } }
```

Mode

Service Object

Description

Set service object as OSPF and specify sub type.

Options

| | |
|-------------------------------|---|
| <i>database-description</i> | OSPF with sub-type of database description. |
| <i>hello</i> | OSPF with sub-type of hello. |
| <i>link-state-acknowledge</i> | OSPF with sub-type of link state acknowledge. |
| <i>link-state-request</i> | OSPF with sub-type of link state request. |
| <i>link-state-update</i> | OSPF with sub-type of link state update. |
| <i>none</i> | OSPF with sub-type of none. |

Example

```
ospf hello
```

Syntax

```
pim { { { assert | bootstrap | candidate-rp | graft | graft-acknowledge | hello | join-prune | none | register | register-stop | state-refresh } } }
```

Mode

Service Object

Description

Set service object as PIM and specify sub type.

Options

| | |
|--------------------------|---|
| <i>assert</i> | PIM with sub-type of assert. |
| <i>bootstrap</i> | PIM with sub-type of bootstrap. |
| <i>candidate-rp</i> | PIM with sub-type of candidate rp. |
| <i>graft</i> | PIM with sub-type of graft. |
| <i>graft-acknowledge</i> | PIM with sub-type of graft acknowledge. |
| <i>hello</i> | PIM with sub-type of hello. |
| <i>join-prune</i> | PIM with sub-type of join/prune. |
| <i>none</i> | PIM with sub-type of none. |
| <i>register</i> | PIM with sub-type of register. |
| <i>register-stop</i> | PIM with sub-type of register stop. |
| <i>state-refresh</i> | PIM with sub-type of state refresh. |

Example

```
pim none
```

Syntax

```
l2tp
```

Mode

Service Object

Description

Set service object as l2tp.

Example

```
l2tp
```

Syntax

```
ipcomp
```

Mode

Service Object

Description

Set service object as ipcomp.

Example

```
ipcomp
```

Syntax

name <SVC_GROUP_NAME>

Mode

Service Group

Description

Set service group name.

Options

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

Example

name "Corporate Servers "

Syntax

uuid <UUID>

Mode

Service Group

Description

Set service group UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c

Syntax

no uuid

Mode

Service Group

Description

Clear service group UUID.

Example

no uuid

Syntax

no service-object <SVC_NAME>

Mode

Service Group

Description

Remove service object from group.

Options

<SVC_NAME> Service object name.
Example: *HTTPS*

Example

```
no service-object "Corp E-mail Server"
```

Syntax

```
service-object <SVC_NAME>
```

Mode

Service Group

Description

Assign service object to group.

Options

<SVC_NAME> Service object name.
Example: *HTTPS*

Example

```
service-object "Corp E-mail Server"
```

Syntax

```
no service-group <SVC_GROUP_NAME>
```

Mode

Service Group

Description

Remove service group from group.

Options

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

Example

```
no service-group "Corp Web Servers"
```

Syntax

```
service-group <SVC_GROUP_NAME>
```

Mode

Service Group

Description

Assign service group to group.

Options

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

Example

```
service-group "Corp Web Servers"
```

Syntax

```
zone [ uuid ] <ZONE_NAME>
```

Mode

Config

Description

Add/Edit a Zone.

Options

uuid Edit a zone by UUID.
<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
zone "Office Servers"
```

Syntax

```
no zone [ uuid ] <ZONE_NAME>
```

Mode

Config

Description

Delete a custom zone.

Options

uuid Delete a custom zone by UUID.
<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
no zone "Office Servers"
```

Syntax

```
no zones
```

Mode

Config

Description

Delete all custom zones.

Example

```
no zones
```

Syntax

guest-services

Mode

Zone

Description

Enable zone guest services and enter configuration mode.

Example

guest-services

Syntax

no guest-services

Mode

Zone

Description

Disable zone guest services.

Example

no guest-services

Syntax

wireless

Mode

Zone

Description

Enter wireless zone configuration mode.

Example

wireless

Syntax

uuid <UUID>

Mode

Zone

Description

Set zone object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

Zone

Description

Clear zone object UUID.

Example

```
no uuid
```

Syntax

```
name <ZONE_NAME>
```

Mode

Zone

Description

Set Zone Name.

Options

<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
name guest
```

Syntax

```
security-type { encrypted | management | public | sslvpn | trusted | untrusted | wireless }
```

Mode

Zone

Description

Set zone security type.

Options

encrypted VPN zone.

management Management zone.

public Public zone.

sslvpn SSLVPN zone.

trusted Trusted zone.

untrusted WAN/MULTICAST zone.

wireless Wireless zone.

Example

```
security-type public
```

Syntax

```
no security-type
```

Mode

Zone

Description

Disable zone security type.

Example

```
no security-type
```

Syntax

```
interface-trust
```

Mode

Zone

Description

Enable allow interface trust.

Example

```
interface-trust
```

Syntax

```
no interface-trust
```

Mode

Zone

Description

Disable allow interface trust.

Example

```
no interface-trust
```

Syntax

```
auto-generate-access-rules { allow-from-higher | allow-from-to-equal | allow-to-lower | deny-from-lower }
```

Mode

Zone

Description

Enable auto generate access rules.

Options

allow-from-higher Allow traffic from zones with higher trust level.

allow-from-to-equal Allow traffic between zones with the same trust level.

allow-to-lower Allow traffic to zones with lower trust level.

deny-from-lower Deny traffic from zones with lower trust level.

Example

```
auto-generate-access-rules allow-from-to-equal
```

Syntax

```
no auto-generate-access-rules { allow-from-higher | allow-from-to-equal | allow-to-lower | deny-from-lower }
```

Mode

Zone

Description

Disable auto generate access rules.

Options

allow-from-higher Allow traffic from zones with higher trust level.

allow-from-to-equal Allow traffic between zones with the same trust level.

allow-to-lower Allow traffic to zones with lower trust level.

deny-from-lower Deny traffic from zones with lower trust level.

Example

```
no auto-generate-access-rules allow-from-to-equal
```

Syntax

```
websense-content-filtering
```

Mode

Zone

Description

Enable enforce websense enterprise content filtering service.

Example

```
websense-content-filtering
```

Syntax

```
no websense-content-filtering
```

Mode

Zone

Description

Disable enforce websense enterprise content filtering service.

Example

```
no websense-content-filtering
```

Syntax

```
client { anti-virus | content-filtering }
```

Mode

Zone

Description

Enable client services.

Options

anti-virus Enable client anti-virus enforcement service.

content-filtering Enable client content filtering services enforcement service.

Example

```
client anti-virus
```

Syntax

```
no client { anti-virus | content-filtering }
```

Mode

Zone

Description

Disable client services.

Options

anti-virus Disable client anti-virus enforcement service.

content-filtering Disable client content filtering services enforcement service.

Example

```
no client anti-virus
```

Syntax

```
gateway-anti-virus
```

Mode

Zone

Description

Enable gateway anti-virus service.

Example

gateway-anti-virus

Syntax

no gateway-anti-virus

Mode

Zone

Description

Disable gateway anti-virus service.

Example

no gateway-anti-virus

Syntax

intrusion-prevention

Mode

Zone

Description

Enable intrusion prevention service.

Example

intrusion-prevention

Syntax

no intrusion-prevention

Mode

Zone

Description

Disable intrusion prevention service.

Example

no intrusion-prevention

Syntax

app-control

Mode

Zone

Description

Enable app control service.

Example

app-control

Syntax

no app-control

Mode

Zone

Description

Disable app control service.

Example

no app-control

Syntax

anti-spyware

Mode

Zone

Description

Enable Anti-Spyware Service.

Example

anti-spyware

Syntax

no anti-spyware

Mode

Zone

Description

Disable anti-spyware service.

Example

no anti-spyware

Syntax

create-group-vpn

Mode

Zone

Description

Enable automatic creation of group VPN for this zone.

Example

create-group-vpn

Syntax

no create-group-vpn

Mode

Zone

Description

Disable automatic creation of group VPN for this zone.

Example

no create-group-vpn

Syntax

ssl-control

Mode

Zone

Description

Enable SSL-Control on this zone.

Example

ssl-control

Syntax

no ssl-control

Mode

Zone

Description

Disable SSL-Control on this zone.

Example

no ssl-control

Syntax

dpi-ssl-client

Mode

Zone

Description

Enable SSL client inspection.

Example

dpi-ssl-client

Syntax

no dpi-ssl-client

Mode

Zone

Description

Disable SSL client inspection.

Example

no dpi-ssl-client

Syntax

dpi-ssl-server

Mode

Zone

Description

Enable SSL server inspection.

Example

dpi-ssl-server

Syntax

no dpi-ssl-server

Mode

Zone

Description

Disable SSL server inspection.

Example

no dpi-ssl-server

Syntax

sslvpn-access

Mode

Zone

Description

Enable SSL-VPN access for this zone.

Example

sslvpn-access

Syntax

no sslvpn-access

Mode

Zone

Description

Disable SSL-VPN access for this zone.

Example

```
no sslvpn-access
```

Syntax

```
inter-guest
```

Mode

Guest Services

Description

Enable inter-guest communication.

Example

```
inter-guest
```

Syntax

```
no inter-guest
```

Mode

Guest Services

Description

Disable inter-guest communication.

Example

```
no inter-guest
```

Syntax

```
bypass client { anti-virus | content-filtering }
```

Mode

Guest Services

Description

Enable bypass anti-virus check or client content filtering for guests.

Options

anti-virus Enable bypass anti-virus check for guests.

content-filtering Enable bypass client content filtering check for guests.

Example

```
bypass anti-virus
```

Syntax

```
no bypass client { anti-virus | content-filtering }
```

Mode

Guest Services

Description

Disable bypass anti-virus check or client content filtering for guests.

Options

anti-virus Disable bypass anti-virus check for guests.

content-filtering Disable bypass client content filtering check for guests.

Example

```
no bypass anti-virus
```

Syntax

```
external-auth
```

Mode

Guest Services

Description

Enable external guest authentication and enter its configuration mode.

Example

```
external-auth
```

Syntax

```
no external-auth
```

Mode

Guest Services

Description

Disable external guest authentication.

Example

```
no external-auth
```

Syntax

```
policy-page-non-authentication
```

Mode

Guest Services

Description

Enable policy page without authentication and enter its configuration mode.

Example

policy-page-non-authentication

Syntax

no policy-page-non-authentication

Mode

Guest Services

Description

Disable policy page without authentication.

Example

no policy-page-non-authentication

Syntax

client-redirect { http | https }

Mode

External Guest Authentication

Description

Set local web server settings for client redirect.

Options

http Set protocol HTTP.

https Set protocol HTTPS.

Example

client-redirect https

Syntax

web-server-1 protocol { http | https } { [ipv6] { fqdn <ADDR_FQDN> | host <ADDR_FQDNHOST_ADDR> | name <ADDR_FQDNHOST_ADDR_MIXED> } } [port <IPV4_PORT>]

Mode

External Guest Authentication

Description

Set the external web server 1 protocol.

Options

http Set protocol HTTP.

https Set protocol HTTPS.

ipv6 IPv6 address.

fqdn Address object full qualified domain name.

<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

host Configure the external web server IP addresses or hostname.

| | |
|---|--|
| <ADDR_FQDNHOST_ADDR> | FQDN/host address object name. Example: <i>Web Server</i> |
| name | Configure webserver to named address object. |
| <ADDR_FQDNHOST_ADDR_MIXED> | FQDN/host address object name. Example: <i>Web Server</i> |
| port | Configure the external web server port. |
| <IPV4_PORT> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
web-server-1 protocol https host 192.168.168.152 port 443
```

Syntax

```
web-server-2 protocol { http | https } { [ ipv6 ] { fqdn <ADDR_FQDN> | host <ADDR_FQDNHOST_ADDR> | name <ADDR_FQDNHOST_ADDR_MIXED> } } [ port <IPV4_PORT> ]
```

Mode

External Guest Authentication

Description

Set the external web server 2 protocol.

Options

| | |
|---|--|
| http | Set protocol HTTP. |
| https | Set protocol HTTPS. |
| ipv6 | IPv6 address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| host | Configure the external web server IP addresses or hostname. |
| <ADDR_FQDNHOST_ADDR> | FQDN/host address object name. Example: <i>Web Server</i> |
| name | Configure webserver to named address object. |
| <ADDR_FQDNHOST_ADDR_MIXED> | FQDN/host address object name. Example: <i>Web Server</i> |
| port | Configure the external web server port. |
| <IPV4_PORT> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
web-server-2 protocol https host 192.168.168.152 port 443
```

Syntax

```
no web-server-2
```

Mode

External Guest Authentication

Description

Disable the external web server 2.

Example

```
no web-server-2
```

Syntax

```
web-server timeout <UINT8>
```

Mode

External Guest Authentication

Description

Set the external web server connection timeout.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
web-server timeout 10
```

Syntax

```
message-auth [ method { md5 | sha1 | sha256 } ] [ shared-secret <WORD> confirm-secret <WORD> ]
```

Mode

External Guest Authentication

Description

Enable external message authentication.

Options

| | |
|--|--|
| method | Set external message authentication method. |
| md5 | Use HMAC - MD5 authentication. |
| sha1 | Use HMAC - SHA1 authentication. |
| sha256 | Use HMAC - SHA256 authentication. |
| shared-secret <WORD> | Set external message authentication shared secret. Word in the form: WORD or \"QUOTED STRING\". Example: abc |
| confirm-secret <WORD> | Confirm external message authentication shared secret. Word in the form: WORD or \"QUOTED STRING\". Example: abc |

Example

```
message-auth method md5 shared-secret donttell confirm-secret donttell
```

Syntax

```
no message-auth
```

Mode

External Guest Authentication

Description

Disable external message authentication.

Example

no message-auth

Syntax

social-network [facebook | google | twitter]

Mode

External Guest Authentication

Description

Enable specified social network login.

Options

facebook Enable Facebook social network login.

google Enable Google social network login.

twitter Enable Twitter social network login.

Example

social-network

Syntax

no social-network [facebook | google | twitter]

Mode

External Guest Authentication

Description

Disable social network login.

Options

facebook Disable Facebook social network login.

google Disable Google social network login.

twitter Disable Twitter social network login.

Example

no social-network

Syntax

wechat-qr-auth

Mode

External Guest Authentication

Description

Enable WeChat QR code authentication.

Example

wechat-qr-auth

Syntax

no wechat-qr-auth

Mode

External Guest Authentication

Description

Disable WeChat QR code authentication.

Example

no wechat-qr-auth

Syntax

only-qr-auth

Mode

External Guest Authentication

Description

Enable WeChat QR code authentication only.

Example

only-qr-auth

Syntax

no only-qr-auth

Mode

External Guest Authentication

Description

Disable WeChat QR code authentication only.

Example

no only-qr-auth

Syntax

qr-auth-page <WORD>

Mode

External Guest Authentication

Description

Set WeChat QR code authentication page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
qr-auth-page login.html
```

Syntax

```
no qr-auth-page
```

Mode

External Guest Authentication

Description

Clear WeChat QR code authentication page.

Example

```
no qr-auth-page
```

Syntax

```
auth-pages web-server-1 login <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 1 login page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-1 login login.html
```

Syntax

```
no auth-pages web-server-1 login
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 1 login page.

Example

```
no auth-pages web-server-1 login
```

Syntax

```
auth-pages web-server-1 expiration <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 1 session expiration page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-1 expiration exp.html
```

Syntax

```
no auth-pages web-server-1 expiration
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 1 session expiration page.

Example

```
no auth-pages web-server-1 expiration
```

Syntax

```
auth-pages web-server-1 timeout <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 1 idle timeout page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-1 timeout idle.html
```

Syntax

```
no auth-pages web-server-1 timeout
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 1 idle timeout page.

Example

```
no auth-pages web-server-1 timeout
```

Syntax

```
auth-pages web-server-1 max-sessions <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 1 max sessions page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-1 max-sessions max.html
```

Syntax

```
no auth-pages web-server-1 max-sessions
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 1 max sessions page.

Example

```
no auth-pages web-server-1 max-sessions
```

Syntax

```
auth-pages web-server-1 traffic-exceeded <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 1 traffic exceeded page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-1 traffic-exceeded trafficExceeded.html
```

Syntax

```
no auth-pages web-server-1 traffic-exceeded
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 1 traffic exceeded page.

Example

```
no auth-pages web-server-1 traffic-exceeded
```

Syntax

```
auth-pages web-server-2 login <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 2 login page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-2 login login.html
```

Syntax

```
no auth-pages web-server-2 login
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 2 login page.

Example

```
no auth-pages web-server-2 login
```

Syntax

```
auth-pages web-server-2 expiration <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 2 session expiration page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-2 expiration exp.html
```

Syntax

```
no auth-pages web-server-2 expiration
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 2 session expiration page.

Example

```
no auth-pages web-server-2 expiration
```

Syntax

```
auth-pages web-server-2 timeout <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 2 idle timeout page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-2 timeout idle.html
```

Syntax

```
no auth-pages web-server-2 timeout
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 2 idle timeout page.

Example

```
no auth-pages web-server-2 timeout
```

Syntax

```
auth-pages web-server-2 max-sessions <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 2 max sessions page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-2 max-sessions max.html
```

Syntax

```
no auth-pages web-server-2 max-sessions
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 2 max sessions page.

Example

```
no auth-pages web-server-2 max-sessions
```

Syntax

```
auth-pages web-server-2 traffic-exceeded <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 2 traffic exceeded page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-2 traffic-exceeded trafficExceeded.html
```

Syntax

```
no auth-pages web-server-2 traffic-exceeded
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 2 traffic exceeded page.

Example

```
no auth-pages web-server-2 traffic-exceeded
```

Syntax

```
web-content redirect { custom <WORD> | use-default }
```

Mode

External Guest Authentication

Description

Configure the Web content redirect message.

Options

custom Set a custom Web content redirect message.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

use-default Use the default Web content redirect message.

Example

```
web-content redirect custom "My custom redirect message"
```

Syntax

```
web-content server-down { custom <WORD> | use-default }
```

Mode

External Guest Authentication

Description

Configure the Web content redirect message.

Options

custom Set a custom Web content server down message.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

use-default Use the default Web content server down message.

Example

```
web-content server-down custom "My custom server down message"
```

Syntax

```
logout-expired { cgi { web-server-1 <WORD> | web-server-2 <WORD> } | every <UINT8> }
```

Mode

External Guest Authentication

Description

Enable auto-session logout.

Options

cgi Set logout CGI.

web-server-1 Set logout cgi of web server 1.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

web-server-2 Set logout cgi of web server 2.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

every Set auto-logout expired session every (minutes).
<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
logout-expired every 20
logout-expired cgi web-server-1 expired.cgi
logout-expired cgi web-server-2 expired.cgi
```

Syntax

```
no logout-expired [ cgi { web-server-1 | web-server-2 } ]
```

Mode

External Guest Authentication

Description

Disable auto-session logout.

Options

- cgi** Clear logout CGI.
- web-server-1** Clear logout cgi of web server 1.
- web-server-2** Clear logout cgi of web server 2.

Example

```
no logout-expired
```

Syntax

```
status-check { cgi { web-server-1 <WORD> | web-server-2 <WORD> } | every <UINT8> }
```

Mode

External Guest Authentication

Description

Enable server status check.

Options

- cgi** Set server status CGI.
- web-server-1** Set server status CGI of web server 1.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- web-server-2** Set server status CGI of web server 2.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- every** Set check server status every (minutes).
<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
status-check every 20
status-check cgi web-server-1 status.cgi
status-check cgi web-server-2 status.cgi
```

Syntax

```
no status-check [ cgi { web-server-1 | web-server-2 } ]
```

Mode

External Guest Authentication

Description

Disable server status check.

Options

- cgi** Set server status CGI.
- web-server-1** Set server status CGI of web server 1.
- web-server-2** Set server status CGI of web server 2.

Example

```
no status-check
```

Syntax

```
session-sync { cgi { web-server-1 <WORD> | web-server-2 <WORD> } | every <UINT8> }
```

Mode

External Guest Authentication

Description

Enable session synchronization.

Options

- cgi** Set session sync CGI.
- web-server-1** Set session sync CGI of web server 1.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- web-server-2** Set session sync CGI of web server 2.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- every** Set synchronize every (minutes).
<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
session-sync every 20  
session-sync cgi web-server-1 sync.cgi  
session-sync cgi web-server-2 sync.cgi
```

Syntax

```
no session-sync [ cgi { web-server-1 | web-server-2 } ]
```

Mode

External Guest Authentication

Description

Disable session synchronization.

Options

- cgi** Set session sync CGI.
- web-server-1** Set session sync CGI of web server 1.
- web-server-2** Set session sync CGI of web server 2.

Example

```
no session-sync
```

Syntax

```
guest-usage-policy <WORD>
```

Mode

Policy Page Without Authentication

Description

Set custom login page which may include HTML formatting.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
guest-usage-policy "Welcome to Sonicwall."
```

Syntax

```
no guest-usage-policy
```

Mode

Policy Page Without Authentication

Description

Clear custom login page.

Example

```
no guest-usage-policy
```

Syntax

```
idle-timeout <UINT32> unit { days | hours | minutes | seconds }
```

Mode

Policy Page Without Authentication

Description

Set idle timeout for custom guest policy page.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

unit Set the idle timeout in seconds.

days Set the idle timeout in days.

hours Set the idle timeout in hours.

minutes Set the idle timeout in minutes.

seconds Set the idle timeout in seconds.

Example

```
idle-timeout 15 unit minutes
```

Syntax

```
custom-auth-page
```

Mode

Guest Services

Description

Enable custom authentication page and enter its configuration mode.

Example

```
custom-auth-page
```

Syntax

```
no custom-auth-page
```

Mode

Guest Services

Description

Disable custom authentication page.

Example

```
no custom-auth-page
```

Syntax

```
post-auth <WEB_URL>
```

Mode

Guest Services

Description

Enable page to direct users to after successful authentication.

Options

<WEB_URL> URL in the form: http://host/file.
Example: `http://www.example.com/products/`

Example

```
post-auth http://192.168.168.1/postauth.html
```

Syntax

```
no post-auth
```

Mode

Guest Services

Description

Disable page to direct users to after successful authentication.

Example

```
no post-auth
```

Syntax

```
bypass-guest-auth { all | group <ADDR_MAC_GROUP> | mac <ADDR_MAC> | name <ADDR_MAC_NAME> }
```

Mode

Guest Services

Description

Enable bypass guest authentication.

Options

| | |
|-------------------------------|---|
| all | All MAC addresses. |
| group | Address group name. |
| <ADDR_MAC_GROUP> | MAC group address object name. Example: <i>Sales & Marketing Network Access Points</i> |
| mac | MAC address. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | MAC address object name. |
| <ADDR_MAC_NAME> | MAC address object name. Example: <i>Sales Network Access Point</i> |

Example

```
bypass-guest-auth mac 020102030405
```

Syntax

```
no bypass-guest-auth
```

Mode

Guest Services

Description

Disable bypass guest authentication.

Example

```
no bypass-guest-auth
```

Syntax

```
smtp-redirect { host <ADDR_HOST> | name <ADDR_HOST_NAME> }
```

Mode

Guest Services

Description

Enable redirect SMTP traffic to specified server.

Options

host Set the SMTP server to host address.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Set the SMTP server as named address object.
<ADDR_HOST_NAME> Host address object name.
 Example: *Web Server*

Example

```
smtp-redirect host 192.168.168.152
```

Syntax

```
no smtp-redirect
```

Mode

Guest Services

Description

Disable redirect SMTP traffic.

Example

```
no smtp-redirect
```

Syntax

```
deny-networks { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Guest Services

Description

Enable blocking of traffic to the named network.

Options

ipv6 IPv6 address object.

host Set the denied networks to host address.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

network Set the denied networks to network address.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
 Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Set the denied networks to range of addresses.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

fqdn Address object full qualified domain name.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.

Example: *example.com*

group Set the denied networks as named address group.

<ADDR_GROUP_NAME_MIXED> Group address object name.
Example: *Sales Group*

mac Set the denied networks to MAC address.

<ADDR_MAC> Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.

name Set the denied networks as named address object.

<ADDR_NAME_MIXED> Address object name.
Example: *Web Server*

Example

```
deny-networks network 192.168.168.0 255.255.255.0
```

Syntax

```
no deny-networks
```

Mode

Guest Services

Description

Disable blocking of traffic to the named network.

Example

```
no deny-networks
```

Syntax

```
pass-networks { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Guest Services

Description

Enable allowing of traffic to the named network.

Options

ipv6 IPv6 address object.

host Set the pass networks to host address.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

network Set the pass networks to network address.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Set the pass networks to range of addresses.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

| | |
|--------------------------------------|---|
| <i>fqdn</i> | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| <i>group</i> | Set the pass networks as named address group. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| <i>mac</i> | Set the pass networks to MAC address. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| <i>name</i> | Set the pass networks as named address object. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
pass-networks network 192.168.168.0 255.255.255.0
```

Syntax

```
no pass-networks
```

Mode

Guest Services

Description

Disable allowing of traffic to the named network.

Example

```
no pass-networks
```

Syntax

```
max-guests <UINT16>
```

Mode

Guest Services

Description

Specify the maximum number of guest users allowed to connect to the WLAN zone.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
max-guests 10
```

Syntax

```
dynamic-address-translation
```

Mode

Guest Services

Description

Enable dynamic address translation.

Example

```
dynamic-address-translation
```

Syntax

```
no dynamic-address-translation
```

Mode

Guest Services

Description

Disable dynamic address translation.

Example

```
no dynamic-address-translation
```

Syntax

```
footer { text <WORD> | url <WEB_URL> }
```

Mode

Custom Authentication Page

Description

Configure custom login page footer.

Options

| | |
|------------------------|--|
| text | Use configured text for custom login page footer. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| url | Use configured url location for custom page footer. |
| <WEB_URL> | URL in the form: http://host/file. Example: <i>http://www.example.com/products/</i> |

Example

```
footer url http://192.168.168.1/footer.html
```

Syntax

```
header { text <WORD> | url <WEB_URL> }
```

Mode

Custom Authentication Page

Description

Configure custom login page header.

Options

| | |
|---------------------|---|
| text | Use configured text for custom login page header. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

url Use configured url location for custom login page header.
<WEB_URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

```
header url http://192.168.168.1/header.html
```

Syntax

```
sslvpn-enforcement server { host <ADDR_HOST> | name <ADDR_HOST_NAME> } service { name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

Wireless

Description

Enable SSLVPN enforcement.

Options

| | |
|-------------------------------|---|
| server | Set the SSLVPN server as a named address object. |
| host | Set the SSLVPN server to host address. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Set the SSLVPN server as named address object. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| service | Set the SSLVPN service as a named service object. |
| name | Set the SSLVPN service as named service object. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Set the SSLVPN service as a protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
sslvpn-enforcement server name "SSLVPN Server" service name "SSLVPN Service"
```

Syntax

```
no sslvpn-enforcement
```

Mode

Wireless

Description

Disable SSLVPN enforcement.

Example

```
no sslvpn-enforcement
```

Syntax

```
wifi-sec-enforcement [ exception-service { name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } ]
```

Mode

Wireless

Description

Enable WiFiSec enforcement.

Options

exception-service Specify services that are allowed to bypass wifisec enforcement.

name Name of service object for the exception service.
<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Set the WiFiSec exception service as a protocol.
<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
wifi-sec-enforcement  
wifi-sec-enforcement service name "SSLVPN Service"
```

Syntax

```
no wifi-sec-enforcement [ exception-service ]
```

Mode

Wireless

Description

Disable WiFiSec enforcement.

Options

exception-service Disable WiFiSec enforcement exception service.

Example

```
no wifi-sec-enforcement
```

Syntax

```
wifi-sec-for-site-to-site-vpn
```

Mode

Wireless

Description

Enable WiFiSec for site-to-site VPN tunnel traversal.

Example

```
wifi-sec-for-site-to-site-vpn
```

Syntax

```
no wifi-sec-for-site-to-site-vpn
```

Mode

Wireless

Description

Disable WiFiSec for site-to-site VPN tunnel traversal.

Example

```
no wifi-sec-for-site-to-site-vpn
```

Syntax

```
trust-wpa-traffic-as-wifi-sec
```

Mode

Wireless

Description

Trust WPA / WPA2 traffic as WiFiSec.

Example

```
trust-wpa-traffic-as-wifi-sec
```

Syntax

```
no trust-wpa-traffic-as-wifi-sec
```

Mode

Wireless

Description

Disable trust WPA / WPA2 traffic as WiFiSec.

Example

```
no trust-wpa-traffic-as-wifi-sec
```

Syntax

```
sonicpoint profile { ac | n | ndr | wave2 } { auto-provisioning | profile-name <SONICPOINT_N_PROFILE_NAME> }
```

Mode

Wireless

Description

Set the sonicpoint provisioning profile.

Options

ac SonicPoint ACe/ACi/N2/W2.

n SonicPoint N.

ndr SonicPoint NDR.

| | |
|--|--|
| wave2 | SonicPoint ACWave2. |
| auto-provisioning | Enable auto provisioning sonicpoint profile. |
| profile-name | SonicPoint profile name. |
| <SONICPOINT_N_PROFILE_NAME> | SonicPointN provisioning profile name. Example: <i>mySonicpointnProfile</i> |

Example

```
sonicpoint profile n profile-name "Public SonicPointNs"
sonicpoint profile n auto-provisioning
```

Syntax

```
no sonicpoint profile { ac | n | ndr | wave2 } auto-provisioning
```

Mode

Wireless

Description

Disable auto provisioning sonicpoint profile.

Options

| | |
|--------------------------|---|
| ac | SonicPoint ACe/ACi/N2/W2. |
| n | SonicPoint N. |
| ndr | SonicPoint NDR. |
| wave2 | SonicPoint ACWave2. |
| auto-provisioning | Disable auto provisioning sonicpoint profile. |

Example

```
no sonicpoint profile n auto-provisioning
```

Syntax

```
bypass-gateway-firewalling
```

Mode

Wireless

Description

Enforce local wireless zone traffic to bypass gateway firewalling.

Example

```
bypass-gateway-firewalling
```

Syntax

```
no bypass-gateway-firewalling
```

Mode

Wireless

Description

Disable local wireless zone traffic to bypass gateway firewalling.

Example

```
no bypass-gateway-firewalling
```

Syntax

```
only-sonicpoint-traffic
```

Mode

Wireless

Description

Enable only allow traffic generated by a SonicPoint/SonicPointN.

Example

```
only-sonicpoint-traffic
```

Syntax

```
no only-sonicpoint-traffic
```

Mode

Wireless

Description

Disable only allow traffic generated by a SonicPoint/SonicPointN.

Example

```
no only-sonicpoint-traffic
```

Syntax

```
auto-channel-limitation
```

Mode

Wireless

Description

Enable prefer SonicPoint/SonicWave 2.4GHz auto channel selection to be 1, 6 and 11 only.

Example

```
auto-channel-limitation
```

Syntax

```
no auto-channel-limitation
```

Mode

Wireless

Description

Disable prefer SonicPoint/SonicWave 2.4GHz auto channel selection to be 1, 6 and 11 only.

Example

```
no auto-channel-limitation
```

Syntax

```
sonicwave-online-registration
```

Mode

Wireless

Description

Enable enforce SonicWave license activation from secure trusted license manager.

Example

```
sonicpoint-management
```

Syntax

```
no sonicwave-online-registration
```

Mode

Wireless

Description

Disable enforce SonicWave license activation from secure trusted license manager.

Example

```
no sonicwave-online-registration
```

Syntax

```
sonicpoint-management
```

Mode

Wireless

Description

Enable SonicPoint/SonicWave management.

Example

```
sonicpoint-management
```

Syntax

```
no sonicpoint-management
```

Mode

Wireless

Description

Disable SonicPoint/SonicWave management.

Example

```
no sonicpoint-management
```

Syntax

```
local-radius-server
```

Mode

Zone

Description

Enable zone local radius server and enter configuration mode.

Example

```
local-radius-server
```

Syntax

```
no local-radius-server
```

Mode

Zone

Description

Disable zone local radius server.

Example

```
no local-radius-server
```

Syntax

```
interface-server-numbers <UINT16>
```

Mode

Radius Server

Description

Specify the interface server numbers.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
interface-server-numbers 8
```

Syntax

```
port <UINT32>
```

Mode

Radius Server

Description

Set radius server port.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
port 1812
```

Syntax

```
client-password <ENC_PASSWORD>
```

Mode

Radius Server

Description

Set radius client password.

Options

<ENC_PASSWORD> Password.
Example: secret

Example

```
client-password mywpapassphrase
```

Syntax

```
tls-cache
```

Mode

Radius Server

Description

Enable local radius server tls cache.

Example

```
tls-cache
```

Syntax

```
no tls-cache
```

Mode

Radius Server

Description

Disable local radius server tls cache.

Example

```
no tls-cache
```

Syntax

```
tls-cache-lifetime <UINT8>
```

Mode

Radius Server

Description

Specify the radius server tls cache lifetime(h).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
tls-cache-lifetime 1
```

Syntax

```
ldap-server
```

Mode

Radius Server

Description

Enable zone ldap server and enter configuration mode.

Example

```
ldap-server
```

Syntax

```
no ldap-server
```

Mode

Radius Server

Description

Disable zone ldap server.

Example

```
no ldap-server
```

Syntax

```
server <HOSTNAME>
```

Mode

LDAP Server

Description

Specify the ldap server name or ip.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

server 192.168.168.1

Syntax

no server

Mode

LDAP Server

Description

Clear the ldap server name or ip.

Example

no server

Syntax

base-dn <WORD>

Mode

LDAP Server

Description

Specify the ldap server base dn.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

base-dn "ou=radius,dc=sonicwall,dc=com"

Syntax

no base-dn

Mode

LDAP Server

Description

Clear the ldap server base dn.

Example

no base-dn

Syntax

identity-dn <WORD>

Mode

LDAP Server

Description

Specify the ldap server identity dn.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
identity-dn "cn=snwlradius,ou=admins,ou=radius,dc=sonicwall,dc=com"
```

Syntax

```
no identity-dn
```

Mode

LDAP Server

Description

Clear the ldap server identity dn.

Example

```
no identity-dn
```

Syntax

```
identity-dn-password <ENC_PASSWORD>
```

Mode

LDAP Server

Description

Set ldap identity dn password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
identity-dn-password mypassphrase
```

Syntax

```
no identity-dn-password
```

Mode

LDAP Server

Description

Clear ldap identity dn password.

Example

```
no identity-dn-password
```

Syntax

```
tls
```

Mode

LDAP Server

Description

Enable ldap server tls.

Example

```
tls
```

Syntax

```
no tls
```

Mode

LDAP Server

Description

Disable ldap server tls.

Example

```
no tls
```

Syntax

```
cache
```

Mode

LDAP Server

Description

Enable ldap cache.

Example

```
cache
```

Syntax

```
no cache
```

Mode

LDAP Server

Description

Disable ldap server cache.

Example

```
no cache
```

Syntax

```
cache-lifetime <UINT32>
```

Mode

LDAP Server

Description

Specify the ldap server cache lifetime(s).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
cache-lifetime 86400
```

Syntax

```
active-directory-server
```

Mode

Radius Server

Description

Enable zone active directory server and enter configuration mode.

Example

```
active-directory-server
```

Syntax

```
no active-directory-server
```

Mode

Radius Server

Description

Disable zone active directory server.

Example

```
no active-directory-server
```

Syntax

```
domain <HOSTNAME>
```

Mode

Active Directory Server

Description

Specify the active directory server domain.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
domain wirelessdev
```

Syntax

no domain

Mode

Active Directory Server

Description

Clear the active directory server domain.

Example

no domain

Syntax

full-name <WORD>

Mode

Active Directory Server

Description

Specify the active directory server full name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

full-name wirelessdev.com

Syntax

no full-name

Mode

Active Directory Server

Description

Clear the active directory server full name.

Example

no domain

Syntax

admin-user-name <WORD>

Mode

Active Directory Server

Description

Specify the active directory server admin user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
admin-user-name wirelessDev
```

Syntax

```
no admin-user-name
```

Mode

Active Directory Server

Description

Clear the active directory server admin user name.

Example

```
no admin-user-name
```

Syntax

```
admin-user-password <ENC_PASSWORD>
```

Mode

Active Directory Server

Description

Set active directory server admin user password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
admin-user-password mypassphrase
```

Syntax

```
no admin-user-password
```

Mode

Active Directory Server

Description

Clear active directory server admin user password.

Example

```
no admin-user-password
```

Syntax

```
show address-objects [ fqdn | ipv4 [ { host | network | range } ] | ipv6 [ { host | network | range } ] | mac ] [ { custom | default } ] [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show all address objects.

Options

| | |
|----------------------------|---|
| <i>fqdn</i> | Show FQDN address objects. |
| <i>ipv4</i> | Show only IPv4 address objects. |
| <i>host</i> | Show host address objects. |
| <i>network</i> | Show network address objects. |
| <i>range</i> | Show range address objects. |
| <i>ipv6</i> | Show only IPv6 address objects. |
| <i>host</i> | Show host address objects. |
| <i>network</i> | Show network address objects. |
| <i>range</i> | Show range address objects. |
| <i>mac</i> | Show MAC address objects. |
| <i>custom</i> | Show custom configuration. |
| <i>default</i> | Show system/factory default configuration. |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |
| <i>status</i> | Show address object status. |

Example

```
show address-objects
```

Syntax

```
show address-object ipv4 [ uuid ] <ADDR_HOST_NETWORK_RANGE_NAME> [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show an IPv4 address object.

Options

| | |
|---|---|
| <i>uuid</i> | Show an IPv4 address object by UUID. |
| <i><ADDR_HOST_NETWORK_RANGE_NAME></i> | Host/network/range address object name. Example: <i>Web Server</i> |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |
| <i>status</i> | Show address object status. |

Example

```
show address-object ipv4 "X0 IP"
```

Syntax

```
show address-object ipv6 [ uuid ] <ADDR_HOST_NETWORK_RANGE_NAME> [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show an IPv6 address object.

Options

| | |
|---|---|
| uuid | Show an IPv6 address object by UUID. |
| <ADDR_HOST_NETWORK_RANGE_NAME> | Host/network/range address object name. Example: <i>Web Server</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| status | Show address object status. |

Example

```
show address-object ipv6 "X0 IPv6 Link-Local Address"
```

Syntax

```
show address-object mac [ uuid ] <ADDR_MAC_NAME> [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show a MAC address object.

Options

| | |
|------------------------------|---|
| uuid | Show a MAC address object by UUID. |
| <ADDR_MAC_NAME> | MAC address object name. Example: <i>Sales Network Access Point</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| status | Show address object status. |

Example

```
show address-object mac "Web Server MAC"
```

Syntax

```
show address-object fqdn [ uuid ] <ADDR_FQDN_NAME> [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show a FQDN address object.

Options

| | |
|-------------------------------|--------------------------------------|
| uuid | Show an FQDN address object by UUID. |
| <ADDR_FQDN_NAME> | FQDN address object name. |

Example: *www.example.com*

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.
- status*** Show address object status.

Example

```
show address-object fqdn "Web Server FQDN"
```

Syntax

```
show address-groups [ ipv4 | ipv6 ] [ { custom | default } ] [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show all address groups.

Options

- ipv4*** Show only IPv4 address groups.
- ipv6*** Show only IPv6 address groups.
- custom*** Show custom configuration.
- default*** Show system/factory default configuration.
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.
- status*** Show address group status.

Example

```
show address-groups
```

Syntax

```
show address-group ipv4 [ uuid ] <ADDR_GROUP_NAME> [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show an address group.

Options

- uuid*** Show an IPv4 address group by UUID.
- <ADDR_GROUP_NAME>** Group address object name.
Example: *Sales Group*
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.
- status*** Show address group status.

Example

```
show address-group ipv4 "LAN Subnets"
```

Syntax

```
show address-group ipv6 [ uuid ] <ADDR_GROUP_NAME> [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show an address group.

Options

| | |
|--------------------------------|---|
| uuid | Show an IPv6 address group by UUID. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| status | Show address group status. |

Example

```
show address-group ipv6 "DMZ IPv6 Subnets"
```

Syntax

```
show schedules [ all | mixed | once | recurring ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all Schedule Objects.

Options

| | |
|----------------------------|--|
| all | Show all Schedule Objects. |
| mixed | Show all Schedule Objects set for both recurring schedule and single occurrence. |
| once | Show all Schedule Objects set for single occurrence. |
| recurring | Show all Schedule Objects set for recurring. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show schedules
```

Syntax

```
show schedule [ uuid ] <SCHED_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show a Schedule Object.

Options

| | |
|----------------------------|---|
| uuid | Show a schedule object by UUID. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show schedule "Work Hours"
```

Syntax

```
show service-objects [ 6over4 | ah | eigrp | esp | gre | icmp | icmpv6 | igmp | l2tp | ospf | pim | tcp | udp ] [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show all service objects.

Options

| | |
|----------------------------|---|
| 6over4 | Show 6over4 service objects. |
| ah | Show AH service objects. |
| eigrp | Show EIGRP service objects. |
| esp | Show ESP service objects. |
| gre | Show GRE service objects. |
| icmp | Show ICMP service objects. |
| icmpv6 | Show ICMPV6 service objects. |
| igmp | Show IGMP service objects. |
| l2tp | Show l2tp service objects. |
| ospf | Show OSPF service objects. |
| pim | Show PIM service objects. |
| tcp | Show TCP service objects. |
| udp | Show UDP service objects. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| status | Show service object status. |

Example

show service-objects

Syntax

```
show service-object [ uuid ] <SVC_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show service object.

Options

- uuid** Show a service object by UUID.
- <SVC_NAME>** Service object name.
Example: *HTTPS*
- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.

Example

```
show service-object "Corp Servers"
```

Syntax

```
show service-groups [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show all service groups.

Options

- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.
- status** Show service group status.

Example

```
show service-groups
```

Syntax

```
show service-group [ uuid ] <SVC_GROUP_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show service group.

Options

- uuid** Show a service group by UUID.

- <SVC_GROUP_NAME>** Service object group name.
Example: *VOIP*
- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.

Example

```
show service-group "Citrix"
```

Syntax

```
show zones [ status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all Zone Objects.

Options

- status** Show zones status.
- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.

Example

```
show zones
```

Syntax

```
show zone [ uuid ] <ZONE_NAME> [ status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show a Zone Object.

Options

- uuid** Show a zone object by UUID.
- <ZONE_NAME>** Zone object name.
Example: *DMZ*
- status** Show zone status.
- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.

Example

```
show zone "LAN"
```

Syntax

```
clear interface [ ipv4 | ipv6 ] statistics
```

Mode

All Modes
Top Level

Description

Reset interface statistics.

Options

ipv4 Reset interface IPv4 statistics.

ipv6 Reset interface IPv6 statistics.

statistics Reset interface statistics.

Example

```
clear interface statistics
```

Syntax

```
interfaces display-all-traffic
```

Mode

Config

Description

Enable display all traffic.

Example

```
interfaces display-all-traffic
```

Syntax

```
no interfaces display-all-traffic
```

Mode

Config

Description

Disable display all traffic.

Example

```
no interfaces display-all-traffic
```

Syntax

```
shutdown <CONFIGURABLE_INTERFACE>
```

Mode

Config

Description

Shutdown specified port.

Options

<CONFIGURABLE_INTERFACE> Interface name.
Example: X0

Example

```
shutdown X2
```

Syntax

```
no shutdown <CONFIGURABLE_INTERFACE>
```

Mode

Config

Description

Enable specified port.

Options

<CONFIGURABLE_INTERFACE> Interface name.
Example: X0

Example

```
no shutdown X2
```

Syntax

```
interface [ ipv6 ] <CONFIGURABLE_INTERFACE> [ vlan <VLAN_TAG> ] [ tunnel <WLAN_TUNNEL_ID> ]
```

Mode

Config

Description

Configure interface or add/edit sub-interface or WLAN tunnel interface.

Options

ipv6 Configure interface IPv6 parameters.
<CONFIGURABLE_INTERFACE> Interface name.
Example: X0

vlan Configure VLAN sub-interface.
<VLAN_TAG> VLAN tag.
Example: 23

tunnel Configure WLAN tunnel interface.
<WLAN_TUNNEL_ID> WLAN tunnel ID.
Example: 1

Example

```
interface X1
interface X1 vlan 100
interface WT0
interface X1 tunnel 1
interface X1 vlan 100 tunnel 2
interface WT1 vlan 200
interface ipv6 X1
interface ipv6 X1 vlan 100
interface ipv6 WT0
interface ipv6 X1 tunnel 1
interface ipv6 X1 vlan 100 tunnel 2
interface ipv6 WT1 vlan 200
```

Syntax

```
no interface <CONFIGURABLE_INTERFACE> [ vlan <VLAN_TAG> ] [ tunnel <WLAN_TUNNEL_ID> ]
```

Mode

Config

Description

Delete sub-interface or WLAN tunnel interface.

Options

| | |
|---------------------------------------|---------------------------------------|
| <CONFIGURABLE_INTERFACE> | Interface name. Example: <i>X0</i> |
| vlan | Delete VLAN sub-interface. |
| <VLAN_TAG> | VLAN tag. Example: <i>23</i> |
| tunnel | Delete WLAN tunnel interface. |
| <WLAN_TUNNEL_ID> | WLAN tunnel ID. Example: <i>1</i> |

Example

```
no interface X1 vlan 101
no interface WT0
no interface WT1 vlan 100
no interface X1 tunnel 1
no interface X1 vlan 101 tunnel 2
```

Syntax

```
tunnel-interface 4to6 <TUNNEL6_TUNNEL_INTERFACE>
```

Mode

Config

Description

Add/edit 4to6 tunnel interface.

Options

| | |
|---|--|
| <TUNNEL6_TUNNEL_INTERFACE> | Tunnel6 tunnel interface name. Example: <i>tunnel6TunnelInterface</i> |
|---|--|

Example

```
tunnel-interface 4to6 CorpTunnel6Tunnel
```

Syntax

```
no tunnel-interface 4to6 <TUNNEL6_TUNNEL_INTERFACE>
```

Mode

Config

Description

Delete 4to6 tunnel interface.

Options

| | |
|---|--|
| <TUNNEL6_TUNNEL_INTERFACE> | Tunnel6 tunnel interface name. Example: <i>tunnel6TunnelInterface</i> |
|---|--|

Example

```
no tunnel-interface 4to6 CorpTunnel6Tunnel
```

Syntax

name <TUNNEL6_TUNNEL_INTERFACE>

Mode

Tunnel6 Tunnel Interface

Description

Set 4to6 tunnel interface name.

Options

<TUNNEL6_TUNNEL_INTERFACE> Tunnel6 tunnel interface name.
Example: *tunnel6TunnelInterface*

Example

name 4to6Tunnel

Syntax

comment <WORD>

Mode

Tunnel6 Tunnel Interface

Description

Set 4to6 tunnel interface comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Tunnel6 tunnel to Corporate"

Syntax

no comment

Mode

Tunnel6 Tunnel Interface

Description

Clear tunnel interface comment.

Example

no comment

Syntax

flow-reporting

Mode

Tunnel6 Tunnel Interface

Description

Enable flow reporting on the interface.

Example

flow-reporting

Syntax

no flow-reporting

Mode

Tunnel6 Tunnel Interface

Description

Disable flow reporting on the interface.

Example

no flow-reporting

Syntax

send-icmp-fragmentation

Mode

Tunnel6 Tunnel Interface

Description

Enable send ICMP Fragmentation Needed for outbound packets over the Interface MTU.

Example

send-icmp-fragmentation

Syntax

no send-icmp-fragmentation

Mode

Tunnel6 Tunnel Interface

Description

Disable ICMP fragmentation needed message generation.

Example

no send-icmp-fragmentation

Syntax

fragment-packets

Mode

Tunnel6 Tunnel Interface

Description

Enable fragment non-VPN outbound packets larger than this interface's MTU.

Example

fragment-packets

Syntax

no fragment-packets

Mode

Tunnel6 Tunnel Interface

Description

Disable fragment non-VPN outbound packets larger than this interface's MTU.

Example

no fragment-packets

Syntax

ignore-df-bit

Mode

Tunnel6 Tunnel Interface

Description

Enable ignore don't fragment (DF) bit.

Example

ignore-df-bit

Syntax

no ignore-df-bit

Mode

Tunnel6 Tunnel Interface

Description

Disable ignore don't fragment (DF) bit.

Example

no ignore-df-bit

Syntax

type { dslite | gre4to6 }

Mode

Tunnel6 Tunnel Interface

Description

Set the tunnel interface tunnel6 type.

Options

dslite Dslite tunnel.

gre4to6 gre4to6 tunnel.

Example

```
type dslite
```

Syntax

```
bound-to interface <TUNNEL6_TUNNEL_BOUND_TO_INTERFACE>
```

Mode

dslite Tunnel Interface

Description

Set dslite software tunnel interface bound to.

Options

<TUNNEL6_TUNNEL_BOUND_TO_INTERFACE> Interface name.
Example: X0

Example

```
bound-to interface X1
```

Syntax

```
no bound-to
```

Mode

dslite Tunnel Interface

Description

Clear dslite software tunnel interface bound to.

Example

```
no bound-to
```

Syntax

```
bound-to interface <TUNNEL6_TUNNEL_BOUND_TO_INTERFACE>
```

Mode

6to4 Tunnel Interface

Description

Set gre4to6 tunnel interface bound to.

Options

<TUNNEL6_TUNNEL_BOUND_TO_INTERFACE> Interface name.
Example: X0

Example

```
bound to interface X1
```

Syntax

```
no bound-to
```

Mode

6to4 Tunnel Interface

Description

Clear gre4to6 tunnel interface bound to.

Example

```
no bound-to
```

Syntax

```
local { dynamic | ipv6 <IPV6_HOST> }
```

Mode

dslite Tunnel Interface

Description

Set dslite tunnel interface local IPv6 address.

Options

- dynamic** Set dslite tunnel interface primary local IPv6 address.
- ipv6** Set dslite tunnel interface static local IPv6 address.
- <IPV6_HOST>** IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
local ipv6 1030::C9B4:FF12:48AA:1A2B
```

Syntax

```
remote { dynamic | fqdn <WORD> | ipv6 <IPV6_HOST> }
```

Mode

dslite Tunnel Interface

Description

Set dslite tunnel interface remote IPv6 address.

Options

- dynamic** Set dslite tunnel interface remote IPv6 address via DHCP.
- fqdn** Set dslite tunnel interface static remote IPv6 address via FQDN
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: abc
- ipv6** Set dslite tunnel interface static remote IPv6 address.
- <IPV6_HOST>** IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
remote ipv6 1030::C9B4:FF12:48AA:1A2B
```

Syntax

```
local-ipv4 <IPV4_HOST>
```

Mode

dslite Tunnel Interface

Description

Set dslite tunnel interface local IPv4 address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
local-ipv4 10.10.10.10
```

Syntax

```
no local-ipv4
```

Mode

dslite Tunnel Interface

Description

Clear dslite tunnel interface local IPv4 address.

Example

```
no local-ipv4
```

Syntax

```
remote ipv6 <IPV6_HOST>
```

Mode

6to4 Tunnel Interface

Description

Set gre4to6 tunnel interface remote IPv6 address.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
remote 1030::C9B4:FF12:48AA:1A2B
```

Syntax

```
no remote
```

Mode

6to4 Tunnel Interface

Description

Clear gre4to6 tunnel interface remote IPv6 address.

Example

```
no remote
```

Syntax

```
local { dynamic | ipv6 <IPV6_HOST> }
```

Mode

6to4 Tunnel Interface

Description

Set gre4to6 tunnel interface local IPv6 address.

Options

- dynamic** Set gre4to6 tunnel interface primary local IPv6 address.
- ipv6** Set gre4to6 tunnel interface static local IPv6 address.
- <IPV6_HOST>** IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
local ip 1030::C9B4:FF12:48AA:1A2B
```

Syntax

```
ip <IPV4_HOST> [ netmask <IPV4_MASK> ]
```

Mode

6to4 Tunnel Interface

Description

Set gre4to6 tunnel interface IP address.

Options

- <IPV4_HOST>** IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168
- netmask** Set interface netmask.
- <IPV4_MASK>** IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: 255.255.255.0

Example

```
ip 10.10.10.10 netmask 255.255.255.0
```

Syntax

```
no ip
```

Mode

6to4 Tunnel Interface

Description

Clear gre4to6 tunnel interface IP address.

Example

```
no ip
```

Syntax

```
tunnel-interface vpn <VPN_TUNNEL_INTERFACE>
```

Mode

Config

Description

Add/edit VPN tunnel interface.

Options

<VPN_TUNNEL_INTERFACE> VPN tunnel interface name.
Example: *vpnTunnelInterface*

Example

```
tunnel-interface vpn CorpVPNTunnel
```

Syntax

```
no tunnel-interface vpn <VPN_TUNNEL_INTERFACE>
```

Mode

Config

Description

Delete VPN tunnel interface.

Options

<VPN_TUNNEL_INTERFACE> VPN tunnel interface name.
Example: *vpnTunnelInterface*

Example

```
no tunnel-interface vpn CorpVPNTunnel
```

Syntax

```
policy <VPN_TUNNEL_POLICY_NAME>
```

Mode

Tunnel Interface VPN

Description

Set tunnel interface VPN policy.

Options

<VPN_TUNNEL_POLICY_NAME> Tunnel interface VPN policy name.
Example: *Remote Office*

Example

```
policy "Remote Office"
```

Syntax

```
renew [ ipv6 ] <DHCP_INTERFACE>
```

Mode

Config

Description

Renew interface DHCP lease.

Options

| | |
|-------------------------------|--------------------------------|
| ipv6 | Renew interface DHCPv6 lease. |
| <DHCP_INTERFACE> | Interface name. Example: X0 |

Example

```
renew X5
```

Syntax

```
release [ ipv6 ] <DHCP_INTERFACE>
```

Mode

Config

Description

Release designated interface DHCP lease.

Options

| | |
|-------------------------------|---------------------------------|
| ipv6 | Release interface DHCPv6 lease. |
| <DHCP_INTERFACE> | Interface name. Example: X0 |

Example

```
release X5
```

Syntax

```
connect <CONNECT_INTERFACE>
```

Mode

Config

Description

Connect designated interface to PPTP/L2TP/PPPoE server.

Options

| | |
|----------------------------------|--------------------------------|
| <CONNECT_INTERFACE> | Interface name. Example: X0 |
|----------------------------------|--------------------------------|

Example

```
connect X5
```

Syntax

```
disconnect <CONNECT_INTERFACE>
```

Mode

Config

Description

Disconnect designated interface from PPTP/L2TP/PPPoE server.

Options

<CONNECT_INTERFACE> Interface name.
Example: *X0*

Example

```
disconnect X5
```

Syntax

```
link-speed { auto-negotiate | full { { 10 | 100 | 1000 | 10000 | 2500 | 5000 } } | half { { 10 | 100 } } }
```

Mode

Interface

Description

Set interface link speed.

Options

auto-negotiate Set interface link speed to auto-negotiate.

full Full duplex.

10 Set interface link speed to 10 Mbps-full duplex.

100 Set interface link speed to 100 Mbps-full duplex.

1000 Set interface link speed to 1000 Mbps-full duplex.

10000 Set interface link speed to 10 Gbps(10000 Mbps)-full duplex.

2500 Set interface link speed to 2500 Mbps-full duplex.

5000 Set interface link speed to 5000 Mbps-full duplex.

half Half duplex.

10 Set interface link speed to 10 Mbps-half duplex.

100 Set interface link speed to 100 Mbps-half duplex.

Example

```
link-speed half 100
```

Syntax

```
comment <WORD>
```

Mode

Interface
Tunnel Interface VPN

Description

Set interface comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Interface X0"
```

Syntax

```
no comment
```

Mode

Interface
Tunnel Interface VPN

Description

Clear interface comment.

Example

```
no comment
```

Syntax

```
bandwidth-management egress <DECIMAL>
```

Mode

Interface

Description

Enable and set egress bandwidth management in Kbps.

Options

<DECIMAL> Decimal in the form: n+.n+.
Example: *0.999*

Example

```
bandwidth-management egress 1000
```

Syntax

```
no bandwidth-management egress
```

Mode

Interface

Description

Disable egress bandwidth management.

Example

```
no bandwidth-management egress
```

Syntax

bandwidth-management ingress <DECIMAL>

Mode

Interface

Description

Enable and set ingress bandwidth management in Kbps.

Options

<DECIMAL> Decimal in the form: n+.n+.
Example: 0.999

Example

bandwidth-management ingress 1000

Syntax

no bandwidth-management ingress

Mode

Interface

Description

Disable ingress bandwidth management.

Example

no bandwidth-management ingress

Syntax

send-icmp-fragmentation

Mode

Interface

Description

Enable ICMP fragmentation needed message generation.

Example

send-icmp-fragmentation

Syntax

no send-icmp-fragmentation

Mode

Interface

Description

Suppress ICMP fragmentation needed message generation.

Example

no send-icmp-fragmentation

Syntax

fragment-packets

Mode

Interface
Tunnel Interface VPN

Description

Enable fragment non-VPN outbound packets larger than this interface's MTU.

Example

fragment-packets

Syntax

no fragment-packets

Mode

Interface
Tunnel Interface VPN

Description

Disable fragment non-VPN outbound packets larger than this interface's MTU.

Example

no fragment-packets

Syntax

ignore-df-bit

Mode

Interface
Tunnel Interface VPN

Description

Enable ignore don't fragment (DF) bit.

Example

ignore-df-bit

Syntax

no ignore-df-bit

Mode

Interface
Tunnel Interface VPN

Description

Disable ignore don't fragment (DF) bit.

Example

no ignore-df-bit

Syntax

```
mtu <UINT16>
```

Mode

Interface

Description

Set interface MTU.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
mtu 1500
```

Syntax

```
https-redirect
```

Mode

Interface
Dialup

Description

Enable redirection from HTTP to HTTPS.

Example

```
https-redirect
```

Syntax

```
no https-redirect
```

Mode

Interface
Dialup

Description

Disable redirection from HTTP to HTTPS.

Example

```
no https-redirect
```

Syntax

```
management { http | https | ping | snmp | ssh }
```

Mode

Interface
Dialup
Tunnel Interface VPN

Description

Enable management for the specified protocols.

Options

http HTTP.

https HTTPS.

ping Ping.

snmp SNMP.

ssh SSH.

Example

```
management https
```

Syntax

```
no management { http | https | ping | snmp | ssh }
```

Mode

Interface
Dialup
Tunnel Interface VPN

Description

Disable management for the specified protocols.

Options

http HTTP.

https HTTPS.

ping Ping.

snmp SNMP.

ssh SSH.

Example

```
no management https
```

Syntax

```
user-login [ http ] [ https ]
```

Mode

Interface
Dialup
Tunnel Interface VPN

Description

Enable user login for the specified protocols.

Options

http HTTP.

https HTTPS.

Example

```
user-login http
```

Syntax

```
no user-login [ http ] [ https ]
```

Mode

Interface
Dialup
Tunnel Interface VPN

Description

Disable user login for the specified protocols.

Options

http HTTP.
https HTTPS.

Example

```
no user-login http
```

Syntax

```
mac { default | override <INTERFACE_MAC> }
```

Mode

Interface

Description

Set MAC address used for this interface.

Options

default Factory configured MAC.

override Override factory configured MAC.
<INTERFACE_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
mac override 00:17:C5:0F:73:F4
```

Syntax

```
flow-reporting
```

Mode

Interface
Tunnel Interface VPN

Description

Enable flow reporting on the interface.

Example

```
flow-reporting
```

Syntax

no flow-reporting

Mode

Interface
Tunnel Interface VPN

Description

Disable flow reporting on the interface.

Example

no flow-reporting

Syntax

multicast

Mode

Interface
Tunnel Interface VPN

Description

Enable multicast support.

Example

multicast

Syntax

no multicast

Mode

Interface
Tunnel Interface VPN

Description

Disable multicast support.

Example

no multicast

Syntax

cos-8021p

Mode

Interface

Description

Enable 802.1p support.

Example

cos-8021p

Syntax

no cos-8021p

Mode

Interface

Description

Disable 802.1p support.

Example

no cos-8021p

Syntax

exclude-route

Mode

Interface

Description

Enable exclude from route advertisement (NSM, OSPF, BGP, RIP).

Example

exclude-route

Syntax

no exclude-route

Mode

Interface

Description

Disable exclude from route advertisement (NSM, OSPF, BGP, RIP).

Example

no exclude-route

Syntax

asymmetric-route

Mode

Interface
Tunnel Interface VPN

Description

Enable asymmetric route.

Example

asymmetric-route

Syntax

```
no asymmetric-route
```

Mode

Interface
Tunnel Interface VPN

Description

Disable asymmetric route.

Example

```
no asymmetric-route
```

Syntax

```
default-8021p-cos { background | best-effort | controlled-load | excellent-effort | network-control | spare | video | voice }
```

Mode

Interface

Description

Enable default 802.1p CoS.

Options

| | |
|-------------------------|--------------------------|
| background | 1-Background. |
| best-effort | 0-Best effort. |
| controlled-load | 4-Controlled load. |
| excellent-effort | 3-Excellent effort. |
| network-control | 7-Network control. |
| spare | 2-Spare. |
| video | 5-Video(<100ms latency). |
| voice | 6-Voice(<10ms latency). |

Example

```
default-8021p-cos best-effort
```

Syntax

```
no default-8021p-cos
```

Mode

Interface

Description

Disable default 802.1p CoS.

Example

```
no default-8021p-cos
```

Syntax

```
shutdown-port
```

Mode

Interface

Description

Enable shutdown port.

Example

```
shutdown-port
```

Syntax

```
no shutdown-port
```

Mode

Interface

Description

Disable shutdown port.

Example

```
no shutdown-port
```

Syntax

```
port aggregation aggregate <UINT8> <PORT_GROUP_INTERFACE>
```

Mode

Interface

Description

Set link aggregation.

Options

| | |
|------------------------|---|
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| <PORT_GROUP_INTERFACE> | Interface name. Example: X0 |

Example

```
port aggregation aggregate 1 X3  
port aggregation aggregate 2 X4  
port aggregation aggregate 3 X5
```

Syntax

```
no port aggregation aggregate <UINT8>
```

Mode

Interface

Description

Disable link aggregate port.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
no port aggregation aggregate 1
```

Syntax

```
port aggregation paired-aggregate <UINT8> <PORT_GROUP_INTERFACE>
```

Mode

Interface

Description

Set paired interface link aggregation.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

<PORT_GROUP_INTERFACE> Interface name.
Example: X0

Example

```
port aggregation paired-aggregate 1 X6  
port aggregation paired-aggregate 2 X7  
port aggregation paired-aggregate 3 X8
```

Syntax

```
no port aggregation paired-aggregate <UINT8>
```

Mode

Interface

Description

Disable paired interface link aggregate port.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
no port aggregation paired-aggregate 1
```

Syntax

```
port redundancy <PORT_GROUP_INTERFACE>
```

Mode

Interface

Description

Set port redundancy.

Options

<PORT_GROUP_INTERFACE> Interface name.
Example: X0

Example

```
port redundancy X3
```

Syntax

```
no port redundancy-aggregation
```

Mode

Interface

Description

Disable port redundancy and link aggregation.

Example

```
no port redundancy-aggregation
```

Syntax

```
load-balancing-vip <IPV4_HOST>
```

Mode

Interface

Description

Set the LAN load balancing virtual IP address for active-active cluster.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
load-balancing-vip 10.10.10.15
```

Syntax

```
no load-balancing-vip
```

Mode

Interface

Description

Remove the LAN load balancing virtual IP address for active-active cluster.

Example

```
no load-balancing-vip
```

Syntax

```
routed-mode { any | interface <PHYS_WAN_INTERFACE> }
```

Mode

Interface

Description

Enable routed mode and set the associated interface - Add NAT policy to prevent inbound / outbound translation.

Options

| | |
|--|---|
| <i>any</i> | Use any interface. |
| <i>interface</i> | Specify interface. |
| <i><PHYS_WAN_INTERFACE></i> | WAN interface name. Example: <i>X1</i> |

Example

```
routed-mode interface X1
```

Syntax

```
no routed-mode
```

Mode

Interface

Description

Disable routed mode.

Example

```
no routed-mode
```

Syntax

```
sonicpoint limit <SONICPOINT_LIMIT>
```

Mode

Interface

Description

Set SonicPoint limit.

Options

| | |
|--|--|
| <i><SONICPOINT_LIMIT></i> | SonicPoint limit per interface. Example: <i>8</i> |
|--|--|

Example

```
sonicpoint limit 8
```

Syntax

```
sonicpoint reserve-address { dynamic | manual <IPV4_HOST> }
```

Mode

Interface

Description

Set dynamically or manually reserve SonicPoint address.

Options

| | |
|--------------------------|--|
| dynamic | Dynamically reserve SonicPoint address. |
| manual | Manually reserve SonicPoint address. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |

Example

```
sonicpoint reserve-address dynamic
```

Syntax

```
ip-assignment <INTERFACE_ZONE_NAME> [ mode ] { dhcp | l2bridge | l2tp | portshield <PORTSHIELD_TO_INTERFACE> | pppoe | pptp | static | tap-mode | transparent | unnumbered | wire-mode }
```

Mode

Interface
Tunnel Interface VPN

Description

Set interface zone and IP assignment.

Options

| | |
|--|---|
| <INTERFACE_ZONE_NAME> | Zone object name. Example: DMZ |
| mode | Interface IP assignment mode. |
| dhcp | IP address obtained by DHCP. |
| l2bridge | Interface uses layer two bridging (IP route option). |
| l2tp | Interface uses layer2 tunneling protocol. |
| portshield | Interface is portshielded. |
| <PORTSHIELD_TO_INTERFACE> | Interface name. Example: X0 |
| pppoe | Interface uses point to point protocol over ethernet. |
| pptp | Interface uses point to point tunneling protocol. |
| static | Static IP address assignment. |
| tap-mode | Interface in tap mode. |
| transparent | Interface uses transparent bridging (splice L3 subnet). |
| unnumbered | Unnumbered IP address assignment. |
| wire-mode | Interfaces paired in wire mode. |

Example

```
ip-assignment WAN dhcp  
ip-assignment WLAN static  
ip-assignment LAN l2bridge  
ip-assignment MGMT static  
ip-assignment LAN wire-mode
```

Syntax

```
no ip-assignment
```

Mode

Interface

Description

Clear interface zone and IP assignment.

Example

```
no ip-assignment
```

Syntax

```
native-bridge <NATIVE_BRIDGE_INTERFACE>
```

Mode

Interface

Description

Configure this interface to native bridge mode and set the interface to which native bridge to.

Options

<NATIVE_BRIDGE_INTERFACE> Interface name.
Example: *X0*

Example

```
native-bridge X0
```

Syntax

```
no native-bridge
```

Mode

Interface

Description

Disable native bridge mode.

Example

```
no native-bridge
```

Syntax

```
firewalling
```

Mode

Interface

Description

Enable firewalling with other bridge members.

Example

```
firewalling
```

Syntax

no firewalling

Mode

Interface

Description

Disable firewalling with other bridge members.

Example

no firewalling

Syntax

type { bypass | inspect | secure }

Mode

Wire Mode

Description

Set the type for wiremode.

Options

bypass Bypass (via internal switch / relay).

inspect Inspect (passive deep packet inspection of mirrored traffic).

secure Secure (active deep packet inspection of inline traffic).

Example

type secure

Syntax

paired-interface <PORT_GROUP_INTERFACE>

Mode

Wire Mode

Description

Set the paired interface for wiremode.

Options

<PORT_GROUP_INTERFACE> Interface name.
Example: *X0*

Example

paired-interface X3

Syntax

no paired-interface

Mode

Wire Mode

Description

Clear the paired interface for wiremode.

Example

```
no paired-interface
```

Syntax

```
paired-interface-zone <WIRE_INTERFACE_ZONE_NAME>
```

Mode

Wire Mode

Description

Set the paired interface zone for wiremode.

Options

<WIRE_INTERFACE_ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
paired-interface-zone LAN
```

Syntax

```
stateful-inspection
```

Mode

Wire Mode
Tap Mode

Description

Enable stateful inspection.

Example

```
stateful-inspection
```

Syntax

```
no stateful-inspection
```

Mode

Wire Mode
Tap Mode

Description

Disable stateful inspection.

Example

```
no stateful-inspection
```

Syntax

```
linkstate-propagation
```

Mode

Wire Mode

Description

Enable link state propagation.

Example

```
linkstate-propagation
```

Syntax

```
no linkstate-propagation
```

Mode

Wire Mode

Description

Disable link state propagation.

Example

```
no linkstate-propagation
```

Syntax

```
restrict-analysis
```

Mode

Wire Mode

Description

Enable restrict analysis at resource limit.

Example

```
restrict-analysis
```

Syntax

```
no restrict-analysis
```

Mode

Wire Mode

Description

Disable restrict analysis at resource limit.

Example

```
no restrict-analysis
```

Syntax

```
bypass-on-malfunction
```

Mode

Wire Mode

Description

Set engage physical bypass on malfunction.

Example

```
bypass-on-malfunction
```

Syntax

```
no bypass-on-malfunction
```

Mode

Wire Mode

Description

Clear engage physical bypass on malfunction.

Example

```
no bypass-on-malfunction
```

Syntax

```
ip <IPV4_HOST> [ netmask <IPV4_MASK> ]
```

Mode

Static IP Assignment

Description

Set interface IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

netmask Set interface netmask.

<IPV4_MASK> IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: 255.255.255.0

Example

```
ip 10.10.10.10 netmask 255.255.255.0
```

Syntax

```
no ip
```

Mode

Static IP Assignment

Description

Clear interface IP address.

Example

```
no ip
```

Syntax

```
virtual-group <VIRTUAL_GROUP_ID> { backup-ip <IPV4_HOST> | ip <IPV4_HOST> }
```

Mode

Static IP Assignment

Description

Set interface virtual group IP address.

Options

| | |
|---------------------------------|--|
| <VIRTUAL_GROUP_ID> | Integer in the form: D OR 0xHH. Example: 1 |
| backup-ip | Secondary IP address. |
| <IPV4_HOST> | IPv4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| ip | IP address. |
| <IPV4_HOST> | IPv4 Address in the form: a.b.c.d. Example: 192.168.168.168 |

Example

```
virtual-group 2 ip 10.10.10.12
```

Syntax

```
no virtual-group <VIRTUAL_GROUP_ID> { backup-ip | ip }
```

Mode

Static IP Assignment

Description

Clear interface virtual group IP address.

Options

| | |
|---------------------------------|---|
| <VIRTUAL_GROUP_ID> | Integer in the form: D OR 0xHH. Example: 1 |
| backup-ip | Secondary IP address. |
| ip | IP address. |

Example

```
no virtual-group 2 ip
```

Syntax

```
netmask <IPV4_MASK>
```

Mode

Static IP Assignment

Description

Set interface subnet mask.

Options

| | |
|--------------------------|---|
| <IPV4_MASK> | IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D. Example: 255.255.255.0 |
|--------------------------|---|

Example

```
netmask 255.255.255.0
```

Syntax

```
no netmask
```

Mode

Static IP Assignment

Description

Clear interface subnet mask.

Example

```
no netmask
```

Syntax

```
backup-ip <IPV4_HOST>
```

Mode

Static IP Assignment

Description

Set MGMT interface IP address (Secondary).

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
backup-ip 10.10.10.10
```

Syntax

```
no backup-ip
```

Mode

Static IP Assignment

Description

Clear MGMT interface IP address (Secondary).

Example

```
no backup-ip
```

Syntax

```
dns primary <IPV4_HOST>
```

Mode

Static IP Assignment

Description

Set the primary DNS server IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
dns primary 192.168.168.169
```

Syntax

```
dns secondary <IPV4_HOST>
```

Mode

Static IP Assignment

Description

Set the secondary DNS server IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
dns secondary 192.168.168.170
```

Syntax

```
dns tertiary <IPV4_HOST>
```

Mode

Static IP Assignment

Description

Set the tertiary DNS server IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
dns tertiary 192.168.168.171
```

Syntax

```
no dns primary
```

Mode

Static IP Assignment

Description

Clear the primary DNS server IP address.

Example

```
no dns primary
```

Syntax

no dns secondary

Mode

Static IP Assignment

Description

Clear the secondary DNS server IP address.

Example

no dns secondary

Syntax

no dns tertiary

Mode

Static IP Assignment

Description

Clear the tertiary DNS server IP address.

Example

no dns tertiary

Syntax

gateway <IPV4_HOST>

Mode

Static IP Assignment

Description

Set interface gateway.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

gateway 10.10.10.1

Syntax

no gateway

Mode

Static IP Assignment

Description

Clear interface gateway.

Example

no gateway

Syntax

hostname <WORD>

Mode

DHCP IP Assignment

Description

Set DHCP hostname.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

hostname mydhcpclient

Syntax

no hostname

Mode

DHCP IP Assignment

Description

Clear DHCP hostname.

Example

no hostname

Syntax

release

Mode

DHCP IP Assignment

Description

Release designated interface DHCP lease.

Example

release

Syntax

renew

Mode

DHCP IP Assignment

Description

Renew interface DHCP lease.

Example

```
renew
```

Syntax

```
renew-on-startup
```

Mode

DHCP IP Assignment

Description

Enable request renew of previous IP on startup.

Example

```
renew-on-startup
```

Syntax

```
no renew-on-startup
```

Mode

DHCP IP Assignment

Description

Disable request renew of previous IP on startup.

Example

```
no renew-on-startup
```

Syntax

```
renew-on-link-up
```

Mode

DHCP IP Assignment

Description

Enable renew DHCP lease on any link up occurrence.

Example

```
renew-on-link-up
```

Syntax

```
no renew-on-link-up
```

Mode

DHCP IP Assignment

Description

Disable renew DHCP lease on any link up occurrence.

Example

no renew-on-link-up

Syntax

initiate-renewals-with-discover

Mode

DHCP IP Assignment

Description

Enable initiate renewals with a discover when using DHCP.

Example

initiate-renewals-with-discover

Syntax

no initiate-renewals-with-discover

Mode

DHCP IP Assignment

Description

Disable initiate renewals with a discover when using DHCP.

Example

no initiate-renewals-with-discover

Syntax

force-discover-interval <UINT32>

Mode

DHCP IP Assignment

Description

Enable and set the DHCP discovers interval during lease acquisition.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

force-discover-interval 8

Syntax

no force-discover-interval

Mode

DHCP IP Assignment

Description

Disable force DHCP discovers interval during lease acquisition.

Example

```
no force-discover-interval
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

PPTP IP Assignment

Description

Set the wan pptp reconnect schedule.

Options

| | |
|---------------------------------|---|
| <i>always-on</i> | Always on. |
| <i>days</i> | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| <i>time</i> | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <i>name</i> | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule name "Work Hours"
```

Syntax

```
dynamic
```

Mode

PPTP IP Assignment

Description

Enable dynamic acquisition of IP configuration data.

Example

```
dynamic
```

Syntax

```
no dynamic
```

Mode

PPTP IP Assignment

Description

Disable dynamic acquisition of IP configuration data.

Example

no dynamic

Syntax

gateway <IPV4_HOST>

Mode

PPTP IP Assignment

Description

Set interface gateway.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

gateway 10.10.10.1

Syntax

no gateway

Mode

PPTP IP Assignment

Description

Clear interface gateway.

Example

no gateway

Syntax

hostname <WORD>

Mode

PPTP IP Assignment

Description

Set PPTP hostname.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

hostname mypptpclient

Syntax

no hostname

Mode

PPTP IP Assignment

Description

Clear PPTP hostname.

Example

```
no hostname
```

Syntax

```
inactivity <UINT16>
```

Mode

PPTP IP Assignment

Description

Enable the PPTP inactivity timer.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
inactivity 10
```

Syntax

```
no inactivity
```

Mode

PPTP IP Assignment

Description

Disable the PPTP inactivity timer.

Example

```
no inactivity
```

Syntax

```
ip <IPV4_HOST> [ netmask <IPV4_MASK> ]
```

Mode

PPTP IP Assignment

Description

Set PPTP IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

netmask Set interface netmask.

<IPV4_MASK> IPV4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: 255.255.255.0

Example

```
ip 10.10.10.10 netmask 255.255.255.0
```

Syntax

```
no ip
```

Mode

PPTP IP Assignment

Description

Clear PPTP IP address.

Example

```
no ip
```

Syntax

```
password <ENC_PASSWORD>
```

Mode

PPTP IP Assignment

Description

Set PPTP user password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password mysecret
```

Syntax

```
no password
```

Mode

PPTP IP Assignment

Description

Clear PPTP user password.

Example

```
no password
```

Syntax

```
release
```

Mode

PPTP IP Assignment

Description

Release designated interface DHCP lease.

Example

```
release
```

Syntax

```
renew
```

Mode

PPTP IP Assignment

Description

Renew interface DHCP lease.

Example

```
renew
```

Syntax

```
server <IPV4_HOST>
```

Mode

PPTP IP Assignment

Description

Set PPTP server IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
server 10.10.10.10
```

Syntax

```
no server
```

Mode

PPTP IP Assignment

Description

Clear PPTP server IP address.

Example

```
no server
```

Syntax

```
user-name <WORD>
```

Mode

PPTP IP Assignment

Description

Set PPTP user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-name pptpuser
```

Syntax

```
no user-name
```

Mode

PPTP IP Assignment

Description

Clear PPTP user name.

Example

```
no user-name
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

L2TP IP Assignment

Description

Set the wan l2tp reconnect schedule.

Options

| | |
|---------------------------------|---|
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule name "Work Hours"
```

Syntax

```
dynamic
```

Mode

L2TP IP Assignment

Description

Enable dynamic acquisition of IP configuration data.

Example

```
dynamic
```

Syntax

```
no dynamic
```

Mode

L2TP IP Assignment

Description

Disable dynamic acquisition of IP configuration data.

Example

```
no dynamic
```

Syntax

```
gateway <IPV4_HOST>
```

Mode

L2TP IP Assignment

Description

Set interface gateway.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
gateway 10.10.10.1
```

Syntax

```
no gateway
```

Mode

L2TP IP Assignment

Description

Clear interface gateway.

Example

```
no gateway
```

Syntax

```
hostname <WORD>
```

Mode

L2TP IP Assignment

Description

Set L2TP hostname.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
hostname myl2tpclient
```

Syntax

```
no hostname
```

Mode

L2TP IP Assignment

Description

Clear L2TP hostname.

Example

```
no hostname
```

Syntax

```
inactivity <UINT16>
```

Mode

L2TP IP Assignment

Description

Enable the L2TP inactivity timer.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
inactivity 10
```

Syntax

```
no inactivity
```

Mode

L2TP IP Assignment

Description

Disable the L2TP inactivity timer.

Example

```
no inactivity
```

Syntax

```
ip <IPV4_HOST> [ netmask <IPV4_MASK> ]
```

Mode

L2TP IP Assignment

Description

Set L2TP IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

netmask Set interface netmask.

<IPV4_MASK> IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: *255.255.255.0*

Example

```
ip 10.10.10.10 netmask 255.255.255.0
```

Syntax

```
no ip
```

Mode

L2TP IP Assignment

Description

Clear L2TP IP address.

Example

```
no ip
```

Syntax

```
password <ENC_PASSWORD>
```

Mode

L2TP IP Assignment

Description

Set L2TP user password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password mysecret
```

Syntax

```
no password
```

Mode

L2TP IP Assignment

Description

Clear L2TP password.

Example

```
no password
```

Syntax

```
release
```

Mode

L2TP IP Assignment

Description

Release designated interface DHCP lease.

Example

```
release
```

Syntax

```
renew
```

Mode

L2TP IP Assignment

Description

Renew interface DHCP lease.

Example

```
renew
```

Syntax

```
server <IPV4_HOST>
```

Mode

L2TP IP Assignment

Description

Set L2TP server IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
server 10.10.10.10
```

Syntax

```
no server
```

Mode

L2TP IP Assignment

Description

Clear L2TP server IP address.

Example

```
no server
```

Syntax

```
shared-secret <ENC_PASSWORD>
```

Mode

L2TP IP Assignment

Description

Set L2TP password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
shared-secret myl2tpsecret
```

Syntax

```
no shared-secret
```

Mode

L2TP IP Assignment

Description

Clear L2TP shared secret.

Example

```
no shared-secret
```

Syntax

```
user-name <WORD>
```

Mode

L2TP IP Assignment

Description

Set L2TP user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-name l2tpuser
```

Syntax

no user-name

Mode

L2TP IP Assignment

Description

Clear L2TP user name.

Example

no user-name

Syntax

dynamic

Mode

PPPoE IP Assignment

Description

Enable dynamic acquisition of IP configuration data.

Example

dynamic

Syntax

no dynamic

Mode

PPPoE IP Assignment

Description

Disable dynamic acquisition of IP configuration data.

Example

no dynamic

Syntax

unnumbered <UNNUMBERED_INTERFACE_NAME>

Mode

PPPoE IP Assignment

Description

Set unnumbered interface.

Options

<UNNUMBERED_INTERFACE_NAME> Interface name.
Example: X0

Example

unnumbered X3

Syntax

no unnumbered

Mode

PPPoE IP Assignment

Description

Clear unnumbered interface.

Example

no unnumbered

Syntax

inactivity <UINT16>

Mode

PPPoE IP Assignment

Description

Enable the PPPoE inactivity timer.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

inactivity 10

Syntax

no inactivity

Mode

PPPoE IP Assignment

Description

Disable the PPPoE inactivity timer.

Example

no inactivity

Syntax

ip <IPV4_HOST>

Mode

PPPoE IP Assignment

Description

Set PPPoE IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
ip 10.10.10.10
```

Syntax

```
no ip
```

Mode

PPPoE IP Assignment

Description

Clear PPPoE IP address.

Example

```
no ip
```

Syntax

```
lcp-echo-packets
```

Mode

PPPoE IP Assignment

Description

Enable strictly use LCP echo packets for server keep-alive.

Example

```
lcp-echo-packets
```

Syntax

```
no lcp-echo-packets
```

Mode

PPPoE IP Assignment

Description

Disable strictly use LCP echo packets for server keep-alive.

Example

```
no lcp-echo-packets
```

Syntax

```
password <ENC_PASSWORD>
```

Mode

PPPoE IP Assignment

Description

Set PPPoE user password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password mysecret
```

Syntax

```
no password
```

Mode

PPPoE IP Assignment

Description

Clear PPPoE password.

Example

```
no password
```

Syntax

```
service-name <WORD>
```

Mode

PPPoE IP Assignment

Description

Set PPPoE service Name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
service-name mypppoeservice
```

Syntax

```
no service-name
```

Mode

PPPoE IP Assignment

Description

Clear PPPoE service Name.

Example

```
no service-name
```

Syntax

```
reconnect <UINT16>
```

Mode

PPPoE IP Assignment

Description

Enable and set reconnect the PPPoE client if the server does not send traffic for specified minutes.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
reconnect 5
```

Syntax

```
no reconnect
```

Mode

PPPoE IP Assignment

Description

Disable reconnect the PPPoE client if the server does not send traffic.

Example

```
no reconnect
```

Syntax

```
user-name <WORD>
```

Mode

PPPoE IP Assignment

Description

Set PPPoE user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
user-name pppouser
```

Syntax

```
no user-name
```

Mode

PPPoE IP Assignment

Description

Clear PPPoE user name.

Example

```
no user-name
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

PPPoE IP Assignment

Description

Set the wan pppoe reconnect schedule.

Options

| | |
|---------------------------------|---|
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule name "Work Hours"
```

Syntax

```
bridge-to <L2BRIDGE_INTERFACE>
```

Mode

L2 Bridge

Description

Configure interface to which this interface is bridged to.

Options

| | |
|-----------------------------------|---------------------------------------|
| <L2BRIDGE_INTERFACE> | Interface name. Example: <i>X0</i> |
|-----------------------------------|---------------------------------------|

Example

```
bridge-to X1
```

Syntax

```
block-non-ip
```

Mode

L2 Bridge

Description

Enable block all non-IP traffic.

Example

```
block-non-ip
```

Syntax

```
no block-non-ip
```

Mode

L2 Bridge

Description

Disable block all non-IP traffic.

Example

```
no block-non-ip
```

Syntax

```
route-on-bridge-pair
```

Mode

L2 Bridge

Description

Route traffic on this bridge-pair.

Example

```
route-on-bridge-pair
```

Syntax

```
no route-on-bridge-pair
```

Mode

L2 Bridge

Description

Never route traffic on this bridge-pair.

Example

```
no route-on-bridge-pair
```

Syntax

```
only-sniff
```

Mode

L2 Bridge

Description

Enable only sniff traffic on this bridge-pair.

Example

only-sniff

Syntax

no only-sniff

Mode

L2 Bridge

Description

Disable only sniff traffic on this bridge-pair.

Example

no only-sniff

Syntax

stateful-inspection

Mode

L2 Bridge

Description

Enable stateful-inspection on this bridge-pair.

Example

stateful-inspection

Syntax

no stateful-inspection

Mode

L2 Bridge

Description

Disable stateful-inspection on this bridge-pair.

Example

no stateful-inspection

Syntax

bypass-on-malfunction

Mode

L2 Bridge

Description

Set engage physical bypass on malfunction.

Example

bypass-on-malfunction

Syntax

no bypass-on-malfunction

Mode

L2 Bridge

Description

Clear engage physical bypass on malfunction.

Example

no bypass-on-malfunction

Syntax

vlan-filtering-mode { allow | block }

Mode

L2 Bridge

Description

Set VLAN filtering Mode.

Options

allow Allow.

block Block.

Example

vlan-filtering-mode block

Syntax

filtered-vlan <VLAN_FILTER_TAG>

Mode

L2 Bridge

Description

Add specified VLAN to filter.

Options

<VLAN_FILTER_TAG> Filtered VLAN ID list.
Example: 23

Example

filtered-vlan 100

Syntax

no filtered-vlan <VLAN_FILTER_TAG>

Mode

L2 Bridge

Description

Remove specified VLAN from filter.

Options

<VLAN_FILTER_TAG> Filtered VLAN ID list.
Example: 23

Example

```
no filtered-vlan 100
```

Syntax

```
no filtered-vlans
```

Mode

L2 Bridge

Description

Remove all filtered VLANs.

Example

```
no filtered-vlans
```

Syntax

```
no transparent-range
```

Mode

Transparent

Description

Clear the WAN addresses that are connected to this interface.

Example

```
no transparent-range
```

Syntax

```
transparent-range { group <WAN_ADDR_GROUP_NAME> | host <WAN_ADDR_HOST> | name <WAN_ADDR_HOST_NETWORK_RANGE_NAME> | network <WAN_ADDR_NETWORK> <ADDR_MASK> | range <WAN_ADDR_BEGIN> <ADDR_END> }
```

Mode

Transparent

Description

Set the WAN addresses that are connected to this interface.

Options

group
<WAN_ADDR_GROUP_NAME> Set transparent addresses to named address group.
WAN group address object name.
Example: Sales Group

host
<WAN_ADDR_HOST> Set transparent address as host address.
WAN address object IPv4 host address in the form: D.D.D.D.

Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Set transparent addresses to named address object.
<WAN_ADDR_HOST_NETWORK_RANGE_NAME> WAN address object name.
Example: *X1 IP*

network Set transparent addresses to network address.
<WAN_ADDR_NETWORK> WAN address object IPv4 network in the form: D.D.D.D.
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*
<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range Set transparent addresses to range of addresses.
<WAN_ADDR_BEGIN> WAN address object IPv4 starting range in the form: D.D.D.D.
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*
<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

transparent-range name "WAN Transparent Range"

Syntax

gratuitous-arp-wan-forwarding

Mode

Transparent

Description

Enable gratuitous ARP forwarding towards WAN.

Example

gratuitous-arp-wan-forwarding

Syntax

no gratuitous-arp-wan-forwarding

Mode

Transparent

Description

Disable gratuitous ARP forwarding towards WAN.

Example

no gratuitous-arp-wan-forwarding

Syntax

gratuitous-arp-wan-generation

Mode

Transparent

Description

Enable automatic gratuitous ARP generation towards WAN.

Example

```
gratuitous-arp-wan-generation
```

Syntax

```
no gratuitous-arp-wan-generation
```

Mode

Transparent

Description

Disable automatic gratuitous ARP generation towards WAN.

Example

```
no gratuitous-arp-wan-generation
```

Syntax

```
type { modem | wwan }
```

Mode

Interface

Description

Set dialup type and enter configuration mode.

Options

modem Analog modem.

wwan WWAN/mobile.

Example

```
type wwan
```

Syntax

```
dialup
```

Mode

Config

Description

Enter dialup configuration mode.

Example

```
dialup
```

Syntax

```
type { auto-detect | modem | wwan }
```

Mode

Dialup

Description

Set dialup type and enter configuration mode.

Options

| | |
|---------------------------|---------------|
| <i>auto-detect</i> | Auto-detect. |
| <i>modem</i> | Analog modem. |
| <i>wwan</i> | WWAN/mobile. |

Example

```
type wwan
```

Syntax

```
clear profile <CLEAR_CONNECTION_PROFILE_NAME> data-usage { all | billing-cycle | day | month | week | year }
```

Mode

WWAN

Description

Clear WWAN data usage information.

Options

| | |
|---|---|
| <i><CLEAR_CONNECTION_PROFILE_NAME></i> | Connection profile name. Example: <i>AT&T (Standard)</i> |
| <i>data-usage</i> | Data usage. |
| <i>all</i> | Specify period to clear. |
| <i>billing-cycle</i> | Clear billing cycle data usage information. |
| <i>day</i> | Specify period to clear. |
| <i>month</i> | Specify period to clear. |
| <i>week</i> | Specify period to clear. |
| <i>year</i> | Specify period to clear. |

Example

```
clear profile "Corp Primary Dialup" data-usage year
```

Syntax

```
clear session-history
```

Mode

WWAN

Description

Clear WWAN session history.

Options

| | |
|-------------------------------|-----------------------|
| <i>session-history</i> | WWAN session history. |
|-------------------------------|-----------------------|

Example

```
clear session-history
```

Syntax

```
speaker-volume
```

Mode

Modem

Description

Turn on speaker volume.

Example

```
speaker-volume
```

Syntax

```
no speaker-volume
```

Mode

Modem

Description

Turn off speaker volume.

Example

```
no speaker-volume
```

Syntax

```
initialize { at-commands <WORD> | use-in <MODEM_COUNTRY> }
```

Mode

Modem

Description

Set modem initialization for connection.

Options

| | |
|------------------------------|---|
| at-commands | Initialize modem connection using AT commands. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| use-in | Initialize mode connections for use in specified country. |
| <MODEM_COUNTRY> | Country. Example: <i>United States</i> |

Example

```
initialize use-in USA
```

Syntax

```
connect-on-data { av-profile-updates | firmware-update-requests | gms-heartbeats | licensed-updates | ntp-packets | snmp-traps |
syslog-traffic | system-log-emails }
```

Mode

WWAN
Modem

Description

Enable connect on data categories.

Options

| | |
|--|---------------------------|
| <i>av-profile-updates</i> | AV profile updates. |
| <i>firmware-update-requests</i> | Firmware update requests. |
| <i>gms-heartbeats</i> | GMS heartbeats. |
| <i>licensed-updates</i> | Licensed updates. |
| <i>ntp-packets</i> | NTP packets. |
| <i>snmp-traps</i> | SNMP traps. |
| <i>syslog-traffic</i> | Syslog traffic. |
| <i>system-log-emails</i> | System log emails. |

Example

```
connect-on-data ntp-packets
```

Syntax

```
no connect-on-data { av-profile-updates | firmware-update-requests | gms-heartbeats | licensed-updates | ntp-packets | snmp-traps
| syslog-traffic | system-log-emails }
```

Mode

WWAN
Modem

Description

Disable connect on data categories.

Options

| | |
|--|---------------------------|
| <i>av-profile-updates</i> | AV profile updates. |
| <i>firmware-update-requests</i> | Firmware update requests. |
| <i>gms-heartbeats</i> | GMS heartbeats. |
| <i>licensed-updates</i> | Licensed updates. |
| <i>ntp-packets</i> | NTP packets. |
| <i>snmp-traps</i> | SNMP traps. |
| <i>syslog-traffic</i> | Syslog traffic. |
| <i>system-log-emails</i> | System log emails. |

Example

no connect-on-data ntp-packets

Syntax

remote-trigger-dialout [authentication <WORD>]

Mode

WWAN
Modem

Description

Enable remotely triggered dial-out.

Options

authentication Authentication required.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

remote-trigger-dialout authentication password

Syntax

no remote-trigger-dialout [authentication]

Mode

WWAN
Modem

Description

Disable remotely triggered dial-out.

Options

authentication Disable require authentication.

Example

no remote-trigger-dialout

Syntax

max-hosts <UINT32>

Mode

WWAN
Modem

Description

Set maximum number of host connections.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

max-hosts 100

Syntax

no max-hosts

Mode

WWAN
Modem

Description

Set maximum number of host connections to unlimited.

Example

no max-hosts

Syntax

bandwidth-management egress

Mode

WWAN
Modem

Description

Enable egress bandwidth management.

Example

bandwidth-management egress

Syntax

no bandwidth-management egress

Mode

WWAN
Modem

Description

Disable egress bandwidth management.

Example

no bandwidth-management egress

Syntax

bandwidth-management ingress

Mode

WWAN
Modem

Description

Enable ingress bandwidth management.

Example

bandwidth-management ingress

Syntax

```
no bandwidth-management ingress
```

Mode

WWAN
Modem

Description

Disable ingress bandwidth management.

Example

```
no bandwidth-management ingress
```

Syntax

```
compression-multiplier <COMPRESSION_MULTIPLIE>
```

Mode

WWAN
Modem

Description

Set the bandwidth management compression multiplier.

Options

<COMPRESSION_MULTIPLIE> Compression multiple.
Example: 3.0x

Example

```
compression-multiplier 3.0x
```

Syntax

```
preferred-profile { primary <CONNECTION_PROFILE_NAME> | secondary <CONNECTION_PROFILE_NAME> | tertiary <CONNECTION_PROFILE_NAME> }
```

Mode

WWAN
Modem

Description

Set preferred connection profiles.

Options

primary Primary connection profile.
<CONNECTION_PROFILE_NAME> Connection profile name.
Example: AT&T (Standard)

secondary Alternate 1 connection profile.
<CONNECTION_PROFILE_NAME> Connection profile name.
Example: AT&T (Standard)

tertiary Alternate 2 connection profile.
<CONNECTION_PROFILE_NAME> Connection profile name.
Example: AT&T (Standard)

Example

```
preferred-profile primary "Corp Primary Dialup"  
preferred-profile tertiary "Corp Alternate Dialup"
```

Syntax

```
no preferred-profile { primary | secondary | tertiary }
```

Mode

WWAN
Modem

Description

Clear preferred connection profiles.

Options

primary Primary connection profile.

secondary Alternate 1 connection profile.

tertiary Alternate 2 connection profile.

Example

```
no preferred-profile primary
```

Syntax

```
connection-profile <CONNECTION_PROFILE_NAME>
```

Mode

Dialup

Description

Add/Edit connection profile and enter its configuration mode.

Options

<CONNECTION_PROFILE_NAME> Connection profile name.
Example: *AT&T (Standard)*

Example

```
connection-profile "Corp Primary Dialup"
```

Syntax

```
connection-profile <CONNECTION_PROFILE_NAME>
```

Mode

Dialup

Description

Add/Edit connection profile and enter its configuration mode.

Options

<CONNECTION_PROFILE_NAME> Connection profile name.
Example: *AT&T (Standard)*

Example

```
connection-profile "Corp Primary Dialup"
```

Syntax

no connection-profile <CONNECTION_PROFILE_NAME>

Mode

Dialup

Description

Delete connection profile.

Options

<CONNECTION_PROFILE_NAME> Connection profile name.
Example: *AT&T* (*Standard*)

Example

no connection-profile "Corp Primary Dialup"

Syntax

country <WORD>

Mode

WWAN Profile

Description

Set connection profile country.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

country USA

Syntax

provider <WORD>

Mode

WWAN Profile

Description

Set connection profile provider.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

provider AT&T

Syntax

plan-type <WORD>

Mode

WWAN Profile

Description

Set connection profile plan type.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
plan-type standard
```

Syntax

```
name <WORD>
```

Mode

WWAN Profile
Modem Profile

Description

Set connection profile name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name "Corp Connection Profile"
```

Syntax

```
service-type { cdma-edvo | gprs-edge-hspa }
```

Mode

WWAN Profile

Description

Set connection profile service type.

Options

cdma-edvo CDMA/EDVO.

gprs-edge-hspa GPRS/EDGE/HSPA.

Example

```
service-type cdma-edvo
```

Syntax

```
no service-type
```

Mode

WWAN Profile

Description

Clear connection profile service type.

Example

```
no service-type
```

Syntax

```
dialed-number <WORD>
```

Mode

WWAN Profile

Description

Set connection profile dialed number.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
dialed-number *99#
```

Syntax

```
primary-dialed-number <WORD>
```

Mode

Modem Profile

Description

Set connection profile primary dialed number.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
primary-dialed-number 555-555-5555
```

Syntax

```
secondary-dialed-number <WORD>
```

Mode

Modem Profile

Description

Set connection profile secondary dialed number.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
secondary-dialed-number 777-777-7777
```

Syntax

```
user-name <WORD>
```

Mode

WWAN Profile
Modem Profile

Description

Set connection profile user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-name ISPDA@CINGULARGPRS.COM
```

Syntax

```
user-password <WORD>
```

Mode

WWAN Profile
Modem Profile

Description

Set connection profile user password.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-password thisismypassword
```

Syntax

```
access-point-name <WORD>
```

Mode

WWAN Profile

Description

Set connection profile access point name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
access-point-name ISP.CINGULAR
```

Syntax

```
connect-type { connect-on-data | manual | persistent }
```

Mode

WWAN Profile
Modem Profile

Description

Set connection profile connect type.

Options

connect-on-data Connect on data.

manual Manual connection.

persistent Persistent connection.

Example

```
connect-type persistent
```

Syntax

```
inactivity-disconnect <UINT16>
```

Mode

WWAN Profile
Modem Profile

Description

Enable and set connection profile inactivity disconnect time in minutes.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
inactivity-disconnect 10
```

Syntax

```
no inactivity-disconnect
```

Mode

WWAN Profile
Modem Profile

Description

Disable connection profile inactivity disconnect time.

Example

```
no inactivity-disconnect
```

Syntax

```
max-connection-speed { 14400 | 19200 | 2400 | 38400 | 4800 | 57600 | 9600 | auto }
```

Mode

Modem Profile

Description

Set max connection speed.

Options

14400 Max connection speed.

19200 Max connection speed.

2400 Max connection speed.

38400 Max connection speed.

4800 Max connection speed.

57600 Max connection speed.

9600 Max connection speed.

auto Max connection speed.

Example

```
max-connection-speed 3600
```

Syntax

```
max-connection-time <UINT16>
```

Mode

WWAN Profile
Modem Profile

Description

Enable and set connection profile maximum connection time in minutes.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
max-connection-time 30
```

Syntax

```
no max-connection-time
```

Mode

WWAN Profile
Modem Profile

Description

Disable connection profile maximum connection time.

Example

```
no max-connection-time
```

Syntax

```
delay-before-reconnect <UINT16>
```

Mode

WWAN Profile
Modem Profile

Description

Enable and set connection profile delay before reconnect in minutes.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
delay-before-reconnect 2
```

Syntax

```
no delay-before-reconnect
```

Mode

WWAN Profile
Modem Profile

Description

Clear connection profile delay before reconnect.

Example

```
no delay-before-reconnect
```

Syntax

```
call-waiting [ string <CALL_WAIT_STRING> ]
```

Mode

Modem Profile

Description

Enable call waiting and set call waiting string.

Options

string Set call waiting string.
<CALL_WAIT_STRING> Call wait string.
Example: 1170

Example

```
call-waiting
```

Syntax

no call-waiting

Mode

Modem Profile

Description

Disable call waiting.

Example

no call-waiting

Syntax

dial-retries <UINT16>

Mode

WWAN Profile
Modem Profile

Description

Enable and set connection profile dial retries per phone number.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

dial-retries 3

Syntax

no dial-retries

Mode

WWAN Profile
Modem Profile

Description

Disable connection profile dial retries per phone number.

Example

no dial-retries

Syntax

delay-between-retries <UINT32>

Mode

WWAN Profile
Modem Profile

Description

Enable and set connection profile delay between retries in minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

delay-between-retries 5

Syntax

vpn-when-dialed

Mode

WWAN Profile
Modem Profile

Description

VPN remains enabled when dialed.

Example

vpn-when-dialed

Syntax

no vpn-when-dialed

Mode

WWAN Profile
Modem Profile

Description

Disable VPN when dialed.

Example

no vpn-when-dialed

Syntax

force-pap

Mode

WWAN Profile

Description

Enable force PAP authentication.

Example

force-pap

Syntax

no force-pap

Mode

WWAN Profile

Description

Disable force PAP authentication.

Example

```
no force-pap
```

Syntax

```
ip-assignment { automatic | static <IPV4_HOST> }
```

Mode

WWAN Profile
Modem Profile

Description

Set IP address manually or if obtained automatically.

Options

automatic Obtain an IP address automatically.

static Specify IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
ip-assignment static 204.16.16.1
```

Syntax

```
dns-assignment { { [ primary <IPV4_HOST> ] [ secondary <IPV4_HOST> ] } | automatic }
```

Mode

WWAN Profile
Modem Profile

Description

Set whether DNS obtained automatically or set manually with the associated DNS server IP addresses.

Options

primary Specify primary DNS server IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

secondary Specify secondary DNS server IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

automatic Obtain an IP address of DNS servers automatically.

Example

```
dns-assignment primary 4.2.2.1
```

Syntax

```
schedule [ sun <PROFILE_TIME_HHMM> <PROFILE_TIME_HHMM> ] [ mon <PROFILE_TIME_HHMM> <PROFILE_TIME_HHMM> ] [ tue <PROFILE_TIME_HHMM> <PROFILE_TIME_HHMM> ] [ wed <PROFILE_TIME_HHMM> <PROFILE_TIME_HHMM> ] [ thu <PROFILE_TIME_HHMM> <PROFILE_TIME_HHMM> ] [ fri <PROFILE_TIME_HHMM> <PROFILE_TIME_HHMM> ] [ sat <PROFILE_TIME_HHMM> <PROFILE_TIME_HHMM> ]
```

Mode

Description

Enable and set the schedule when the modem can connect during.

Options

| | |
|----------------------------------|--|
| <i>sun</i> | Day of the week. |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <i>mon</i> | Day of the week. |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <i>tue</i> | Day of the week. |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <i>wed</i> | Day of the week. |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <i>thu</i> | Day of the week. |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <i>fri</i> | Day of the week. |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <i>sat</i> | Day of the week. |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |
| <PROFILE_TIME_HHMM> | Time in the form: DD:DD. Example: 12:00 |

Example

```
schedule mon 8:00 18:00 wed 9:00 17:00
```

Syntax

```
no schedule [ sun ] [ mon ] [ tue ] [ wed ] [ thu ] [ fri ] [ sat ]
```

Mode

WWAN Profile

Description

Disable the schedule when the modem can connect during.

Options

| | |
|------------|------------------|
| <i>sun</i> | Day of the week. |
| <i>mon</i> | Day of the week. |
| <i>tue</i> | Day of the week. |
| <i>wed</i> | Day of the week. |
| <i>thu</i> | Day of the week. |
| <i>fri</i> | Day of the week. |
| <i>sat</i> | Day of the week. |

Example

no schedule

Syntax

```
data-usage-limiting [ billing-start <UINT8> ] [ limit <UINT32> ] [ units { gb | kb | mb | minutes } ]
```

Mode

WWAN Profile

Description

Enable and set data usage limiting.

Options

| | |
|-----------------------|---|
| billing-start | Set billing start date. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| limit | Set data usage limit. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: 123 |
| units | Set units for data usage limit. |
| gb | Gigabytes. |
| kb | Kilobytes. |
| mb | Megabytes. |
| minutes | Minutes. |

Example

```
data-usage-limiting
```

Syntax

```
no data-usage-limiting [ billing-start | limit ]
```

Mode

WWAN Profile

Description

Disable data usage limiting.

Options

| | |
|----------------------|-------------------------|
| billing-start | Set billing start date. |
| limit | Set data usage limit. |

Example

```
no data-usage-limiting
```

Syntax

```
chat-script <WORD>
```

Mode

WWAN Profile
Modem Profile

Description

Set chat script.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
chat-script "chat-script gsm "" "ATDT*98*1#" TIMEOUT 60"
```

Syntax

```
no chat-script
```

Mode

WWAN Profile
Modem Profile

Description

Clear chat script.

Example

```
no chat-script
```

Syntax

```
arp
```

Mode

Config

Description

Enter ARP configuration mode.

Example

```
arp
```

Syntax

```
no entry <ARP_IPV4_HOST> <ARP_MAC> <ARP_INTERFACE>
```

Mode

ARP

Description

Deletes an ARP entry.

Options

<ARP_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

<ARP_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

<ARP_INTERFACE> Interface name.
Example: *X0*

Example

```
no entry 10.10.10.10 00:01:02:03:04:05 X0
```

Syntax

```
no entries
```

Mode

ARP

Description

Deletes all ARP entries.

Example

```
no entries
```

Syntax

```
entry <ARP_IPV4_HOST> <ARP_MAC> <ARP_INTERFACE>
```

Mode

ARP

Description

Add/edit an ARP entry.

Options

- <ARP_IPV4_HOST>** IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*
- <ARP_MAC>** MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*
- <ARP_INTERFACE>** Interface name.
Example: *X0*

Example

```
entry 10.10.10.10 00:01:02:03:04:05 X0
```

Syntax

```
timeout <UINT16>
```

Mode

ARP

Description

Set the ARP cache entry timeout in minutes.

Options

- <UINT16>** Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
timeout 10
```

Syntax

glean

Mode

ARP

Description

Enable glean source data from ARP requests.

Example

glean

Syntax

no glean

Mode

ARP

Description

Disable glean source data from ARP requests.

Example

no glean

Syntax

ip <ARP_IPV4_HOST>

Mode

Static ARP

Description

Configure static ARP IP.

Options

<ARP_IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

ip 10.10.10.10

Syntax

mac <ARP_MAC>

Mode

Static ARP

Description

Configure static ARP MAC address.

Options

<ARP_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD

Example

```
mac 00:01:02:03:04:05
```

Syntax

```
interface <ARP_INTERFACE>
```

Mode

Static ARP

Description

Configure static ARP interface.

Options

<ARP_INTERFACE> Interface name.
Example: *X0*

Example

```
interface X0
```

Syntax

```
publish
```

Mode

Static ARP

Description

Publish ARP entry.

Example

```
publish
```

Syntax

```
no publish
```

Mode

Static ARP

Description

Disable publishing of ARP entry.

Example

```
no publish
```

Syntax

```
bind-mac
```

Mode

Static ARP

Description

Enable MAC binding.

Example

```
bind-mac
```

Syntax

```
no bind-mac
```

Mode

Static ARP

Description

Disable MAC binding.

Example

```
no bind-mac
```

Syntax

```
dynamic
```

Mode

Static ARP

Description

Enable update IP address dynamically.

Example

```
dynamic
```

Syntax

```
no dynamic
```

Mode

Static ARP

Description

Disable update IP address dynamically.

Example

```
no dynamic
```

Syntax

```
clear arp cache entries
```

Mode

Config
ARP

Description

Clear all non-permanent entries.

Example

```
clear arp cache entries
```

Syntax

```
clear arp cache entry <ARP_FLUSH_IPV4_HOST> <ARP_FLUSH_INTERFACE>
```

Mode

Config
ARP

Description

Clear an ARP entry.

Options

<ARP_FLUSH_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

<ARP_FLUSH_INTERFACE> Interface name.
Example: X0

Example

```
clear arp cache entry 10.10.10.10 X0
```

Syntax

```
dns server { inherit | ipv6 { inherit | preferred | static { primary <HOST_IP> | secondary <HOST_IP> | tertiary <HOST_IP> } } |  
static { primary <HOST_IP> | secondary <HOST_IP> | tertiary <HOST_IP> } }
```

Mode

Config

Description

Set DNS server.

Options

inherit Inherit DNS servers.

ipv6 Set IPv6 DNS server

inherit Inherit DNS servers.

preferred Prefer IPv6 DNS Servers.

static Set static DNS server

primary Specify primary DNS server IP address.

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

secondary Specify secondary DNS server IP address.

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

tertiary Specify tertiary DNS server IP address.

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

static Set static DNS server

primary Specify primary DNS server IP address.

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

secondary Specify secondary DNS server IP address.

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

tertiary Specify tertiary DNS server IP address.

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

```
dns server static primary 192.168.168.165
dns server static secondary 192.168.168.165
dns server static tertiary 192.168.168.165
dns server inherit
dns server ipv6 preferred
dns server ipv6 static primary fe80::0001
dns server ipv6 static secondary fe80::0001
dns server ipv6 static tertiary fe80::0001
dns server ipv6 inherit
```

Syntax

```
no dns server { ipv6 { preferred | static { primary | secondary | tertiary } } | static { primary | secondary | tertiary } }
```

Mode

Config

Description

Clear DNS server.

Options

ipv6 Clear IPv6 DNS server

preferred Do not prefer IPv6 DNS Servers.

static Clear static DNS server

primary Clear primary DNS server IP address.

secondary Clear secondary DNS server IP address.

tertiary Clear tertiary DNS server IP address.

static Clear static DNS server

primary Clear primary DNS server IP address.

secondary Clear secondary DNS server IP address.

tertiary Clear tertiary DNS server IP address.

Example

```
no dns server static primary
no dns server static secondary
no dns server static tertiary
no dns server ipv6 preferred
no dns server ipv6 static primary
no dns server ipv6 static secondary
no dns server ipv6 static tertiary
```

Syntax

```
dns rebinding [ action { drop-dns-reply | log-attack-only | return-query-refused } ] [ allowed-domains { fqdn <ADDR_FQDN> | group <ADDR_CUSTOM_FQDN_GROUP> | name <ADDR_FQDN_NAME> } ]
```

Mode

Config

Description

Enable and configure DNS rebinding attack prevention.

Options

| | |
|--|---|
| action | Set action when experiencing attack. |
| drop-dns-reply | Log the attack and drop the DNS reply. |
| log-attack-only | Log the attack only. |
| return-query-refused | Log the attack and return a query refused reply. |
| allowed-domains | Specify the domains for which checking is not done. |
| fqdn <ADDR_FQDN> | Create FQDN address object with same name as defined. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group <ADDR_CUSTOM_FQDN_GROUP> | Specify FQDN group name. Custom FQDN group address object name. Example: <i>Forbidden Domains</i> |
| name <ADDR_FQDN_NAME> | Specify FQDN address object name. FQDN address object name. Example: <i>www.example.com</i> |

Example

```
dns rebinding action drop-dns-reply allowed-domains name "DNS RAP WHITELIST"
```

Syntax

```
no dns rebinding [ allowed-domains ]
```

Mode

Config

Description

Disable DNS rebinding attack prevention.

Options

allowed-domains Clear DNS rebinding allowed domains.

Example

```
no dns rebinding
```

Syntax

```
dns fqdn-binding
```

Mode

Config

Description

Enable FQDN object only cache DNS reply from sanctioned server.

Example

```
dns fqdn-binding
```

Syntax

```
no dns fqdn-binding
```

Mode

Config

Description

Disable FQDN object only cache DNS reply from sanctioned server.

Example

```
no dns fqdn-binding
```

Syntax

```
dns split-servers
```

Mode

Config

Description

Enable proxying of split DNS servers.

Example

```
dns split-servers
```

Syntax

```
no dns split-servers
```

Mode

Config

Description

Disable proxying of split DNS servers.

Example

```
no dns split-servers
```

Syntax

```
dns fqdn-over-tcp-dns
```

Mode

Config

Description

Enable DNS host name lookup over TCP for FQDN.

Example

dns fqdn-over-tcp-dns

Syntax

no dns fqdn-over-tcp-dns

Mode

Config

Description

Disable DNS host name lookup over TCP for FQDN.

Example

no dns fqdn-over-tcp-dns

Syntax

clear dns cache [interface-reverse]

Mode

Config

Description

Clear DNS cache.

Options

interface-reverse Clear interface names reverse DNS cache.

Example

clear dns cache

Syntax

no dynamic-dns profile [ipv6] <DDNS_PROFILE_NAME>

Mode

Config

Description

Deletes a dynamic DNS profile.

Options

ipv6 Delete IPv6 dynamic DNS Profile.
<DDNS_PROFILE_NAME> Dynamic DNS profile name.
Example: *mydns*

Example

no dynamic-dns profile "abc"
no dynamic-dns profile ipv6 "xyz"

Syntax

no dynamic-dns profiles [ipv6]

Mode

Config

Description

Deletes all dynamic DNS profiles.

Options

ipv6 Delete all IPv6 dynamic DNS Profiles.

Example

```
no dynamic-dns profiles
no dynamic-dns profiles ipv6
```

Syntax

```
dynamic-dns profile [ ipv6 ] <DDNS_PROFILE_NAME>
```

Mode

Config

Description

Add/edit a dynamic DNS profile.

Options

ipv6 Add/edit a IPv6 dynamic DNS Profile.
<DDNS_PROFILE_NAME> Dynamic DNS profile name.
Example: *mydns*

Example

```
dynamic-dns profile CorpNoIP
dynamic-dns profile ipv6 CorpNoIP
```

Syntax

```
profile-name <DDNS_PROFILE_NAME>
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Edit a dynamic DNS profile name.

Options

<DDNS_PROFILE_NAME> Dynamic DNS profile name.
Example: *mydns*

Example

```
profile-name CorpNoIP
```

Syntax

```
enable
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Enable dynamic DNS profile.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Disable dynamic DNS profile.

Example

```
no enable
```

Syntax

```
use-online
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Enable use online settings.

Example

```
use-online
```

Syntax

```
no use-online
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Disable use online settings.

Example

```
no use-online
```

Syntax

```
provider { changeip | dyn | noip }
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Select dynamic DNS provider.

Options

changeip changeip.com.

dyn dyn.com.

noip No-IP.com.

Example

```
provider noip
```

Syntax

```
user-name <WORD>
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Set dynamic DNS user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-name ddnsadmin
```

Syntax

```
no user-name
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Clear dynamic DNS user name.

Example

```
no user-name
```

Syntax

```
password <ENC_PASSWORD>
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Set dynamic DNS password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password thisisasecret
```

Syntax

```
no password
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Clear dynamic DNS password.

Example

```
no password
```

Syntax

```
domain <HOSTNAME>
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Set dynamic DNS domain.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
domain testsite.hopto.org
```

Syntax

```
no domain
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Clear dynamic DNS domain.

Example

```
no domain
```

Syntax

```
bound-to { any | interface <WAN_INTERFACE> }
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Set dynamic DNS WAN interface to bind to.

Options

any Any interface.

interface Specify interface.
<WAN_INTERFACE> WAN interface name.
Example: *X1*

Example

```
bound-to interface X1
```

Syntax

```
online-settings { detect | manual <HOST_IP> | set-to-wan }
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Configure dynamic DNS online settings.

Options

detect Let the dynamic DNS provider detect the IP address.

manual Specify the IP address manually.
<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

set-to-wan Automatically set the IP address to the primary WAN IP address.

Example

```
online-settings manual 10.10.10.10
```

Syntax

```
offline-settings { do-nothing | make-host-unknown | manual <IPV4_HOST> | use-previous }
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Configure dynamic DNS offline settings.

Options

| | |
|---------------------------------|--|
| <i>do-nothing</i> | Allows the previously registered IP address to remain current with the Provider. |
| <i>make-host-unknown</i> | Let the dynamic DNS provider detect the IP address. |
| <i>manual</i> | Specify the IP address manually. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| <i>use-previous</i> | Use the off-line IP address previously configured at the provider's site. |

Example

```
offline-settings manual 10.10.10.10
```

Syntax

```
service-type { custom | dynamic | static }
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Configure dynamic DNS service type.

Options

custom Custom.

dynamic Dynamic.

static Static.

Example

```
service-type dynamic
```

Syntax

```
dhcp-server [ ipv4 | ipv6 ]
```

Mode

Config

Description

Enter DHCP server configuration mode.

Options

ipv4 Enter IPv4 DHCP server configuration mode.

ipv6 Enter IPv6 DHCP server configuration mode.

Example

```
dhcp-server
```

Syntax

enable

Mode

DHCP Server

Description

Enable DHCP server.

Example

enable

Syntax

no enable

Mode

DHCP Server

Description

Disable DHCP server.

Example

no enable

Syntax

conflict-detection

Mode

DHCP Server

Description

Enable DHCP server conflict detection.

Example

conflict-detection

Syntax

no conflict-detection

Mode

DHCP Server

Description

Disable DHCP server conflict detection.

Example

no conflict-detection

Syntax

persistence [monitoring-interval <UINT16>]

Mode

DHCP Server

Description

Enable/configure DHCP server persistence.

Options

monitoring-interval Set DHCP server persistence monitoring interval in minutes.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

persistence

Syntax

no persistence

Mode

DHCP Server

Description

Disable DHCP server persistence.

Example

no persistence

Syntax

scope

Mode

DHCP Server

Description

DHCP scope.

Example

scope

Syntax

scope dynamic <SCOPE_START_IPV4_HOST> <SCOPE_END_IPV4_HOST>

Mode

DHCP Server

Description

Add/edit dynamic DHCP scope and enter its configuration mode.

Options

<SCOPE_START_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168
<SCOPE_END_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
scope dynamic 192.168.168.100 192.168.168.200
```

Syntax

```
no scope dynamic <SCOPE_START_IPV4_HOST> <SCOPE_END_IPV4_HOST>
```

Mode

DHCP Server

Description

Delete dynamic DHCP scope.

Options

<SCOPE_START_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

<SCOPE_END_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
no scope dynamic 192.168.168.100 192.168.168.200
```

Syntax

```
scope static <STATIC_SCOPE_IPV4_HOST> <STATIC_SCOPE_MAC>
```

Mode

DHCP Server

Description

Add/edit static DHCP scope and enter its configuration mode.

Options

<STATIC_SCOPE_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

<STATIC_SCOPE_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD

Example

```
scope static 192.168.168.101 00:01:02:03:04:05
```

Syntax

```
no scope static <STATIC_SCOPE_IPV4_HOST> <STATIC_SCOPE_MAC>
```

Mode

DHCP Server

Description

Delete static DHCP scope.

Options

<STATIC_SCOPE_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

<STATIC_SCOPE_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD

Example

```
no scope static 192.168.168.101 00:01:02:03:04:05
```

Syntax

```
no scopes dynamic
```

Mode

DHCP Server

Description

Delete all dynamic DHCP scopes.

Example

```
no scopes dynamic
```

Syntax

```
no scopes static
```

Mode

DHCP Server

Description

Delete all static DHCP entries.

Example

```
no scopes static
```

Syntax

```
no scopes
```

Mode

DHCP Server

Description

Delete all DHCP server lease scopes.

Example

```
no scopes
```

Syntax

```
clear lease <DHCP_LEASE_IPV4_HOST>
```

Mode

DHCP Server

Description

Delete DHCP server lease.

Options

<DHCP_LEASE_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
clear lease 1.1.1.1
```

Syntax

```
clear leases
```

Mode

DHCP Server

Description

Delete all DHCP server leases.

Example

```
clear leases
```

Syntax

```
option
```

Mode

DHCP Server

Description

DHCP server option.

Example

```
option
```

Syntax

```
option object <DHCP_OPTION_OBJECT>
```

Mode

DHCP Server

Description

Add/edit DHCP server option object and enter its configuration mode.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: Corp Network DHCP Options

Example

```
option object "LAN Specific DHCP Option"
```

Syntax

```
no option object <DHCP_OPTION_OBJECT>
```

Mode

DHCP Server

Description

Delete DHCP server option object.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
no option object "LAN Specific DHCP Option"
```

Syntax

```
no option objects
```

Mode

DHCP Server

Description

Delete all DHCP server option objects.

Example

```
no option objects
```

Syntax

```
option group <DHCP_OPTION_GROUP>
```

Mode

DHCP Server

Description

Add/edit DHCP server option group and enter its configuration mode.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
option group "LAN Specific DHCP Options"
```

Syntax

```
no option group <DHCP_OPTION_GROUP>
```

Mode

DHCP Server

Description

Delete DHCP server option group.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
no option group "LAN Specific DHCP Options"
```

Syntax

```
no option groups
```

Mode

DHCP Server

Description

Delete all DHCP server option groups.

Example

```
no option groups
```

Syntax

```
trusted-relay-agents <ADDR_DHCP_TRUSTED_RELAY_AGENT_GROUP>
```

Mode

DHCP Server

Description

Enable and set trusted DHCP relay agent list.

Options

<ADDR_DHCP_TRUSTED_RELAY_AGENT_GROUP> Group address object name.
Example: *Default Trusted Relay Agent List*

Example

```
trusted-relay-agents "Trusted Relay Agents"
```

Syntax

```
no trusted-relay-agents
```

Mode

DHCP Server

Description

Disable trusted DHCP relay agent list.

Example

```
no trusted-relay-agents
```

Syntax

```
enable
```

Mode

Dynamic Scope

Description

Enable dynamic DHCP scope.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Dynamic Scope

Description

Disable dynamic DHCP scope.

Example

```
no enable
```

Syntax

```
range <IPV4_HOST> <IPV4_HOST>
```

Mode

Dynamic Scope

Description

Set DHCP dynamic scope range.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
range 192.168.168.100 192.168.168.200
```

Syntax

```
lease-time <UINT16>
```

Mode

Dynamic Scope

Description

Set dynamic DHCP scope lease time.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
lease-time 1440
```

Syntax

```
default-gateway <IPV4_HOST>
```

Mode

Dynamic Scope

Description

Set dynamic DHCP scope default gateway.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
default-gateway 192.168.168.254
```

Syntax

```
netmask <IPV4_MASK>
```

Mode

Dynamic Scope

Description

Set dynamic DHCP scope subnet mask.

Options

<IPV4_MASK> IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: 255.255.255.0

Example

```
netmask 255.255.255.0
```

Syntax

```
comment <WORD>
```

Mode

Dynamic Scope

Description

Set dynamic DHCP scope comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
comment "my dynamic scope"
```

Syntax

```
no comment
```

Mode

Dynamic Scope

Description

Clear dynamic DHCP scope comment.

Example

```
no comment
```

Syntax

```
allow-bootp
```

Mode

Dynamic Scope

Description

Enable allow BOOTP clients to use range.

Example

```
allow-bootp
```

Syntax

```
no allow-bootp
```

Mode

Dynamic Scope

Description

Disable allow BOOTP clients to use range.

Example

```
no allow-bootp
```

Syntax

```
domain-name <HOSTNAME>
```

Mode

Dynamic Scope

Description

Set DHCP domain name.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
domain-name example.com
```

Syntax

```
no domain-name
```

Mode

Dynamic Scope

Description

Clear DHCP domain name.

Example

```
no domain-name
```

Syntax

```
dns server { inherit | static { primary <IPV4_HOST> | secondary <IPV4_HOST> | tertiary <IPV4_HOST> } }
```

Mode

Dynamic Scope

Description

Manually set DNS settings or inherit DNS settings dynamically from the sonicwall's DNS settings.

Options

- inherit** Inherit DNS servers.
- static** Static DNS server.
- primary** Specify primary DNS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*
- secondary** Specify secondary DNS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*
- tertiary** Specify tertiary DNS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
dns server static primary 192.168.168.165  
dns server inherit
```

Syntax

```
no dns server static { primary | secondary | tertiary }
```

Mode

Dynamic Scope

Description

Manually clear DNS server IP address.

Options

- static** Clear static DNS server IP address.
- primary** Clear primary DNS server IP address.
- secondary** Clear secondary DNS server IP address.
- tertiary** Clear tertiary DNS server IP address.

Example

```
no dns server static primary
```

Syntax

```
wins { primary <IPV4_HOST> | secondary <IPV4_HOST> }
```

Mode

Dynamic Scope

Description

Set the WINS server IP address.

Options

primary Primary WINS server IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

secondary Secondary WINS server IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
wins primary 192.168.168.169
```

Syntax

```
no wins { primary | secondary }
```

Mode

Dynamic Scope

Description

Clear the WINS server IP address.

Options

primary Primary WINS server IP address.

secondary Secondary WINS server IP address.

Example

```
no wins primary
```

Syntax

```
call-manager { primary <WORD> | secondary <WORD> | tertiary <WORD> }
```

Mode

Dynamic Scope

Description

Set VOIP call managers.

Options

primary Specify primary VOIP call manager IP address.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

secondary Specify secondary VOIP call manager IP address.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

tertiary Specify tertiary VOIP call manager address.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
call-manager primary 192.168.168.161
```

Syntax

```
no call-manager { primary | secondary | tertiary }
```

Mode

Dynamic Scope

Description

Clear VOIP call managers.

Options

primary Clear primary VOIP call manager IP address.

secondary Clear secondary VOIP call manager IP address.

tertiary Clear tertiary VOIP call manager address.

Example

```
no call-manager primary
```

Syntax

```
network-boot { boot-file <WORD> | next-server <IPV4_HOST> | server-name <WORD> }
```

Mode

Dynamic Scope

Description

Set network boot parameters.

Options

boot-file Specify boot file.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

next-server Specify next server.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

server-name Specify server name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
network-boot next-server 192.168.168.161
```

Syntax

```
no network-boot { boot-file | next-server | server-name }
```

Mode

Dynamic Scope

Description

Clear network boot parameters.

Options

boot-file Clear boot file.

next-server Clear next server.

server-name Clear server name.

Example

```
no network-boot next-server
```

Syntax

```
no generic-option
```

Mode

Dynamic Scope

Description

Clear DHCP generic option group.

Example

```
no generic-option
```

Syntax

```
generic-option { group <DHCP_OPTION_GROUP> | object <DHCP_OPTION_OBJECT> }
```

Mode

Dynamic Scope

Description

Set DHCP generic option group.

Options

group Specify generic option group.
<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

object Specify generic option object.
<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
generic-option object "NetServers"
```

Syntax

```
always-send-option
```

Mode

Dynamic Scope

Description

Enable send generic options always.

Example

```
always-send-option
```

Syntax

```
no always-send-option
```

Mode

Dynamic Scope

Description

Disable send generic options always.

Example

```
no always-send-option
```

Syntax

```
enable
```

Mode

Static Scope

Description

Enable static DHCP server scope.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Static Scope

Description

Disable DHCP server scope.

Example

no enable

Syntax

name <WORD>

Mode

Static Scope

Description

Set DHCP static scope name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name "My Domain Server"

Syntax

no name

Mode

Static Scope

Description

Clear DHCP static scope name.

Example

no name

Syntax

ip <STATIC_SCOPE_IPV4_HOST>

Mode

Static Scope

Description

Set DHCP static scope IP address.

Options

<STATIC_SCOPE_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

ip 10.10.10.10

Syntax

mac <STATIC_SCOPE_MAC>

Mode

Static Scope

Description

Set DHCP static scope ethernet address.

Options

<STATIC_SCOPE_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
mac 00:01:02:03:04:05
```

Syntax

```
lease-time <UINT16>
```

Mode

Static Scope

Description

Set DHCP static scope lease time.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
lease-time 1440
```

Syntax

```
default-gateway <IPV4_HOST>
```

Mode

Static Scope

Description

Set DHCP static scope default gateway.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
default-gateway 192.168.168.254
```

Syntax

```
netmask <IPV4_MASK>
```

Mode

Static Scope

Description

Set DHCP static scope subnet mask.

Options

<IPV4_MASK> IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: 255.255.255.0

Example

```
netmask 255.255.255.0
```

Syntax

```
comment <WORD>
```

Mode

Static Scope

Description

Set DHCP static scope comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
comment "my static scope"
```

Syntax

```
no comment
```

Mode

Static Scope

Description

Clear DHCP static scope comment.

Example

```
no comment
```

Syntax

```
domain-name <HOSTNAME>
```

Mode

Static Scope

Description

Set DHCP domain name.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: example.com

Example

```
domain-name example.com
```

Syntax

no domain-name

Mode

Static Scope

Description

Clear DHCP domain name.

Example

no domain-name

Syntax

```
dns server { inherit | static { primary <IPV4_HOST> | secondary <IPV4_HOST> | tertiary <IPV4_HOST> } }
```

Mode

Static Scope

Description

Manually set DNS settings or inherit DNS settings dynamically from the sonicwall's DNS settings.

Options

| | |
|---------------------------------|---|
| <i>inherit</i> | Inherit DNS servers. |
| <i>static</i> | Static DNS server. |
| <i>primary</i> | Specify primary DNS server IP address. |
| <i><IPV4_HOST></i> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |
| <i>secondary</i> | Specify secondary DNS server IP address. |
| <i><IPV4_HOST></i> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |
| <i>tertiary</i> | Specify tertiary DNS server IP address. |
| <i><IPV4_HOST></i> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |

Example

```
dns server inherit  
dns server static primary 192.168.168.165
```

Syntax

```
no dns server static { primary | secondary | tertiary }
```

Mode

Static Scope

Description

Manually clear DNS server IP address.

Options

| | |
|-----------------------|--------------------------------------|
| <i>static</i> | Static DNS server. |
| <i>primary</i> | Clear primary DNS server IP address. |

secondary Clear secondary DNS server IP address.

tertiary Clear tertiary DNS server IP address.

Example

```
no dns server static primary
```

Syntax

```
wins { primary <IPV4_HOST> | secondary <IPV4_HOST> }
```

Mode

Static Scope

Description

Set the WINS server IP address.

Options

primary Primary WINS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

secondary Secondary WINS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
wins primary 192.168.168.169
```

Syntax

```
no wins { primary | secondary }
```

Mode

Static Scope

Description

Clear the WINS server IP address.

Options

primary Primary WINS server IP address.

secondary Secondary WINS server IP address.

Example

```
no wins primary
```

Syntax

```
call-manager { primary <WORD> | secondary <WORD> | tertiary <WORD> }
```

Mode

Static Scope

Description

Set VOIP call managers.

Options

- primary** Specify primary VOIP call manager IP address.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- secondary** Specify secondary VOIP call manager IP address.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- tertiary** Specify tertiary VOIP call manager address.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
call-manager manual primary 192.168.168.161
```

Syntax

```
no call-manager { primary | secondary | tertiary }
```

Mode

Static Scope

Description

Clear VOIP call managers.

Options

- primary** Clear primary VOIP call manager IP address.
- secondary** Clear secondary VOIP call manager IP address.
- tertiary** Clear tertiary VOIP call manager address.

Example

```
no call-manager primary
```

Syntax

```
network-boot { boot-file <WORD> | next-server <IPV4_HOST> | server-name <WORD> }
```

Mode

Static Scope

Description

Set network boot parameters.

Options

- boot-file** Specify boot file.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- next-server** Specify next server.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

server-name Specify server name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
network-boot next-server 192.168.168.161
```

Syntax

```
no network-boot { boot-file | next-server | server-name }
```

Mode

Static Scope

Description

Clear network boot parameters.

Options

boot-file Clear boot file.

next-server Clear next server.

server-name Clear server name.

Example

```
no network-boot next-server
```

Syntax

```
no generic-option
```

Mode

Static Scope

Description

Clear DHCP generic option group.

Example

```
no generic-option
```

Syntax

```
generic-option { group <DHCP_OPTION_GROUP> | object <DHCP_OPTION_OBJECT> }
```

Mode

Static Scope

Description

Set DHCP generic option group.

Options

group Specify generic option group.

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

object Specify generic option object.
<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
generic-option object "NetServers"
```

Syntax

```
always-send-option
```

Mode

Static Scope

Description

Enable send generic options always.

Example

```
always-send-option
```

Syntax

```
no always-send-option
```

Mode

Static Scope

Description

Disable send generic options always.

Example

```
no always-send-option
```

Syntax

```
name <DHCP_OPTION_OBJECT>
```

Mode

DHCP Option

Description

Set DHCP server option object name.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
name "LAN Specific DHCP Option"
```

Syntax

```
number <UINT8>
```

Mode

DHCP Option

Description

Set DHCP server option object number.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
number 53
```

Syntax

```
array
```

Mode

DHCP Option

Description

Enable DHCP server option array.

Example

```
array
```

Syntax

```
no array
```

Mode

DHCP Option

Description

Disable DHCP server option array.

Example

```
no array
```

Syntax

```
no value
```

Mode

DHCP Option

Description

Clear DHCP server option object value.

Example

```
no value
```

Syntax


```
value { boolean <UINT8> | domain-name <HOSTNAME> | four-byte <UINT32> | hex-string <HEX_STRING> | ip <IPV4_HOST> | one-byte <UINT8> | string <WORD> | two-byte <UINT16> }
```

Mode

DHCP Option

Description

Set DHCP server option object value.

Options

| | |
|---------------------------|---|
| boolean | Option object type: boolean. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| domain-name | Option object type: domain name. |
| <HOSTNAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i> |
| four-byte | Option object type: four byte. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: 123 |
| hex-string | Option object type: hex string. |
| <HEX_STRING> | String of hexadecimal digits. Example: 0123456989abcdef |
| ip | Option object type: IP address. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| one-byte | Option object type: one byte. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| string | Option object type: string. |
| <WORD> | Word in the form: WORD or "QUOTED STRING". Example: <i>abc</i> |
| two-byte | Option object type: two byte. |
| <UINT16> | Integer in the form: D OR 0xHHHH. Example: 123 |

Example

```
value ip 192.168.168.168
```

Syntax

```
name <DHCP_OPTION_GROUP>
```

Mode

DHCP Option Group

Description

Set DHCP server option group name.

Options

| | |
|----------------------------------|---|
| <DHCP_OPTION_GROUP> | DHCP server option group name. Example: <i>Corp Network DHCP Group</i> |
|----------------------------------|---|

Example

```
name "LAN Specific DHCP Option"
```

Syntax

```
option object <DHCP_OPTION_OBJECT>
```

Mode

DHCP Option Group

Description

Add DHCP server option object to group.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
option object "LAN Specific DHCP Option"
```

Syntax

```
no option object <DHCP_OPTION_GROUP_OBJECT>
```

Mode

DHCP Option Group

Description

Remove DHCP server option object from group.

Options

<DHCP_OPTION_GROUP_OBJECT> DHCP server option object name in specify option group.
Example: *Corp Network DHCP Group*

Example

```
no option object "LAN Specific DHCP Option"
```

Syntax

```
option group <DHCP_OPTION_GROUP>
```

Mode

DHCP Option Group

Description

Add DHCP server option group to group.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
option group group1
```

Syntax

```
no option group <DHCP_OPTION_GROUP_GROUP>
```

Mode

DHCP Option Group

Description

Remove DHCP server option group from group.

Options

<DHCP_OPTION_GROUP_GROUP> DHCP server option group name in specify option group.
Example: *Corp Network DHCP Group*

Example

```
no option group group1
```

Syntax

```
clear failover-lb [ ipv4 | ipv6 ] statistics
```

Mode

All Modes
Top Level

Description

Reset failover and load balancing statistics.

Options

ipv4 Reset interface IPv4 statistics.

ipv6 Reset interface IPv6 statistics.

statistics Reset failover and load balancing statistics.

Example

```
clear failover-lb statistics
```

Syntax

```
failover-lb
```

Mode

Config

Description

Enter failover and load balancing configuration mode.

Example

```
failover-lb
```

Syntax

```
enable
```

Mode

Failover & LB

Description

Enable failover and load balancing.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Failover & LB

Description

Disable failover and load balancing.

Example

```
no enable
```

Syntax

```
respond-to-probes [ any-tcp-syn { port <IPV4_PORT> } | disable-any-tcp-syn ]
```

Mode

Failover & LB

Description

Enable respond to probes.

Options

| | |
|---------------------------------|--|
| <i>any-tcp-syn</i> | Enable responding to any TCP SYN. |
| <i>port</i> | TCP port. |
| <i><IPV4_PORT></i> | Integer in the form: D OR 0xHHHH. Example: 80 |

| | |
|-----------------------------------|------------------------------------|
| <i>disable-any-tcp-syn</i> | Disable responding to any TCP SYN. |
|-----------------------------------|------------------------------------|

Example

```
respond-to-probes any-tcp-syn port 8080
```

Syntax

```
no respond-to-probes
```

Mode

Failover & LB

Description

Disable respond to probes.

Example

```
no respond-to-probes
```

Syntax

```
group <FLB_GROUP_NAME>
```

Mode

Failover & LB

Description

Add/Edit load balancing group.

Options

<FLB_GROUP_NAME> Failover & LB group name.
Example: *myFLBGroup*

Example

```
group " Default LB Group"
```

Syntax

```
type { basic | ratio | round-robin | spillover }
```

Mode

LB Group

Description

Configure failover and load balancing type.

Options

basic Connection use primary member unless failover occurs.

ratio Connections use members according to the set percentages.

round-robin Connections cycle through members in round robin fashion.

spillover Connections use primary member until bandwidth is exceeded.

Example

```
type round-robin
```

Syntax

```
preempt
```

Mode

LB Group

Description

Enable preempt and failback to preferred member when possible.

Example

```
preempt
```

Syntax

```
no preempt
```

Mode

LB Group

Description

Disable preempt and failback to preferred member when possible.

Example

```
no preempt
```

Syntax

```
spillover-bandwidth <UINT32>
```

Mode

LB Group

Description

Set the bandwidth at which spill-over occurs in Kbps.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
spillover-bandwidth 1000
```

Syntax

```
address-binding
```

Mode

LB Group

Description

Enable use source and destination IP address binding.

Example

```
address-binding
```

Syntax

```
no address-binding
```

Mode

LB Group

Description

Disable use source and destination IP address binding.

Example

```
no address-binding
```

Syntax

```
auto-adjust-ratio
```

Mode

LB Group

Description

Automatically adjust all member ratios so total is 100%.

Example

```
auto-adjust-ratio
```

Syntax

```
interface <FLB_GROUP_MEMBER>
```

Mode

LB Group

Description

Edit interface load balancing group member.

Options

<FLB_GROUP_MEMBER> WAN interface name.
Example: X0

Example

```
interface X2
```

Syntax

```
no interface <FLB_CURRENT_GROUP_MEMBER>
```

Mode

LB Group

Description

Remove interface load balancing group member.

Options

<FLB_CURRENT_GROUP_MEMBER> Group member name.
Example: X0

Example

```
no interface X2
```

Syntax

```
final-backup <FLB_FINAL_BACKUP>
```

Mode

LB Group

Description

Add/Replace final backup interface in load balancing group.

Options

<FLB_FINAL_BACKUP> WAN interface name.
Example: X0

Example

```
final-backup X4
```

Syntax

```
no final-backup
```

Mode

LB Group

Description

Remove final backup interface in load balancing group.

Example

```
no final-backup
```

Syntax

```
probing
```

Mode

LB Group

Description

Enter probing configuration mode.

Example

```
probing
```

Syntax

```
health-check <UINT16>
```

Mode

Probing

Description

Set the interval to perform health check of member (logical probing, physical link-check) in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
health-check 5
```

Syntax

```
missed-intervals <UINT16>
```

Mode

Probing

Description

Set the number of intervals to deactivate the member after.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
missed-intervals 6
```

Syntax

```
successful-intervals <UINT16>
```

Mode

Probing

Description

Set the number of intervals to reactivate the member after.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
successful-intervals 3
```

Syntax

```
global-responder
```

Mode

Probing

Description

Enable probing on all members using SonicWall's global responder.

Example

```
global-responder
```

Syntax

```
no global-responder
```

Mode

Probing

Description

Disable probing on all members using SonicWall's global responder and set to physical monitoring only.

Example

```
no global-responder
```

Syntax

rank <UINT32>

Mode

LB Group Member

Description

Interface rank.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

rank 2

Syntax

percent <FLB_CURRENT_GROUP_MEMBER> <UINT8>

Mode

LB Group

Description

Set the member usage percent for the interface.

Options

<FLB_CURRENT_GROUP_MEMBER> Group member name.
Example: *X0*

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

percent X1 55

Syntax

probe-type { logical | physical }

Mode

LB Group Member

Description

Configure probing type.

Options

logical Use logical/probe monitoring.

physical Use only physical checking of member status, no probing.

Example

probe-type logical

Syntax

probe-condition { always | both | either | main }

Mode

LB Group Member

Description

Configure under what condition probes succeed.

Options

always Always succeeds (no probing).

both Probes succeed when both main target and alternate target respond.

either Probes succeed when either main target or alternate target responds.

main Probes succeed when main target responds.

Example

```
probe-condition either
```

Syntax

```
main-target [ protocol { ping | tcp <IPV4_PORT> } ] [ host <HOSTNAME_MIXED> ]
```

Mode

LB Group Member

Description

Configure main target probe settings.

Options

protocol Set the probe protocol.

ping Ping probes.

tcp TCP SYN probes.

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

host Target name or IP address.

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

```
main-target protocol tcp 8080 host 192.168.168.254  
main-target protocol tcp 8080 host fe00::1
```

Syntax

```
alternate-target [ protocol { ping | tcp <IPV4_PORT> } ] [ host <HOSTNAME_MIXED> ]
```

Mode

LB Group Member

Description

Configure alternate target probe settings.

Options

protocol Set the probe protocol.

ping Ping probes.

tcp TCP SYN probes.

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

host Target Name or IP address.

<HOSTNAME_MIXED> IPV4: hostname in the form: D.D.D.D or hostname\nIPV6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

```
alternate-target protocol tcp 8080 host 192.168.168.253  
alternate-target protocol tcp 8080 host fe00::1
```

Syntax

```
default-target <IP_V4V6_HOST>
```

Mode

LB Group Member

Description

Configure the default target.

Options

<IP_V4V6_HOST> IPV4: address in the form: D.D.D.D\nIPV6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
default-target 192.168.168.254  
default-target fe00::1
```

Syntax

```
no default-target
```

Mode

LB Group Member

Description

Clear the default target.

Example

```
no default-target
```

Syntax

```
ip-helper [ ipv6 ]
```

Mode

Config

Description

Configure IP helper.

Options

ipv6 Configure IPv6 helper.

Example

```
ip-helper
```

Syntax

```
enable
```

Mode

IP Helper

Description

Enable IP helper.

Example

```
enable
```

Syntax

```
no enable
```

Mode

IP Helper

Description

Disable IP helper.

Example

```
no enable
```

Syntax

```
policy protocol dhcpv6 source { group <ADDR_GROUP_NAME> | interface <IPH_INTERFACE> | name <ADDR_NETWORK_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | zone <ZONE_NO_MULTICAST_NAME> } destination <IPV6_HOST> [ egressif <IPH_INTERFACE> ]
```

Mode

IPv6 Helper

Options

| | |
|-----------------|---|
| protocol | Specify the IP helper relay protocol. |
| dhcpv6 | Specify the IP helper dhcpv6 relay protocol |
| source | Specify source. |

| | |
|--------------------------------|---|
| group | IP helper policy source address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |

| | |
|------------------------------|---|
| interface | IP helper policy source interface. |
| <IPH_INTERFACE> | IP helper interface name. Example: <i>X1</i> |

| | |
|----------------------------------|---|
| name | IP helper policy source address object name. |
| <ADDR_NETWORK_NAME> | Network address object name. Example: <i>Sales Network</i> |

| | |
|-----------------------------|---|
| network | IP helper policy source network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

zone IP helper policy source zone.

<ZONE_NO_MULTICAST_NAME> Zone object name.
Example: *DMZ*

destination Specify destination.

<IPv6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

egressif Set Egress Interface

<IPH_INTERFACE> IP helper interface name.
Example: *X1*

Syntax

```
no policy protocol dhcpv6 source { group <ADDR_GROUP_NAME> | interface <IPH_INTERFACE> | name <ADDR_NETWORK_NAME> | network
<ADDR_NETWORK> <ADDR_MASK> | zone <ZONE_NO_MULTICAST_NAME> } destination <IPv6_HOST> [ egressif <IPH_INTERFACE> ]
```

Mode

IPv6 Helper

Options

protocol Specify the IP helper relay protocol.

dhcpv6 Specify the IP helper dhcpv6 relay protocol

source Specify source.

group IP helper policy source address object group.

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

interface IP helper policy source interface.

<IPH_INTERFACE> IP helper interface name.
Example: *X1*

name IP helper policy source address object name.

<ADDR_NETWORK_NAME> Network address object name.
Example: *Sales Network*

network IP helper policy source network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

zone IP helper policy source zone.

<ZONE_NO_MULTICAST_NAME> Zone object name.
Example: *DMZ*

destination Specify destination.

<IPv6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

egressif Set Egress Interface

<IPH_INTERFACE> IP helper interface name.
Example: *X1*

Example

```
no policy protocol dhcpv6 source "Interface X0" destination 4::4
```

Syntax

```
policy protocol <IPH_PROTOCOL> source { group <ADDR_GROUP_NAME> | interface <IPH_INTERFACE> | name <ADDR_NETWORK_NAME> | network
<ADDR_NETWORK> <ADDR_MASK> | zone <ZONE_NO_MULTICAST_NAME> } destination { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name
<ADDR_IPH_POLICY_DST_NAME> | network <ADDR_NETWORK> <ADDR_MASK> }
```

Mode

Description

Add/Edit IP helper policy.

Options

| | |
|---|--|
| protocol | Specify the IP helper relay protocol. |
| <IPH_PROTOCOL> | IP Helper relay protocol name. Example: <i>mydns</i> |
| source | Specify source. |
| group | IP helper policy source address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| interface | IP helper policy source interface. |
| <IPH_INTERFACE> | IP helper interface name. Example: <i>X1</i> |
| name | IP helper policy source address object name. |
| <ADDR_NETWORK_NAME> | Network address object name. Example: <i>Sales Network</i> |
| network | IP helper policy source network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| zone | IP helper policy source zone. |
| <ZONE_NO_MULTICAST_NAME> | Zone object name. Example: <i>DMZ</i> |
| destination | Specify destination. |
| group | Destination address object group name. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Destination address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Destination address object name. |
| <ADDR_IPH_POLICY_DST_NAME> | Host or network address object name. Example: <i>Web Server</i> |
| network | IP helper policy source network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |

Example

```
policy protocol netBIOS source name "X0 Subnet" destination name "X1 Subnet"
```

Syntax

```
no policy protocol <IPH_PROTOCOL> source { group <ADDR_GROUP_NAME> | interface <IPH_INTERFACE> | name <ADDR_NETWORK_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | zone <ZONE_NO_MULTICAST_NAME> } destination { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_IPH_POLICY_DST_NAME> | network <ADDR_NETWORK> <ADDR_MASK> }
```

Mode

IP Helper

Description

Delete IP helper policy.

Options

| | |
|---|--|
| protocol <IPH_PROTOCOL> | Specify the IP helper relay protocol. IP Helper relay protocol name. Example: <i>mydns</i> |
| source | Specify source. |
| group <ADDR_GROUP_NAME> | IP helper policy source address object group. Group address object name. Example: <i>Sales Group</i> |
| interface <IPH_INTERFACE> | IP helper policy source interface. IP helper interface name. Example: <i>X1</i> |
| name <ADDR_NETWORK_NAME> | IP helper policy source address object name. Network address object name. Example: <i>Sales Network</i> |
| network <ADDR_NETWORK> | IP helper policy source network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| zone <ZONE_NO_MULTICAST_NAME> | IP helper policy source zone. Zone object name. Example: <i>DMZ</i> |
| destination | Specify destination. |
| group <ADDR_GROUP_NAME> | Destination address object group name. Group address object name. Example: <i>Sales Group</i> |
| host <ADDR_HOST> | Destination address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <ADDR_IPH_POLICY_DST_NAME> | Destination address object name. Host or network address object name. Example: <i>Web Server</i> |
| network <ADDR_NETWORK> | IP helper policy source network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |

Example

```
no policy source "Interface X0" destination name "File Server" protocol netBIOS
```

Syntax

```
no policies
```

Mode

IP Helper

Description

Delete all IP helper Policies.

Example

```
no policies
```

Syntax

```
protocol { enable | name } <IPH_PROTOCOL>
```

Mode

IP Helper

Description

Add/Edit IP helper protocol.

Options

enable Enable specified IP helper relay protocol.

name IP helper relay protocol name.

<IPH_PROTOCOL> IP Helper relay protocol name.
Example: *mydns*

Example

```
protocol name mydns
```

Syntax

```
no protocol { enable | name } <IPH_PROTOCOL>
```

Mode

IP Helper

Description

Delete IP helper relay protocol.

Options

enable Enable IP Helper settings or objects.

name IP helper relay protocol name.

<IPH_PROTOCOL> IP Helper relay protocol name.
Example: *mydns*

Example

```
no protocol name mydns
```

Syntax

```
no protocols
```

Mode

IP Helper

Description

Delete all IP helper relay protocols.

Example

```
no protocols
```

Syntax

enable

Mode

IP Helper Policy
IPV6 Helper Policy

Description

Enable IP helper policy.

Example

enable

Syntax

no enable

Mode

IP Helper Policy
IPV6 Helper Policy

Description

Disable IP helper policy.

Example

no enable

Syntax

protocol <IPH_PROTOCOL>

Mode

IP Helper Policy

Description

Specify IP helper relay protocol associated with this policy.

Options

<IPH_PROTOCOL> IP Helper relay protocol name.
Example: *mydns*

Example

protocol mydns

Syntax

source { *group* <ADDR_GROUP_NAME> | *interface* <IPH_INTERFACE> | *name* <ADDR_NETWORK_NAME> | *network* <ADDR_NETWORK> <ADDR_MASK> | *zone* <ZONE_NO_MULTICAST_NAME> }

Mode

IP Helper Policy
IPV6 Helper Policy

Description

Specify source zone or interface for IP helper policy.

Options

| | |
|---|---|
| group <ADDR_GROUP_NAME> | IP helper policy source address object group. Group address object name. Example: <i>Sales Group</i> |
| interface <IPH_INTERFACE> | IP helper policy source interface. IP helper interface name. Example: <i>X1</i> |
| name <ADDR_NETWORK_NAME> | IP helper policy source address object name. Network address object name. Example: <i>Sales Network</i> |
| network <ADDR_NETWORK> | IP helper policy source network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| zone <ZONE_NO_MULTICAST_NAME> | IP helper policy source zone. Zone object name. Example: <i>DMZ</i> |

Example

```
source InterfaceX0
```

Syntax

```
destination { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_IPH_POLICY_DST_NAME> | network <ADDR_NETWORK> <ADDR_MASK> }
```

Mode

IP Helper Policy

Description

Specify IP helper policy destination.

Options

| | |
|---|---|
| group <ADDR_GROUP_NAME> | Destination address object group name. Group address object name. Example: <i>Sales Group</i> |
| host <ADDR_HOST> | Destination address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <ADDR_IPH_POLICY_DST_NAME> | Destination address object name. Host or network address object name. Example: <i>Web Server</i> |
| network <ADDR_NETWORK> | IP helper policy source network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |

Example

```
destination name "mydest"
```

Syntax

comment <WORD>

Mode

IP Helper Policy
IPV6 Helper Policy

Description

Specify comment for IP helper policy.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Need to allow NetBIOS between clients"

Syntax

no comment

Mode

IP Helper Policy
IPV6 Helper Policy

Description

Clear comment for IP helper policy.

Example

no comment

Syntax

destination <IPV6_HOST>

Mode

IPV6 Helper Policy

Description

Specify IPv6 helper policy destination.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

destination 1::1

Syntax

egressif <IPH_INTERFACE>

Mode

IPV6 Helper Policy

Description

Specify IPv6 helper policy egressif.

Options

<IPH_INTERFACE> IP helper interface name.
Example: *X1*

Example

Set Egress Interface

Syntax

name <IPH_PROTOCOL>

Mode

IP Helper Protocol

Description

Specify IP Helper relay protocol name.

Options

<IPH_PROTOCOL> IP Helper relay protocol name.
Example: *mydns*

Example

name mydns

Syntax

enable

Mode

IP Helper Protocol

Description

Enable IP helper relay protocol.

Example

enable

Syntax

no enable

Mode

IP Helper Protocol

Description

Disable IP helper relay protocol.

Example

no enable

Syntax

no port1

Mode

IP Helper Protocol

Description

Clear IP helper relay protocol beginning UDP port.

Example

no port1

Syntax

port1 <IPV4_PORT>

Mode

IP Helper Protocol

Description

Specify IP helper relay protocol beginning UDP port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

port1 53

Syntax

no port2

Mode

IP Helper Protocol

Description

Clear IP helper relay protocol ending UDP port.

Example

no port2

Syntax

port2 <IPV4_PORT>

Mode

IP Helper Protocol

Description

Specify IP helper relay protocol ending UDP port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

Syntax

```
timeout { 10 | 20 | 30 | 40 | 50 | 60 }
```

Mode

IP Helper Protocol

Description

Specify IP helper relay protocol timeout.

Options

10 Timeout value (in seconds).

20 Timeout value (in seconds).

30 Timeout value (in seconds).

40 Timeout value (in seconds).

50 Timeout value (in seconds).

60 Timeout value (in seconds).

Example

```
timeout 20
```

Syntax

```
source-translation
```

Mode

IP Helper Protocol

Description

Allow IP source translation for IP helper relay protocol.

Example

```
source-translation
```

Syntax

```
no source-translation
```

Mode

IP Helper Protocol

Description

Enable allowing IP source translation for IP helper relay protocol.

Example

```
no source-translation
```

Syntax

```
raw
```

Mode

IP Helper Protocol

Description

Enable raw mode for IP helper relay protocol.

Example

```
raw
```

Syntax

```
no raw
```

Mode

IP Helper Protocol

Description

Disable raw mode for IP helper relay protocol.

Example

```
no raw
```

Syntax

```
mac-ip-anti-spoof [ ipv6 ]
```

Mode

Config

Description

Configure MAC-IP anti-spoof settings.

Options

ipv6 Enter IPv6 MAC-IP anti-spoof configuration mode.

Example

```
mac-ip-anti-spoof
```

Syntax

```
interface <MAC_IP_ANTI_SPOOF_INTERFACE>
```

Mode

MAC Anti-Spoof

Description

Configure MAC-IP anti-spoof for the specified interface.

Options

<MAC_IP_ANTI_SPOOF_INTERFACE> MAC-IP anti-spoof interface.
Example: X0

Example

```
interface X1
```

Syntax

```
interface <MAC_IP_ANTI_SPOOF_INTERFACE>
```

Mode

IPv6 MAC Anti-Spoof

Description

Configure IPv6 MAC-IP anti-spoof for the specified interface.

Options

<MAC_IP_ANTI_SPOOF_INTERFACE> MAC-IP anti-spoof interface.
Example: X0

Example

```
interface X1
```

Syntax

```
cache entry <MAC_IP_ANTI_SPOOF_STATIC_IP> <MAC_IP_ANTI_SPOOF_STATIC_MAC> <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>
```

Mode

MAC Anti-Spoof

Description

Add/edit an MAC-IP anti-spoof cache entry.

Options

<MAC_IP_ANTI_SPOOF_STATIC_IP> MAC-IP anti-spoof static ip.
Example: 2001:cdba:0000:0000:0000:3257:9652

<MAC_IP_ANTI_SPOOF_STATIC_MAC> MAC-IP anti-spoof static mac.
Example: 00:0C:F1:56:98:AD

<MAC_IP_ANTI_SPOOF_STATIC_INTERFACE> MAC-IP anti-spoof enabled static interface.
Example: X0

Example

```
cache entry 10.10.10.10 00:01:02:03:04:05 X0
```

Syntax

```
no cache entry <MAC_IP_ANTI_SPOOF_STATIC_IP> <MAC_IP_ANTI_SPOOF_STATIC_MAC> <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>
```

Mode

MAC Anti-Spoof

Description

Delete an MAC-IP anti-spoof cache entry.

Options

<MAC_IP_ANTI_SPOOF_STATIC_IP> MAC-IP anti-spoof static ip.
Example: 2001:cdba:0000:0000:0000:3257:9652

<MAC_IP_ANTI_SPOOF_STATIC_MAC> MAC-IP anti-spoof static mac.
Example: 00:0C:F1:56:98:AD

<MAC_IP_ANTI_SPOOF_STATIC_INTERFACE> MAC-IP anti-spoof enabled static interface.

Example: X0

Example

```
no cache entry 10.10.10.10 00:01:02:03:04:05 X0
no cache entry 1030::C9B4:FF12:48AA:1A2B 00:01:02:03:04:05 X0
```

Syntax

```
cache entry <MAC_IP_ANTI_SPOOF_STATIC_IP> <MAC_IP_ANTI_SPOOF_STATIC_MAC> <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>
```

Mode

IPv6 MAC Anti-Spoof

Description

Add/edit an IPv6 MAC-IP anti-spoof cache entry.

Options

| | |
|--------------------------------------|--|
| <MAC_IP_ANTI_SPOOF_STATIC_IP> | MAC-IP anti-spoof static ip. Example: 2001:cdba:0000:0000:0000:0000:3257:9652 |
| <MAC_IP_ANTI_SPOOF_STATIC_MAC> | MAC-IP anti-spoof static mac. Example: 00:0C:F1:56:98:AD |
| <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE> | MAC-IP anti-spoof enabled static interface. Example: X0 |

Example

```
cache entry 1030::C9B4:FF12:48AA:1A2B 00:01:02:03:04:05 X0
```

Syntax

```
no cache entry <MAC_IP_ANTI_SPOOF_STATIC_IP> <MAC_IP_ANTI_SPOOF_STATIC_MAC> <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>
```

Mode

IPv6 MAC Anti-Spoof

Description

Delete an MAC-IP anti-spoof cache entry.

Options

| | |
|--------------------------------------|--|
| <MAC_IP_ANTI_SPOOF_STATIC_IP> | MAC-IP anti-spoof static ip. Example: 2001:cdba:0000:0000:0000:0000:3257:9652 |
| <MAC_IP_ANTI_SPOOF_STATIC_MAC> | MAC-IP anti-spoof static mac. Example: 00:0C:F1:56:98:AD |
| <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE> | MAC-IP anti-spoof enabled static interface. Example: X0 |

Example

```
no cache entry 10.10.10.10 00:01:02:03:04:05 X0
no cache entry 1030::C9B4:FF12:48AA:1A2B 00:01:02:03:04:05 X0
```

Syntax

```
no cache entries [ ipv4 | ipv6 ]
```

Mode

MAC Anti-Spoof
IPv6 MAC Anti-Spoof

Description

Delete all MAC-IP anti-spoof cache entries.

Options

ipv4 Delete all MAC-IP anti-spoof IPv4 cache entries.

ipv6 Delete all MAC-IP anti-spoof IPv6 cache entries.

Example

```
no cache entries
```

Syntax

```
router
```

Mode

MAC Anti-Spoof Cache

Description

Device is a router(a network exist behind this device).

Example

```
router
```

Syntax

```
no router
```

Mode

MAC Anti-Spoof Cache

Description

Device is not a router.

Example

```
no router
```

Syntax

```
blacklisted
```

Mode

MAC Anti-Spoof Cache

Description

Device is blacklisted.

Example

```
blacklisted
```

Syntax

```
no blacklisted
```

Mode

MAC Anti-Spoof Cache

Description

Device is not blacklisted.

Example

```
no blacklisted
```

Syntax

```
ip <MAC_IP_ANTI_SPOOF_STATIC_IP>
```

Mode

MAC Anti-Spoof Cache

Description

IP address.

Options

```
<MAC_IP_ANTI_SPOOF_STATIC_IP> MAC-IP anti-spoof static ip.  
Example: 2001:cdba:0000:0000:0000:0000:3257:9652
```

Syntax

```
mac <MAC_IP_ANTI_SPOOF_STATIC_MAC>
```

Mode

MAC Anti-Spoof Cache

Description

MAC address.

Options

```
<MAC_IP_ANTI_SPOOF_STATIC_MAC> MAC-IP anti-spoof static mac.  
Example: 00:0C:F1:56:98:AD
```

Syntax

```
interface <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>
```

Mode

MAC Anti-Spoof Cache

Description

Interface.

Options

```
<MAC_IP_ANTI_SPOOF_STATIC_INTERFACE> MAC-IP anti-spoof enabled static interface.  
Example: X0
```

Syntax

```
clear cache statistics
```

Mode

MAC Anti-Spoof

Description

Clear MAC-IP anti-spoof cache statistics.

Example

```
clear cache statistics
```

Syntax

```
clear spoof-detected-list
```

Mode

MAC Anti-Spoof

Description

Clear the whole spoof detected list.

Example

```
clear spoof-detected-list
```

Syntax

```
resolve spoof-detected-list
```

Mode

MAC Anti-Spoof

Description

Resolve names for the whole spoof detected list.

Options

spoof-detected-list Spoof detected list.

Example

```
resolve spoof-detected-list
```

Syntax

```
router
```

Mode

IPv6 MAC Anti-Spoof Cache

Description

Device is a router(a network exist behind this device).

Example

```
router
```

Syntax

no router

Mode

IPv6 MAC Anti-Spoof Cache

Description

Device is not a router.

Example

no router

Syntax

blacklisted

Mode

IPv6 MAC Anti-Spoof Cache

Description

Device is blacklisted.

Example

blacklisted

Syntax

no blacklisted

Mode

IPv6 MAC Anti-Spoof Cache

Description

Device is not blacklisted.

Example

no blacklisted

Syntax

ip <MAC_IP_ANTI_SPOOF_STATIC_IP>

Mode

IPv6 MAC Anti-Spoof Cache

Description

IP address.

Options

<MAC_IP_ANTI_SPOOF_STATIC_IP> MAC-IP anti-spoof static ip.
Example: *2001:cdba:0000:0000:0000:0000:3257:9652*

Syntax

mac <MAC_IP_ANTI_SPOOF_STATIC_MAC>

Mode

IPv6 MAC Anti-Spoof Cache

Description

MAC address.

Options

<MAC_IP_ANTI_SPOOF_STATIC_MAC> MAC-IP anti-spoof static mac.
Example: *00:0C:F1:56:98:AD*

Syntax

interface <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>

Mode

IPv6 MAC Anti-Spoof Cache

Description

Interface.

Options

<MAC_IP_ANTI_SPOOF_STATIC_INTERFACE> MAC-IP anti-spoof enabled static interface.
Example: *X0*

Syntax

clear cache statistics

Mode

IPv6 MAC Anti-Spoof

Description

Clear IPv6 MAC-IP anti-spoof cache statistics.

Example

clear cache statistics

Syntax

clear spoof-detected-list

Mode

IPv6 MAC Anti-Spoof

Description

Clear the whole IPv6 spoof detected list.

Example

clear spoof-detected-list

Syntax

```
resolve spoof-detected-list
```

Mode

IPv6 MAC Anti-Spoof

Description

Resolve names for the whole IPv6 spoof detected list.

Options

spoof-detected-list IPv6 spoof detected list.

Example

```
resolve spoof-detected-list
```

Syntax

```
enable
```

Mode

MAC Anti-Spoof IF

Description

Enable MAC-IP based anti-spoofing on this interface.

Example

```
enable
```

Syntax

```
no enable
```

Mode

MAC Anti-Spoof IF

Description

Disable MAC-IP based anti-spoofing on this interface.

Example

```
no enable
```

Syntax

```
static-arp
```

Mode

MAC Anti-Spoof IF

Description

Enable population of MAC-IP anti-spoof from static ARP entries.

Example

```
static-arp
```

Syntax

no static-arp

Mode

MAC Anti-Spoof IF

Description

Disable population of MAC-IP anti-spoof from static ARP entries.

Example

no static-arp

Syntax

dhcp-server

Mode

MAC Anti-Spoof IF

Description

Enable population of MAC-IP anti-spoof entry from DHCP lease (SonicWall's DHCP server).

Example

dhcp-server

Syntax

no dhcp-server

Mode

MAC Anti-Spoof IF

Description

Disable population of MAC-IP anti-spoof entry from DHCP lease (SonicWall's DHCP server).

Example

no dhcp-server

Syntax

dhcp-relay

Mode

MAC Anti-Spoof IF

Description

Enable population of MAC-IP anti-spoof entry from DHCP lease (DHCP relay - IP helper).

Example

dhcp-relay

Syntax

no dhcp-relay

Mode

MAC Anti-Spoof IF

Description

Disable population of MAC-IP anti-spoof entry from DHCP lease (DHCP relay - IP helper).

Example

no dhcp-relay

Syntax

arp-lock

Mode

MAC Anti-Spoof IF

Description

Enable locking of MAC-IP binding in ARP cache to prevent ARP poisoning from others.

Example

arp-lock

Syntax

no arp-lock

Mode

MAC Anti-Spoof IF

Description

Disable locking of MAC-IP binding in ARP cache.

Example

no arp-lock

Syntax

arp-watch

Mode

MAC Anti-Spoof IF

Description

Enable prevention of ARP poisoning of connected machines.

Example

arp-watch

Syntax

no arp-watch

Mode

MAC Anti-Spoof IF

Description

Disable prevention of ARP poisoning of connected machines.

Example

```
no arp-watch
```

Syntax

```
enforce-ingress
```

Mode

MAC Anti-Spoof IF

Description

Enable enforcement of ingress anti-spoof - drop packets not matching MAC-IP anti-spoof cache.

Example

```
enforce-ingress
```

Syntax

```
no enforce-ingress
```

Mode

MAC Anti-Spoof IF

Description

Disable enforcement of ingress anti-spoof.

Example

```
no enforce-ingress
```

Syntax

```
spooof-detection
```

Mode

MAC Anti-Spoof IF

Description

Enable creation of MAC-IP spooof detected list for packets failing to match anti-spoof cache.

Example

```
spooof-detection
```

Syntax

```
no spooof-detection
```

Mode

MAC Anti-Spoof IF

Description

Disable creation of MAC-IP spoof detected list for packets failing to match anti-spoof cache.

Example

```
no spoof-detection
```

Syntax

```
allow-management
```

Mode

MAC Anti-Spoof IF

Description

Enable all traffic destined to the box to be allowed without a valid MAC-IP anti-spoof cache.

Example

```
allow-management
```

Syntax

```
no allow-management
```

Mode

MAC Anti-Spoof IF

Description

Disable all traffic destined to the box to be allowed without a valid MAC-IP anti-spoof cache.

Example

```
no allow-management
```

Syntax

```
enable
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Enable MAC-IP based anti-spoofing on this interface.

Example

```
enable
```

Syntax

```
no enable
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Disable MAC-IP based anti-spoofing on this interface.

Example

```
no enable
```

Syntax

```
static-ndp
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Enable population of IPv6 MAC-IP anti-spoof from static NDP entries.

Example

```
static-ndp
```

Syntax

```
no static-ndp
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Disable population of IPv6 MAC-IP anti-spoof from static NDP entries.

Example

```
no static-ndp
```

Syntax

```
ndp-lock
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Enable locking of IPv6 MAC-IP binding in NDP cache to prevent NDP poisoning from others.

Example

```
ndp-lock
```

Syntax

```
no ndp-lock
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Disable locking of IPv6 MAC-IP binding in NDP cache.

Example

```
no ndp-lock
```

Syntax

```
enforce-ingress
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Enable enforcement of ingress anti-spoof - drop packets not matching MAC-IP anti-spoof cache.

Example

```
enforce-ingress
```

Syntax

```
no enforce-ingress
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Disable enforcement of ingress anti-spoof.

Example

```
no enforce-ingress
```

Syntax

```
spooof-detection
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Enable creation of MAC-IP spooof detected list for packets failing to match anti-spoof cache.

Example

```
spooof-detection
```

Syntax

```
no spooof-detection
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Disable creation of MAC-IP spooof detected list for packets failing to match anti-spoof cache.

Example

```
no spoof-detection
```

Syntax

```
allow-management
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Enable all traffic destined to the box to be allowed without a valid MAC-IP anti-spoof cache.

Example

```
allow-management
```

Syntax

```
no allow-management
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Disable all traffic destined to the box to be allowed without a valid MAC-IP anti-spoof cache.

Example

```
no allow-management
```

Syntax

```
no nat-policy inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ]
```

Mode

Config

Description

Delete a NAT policy.

Options

| | |
|------------------------------|---|
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| outbound | Outbound interface. |
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| source | Original source ("Any" if not specified). |
| any | Any host. |
| fqdn | FQDN. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. |

Example: *example.com*

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

translated-source Translated source ("Original" if not specified).

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

original Original source IP.

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

destination Original destination ("Any" if not specified).

any Any host.

fqdn FQDN.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

translated-destination Translated destination ("Original" if not specified).

embedded-ipv4-address Embedded ipv4 address.

group Address object group.

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

original Original destination IP.

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

service Original service ("Any" if not specified).

any Any service.

group Service group.

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

icmp-udp-tcp ICMP UDP TCP service.

name Service object name.

<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Service object protocol.

<SVC_PROTOCOL> Service protocol.
Example: *TCP*

| | |
|-------------------------------|---|
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: 80 |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: 80 |
| translated-service | Translated service ("Original" if not specified). |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: VOIP |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: HTTPS |
| original | Original service. |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: TCP |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: 80 |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: 80 |

Example

```
no nat-policy inbound X3 outbound X4 source any translated-source original destination name "Web Server Public" translated-destination name "Web Server Private" service "My Web Services" translated-service original
```

Syntax

```
no nat-policy ipv6 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ]
```

Mode

Config

Description

Delete a IPv6 NAT policy.

Options

| | |
|--------------------------------|--|
| <NAT_INTERFACE> | Interface name. Example: X0 |
| outbound | Outbound interface. |
| <NAT_INTERFACE> | Interface name. Example: X0 |
| source | Original source ("Any" if not specified). |
| any | Any host. |
| fqdn | FQDN. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: example.com |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: Sales Group |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n |

name Address object name.
<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

translated-source Translated source ("Original" if not specified).

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

original Original source IP.

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

destination Original destination ("Any" if not specified).

any Any host.

fqdn FQDN.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

translated-destination Translated destination ("Original" if not specified).

embedded-ipv4-address Embedded ipv4 address.

group Address object group.

<ADDR_GROUP_NAME> Group address object name. Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name. Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

original Original destination IP.

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

service Original service ("Any" if not specified).

any Any service.

group Service group.

<SVC_GROUP_NAME> Service object group name. Example: *VOIP*

icmp-udp-tcp ICMP UDP TCP service.

name Service object name.

<SVC_NAME> Service object name. Example: *HTTPS*

protocol Service object protocol.

<SVC_PROTOCOL> Service protocol. Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH. Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH. Example: *80*

translated-service Translated service ("Original" if not specified).

group Service group.

<SVC_GROUP_NAME> Service object group name. Example: *VOIP*

name Service object name.

| | |
|-------------------------------|---|
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| original | Original service. |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
no nat-policy ipv6 inbound X3 outbound X4 source any translated-source original destination name "Web Server Public" translated-destination name "Web Server Private" service "My Web Services" translated-service original
```

Syntax

```
no nat-policy uuid <UUID>
```

Mode

Config

Description

Delete a NAT policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
no nat-policy uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no nat-policy name <NAT_POLICY_NAME>
```

Mode

Config

Description

Delete a NAT policy by associated name.

Options

<NAT_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no nat-policy name OfficeNatPolicy
```

Syntax

```
no nat-policy ipv6 uuid <UUID>
```

Mode

Config

Description

Delete an IPv6 NAT policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: `138a224d-c4c7-d621-0a00-c0eae49ce84c`

Example

```
no nat-policy ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no nat-policy ipv6 name <NAT_POLICY_NAME>
```

Mode

Config

Description

Delete an IPv6 NAT policy by associated name.

Options

<NAT_POLICY_NAME> Word in the form: WORD or "QUOTED STRING".
Example: `abc`

Example

```
no nat-policy ipv6 name OfficeNatPolicyV6
```

Syntax

```
no nat-policies [ ipv4 | ipv6 | nat64 ]
```

Mode

Config

Description

Delete all NAT policies.

Options

ipv4 Delete all IPv4 NAT policies.

ipv6 Delete all IPv6 NAT policies.

nat64 Delete all NAT64 policies.

Example

```
no nat-policies
```

Syntax

```
nat-policy inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN>
```

```
<ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> |
network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-destination { { embedded-ipv4-address |
group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN>
<ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL>
<SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol
<SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ primitive ]
```

Mode

Config

Description

Add/edit a NAT policy and enter its configuration mode.

Options

| | |
|--------------------------------|---|
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| outbound | Outbound interface. |
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| source | Original source ("Any" if not specified). |
| any | Any host. |
| fqdn | FQDN. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| translated-source | Translated source ("Original" if not specified). |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n |

Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

original Original source IP.

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

destination Original destination ("Any" if not specified).

any Any host.

fqdn FQDN.

<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address object group.

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

translated-destination Translated destination ("Original" if not specified).

embedded-ipv4-address Embedded ipv4 address.

group Address object group.

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

| | |
|-------------------------------|--|
| original | Original destination IP. |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| service | Original service ("Any" if not specified). |
| any | Any service. |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| icmp-udp-tcp | ICMP UDP TCP service. |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| translated-service | Translated service ("Original" if not specified). |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| original | Original service. |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| primitive | Configure a primitive NAT policy in one-line. |

Example

```
nat-policy inbound X3 outbound X4 source any translated-source original destination name "Web Server Public" translated-destination name "Web Server Private" service "My Web Services" translated-service original
```

Syntax

```
nat-policy ipv6 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ primitive ]
```

Mode

Config

Description

Add/edit a IPv6 NAT policy and enter its configuration mode.

Options

| | |
|--------------------------------|--|
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| outbound | Outbound interface. |
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| source | Original source ("Any" if not specified). |
| any | Any host. |
| fqdn | FQDN. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| translated-source | Translated source ("Original" if not specified). |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| original | Original source IP. |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

destination Original destination ("Any" if not specified).

any Any host.

fqdn FQDN.

<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address object group.

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

translated-destination Translated destination ("Original" if not specified).

embedded-ipv4-address Embedded ipv4 address.

group Address object group.

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

original Original destination IP.

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

service Original service ("Any" if not specified).

| | |
|-------------------------------|---|
| any | Any service. |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| icmp-udp-tcp | ICMP UDP TCP service. |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| translated-service | Translated service ("Original" if not specified). |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| original | Original service. |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| primitive | Configure a primitive IPv6 NAT policy in one-line. |

Example

```
nat-policy ipv6 inbound X3 outbound X4 source any translated-source original destination name "Web Server Public" translated-destination name "Web Server Private" service "My Web Services" translated-service original
```

Syntax

```
nat-policy uuid <UUID>
```

Mode

Config

Description

Edit a NAT policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
nat-policy uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
nat-policy name <NAT_POLICY_NAME>
```

Mode

Config

Description

Edit a NAT policy by associated name.

Options

<NAT_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
nat-policy name OfficeNatPolicy
```

Syntax

```
nat-policy ipv6 uuid <UUID>
```

Mode

Config

Description

Edit an IPv6 NAT policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
nat-policy ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
nat-policy ipv6 name <NAT_POLICY_NAME>
```

Mode

Config

Description

Edit an IPv6 NAT policy by associated name.

Options

<NAT_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
nat-policy ipv6 name OfficeNatPolicyV6
```

Syntax

```
no nat-policy nat64 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-
```

```
source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range
<ADDR_BEGIN> <ADDR_END> } } } [ pref64 { { any | group <ADDR_GROUP_NAME> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> }
} ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network
<ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-
tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group
<SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ]
```

Mode

Config

Description

Delete a NAT64 policy.

Options

| | |
|--------------------------------|---|
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| outbound | Outbound interface. |
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| source | IPv6 original source. |
| any | Any host. |
| fqdn | FQDN. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| translated-source | Translated IPv4 source. |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n |

| | |
|--------------------------------|--|
| | Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| original | Original source IP. |
| range | Address object range. |
| <ADDR_BEGIN> | IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| pref64 | NAT64 prefix. |
| any | Any host. |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| translated-destination | Translated destination. |
| embedded-ipv4-address | Embedded ipv4 address. |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| original | Original destination IP. |
| range | Address object range. |
| <ADDR_BEGIN> | IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| service | Original service. |
| any | Any service. |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |

| | |
|----------------------------------|---|
| <i>icmp-udp-tcp</i> | ICMP UDP TCP service. |
| <i>name</i> | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| <i>protocol</i> | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <i>translated-service</i> | Translated service. |
| <i>group</i> | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| <i>name</i> | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| <i>original</i> | Original service. |
| <i>protocol</i> | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
no nat-policy nat64 inbound any outbound any source any translated-source X1 pref64 name nat64A0 translated-destination embedded-ipv4-address service icmp-udp-tcp translated-service original
```

Syntax

```
no nat-policy nat64 uuid <UUID>
```

Mode

Config

Description

Delete a NAT64 policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
no nat-policy nat64 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no nat-policy nat64 name <NAT_POLICY_NAME>
```

Mode

Config

Description

Delete an NAT64 policy by associated name.

Options

<NAT_POLICY_NAME> Word in the form: WORD or "QUOTED STRING".
Example: *abc*

Example

```
no nat-policy nat64 name OfficeNatPolicy64
```

Syntax

```
nat-policy nat64 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ pref64 { { any | group <ADDR_GROUP_NAME> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> } } ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ primitive ]
```

Mode

Config

Description

Add/edit a NAT64 policy and enter its configuration mode.

Options

| | |
|--------------------------------|--|
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| outbound | Outbound interface. |
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| source | IPv6 original source. |
| any | Any host. |
| fqdn | FQDN. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |

translated-source Translated IPv4 source.

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

original Original source IP.

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

pref64 NAT64 prefix.

any Any host.

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

name Address object name.
<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

translated-destination Translated destination.

embedded-ipv4-address Embedded ipv4 address.

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.

Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

| | |
|-------------------------------|--|
| original | Original destination IP. |
| range | Address object range. |
| <ADDR_BEGIN> | IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| service | Original service. |
| any | Any service. |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| icmp-udp-tcp | ICMP UDP TCP service. |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| translated-service | Translated service. |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| original | Original service. |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| primitive | Configure a primitive NAT64 policy in one-line. |

Example

```
nat-policy nat64 inbound any outbound any source any translated-source X1 pref64 name nat64AO translated-destination embedded-  
ipv4-address service icmp-udp-tcp translated-service original
```

Syntax

```
nat-policy nat64 uuid <UUID>
```

Mode

Config

Description

Edit an NAT64 NAT policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
nat-policy nat64 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
nat-policy nat64 name <NAT_POLICY_NAME>
```

Mode

Config

Description

Edit an NAT64 policy by associated name.

Options

<NAT_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
nat-policy nat64 name OfficeNatPolicy64
```

Syntax

```
uuid <UUID>
```

Mode

NAT

Description

Nat policy UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

NAT

Description

Clear nat policy UUID.

Example

```
no uuid
```

Syntax

`uuid <UUID>`

Mode

IPv6 NAT

Description

Nat policy UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: `138a224d-c4c7-d621-0a00-c0eae49ce84c`

Example

`uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c`

Syntax

`no uuid`

Mode

IPv6 NAT

Description

Clear nat policy UUID.

Example

`no uuid`

Syntax

`uuid <UUID>`

Mode

NAT64 Policy

Description

Nat policy UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: `138a224d-c4c7-d621-0a00-c0eae49ce84c`

Example

`uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c`

Syntax

`no uuid`

Mode

NAT64 Policy

Description

Clear nat policy UUID.

Example

```
no uuid
```

Syntax

```
name <WORD>
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Nat policy name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name OfficeNatPolicy
```

Syntax

```
no name
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Clear NAT policy name.

Example

```
name OfficeNatPolicy
```

Syntax

```
priority { auto | manual <UINT32> }
```

Mode

NAT
IPv6 NAT

Description

Set NAT policy priority.

Options

auto Set auto priority(priority = 0) for NAT policy.

manual Set manual priority for NAT policy.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
priority auto  
priority manual 1
```

Syntax

```
comment <WORD>
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Specify a comment for this NAT policy.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
comment "Public HTTP Server"
```

Syntax

```
no comment
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Clear NAT policy comment.

Example

```
no comment
```

Syntax

```
enable
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Enable NAT policy.

Example

```
enable
```

Syntax

no enable

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Enable NAT policy.

Example

no enable

Syntax

inbound <NAT_INTERFACE>

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Specify the inbound interface for the NAT policy.

Options

<NAT_INTERFACE> Interface name.
Example: *X0*

Example

inbound X1

Syntax

outbound <NAT_INTERFACE>

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Specify the outbound interface for the NAT policy.

Options

<NAT_INTERFACE> Interface name.
Example: *X0*

Example

outbound X0

Syntax

destination { { *any* | *fqdn* <ADDR_FQDN> | *group* <ADDR_GROUP_NAME> | *host* <ADDR_HOST> | *name* <ADDR_NAME> | *network* <ADDR_NETWORK>
<ADDR_MASK> | *range* <ADDR_BEGIN> <ADDR_END> } }

Mode

Description

Specify the original destination for the NAT policy.

Options

| | |
|--------------------------------|--|
| any | Any host. |
| fqdn | FQDN. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
destination name "Web Server Public"
```

Syntax

```
source { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK>  
<ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

Description

Specify the original source for the NAT policy.

Options

| | |
|--------------------------|--|
| any | Any host. |
| fqdn | FQDN. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address object group. |

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

source any

Syntax

```
service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Specify the original service for the NAT policy.

Options

any Any service.

group Service group.

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

icmp-udp-tcp ICMP UDP TCP service.

name Service object name.

<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Service object protocol.

<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

service name "My Web Services"

Syntax

reflexive

Mode

NAT
IPv6 NAT

Description

Configure a reflexive rule.

Example

reflexive

Syntax

no reflexive

Mode

NAT
IPv6 NAT

Description

Disable configuration of a reflexive rule.

Example

no reflexive

Syntax

```
translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Specify the translated destination for the NAT policy.

Options

| | |
|---|---|
| <i>embedded-ipv4-address</i> | Embedded ipv4 address. |
| <i>group</i> <ADDR_GROUP_NAME> | Address object group. Group address object name. Example: <i>Sales Group</i> |
| <i>host</i> <ADDR_HOST> | Address object host. IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <i>name</i> <ADDR_NAME> | Address object name. Address object name. Example: <i>Web Server</i> |

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

original Original destination IP.

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

translated-destination name "Web Server Private"

Syntax

```
translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

NAT
IPv6 NAT

Description

Specify the translated source for the NAT policy.

Options

group Address object group.

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

original Original source IP.

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

translated-source original

Syntax

```
translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Specify the translated service for the NAT policy.

Options

| | |
|-------------------------------|---|
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| original | Original service. |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
translated-service original
```

Syntax

```
override-mac <MAC>
```

Mode

NAT

Description

Specify the override mac for the NAT policy.

Options

<MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
override-mac 00:17:C5:0F:73:F4
```

Syntax

```
source { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

NAT64 Policy

Description

Specify the original source for the NAT64 policy.

Options

| | |
|--------------------------------|--|
| any | Any host. |
| fqdn | FQDN. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
source any
```

Syntax

```
translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

NAT64 Policy

Description

Specify the translated source for the NAT64 policy.

Options

| | |
|--------------------------------|--|
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

original Original source IP.

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
translated-source "X1 IP"
```

Syntax

```
pref64 { { any | group <ADDR_GROUP_NAME> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> } }
```

Mode

NAT64 Policy

Description

Specify the prefix for the NAT64 policy.

Options

any Any host.

group Address object group.

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

Example

```
pref64 name nat64A0
```

Syntax

```
virtual-group { any | id <VIRTUAL_GROUP_ID> }
```

Mode

NAT

Description

Specify virtual group for the NAT policy.

Options

| | |
|---------------------------------|---|
| any | Any virtual group. |
| id | Virtual group id. |
| <VIRTUAL_GROUP_ID> | Integer in the form: D OR 0xHH. Example: 1 |

Example

```
virtual-group any
```

Syntax

```
high-availability
```

Mode

NAT
IPv6 NAT

Description

NAT high availability and load balancing configuration mode.

Example

```
high-availability
```

Syntax

```
nat-method { block-remap | random-distribution | round-robin | sticky-ip | symmetrical-remap }
```

Mode

NAT
IPv6 NAT

Description

Set the NAT destination translation method.

Options

| | |
|----------------------------|----------------------|
| block-remap | Block remap. |
| random-distribution | Random distribution. |
| round-robin | Round robin. |
| sticky-ip | Sticky IP. |
| symmetrical-remap | Symmetrical remap. |

Example

```
nat-method sticky-ip
```

Syntax

```
source-port-remap
```

Mode

NAT

Description

Enable source port remap.

Example

```
source-port-remap
```

Syntax

```
no source-port-remap
```

Mode

NAT

Description

Disable source port remap.

Example

```
no source-port-remap
```

Syntax

```
probing
```

Mode

High Availability

Description

Enable HA probing and enter configuration mode.

Example

```
probing
```

Syntax

```
no probing
```

Mode

High Availability

Description

Disable HA probing.

Example

```
no probing
```

Syntax

```
probe-every <UINT16>
```

Mode

High Availability Probe

Description

Set probe interval (in seconds).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
probe-every 5
```

Syntax

```
probe-type { icmp-ping | tcp <IPV4_PORT> }
```

Mode

High Availability Probe

Description

Set probe IP type.

Options

icmp-ping ICMP ping probe.

tcp TCP probe.

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
probe-type tcp 80
```

Syntax

```
reply-timeout <UINT16>
```

Mode

High Availability Probe

Description

Set reply timeout (in seconds).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
reply-timeout 5
```

Syntax

```
deactivate-after <UINT16>
```

Mode

High Availability Probe

Description

Set number of missed probes required before deactivating the NAT policy.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
deactivate-after 4
```

Syntax

```
reactivate-after <UINT16>
```

Mode

High Availability Probe

Description

Set number of successful probes required before reactivating the NAT policy.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
reactivate-after 3
```

Syntax

```
rst-as-miss
```

Mode

High Availability Probe

Description

Enable count RST response as miss.

Example

```
rst-as-miss
```

Syntax

```
no rst-as-miss
```

Mode

High Availability Probe

Description

Disable count RST response as miss.

Example

```
no rst-as-miss
```

Syntax

```
port-probing
```

Mode

High Availability Probe

Description

Enable port probing.

Example

```
port-probing
```

Syntax

```
no port-probing
```

Mode

High Availability Probe

Description

Disable port probing.

Example

```
no port-probing
```

Syntax

```
no network-monitor policy [ ipv6 ] <NETMON_NAME>
```

Mode

Config

Description

Delete network monitor policy.

Options

ipv6 Delete IPv6 network monitor policy.
<NETMON_NAME> Atom Object name.
Example: *Web Services Monitor*

Example

```
no network-monitor policy "Remote Servers"  
no network-monitor policy ipv6 "IPv6 Remote Servers"
```

Syntax

```
no network-monitor policies [ ipv6 ]
```

Mode

Config

Description

Delete all network monitor policies.

Options

ipv6 Delete IPv6 network monitor policies.

Example

```
no network-monitor policies  
no network-monitor policies ipv6
```

Syntax

```
clear network-monitor statistics
```

Mode

Config

Description

Clear network monitor statistics.

Example

```
clear network-monitor statistics
```

Syntax

```
network-monitor policy [ ipv6 ] <NETMON_NAME>
```

Mode

Config

Description

Add/edit a network monitor policy.

Options

ipv6 Add/edit an IPv6 network monitor policy.
<NETMON_NAME> Atom Object name.
Example: *Web Services Monitor*

Example

```
network-monitor policy "Remote Servers"  
network-monitor policy ipv6 "IPv6 Remote Servers"
```

Syntax

```
name <NETMON_NAME>
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Edit a network monitor policy name.

Options

<NETMON_NAME> Atom Object name.
Example: *Web Services Monitor*

Example

```
name "Remote Servers"
```

Syntax

```
no probe target
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Clear the probe target.

Example

```
no probe target
```

Syntax

```
probe target { fqdn <ADDR_FQDN> | group <ADDR_FHR_GROUP> | host <ADDR_HOST> | name <ADDR_FQDN_HOST_RANGE_NAME> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set the probe target.

Options

| | |
|--|---|
| fqdn <ADDR_FQDN> | Set the probe target to FQDN address. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group <ADDR_FHR_GROUP> | Set the probe target to group address object. FQDN/host/range group address object name. Example: <i>Web Server Group</i> |
| host <ADDR_HOST> | Set the probe target to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <ADDR_FQDN_HOST_RANGE_NAME> | Set the probe target to named address object. FQDN/host/range address object name. Example: <i>Web Server</i> |
| range <ADDR_BEGIN> <ADDR_END> | Set the probe target to range of addresses. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
probe target name "Remote Target"
```

Syntax

```
next-hop { host <ADDR_HOST> | name <ADDR_HOST_NAME> }
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set the next hop gateway.

Options

| | |
|-------------------------------|--|
| host | Set the next hop to host address. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Set the next hop to named address object. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |

Example

```
next-hop name "X1 Default Gateway"
```

Syntax

```
no next-hop
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Clear the next hop gateway.

Example

```
no next-hop
```

Syntax

```
local-ip { host <NETMON_HOST> | name <ADDR_HOST_NAME> }
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set the local IP address.

Options

| | |
|-------------------------------|--|
| host | Set the local IP to host address. |
| <NETMON_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Set the local IP to named address object. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |

Example

```
local-ip name "X1 IP"
```

Syntax

```
no local-ip
```

Mode

Description

Clear the local IP address.

Example

```
no local-ip
```

Syntax

```
outbound-interface <NETMON_INTERFACE>
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set outbound interface.

Options

<NETMON_INTERFACE> Interface name.
Example: *X0*

Example

```
outbound-interface X2
```

Syntax

```
probe type { ping [ explicit | non-explicit ] | tcp { [ explicit | non-explicit ] port <IPV4_PORT> } }
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set network monitor policy probe type.

Options

ping Ping probe.

explicit Ping probe using explicit route.

non-explicit Ping probe.

tcp TCP probe.

explicit TCP probe using explicit route.

non-explicit TCP probe.

port Set TCP probe port.

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
probe type ping
probe type ping explicit
probe type tcp explicit port 80
probe type tcp port 80
```

Syntax

probe interval <UINT16>

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set probe host interval.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

probe interval 5

Syntax

reply-timeout <UINT8>

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set probing reply timeout.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

reply-timeout 2

Syntax

interval missed <UINT8>

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Probe state is set to DOWN after specified number of missed intervals.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

interval missed 3

Syntax

```
interval successful <UINT8>
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Probe state is set to UP after specified number of successful intervals.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
interval successful 3
```

Syntax

```
must-respond
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Enable all hosts must respond.

Example

```
must-respond
```

Syntax

```
no must-respond
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Disable all hosts must respond.

Example

```
no must-respond
```

Syntax

```
rst-as-miss
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Enable RST response counts as miss.

Example

rst-as-miss

Syntax

no rst-as-miss

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Disable RST response counts as miss.

Example

no rst-as-miss

Syntax

comment <WORD>

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set network monitor policy comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Remote Servers"

Syntax

no comment

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Clear network monitor policy comment.

Example

no comment

Syntax

routing

Mode

Config

Description

Enter routing configuration mode.

Example

```
routing
```

Syntax

```
mode { advanced | simple }
```

Mode

Routing

Description

Routing mode.

Options

advanced Advanced routing.

simple Simple RIP advertisement.

Example

```
mode simple  
mode advanced
```

Syntax

```
nsm
```

Mode

Routing

Description

Configure network services module (NSM) protocol.

Example

```
nsm
```

Syntax

```
ospf
```

Mode

Routing

Description

Configure open shortest path first (OSPF) protocol.

Example

```
ospf
```

Syntax

rip

Mode

Routing

Description

Configure routing information protocol (RIP).

Example

rip

Syntax

ospfv3

Mode

Routing

Description

Configure Open Shortest Path First (OSPFv3) protocol.

Example

ospfv3

Syntax

ripng

Mode

Routing

Description

Configure Routing Information Protocol (RIPng).

Example

ripng

Syntax

no bgp

Mode

Routing

Description

Disable border gateway protocol (BGP).

Example

no bgp

Syntax

bgp

Mode

Routing

Description

Enable and configure border gateway protocol (BGP).

Example

```
bgp
```

Syntax

```
default-route-metric <UINT8>
```

Mode

Routing

Description

Set metric for default routes received from advanced routing protocols.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
default-route-metric 110
```

Syntax

```
metric-priority
```

Mode

Routing

Description

Enable prioritize routes by metric within route classes.

Example

```
metric-priority
```

Syntax

```
no metric-priority
```

Mode

Routing

Description

Disable prioritize routes by metric within route classes.

Example

```
no metric-priority
```

Syntax

```
no route-policy interface <ROUTING_INTERFACE_NAME> metric <UINT8> [ source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> |
name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { {
any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name <ROUTING_POLICY_DEST_FHNR_NAME> | network
<ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ app <ROUTING_POLICY_APP_MATCH_OBJECT> | service { { any | group
<SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ gateway { { default | host
<ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ path-selection-profile <ROUTE_PATH_SELECTION_PROFILE_NAME> ] [ nexthop-number <UINT8>
interface2 <ROUTING_INTERFACE_NAME> [ gateway2 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ interface3
<ROUTING_INTERFACE_NAME> [ gateway3 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] [ interface4
<ROUTING_INTERFACE_NAME> [ gateway4 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] ]
```

Mode

Config
Routing

Description

Delete a route policy.

Options

| | |
|---|--|
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| metric | Route policy metric. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| source | Route policy source. |
| any | Any host. |
| group | Address group name. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NETWORK_RANGE_NAME> | Host/network/range address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| destination | Route policy destination. |
| any | Any host. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |

| | |
|--|---|
| <ROUTING_POLICY_DEST_FHNR_NAME> | FQDN/host/network/range address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| app | Route policy application match-object. |
| <ROUTING_POLICY_APP_MATCH_OBJECT> | Route application match-object name. Example: <i>abc</i> |
| service | Route policy service. |
| any | Any service. |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| gateway | Route policy gateway. |
| default | Default gateway 0.0.0.0/: |
| host | Gateway IP. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| path-selection-profile | Route policy SD-WAN path selection profile. |
| <ROUTE_PATH_SELECTION_PROFILE_NAME> | Word in the form: WORD or "QUOTED STRING". Example: <i>abc</i> |
| nextthop-number | the nextthop number. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| interface2 | Route policy 2nd interface. |
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| gateway2 | Route policy 2nd gateway. |
| default | Default gateway 0.0.0.0/: |
| host | Gateway IP. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |

| | |
|---------------------------------------|--|
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| interface3 | Route policy 3rd interface. |
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| gateway3 | Route policy 2nd gateway. |
| default | Default gateway 0.0.0.0/:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| interface4 | Route policy 4th interface. |
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| gateway4 | Route policy 4th gateway. |
| default | Default gateway 0.0.0.0/:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |

Example

```
no route-policy interface X4 metric 255 service name "FTP" gateway default
```

Syntax

```
no route-policy ipv6 interface <ROUTING_INTERFACE_NAME> metric <UINT8> [ source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name <ROUTING_POLICY_DEST_FHNR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ app <ROUTING_POLICY_APP_MATCH_OBJECT> | service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ gateway { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ nexthop-number <UINT8> interface2 <ROUTING_INTERFACE_NAME> [ gateway2 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ interface3 <ROUTING_INTERFACE_NAME> [ gateway3 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] [ interface4 <ROUTING_INTERFACE_NAME> [ gateway4 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] ]
```

Mode

Config
Routing

Description

Delete an IPv6 route policy.

Options

| | |
|---------------------------------------|---|
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| metric | Route policy metric. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| source | Route policy source. |
| any | Any host. |
| group | Address group name. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_HOST_NETWORK_RANGE_NAME> Host/network/range address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

destination Route policy destination.

any Any host.

fqdn Address object full qualified domain name.

<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address group name.

<ADDR_GROUP_NAME_WITH_MIXED> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ROUTING_POLICY_DEST_FHNR_NAME> FQDN/host/network/range address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

app Route policy application match-object.

<ROUTING_POLICY_APP_MATCH_OBJECT> Route application match-object name.
Example: *abc*

service Route policy service.

any Any service.

group Service group.

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

name Service object name.
<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Service object protocol.
<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

gateway Route policy gateway.

default Default gateway 0.0.0.0/::

host Gateway IP.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_HOST_NAME> Host address object name.
Example: *Web Server*

nexthop-number the nexthop number.
<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

interface2 Route policy 2nd interface.
<ROUTING_INTERFACE_NAME> Route interface name.
Example: *X0*

gateway2 Route policy 2nd gateway.

default Default gateway 0.0.0.0/::

host Gateway IP.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_HOST_NAME> Host address object name.
Example: *Web Server*

interface3 Route policy 3rd interface.
<ROUTING_INTERFACE_NAME> Route interface name.
Example: *X0*

gateway3 Route policy 2nd gateway.

default Default gateway 0.0.0.0/::

host Gateway IP.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_HOST_NAME> Host address object name.
Example: *Web Server*

interface4 Route policy 4th interface.
<ROUTING_INTERFACE_NAME> Route interface name.
Example: *X0*

gateway4 Route policy 4th gateway.

default Default gateway 0.0.0.0/::

host Gateway IP.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_HOST_NAME> Host address object name.
Example: *Web Server*

Example

```
no route-policy ipv6 interface X4 metric 255 service name "FTP" gateway default
```

Syntax

```
no route-policy uuid <UUID>
```

Mode

Config
Routing

Description

Delete a route policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
no route-policy uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no route-policy ipv6 uuid <UUID>
```

Mode

Config
Routing

Description

Delete an IPv6 route policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
no route-policy ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no route-policies [ ipv4 | ipv6 ]
```

Mode

Config
Routing

Description

Delete all route policies.

Options

ipv4 Delete all IPv4 route policies.

ipv6 Delete all IPv6 route policies.

Example

```
no route-policies
no route-policies ipv4
no route-policies ipv6
```

Syntax

```
route-policy interface <ROUTING_INTERFACE_NAME> metric <UINT8> [ source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> |
name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { {
any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name <ROUTING_POLICY_DEST_FHNR_NAME> | network
<ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ app <ROUTING_POLICY_APP_MATCH_OBJECT> | service { { any | group
<SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ gateway { { default | host
<ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ path-selection-profile <ROUTE_PATH_SELECTION_PROFILE_NAME> ] [ nexthop-number <UINT8>
interface2 <ROUTING_INTERFACE_NAME> [ gateway2 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ interface3
<ROUTING_INTERFACE_NAME> [ gateway3 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ interface4
<ROUTING_INTERFACE_NAME> [ gateway4 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] [ primitive ]
```

Mode

Config
Routing

Description

Add/edit a route policy.

Options

| | |
|---|---|
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| metric | Route policy metric. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| source | Route policy source. |
| any | Any host. |
| group | Address group name. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NETWORK_RANGE_NAME> | Host/network/range address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| destination | Route policy destination. |
| any | Any host. |
| fqdn | Address object full qualified domain name. |

| | |
|--|---|
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ROUTING_POLICY_DEST_FHNR_NAME> | FQDN/host/network/range address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| app | Route policy application match-object. |
| <ROUTING_POLICY_APP_MATCH_OBJECT> | Route application match-object name. Example: <i>abc</i> |
| service | Route policy service. |
| any | Any service. |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| gateway | Route policy gateway. |
| default | Default gateway 0.0.0.0/:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| path-selection-profile | Route policy SD-WAN path selection profile. |
| <ROUTE_PATH_SELECTION_PROFILE_NAME> | Word in the form: WORD or "QUOTED STRING". Example: <i>abc</i> |
| next-hop-number | the next-hop number. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |

| | |
|---------------------------------------|---|
| interface2 | Route policy 2nd interface. |
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| gateway2 | Route policy 2nd gateway. |
| default | Default gateway 0.0.0.0/:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| interface3 | Route policy 3rd interface. |
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| gateway3 | Route policy 2nd gateway. |
| default | Default gateway 0.0.0.0/:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| interface4 | Route policy 4th interface. |
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| gateway4 | Route policy 4th gateway. |
| default | Default gateway 0.0.0.0/:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| primitive | Configure a primitive route policy in one-line. |

Example

```
route-policy interface X4 metric 255 source any destination any service any gateway default
```

Syntax

```
route-policy ipv6 interface <ROUTING_INTERFACE_NAME> metric <UINT8> [ source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name <ROUTING_POLICY_DEST_FHNR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ app <ROUTING_POLICY_APP_MATCH_OBJECT> | service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ gateway { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ nexthop-number <UINT8> interface2 <ROUTING_INTERFACE_NAME> [ gateway2 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] [ interface3 <ROUTING_INTERFACE_NAME> [ gateway3 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] [ interface4 <ROUTING_INTERFACE_NAME> [ gateway4 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] [ primitive ]
```

Mode

Config
Routing

Description

Add/edit a IPv6 route policy.

Options

| | |
|--|--|
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| metric | Route policy metric. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| source | Route policy source. |
| any | Any host. |
| group | Address group name. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NETWORK_RANGE_NAME> | Host/network/range address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| destination | Route policy destination. |
| any | Any host. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ROUTING_POLICY_DEST_FHNR_NAME> | FQDN/host/network/range address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n |

Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

| | |
|--|---|
| app | Route policy application match-object. |
| <ROUTING_POLICY_APP_MATCH_OBJECT> | Route application match-object name. Example: <i>abc</i> |
| service | Route policy service. |
| any | Any service. |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| gateway | Route policy gateway. |
| default | Default gateway 0.0.0.0/:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| next-hop-number | the next-hop number. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| interface2 | Route policy 2nd interface. |
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| gateway2 | Route policy 2nd gateway. |
| default | Default gateway 0.0.0.0/:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| interface3 | Route policy 3rd interface. |
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| gateway3 | Route policy 2nd gateway. |
| default | Default gateway 0.0.0.0/:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| interface4 | Route policy 4th interface. |
| <ROUTING_INTERFACE_NAME> | Route interface name. |

| | |
|-------------------------------|---|
| gateway4 | Example: <i>X0</i> Route policy 4th gateway. |
| default | Default gateway 0.0.0.0/: |
| host | Gateway IP. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| primitive | Configure a primitive IPv6 route policy in one-line. |

Example

```
route-policy ipv6 interface X4 metric 255 source any destination any service any gateway default
```

Syntax

```
route-policy uuid <UUID>
```

Mode

Config
Routing

Description

Edit a route policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
route-policy uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
uuid <UUID>
```

Mode

Route Policy

Description

Route policy UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid 3824334935410777187
```

Syntax

no uuid

Mode

Route Policy

Description

Clear route policy UUID.

Example

no uuid

Syntax

route-policy ipv6 uuid <UUID>

Mode

Config
Routing

Description

Edit an IPv6 route policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

route-policy ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

uuid <UUID>

Mode

IPv6 Route Policy

Description

Route policy UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

Route Policy

Description

Clear route policy UUID.

Example

```
no uuid
```

Syntax

```
source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK>  
<ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy source.

Options

| | |
|---|--|
| any | Any host. |
| group <ADDR_GROUP_NAME> | Address group name. Group address object name. Example: <i>Sales Group</i> |
| host <ADDR_HOST> | Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <ADDR_HOST_NETWORK_RANGE_NAME> | Address object name. Host/network/range address object name. Example: <i>Web Server</i> |
| network <ADDR_NETWORK> <ADDR_MASK> | Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:efe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> <ADDR_END> | Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:efe\n</i> |

Example

```
source name "X0 Default Gateway"  
source group "Corp LAN2"  
source any
```

Syntax

```
destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name  
<ROUTING_POLICY_DEST_FHNR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy destination.

Options

| | |
|---|---|
| any | Any host. |
| fqdn <ADDR_FQDN> | Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group <ADDR_GROUP_NAME_WITH_MIXED> | Address group name. Group address object name. Example: <i>Sales Group</i> |
| host <ADDR_HOST> | Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <ROUTING_POLICY_DEST_FHNR_NAME> | Address object name. FQDN/host/network/range address object name. Example: <i>Web Server</i> |
| network <ADDR_NETWORK> <ADDR_MASK> | Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> <ADDR_END> | Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
destination name "X0 Default Gateway"  
destination group "Corp LAN2"  
destination any
```

Syntax

```
service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy service.

Options

| | |
|----------------------------------|---|
| any | Any service. |
| group <SVC_GROUP_NAME> | Service group. Service object group name. Example: <i>VOIP</i> |
| name <SVC_NAME> | Service object name. Service object name. Example: <i>HTTPS</i> |

| | |
|-------------------------------|---|
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
service name "LAN Service"
```

Syntax

```
app <ROUTING_POLICY_APP_MATCH_OBJECT>
```

Mode

Route Policy
IPV6 Route Policy

Description

set route policy application match-object.

Options

| | |
|--|---|
| <ROUTING_POLICY_APP_MATCH_OBJECT> | Route application match-object name. Example: <i>abc</i> |
|--|---|

Example

```
app IM_App
```

Syntax

```
gateway { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } }
```

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy gateway.

Options

| | |
|-------------------------------|---|
| default | Default gateway 0.0.0.0/:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |

Example

```
gateway name "X0 Default Gateway"  
gateway default
```

Syntax

```
path-selection-profile <ROUTE_PATH_SELECTION_PROFILE_NAME>
```

Mode

Route Policy

Description

Set route policy SD-WAN path selection profile.

Options

<ROUTE_PATH_SELECTION_PROFILE_NAME> Word in the form: WORD or "QUOTED STRING".
Example: *abc*

Example

```
path-selection-profile sdwanProfile
```

Syntax

```
no path-selection-profile
```

Mode

Route Policy

Description

Clear route policy SD-WAN path selection profile.

Example

```
no path-selection-profile
```

Syntax

```
interface <ROUTING_INTERFACE_NAME>
```

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy interface.

Options

<ROUTING_INTERFACE_NAME> Route interface name.
Example: *X0*

Example

```
interface X2
```

Syntax

```
gateway2 { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> }
```

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy 2nd gateway.

Options

| | |
|-------------------------------|--|
| default | Default gateway 0.0.0.0/:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |

Example

```
gateway name "X0 Default Gateway"  
gateway default
```

Syntax

```
interface2 <ROUTING_INTERFACE_NAME>
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy 2nd interface.

Options

| | |
|---------------------------------------|---|
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
|---------------------------------------|---|

Example

```
interface X2
```

Syntax

```
gateway3 { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> }
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy 3rd gateway.

Options

| | |
|-------------------------------|--|
| default | Default gateway 0.0.0.0/:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |

Example


```
gateway name "X0 Default Gateway"  
gateway default
```

Syntax

```
interface3 <ROUTING_INTERFACE_NAME>
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy 3rd interface.

Options

<ROUTING_INTERFACE_NAME> Route interface name.
Example: *X0*

Example

```
interface X2
```

Syntax

```
gateway4 { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> }
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy 4th gateway.

Options

default Default gateway 0.0.0.0/::

host Gateway IP.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_HOST_NAME> Host address object name.
Example: *Web Server*

Example

```
gateway name "X0 Default Gateway"  
gateway default
```

Syntax

```
interface4 <ROUTING_INTERFACE_NAME>
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route 4th policy interface.

Options

<ROUTING_INTERFACE_NAME> Route interface name.
Example: *X0*

Example

```
interface X2
```

Syntax

```
nexthop-number <UINT8>
```

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy nexthop number.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
nexthop-number 2
```

Syntax

```
metric <UINT8>
```

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy metric.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
metric 1
```

Syntax

```
no name
```

Mode

Route Policy
IPV6 Route Policy

Description

Clear route policy name.

Example

```
no name
```

Syntax

name <WORD>

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name "Route to Corporate Servers"

Syntax

no comment

Mode

Route Policy
IPV6 Route Policy

Description

Clear route policy comment.

Example

no comment

Syntax

comment <WORD>

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Route to Corporate Servers"

Syntax

disable-on-interface-down

Mode

Route Policy
IPV6 Route Policy

Description

Disable route when the interface is disconnected.

Example

```
disable-on-interface-down
```

Syntax

```
no disable-on-interface-down
```

Mode

Route Policy
IPV6 Route Policy

Description

Leave route enabled when the interface is disconnected.

Example

```
no disable-on-interface-down
```

Syntax

```
vpn-precedence
```

Mode

Route Policy
IPV6 Route Policy

Description

Allow VPN path to take precedence.

Example

```
vpn-precedence
```

Syntax

```
no vpn-precedence
```

Mode

Route Policy
IPV6 Route Policy

Description

Disable allow VPN path to take precedence.

Example

```
no vpn-precedence
```

Syntax

```
tcp-acceleration
```

Mode

Route Policy

Description

Enable permit TCP acceleration.

Example

```
tcp-acceleration
```

Syntax

```
no tcp-acceleration
```

Mode

Route Policy

Description

Disable permit TCP acceleration.

Example

```
no tcp-acceleration
```

Syntax

```
wxa-group <WXA_GROUP_NAME>
```

Mode

Route Policy

Description

Configure WXA group.

Options

<WXA_GROUP_NAME> WXA group name.
Example: *Group One*

Example

```
wxa-group "Group One"
```

Syntax

```
no wxa-group
```

Mode

Route Policy

Description

Clear WXA group.

Example

```
no wxa-group
```

Syntax

auto-add-access-rules

Mode

Route Policy
IPV6 Route Policy

Description

Enable auto-add access rules.

Example

auto-add-access-rules

Syntax

no auto-add-access-rules

Mode

Route Policy
IPV6 Route Policy

Description

Disable auto-add access rules.

Example

no auto-add-access-rules

Syntax

probe <NETMON_NAME>

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy probing.

Options

<NETMON_NAME> Atom Object name.
Example: *Web Services Monitor*

Example

probe Web-Servers

Syntax

no probe

Mode

Route Policy
IPV6 Route Policy

Description

Disable route policy probing.

Example

no probe

Syntax

disable-when-probes-succeed

Mode

Route Policy
IPV6 Route Policy

Description

Disable route when probe succeeds.

Example

disable-when-probes-succeed

Syntax

no disable-when-probes-succeed

Mode

Route Policy
IPV6 Route Policy

Description

Do not disable route when probe succeeds.

Example

no disable-when-probes-succeed

Syntax

default-probe-state-up

Mode

Route Policy
IPV6 Route Policy

Description

Set probe default state to up.

Example

default-probe-state-up

Syntax

no default-probe-state-up

Mode

Route Policy
IPV6 Route Policy

Description

Set probe default state to down.

Example

no default-probe-state-up

Syntax

ipv6 default-route-metric <UINT8>

Mode

Routing

Description

Apply the metric to IPv6 default routes learned through router advertisement.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

ipv6 default-route-metric 20

Syntax

web-proxy

Mode

Config

Description

Set automatic proxy forwarding (web only).

Example

web-proxy

Syntax

no server

Mode

Web Proxy

Description

Clear web proxy hostname/IP and port.

Example

no server

Syntax

server <HOSTNAME> port <UINT16>

Mode

Web Proxy

Description

Set web proxy hostname/IP and port.

Options

- <HOSTNAME>** Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*
- port** Set web proxy TCP port.
- <UINT16>** Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
server 10.10.10.100 port 3129
```

Syntax

```
bypass-upon-failure
```

Mode

Web Proxy

Description

Enable bypass proxy servers upon proxy server failure.

Example

```
bypass-upon-failure
```

Syntax

```
no bypass-upon-failure
```

Mode

Web Proxy

Description

Disable bypass proxy servers upon proxy server failure.

Example

```
no bypass-upon-failure
```

Syntax

```
forward-public-requests
```

Mode

Web Proxy

Description

Enable forward public zone client requests to proxy server.

Example

```
forward-public-requests
```

Syntax

```
no forward-public-requests
```

Mode

Web Proxy

Description

Disable forward public zone client requests to proxy server.

Example

```
no forward-public-requests
```

Syntax

```
user-proxy-server <HOSTNAME>
```

Mode

Web Proxy

Description

Add proxy server through which users' web requests may come.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
user-proxy-server example.com
```

Syntax

```
no user-proxy-server <USER_NETPROXY_SERVER>
```

Mode

Web Proxy

Description

Delete proxy server through which users' web requests may come.

Options

<USER_NETPROXY_SERVER> User net proxy server.
Example: *example.com*

Example

```
no user-proxy-server example.com
```

Syntax

```
no user-proxy-servers
```

Mode

Web Proxy

Description

Delete all proxy servers through which users' web requests may come.

Example

```
no user-proxy-servers
```

Syntax

```
no ndp entry <NDP_IPV6_HOST> <NDP_MAC> <NDP_INTERFACE>
```

Mode

Config

Description

Delete an NDP entry.

Options

<NDP_IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

<NDP_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD

<NDP_INTERFACE> Interface name.
Example: X0

Example

```
no ndp entry 2001:10:10:10:2D0:02BB:03CC:04DD 02:BB:03:CC:04:DD X0
```

Syntax

```
no ndp entries
```

Mode

Config

Description

Delete all NDP entries.

Example

```
no ndp entries
```

Syntax

```
ndp reachable-time <UINT16>
```

Mode

Config

Description

Set neighbor discovery base reachable time in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
ndp reachable-time 30
```

Syntax

```
no ndp reachable-time
```

Mode

Config

Description

Clear neighbor discovery base reachable time.

Example

```
no ndp reachable-time
```

Syntax

```
ndp entry <NDP_IPV6_HOST> <NDP_MAC> <NDP_INTERFACE>
```

Mode

Config

Description

Add/edit an NDP entry.

Options

- <NDP_IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b
- <NDP_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD
- <NDP_INTERFACE> Interface name.
Example: X0

Example

```
ndp entry 2001:10:10:10:2D0:02BB:03CC:04DD 02:BB:03:CC:04:DD X0
```

Syntax

```
ip <NDP_IPV6_HOST>
```

Mode

Static NDP

Description

Configure static NDP IP.

Options

- <NDP_IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
ip 2001:10:10:10:2D0:02BB:03CC:04DD
```

Syntax

```
mac <NDP_MAC>
```

Mode

Static NDP

Description

Configure static NDP MAC address.

Options

- <NDP_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.

Example: 00:0C:F1:56:98:AD

Example

```
mac 00:01:02:03:04:05
```

Syntax

```
interface <NDP_INTERFACE>
```

Mode

Static NDP

Description

Configure static NDP interface.

Options

<NDP_INTERFACE> Interface name.
Example: X0

Example

```
interface X0
```

Syntax

```
clear ndp cache entries
```

Mode

Config

Description

Clear all non-permanent entries.

Example

```
clear ndp cache entries
```

Syntax

```
clear ndp cache entry <NDP_FLUSH_IPV6_HOST> <NDP_FLUSH_IF_NAME>
```

Mode

Config

Description

Clear one NDP entry.

Options

<NDP_FLUSH_IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

<NDP_FLUSH_IF_NAME> Interface name.
Example: X0

Example

```
clear ndp cache entry 2001:10:10:10:2D0:02BB:03CC:04DD X0
```

Syntax

```
tunnel-interface ipv6 <IPV6_TUNNEL_INTERFACE>
```

Mode

Config

Description

Add/edit tunnel interface.

Options

<IPV6_TUNNEL_INTERFACE> IPv6 Interface name.
Example: *myTunnelInterface*

Example

```
tunnel-interface ipv6 CorpIPv6Tunnel
```

Syntax

```
no tunnel-interface ipv6 <IPV6_TUNNEL_INTERFACE>
```

Mode

Config

Description

Delete tunnel interface.

Options

<IPV6_TUNNEL_INTERFACE> IPv6 Interface name.
Example: *myTunnelInterface*

Example

```
no tunnel-interface ipv6 CorpIPv6Tunnel
```

Syntax

```
name <IPV6_TUNNEL_INTERFACE>
```

Mode

Tunnel Interface

Description

Set tunnel interface name.

Options

<IPV6_TUNNEL_INTERFACE> IPv6 Interface name.
Example: *myTunnelInterface*

Example

```
name CorpIPv6Tunnel
```

Syntax

```
zone <INTERFACE_ZONE_NAME>
```

Mode

Tunnel Interface

Description

Set tunnel interface zone.

Options

<INTERFACE_ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
zone WAN
```

Syntax

```
no zone
```

Mode

Tunnel Interface

Description

Clear tunnel interface zone.

Example

```
no zone
```

Syntax

```
type { 6rd | 6to4 | gre | isatap | manual }
```

Mode

Tunnel Interface

Description

Set the tunnel interface type.

Options

6rd 6rd tunnel.

6to4 IPv6 6to4 tunnel.

gre GRE tunnel.

isatap ISATAP tunnel.

manual Manual tunnel.

Example

```
type manual
```

Syntax

```
ip <IPV6_HOST>
```

Mode

Manual Tunnel Interface
GRE Tunnel Interface
6to4 Tunnel Interface
6rd Tunnel Interface

Description

Set tunnel interface IPv6 address.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
ip 3ffe:1900:4545::f8ff:fe21:67cf
```

Syntax

```
no ip
```

Mode

Manual Tunnel Interface
GRE Tunnel Interface
6to4 Tunnel Interface
6rd Tunnel Interface

Description

Clear tunnel interface IPv6 address.

Example

```
no ip
```

Syntax

```
prefix-length <UINT8>
```

Mode

Manual Tunnel Interface
GRE Tunnel Interface
6to4 Tunnel Interface
6rd Tunnel Interface

Description

Set interface IPv6 prefix length.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
prefix-length 64
```

Syntax

```
comment <WORD>
```

Mode

Tunnel Interface

Description

Set tunnel interface comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "IPv6 tunnel to Corporate"
```

Syntax

```
no comment
```

Mode

Tunnel Interface

Description

Clear tunnel interface comment.

Example

```
no comment
```

Syntax

```
management { http | https | ping | snmp | ssh }
```

Mode

Interface IPv6
Tunnel Interface

Description

Enable management for the specified protocols.

Options

http HTTP.

https HTTPS.

ping Ping.

snmp SNMP.

ssh SSH.

Example

```
management https
```

Syntax

```
no management { http | https | ping | snmp | ssh }
```

Mode

Interface IPv6
Tunnel Interface

Description

Disable management for the specified protocols.

Options

http HTTP.

https HTTPS.

ping Ping.

snmp SNMP.

ssh SSH.

Example

```
no management https
```

Syntax

```
user-login [ http ] [ https ]
```

Mode

Interface IPv6
Tunnel Interface

Description

Enable user login for the specified protocols.

Options

http HTTP.

https HTTPS.

Example

```
user-login http https
```

Syntax

```
no user-login [ http ] [ https ]
```

Mode

Interface IPv6
Tunnel Interface

Description

Disable user login for the specified protocols.

Options

http HTTP.

https HTTPS.

Example

```
no user-login http
```

Syntax

```
https-redirect
```

Mode

Interface IPv6
Tunnel Interface

Description

Enable redirection from HTTP to HTTPS.

Example

```
https-redirect
```

Syntax

```
no https-redirect
```

Mode

Interface IPv6
Tunnel Interface

Description

Disable redirection from HTTP to HTTPS.

Example

```
no https-redirect
```

Syntax

```
remote ipv4-address { host <TUNNEL_IPV4_ADDR_HOST> | name <TUNNEL_IPV4_ADDR_HOST_NAME> }
```

Mode

Manual Tunnel Interface

Description

Configure the remote IPv4 address.

Options

| | |
|--------------------------------------|---|
| host | Configure the remote IPv4 address to host address. |
| <TUNNEL_IPV4_ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |

| | |
|---|--|
| name | Configure the remote IPv4 address to named address object. |
| <TUNNEL_IPV4_ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |

Example

```
remote ipv4-address host 198.165.165.4
```

Syntax

```
no remote ipv4-address
```

Mode

Manual Tunnel Interface

Description

Clear the remote IPv4 address.

Example

```
no remote ipv4-address
```

Syntax

```
remote ipv6-network { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

Manual Tunnel Interface

Description

Configure the remote IPv6 network.

Options

| | |
|--------------------------------|--|
| group | Configure the remote IPv6 network to named address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Configure the remote network to host address. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Configure the remote IPv6 network to named address object. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Configure the remote network to network address. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Configure the remote network to range of addresses. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
remote ipv6-network name IPv6RemoteNetwork
```

Syntax

```
no remote ipv6-network
```

Mode

Manual Tunnel Interface

Description

Clear the remote IPv6 network.

Example

```
no remote ipv6-network
```

Syntax

```
bound-to { any | interface <IPV6_TUNNEL_BOUND_TO_INTERFACE> }
```

Mode

Manual Tunnel Interface

Description

Set tunnel interface bound to.

Options

any Bound to any interface.

interface Bound to interface.

<IPV6_TUNNEL_BOUND_TO_INTERFACE> Interface name.
Example: *X0*

Example

```
bound-to interface X1
```

Syntax

```
link-mtu <UINT16>
```

Mode

Manual Tunnel Interface

Description

Set tunnel interface link MTU.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
link-mtu 1500
```

Syntax

```
remote ipv4-address { host <TUNNEL_IPV4_ADDR_HOST> | name <TUNNEL_IPV4_ADDR_HOST_NAME> }
```

Mode

GRE Tunnel Interface

Description

Configure the remote IPv4 address.

Options

host Configure the remote IPv4 address to host address.
<TUNNEL_IPV4_ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH\nExample: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Configure the remote IPv4 address to named address object.
<TUNNEL_IPV4_ADDR_HOST_NAME> Host address object name.
Example: *Web Server*

Example

```
remote ipv4-address host 198.165.165.4
```

Syntax

```
no remote ipv4-address
```

Mode

GRE Tunnel Interface

Description

Clear the remote IPv4 address.

Example

```
no remote ipv4-address
```

Syntax

```
remote ipv6-network { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

GRE Tunnel Interface

Description

Configure the remote IPv6 network.

Options

| | |
|-----------------------------------|--|
| group <ADDR_GROUP_NAME> | Configure the remote IPv6 network to named address object group. Group address object name. Example: <i>Sales Group</i> |
| host <ADDR_HOST> | Configure the remote network to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <ADDR_NAME> | Configure the remote IPv6 network to named address object. Address object name. Example: <i>Web Server</i> |
| network <ADDR_NETWORK> | Configure the remote network to network address. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> | Configure the remote network to range of addresses. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
remote ipv6-network name IPv6RemoteNetwork
```

Syntax

```
no remote ipv6-network
```

Mode

GRE Tunnel Interface

Description

Clear the remote IPv6 network.

Example

```
no remote ipv6-network
```

Syntax

```
bound-to { any | interface <IPV6_TUNNEL_BOUND_TO_INTERFACE> }
```

Mode

GRE Tunnel Interface

Description

Set tunnel interface bound to.

Options

any Bound to any interface.

interface Bound to interface.

<IPV6_TUNNEL_BOUND_TO_INTERFACE> Interface name.
Example: *X0*

Example

```
bound-to interface X1
```

Syntax

```
link-mtu <UINT16>
```

Mode

GRE Tunnel Interface

Description

Set tunnel interface link MTU.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
link-mtu 1500
```

Syntax

```
bound-to { any | interface <IPV6_TUNNEL_BOUND_TO_INTERFACE> }
```

Mode

6to4 Tunnel Interface

Description

Set 6to4 tunnel interface bound to.

Options

any Bound to any interface.

interface Bound to interface.

<IPV6_TUNNEL_BOUND_TO_INTERFACE> Interface name.
Example: *X0*

Example

bound-to interface X1

Syntax

enable

Mode

6to4 Tunnel Interface

Description

Enable IPv6 6to4 tunnel.

Example

enable

Syntax

no enable

Mode

6to4 Tunnel Interface

Description

Disable IPv6 6to4 tunnel.

Example

no enable

Syntax

link-mtu <UINT16>

Mode

6to4 Tunnel Interface

Description

Set tunnel interface link MTU.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
link-mtu 1500
```

Syntax

```
bound-to interface <IPV6_TUNNEL_BOUND_TO_INTERFACE>
```

Mode

6rd Tunnel Interface

Description

Set tunnel interface bound to.

Options

| | |
|---|---------------------------------------|
| interface | Bound to interface. |
| <IPV6_TUNNEL_BOUND_TO_INTERFACE> | Interface name. Example: <i>X0</i> |

Example

```
bound-to interface X1
```

Syntax

```
no bound-to
```

Mode

6rd Tunnel Interface

Description

Clear tunnel interface bound to.

Example

```
no bound-to
```

Syntax

```
dynamic
```

Mode

6rd Tunnel Interface

Description

Enable dynamic acquisition of IP configuration data.

Example

```
dynamic
```

Syntax

```
no dynamic
```

Mode

6rd Tunnel Interface

Description

Disable dynamic acquisition of IP configuration data.

Example

```
no dynamic
```

Syntax

```
6rd prefix <IPV6_HOST>
```

Mode

6rd Tunnel Interface

Description

Set tunnel interface 6rd prefix.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
6rd prefix 2001::
```

Syntax

```
no 6rd prefix
```

Mode

6rd Tunnel Interface

Description

Clear tunnel interface 6rd prefix.

Example

```
no 6rd prefix
```

Syntax

```
6rd prefix-length <UINT8>
```

Mode

6rd Tunnel Interface

Description

Set tunnel interface 6rd prefix length.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
6rd prefix-length 64
```

Syntax

no 6rd prefix-length

Mode

6rd Tunnel Interface

Description

Clear tunnel interface 6rd prefix length.

Example

no 6rd prefix-length

Syntax

border-relay-ipv4-address <IPV4_HOST>

Mode

6rd Tunnel Interface

Description

Set tunnel interface border relay IPv4 address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

border-relay-ipv4-address 10.10.10.10

Syntax

no border-relay-ipv4-address

Mode

6rd Tunnel Interface

Description

Clear tunnel interface border relay IPv4 address.

Example

no border-relay-ipv4-address

Syntax

mask-length <UINT8>

Mode

6rd Tunnel Interface

Description

Set tunnel interface IPv4 mask length.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
mask-length 64
```

Syntax

```
no mask-length
```

Mode

6rd Tunnel Interface

Description

Clear tunnel interface IPv4 mask length.

Example

```
no mask-length
```

Syntax

```
link-mtu <UINT16>
```

Mode

6rd Tunnel Interface

Description

Set tunnel interface link MTU.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
link-mtu 1500
```

Syntax

```
default-route
```

Mode

6rd Tunnel Interface

Description

Enable add default route.

Example

```
default-route
```

Syntax

```
no default-route
```

Mode

6rd Tunnel Interface

Description

Disable add default route.

Example

```
no default-route
```

Syntax

```
bound-to interface <IPV6_TUNNEL_BOUND_TO_INTERFACE>
```

Mode

ISATAP Tunnel Interface

Description

Set tunnel interface bound to.

Options

| | |
|---|---------------------------------------|
| interface | Bound to interface. |
| <IPV6_TUNNEL_BOUND_TO_INTERFACE> | Interface name. Example: <i>X0</i> |

Example

```
bound-to interface X1
```

Syntax

```
no bound-to
```

Mode

ISATAP Tunnel Interface

Description

Clear tunnel interface bound to.

Example

```
no bound-to
```

Syntax

```
prefix { name <ISATAP_ADDR_NETWORK_NAME> | network <ISATAP_ADDR_NETWORK> <ISATAP_ADDR_MASK> }
```

Mode

ISATAP Tunnel Interface

Description

Set tunnel interface IPv6 subnet prefix.

Options

| | |
|---|--|
| name | Set tunnel interface IPv6 subnet prefix to named address object. |
| <ISATAP_ADDR_NETWORK_NAME> | Network address object name. Example: <i>Sales Network</i> |

| | |
|------------------------------------|--|
| network | Set tunnel interface IPv6 subnet prefix to network address. |
| <ISATAP_ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |

| | |
|---------------------------------|--|
| <ISATAP_ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n |
|---------------------------------|--|

Example: `IPV4: 255.255.255.0\nIPV6: /64\n`

Example

```
prefix name ipv6Network
```

Syntax

```
no prefix
```

Mode

ISATAP Tunnel Interface

Description

Clear tunnel interface IPv6 subnet prefix.

Example

```
no prefix
```

Syntax

```
link-mtu <UINT16>
```

Mode

ISATAP Tunnel Interface

Description

Set tunnel interface link MTU.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
link-mtu 1500
```

Syntax

```
ipv6-traffic
```

Mode

Interface IPv6

Description

Enable IPv6 traffic on this interface.

Example

```
ipv6-traffic
```

Syntax

```
no ipv6-traffic
```

Mode

Interface IPv6

Description

Disable IPv6 traffic on this interface.

Example

```
no ipv6-traffic
```

Syntax

```
listen-router-advertisement
```

Mode

Interface IPv6

Description

Enable listening to route advertisement.

Example

```
listen-router-advertisement
```

Syntax

```
no listen-router-advertisement
```

Mode

Interface IPv6

Description

Disable listening to route advertisement.

Example

```
no listen-router-advertisement
```

Syntax

```
stateless-address-autoconfig
```

Mode

Interface IPv6

Description

Enable stateless address autoconfiguration.

Example

```
stateless-address-autoconfig
```

Syntax

```
no stateless-address-autoconfig
```

Mode

Interface IPv6

Description

Disable stateless address autoconfiguration.

Example

```
no stateless-address-autoconfig
```

Syntax

```
duplicate-address-detection-transmits <UINT8>
```

Mode

Interface IPv6

Description

Set duplicate address detection transmits.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
duplicate-address-detection-transmits 1
```

Syntax

```
no duplicate-address-detection-transmits
```

Mode

Interface IPv6

Description

Clear duplicate address detection transmits.

Example

```
no duplicate-address-detection-transmits
```

Syntax

```
reachable-time <UINT16>
```

Mode

Interface IPv6

Description

Set neighbor discovery base reachable time in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
reachable-time 30
```

Syntax

no reachable-time

Mode

Interface IPv6

Description

Clear neighbor discovery base reachable time.

Example

no reachable-time

Syntax

max ndp-size <UINT32>

Mode

Interface IPv6

Description

Set max NDP size per interface.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

max ndp-size 30

Syntax

no max ndp-size

Mode

Interface IPv6

Description

Clear max NDP size per interface.

Example

no max ndp-size

Syntax

ip-assignment [*mode*] { *auto* | *dhcpv6* | *l2bridge* | *pppoe6* | *static* }

Mode

Interface IPv6

Description

Set interface IPv6 assignment.

Options

mode Interface IP assignment mode.

auto Interface IPv6 configuration set to auto.

dhcpv6 Interface IPv6 configuration obtained by dhcpv6.

l2bridge Interface uses layer two bridging.

pppoe6 PPPoE IPv6 configuration assignment.

static Static IPv6 configuration assignment.

Example

```
ip-assignment dhcpv6
ip-assignment static
ip-assignment auto
ip-assignment pppoe6
```

Syntax

```
no ip-assignment
```

Mode

Interface IPv6

Description

Clear interface IPv6 assignment.

Example

```
no ip-assignment
```

Syntax

```
ip <IPV6_HOST>
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Set interface IPv6 address.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
ip 3ffe:1900:4545::f8ff:fe21:67cf
```

Syntax

```
no ip
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Clear interface IPv6 address.

Example

```
no ip
```

Syntax

prefix-length <UINT8>

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Set interface IPv6 prefix length.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

prefix-length 64

Syntax

dns primary <IPv6_HOST>

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Set the primary DNS server IP address.

Options

<IPv6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

dns primary 3ffe:1900:4545::f8ff:fe21:67cf

Syntax

dns secondary <IPv6_HOST>

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Set the secondary DNS server IP address.

Options

<IPv6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

dns secondary 3ffe:1900:4545::f8ff:fe21:67cf

Syntax

```
dns tertiary <IPV6_HOST>
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Set the tertiary DNS server IP address.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
dns tertiary 3ffe:1900:4545::f8ff:fe21:67cf
```

Syntax

```
no dns primary
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Clear the primary DNS server IP address.

Example

```
no dns primary
```

Syntax

```
no dns secondary
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Clear the secondary DNS server IP address.

Example

```
no dns secondary
```

Syntax

```
no dns tertiary
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Clear the tertiary DNS server IP address.

Example

no dns tertiary

Syntax

gateway <IPV6_HOST>

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Set interface gateway.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

gateway 3ffe:1900:4545:201::202

Syntax

no gateway

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Clear interface gateway.

Example

no gateway

Syntax

advertise subnet-prefix

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Enable advertise subnet prefix of IPv6 primary static address.

Example

advertise subnet-prefix

Syntax

no advertise subnet-prefix

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Disable advertise subnet prefix of IPv6 primary static address.

Example

```
no advertise subnet-prefix
```

Syntax

```
extra-ip [ type ] { 6rd <IPV6_EXTRA_ADDR> | prefix-delegation <IPV6_EXTRA_ADDR> | static <IPV6_EXTRA_ADDR> }
```

Mode

Static IPv6 Assignment

Description

Add/edit extra interface IPv6 address.

Options

| type | Type |
|--------------------------------|--|
| 6rd | Add downstream IPv6 address delegated from 6rd |
| <IPV6_EXTRA_ADDR> | IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b |
| prefix-delegation | Add downstream IPv6 address delegated from DHCP-PD |
| <IPV6_EXTRA_ADDR> | IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b |
| static | Add static IPv6 address |
| <IPV6_EXTRA_ADDR> | IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b |

Example

```
extra-ip static 3ffe:1900:4545::f8ff:fe21:67c2
```

Syntax

```
no extra-ip { 6rd | prefix-delegation | static } <IPV6_EXTRA_ADDR>
```

Mode

Static IPv6 Assignment

Description

Delete extra interface IPv6 address.

Options

| | |
|--------------------------------|--|
| 6rd | Delete downstream IPv6 address delegated from 6rd |
| prefix-delegation | Delete downstream IPv6 address delegated from DHCP-PD |
| static | Delete static IPv6 address |
| <IPV6_EXTRA_ADDR> | IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b |

Example

```
no extra-ip static 3ffe:1900:4545::f8ff:fe21:67c2
```

Syntax

no extra-ipv6-addresses

Mode

Static IPv6 Assignment

Description

Delete all extra interface IPv6 addresses.

Example

no extra-ipv6-addresses

Syntax

router-advertisement

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Enter router advertisement configuration mode.

Example

router-advertisement

Syntax

multicast

Mode

Interface IPv6

Description

Enable IPv6 multicast support.

Example

multicast

Syntax

no multicast

Mode

Interface IPv6

Description

Disable IPv6 multicast support.

Example

no multicast

Syntax

```
type { 6rd | prefix-delegation | static }
```

Mode

IPv6 Extra Address

Description

Set interface IPv6 extra address type.

Options

| | |
|--------------------------|--|
| 6rd | Add downstream IPv6 address delegated from 6rd |
| prefix-delegation | Add downstream IPv6 address delegated from DHCP-PD |
| static | Add static IPv6 address |

Example

```
type static
```

Syntax

```
ip <IPv6_EXTRA_ADDR>
```

Mode

IPv6 Extra Address

Description

Set interface IPv6 address.

Options

<IPv6_EXTRA_ADDR> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
ip 3ffe:1900:4545::f8ff:fe21:67cf
```

Syntax

```
prefix-length <UINT8>
```

Mode

IPv6 Extra Address

Description

Set interface IPv6 prefix length.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
prefix-length 64
```

Syntax

```
delegated-prefix name <DELEGATED_PREFIX_ADDR_HOST_NAME>
```


Mode

IPv6 Extra Address

Description

Set delegated prefix assignment.

Options

| | |
|---|---|
| <i>name</i> | Set delegated prefix to named address object. |
| <i><DELEGATED_PREFIX_ADDR_HOST_NAME></i> | Host address object name. Example: <i>Web Server</i> |

Example

```
delegated-prefix-assignment
```

Syntax

```
no delegated-prefix
```

Mode

IPv6 Extra Address

Description

Clear delegated prefix assignment.

Example

```
no delegated-prefix
```

Syntax

```
preferred ip <IPv6_EXTRA_ADDR>
```

Mode

IPv6 Extra Address

Description

Set interface preferred IPv6 address.

Options

| | |
|---------------------------------------|---|
| <i><IPv6_EXTRA_ADDR></i> | IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i> |
|---------------------------------------|---|

Example

```
preferred ip 3ffe:1900:4545::f8ff:fe21:67cf
```

Syntax

```
preferred prefix-length <UINT8>
```

Mode

IPv6 Extra Address

Description

Set interface IPv6 preferred prefix length.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
preferred prefix-length 64
```

Syntax

```
no preferred prefix-length
```

Mode

IPv6 Extra Address

Description

Clear interface IPv6 preferred prefix length.

Example

```
no preferred prefix-length
```

Syntax

```
advertise subnet-prefix
```

Mode

IPv6 Extra Address

Description

Enable advertise subnet prefix of IPv6 address.

Example

```
advertise subnet-prefix
```

Syntax

```
no advertise subnet-prefix
```

Mode

IPv6 Extra Address

Description

Disable advertise subnet prefix of IPv6 address.

Example

```
no advertise subnet-prefix
```

Syntax

```
enable
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Enable IPv6 router advertisement.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Disable IPv6 router advertisement.

Example

```
no enable
```

Syntax

```
interval { max <UINT32> | min <UINT32> }
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Set IPv6 router advertisement interval range.

Options

max Router advertisement interval range maximum.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

min Router advertisement interval range minimum.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
interval min 200
```

Syntax

```
link-mtu <UINT32>
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Set IPv6 router advertisement link MTU.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
link-mtu 1400
```

Syntax

no link-mtu

Mode

Static IPv6 Assignment Router Advertisement

Description

Set IPv6 router advertisement link MTU as unspecified.

Example

no link-mtu

Syntax

reachable-time <UINT32>

Mode

Static IPv6 Assignment Router Advertisement

Description

Set the time the node assumes the neighbor is reachable in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

reachable-time 5

Syntax

no reachable-time

Mode

Static IPv6 Assignment Router Advertisement

Description

Clear the time the node assumes the neighbor is reachable as unspecified.

Example

no reachable-time

Syntax

retransmit-timer <UINT32>

Mode

Static IPv6 Assignment Router Advertisement

Description

Set the time between retransmitted neighbor solicitation messages in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
retransmit-timer 30
```

Syntax

```
no retransmit-timer
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Clear the time between retransmitted neighbor solicitation messages as unspecified.

Example

```
no retransmit-timer
```

Syntax

```
current-hop-limit <UINT8>
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Set current hop limit.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
current-hop-limit 64
```

Syntax

```
no current-hop-limit
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Set current hop limit as unspecified.

Example

```
no current-hop-limit
```

Syntax

```
router lifetime <UINT16>
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Configure the lifetime when a router is accepted as the default router in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
router lifetime 1800
```

Syntax

```
no router lifetime
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Clear the lifetime when a router is accepted as the default router as unspecified.

Example

```
no router lifetime
```

Syntax

```
router preference { high | low | medium }
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Configure router preference when a router is accepted as the default router.

Options

high Set the router preference as high.

low Set the router preference as low.

medium Set the router preference as medium.

Example

```
router preference low
```

Syntax

```
managed
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Enable IPv6 addresses as available via stateful addresses configuration.

Example

managed

Syntax

no managed

Mode

Static IPv6 Assignment Router Advertisement

Description

Disable IPv6 addresses as available via stateful addresses configuration.

Example

no managed

Syntax

other-config

Mode

Static IPv6 Assignment Router Advertisement

Description

Enable non-address configuration as available via stateful addresses configuration.

Example

other-config

Syntax

no other-config

Mode

Static IPv6 Assignment Router Advertisement

Description

Disable non-address configuration as available via stateful addresses configuration.

Example

no other-config

Syntax

prefix <IPV6_ADVERTISING_PREFIX>

Mode

Static IPv6 Assignment Router Advertisement

Description

Add/edit advertising prefix.

Options

<IPV6_ADVERTISING_PREFIX> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2001::

Example

```
prefix 2001:1:1:1::
```

Syntax

```
no prefix <IPV6_ADVERTISING_PREFIX>
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Delete the specified advertising prefix.

Options

<IPV6_ADVERTISING_PREFIX> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2001::

Example

```
no prefix 2001:1:1:1::
```

Syntax

```
no prefixes
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Delete all advertising prefixes.

Example

```
no prefixes
```

Syntax

```
prefix <IPV6_ADVERTISING_PREFIX>
```

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Set advertising prefix.

Options

<IPV6_ADVERTISING_PREFIX> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2001::

Example

```
prefix 2001:1:1:1::
```

Syntax

```
valid-lifetime <UINT32>
```

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Set advertising prefix valid lifetime in minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
valid-lifetime 10
```

Syntax

```
preferred lifetime <UINT32>
```

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Set advertising prefix valid preferred lifetime in minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
preferred lifetime 10
```

Syntax

```
on-link
```

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Enable using prefix for on-link determination.

Example

```
on-link
```

Syntax

```
no on-link
```

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Disable using prefix for on-link determination.

Example

no on-link

Syntax

autonomous

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Enable autonomous address configuration indicating prefix can be used for stateless address configuration.

Example

autonomous

Syntax

no autonomous

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Disable autonomous address configuration.

Example

no autonomous

Syntax

prefix-delegation

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Enable DHCPv6 prefix delegation.

Example

prefix-delegation

Syntax

no prefix-delegation

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Disable DHCPv6 prefix delegation.

Example

```
no prefix-delegation
```

Syntax

```
preferred <IPV6_HOST> <UINT8>
```

Mode

Prefix delegation

Description

Enable send preferred delegated prefix.

Options

- <IPV6_HOST>** IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: `2000:0000:0000:ff68:0205:62ef:ee8d:f25b`
- <UINT8>** Integer in the form: D OR 0xHH.
Example: `123`

Example

```
preferred 2001:: 64
```

Syntax

```
no preferred
```

Mode

Prefix delegation

Description

Disable send preferred delegated prefix.

Example

```
no preferred
```

Syntax

```
send-hints
```

Mode

Prefix delegation

Description

Enable send hints for renewing previous delegated prefix on startup.

Example

```
send-hints
```

Syntax

```
no send-hints
```

Mode

Prefix delegation

Description

Disable send hints for renewing previous delegated prefix on startup.

Example

```
no send-hints
```

Syntax

```
rapid-commit
```

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Enable use rapid commit option.

Example

```
rapid-commit
```

Syntax

```
no rapid-commit
```

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Disable use rapid commit option.

Example

```
no rapid-commit
```

Syntax

```
send-hints
```

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Enable send hints for renewing previous IP on startup.

Example

```
send-hints
```

Syntax

```
no send-hints
```

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Disable send hints for renewing previous IP on startup.

Example

```
no send-hints
```

Syntax

```
aftr-name-option
```

Mode

DHCPv6 Assignment

Description

Enable use AFTR (Address Family Transition Router) name option.

Example

```
aftr-name-option
```

Syntax

```
no aftr-name-option
```

Mode

DHCPv6 Assignment

Description

Disable use AFTR (Address Family Transition Router) name option.

Example

```
no aftr-name-option
```

Syntax

```
mode { auto | manual }
```

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Set dhcpv6 mode.

Options

auto Automatic.

manual Manual.

Example

```
mode manual
```

Syntax

info-only

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Enable only request stateless information.

Example

info-only

Syntax

no info-only

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Disable only request stateless information.

Example

no info-only

Syntax

release delegated-prefix

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Release designated interface lease or delegated prefixes acquired via DHCPv6.

Options

delegated-prefix Release delegated prefixes acquired via DHCPv6.

Example

release

Syntax

renew delegated-prefix

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Renew designated interface lease or delegated prefixes acquired via DHCPv6.

Options

delegated-prefix Renew delegated prefixes acquired via DHCPv6.

Example

```
renew
```

Syntax

```
mode-assignment { auto | dhcpv6 | static }
```

Mode

PPPoEv6 Assignment

Description

Set PPPoE IPv6 address mode.

Options

auto Set PPPoE6 to auto mode.

dhcpv6 Set PPPoE6 to dhcpv6 mode.

static Set PPPoE6 to static mode.

Example

```
mode-assignment dhcpv6
mode-assignment static
mode-assignment auto
```

Syntax

```
reconnect <UINT16>
```

Mode

PPPoEv6 Assignment

Description

Enable and set reconnect the PPPOE client if the server does not send traffic for specified minutes.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
reconnect 5
```

Syntax

```
no reconnect
```

Mode

PPPoEv6 Assignment

Description

Disable reconnect the PPPOE client if the server does not send traffic.

Example

```
no reconnect
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

PPPoEv6 Assignment

Description

Set the wan pppoe reconnect schedule.

Options

| | |
|---------------------------------|---|
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule name "Work Hours"
```

Syntax

```
inactivity <UINT16>
```

Mode

PPPoEv6 Assignment

Description

Enable the pppoe inactivity timer.

Options

| | |
|-----------------------|--|
| <UINT16> | Integer in the form: D OR 0xHHHH. Example: <i>123</i> |
|-----------------------|--|

Example

```
inactivity 10
```

Syntax

```
no inactivity
```

Mode

PPPoEv6 Assignment

Description

Disable the pppoe inactivity timer.

Example

no inactivity

Syntax

lcp-echo-packets

Mode

PPPoEv6 Assignment

Description

Enable strictly use LCP echo packets for server keep-alive.

Example

lcp-echo-packets

Syntax

no lcp-echo-packets

Mode

PPPoEv6 Assignment

Description

Disable strictly use LCP echo packets for server keep-alive.

Example

no lcp-echo-packets

Syntax

server-keepalive <UINT16>

Mode

PPPoEv6 Assignment

Description

Enable reconnect pppoe if the server does not send traffic for the specified minutes.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

server-keepalive 10

Syntax

no server-keepalive

Mode

PPPoEv6 Assignment

Description

Disable reconnect pppoe if the server does not send traffic for the specified minutes.

Example

no server-keepalive

Syntax

enable

Mode

IPv6 DHCP Server

Description

Enable IPv6 DHCP server.

Example

enable

Syntax

no enable

Mode

IPv6 DHCP Server

Description

Disable IPv6 DHCP server.

Example

no enable

Syntax

option

Mode

IPv6 DHCP Server

Description

DHCP server IPv6 option.

Example

option

Syntax

option object <DHCP_OPTION_OBJECT>

Mode

IPv6 DHCP Server

Description

Add/edit IPv6 DHCP server option object.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
option object "LAN Specific DHCP Option"
```

Syntax

```
no option object <DHCP_OPTION_OBJECT>
```

Mode

IPv6 DHCP Server

Description

Delete IPv6 DHCP server option object.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
no option object "LAN Specific DHCP Option"
```

Syntax

```
no option objects
```

Mode

IPv6 DHCP Server

Description

Delete all IPv6 DHCP server option objects.

Example

```
no option objects
```

Syntax

```
name <DHCP_OPTION_OBJECT>
```

Mode

IPv6 DHCP Option Object

Description

Set IPv6 DHCP server option object name.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
name "LAN Specific DHCP Option"
```

Syntax

number <DHCP_IPV6_OPTION_OBJECT_NUMBER>

Mode

IPv6 DHCP Option Object

Description

Set IPv6 DHCP server option object number.

Options

<DHCP_IPV6_OPTION_OBJECT_NUMBER> IPv6 DHCP server option object number.
Example: 12

Example

number 12

Syntax

array

Mode

IPv6 DHCP Option Object

Description

Enable IPv6 DHCP server option object array.

Example

array

Syntax

no array

Mode

IPv6 DHCP Option Object

Description

Disable IPv6 DHCP server option object array.

Example

no array

Syntax

value { boolean <UINT8> | domain-name <HOSTNAME> | four-byte <UINT32> | ip <IPV6_HOST> | one-byte <UINT8> | string <WORD> | two-byte <UINT16> }

Mode

IPv6 DHCP Option Object

Description

Set IPv6 DHCP server option object value. If Option Array is checked , multiple values can be entered separated by ;.

Options

| | |
|--------------------------|--|
| boolean | Option object type: boolean. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| domain-name | Option object type: domain name. |
| <HOSTNAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i> |
| four-byte | Option object type: four byte data. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: 123 |
| ip | Option object type: IP address. |
| <IPV6_HOST> | IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b |
| one-byte | Option object type: one byte. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| string | Option object type: string. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| two-byte | Option object type: two byte. |
| <UINT16> | Integer in the form: D OR 0xHHHH. Example: 123 |

Example

```
value ip fe80::1
value domain-name domainName
value four-byte 123
value two-byte 123
value one-byte 23
value string "String value"
value boolean 0
```

Syntax

```
no value
```

Mode

IPv6 DHCP Option Object

Description

Clear IPv6 DHCP server option object value.

Example

```
no value
```

Syntax

```
option group <DHCP_OPTION_GROUP>
```

Mode

IPv6 DHCP Server

Description

Add/edit IPv6 DHCP server option group.

Options

| | |
|----------------------------------|---|
| <DHCP_OPTION_GROUP> | DHCP server option group name. Example: <i>Corp Network DHCP Group</i> |
|----------------------------------|---|

Example

```
option group "LAN Specific DHCP Options"
```

Syntax

```
no option group <DHCP_OPTION_GROUP>
```

Mode

IPv6 DHCP Server

Description

Delete one IPv6 DHCP server option group.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
no option group "LAN Specific DHCP Options"
```

Syntax

```
no option groups
```

Mode

IPv6 DHCP Server

Description

Delete all IPv6 DHCP server option groups.

Example

```
no option groups
```

Syntax

```
name <DHCP_OPTION_GROUP>
```

Mode

IPv6 DHCP Server Option Group

Description

Set IPv6 DHCP server option group name.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
name "LAN Specific DHCP Options"
```

Syntax

```
option object <DHCP_OPTION_OBJECT>
```

Mode

IPv6 DHCP Server Option Group

Description

Add IPv6 DHCP server option object to group.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
option object "Specific DHCP Options"
```

Syntax

```
no option object <DHCP_OPTION_GROUP_OBJECT>
```

Mode

IPv6 DHCP Server Option Group

Description

Remove IPv6 DHCP server option object from group.

Options

<DHCP_OPTION_GROUP_OBJECT> DHCP server option object name in specify option group.
Example: *Corp Network DHCP Group*

Example

```
no option object "Specific DHCP Options"
```

Syntax

```
option group <DHCP_OPTION_GROUP>
```

Mode

IPv6 DHCP Server Option Group

Description

Add IPv6 DHCP server option group to group.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
option group "Specific DHCP Options"
```

Syntax

```
no option group <DHCP_OPTION_GROUP_GROUP>
```

Mode

IPv6 DHCP Server Option Group

Description

Remove IPv6 DHCP server option group from group.

Options

<DHCP_OPTION_GROUP_GROUP> DHCP server option group name in specify option group.
Example: *Corp Network DHCP Group*

Example

```
no option group "Specific DHCP Options"
```

Syntax

```
scope dynamic <DHCP_IPV6_DYNAMIC_SCOPE_NAME>
```

Mode

IPv6 DHCP Server

Description

Add/edit IPv6 DHCP dynamic scope and enter its configuration mode.

Options

<DHCP_IPV6_DYNAMIC_SCOPE_NAME> IPv6 DHCP server dynamic scope name.
Example: *abc*

Example

```
scope dynamic "dyanmicScope"
```

Syntax

```
no scope dynamic <DHCP_IPV6_DYNAMIC_SCOPE_NAME>
```

Mode

IPv6 DHCP Server

Description

Delete one IPv6 DHCP dynamic scope.

Options

<DHCP_IPV6_DYNAMIC_SCOPE_NAME> IPv6 DHCP server dynamic scope name.
Example: *abc*

Example

```
no scope dynamic "dyanmicScope"
```

Syntax

```
no scopes dynamic
```

Mode

IPv6 DHCP Server

Description

Delete all IPv6 DHCP server dynamic scope.

Example

```
no scopes dynamic
```

Syntax

name <DHCP_IPV6_DYNAMIC_SCOPE_NAME>

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server dynamic scope name.

Options

<DHCP_IPV6_DYNAMIC_SCOPE_NAME> IPv6 DHCP server dynamic scope name.
Example: *abc*

Example

name "Dynamic Scope Name"

Syntax

enable

Mode

IPv6 DHCP Server Dynamic Scope

Description

Enable IPv6 DHCP server dynamic scope.

Example

enable

Syntax

no enable

Mode

IPv6 DHCP Server Dynamic Scope

Description

Disable IPv6 DHCP server dynamic scope.

Example

no enable

Syntax

prefix <IPv6_HOST>

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server dynamic scope prefix.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
prefix fe00::
```

Syntax

```
no prefix
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope prefix.

Example

```
no prefix
```

Syntax

```
range <IPV6_HOST> <IPV6_HOST>
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP dynamic scope range.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
range fe00::1 fe00::2014
```

Syntax

```
no range
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope range.

Example

```
no range
```

Syntax

```
lifetime valid <UINT32>
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server dynamic scope valid lifetime (minutes).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
lifetime valid 2160
```

Syntax

```
no lifetime valid
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope valid lifetime.

Example

```
no lifetime valid
```

Syntax

```
lifetime preferred <UINT32>
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server dynamic scope preferred lifetime (minutes).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
lifetime preferred 1440
```

Syntax

```
no lifetime preferred
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope preferred lifetime.

Example

```
no lifetime preferred
```

Syntax

`comment <WORD>`

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server dynamic scope comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: `abc`

Example

`comment "Comment for dynamic scope"`

Syntax

`no comment`

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope comment.

Example

`no comment`

Syntax

`always-send-option`

Mode

IPv6 DHCP Server Dynamic Scope

Description

Enable IPv6 DHCP server dynamic scope always send IPv6 options.

Example

`always-send-option`

Syntax

`no always-send-option`

Mode

IPv6 DHCP Server Dynamic Scope

Description

Diablo IPv6 DHCP server dynamic scope always send IPv6 options.

Example

```
no always-send-option
```

Syntax

```
domain-name <HOSTNAME>
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server dynamic scope domain name.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
domain-name example.com
```

Syntax

```
no domain-name
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope domain name.

Example

```
no domain-name
```

Syntax

```
dns server { inherit | static { primary <IPV6_HOST> | secondary <IPV6_HOST> | tertiary <IPV6_HOST> } }
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

set IPv6 DHCP server DNS settings or inherit DNS settings dynamically from the sonicwall's DNS settings.

Options

inherit Inherit DNS servers.

static Static DNS server.

primary Specify primary DNS server IP address.

<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

secondary Specify secondary DNS server IP address.

<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

tertiary Specify tertiary DNS server IP address.
<IPv6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
dns server primary fe80::1  
dns server inherit
```

Syntax

```
no dns server static { primary | secondary | tertiary }
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope DNS server IP.

Options

static Clear static IPv6 DHCP server dynamic scope DNS server IP.

primary Clear primary DNS server IP address.

secondary Clear secondary DNS server IP address.

tertiary Clear tertiary DNS server IP address.

Example

```
no dns server primary
```

Syntax

```
generic-option { group <DHCP_OPTION_GROUP> | object <DHCP_OPTION_OBJECT> }
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server option object or group for dynamic scope.

Options

group Set IPv6 DHCP server option group for dynamic scope.
<DHCP_OPTION_GROUP> DHCP server option group name.
Example: Corp Network DHCP Group

object Set IPv6 DHCP server option object for dynamic scope.
<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: Corp Network DHCP Options

Example

```
generic-option object "Specific object DHCP Option" generic-option group "Specific Group DHCP Option"
```

Syntax

```
no generic-option
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope generic option.

Example

```
no generic-option
```

Syntax

```
scope static <DHCP_IPV6_STATIC_SCOPE_NAME>
```

Mode

IPv6 DHCP Server

Description

Add/edit IPv6 DHCP server static scope.

Options

<DHCP_IPV6_STATIC_SCOPE_NAME> IPv6 DHCP server static scope name.
Example: *abc*

Example

```
scope static "dhcps6StaticName"
```

Syntax

```
no scope static <DHCP_IPV6_STATIC_SCOPE_NAME>
```

Mode

IPv6 DHCP Server

Description

Delete IPv6 DHCP server static scope.

Options

<DHCP_IPV6_STATIC_SCOPE_NAME> IPv6 DHCP server static scope name.
Example: *abc*

Example

```
no scope static fe00::1
```

Syntax

```
no scopes static
```

Mode

IPv6 DHCP Server

Description

Delete all IPv6 DHCP server static scopes.

Example

```
no scopes static
```

Syntax

enable

Mode

IPv6 DHCP Server Static Scope

Description

Enable IPv6 DHCP server static scope.

Example

enable

Syntax

no enable

Mode

IPv6 DHCP Server Static Scope

Description

Disable IPv6 DHCP server static scope.

Example

no enable

Syntax

name <DHCP_IPV6_STATIC_SCOPE_NAME>

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope name.

Options

<DHCP_IPV6_STATIC_SCOPE_NAME> IPv6 DHCP server static scope name.
Example: *abc*

Example

name "Static scope Name"

Syntax

no name

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope name.

Example

```
no name
```

Syntax

```
prefix <IPV6_HOST>
```

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope prefix.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
prefix fe00::
```

Syntax

```
no prefix
```

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope prefix.

Example

```
no prefix
```

Syntax

```
ip <IPV6_HOST>
```

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope IP.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
ip fe80::10
```

Syntax

```
no ip
```

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope IP.

Example

```
no ip
```

Syntax

```
iaid <UINT32>
```

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope IAID.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
iaid 2014
```

Syntax

```
no iaaid
```

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope IAID.

Example

```
no iaaid
```

Syntax

```
duid <WORD>
```

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope DUID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
duid 0003000110F0A0F3A23B
```

Syntax

no duid

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope DUID.

Example

no duid

Syntax

lifetime { preferred <UINT32> | valid <UINT32> }

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope valid or preferred lifetime (minutes).

Options

preferred Set IPv6 DHCP server static scope preferred lifetime (minutes).

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

valid Set IPv6 DHCP server static scope valid lifetime (minutes).

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

lifetime valid 2160
lifetime preferred 1440

Syntax

no lifetime { preferred | valid }

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope valid or preferred lifetime.

Options

preferred Clear IPv6 DHCP server static scope preferred lifetime.

valid Clear IPv6 DHCP server static scope valid lifetime.

Example

no lifetime valid
no lifetime preferred

Syntax

comment <WORD>

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

commnet "IPv6 DHCP server commnet"

Syntax

no comment

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope comment.

Example

no comment

Syntax

always-send-option

Mode

IPv6 DHCP Server Static Scope

Description

Enable send IPv6 DHCP server options always.

Example

always-send-option

Syntax

no always-send-option

Mode

IPv6 DHCP Server Static Scope

Description

Disable send IPv6 DHCP server options always.

Example

no always-send-option

Syntax

domain-name <HOSTNAME>

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope domain name.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

domain-name "IPv6 DHCP server domain name"

Syntax

no domain-name

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope domain name.

Example

no domain-name

Syntax

dns server { inherit | static { primary <IPV6_HOST> | secondary <IPV6_HOST> | tertiary <IPV6_HOST> } }

Mode

IPv6 DHCP Server Static Scope

Description

set IPv6 DHCP server DNS settings or inherit DNS settings dynamically from the SonicWall's DNS settings.

Options

inherit Inherit DNS servers.

static Static DNS server.

primary Specify primary DNS server IP address.

<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

secondary Specify secondary DNS server IP address.

<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

tertiary Specify tertiary DNS server IP address.

<IPv6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
dns server primary fe80::1  
dns server inherit
```

Syntax

```
no dns server { primary | secondary | tertiary }
```

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope DNS server IP.

Options

primary Clear primary DNS server IP address.

secondary Clear secondary DNS server IP address.

tertiary Clear tertiary DNS server IP address.

Example

```
no dns server primary
```

Syntax

```
generic-option { group <DHCP_OPTION_GROUP> | object <DHCP_OPTION_OBJECT> }
```

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server option object or group for static scope.

Options

group Set IPv6 DHCP server option group for static scope.
<DHCP_OPTION_GROUP> DHCP server option group name.
Example: Corp Network DHCP Group

object Set IPv6 DHCP server option object for static scope.
<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: Corp Network DHCP Options

Example

```
generic-option object "Specific object DHCP Option" generic-option group "Specific Group DHCP Option"
```

Syntax

```
no generic-option
```

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope generic option.

Example

```
no generic-option
```

Syntax

```
clear lease <DHCP_IPV6_LEASE_HOST>
```

Mode

IPv6 DHCP Server

Description

Delete IPv6 DHCP server lease.

Options

<DHCP_IPV6_LEASE_HOST> IPv6 DHCP server lease IP.
Example: `2000:0000:0000:ff68:0205:62ef:ee8d:f25b`

Example

```
clear lease fe80::100
```

Syntax

```
clear leases
```

Mode

IPv6 DHCP Server

Description

Delete all IPv6 DHCP server leases.

Example

```
clear leases
```

Syntax

```
vlan-translation { ingress interface <VLAN_TRANSLATION_INGRESS_IFACE_NAME> vlan <VLAN_TRANSLATION_INGRESS_VLAN_ID> egress  
interface <VLAN_TRANSLATION_EGRESS_IFACE_NAME> vlan <VLAN_TRANSLATION_EGRESS_VLAN_ID> }
```

Mode

Config

Description

Add/edit VLAN translation and enter its configuration mode.

Options

| | |
|--|---|
| ingress | VLAN translation ingress. |
| interface | Ingress interface. |
| <VLAN_TRANSLATION_INGRESS_IFACE_NAME> | Ingress interface name. Example: <code>X0</code> |
| vlan | Ingress VLAN tag. |
| <VLAN_TRANSLATION_INGRESS_VLAN_ID> | Interface VLAN id. Example: <code>23</code> |
| egress | VLAN translation egress. |

| | |
|---|---------------------------------------|
| interface | Egress interface. |
| <VLAN_TRANSLATION_EGRESS_IFACE_NAME> | Egress interface name. Example: X0 |
| vlan | Egress VLAN tag. |
| <VLAN_TRANSLATION_EGRESS_VLAN_ID> | Interface VLAN id. Example: 23 |

Example

```
vlan-translation ingress interface X1 vlan 111 egress interface X2 vlan 222
```

Syntax

```
no vlan-translation { ingress interface <VLAN_TRANSLATION_INGRESS_IFACE_NAME> vlan <VLAN_TRANSLATION_INGRESS_VLAN_ID> egress interface <VLAN_TRANSLATION_EGRESS_IFACE_NAME> vlan <VLAN_TRANSLATION_EGRESS_VLAN_ID> }
```

Mode

Config

Description

Delete one VLAN translation.

Options

| | |
|--|--|
| ingress | VLAN translation ingress. |
| interface | Ingress interface. |
| <VLAN_TRANSLATION_INGRESS_IFACE_NAME> | Ingress interface name. Example: X0 |
| vlan | Ingress VLAN tag. |
| <VLAN_TRANSLATION_INGRESS_VLAN_ID> | Interface VLAN id. Example: 23 |
| egress | VLAN translation egress. |
| interface | Egress interface. |
| <VLAN_TRANSLATION_EGRESS_IFACE_NAME> | Egress interface name. Example: X0 |
| vlan | Egress VLAN tag. |
| <VLAN_TRANSLATION_EGRESS_VLAN_ID> | Interface VLAN id. Example: 23 |

Example

```
no vlan-translation ingress interface X1 vlan 111 egress interface X2 vlan 222
```

Syntax

```
no vlan-translations
```

Mode

Config

Description

Delete all VLAN translations.

Example

```
no vlan-translations
```

Syntax

```
ingress interface <VLAN_TRANSLATION_INGRESS_IFACE_NAME>
```

Mode

VLAN Translation

Description

Set VLAN translation ingress interface.

Options

<VLAN_TRANSLATION_INGRESS_IFACE_NAME> Ingress interface name.
Example: X0

Example

```
ingress interface X1
```

Syntax

```
ingress vlan <VLAN_TRANSLATION_INGRESS_VLAN_ID>
```

Mode

VLAN Translation

Description

Set VLAN translation ingress VLAN id.

Options

<VLAN_TRANSLATION_INGRESS_VLAN_ID> Interface VLAN id.
Example: 23

Example

```
ingress vlan 111
```

Syntax

```
egress interface <VLAN_TRANSLATION_EGRESS_IFACE_NAME>
```

Mode

VLAN Translation

Description

Set VLAN translation egress interface.

Options

<VLAN_TRANSLATION_EGRESS_IFACE_NAME> Egress interface name.
Example: X0

Example

```
egress interface X2
```

Syntax

```
egress vlan <VLAN_TRANSLATION_EGRESS_VLAN_ID>
```

Mode

VLAN Translation

Description

Set VLAN translation egress VLAN id.

Options

`<VLAN_TRANSLATION_EGRESS_VLAN_ID>` Interface VLAN id.
Example: 23

Example

```
egress vlan 222
```

Syntax

```
reverse
```

Mode

VLAN Translation

Description

Enable reverse translation.

Example

```
reverse
```

Syntax

```
no reverse
```

Mode

VLAN Translation

Description

Disable reverse translation.

Example

```
no reverse
```

Syntax

```
dns-security
```

Mode

Config

Description

Configure and enter DNS security mode.

Example

```
dns-security
```

Syntax

```
dns-sinkhole
```

Mode

DNS Security

Description

Enter DNS Sinkhole mode.

Example

```
dns-sinkhole
```

Syntax

```
enable
```

Mode

DNS Sinkhole

Description

Enable DNS Sinkhole.

Example

```
enable
```

Syntax

```
no enable
```

Mode

DNS Sinkhole

Description

Disable DNS Sinkhole.

Example

```
no enable
```

Syntax

```
action-type { dropping-with-dns-reply-of-forged-ip <IPV4_HOST> <IPV6_HOST> | dropping-with-logs | dropping-with-negative-dns-reply-to-source }
```

Mode

DNS Sinkhole

Description

Set action type.

Options

| | |
|---|--|
| <code>dropping-with-dns-reply-of-forged-ip</code> <code><IPV4_HOST></code> | Dropping, with DNS reply of Forged IP IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| <code><IPV6_HOST></code> | IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b |
| <code>dropping-with-logs</code> | Dropping, with Logs |
| <code>dropping-with-negative-dns-reply-to-source</code> | Dropping, with negative DNS reply to Source |

Example

```
action-type dropping-with-logs  
action-type dropping-with-negative-dns-reply-to-source  
action-type dropping-with-dns-reply-of-forged-ip 127.0.0.1 ::1
```

Syntax

no custom-malicious-entries

Mode

DNS Sinkhole

Description

Delete all the custom malicious entries.

Example

no custom-malicious-entries

Syntax

no custom-malicious-entry <DNS_SINKHOLE_CUSTOM_MALI_DOMAIN_NAME>

Mode

DNS Sinkhole

Description

Delete the specified custom malicious entry.

Options

<DNS_SINKHOLE_CUSTOM_MALI_DOMAIN_NAME> Custom malicious domain name.
Example: *sonicwall.com*

Example

no custom-malicious-entry sonicwall.com

Syntax

custom-malicious-entry <DNS_SINKHOLE_CUSTOM_MALI_DOMAIN_NAME>

Mode

DNS Sinkhole

Description

Add custom malicious entry.

Options

<DNS_SINKHOLE_CUSTOM_MALI_DOMAIN_NAME> Custom malicious domain name.
Example: *sonicwall.com*

Example

custom-malicious-entry sonicwall.com

Syntax

no white-list-entries

Mode

DNS Sinkhole

Description

Delete all the white list entries.

Example

```
no white-list-entries
```

Syntax

```
no white-list-entry <DNS_SINKHOLE_WHITE_LIST_DOMAIN_NAME>
```

Mode

DNS Sinkhole

Description

Delete the specified white list entry.

Options

<DNS_SINKHOLE_WHITE_LIST_DOMAIN_NAME> White list domain name.
Example: *baidu.com*

Example

```
no white-list-entry sonicwall.com
```

Syntax

```
white-list-entry <DNS_SINKHOLE_WHITE_LIST_DOMAIN_NAME>
```

Mode

DNS Sinkhole

Description

Add white list entry.

Options

<DNS_SINKHOLE_WHITE_LIST_DOMAIN_NAME> White list domain name.
Example: *baidu.com*

Example

```
white-list-entry sonicwall.com
```

Syntax

```
dns-tunnel
```

Mode

DNS Security

Description

Enter DNS Tunnel mode.

Example

```
dns-tunnel
```

Syntax

enable

Mode

DNS Tunnel

Description

Enable DNS Tunnel detection.

Example

enable

Syntax

no enable

Mode

DNS Tunnel

Description

Disable DNS Tunnel detection.

Example

no enable

Syntax

block-all

Mode

DNS Tunnel

Description

Block DNS traffic for all the detected clients.

Example

block-all

Syntax

no block-all

Mode

DNS Tunnel

Description

Disable the operation of block DNS traffic.

Example

no block-all

Syntax

no white-list-entries

Mode

DNS Tunnel

Description

Delete all the white list entries.

Example

no white-list-entries

Syntax

no white-list-entry <IPV4_HOST>

Mode

DNS Tunnel

Description

Delete the specified white list entry.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

no white-list-entry 10.10.10.1

Syntax

white-list-entry <IPV4_HOST>

Mode

DNS Tunnel

Description

Add white list entry.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

white-list-entry 10.10.10.1

Syntax

block <IPV4_HOST>

Mode

DNS Tunnel

Description

Block DNS traffic for detected client per demand.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
block ip 10.10.10.1
```

Syntax

```
no block <IPV4_HOST>
```

Mode

DNS Tunnel

Description

Disable the operation of block DNS traffic for detected client per demand.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
block ip 10.10.10.1
```

Syntax

```
show tunnel-interface 4to6 <TUNNEL6_TUNNEL_INTERFACE> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show 4to6 tunnel interface configuration.

Options

<TUNNEL6_TUNNEL_INTERFACE> Tunnel6 tunnel interface name.
Example: tunnel6TunnelInterface

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show tunnel-interface tunnel CorpVPNTunnel
```

Syntax

```
show tunnel-interfaces 4to6 [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all 4to6 tunnel interfaces configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show tunnel-interfaces 4to6
```

Syntax

```
show interfaces [ [ ip ] | [ ipv4 | ipv6 ] [ { { { physical | vlan } [ pending-config ] } | statistics } ] | display-all-traffic | mac ]
```

Mode

All Modes

Description

Show all interfaces.

Options

| | |
|----------------------------|-------------------------------------|
| ip | Show interfaces IP. |
| ipv4 | Show all IPv4 interfaces. |
| ipv6 | Show all IPv6 interfaces. |
| physical | Show physical interfaces. |
| vlan | Show VLAN interfaces. |
| pending-config | Show pending configuration changes. |
| statistics | Show interfaces statistics. |
| display-all-traffic | Show interface statistics option. |
| mac | Show interfaces MAC. |

Example

```
show interfaces
```

Syntax

```
show interface [ ipv4 | ipv6 ] <CONFIGURABLE_INTERFACE> [ vlan <VLAN_TAG> ] [ tunnel <WLAN_TUNNEL_ID> ] [ { dialup { data-usage | session-details <WORD> | sessions | status } | ip | mac | pending-config | statistics } ]
```

Mode

All Modes

Description

Show interface configuration.

Options

| | |
|---------------------------------------|------------------------------------|
| ipv4 | Show IPv4 interface configuration. |
| ipv6 | Show IPv6 interface configuration. |
| <CONFIGURABLE_INTERFACE> | Interface name. Example: X0 |

| | |
|-------------------------------|--|
| vlan | Sub-interface VLAN. |
| <VLAN_TAG> | VLAN tag. Example: 23 |
| tunnel | Configure WLAN tunnel interface. |
| <WLAN_TUNNEL_ID> | WLAN tunnel ID. Example: 1 |
| dialup | Show 3G/Modem status, sessions, or usage. |
| data-usage | Show 3G data usage. |
| session-details | Show 3G session details for specified session. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: abc |
| sessions | Show 3G sessions. |
| status | Show 3G/Modem status. |
| ip | Show interface IP. |
| mac | Show interface MAC. |
| pending-config | Show pending configuration changes. |
| statistics | Show interface statistics. |

Example

```
show interface X1
show interface X1 vlan 100
show interface WT0
show interface X1 tunnel 1
show interface X1 vlan 100 tunnel 2
show interface WT1 vlan 200
show interface ipv6 X1
show interface ipv6 X1 vlan 100
show interface ipv6 WT0
show interface ipv6 X1 tunnel 1
show interface ipv6 X1 vlan 100 tunnel 2
show interface ipv6 WT1 vlan 200
show interface X1 ip
show interface X1 mac
show interface X1 statistics
show interface ipv6 X1 statistics
```

Syntax

```
show tunnel-interface vpn <VPN_TUNNEL_INTERFACE> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show VPN tunnel interface configuration.

Options

| | |
|-------------------------------------|---|
| <VPN_TUNNEL_INTERFACE> | VPN tunnel interface name. Example: vpnTunnelInterface |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show tunnel-interface vpn CorpVPNTunnel
```

Syntax

```
show tunnel-interfaces vpn [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all VPN tunnel interfaces configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show tunnel-interfaces vpn
```

Syntax

```
show dialup [ connection-profile <CONNECTION_PROFILE_NAME> | connection-profiles ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all 3G/4G/LTE/Modem configuration.

Options

connection-profile Show 3G/4G/LTE/Modem connection profile configuration.
<CONNECTION_PROFILE_NAME> Connection profile name.
Example: *AT&T (Standard)*

connection-profiles Show all 3G/4G/LTE/Modem connection profiles configuration.

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show dialup
```

Syntax

```
show arp [ cache | entries | entry <ARP_IPV4_HOST> <ARP_MAC> <ARP_INTERFACE> | statistics ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show ARP status or configuration.

Options

cache Show ARP cache.

| | |
|------------------------------|---|
| entries | Show all static ARP entries. |
| entry | Show a specified static ARP entry. |
| <ARP_IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| <ARP_MAC> | MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: 00:0C:F1:56:98:AD |
| <ARP_INTERFACE> | Interface name. Example: X0 |
| statistics | Show ARP statistics. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show arp
show arp entries
show arp entry 10.10.10.10 00:01:02:03:04:05 X0
show arp cache
show arp statistics
```

Syntax

```
show dns [ [ fqdn-binding | fqdn-over-tcp-dns | rebinding | servers [ ipv4 | ipv6 ] | split-servers ] [ { pending-config | with-pending-config } ] | cache [ interface-reverse ] ]
```

Mode

All Modes

Description

Show DNS configuration.

Options

| | |
|----------------------------|---|
| fqdn-binding | Show DNS binding for FQDN configuration. |
| fqdn-over-tcp-dns | Show DNS host name lookup over TCP for FQDN configuration. |
| rebinding | Show DNS rebinding attack prevention configuration. |
| servers | Show DNS server configuration. |
| ipv4 | Show IPv4 DNS server configuration. |
| ipv6 | Show IPv6 DNS server configuration. |
| split-servers | Show split DNS server configuration. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| cache | Show DNS cache. |
| interface-reverse | Show interface names reverse DNS cache. |

Example

```
show dns servers
```

Syntax

```
show dynamic-dns profiles [ ipv4 | ipv6 ] [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show all dynamic DNS profiles.

Options

| | |
|----------------------------|---|
| ipv4 | Show IPv4 dynamic DNS profiles. |
| ipv6 | Show IPv6 dynamic DNS profiles. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| status | Show all dynamic DNS profiles status. |

Example

```
show dynamic-dns profiles
```

Syntax

```
show dynamic-dns profile [ ipv4 | ipv6 ] <DDNS_PROFILE_NAME> [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show dynamic DNS profile.

Options

| | |
|----------------------------------|---|
| ipv4 | Show IPv4 dynamic DNS profile. |
| ipv6 | Show IPv6 dynamic DNS profile. |
| <DDNS_PROFILE_NAME> | Dynamic DNS profile name. Example: <i>mydns</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| status | Show a dynamic DNS profile status. |

Example

```
show dynamic-dns profile DynDNS.org
```

Syntax

```
show dhcp-server [ [ ipv6 [ [ leases [ statistic ] | option { { group <DHCP_OPTION_GROUP> | groups | object <DHCP_OPTION_OBJECT> | objects } } ] | scope { { dynamic <DHCP_IPV6_DYNAMIC_SCOPE_NAME> | static <DHCP_IPV6_STATIC_SCOPE_NAME> } } ] | scopes { { dynamic | static } } ] ] ] | [ ipv4 [ [ leases [ statistic ] | option { { group <DHCP_OPTION_GROUP> | groups | object <DHCP_OPTION_OBJECT> | objects } } ] | scope { { dynamic <SCOPE_START_IPV4_HOST> <SCOPE_END_IPV4_HOST> | static <STATIC_SCOPE_IPV4_HOST> <STATIC_SCOPE_MAC> } } ] | scopes { { dynamic | static } } ] ] ] [ { pending-config | with-pending-config } ] ]
```

Mode

Description

Show DHCP server configuration.

Options

| | |
|--|--|
| ipv6 | Show IPv6 DHCP server configuration. |
| leases | Show IPv6 DHCP server leases. |
| statistic | Show IPv6 DHCP server leases status. |
| option | IPv6 DHCP server option configuration. |
| group <DHCP_OPTION_GROUP> | Specify option group. DHCP server option group name. Example: <i>Corp Network DHCP Group</i> |
| groups | IPv6 DHCP server all option groups. |
| object <DHCP_OPTION_OBJECT> | Specify option object. DHCP server option object name. Example: <i>Corp Network DHCP Options</i> |
| objects | IPv6 DHCP server all option objects. |
| scope | IPv6 DHCP server static or dynamic scope. |
| dynamic <DHCP_IPV6_DYNAMIC_SCOPE_NAME> | IPv6 DHCP server dynamic configuration. IPv6 DHCP server dynamic scope name. Example: <i>abc</i> |
| static <DHCP_IPV6_STATIC_SCOPE_NAME> | IPv6 DHCP server static configuration. IPv6 DHCP server static scope name. Example: <i>abc</i> |
| scopes | IPv6 DHCP server all static or dynamic scopes. |
| dynamic | IPv6 DHCP server dynamic configuration. |
| static | IPv6 DHCP server static configuration. |
| ipv4 | Show IPv4 DHCP server configuration. |
| leases | Show DHCP server leases. |
| statistic | Show DHCP server leases status. |
| option | DHCP server option configuration. |
| group <DHCP_OPTION_GROUP> | Specify option group. DHCP server option group name. Example: <i>Corp Network DHCP Group</i> |
| groups | All option groups. |
| object <DHCP_OPTION_OBJECT> | Specify option object. DHCP server option object name. Example: <i>Corp Network DHCP Options</i> |
| objects | All option objects. |
| scope | DHCP server static or dynamic scope. |
| dynamic <SCOPE_START_IPV4_HOST> <SCOPE_END_IPV4_HOST> | DHCP server dynamic configuration. IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |

| | |
|---------------------------------------|---|
| static | DHCP server static configuration. |
| <STATIC_SCOPE_IPV4_HOST> | IPv4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| <STATIC_SCOPE_MAC> | MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: 00:0C:F1:56:98:AD |
| scopes | DHCP server all static or dynamic scopes. |
| dynamic | DHCP server dynamic configuration. |
| static | DHCP server static configuration. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show dhcp-server
```

Syntax

```
show failover-lb [ group <FLB_GROUP_NAME> | responder | statistics | status [ group | member ] ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show failover and load balancing status or configuration.

Options

| | |
|-------------------------------|---|
| group | Show failover and load balancing group configuration. |
| <FLB_GROUP_NAME> | Failover & LB group name. Example: myFLBGroup |
| responder | Show status for respond to probes. |
| statistics | Show failover and load balancing statistics. |
| status | Show status of failover and load balancing. |
| group | Show status of all failover and load balancing groups. |
| member | Show status of all failover and load balancing group members. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show failover-lb
show failover-lb status
show failover-lb statistics
```

Syntax

```
show ip-helper [ { policies | protocol <IPH_PROTOCOL> | protocols } [ statistics ] | dhcp-relay-leases | dhcpv6-relay-leases ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show IP helper status or configuration.

Options

| | |
|---|--|
| <i>policies</i> | Show all IP helper policies. |
| <i>protocol</i> <IPH_PROTOCOL> | Show an IP helper relay protocol. IP Helper relay protocol name. Example: <i>mydns</i> |
| <i>protocols</i> | Show all IP helper relay protocols. |
| <i>statistics</i> | Show statistics for policies or specified protocol. |
| <i>dhcp-relay-leases</i> | Show all IP helper DHCP relay leases. |
| <i>dhcpv6-relay-leases</i> | Show all IP helper DHCPv6 relay leases. |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |

Example

```
show ip-helper
```

Syntax

```
show mac-ip-anti-spoof [ ipv4 | ipv6 ] [ cache { { entries [ status ] | entry <MAC_IP_ANTI_SPOOF_STATIC_IP>  
<MAC_IP_ANTI_SPOOF_STATIC_MAC> <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE> } } | detected-list | interface <MAC_IP_ANTI_SPOOF_INTERFACE>  
| interfaces | lookup-statistics } [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show MAC-IP anti-spoof configuration and information.

Options

| | |
|---|--|
| <i>ipv4</i> | Show IPv4 MAC-IP anti-spoof configuration. |
| <i>ipv6</i> | Show IPv6 MAC-IP anti-spoof configuration. |
| <i>cache</i> | Show MAC-IP anti-spoof cache. |
| <i>entries</i> | Show all MAC anti-spoof cache entries. |
| <i>status</i> | Show all MAC-IP anti-spoof cache entries status. |
| <i>entry</i> <MAC_IP_ANTI_SPOOF_STATIC_IP> | Show an MAC anti-spoof cache entry. MAC-IP anti-spoof static ip. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i> |
| <MAC_IP_ANTI_SPOOF_STATIC_MAC> | MAC-IP anti-spoof static mac. Example: <i>00:0C:F1:56:98:AD</i> |
| <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE> | MAC-IP anti-spoof enabled static interface. Example: <i>X0</i> |
| <i>detected-list</i> | Show MAC-IP anti-spoof spoof detected list. |
| <i>interface</i> <MAC_IP_ANTI_SPOOF_INTERFACE> | Show MAC-IP anti-spoof interface configuration. MAC-IP anti-spoof interface. Example: <i>X0</i> |

| | |
|----------------------------|---|
| interfaces | Show MAC-IP anti-spoof configuration for all interfaces. |
| lookup-statistics | Show MAC-IP anti-spoof lookup statistics. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show mac-ip-anti-spoof
```

Syntax

```
show nat-policies [ ipv4 | ipv6 | nat64 ] [ statistics ] [ { custom | default } ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all NAT policies.

Options

| | |
|----------------------------|---|
| ipv4 | Show only IPv4 NAT policies. |
| ipv6 | Show only IPv6 NAT policies. |
| nat64 | Show only NAT64 policies. |
| statistics | Show statistics for all nat policies. |
| custom | Show custom configuration. |
| default | Show system/factory default configuration. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show nat-policies
```

Syntax

```
show nat-policy ipv4 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ statistics ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NAT policy.

Options

| | |
|--------------------------------|--|
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| outbound | Outbound interface. |
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| source | Original source ("Any" if not specified). |
| any | Any host. |
| fqdn | FQDN. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| translated-source | Translated source ("Original" if not specified). |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| original | Original source IP. |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| destination | Original destination ("Any" if not specified). |

any Any host.

fqdn FQDN.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
 Example: *example.com*

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
 Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_NAME> Address object name.
 Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
 Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

translated-destination Translated destination ("Original" if not specified).

embedded-ipv4-address Embedded ipv4 address.

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
 Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_NAME> Address object name.
 Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
 Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

original Original destination IP.

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

service Original service ("Any" if not specified).

any Any service.

group Service group.

| | |
|-------------------------------|---|
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| icmp-udp-tcp | ICMP UDP TCP service. |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| translated-service | Translated service ("Original" if not specified). |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| original | Original service. |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| statistics | Show statistics for specified nat policy. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show nat-policy inbound X3 outbound X4 source any translated-source original destination name "Web Server Public" translated-destination name "Web Server Private" service "My Web Services" translated-service original
```

Syntax

```
show nat-policy ipv6 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ statistics ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show IPv6 NAT policy.

Options

| | |
|------------------------------|---------------------------------------|
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| outbound | Outbound interface. |

| | |
|--------------------------------|--|
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| source | Original source ("Any" if not specified). |
| any | Any host. |
| fqdn | FQDN. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| translated-source | Translated source ("Original" if not specified). |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| original | Original source IP. |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| destination | Original destination ("Any" if not specified). |
| any | Any host. |
| fqdn | FQDN. |

<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address object group.

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

translated-destination Translated destination ("Original" if not specified).

embedded-ipv4-address Embedded ipv4 address.

group Address object group.

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

original Original destination IP.

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

service Original service ("Any" if not specified).

any Any service.

group Service group.

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

icmp-udp-tcp ICMP UDP TCP service.

| | |
|-------------------------------|---|
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| translated-service | Translated service ("Original" if not specified). |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| original | Original service. |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| statistics | Show statistics for specified nat policy. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show nat-policy ipv6 inbound X3 outbound X4 source any translated-source original destination name "Web Server Public" translated-destination name "Web Server Private" service "My Web Services" translated-service original
```

Syntax

```
show nat-policy nat64 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ pref64 { { any | group <ADDR_GROUP_NAME> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> } } ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ statistics ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NAT64 policy.

Options

| | |
|------------------------------|---------------------------------------|
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| outbound | Outbound interface. |
| <NAT_INTERFACE> | Interface name. Example: <i>X0</i> |
| source | Original source. |

any Any host.

fqdn FQDN.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
 Example: *example.com*

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
 Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_NAME> Address object name.
 Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*
<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
 Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*
<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

translated-source Translated source.

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
 Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_NAME> Address object name.
 Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*
<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
 Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

original Original address IP.

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*
<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

pref64 Original destination.

any Any host.

group Address object group.
<ADDR_GROUP_NAME> Group address object name.
 Example: *Sales Group*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

translated-destination Translated destination.

embedded-ipv4-address Embedded ipv4 address.

group Address object group.

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

original Original destination IP.

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

service Original service.

any Any service.

group Service group.

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

icmp-udp-tcp ICMP UDP TCP service.

name Service object name.

<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Service object protocol.

<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

translated-service Translated service.

group Service group.

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

name Service object name.

<SVC_NAME> Service object name.

Example: *HTTPS*

| | |
|-------------------------------|---|
| <i>original</i> | Original service. |
| <i>protocol</i> | Service object protocol. |
| <i><SVC_PROTOCOL></i> | Service protocol. Example: <i>TCP</i> |
| <i><SVC_PORT_BEGIN></i> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <i><SVC_PORT_END></i> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <i>statistics</i> | Show statistics for specified nat policy. |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |

Example

```
show nat-policy nat64 inbound X3 outbound X4 source any translated-source X1 pref64 name nat64A0 translated-destination embedded-ipv4-address service icmp-udp-tcp translated-service original
```

Syntax

```
show nat-policy ipv4 uuid <UUID> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NAT policy by associated UUID.

Options

| | |
|----------------------------|---|
| <i><UUID></i> | Universally Unique Identifier (UUID). Min: 36 Max: 36 Example: <i>138a224d-c4c7-d621-0a00-c0eae49ce84c</i> |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |

Example

```
show nat-policy ipv4 uuid 3824336935410777187
```

Syntax

```
show nat-policy ipv6 uuid <UUID> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NAT policy by associated UUID.

Options

| | |
|-----------------------|---|
| <i><UUID></i> | Universally Unique Identifier (UUID). Min: 36 Max: 36 Example: <i>138a224d-c4c7-d621-0a00-c0eae49ce84c</i> |
| <i>pending-config</i> | Show pending configuration changes. |

with-pending-config View current configuration with pending changes included in the output.

Example

```
show nat-policy ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
show nat-policy nat64 uuid <UUID> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NAT policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: `138a224d-c4c7-d621-0a00-c0eae49ce84c`

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show nat-policy nat64 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
show nat-policy ipv4 name <NAT_POLICY_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NAT policy by associated name.

Options

<NAT_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: `abc`

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show nat-policy ipv4 name "OfficeNatPolicy"
```

Syntax

```
show nat-policy ipv6 name <NAT_POLICY_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NAT policy by associated name.

Options

<NAT_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show nat-policy ipv6 name "OfficeNatPolicyV6"
```

Syntax

```
show nat-policy nat64 name <NAT_POLICY_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NAT policy by associated name.

Options

<NAT_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show nat-policy nat64 name "OfficeNatPolicy64"
```

Syntax

```
show network-monitor policies [ ipv4 | ipv6 ] [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show all network monitor policies.

Options

ipv4 Show IPv4 network monitor policies.

ipv6 Show IPv6 network monitor policies.

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

status Show all network monitor policies status.

Example

```
show network-monitor policies
```

Syntax

```
show network-monitor policy [ ipv4 | ipv6 ] <NETMON_NAME> [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show network monitor policy.

Options

| | |
|----------------------------|---|
| ipv4 | Show IPv4 network monitor policies. |
| ipv6 | Show IPv6 network monitor policy. |
| <NETMON_NAME> | Atom Object name. Example: <i>Web Services Monitor</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| status | Show a specific network monitor policy status. |

Example

```
show network-monitor policy "Remote Servers"
```

Syntax

```
show routing mode [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show routing mode.

Options

| | |
|----------------------------|---|
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show routing mode
```

Syntax

```
show route-policies [ ipv4 | ipv6 ] [ { dynamic | system } ] [ { custom | default } ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all route policies.

Options

| | |
|----------------------------|---|
| ipv4 | Show only IPv4 route policies. |
| ipv6 | Show only IPv6 route policies. |
| dynamic | Show all dynamic route policies. |
| system | Show all ephemeral system route policies. |
| custom | Show custom configuration. |
| default | Show system/factory default configuration. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show route-policies
```

Syntax

```
show route-policy ipv4 interface <ROUTING_INTERFACE_NAME> metric <UINT8> [ source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name <ROUTING_POLICY_DEST_FHNR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ gateway { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ path-selection-profile <ROUTE_PATH_SELECTION_PROFILE_NAME> ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show a route policy.

Options

| | |
|--|--|
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| metric | Route policy metric. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| source | Route policy source. |
| any | Any host. |
| group <ADDR_GROUP_NAME> | Address group name. Group address object name. Example: <i>Sales Group</i> |
| host <ADDR_HOST> | Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <ADDR_HOST_NETWORK_RANGE_NAME> | Address object name. Host/network/range address object name. Example: <i>Web Server</i> |
| network <ADDR_NETWORK> | Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: |

| | |
|--|---|
| | <p>HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n</p> <p>Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i></p> |
| <ADDR_MASK> | <p>IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n</p> <p>Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i></p> |
| range | Address object range. |
| <ADDR_BEGIN> | <p>IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n</p> <p>Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i></p> |
| <ADDR_END> | <p>IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n</p> <p>Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i></p> |
| destination | Route policy destination. |
| any | Any host. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | <p>FQDN in the form: example.com or *.example.com.</p> <p>Example: <i>example.com</i></p> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | <p>Group address object name.</p> <p>Example: <i>Sales Group</i></p> |
| host | Address object host. |
| <ADDR_HOST> | <p>IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n</p> <p>Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i></p> |
| name | Address object name. |
| <ROUTING_POLICY_DEST_FHNR_NAME> | <p>FQDN/host/network/range address object name.</p> <p>Example: <i>Web Server</i></p> |
| network | Address object network. |
| <ADDR_NETWORK> | <p>IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n</p> <p>Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i></p> |
| <ADDR_MASK> | <p>IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n</p> <p>Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i></p> |
| range | Address object range. |
| <ADDR_BEGIN> | <p>IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n</p> <p>Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i></p> |
| <ADDR_END> | <p>IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n</p> <p>Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i></p> |
| service | Route policy service. |
| any | Any service. |
| group | Service group. |
| <SVC_GROUP_NAME> | <p>Service object group name.</p> <p>Example: <i>VOIP</i></p> |
| name | Service object name. |
| <SVC_NAME> | <p>Service object name.</p> <p>Example: <i>HTTPS</i></p> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | <p>Service protocol.</p> <p>Example: <i>TCP</i></p> |
| <SVC_PORT_BEGIN> | <p>Integer in the form: D OR 0xHHHH.</p> <p>Example: <i>80</i></p> |
| <SVC_PORT_END> | <p>Integer in the form: D OR 0xHHHH.</p> <p>Example: <i>80</i></p> |
| gateway | Route policy gateway. |
| default | Default gateway 0.0.0.0/: |
| host | Gateway IP. |

| | |
|--|--|
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| path-selection-profile | Route policy SD-WAN path selection profile. |
| <ROUTE_PATH_SELECTION_PROFILE_NAME> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show route-policy interface X4 metric 255 service name "FTP"
```

Syntax

```
show route-policy ipv6 interface <ROUTING_INTERFACE_NAME> metric <UINT8> [ source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name <ROUTING_POLICY_DEST_FHNR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ gateway { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show an IPv6 route policy.

Options

| | |
|---|--|
| <ROUTING_INTERFACE_NAME> | Route interface name. Example: <i>X0</i> |
| metric | Route policy metric. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| source | Route policy source. |
| any | Any host. |
| group | Address group name. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NETWORK_RANGE_NAME> | Host/network/range address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |

| | |
|--|---|
| | <pre> HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n </pre> |
| destination | Route policy destination. |
| any | Any host. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ROUTING_POLICY_DEST_FHNR_NAME> | FQDN/host/network/range address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| service | Route policy service. |
| any | Any service. |
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| gateway | Route policy gateway. |
| default | Default gateway 0.0.0.0:: |
| host | Gateway IP. |
| <ADDR_HOST> | IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_NAME> | Host address object name. Example: <i>Web Server</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show route-policy ipv6 interface X4 metric 255 service name "FTP"
```

Syntax

```
show route-policy ipv4 uuid <UUID>
```

Mode

All Modes

Description

Show an IPv4 route policy by associated ID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
show route-policy ipv4 id 3
```

Syntax

```
show route-policy ipv6 uuid <UUID>
```

Mode

All Modes

Description

Show an IPv6 route policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
show route-policy ipv6 id 3
```

Syntax

```
show route-policy ipv4 name <ROUTING_POLICY_NAME>
```

Mode

All Modes

Description

Show an IPv4 route policy by associated name.

Options

<ROUTING_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
show route-policy ipv4 name "Default Route - IPv4"
```

Syntax

```
show route-policy ipv6 name <ROUTING_POLICY_NAME>
```

Mode

All Modes

Description

Show an IPv6 route policy by associated name.

Options

<ROUTING_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
show route-policy ipv6 name "Default Route - IPv6"
```

Syntax

```
show routing nsm [ database | interface ]
```

Mode

All Modes

Description

Show routing NSM status or configuration.

Options

database Database summary.

interface Interface status and configuration.

Example

```
show routing nsm
```

Syntax

```
show routing rip [ database ]
```

Mode

All Modes

Description

Show routing RIP status or configuration.

Options

database Database summary.

Example

```
show routing rip
```

Syntax

```
show routing ospf [ database | neighbor | routes ]
```

Mode

All Modes

Description

Show routing OSPF status or configuration.

Options

database Database summary.

neighbor Neighbor list.

routes OSPF routing table.

Example

```
show routing ospf
```

Syntax

```
show routing bgp [ neighbor | summary | unicast ]
```

Mode

All Modes

Description

Show routing BGP status or configuration.

Options

neighbor Neighbor list.

summary Summary of BGP neighbor status.

unicast

Example

```
show routing bgp
```

Syntax

```
show routing ripng [ database ]
```

Mode

All Modes

Description

Show routing RIPNG status or configuration.

Options

database Database summary.

Example

```
show routing ripng
```

Syntax

```
show routing ospfv3 [ database | neighbor | routes ]
```

Mode

All Modes

Description

Show routing OSPFv3 status or configuration.

Options

database Database summary.

neighbor Neighbor list.

routes OSPF routing table.

Example

```
show routing ospfv3
```

Syntax

```
show web-proxy [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show web proxy configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show web-proxy
```

Syntax

```
show ndp [ cache | entries | entry <NDP_IPV6_HOST> <NDP_MAC> <NDP_INTERFACE> ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NDP status or configuration.

Options

cache Show NDP caches.

entries Show all static NDP entries.

entry Show a static NDP entry.

<NDP_IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

<NDP_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD

<NDP_INTERFACE> Interface name.
Example: X0

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show ndp entries
show ndp
show ndp entry 2001:10:10:10:2D0:02BB:03CC:04DD 02:BB:03:CC:04:DD X0
show ndp cache
```

Syntax

```
show tunnel-interface ipv6 <IPv6_TUNNEL_INTERFACE> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show IPv6 tunnel interface configuration.

Options

<IPv6_TUNNEL_INTERFACE> IPv6 Interface name.
Example: myTunnelInterface

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show tunnel-interface ipv6 CorpIPv6Tunnel
```

Syntax

```
show tunnel-interfaces ipv6 [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all IPv6 tunnel interfaces configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show tunnel-interfaces ipv6
```

Syntax

```
show vlan-translation { ingress interface <VLAN_TRANSLATION_INGRESS_IFACE_NAME> vlan <VLAN_TRANSLATION_INGRESS_VLAN_ID> egress
interface <VLAN_TRANSLATION_EGRESS_IFACE_NAME> vlan <VLAN_TRANSLATION_EGRESS_VLAN_ID> } [ { pending-config | with-pending-config }
| status ]
```

Mode

All Modes

Description

Show VLAN translation configuration or status.

Options

| | |
|--|---|
| ingress | VLAN translation ingress. |
| interface | Ingress interface. |
| <VLAN_TRANSLATION_INGRESS_IFACE_NAME> | Ingress interface name. Example: X0 |
| vlan | Ingress VLAN tag. |
| <VLAN_TRANSLATION_INGRESS_VLAN_ID> | Interface VLAN id. Example: 23 |
| egress | VLAN translation egress. |
| interface | Egress interface. |
| <VLAN_TRANSLATION_EGRESS_IFACE_NAME> | Egress interface name. Example: X0 |
| vlan | Egress VLAN tag. |
| <VLAN_TRANSLATION_EGRESS_VLAN_ID> | Interface VLAN id. Example: 23 |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| status | Show VLAN translation configuration status. |

Example

```
show vlan-translation ingress interface X1 vlan 111 egress interface X2 vlan 222
show vlan-translation ingress interface X1 vlan 111 egress interface X2 vlan 222 status
```

Syntax

```
show vlan-translations [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show all VLAN translations configuration or status.

Options

| | |
|----------------------------|---|
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| status | Show all VLAN translations status. |

Example

```
show vlan-translations
show vlan-translations status
```

Syntax

```
show dns-security [ [ dns-sinkhole | dns-tunnel ] [ { pending-config | with-pending-config } ] | status { sinkhole-statistical | tunnel-clients } ]
```

Mode

All Modes

Description

Show DNS Security configuration.

Options

| | |
|------------------------------------|---|
| <i>dns-sinkhole</i> | Show DNS Sinkhole configuration. |
| <i>dns-tunnel</i> | Show DNS Tunnel detection configuration. |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |
| <i>status</i> | Show the DNS Security status. |
| <i>sinkhole-statistical</i> | Show the DNS Security DNS Sinkhole statistical status. |
| <i>tunnel-clients</i> | Show the DNS Security DNS tunnel detected clients status. |

Example

```
show dns-security
show dns-security dns-sinkhole
show dns-security dns-tunnel
show dns-security status sinkhole-statistical
show dns-security status tunnel-clients
```

Syntax

```
firewall
```

Mode

Config

Description

Configure firewall settings.

Example

```
firewall
```

Syntax

```
stealth-mode
```

Mode

All Modes

Description

Enable stealth mode.

Example

```
stealth-mode
```

Syntax

no stealth-mode

Mode

All Modes

Description

Disable stealth mode.

Example

no stealth-mode

Syntax

randomize-id

Mode

All Modes

Description

Enable randomize IP ID.

Example

randomize-id

Syntax

no randomize-id

Mode

All Modes

Description

Disable randomize IP ID.

Example

no randomize-id

Syntax

decrement ttl

Mode

All Modes

Description

Enable decrement IP TTL for forwarded traffic.

Example

decrement ttl

Syntax

```
no decrement ttl
```

Mode

All Modes

Description

Disable decrement IP TTL for forwarded traffic.

Example

```
no decrement ttl
```

Syntax

```
icmp time-exceeded-packets
```

Mode

All Modes

Description

Generate ICMP time-exceeded packets.

Example

```
icmp time-exceeded-packets
```

Syntax

```
no icmp time-exceeded-packets
```

Mode

All Modes

Description

Never generate ICMP time-exceeded packets.

Example

```
no icmp time-exceeded-packets
```

Syntax

```
ftp-transforms-in-service-object { group <SVC_GROUP_NAME> | name <SVC_NAME> }
```

Mode

All Modes

Description

Enable FTP transformations for TCP port(s) in service object.

Options

| | |
|-------------------------------|--|
| group | Service group name. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. |

Example: *HTTPS*

Example

ftp-transforms-in-service-object name Ping

Syntax

sqlnet

Mode

All Modes

Description

Enable support for oracle (SQLNet).

Example

sqlnet

Syntax

no sqlnet

Mode

All Modes

Description

Disable support for oracle (SQLNet).

Example

no sqlnet

Syntax

rtsp-transformations

Mode

All Modes

Description

Enable RTSP transformations.

Example

rtsp-transformations

Syntax

no rtsp-transformations

Mode

All Modes

Description

Disable RTSP transformations.

Example

```
no rtsp-transformations
```

Syntax

```
drop source-routed
```

Mode

All Modes

Description

Enable drop source routed IP packets.

Example

```
drop source-routed
```

Syntax

```
no drop source-routed
```

Mode

All Modes

Description

Disable drop source routed IP packets.

Example

```
no drop source-routed
```

Syntax

```
starting-vlan <UINT16>
```

Mode

All Modes

Description

Set starting VLAN ID.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
starting-vlan 2
```

Syntax

```
connections { highest | optimized | recommended }
```

Mode

All Modes

Description

Set the type of connections.

Options

highest UTM services (application firewall, anti-spyware, gateway AV, and IPS engine) disabled for highest number of SPI connections.

optimized Optimized for deployments requiring more UTM connections but less performance critical.

recommended Recommended for normal deployments with UTM services enabled.

Example

```
connections highest
```

Syntax

```
force-ftp-data
```

Mode

All Modes

Description

Force inbound and outbound FTP data connections to use the default port: 20.

Example

```
force-ftp-data
```

Syntax

```
no force-ftp-data
```

Mode

All Modes

Description

Disable force inbound and outbound FTP data connections to use the default port: 20.

Example

```
no force-ftp-data
```

Syntax

```
apply-rules-for-intra-lan
```

Mode

All Modes

Description

Enable apply firewall rules for intra-LAN traffic to/from the same interface.

Example

```
apply-rules-for-intra-lan
```

Syntax

```
no apply-rules-for-intra-lan
```

Mode

All Modes

Description

Disable apply firewall rules for intra-LAN traffic to/from the same interface.

Example

```
no apply-rules-for-intra-lan
```

Syntax

```
issue-rst-for-outgoing-discards
```

Mode

All Modes

Description

Enable always issue RST for discarded outgoing TCP connections.

Example

```
issue-rst-for-outgoing-discards
```

Syntax

```
no issue-rst-for-outgoing-discards
```

Mode

All Modes

Description

Disable always issue RST for discarded outgoing TCP connections.

Example

```
no issue-rst-for-outgoing-discards
```

Syntax

```
icmp redirect-on-lan
```

Mode

All Modes

Description

Enable ICMP redirect on LAN zone.

Example

```
icmp redirect-on-lan
```

Syntax

```
no icmp redirect-on-lan
```

Mode

All Modes

Description

Disable ICMP redirect on LAN zone.

Example

```
no icmp redirect-on-lan
```

Syntax

```
ip checksum-enforcement
```

Mode

All Modes

Description

Enable IP header checksum enforcement.

Example

```
ip checksum-enforcement
```

Syntax

```
no ip checksum-enforcement
```

Mode

All Modes

Description

Disable IP header checksum enforcement.

Example

```
no ip checksum-enforcement
```

Syntax

```
udp checksum-enforcement
```

Mode

All Modes

Description

Enable UDP checksum enforcement.

Example

```
udp checksum-enforcement
```

Syntax

```
no udp checksum-enforcement
```

Mode

All Modes

Description

Disable UDP checksum enforcement.

Example

```
no udp checksum-enforcement
```

Syntax

```
jumbo-frame
```

Mode

All Modes

Description

Enable support jumbo frame.

Example

```
jumbo-frame
```

Syntax

```
no jumbo-frame
```

Mode

All Modes

Description

Disable support jumbo frame.

Example

```
no jumbo-frame
```

Syntax

```
ipv6 drop { all-traffic | reserved-address-packets | routing-header-0 }
```

Mode

All Modes

Description

Configure firewall IPv6 drop actions.

Options

- | | |
|--|---|
| <i>all-traffic</i> | Enable drop all IPv6 traffic processing on this firewall. |
| <i>reserved-address-packets</i> | Enable drop and log network packets whose source or destination address is reserved by RFC. |
| <i>routing-header-0</i> | Enable drop IPv6 routing header type 0 packets. |

Example

```
ipv6 drop all-ipv6-traffic  
ipv6 drop routing-header-0  
ipv6 drop reserved-address-packets
```

Syntax

```
no ipv6 drop { all-traffic | reserved-address-packets | routing-header-0 }
```

Mode

All Modes

Description

Configure firewall IPv6 drop actions.

Options

| | |
|--|--|
| <i>all-traffic</i> | Disable drop all IPv6 traffic processing on this firewall. |
| <i>reserved-address-packets</i> | Disable drop and log network packets whose source or destination address is reserved by RFC. |
| <i>routing-header-0</i> | Disable drop IPv6 routing header type 0 packets. |

Example

```
no ipv6 all-ipv6-traffic
no ipv6 drop routing-header-0
no ipv6 drop reserved-address-packets
```

Syntax

```
ipv6 decrement hop-limit
```

Mode

All Modes

Description

Enable decrement IPv6 hop limit for forwarded traffic.

Example

```
ipv6 decrement hop-limit
```

Syntax

```
no ipv6 decrement hop-limit
```

Mode

All Modes

Description

Disable decrement IPv6 hop limit for forwarded traffic.

Example

```
no ipv6 decrement hop-limit
```

Syntax

```
ipv6 icmp { destination-unreachable | parameter-problem | redirect | time-exceeded }
```

Mode

All Modes

Description

Set IPv6 ICMP packets.

Options

| | |
|---------------------------------------|--|
| <i>destination-unreachable</i> | Generate IPv6 ICMP destination unreachable packets |
| <i>parameter-problem</i> | Generate IPv6 ICMP parameter problem packets |
| <i>redirect</i> | Generate IPv6 ICMP redirect packets |
| <i>time-exceeded</i> | Generate IPv6 ICMP time-exceeded packets |

Example

```
ipv6 icmp time-exceeded
ipv6 icmp destination-unreachable
ipv6 icmp redirect
ipv6 icmp parameter-problem
```

Syntax

```
no ipv6 icmp { destination-unreachable | parameter-problem | redirect | time-exceeded }
```

Mode

All Modes

Description

Set IPv6 ICMP packets.

Options

| | |
|---------------------------------------|--|
| <i>destination-unreachable</i> | Never generate IPv6 ICMP destination unreachable packets |
| <i>parameter-problem</i> | Never generate IPv6 ICMP parameter problem packets |
| <i>redirect</i> | Never generate IPv6 ICMP redirect packets |
| <i>time-exceeded</i> | Never generate IPv6 ICMP time-exceeded packets |

Example

```
no ipv6 icmp time-exceeded
no ipv6 icmp destination-unreachable
no ipv6 icmp redirect
no ipv6 icmp parameter-problem
```

Syntax

```
ipv6 site-local-unicast
```

Mode

All Modes

Description

Enable allow to use site-local-unicast address.

Example

```
ipv6 site-local-unicast
```

Syntax

no ipv6 site-local-unicast

Mode

All Modes

Description

Disable allow to use site-local-unicast address.

Example

no ipv6 site-local-unicast

Syntax

ipv6 extension-header-check

Mode

All Modes

Description

Enable enforce IPv6 extension header validation.

Example

ipv6 extension-header-check

Syntax

no ipv6 extension-header-check

Mode

All Modes

Description

Disable enforce IPv6 extension header validation.

Example

no ipv6 extension-header-check

Syntax

ipv6 extension-header-order-check

Mode

All Modes

Description

Enable enforce IPv6 extension header order check.

Example

ipv6 extension-header-order-check

Syntax

```
no ipv6 extension-header-order-check
```

Mode

All Modes

Description

Disable enforce IPv6 extension header order check.

Example

```
no ipv6 extension-header-order-check
```

Syntax

```
ipv6 netbios-for-isatap
```

Mode

All Modes

Description

Enable NetBIOS name query response for ISATAP.

Example

```
ipv6 netbios-for-isatap
```

Syntax

```
no ipv6 netbios-for-isatap
```

Mode

All Modes

Description

Disable NetBIOS name query response for ISATAP.

Example

```
no ipv6 netbios-for-isatap
```

Syntax

```
control-plane-flood-protection [ threshold <UINT8> ]
```

Mode

All Modes

Description

Enable control plane flood protection and set the threshold (CPU %).

Options

threshold Set the threshold (CPU %).
<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
control-plane-flood-protection
control-plane-flood-protection threshold 75
```

Syntax

```
no control-plane-flood-protection
```

Mode

All Modes

Description

Disable control plane flood protection.

Example

```
no control-plane-flood-protection
```

Syntax

```
bandwidth-management
```

Mode

Config

Description

Enter bandwidth management configuration mode.

Example

```
bandwidth-management
```

Syntax

```
no type
```

Mode

Bandwidth Mangement

Description

Diabile bandwidth management type.

Example

```
no type
```

Syntax

```
type { advanced | global }
```

Mode

Bandwidth Mangement

Description

Set bandwidth management type.

Options

advanced Advanced.

global Global.

Example

```
type global
```

Syntax

```
priority { high | highest | low | lowest | medium | medium-high | medium-low | realtime } [ guaranteed <UINT8> ] [ maximum <UINT8> ]
```

Mode

Bandwidth Mangement

Description

Set the specified priority.

Options

high High 2.

highest Highest 1.

low Low 6.

lowest Lowest 7.

medium Medium 4.

medium-high Medium-high 3.

medium-low Medium-low 5.

realtime Realtime 0.

guaranteed Guaranteed percent.

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

maximum Maximum/burst percent.

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
priority medium-high guaranteed 30 maximum 80
```

Syntax

```
no priority { high | highest | low | lowest | medium | medium-high | medium-low | realtime }
```

Mode

Bandwidth Mangement

Description

Disable the specified priority.

Options

high High 2.

highest Highest 1.

| | |
|--------------------|----------------|
| low | Low 6. |
| lowest | Lowest 7. |
| medium | Medium 4. |
| medium-high | Medium-high 3. |
| medium-low | Medium-low 5. |
| realtime | Realtime 0. |

Example

```
no priority medium-low
```

Syntax

```
no multicast
```

Mode

Config

Description

Disable multicast.

Example

```
no multicast
```

Syntax

```
multicast
```

Mode

Config

Description

Configure multicast.

Example

```
multicast
```

Syntax

```
require-igmp-membership [ timeout <UINT8> ]
```

Mode

Multicast

Description

Enable require IGMP membership reports for multicast data forwarding.

Options

- timeout** Set the multicast state table entry timeout in minutes.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123

Example

```
require-igmp-membership
```

Syntax

```
no require-igmp-membership
```

Mode

Multicast

Description

Disable require IGMP membership reports for multicast data forwarding.

Example

```
no require-igmp-membership
```

Syntax

```
reception { all | group <MULTICAST_ADDR_GROUP_NAME> | host <MULTICAST_ADDR_HOST> | name <MULTICAST_ADDR_NAME> | network <MULTICAST_ADDR_NETWORK> <MULTICAST_ADDR_MASK> | range <MULTICAST_ADDR_BEGIN> <MULTICAST_ADDR_END> }
```

Mode

Multicast

Description

Enable reception for the specified multicast addresses.

Options

| | |
|---|---|
| all | All multicast host. |
| group <MULTICAST_ADDR_GROUP_NAME> | Multicast address object group. Multicast address group name. Example: <i>Multicast Group</i> |
| host <MULTICAST_ADDR_HOST> | Multicast address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <MULTICAST_ADDR_NAME> | Multicast address object name. Multicast address object name. Example: <i>Multicast Address</i> |
| network <MULTICAST_ADDR_NETWORK> <MULTICAST_ADDR_MASK> | Multicast address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <MULTICAST_ADDR_BEGIN> <MULTICAST_ADDR_END> | Multicast address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
reception all
reception name "Multicast Address"
reception group "Multicast Group"
```



```
reception host 224.0.0.12
reception range 192.168.168.10 192.168.168.20
reception network 192.168.168.0 255.255.255.0
```

Syntax

```
clear multicast state-entries
```

Mode

Multicast

Description

Clear all the IGMP state entries.

Example

```
clear multicast state-entries
```

Syntax

```
clear multicast state-entry address <MULTICAST_GROUP_IPV4_HOST> interface <MULTICAST_INTERFACE>
```

Mode

Multicast

Description

Clear the specified IGMP state entry.

Options

| | |
|--|--|
| address | Specified multicast group address. |
| <MULTICAST_GROUP_IPV4_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| interface | Specified interface/ vpn tunnel. |
| <MULTICAST_INTERFACE> | Multicast interface name. Example: <i>X0</i> |

Example

```
clear multicast state-entry address 2.2.2.2 interface X1
```

Syntax

```
no access-rule from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> action { { allow | deny | discard } } [ source { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ port { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] } ] [ service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ destination { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] } ] [ schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } } ]
```

Mode

Config

Description

Delete firewall access rule policy.

Options

| | |
|--------------------------------------|--|
| <ACCESS_RULE_ZONE_NAME> | Zone object name. Example: <i>DMZ</i> |
| to | Destination zone. |

| | |
|---|---|
| <ACCESS_RULE_ZONE_NAME> | Zone object name. Example: <i>DMZ</i> |
| action | Set the action for this access rule. |
| allow | Allow traffic matching the criteria. |
| deny | Deny traffic matching the criteria. |
| discard | Discard traffic matching the criteria. |
| source | Source. |
| address | Source address. |
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_WITH_MIXED> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| port | Source port. |
| any | Any source service. |
| group | Source service Group name. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Source service Object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Source service Object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| service | Service. |
| any | Any destination service. |
| group | Service group name. |

| | |
|---|---|
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| destination | Destination. |
| address | Destination address. |
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_WITH_MIXED> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| schedule | Schedule. |
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

no access-rule from LAN to LAN action allow source address name "X0 IP" port any service name BGP destination address any schedule name "After hours"

Syntax

```
clear access-rule statistics
```

Mode

Config

Description

Clear firewall access rule statistics.

Syntax

```
access-rule from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> action { { allow | deny | discard } } [ source { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ port { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] } ] [ service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ destination { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] } ] [ schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } } ] [ primitive ]
```

Mode

Config

Description

Add/edit firewall access rule and enter configuration mode.

Options

| | |
|---|---|
| <ACCESS_RULE_ZONE_NAME> | Zone object name. Example: <i>DMZ</i> |
| to | Destination zone. |
| <ACCESS_RULE_ZONE_NAME> | Zone object name. Example: <i>DMZ</i> |
| action | Set the action for this access rule. |
| allow | Allow traffic matching the criteria. |
| deny | Deny traffic matching the criteria. |
| discard | Discard traffic matching the criteria. |
| source | Source. |
| address | Source address. |
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |

name Address object name.
<ADDR_NAME_WITH_MIXED> Address object name.
Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n.
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range Address object range.
<ADDR_BEGIN> IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

port Source port.

any Any source service.

group Source service Group name.
<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

name Source service Object name.
<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Source service Object protocol.
<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

service Service.

any Any destination service.

group Service group name.
<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

name Service object name.
<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Service object protocol.
<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

destination Destination.
address Destination address.

any Any address.

fqdn Address object full qualified domain name.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address group name.
<ADDR_GROUP_NAME_WITH_MIXED> Group address object name.
Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:0000:0000\n*

| | |
|-------------------------------------|--|
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_WITH_MIXED> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| schedule | Schedule. |
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |
| primitive | Configure a primitive access rule in one-line. |

Example

access-rule from LAN to LAN action allow source address name "X0 IP" port any service name BGP destination address any schedule name "After hours"

Syntax

access-rule uuid <UUID>

Mode

Config

Description

Edit firewall access rule by UUID and enter configuration mode.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

access-rule uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

```
no access-rule uuid <UUID>
```

Mode

Config

Description

Delete firewall access rule policy by UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
no access-rule uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
access-rule name <ACCESS_RULE_NAME>
```

Mode

Config

Description

Edit firewall access rule by name and enter configuration mode.

Options

<ACCESS_RULE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
access-rule name OfficePolicy
```

Syntax

```
no access-rule name <ACCESS_RULE_NAME>
```

Mode

Config

Description

Delete firewall access rule policy by name.

Options

<ACCESS_RULE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no access-rule name 25
```

Syntax

```
access-rule restore-defaults [ from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> ]
```

Mode

Config

Description

Restore firewall access rules to default settings.

Options

from From zone.

<ACCESS_RULE_ZONE_NAME> Zone object name.
Example: *DMZ*

to To zone.

<ACCESS_RULE_ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
access-rule restore-defaults from LAN to WAN
```

Syntax

```
no access-rule ipv6 from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> action { { allow | deny | discard } } [ source { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ port { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ destination { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] } ] [ schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } } ] }
```

Mode

Config

Description

Delete firewall access rule policy.

Options

<ACCESS_RULE_ZONE_NAME> Zone object name.
Example: *DMZ*

to Destination zone.

<ACCESS_RULE_ZONE_NAME> Zone object name.
Example: *DMZ*

action Set the action for this access rule.

allow Allow traffic matching the criteria.

deny Deny traffic matching the criteria.

discard Discard traffic matching the criteria.

source Source.

address Source address.

any Any address.

fqdn Address object full qualified domain name.

<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address group name.

<ADDR_GROUP_NAME_WITH_MIXED> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

mac Address object mac.

<ADDR_MAC> Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.

name Address object name.
<ADDR_NAME_WITH_MIXED> Address object name.
Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

port Source port.

any Any source service.

group Source service Group name.
<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

name Source service Object name.
<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Source service Object protocol.
<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

service Service.

any Any destination service.

group Service group name.
<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

name Service object name.
<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Service object protocol.
<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

destination Destination.
address Destination address.

any Any address.

fqdn Address object full qualified domain name.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address group name.
<ADDR_GROUP_NAME_WITH_MIXED> Group address object name.
Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

| | |
|-------------------------------------|---|
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_WITH_MIXED> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| schedule | Schedule. |
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
no access-rule ipv6 from LAN to LAN action allow source address name "X0 IP" port any service name BGP destination address any schedule name "After hours"
```

Syntax

```
access-rule ipv6 from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> action { { allow | deny | discard } } [ source { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ port { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] } ] [ service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ destination { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] } ] [ schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } } ] [ primitive ]
```

Mode

Config

Description

Add/Edit firewall access rule and enter configuration mode.

Options

| | |
|--------------------------------------|--|
| <ACCESS_RULE_ZONE_NAME> | Zone object name. Example: <i>DMZ</i> |
| to | Destination Zone. |
| <ACCESS_RULE_ZONE_NAME> | Zone object name. Example: <i>DMZ</i> |
| action | Set the action for this access rule. |

| | |
|---|---|
| allow | Allow traffic matching the criteria. |
| deny | Deny traffic matching the criteria. |
| discard | Discard traffic matching the criteria. |
| source | Source. |
| address | Source address. |
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_WITH_MIXED> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| port | Source port. |
| any | Any source service. |
| group | Source service Group name. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Source service Object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Source service Object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| service | Service. |
| any | Any destination service. |
| group | Service group name. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |

| | |
|---|--|
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| destination | Destination. |
| address | Destination address. |
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_WITH_MIXED> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| schedule | Schedule. |
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |
| primitive | Configure a primitive IPv6 access rule in one-line. |

Example

```
access-rule ipv6 from LAN to LAN action allow source address name "X0 IP" port any service name BGP destination address any
schedule name "After hours"
```

Syntax

```
no access-rule ipv6 uuid <UUID>
```

Mode

Config

Description

Delete firewall access rule policy by UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
no access-rule ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
access-rule ipv6 uuid <UUID>
```

Mode

Config

Description

Edit firewall access rule by UUID and enter configuration mode.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
access-rule ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
access-rule ipv6 name <ACCESS_RULE_NAME>
```

Mode

Config

Description

Edit firewall access rule by name and enter configuration mode.

Options

<ACCESS_RULE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
access-rule ipv6 name OfficePolicyV6
```

Syntax

```
no access-rule ipv6 name <ACCESS_RULE_NAME>
```

Mode

Config

Description

Delete firewall access rule policy by name.

Options

<ACCESS_RULE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no access-rule ipv6 name OfficePolicyV6
```

Syntax

```
access-rule ipv6 restore-defaults [ from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> ]
```

Mode

Config

Description

Restore firewall access rules to default settings.

Options

from From zone.
<ACCESS_RULE_ZONE_NAME> Zone object name.
Example: *DMZ*

to To zone.
<ACCESS_RULE_ZONE_NAME> Zone object name.
Example: *DMZ*

Syntax

```
uuid <UUID>
```

Mode

Access Rule
Access Rule IPv6

Description

Access rule UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

Access Rule
Access Rule IPv6

Description

Clear access rule UUID.

Example

```
no uuid
```

Syntax

```
name <WORD>
```

Mode

Access Rule
Access Rule IPv6

Description

Access rule name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name OfficePolicy
```

Syntax

```
no name
```

Mode

Access Rule
Access Rule IPv6

Description

Clear access rule name.

Example

```
no name
```

Syntax

```
from <ACCESS_RULE_ZONE_NAME>
```

Mode

Access Rule
Access Rule IPv6

Description

Specify a source zone for this access rule.

Options

<ACCESS_RULE_ZONE_NAME> Zone object name.
Example: *DMZ*

Example

from LAN

Syntax

to <ACCESS_RULE_ZONE_NAME>

Mode

Access Rule
Access Rule IPv6

Description

Specify a destination zone for this access rule.

Options

<ACCESS_RULE_ZONE_NAME> Zone object name.
Example: *DMZ*

Example

to LAN

Syntax

action { { allow | deny | discard } }

Mode

Access Rule
Access Rule IPv6

Description

Set the action for this access rule.

Options

allow Allow traffic matching the criteria.

deny Deny traffic matching the criteria.

discard Discard traffic matching the criteria.

Example

action allow

Syntax

max-connections <UINT8>

Mode

Access Rule
Access Rule IPv6

Description

Set the number of connections allowed (% maximum connections).

Options

<UINT8> Integer in the form: D OR 0xHH.

Example: 123

Example

```
max-connections 50
```

Syntax

```
priority { auto | end | manual <UINT32> }
```

Mode

Access Rule
Access Rule IPv6

Description

Set access rule priority.

Options

auto Set auto priority(priority = 0) for access rule.

end Insert the policy at the end.

manual Set manual priority for access rule.

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
priority auto  
priority manual 1
```

Syntax

```
tcp timeout <UINT32>
```

Mode

Access Rule
Access Rule IPv6

Description

Set the TCP connection inactivity timeout (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
tcp timeout 15
```

Syntax

```
udp timeout <UINT32>
```

Mode

Access Rule
Access Rule IPv6

Description

Set the UPD connection inactivity timeout (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
udp timeout 30
```

Syntax

```
fragments
```

Mode

Access Rule
Access Rule IPv6

Description

Allow fragmented packets on this access rule.

Example

```
fragments
```

Syntax

```
no fragments
```

Mode

Access Rule
Access Rule IPv6

Description

Disable fragmented packets on this access rule.

Example

```
no fragments
```

Syntax

```
botnet-filter
```

Mode

Access Rule

Description

Enable Botnet filter.

Example

```
botnet-filter
```

Syntax

```
no botnet-filter
```

Mode

Access Rule

Description

Disable Botnet filter.

Example

```
no botnet-filter
```

Syntax

```
comment <WORD>
```

Mode

Access Rule
Access Rule IPv6

Description

Specify a comment for this access rule.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Access Rule to allow IT to access servers"
```

Syntax

```
no comment
```

Mode

Access Rule
Access Rule IPv6

Description

Clear a comment for this access rule.

Example

```
no comment
```

Syntax

```
connection-limit destination [ threshold <UINT16> ]
```

Mode

Access Rule
Access Rule IPv6

Description

Enable connection limit for each destination IP address.

Options

threshold Set the destination IP address connection limit threshold.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

connection-limit destination threshold 128

Syntax

no connection-limit destination

Mode

Access Rule
Access Rule IPv6

Description

Disable connection limit for each destination IP address.

Example

no connection-limit destination

Syntax

connection-limit source [threshold <UINT16>]

Mode

Access Rule
Access Rule IPv6

Description

Enable connection limit for each source IP address.

Options

threshold Set the source IP address connection limit threshold.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

connection-limit source threshold 128

Syntax

no connection-limit source

Mode

Access Rule
Access Rule IPv6

Description

Disable connection limit for each source IP address.

Example

no connection-limit source

Syntax

tcp urgent

Mode

Access Rule
Access Rule IPv6

Description

Enable allow TCP urgent packets.

Example

```
tcp-urgent
```

Syntax

```
no tcp urgent
```

Mode

Access Rule
Access Rule IPv6

Description

Disable allow TCP urgent packets.

Example

```
no tcp urgent
```

Syntax

```
dpi
```

Mode

Access Rule
Access Rule IPv6

Description

Enable DPI.

Example

```
dpi
```

Syntax

```
no dpi
```

Mode

Access Rule
Access Rule IPv6

Description

Disable DPI.

Example

```
no dpi
```

Syntax

```
dpi-ssl { client | server }
```

Mode

Access Rule
Access Rule IPv6

Description

Enable DPI-SSL client or server.

Options

client Enable DPI-SSL client.

server Enable DPI-SSL server.

Example

```
dpi-ssl client
dpi-ssl server
```

Syntax

```
no dpi-ssl { client | server }
```

Mode

Access Rule
Access Rule IPv6

Description

Disable DPI-SSL client or server.

Options

client Disable DPI-SSL client.

server Disable DPI-SSL server.

Example

```
no dpi-ssl client
no dpi-ssl server
```

Syntax

```
destination address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name  
<ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

Access Rule
Access Rule IPv6

Description

Specify a destination for this access rule.

Options

any Any address.

fqdn Address object full qualified domain name.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address group name.
<ADDR_GROUP_NAME_WITH_MIXED> Group address object name.
Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
 Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

mac Address object mac.
<ADDR_MAC> Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.

name Address object name.
<ADDR_NAME_WITH_MIXED> Address object name.
 Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
 Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n
 Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range Address object range.
<ADDR_BEGIN> IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
 Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
 Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

destination address name "Corporate Servers"

Syntax

service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }

Mode

Access Rule
 Access Rule IPv6

Description

Specify a service for this Access Policy.

Options

any Any destination service.

group Service group name.
<SVC_GROUP_NAME> Service object group name.
 Example: *VOIP*

name Service object name.
<SVC_NAME> Service object name.
 Example: *HTTPS*

protocol Service object protocol.
<SVC_PROTOCOL> Service protocol.
 Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
 Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
 Example: *80*

Example

service "Corporate Servers"

Syntax

enable

Mode

Access Rule
Access Rule IPv6

Description

Enable this access rule.

Example

enable

Syntax

no enable

Mode

Access Rule
Access Rule IPv6

Description

Disable this access rule.

Example

no enable

Syntax

flow-reporting

Mode

Access Rule
Access Rule IPv6

Description

Enable flow reporting.

Example

flow-reporting

Syntax

no flow-reporting

Mode

Access Rule
Access Rule IPv6

Description

Disable flow reporting.

Example

no flow-reporting

Syntax

geo-ip-filter

Mode

Access Rule
Access Rule IPv6

Description

Enable Geo-IP filter.

Example

geo-ip-filter

Syntax

no geo-ip-filter

Mode

Access Rule
Access Rule IPv6

Description

Disable Geo-IP filter.

Example

no geo-ip-filter

Syntax

logging

Mode

Access Rule
Access Rule IPv6

Description

Enable logging when this access rule is used.

Example

logging

Syntax

no logging

Mode

Access Rule
Access Rule IPv6

Description

Disable logging when this access rule is used.

Example

no logging

Syntax

sip

Mode

Access Rule
Access Rule IPv6

Description

Enable SIP transformation.

Example

sip

Syntax

no sip

Mode

Access Rule
Access Rule IPv6

Description

Disable SIP transformation.

Example

no sip

Syntax

h323

Mode

Access Rule
Access Rule IPv6

Description

Enable H.323 transformation.

Example

h323

Syntax

no h323

Mode

Access Rule
Access Rule IPv6

Description

Disable H.323 transformation.

Example

no h323

Syntax

packet-monitoring

Mode

Access Rule
Access Rule IPv6

Description

Enable packet monitoring.

Example

packet-monitoring

Syntax

no packet-monitoring

Mode

Access Rule
Access Rule IPv6

Description

Disable packet monitoring.

Example

no packet-monitoring

Syntax

management

Mode

Access Rule
Access Rule IPv6

Description

Allow management traffic.

Example

management

Syntax

no management

Mode

Access Rule
Access Rule IPv6

Description

Disable management traffic.

Example

no management

Syntax

```
single-sign-on
```

Mode

Access Rule
Access Rule IPv6

Description

Invoke single sign on to authenticate users.

Example

```
single-sign-on
```

Syntax

```
no single-sign-on
```

Mode

Access Rule
Access Rule IPv6

Description

Don't invoke single sign on to authenticate users.

Example

```
no single-sign-on
```

Syntax

```
quality-of-service class-of-service { explicit { { background | best-effort | controlled-load | excellent-effort | network-control  
| spare | video | voice } } | map | preserve }
```

Mode

Access Rule
Access Rule IPv6

Description

Set 802.1p marking action.

Options

| | |
|-------------------------|-------------------------|
| explicit | Set explicit marking. |
| background | Background. |
| best-effort | Best effort. |
| controlled-load | Controlled load. |
| excellent-effort | Excellent effort. |
| network-control | Network control. |
| spare | Spare. |
| video | Video (<100ms latency). |
| voice | Voice (<10ms latency). |
| map | Map marking. |

preserve Preserve marking.

Example

```
quality-of-service class-of-service preserve
```

Syntax

```
cos-override
```

Mode

Access Rule
Access Rule IPv6

Description

Allow 802.1p marking to override DSCP values.

Example

```
cos-override
```

Syntax

```
no cos-override
```

Mode

Access Rule
Access Rule IPv6

Description

Disable allowing 802.1p marking to override DSCP values.

Example

```
no cos-override
```

Syntax

```
no quality-of-service { class-of-service | dscp }
```

Mode

Access Rule
Access Rule IPv6

Description

Clear DSCP and 802.1p marking settings.

Options

class-of-service No 802.1p tagging.

dscp Clear DSCP values.

Example

```
no quality-of-service dscp
```

Syntax

```
quality-of-service dscp { explicit <UINT8> | map | preserve }
```

Mode

Access Rule
Access Rule IPv6

Description

Set DSCP marking action.

Options

- explicit** Set explicit marking.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123
- map** Map marking.
- preserve** Preserve marking.

Example

```
quality-of-service dscp preserve
```

Syntax

```
reflexive
```

Mode

Access Rule
Access Rule IPv6

Description

Configure a reflexive rule.

Example

```
reflexive
```

Syntax

```
no reflexive
```

Mode

Access Rule
Access Rule IPv6

Description

Disable configuration of a reflexive rule.

Example

```
no reflexive
```

Syntax

```
schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } }
```

Mode

Description

Specify a schedule for this access rule.

Options

| | |
|---------------------------------|---|
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule name "IT Maintenance"
```

Syntax

```
source address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

Description

Specify a service for this access rule.

Options

| | |
|---|--|
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_WITH_MIXED> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
source address name "Corporate IT Administration"
```

Syntax

```
source port { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }
```

Mode

Access Rule
Access Rule IPv6

Description

Specify a source port for this access rule.

Options

any Any source service.

group Source service group name.
<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

name Source service object name.
<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Source service object protocol.
<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
source port name "Corporate IT Administration"
```

Syntax

```
users included { { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> } }
```

Mode

Access Rule
Access Rule IPv6

Description

Specify users that apply to this access rule.

Options

administrator Administrator.

| | |
|--------------------------------------|---|
| all | All users. |
| group | Group object name. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guest users. |
| name | User object name. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

users included name "Corporate IT Administrators"

Syntax

users excluded { { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> | none } }

Mode

Access Rule
Access Rule IPv6

Description

Specify users that are excluded from this access rule.

Options

| | |
|--------------------------------------|---|
| administrator | Administrator. |
| group | Group object name. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guest users. |
| name | User object name. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |
| none | No users. |

Example

users excluded name "Corporate Users"

Syntax

bandwidth-management

Mode

Access Rule

Description

Enter ethernet bandwidth management configuration mode.

Example

bandwidth-management

Syntax

bandwidth-management

Mode

Access Rule IPv6

Description

Enter bandwidth management configuration mode.

Example

bandwidth-management

Syntax

```
egress { bandwidth-object <BANDWIDTH_RULE_NAME> | priority { high | highest | low | lowest | medium | medium-high | medium-low | realtime } }
```

Mode

Bandwidth Management
Bandwidth Management IPv6

Description

Enable egress bandwidth management and configure.

Options

| | |
|---|--|
| <i>bandwidth-object</i> | Bandwidth object name. |
| <i><BANDWIDTH_RULE_NAME></i> | Bandwidth object name. Example: <code>\ "Corp High Priority" \</code> |
| <i>priority</i> | Egress traffic priority. |
| <i>high</i> | High 2. |
| <i>highest</i> | Highest 1. |
| <i>low</i> | Low 6. |
| <i>lowest</i> | Lowest 7. |
| <i>medium</i> | Medium 4. |
| <i>medium-high</i> | Medium-high 3. |
| <i>medium-low</i> | Medium-low 5. |
| <i>realtime</i> | Realtime 0. |

Example

```
egress bandwidth-object "Corp High Priority"
```

Syntax

no egress

Mode

Bandwidth Management
Bandwidth Management IPv6

Description

Disable egress bandwidth management.

Example

```
no egress
```

Syntax

```
ingress { bandwidth-object <BANDWIDTH_RULE_NAME> | priority { high | highest | low | lowest | medium | medium-high | medium-low | realtime } }
```

Mode

Bandwidth Management
Bandwidth Management IPv6

Description

Enable ingress bandwidth management and configure.

Options

| | |
|---|--|
| <i>bandwidth-object</i> | Bandwidth object name. |
| <i><BANDWIDTH_RULE_NAME></i> | Bandwidth object name. Example: <code>"Corp High Priority"</code> |
| <i>priority</i> | Ingress traffic priority. |
| <i>high</i> | High 2. |
| <i>highest</i> | Highest 1. |
| <i>low</i> | Low 6. |
| <i>lowest</i> | Lowest 7. |
| <i>medium</i> | Medium 4. |
| <i>medium-high</i> | Medium-high 3. |
| <i>medium-low</i> | Medium-low 5. |
| <i>realtime</i> | Realtime 0. |

Example

```
ingress bandwidth-object "Corp High Priority"
```

Syntax

```
no ingress
```

Mode

Bandwidth Management
Bandwidth Management IPv6

Description

Disable ingress bandwidth management.

Example

```
no ingress
```

Syntax

usage-tracking

Mode

Bandwidth Management
Bandwidth Management IPv6

Description

Enable tracking bandwidth usage.

Example

usage-tracking

Syntax

no usage-tracking

Mode

Bandwidth Management
Bandwidth Management IPv6

Description

Disable tracking bandwidth usage.

Example

no usage-tracking

Syntax

ssl-control

Mode

Config

Description

Enter SSL control mode and configure settings.

Example

ssl-control

Syntax

enable

Mode

SSL Control

Description

Enable SSL control.

Example

enable

Syntax

no enable

Mode

SSL Control

Description

Disable SSL control.

Example

no enable

Syntax

action { block | log }

Mode

SSL Control

Description

Action if an SSL policy violation is detected.

Options

block Block the connection and log the event.

log Log the event.

Example

action block

Syntax

blacklist

Mode

SSL Control

Description

Enable blacklist.

Example

blacklist

Syntax

no blacklist

Mode

SSL Control

Description

Disable blacklist.

Example

no blacklist

Syntax

detect ssl-v2

Mode

SSL Control

Description

Enable detection of SSLv2.

Example

detect ssl-v2

Syntax

no detect ssl-v2

Mode

SSL Control

Description

Disable detection of SSLv2.

Example

no detect ssl-v2

Syntax

detect ssl-v3

Mode

SSL Control

Description

Enable detection of SSLv3.

Example

detect ssl-v3

Syntax

no detect ssl-v3

Mode

SSL Control

Description

Disable detection of SSLv3.

Example

no detect ssl-v3

Syntax

detect weak-ciphers

Mode

SSL Control

Description

Enable detection of weak ciphers.

Example

detect weak-ciphers

Syntax

no detect weak-ciphers

Mode

SSL Control

Description

Disable detection of weak ciphers.

Example

no detect weak-ciphers

Syntax

whitelist

Mode

SSL Control

Description

Enable whitelist.

Example

whitelist

Syntax

no whitelist

Mode

SSL Control

Description

Disable whitelist.

Example

no whitelist

Syntax

detect self-signed

Mode

SSL Control

Description

Enable detection of self-signed certificates.

Example

detect self-signed

Syntax

no detect self-signed

Mode

SSL Control

Description

Disable detection of self-signed certificates.

Example

no detect self-signed

Syntax

detect weak-digest-cert

Mode

SSL Control

Description

Enable detection of weak digest certificates.

Example

detect weak-digest-cert

Syntax

no detect weak-digest-cert

Mode

SSL Control

Description

Disable detection of weak digest certificates.

Example

no detect weak-digest-cert

Syntax

detect expired

Mode

SSL Control

Description

Enable detection of expired certificates.

Example

detect expired

Syntax

no detect expired

Mode

SSL Control

Description

Disable detection of expired certificates.

Example

no detect expired

Syntax

detect untrusted-ca

Mode

SSL Control

Description

Enable detection of certificate signed by an untrusted CA.

Example

detect untrusted-ca

Syntax

no detect untrusted-ca

Mode

SSL Control

Description

Disable detection of certificate signed by an untrusted CA.

Example

no detect untrusted-ca

Syntax

detect tls-v1

Mode

SSL Control

Description

Enable detection of TLSv1.

Example

```
detect tls-v1
```

Syntax

```
no detect tls-v1
```

Mode

SSL Control

Description

Disable detection of TLSv1.

Example

```
no detect tls-v1
```

Syntax

```
blacklist-certificate <BLACKLIST_CERTIFICATE>
```

Mode

SSL Control

Description

Add entry to blacklist.

Options

<BLACKLIST_CERTIFICATE> Word in the form: WORD or \"QUOTED STRING\".
Example: *certificateName*

Example

```
blacklist-certificate www.badguys.com
```

Syntax

```
no blacklist-certificate <BLACKLIST_CERTIFICATE>
```

Mode

SSL Control

Description

Delete an entry from blacklist.

Options

<BLACKLIST_CERTIFICATE> Word in the form: WORD or \"QUOTED STRING\".
Example: *certificateName*

Example

```
no blacklist-certificate www.badguys.com
```

Syntax

no blacklist-certificates

Mode

SSL Control

Description

Delete all entries from blacklist.

Example

no blacklist-certificates

Syntax

whitelist-certificate <WHITELIST_CERTIFICATE>

Mode

SSL Control

Description

Add entry to whitelist.

Options

<WHITELIST_CERTIFICATE> Word in the form: WORD or \"QUOTED STRING\".
Example: *certificateName*

Example

whitelist-certificate www.badguys.com

Syntax

no whitelist-certificate <WHITELIST_CERTIFICATE>

Mode

SSL Control

Description

Delete an entry from whitelist.

Options

<WHITELIST_CERTIFICATE> Word in the form: WORD or \"QUOTED STRING\".
Example: *certificateName*

Example

no whitelist-certificate www.goodguys.com

Syntax

no whitelist-certificates

Mode

SSL Control

Description

Delete all entries from whitelist.

Example

```
no whitelist-certificates
```

Syntax

```
tcp
```

Mode

Config

Description

Configure TCP settings.

Example

```
tcp
```

Syntax

```
enforce-strict-compliance
```

Mode

TCP

Description

Enable enforcement of strict TCP compliance with RFC 793 and RFC 1122.

Example

```
enforce-strict-compliance
```

Syntax

```
no enforce-strict-compliance
```

Mode

TCP

Description

Disable enforcement of strict TCP compliance with RFC 793 and RFC 1122.

Example

```
no enforce-strict-compliance
```

Syntax

```
handshake-enforcement
```

Mode

TCP

Description

Enable TCP handshake enforcement.

Example

handshake-enforcement

Syntax

no handshake-enforcement

Mode

TCP

Description

Disable TCP handshake enforcement.

Example

no handshake-enforcement

Syntax

checksum-enforcement

Mode

TCP

Description

Enable TCP checksum enforcement.

Example

checksum-enforcement

Syntax

no checksum-enforcement

Mode

TCP

Description

Disable TCP checksum enforcement.

Example

no checksum-enforcement

Syntax

drop syn-with-data

Mode

TCP

Description

Enable drop TCP SYN with data packets.

Example

```
drop syn-with-data
```

Syntax

```
no drop syn-with-data
```

Mode

TCP

Description

Disable drop TCP SYN with data packets.

Example

```
no drop syn-with-data
```

Syntax

```
handshake-timeout <UINT32>
```

Mode

TCP

Description

Set the TCP handshake timeout in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
handshake-timeout 4
```

Syntax

```
no handshake-timeout
```

Mode

TCP

Description

Disable the TCP handshake timeout.

Example

```
no handshake-timeout
```

Syntax

```
default-connection-timeout <UINT32>
```

Mode

TCP

Description

Set default TCP connection timeout in minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
default-connection-timeout 15
```

Syntax

```
maximum-segment-lifetime <UINT8>
```

Mode

TCP

Description

Set maximum segment lifetime in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
maximum-segment-lifetime 8
```

Syntax

```
syn-flood-protection-mode { always-proxy | proxy-suspect-attack | watch-and-report }
```

Mode

TCP

Description

Set TCP SYN flood protection mode.

Options

always-proxy Always proxy WAN client connections.

proxy-suspect-attack Proxy WAN client connections when attack is suspected.

watch-and-report Watch and report possible SYN floods.

Example

```
syn-flood-protection-mode watch-and-report
```

Syntax

```
syn-attack-threshold <UINT32>
```

Mode

TCP

Description

Set attack threshold (incomplete connection attempts / second).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
syn-attack-threshold 300
```

Syntax

```
support-tcp-sack
```

Mode

TCP

Description

Enable all LAN/DMZ servers support the TCP SACK option.

Example

```
support-tcp-sack
```

Syntax

```
no support-tcp-sack
```

Mode

TCP

Description

Disable all LAN/DMZ servers support the TCP SACK option.

Example

```
no support-tcp-sack
```

Syntax

```
limit-mss [ max <UINT16> ]
```

Mode

TCP

Description

Enable limit MSS sent to WAN clients (when connections are proxied).

Options

max Set maximum TCP MSS sent to WAN clients.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
limit-mss max 1460
```

Syntax


```
no limit-mss
```

Mode

TCP

Description

Disable limit MSS sent to WAN clients (when connections are proxied).

Example

```
no limit-mss
```

Syntax

```
always-log-syn-packets
```

Mode

TCP

Description

Enable always log SYN packets received.

Example

```
always-log-syn-packets
```

Syntax

```
no always-log-syn-packets
```

Mode

TCP

Description

Disable always log SYN packets received.

Example

```
no always-log-syn-packets
```

Syntax

```
proxy-connections [ service { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN>  
<SVC_PORT_END> } ]
```

Mode

TCP

Description

Enable proxy connections for specific service only and select the specific service.

Options

| | |
|-------------------------------|--|
| service | Set the specific service. |
| any | Any service. |
| group | Service group name. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |

| | |
|-------------------------------|---|
| <i>name</i> | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| <i>protocol</i> | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
proxy-connections
proxy-connections service any
proxy-connections service name HTTP
```

Syntax

```
no proxy-connections
```

Mode

TCP

Description

Disable proxy connections for specific service only.

Example

```
no proxy-connections
```

Syntax

```
syn-flood-blacklisting
```

Mode

TCP

Description

Enable SYN/RST/FIN flood blacklisting on all interfaces.

Example

```
syn-flood-blacklisting
```

Syntax

```
no syn-flood-blacklisting
```

Mode

TCP

Description

Disable SYN/RST/FIN flood blacklisting on all interfaces.

Example

```
no syn-flood-blacklisting
```

Syntax

blacklist-threshold <UINT32>

Mode

TCP

Description

Set threshold for SYN/RST/FIN flood blacklisting (packets / sec).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

blacklist-threshold 1000

Syntax

never-blacklist-wan

Mode

TCP

Description

Enable never blacklist WAN machines.

Example

never-blacklist-wan

Syntax

no never-blacklist-wan

Mode

TCP

Description

Disable never blacklist WAN machines.

Example

no never-blacklist-wan

Syntax

always-allow-management

Mode

TCP

Description

Enable always allow SonicWall management traffic.

Example

always-allow-management

Syntax

no always-allow-management

Mode

TCP

Description

Disable always allow SonicWall management traffic.

Example

no always-allow-management

Syntax

ddos on-wan-interfaces

Mode

TCP

Description

Enable DDOS protection on WAN interfaces.

Example

ddos on-wan-interfaces

Syntax

no ddos on-wan-interfaces

Mode

TCP

Description

Disable DDOS protection on WAN interfaces.

Example

no ddos on-wan-interfaces

Syntax

ddos threshold <UINT32>

Mode

TCP

Description

Set threshold for WAN DDOS protection (non-TCP packets / sec).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
ddos threshold 1000
```

Syntax

```
no ddos threshold
```

Mode

TCP

Description

Clear threshold for WAN DDOS protection.

Example

```
no ddos threshold
```

Syntax

```
ddos fliter-bypass-rate <UINT32>
```

Mode

TCP

Description

Set WAN DDOS filter bypass rate (every n packets).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
ddos fliter-bypass-rate 100
```

Syntax

```
no ddos fliter-bypass-rate
```

Mode

TCP

Description

Clear WAN DDOS filter bypass rate.

Example

```
no ddos fliter-bypass-rate
```

Syntax

```
ddos allow-list-timeout <UINT32>
```

Mode

TCP

Description

Set WAN DDOS allow list timeout.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
ddos allow-list-timeout 100
```

Syntax

```
no ddos allow-list-timeout
```

Mode

TCP

Description

Clear WAN DDOS allow list timeout.

Example

```
no ddos allow-list-timeout
```

Syntax

```
ddos always-allow-management
```

Mode

TCP

Description

Enable always allow SonicWall management traffic (non-tcp floods).

Example

```
ddos always-allow-management
```

Syntax

```
no ddos always-allow-management
```

Mode

TCP

Description

Disable always allow SonicWall management traffic (non-tcp floods).

Example

```
no ddos always-allow-management
```

Syntax

```
ddos always-allow-negotiation
```

Mode

TCP

Description

Enable always allow VPN negotiation traffic (non-tcp floods).

Example

```
ddos always-allow-negotiation
```

Syntax

```
no ddos always-allow-negotiation
```

Mode

TCP

Description

Disable always allow VPN negotiation traffic (non-tcp floods).

Example

```
no ddos always-allow-negotiation
```

Syntax

```
clear tcp statistics
```

Mode

TCP

Description

Clear TCP traffic statistics.

Example

```
clear tcp statistics
```

Syntax

```
no bandwidth-object <BANDWIDTH_RULE_NAME>
```

Mode

Config

Description

Delete a bandwidth object.

Options

<BANDWIDTH_RULE_NAME> Bandwidth object name.
Example: `\\"Corp High Priority\"`

Example

```
no bandwidth-object "Corp High Priority"
```

Syntax

```
no bandwidth-objects
```

Mode

Config

Description

Delete all custom bandwidth objects.

Example

```
no bandwidth-objects
```

Syntax

```
bandwidth-object <BANDWIDTH_OBJ_NAME>
```

Mode

Config

Description

Add/edit a bandwidth object and enter its configuration mode.

Options

<BANDWIDTH_OBJ_NAME> Bandwidth object name.
Example: `"Corp High Priority"`

Example

```
bandwidth-object "Corp High Priority"
```

Syntax

```
name <BANDWIDTH_OBJ_NAME>
```

Mode

Bandwidth Object

Description

Set bandwidth object name.

Options

<BANDWIDTH_OBJ_NAME> Bandwidth object name.
Example: `"Corp High Priority"`

Example

```
name "Corp High Priority"
```

Syntax

```
guaranteed { kbps <UINT32> | mbps <UINT32> }
```

Mode

Bandwidth Object

Description

Set bandwidth object guaranteed bandwidth.

Options

kbps Kilobits per second.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: `123`

mbps Megabits per second.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
guaranteed mbps 50
```

Syntax

```
maximum { kbps <UINT32> | mbps <UINT32> }
```

Mode

Bandwidth Object

Description

Set bandwidth object maximum bandwidth.

Options

kbps Kilobits per second.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

mbps Megabits per second.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
maximum mbps 100
```

Syntax

```
priority { high | highest | low | lowest | medium | medium-high | medium-low | realtime }
```

Mode

Bandwidth Object

Description

Set the bandwidth object traffic priority.

Options

high High 2.
highest Highest 1.
low Low 6.
lowest Lowest 7.
medium Medium 4.
medium-high Medium-high 3.
medium-low Medium-low 5.
realtime Realtime 0.

Example

priority medium-high

Syntax

action { delay | drop }

Mode

Bandwidth Object

Description

Set the bandwidth object violation action.

Options

delay Delay.

drop Drop.

Example

action delay

Syntax

comment <WORD>

Mode

Bandwidth Object

Description

Set comment for the bandwidth object.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Use to insure maximum bandwidth for high priority traffic"

Syntax

no comment

Mode

Bandwidth Object

Description

Clear a comment for the bandwidth object.

Example

no comment

Syntax

per-ip-management { kbps <UINT32> | mbps <UINT32> }

Mode

Bandwidth Object

Description

Enable per IP bandwidth management and set the maximum bandwidth.

Options

kbps Kilobits per second.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

mbps Megabits per second.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
per-ip-management kbps 800
```

Syntax

```
no per-ip-management
```

Mode

Bandwidth Object

Description

Disable per IP bandwidth management.

Example

```
no per-ip-management
```

Syntax

```
udp
```

Mode

Config

Description

Configure UDP settings.

Example

```
udp
```

Syntax

```
default-connection-timeout <UINT32>
```

Mode

UDP

Description

Set default UDP connection timeout in minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
default-connection-timeout 15
```

Syntax

```
flood protection
```

Mode

UDP

Description

Enable UDP flood protection.

Example

```
flood protection
```

Syntax

```
no flood protection
```

Mode

UDP

Description

Disable UDP flood protection.

Example

```
no flood protection
```

Syntax

```
flood attack-threshold <UINT32>
```

Mode

UDP

Description

Set UDP flood attack threshold (UDP packets / sec).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
flood attack-threshold 1000
```

Syntax

```
flood block-timeout <UINT8>
```

Mode

UDP

Description

Set UDP flood attack blocking time (sec).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
flood block-timeout 2
```

Syntax

```
flood protected-dest-list { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

UDP

Description

Set UDP flood attack protected destination list.

Options

| | |
|---|--|
| any | Set UDP flood attack protected destination list to any. |
| group <ADDR_GROUP_NAME> | Set UDP flood attack protected destination list to named address group. Group address object name. Example: <i>Sales Group</i> |
| host <ADDR_HOST> | Set UDP flood attack protected destination list as host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <ADDR_HOST_NETWORK_RANGE_NAME> | Set UDP flood attack protected destination list to named address object. Host/network/range address object name. Example: <i>Web Server</i> |
| network <ADDR_NETWORK> <ADDR_MASK> | Set UDP flood attack protected destination list to network address. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> <ADDR_END> | Set UDP flood attack protected destination list to range of addresses. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
flood protected-dest-list any
```

Syntax

```
clear udp statistics
```

Mode

UDP

Description

Clear UDP traffic statistics.

Example

```
clear udp statistics
```

Syntax

```
icmp
```

Mode

Config

Description

Configure ICMP settings.

Example

```
icmp
```

Syntax

```
flood protection
```

Mode

ICMP

Description

Enable ICMP flood protection.

Example

```
flood protection
```

Syntax

```
no flood protection
```

Mode

ICMP

Description

Disable ICMP flood protection.

Example

```
no flood protection
```

Syntax

```
flood attack-threshold <UINT32>
```

Mode

ICMP

Description

Set ICMP flood attack threshold (ICMP packets / sec).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
flood attack-threshold 1000
```

Syntax

```
flood block-timeout <UINT8>
```

Mode

ICMP

Description

Set ICMP flood attack blocking time (sec).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
flood block-timeout 2
```

Syntax

```
flood protected-dest-list { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

ICMP

Description

Set ICMP flood attack protected destination list.

Options

any Set ICMP flood attack protected destination list to any.

group Set ICMP flood attack protected destination list to named address group.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Set ICMP flood attack protected destination list as host address.
<ADDR_HOST> IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Set ICMP flood attack protected destination list to named address object.
<ADDR_HOST_NETWORK_RANGE_NAME> Host/network/range address object name.
Example: *Web Server*

network Set ICMP flood attack protected destination list to network address.
<ADDR_NETWORK> IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*
<ADDR_MASK> IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n.
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range Set ICMP flood attack protected destination list to range of addresses.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*
<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
flood-protected-dest-list any
```

Syntax

```
clear icmp statistics
```

Mode

ICMP

Description

Clear ICMP traffic statistics.

Example

```
clear icmp statistics
```

Syntax

```
qos-mapping cos <UINT8> [ to-dscp <UINT8> ] [ from-dscp <UINT8> <UINT8> ]
```

Mode

Config

Description

Configure QoS mapping.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

to-dscp Set the DSCP value to map to.

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

from-dscp Set the from DSCP range.

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
qos-mapping cos 0 to-dscp 1 from-dscp 1 6
```

Syntax

```
qos-mapping reset
```

Mode

Config

Description

Reset QoS mapping settings.

Example

```
qos-mapping reset
```

Syntax

```
show firewall [ connection-status ]
```

Mode

All Modes

Description

Show firewall settings.

Options

connection-status Show firewall connections status.

Example

```
show firewall
```

Syntax

```
show bandwidth-management [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show bandwidth management settings.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show bandwidth-management
```

Syntax

```
show multicast [ { pending-config | with-pending-config } | state { entries | entry address <MULTICAST_GROUP_IPV4_HOST> interface <MULTICAST_INTERFACE> } ]
```

Mode

All Modes

Description

Show multicast configuration.

Options

pending-config Show pending configuration changes.

| | |
|--|--|
| with-pending-config | View current configuration with pending changes included in the output. |
| state | Show multicast state. |
| entries | Show multicast state entries. |
| entry | Show a specified multicast state entry. |
| address | Multicast group address. |
| <MULTICAST_GROUP_IPV4_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| interface | Interface or vpn tunnel. |
| <MULTICAST_INTERFACE> | Multicast interface name. Example: <i>X0</i> |

Example

```
show multicast
show multicast state entries
show multicast state entry address 192.168.168.10 interface X0
```

Syntax

```
show access-rule ipv4 from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> action { { allow | deny | discard } } [ source { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ port { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] } ] [ service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ destination { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] } ] [ schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } } ] [ statistics ] [ connection-limit top <UINT8> ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show an access rule.

Options

| | |
|---|--|
| <ACCESS_RULE_ZONE_NAME> | Zone object name. Example: <i>DMZ</i> |
| to | Destination zone. |
| <ACCESS_RULE_ZONE_NAME> | Zone object name. Example: <i>DMZ</i> |
| action | Set the action for this access rule. |
| allow | Allow traffic matching the criteria. |
| deny | Deny traffic matching the criteria. |
| discard | Discard traffic matching the criteria. |
| source | Source. |
| address | Source address. |
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |

mac Address object mac.
<ADDR_MAC> Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.

name Address object name.
<ADDR_NAME_WITH_MIXED> Address object name.
 Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
 Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

port Source port.

any Any source service.

group Source service Group name.
<SVC_GROUP_NAME> Service object group name.
 Example: *VOIP*

name Source service Object name.
<SVC_NAME> Service object name.
 Example: *HTTPS*

protocol Source service Object protocol.
<SVC_PROTOCOL> Service protocol.
 Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
 Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
 Example: *80*

service Destination service.

any Any destination service.

group Service group name.
<SVC_GROUP_NAME> Service object group name.
 Example: *VOIP*

name Service object name.
<SVC_NAME> Service object name.
 Example: *HTTPS*

protocol Service object protocol.
<SVC_PROTOCOL> Service protocol.
 Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
 Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
 Example: *80*

destination Destination.
address Destination address.

any Any address.

fqdn Address object full qualified domain name.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
 Example: *example.com*

group Address group name.
<ADDR_GROUP_NAME_WITH_MIXED> Group address object name.
 Example: *Sales Group*

| | |
|-------------------------------------|--|
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_WITH_MIXED> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| schedule | Schedule. |
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |
| statistics | Show statistics for specified access rule. |
| connection-limit | Show connection statistics of the access rule which has enabled source or destination IP address connection limit. |
| top | Show access rule top connection statistics. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show access-rule ipv4 from LAN to WLAN action allow
```

Syntax

```
show access-rule ipv4 uuid <UUID> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show an IPv4 access rule for associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: `138a224d-c4c7-d621-0a00-c0eae49ce84c`

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show access-rule ipv4 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
show access-rule ipv4 name <ACCESS_RULE_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show an IPv4 access rule for associated name.

Options

<ACCESS_RULE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: `abc`

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show access-rule ipv4 name "OfficePolicy"
```

Syntax

```
show access-rules [ ipv4 | ipv6 ] [ connection-limit | from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> | unused ] [ statistics ] [ { custom | default } ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all access rules.

Options

ipv4 Show IPv4 access rules.

ipv6 Show IPv6 access rules.

connection-limit Show access rules that enabled and on which source or destination IP address connection limit is enabled.

from Source zone.
<ACCESS_RULE_ZONE_NAME> Zone object name.
Example: `DMZ`

to Destination zone.
<ACCESS_RULE_ZONE_NAME> Zone object name.
Example: `DMZ`

unused Show access rules assigned to a Zone that has not been assigned to an interface.

statistics Show statistics for all access rules.

| | |
|----------------------------|---|
| custom | Show custom configuration. |
| default | Show system/factory default configuration. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show access-rules
show access-rules from * to WAN
show access-rules from DMZ to WAN
```

Syntax

```
show access-rule ipv6 from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> action { { allow | deny | discard } } [ source { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ port { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] } ] [ service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ destination { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] } ] [ schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } } ] [ connection-limit top <UINT8> ] [ { pending-config | with-pending-config } ] }
```

Mode

All Modes

Description

Show an access rule.

Options

| | |
|---|---|
| <ACCESS_RULE_ZONE_NAME> | Zone object name. Example: <i>DMZ</i> |
| to | Destination Zone. |
| <ACCESS_RULE_ZONE_NAME> | Zone object name. Example: <i>DMZ</i> |
| action | Set the action for this access rule. |
| allow | Allow traffic matching the criteria. |
| deny | Deny traffic matching the criteria. |
| discard | Discard traffic matching the criteria. |
| source | Source. |
| address | Source address. |
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_WITH_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |

<ADDR_NAME_WITH_MIXED> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

port Source port.

any Any source service.

group Source service Group name.

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

name Source service Object name.

<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Source service Object protocol.

<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

service Destination service.

any Any destination service.

group Service group name.

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

name Service object name.

<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Service object protocol.

<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

destination Destination.

address Destination address.

any Any address.

fqdn Address object full qualified domain name.

<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address group name.

<ADDR_GROUP_NAME_WITH_MIXED> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

| | |
|-------------------------------------|--|
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_WITH_MIXED> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| schedule | Schedule. |
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |
| connection-limit | Show connection statistics of the access rule which has enabled source or destination IP address connection limit. |
| top | Show access rule top connection statistics. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show access-rule ipv6 from LAN to WLAN action allow
```

Syntax

```
show access-rule ipv6 uuid <UUID> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show an IPv6 access rule for associated UUID.

Options

| | |
|-----------------------|---|
| <UUID> | Universally Unique Identifier (UUID). Min: 36 Max: 36 Example: <i>138a224d-c4c7-d621-0a00-c0eae49ce84c</i> |
| pending-config | Show pending configuration changes. |

with-pending-config View current configuration with pending changes included in the output.

Example

```
show access-rule ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
show access-rule ipv6 name <ACCESS_RULE_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show an IPv6 access rule for associated name.

Options

<ACCESS_RULE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show access-rule ipv6 name "OfficePolicyV6"
```

Syntax

```
show ssl-control [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show SSL control configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show ssl-control
```

Syntax

```
show tcp [ { pending-config | with-pending-config } | statistics ]
```

Mode

All Modes

Description

Show TCP configuration or traffic statistics.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.
- statistics*** Show TCP statistics.

Example

```
show tcp
```

Syntax

```
show bandwidth-objects [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all bandwidth objects.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show bandwidth-objects
```

Syntax

```
show bandwidth-object <BANDWIDTH_OBJ_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show a bandwidth object.

Options

- <BANDWIDTH_OBJ_NAME>*** Bandwidth object name.
Example: `"Corp High Priority"`
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show bandwidth-object "Corp High Priority"
```

Syntax

```
show udp [ { pending-config | with-pending-config } | statistics ]
```

Mode

All Modes

Description

Show UDP configuration or traffic statistics.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.
- statistics*** Show UDP statistics.

Example

```
show udp
```

Syntax

```
show icmp [ { pending-config | with-pending-config } | statistics ]
```

Mode

All Modes

Description

Show ICMP configuration or traffic statistics.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.
- statistics*** Show ICMP statistics.

Example

```
show icmp
```

Syntax

```
show qos-mapping [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show QoS mapping.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show qos-mapping
```

Syntax

administration

Mode

Config

Description

Administration settings.

Example

administration

Syntax

firewall-name <WORD>

Mode

Administration

Description

Set the name for the firewall.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

firewall-name "ACME Corporate Firewall"

Syntax

no firewall-name

Mode

Administration

Description

Clear the name for the firewall.

Example

no firewall-name

Syntax

firewall-domain-name <WORD>

Mode

Administration

Description

Set the domain name for the firewall.

Options

<**WORD**> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
firewall-domain-name "ACME Corporate"
```

Syntax

```
no firewall-domain-name
```

Mode

Administration

Description

Clear the domain name for the firewall.

Example

```
no firewall-domain-name
```

Syntax

```
language-override { chinese | chinese-traditional | english | japanese | korean | portuguese }
```

Mode

Administration

Options

chinese Chinese.

chinese-traditional Chinese (Traditional).

english English.

japanese Japanese.

korean Korean.

portuguese Portuguese.

Example

```
language-override english
```

Syntax

```
no language-override
```

Mode

Administration

Example

```
no language-override
```

Syntax

admin name <WORD>

Mode

Administration

Description

Set the name for the built in administrator.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

admin name headhoncho

Syntax

admin password old-password <WORD> new-password <WORD> confirm-password <WORD>

Mode

Administration

Description

Set the password for the built in administrator.

Options

old-password Enter the old password.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

new-password Enter the new password.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

confirm-password Confirm the new password.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

admin password old-password passwd new-password smorgasbord confirm-password smorgasbord

Syntax

admin one-time-password totp

Mode

Administration

Description

Set admin one-time passwords method.

Example

admin one-time-password totp

Syntax

no admin one-time-password

Mode

Administration

Description

Disable one-time password required for the admin.

Example

```
no admin one-time-password
```

Syntax

```
admin unbind-totp-key
```

Mode

Administration

Description

Unbind admin totp key.

Example

```
admin unbind-totp-key
```

Syntax

```
wireless-lan
```

Mode

Administration

Description

Enable wireless LAN.

Example

```
wireless-lan
```

Syntax

```
no wireless-lan
```

Mode

Administration

Description

Disable wireless LAN.

Example

```
no wireless-lan
```

Syntax

```
ipv6
```

Mode

Administration

Description

Enable IPv6.

Example

```
ipv6
```

Syntax

```
no ipv6
```

Mode

Administration

Description

Disable IPv6.

Example

```
no ipv6
```

Syntax

```
password aging [ duration <UINT16> ]
```

Mode

Administration

Description

Enable that password must be changed every set number of days and configure duration.

Options

duration Set the number of days before the password must be changed.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
password aging duration 90
```

Syntax

```
no password aging
```

Mode

Administration

Description

Disable that password must be changed every set number of days.

Example

```
no password aging
```

Syntax

```
password uniqueness [ count <UINT8> ]
```


Mode

Administration

Description

Enable barring of repeated passwords and configure.

Options

- count** Set the number of password changes before repeated password are allowed.
<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
password uniqueness count 5
```

Syntax

```
no password uniqueness
```

Mode

Administration

Description

Disable barring of repeated passwords.

Example

```
no password uniqueness
```

Syntax

```
password enforce-character-difference
```

Mode

Administration

Description

Enable new password must contain 4 characters different from the old password.

Example

```
password enforce-character-difference
```

Syntax

```
no password enforce-character-difference
```

Mode

Administration

Description

Disable new password must contain 4 characters different from the old password.

Example

```
no password enforce-character-difference
```

Syntax

```
password minimum-length <UINT8>
```

Mode

Administration

Description

Set the minimum password length to enforce.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
password minimum-length 8
```

Syntax

```
password complexity alpha-and-numeric-and-symbols
```

Mode

Administration

Description

Set the allowed complexity of the password.

Example

```
password complexity alpha-and-numeric-and-symbols
```

Syntax

```
password complexity alpha-and-numeric
```

Mode

Administration

Description

Set the allowed complexity of the password.

Example

```
password complexity alpha-and-numeric
```

Syntax

```
password complexity type { alpha-and-numeric | alpha-and-numeric-and-symbols }
```

Mode

Administration

Description

Set the allowed complexity of the password.

Options

alpha-and-numeric

Must contain both numbers and letters.

alpha-and-numeric-and-symbols Must contain numbers, letters, and symbols.

Example

```
password complexity alpha-and-numeric-and-symbols
```

Syntax

```
password complexity upper-case <UINT16>
```

Mode

Administration

Description

Set the upper-case complexity of the password.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
password complexity upper-case 1
```

Syntax

```
password complexity lower-case <UINT16>
```

Mode

Administration

Description

Set the lower-case complexity of the password.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
password complexity lower-case 1
```

Syntax

```
password complexity digital <UINT16>
```

Mode

Administration

Description

Set the digital complexity of the password.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

password complexity digital 1

Syntax

password complexity symbolic <UINT16>

Mode

Administration

Description

Set the symbolic complexity of the password.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

password complexity symbolic 1

Syntax

no password complexity [digital | lower-case | symbolic | upper-case]

Mode

Administration

Description

Clear password complexity.

Options

digital Set minimum digital character number.

lower-case Set minimum lower case character number.

symbolic Set minimum symbolic character number.

upper-case Set minimum upper case character number.

Example

no password complexity

Syntax

password constraints-apply-to [builtin-admin] [full-admins] [limited-admins] [local-users] [guest-admins] [system-admins] [crypto-admins] [audit-admins]

Mode

Administration

Description

Set whom to apply the password constraints to.

Options

builtin-admin Built in administrator.

full-admins Other full administrators.

| | |
|-----------------------|-------------------------|
| limited-admins | Limited administrators. |
| local-users | Other local users. |
| guest-admins | Guest admins. |
| system-admins | System administrators |
| crypto-admins | Crypto administrators |
| audit-admins | Audit administrators |

Example

```
password constraints-apply-to builtin-admin full-admins
```

Syntax

```
no password constraints-apply-to [ builtin-admin ] [ full-admins ] [ limited-admins ] [ local-users ] [ guest-admins ] [ system-admins ] [ crypto-admins ] [ audit-admins ]
```

Mode

Administration

Description

Remove setting of whom to apply the password constraints to.

Options

| | |
|-----------------------|----------------------------|
| builtin-admin | Built in administrator. |
| full-admins | Other full administrators. |
| limited-admins | Limited administrators. |
| local-users | Other local users. |
| guest-admins | Guest admins. |
| system-admins | System administrators |
| crypto-admins | Crypto administrators |
| audit-admins | Audit administrators |

Example

```
no password constraints-apply-to builtin-admin full-admins
```

Syntax

```
idle-logout-time <UINT16>
```

Mode

Administration

Description

Set the allowed period of inactivity before administrators are logged out of the management interface.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
idle-logout-time 60
```

Syntax

```
user-lockout [ failures-rate <UINT8> ] [ failures-duration <UINT8> ] [ lockout-duration <UINT8> ]
```

Mode

Administration

Description

Enable administrator / user lockout and set conditions.

Options

| | |
|---------------------------------|--|
| <i>failures-rate</i> | Set the failed login attempts in designed duration before lockout. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| <i>failures-duration</i> | Set the failed in designed duration before lockout. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| <i>lockout-duration</i> | Set number of minutes a user should be locked out. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |

Example

```
user-lockout failures-rate 5 failures-duration 5 lockout-duration 10
```

Syntax

```
no user-lockout
```

Mode

Administration

Description

Disable administrator / user lockout for set conditions.

Example

```
no user-lockout
```

Syntax

```
local-user-lockout
```

Mode

Administration

Description

Enable local administrator/user account lockout (uncheck for login IP address lockout).

Example

```
local-user-lockout
```

Syntax

```
no local-user-lockout
```

Mode

Administration

Description

Disable local administrator/user account lockout (uncheck for login IP address lockout).

Example

```
no local-user-lockout
```

Syntax

log-without-lockout

Mode

Administration

Description

Enable Log event only without lockout.

Example

log-without-lockout

Syntax

no log-without-lockout

Mode

Administration

Description

Disable Log event only without lockout.

Example

no log-without-lockout

Syntax

admin preempt-action { goto-non-config | logout }

Mode

Administration

Description

Set action to do upon preemption by another administrator.

Options

goto-non-config Drop to non-config mode.

logout Logout.

Example

admin preempt-action logout

Syntax

admin preempt-inactivity-timeout <UINT16>

Mode

Administration

Description

Allow preemption by a lower priority administrator after inactivity of (minutes).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
admin preempt-inactivity-timeout 10
```

Syntax

```
inter-admin-messaging <UINT8>
```

Mode

Administration

Description

Enable inter administrator messaging and set the messaging polling interval.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
inter-admin-messaging 10
```

Syntax

```
no inter-admin-messaging
```

Mode

Administration

Description

Disable inter-administrator messaging.

Example

```
no inter-admin-messaging
```

Syntax

```
multiple-admin
```

Mode

Administration

Description

Enable multiple administrative roles.

Example

```
multiple-admin
```

Syntax

no multiple-admin

Mode

Administration

Description

Disable multiple administrative roles.

Example

no multiple-admin

Syntax

enhanced-audit-logging

Mode

Administration

Description

Enable enhanced audit logging.

Example

enhanced-audit-logging

Syntax

no enhanced-audit-logging

Mode

Administration

Description

Disable enhanced audit logging.

Example

no enhanced-audit-logging

Syntax

wireless-controller-mode { non-wireless-controller | normal-firewall | wireless-controller }

Mode

Administration

Description

Set wireless controller mode.

Options

non-wireless-controller Set wireless controller as non wireless controller mode.

normal-firewall Set wireless controller as normal firewall mode.

wireless-controller Set wireless controller as wireless controller mode.

Example

wireless-controller-mode normal-firewall

Syntax

web-management allow-http

Mode

Administration

Description

Allow HTTP management (it is less secure than using HTTPS).

Example

web-management allow-http

Syntax

no web-management allow-http

Mode

Administration

Description

Do not allow HTTP management (it is less secure than using HTTPS).

Example

no web-management allow-http

Syntax

http-port <IPV4_PORT>

Mode

Administration

Description

Set the HTTP management port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

http-port 8080

Syntax

https-port <IPV4_PORT>

Mode

Administration

Description

Set the HTTPS management port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
https-port 4433
```

Syntax

```
web-management certificate { name <CERT_NAME> | use-self-signed }
```

Mode

Administration

Description

Set the HTTPS management server certificate to use.

Options

name Specify certificate.
<CERT_NAME> Certificate name.
Example: *my_cert*

use-self-signed Use self signed certificate.

Example

```
web-management certificate name "ACME Inc."
```

Syntax

```
web-management cert-common-name <WORD>
```

Mode

Administration

Description

Set the self signed certificate common name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
web-management cert-common-name www.acme.com
```

Syntax

```
no web-management cert-common-name
```

Mode

Administration

Description

Clear the self signed certificate common name.

Example

no web-management cert-common-name

Syntax

web-management client-certificate-check

Mode

Administration

Description

Enable client certificate check.

Example

web-management client-certificate-check

Syntax

no web-management client-certificate-check

Mode

Administration

Description

Disable client certificate check.

Example

no web-management client-certificate-check

Syntax

web-management client-certificate-issuer <CERT_ISSUER>

Mode

Administration

Description

Set client certificate issuer.

Options

<CERT_ISSUER> Certificate Issuer.
Example: *Thawte Server CA*

Example

web-management client-certificate-issuer "Thawte Premium Server CA"

Syntax

web-management oosp-check <URL>

Mode

Administration

Description

Enable oosp check.

Options

<URL> URL in the form: http://host/file.
Example: `http://www.example.com/products/`

Example

```
web-management oosp-check http://www.example.com/products/
```

Syntax

```
no web-management oosp-check
```

Mode

Administration

Description

Disable oosp check.

Example

```
no web-management oosp-check
```

Syntax

```
web-management default-table-size <UINT16>
```

Mode

Administration

Description

Set default size of tables within the Web Management User Interface.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: `123`

Example

```
web-management default-table-size 50
```

Syntax

```
web-management refresh-interval <UINT16>
```

Mode

Administration

Description

Set auto-update refresh interval of tables within the web management user interface.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: `123`

Example

```
web-management refresh-interval 15
```

Syntax

```
web-management tooltip [ form-delay <UINT16> ] [ button-delay <UINT16> ] [ text-delay <UINT16> ]
```

Mode

Administration

Description

Enable tooltips in web management UI and configure.

Options

| | |
|------------------------------|---|
| <i>form-delay</i> | Set form tooltip delay. |
| <i><UINT16></i> | Integer in the form: D OR 0xHHHH. Example: 123 |
| <i>button-delay</i> | Set button tooltip delay. |
| <i><UINT16></i> | Integer in the form: D OR 0xHHHH. Example: 123 |
| <i>text-delay</i> | Set text tooltip delay. |
| <i><UINT16></i> | Integer in the form: D OR 0xHHHH. Example: 123 |

Example

```
web-management tooltip form-delay 2000 button-delay 3000 text-delay 500
```

Syntax

```
no web-management tooltip
```

Mode

Administration

Description

Disable tooltips in web management UI and configure.

Example

```
no web-management tooltip
```

Syntax

```
dashboard-as-starting-page
```

Mode

Administration

Description

Use dashboard as starting page.

Example

```
dashboard-as-starting-page
```

Syntax

```
no dashboard-as-starting-page
```

Mode

Administration

Description

Disable to use dashboard as starting page.

Example

```
no dashboard-as-starting-page
```

Syntax

```
tls-and-above
```

Mode

Administration

Description

Enforce TLS 1.1 and above.

Example

```
tls-and-above
```

Syntax

```
no tls-and-above
```

Mode

Administration

Description

Disable enforce TLS 1.1 and above.

Example

```
no tls-and-above
```

Syntax

```
out-of-band-management
```

Mode

Administration

Description

Enable out of band management on management port.

Example

```
out-of-band-management
```

Syntax

```
no out-of-band-management
```

Mode

Administration

Description

Disable out of band management on management port.

Example

```
no out-of-band-management
```

Syntax

```
override-download-url sonicpoint n <WORD>
```

Mode

Administration

Description

Manually specify SonicPoint N image URL (http://).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
override-download-url sonicpoint n my.webserver.local/applications/sonicpointn.img.bin
```

Syntax

```
no override-download-url sonicpoint n
```

Mode

Administration

Description

Disable manually specifying SonicPoint N image URL.

Example

```
no override-download-url sonicpoint n
```

Syntax

```
override-download-url sonicpoint nv <WORD>
```

Mode

Administration

Description

Manually specify SonicPoint Ni/Ne image URL (http://).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
override-download-url sonicpoint nv my.webserver.local/applications/sonicpointnv.img.bin
```

Syntax


```
no override-download-url sonicpoint nv
```

Mode

Administration

Description

Disable manually specifying SonicPoint Ni/Ne image URL.

Example

```
no override-download-url sonicpoint nv
```

Syntax

```
override-download-url sonicpoint ndr <WORD>
```

Mode

Administration

Description

Manually specify SonicPoint NDR image URL (http://).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
override-download-url sonicpoint ndr my.webserver.local/applications/sonicpointndr.img.bin
```

Syntax

```
no override-download-url sonicpoint ndr
```

Mode

Administration

Description

Disable manually specifying SonicPoint NDR image URL.

Example

```
no override-download-url sonicpoint ndr
```

Syntax

```
override-download-url sonicpoint ac <WORD>
```

Mode

Administration

Description

Manually specify SonicPoint AC image URL (http://).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
override-download-url sonicpoint ac my.webserver.local/applications/sonicpointac.img.bin
```

Syntax

```
no override-download-url sonicpoint ac
```

Mode

Administration

Description

Disable manually specifying SonicPoint AC image URL.

Example

```
no override-download-url sonicpoint ac
```

Syntax

```
gms-management { existing-tunnel | https | ipsec-tunnel }
```

Mode

Administration

Description

Enable GMS management and set the type of tunnel to use.

Options

existing-tunnel Use existing tunnel.

https Use HTTPS.

ipsec-tunnel Use IPSEC tunnel.

Example

```
gms-management ssl
```

Syntax

```
no gms-management
```

Mode

Administration

Description

Disable GMS Management.

Example

```
no gms-management
```

Syntax

```
host-name <HOSTNAME>
```

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Set the GMS server IP or hostname.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
host-name 10.10.10.10
```

Syntax

```
syslog-server-port <IPV4_PORT>
```

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Set the syslog server port of the GMS server.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
syslog-server-port 514
```

Syntax

```
no syslog-server-port
```

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Clear syslog server port of the GMS server.

Example

```
no syslog-server-port
```

Syntax

```
heartbeat-status-only
```

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Enable Send Heartbeat Status Messages Only.

Example

```
heartbeat-status-only
```

Syntax

```
no heartbeat-status-only
```

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Disable Send Heartbeat Status Messages Only.

Example

```
no heartbeat-status-only
```

Syntax

```
behind-nat-device ip <IPV4_HOST>
```

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Enable Behind NAT Device indicator and configure IP.

Options

ip Set IP of NAT device.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
behind-nat-device ip 192.168.168.16
```

Syntax

```
no behind-nat-device
```

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Disable Behind NAT Device indicator.

Example

```
no behind-nat-device
```

Syntax

spi <WORD>

Mode

GMS IPSEC

Description

Set Incoming / Outgoing IPSEC SPI.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

spi C50F73F4

Syntax

encryption-type *des-md5*

Mode

GMS IPSEC

Description

Set IPSEC encryption type.

Options

des-md5 DES-MD5.

Example

encryption-type des-md5

Syntax

encryption-key <HEX_STRING>

Mode

GMS IPSEC

Description

Set IPSEC Encryption Key.

Options

<HEX_STRING> String of hexadecimal digits.
Example: *0123456989abcdef*

Example

encryption-key 9f8c6ae4fb897002

Syntax

authentication-key <HEX_STRING>

Mode

GMS IPSEC

Description

Set IPSEC authentication key.

Options

<HEX_STRING> String of hexadecimal digits.
Example: *0123456989abcdef*

Example

```
ipsec-authentication-key bd5a1354f5a5a8e198974d4d997fac5e
```

Syntax

```
reporting-server [ ip <HOSTNAME> ] [ port <IPV4_PORT> ]
```

Mode

GMS HTTPS

Description

Enable Send Syslog Messages to a Distributed GMS Reporting Server and configure.

Options

ip Set distributed GMS reporting server IP address.
<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*
port Set distributed GMS reporting server port.
<IPV4_PORT> Integer in the form: D OR 0xHHHHH.
Example: *80*

Example

```
reporting-server ip 10.10.10.11 port 514
```

Syntax

```
no reporting-server [ ip | port ]
```

Mode

GMS HTTPS

Description

Disable Send Syslog Messages to a Distributed GMS Reporting Server.

Options

ip Clear distributed GMS reporting server IP address.
port Clear distributed GMS reporting server port.

Example

```
no reporting-server
```

Syntax

```
sonicos-api
```

Mode

Administration

Description

Enable SonicOS API.

Example

```
sonicos-api
```

Syntax

```
no sonicos-api
```

Mode

Administration

Description

Disable SonicOS API.

Example

```
no sonicos-api
```

Syntax

```
digest
```

Mode

SonicOS API

Description

Enable SonicOS API HTTP digest access authentication.

Example

```
digest
```

Syntax

```
no digest
```

Mode

SonicOS API

Description

Disable SonicOS API HTTP digest access authentication.

Example

```
no digest
```

Syntax

```
sha256-digest
```

Mode

SonicOS API

Description

Enable SonicOS API HTTP digest SHA256.

Example

```
sha256-digest
```

Syntax

```
no sha256-digest
```

Mode

SonicOS API

Description

Disable SonicOS API HTTP digest SHA256.

Example

```
no sha256-digest
```

Syntax

```
md5-digest
```

Mode

SonicOS API

Description

Enable SonicOS API HTTP digest MD5.

Example

```
md5-digest
```

Syntax

```
no md5-digest
```

Mode

SonicOS API

Description

Disable SonicOS API HTTP digest MD5.

Example

```
no md5-digest
```

Syntax

```
integrity-protection { allowed | enforced }
```

Mode

SonicOS API

Description

SonicOS API digest integrity protection.

Options

allowed Allowed

enforced Enforced

Example

integrity-protection allowed

Syntax

no integrity-protection

Mode

SonicOS API

Description

Disable SonicOS API digest integrity protection.

Example

no integrity-protection disabled

Syntax

chap

Mode

SonicOS API

Description

Enable SonicOS API CHAP authentication.

Example

chap

Syntax

no chap

Mode

SonicOS API

Description

Disable SonicOS API CHAP authentication.

Example

no chap

Syntax

basic

Mode

SonicOS API

Description

Enable SonicOS API HTTP basic access authentication.

Example

```
basic
```

Syntax

```
no basic
```

Mode

SonicOS API

Description

Disable SonicOS API HTTP basic access authentication.

Example

```
no basic
```

Syntax

```
public-key
```

Mode

SonicOS API

Description

Enable SonicOS API public key authentication.

Example

```
public-key
```

Syntax

```
no public-key
```

Mode

SonicOS API

Description

Disable SonicOS API public key authentication.

Example

```
no public-key
```

Syntax

```
rsa-key-size <UINT16>
```

Mode

SonicOS API

Description

SonicOS API public key RSA key size.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
rsa-key-size 1024
```

Syntax

```
rsa-padding-type { pkcsv15 | pkcsv20oaep }
```

Mode

SonicOS API

Description

SonicOS API public key RSA padding type.

Options

pkcsv15 PKCS#1 v1.5

pkcsv20oaep PKCS#1 v2.0 OEAP

Example

```
rsa-padding-type pkcsv20oaep
```

Syntax

```
session-security
```

Mode

SonicOS API

Description

Enable SonicOS API session security.

Example

```
session-security
```

Syntax

```
no session-security
```

Mode

SonicOS API

Description

Disable SonicOS API session security.

Example

```
no session-security
```

Syntax

hold-password

Mode

SonicOS API

Description

Enable SonicOS API can hold user password.

Example

hold-password

Syntax

no hold-password

Mode

SonicOS API

Description

Disable SonicOS API can hold user password.

Example

no hold-password

Syntax

max-nonce <UINT16>

Mode

SonicOS API

Description

SonicOS API session security max nonce.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

max-nonce

Syntax

two-factor-bearer-token

Mode

SonicOS API

Description

Enable SonicOS API two-factor and bearer token authentication.

Example

two-factor-bearer-token

Syntax

no two-factor-bearer-token

Mode

SonicOS API

Description

Disable SonicOS API two-factor and bearer token authentication.

Example

no two-factor-bearer-token

Syntax

snmp

Mode

Config

Description

Enable SNMP and Enter SNMP configuration mode.

Example

snmp

Syntax

no snmp

Mode

Config

Description

Disable SNMP.

Example

no snmp

Syntax

system-name <WORD>

Mode

SNMP

Description

Set the SNMP system name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
system-name "Corporate Gateway"
```

Syntax

```
no system-name
```

Mode

SNMP

Description

Remove the SNMP system name.

Example

```
no system-name
```

Syntax

```
system-contact <WORD>
```

Mode

SNMP

Description

Set the SNMP system contact.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
system-contact "John Doe"
```

Syntax

```
no system-contact
```

Mode

SNMP

Description

Remove the SNMP system contact.

Example

```
no system-contact
```

Syntax

```
system-location <WORD>
```

Mode

SNMP

Description

Set the SNMP system location.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
system-location "Corporate Site"
```

Syntax

```
no system-location
```

Mode

SNMP

Description

Remove the SNMP system location.

Example

```
no system-location
```

Syntax

```
asset-number <WORD>
```

Mode

SNMP

Description

Set the SNMP asset number.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
asset-number Unit001
```

Syntax

```
no asset-number
```

Mode

SNMP

Description

Remove the SNMP asset number.

Example

```
no asset-number
```

Syntax

get-community-name <WORD>

Mode

SNMP

Description

Set the SNMP get community name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

get-community-name public

Syntax

no get-community-name

Mode

SNMP

Description

Remove the SNMP get community name.

Example

no get-community-name

Syntax

trap-community-name <WORD>

Mode

SNMP

Description

Set the SNMP trap community name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

trap-community-name public

Syntax

no trap-community-name

Mode

SNMP

Description

Remove the SNMP trap community name.

Example

no trap-community-name

Syntax

host <UINT8> <HOSTNAME_MIXED>

Mode

SNMP

Description

Set SNMP trap host.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

host 1 192.168.168.201

Syntax

no host <UINT8>

Mode

SNMP

Description

Remove SNMP Trap Host.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

no host 1

Syntax

snmp3 mandatory

Mode

SNMP

Description

Enable mandatory requirement for SNMP3.

Example

snmp3 mandatory

Syntax

no snmp3 mandatory

Mode

SNMP

Description

Disable mandatory requirement for SNMP3.

Example

```
no snmp3 mandatory
```

Syntax

```
snmp3 engine-id <WORD>
```

Mode

SNMP

Description

Set SNMP3 Engine ID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
snmp3 engine-id 80002225030017C5696969
```

Syntax

```
snmp3 increase-subsystem-priority
```

Mode

SNMP

Description

Enable increase subsystem priority for SNMP3.

Example

```
snmp3 increase-subsystem-priority
```

Syntax

```
no snmp3 increase-subsystem-priority
```

Mode

SNMP

Description

Disable increase subsystem priority for SNMP3.

Example

```
no snmp3 increase-subsystem-priority
```

Syntax

```
view <SNMP_VIEW_NAME> oid <WORD>
```

Mode

SNMP

Description

Add/Edit an SNMP view OID list and enter its configuration mode.

Options

| | |
|-------------------------------|--|
| <SNMP_VIEW_NAME> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>ICMP</i> |
| oid | Add an OID to the SNMP view list. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

Example

```
view CorpSNMPViewList oid 1.3.6.1.2.1.32
```

Syntax

```
no view <SNMP_VIEW_NAME> [ oid <SNMP_OID_IN_VIEW> ]
```

Mode

SNMP

Description

Delete an SNMP view OID list.

Options

| | |
|---------------------------------|--|
| <SNMP_VIEW_NAME> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>ICMP</i> |
| oid | Delete an OID from the SNMP view list. |
| <SNMP_OID_IN_VIEW> | SNMP view oid name. Example: <i>1.3.5</i> |

Example

```
no view CorpSNMPViewList oid 1.3.6.1.2.1.32
```

Syntax

```
group <SNMP_GROUP_NAME>
```

Mode

SNMP

Description

Add an SNMP group.

Options

| | |
|--------------------------------|--|
| <SNMP_GROUP_NAME> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>Group1</i> |
|--------------------------------|--|

Example

```
group CorpSNMPGroup
```

Syntax

```
no group <SNMP_GROUP_NAME>
```

Mode

SNMP

Description

Delete an SNMP group.

Options

<SNMP_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

```
no group CorpSNMPGroup
```

Syntax

```
user <SNMP_USER_NAME>
```

Mode

SNMP

Description

Add/Edit an SNMP user and enter its configuration mode.

Options

<SNMP_USER_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

```
user snmp-admin1
```

Syntax

```
no user <SNMP_USER_NAME>
```

Mode

SNMP

Description

Delete an SNMP user.

Options

<SNMP_USER_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

```
no user snmp-admin1
```

Syntax

```
name <WORD>
```

Mode

SNMP User

Description

Set an SNMP user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name snmp-admin1
```

Syntax

```
security-level { authentication-and-privacy | authentication-only }
```

Mode

SNMP User

Description

Set a SNMP user security level.

Options

authentication-and-privacy Use authentication and encryption.

authentication-only Use authentication.

Example

```
security-level authentication-and-privacy  
security-level authentication-only
```

Syntax

```
no security-level
```

Mode

SNMP User

Description

Disable authentication and encryption.

Example

```
no security-level
```

Syntax

```
authentication { md5 <ENC_PASSWORD> | sha1 <ENC_PASSWORD> }
```

Mode

SNMP User

Description

Set a SNMP user authentication type and key.

Options

md5 MD5.
<ENC_PASSWORD> Password.
Example: *secret*

sha1 SHA-1.
<ENC_PASSWORD> Password.
Example: *secret*

Example

```
authentication md5 bd5a1354f5a5a8e198974d4d997fac5e
```

Syntax

```
encryption { aes <ENC_PASSWORD> | des <ENC_PASSWORD> }
```

Mode

SNMP User

Description

Set a SNMP user encryption.

Options

aes AES.
<ENC_PASSWORD> Password.
Example: *secret*

des DES.
<ENC_PASSWORD> Password.
Example: *secret*

Example

```
encryption des 9f8c6ae4fb897002
```

Syntax

```
group <SNMP_GROUP_NAME>
```

Mode

SNMP User

Description

Assign an SNMP group.

Options

<SNMP_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

```
group CorpSNMPGroup
```

Syntax

```
no group
```

Mode

SNMP User

Description

Assign user to *No Group*.

Example

```
no group
```

Syntax

```
access <SNMP_ACCESS_NAME>
```

Mode

SNMP

Description

Add/Edit an SNMP access object and enter its configuration mode.

Options

<SNMP_ACCESS_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

```
access SnpAccessObject
```

Syntax

```
no access <SNMP_ACCESS_NAME>
```

Mode

SNMP

Description

Delete an SNMP access object.

Options

<SNMP_ACCESS_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

```
no access SnpAccessObject
```

Syntax

```
name <WORD>
```

Mode

SNMP Access

Description

Set an SNMP access object name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name *SnmpAccessObject*

Syntax

```
read-view <SNMP_VIEW_NAME>
```

Mode

SNMP Access

Description

Set the SNMP read view.

Options

<SNMP_VIEW_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *ICMP*

Example

```
read-view interfaces
```

Syntax

```
master-group <SNMP_GROUP_NAME>
```

Mode

SNMP Access

Description

Assign a master SNMP3 master group.

Options

<SNMP_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

```
master-group CorpSNMPGroup
```

Syntax

```
security-level { authentication-and-privacy | authentication-only }
```

Mode

SNMP Access

Description

Set SNMP access security level.

Options

authentication-and-privacy Use authentication and encryption.

authentication-only Use authentication.

Example

```
security-level authentication-only  
security-level authentication-and-privacy
```

Syntax

```
no security-level
```

Mode

SNMP Access

Description

Disable authentication and encryption.

Example

```
no security-level
```

Syntax

```
export current-config { cli | exp } { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

All Modes

Description

Export current configuration.

Options

cli Export configuration using the SonicOS E-CLI command format.

exp Export configuration using the SonicOS WebUI (.exp) format.

ftp Export using the FTP protocol.

<FTP_URL> FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/

scp Export using the SCP protocol.

<SCP_URL> SCP URL in the form: scp://username@host/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: scp://username@host/\nscp://host/

Example

```
export current-config cli ftp ftp://user:password@servername/sw-prodname-buildversion-ecli.txt
export current-config cli scp scp://user@server/sw-prodname-buildversion-ecli.txt
```

Syntax

```
export pending-config { cli | exp } { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

All Modes
Top Level

Description

Export pending configuration.

Options

cli Export configuration using the SonicOS E-CLI command format.

exp Export configuration using the SonicOS WebUI (.exp) format.

ftp Export using the FTP protocol.
<FTP_URL> FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'.
Example: ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/

scp Export using the SCP protocol.
<SCP_URL> SCP URL in the form: scp://username@host/\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'.
Example: scp://username@host/\nscp://host/

Example

```
export pending-config cli ftp ftp://user:password@servername/sw-prodname-buildversion-ecli.txt  
export pending-config cli scp scp://user@server/sw-prodname-buildversion-ecli.txt
```

Syntax

```
export firmware { current | system-backup | uploaded } { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

Config

Description

Export the current firmware image off of the appliance.

Options

current Current Firmware.

system-backup Download the system backup firmware image.

uploaded Download the latest uploaded firmware image.

ftp Export using the FTP protocol.
<FTP_URL> FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'.
Example: ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/

scp Export using the SCP protocol.
<SCP_URL> SCP URL in the form: scp://username@host/\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'.
Example: scp://username@host/\nscp://host/

Example

```
export firmware current ftp ftp://user:password@servername/firmware.bin.sig  
export firmware current scp scp://user@server/firmware.bin.sig
```

Syntax

```
export tech-support-report { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

Top Level
Config

Description

Export the technical support report.

Options

ftp Export using the FTP protocol.
<FTP_URL> FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'.
Example: ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/

scp Export using the SCP protocol.
<SCP_URL> SCP URL in the form: scp://username@host/\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'.
Example: scp://username@host/\nscp://host/

Example: `scp://username@host/\nscp://host/`

Example

```
export tech-support-report ftp ftp://user:password@servername/techSupport.wri
export tech-support-report scp scp://user@server/techSupport.wri
```

Syntax

```
firmware auto { download | update }
```

Mode

Config

Description

Enable periodic checking of SonicWall site for firmware update.

Options

download Enable automatic downloading of firmware from SonicWall software site.

update Enable periodic checking of SonicWall site for firmware update.

Example

```
firmware auto update
```

Syntax

```
no firmware auto { download | update }
```

Mode

Config

Description

Disable periodic checking of SonicWall site for firmware update.

Options

download Disable automatic downloading of firmware from SonicWall software site.

update Disable periodic checking of SonicWall site for firmware update.

Example

```
no firmware auto update
```

Syntax

```
firmware diagnostics
```

Mode

Config

Description

Enable booting of firmware with diagnostics mode enabled (if available).

Example

```
firmware diagnostics
```

Syntax

```
no firmware diagnostics
```

Mode

Config

Description

Disable booting of firmware with diagnostics.

Example

```
no firmware diagnostics
```

Syntax

```
firmware backup
```

Mode

Config

Description

Create Backup Settings.

Syntax

```
import firmware { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

Config

Description

Import firmware to the firewall.

Options

ftp Import using the FTP protocol.

<FTP_URL> FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/

scp Import using the SCP protocol.

<SCP_URL> SCP URL in the form: scp://username@host/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: scp://username@host/\nscp://host/

Example

```
import firmware ftp ftp://user:password@servername/firmware.bin.sig
import firmware scp scp://user@server/firmware.bin.sig
```

Syntax

```
import cli { ftp <FTP_URL> | scp <SCP_URL> | terminal } merge [ best-effort ] [ clear-pending ]
```

Mode

Config

Description

Import configuration using the SonicOS E-CLI command format.

Options

| | |
|------------------------|--|
| ftp | Import using the FTP protocol. |
| <FTP_URL> | FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <code>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</code> |
| scp | Import using the SCP protocol. |
| <SCP_URL> | SCP URL in the form: scp://username@host/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <code>scp://username@host/\\nscp://host/</code> |
| terminal | Import using the terminal. |
| merge | Combines configuration imported with the current configuration running and saved to the device. |
| best-effort | Ignore validation errors and import only valid configuration (best effort). |
| clear-pending | Clear pending changes. |

Example

```
import cli ftp ftp://user:password@servername/current-config-cli.txt merge best-effort
import cli ftp ftp://user:password@servername/current-config-cli.txt merge
import cli scp scp://user@server/current-config-cli.txt merge best-effort
import cli terminal merge
```

Syntax

```
restart [ at <TIME_YYYYMMDDHHMMSS> | cancel | in <UINT32> { days | hours | minutes } | now | time <UINT32> ]
```

Mode

Top Level
Config

Description

Restart SonicOS - now or after an interval of time.

Options

| | |
|------------------------------------|--|
| at | Restart at the time specified. |
| <TIME_YYYYMMDDHHMMSS> | Timestamp in the form: YYYY:MM:DD:HH:MM:SS. Example: <code>2010:06:30:23:30:59</code> |
| cancel | Cancel restart. |
| in | Restart after the specified interval. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: <code>123</code> |
| days | Set in days. |
| hours | Set in hours. |
| minutes | Set in minutes. |
| now | Restart immediately. |
| time | Restart after the specified number of seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: <code>123</code> |

Example

```
restart
```

Syntax

safemode

Mode

Top Level

Description

Restart the device and enter safemode.

Example

safemode

Syntax

restore-defaults

Mode

Config

Description

Restore the device to factory default settings.

Example

restore-defaults

Syntax

boot { { { current | uploaded } [backup | factory-default] } | system-backup }

Mode

Config

Description

Boot current or uploaded firmware image with current or default settings or boot system backup.

Options

| | |
|------------------------|--|
| <i>current</i> | Boot current firmware image. |
| <i>uploaded</i> | Boot the latest uploaded firmware image. |
| <i>backup</i> | Boot firmware with backup settings. |
| <i>factory-default</i> | Boot current firmware with default settings. |
| <i>system-backup</i> | Boot system backup firmware. |

Example

boot current factory-default

Syntax

time

Mode

Config

Description

Enter time configuration mode.

Example

```
time
```

Syntax

```
time <TIME_HHMMSS>
```

Mode

Time

Description

Specify time.

Options

<TIME_HHMMSS> Time in the form: DD:DD:DD.
Example: 12:00:00

Example

```
time 12:30:59
```

Syntax

```
date <DATE_YYYYMMDD>
```

Mode

Time

Description

Specify date.

Options

<DATE_YYYYMMDD> Date in the form: YYYY:MM:DD.
Example: 2010:06:30

Example

```
date 2010:06:31
```

Syntax

```
time-zone <TIME_ZONE>
```

Mode

Time

Description

Specify time zone.

Options

<TIME_ZONE> Time Zone.
Example: *pacific-time*

Example

```
time-zone pacific-time
time-zone atlantic-time
time-zone russia-gmt+7
time-zone china,philippines
```

Syntax

```
use-ntp
```

Mode

Time

Description

Enable use of NTP servers to obtain time.

Example

```
use-ntp
```

Syntax

```
no use-ntp
```

Mode

Time

Description

Disable use of NTP servers to obtain time.

Example

```
no use-ntp
```

Syntax

```
daylight-savings
```

Mode

Time

Description

Enable automatic adjustment of clock for daylight saving time.

Example

```
daylight-savings
```

Syntax

```
no daylight-savings
```

Mode

Time

Description

Disable automatic adjustment of clock for daylight saving time.

Example

no daylight-savings

Syntax

universal

Mode

Time

Description

Enable display of UTC in logs (instead of local time).

Example

universal

Syntax

no universal

Mode

Time

Description

Disable display of UTC in logs (instead of local time).

Example

no universal

Syntax

international-format

Mode

Time

Description

Enable display of date in international format.

Example

international-format

Syntax

no international-format

Mode

Time

Description

Disable display of date in international format.

Example

no international-format

Syntax

only-custom-ntp

Mode

Time

Description

Enable only use custom NTP servers.

Example

only-custom-ntp

Syntax

no only-custom-ntp

Mode

Time

Description

Disable only use custom NTP servers.

Example

no only-custom-ntp

Syntax

ntp-server <NTP_SERVER> [md5 trust-key-no <UINT16> key-number <UINT16> password <WORD> | no-auth]

Mode

Time

Description

Add a server to the NTP server list.

Options

<NTP_SERVER> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

md5 NTP server uses MD5 authentication.

trust-key-no Trust key.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

key-number Key number.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

password Password.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

no-auth NTP server doesn't require authentication.

Example

ntp-server 192.168.168.160 no-auth
ntp-server 2016:12:15::2016 no-auth

```
ntp-server 192.168.168.160 md5 trust-key-no 10 key-number 20 password password
```

Syntax

```
no ntp-server <NTP_SERVER>
```

Mode

Time

Description

Remove a server from the NTP server list.

Options

<NTP_SERVER> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

```
no ntp-server 192.168.168.160
```

Syntax

```
no ntp-servers
```

Mode

Time

Description

Remove all servers from the NTP server list.

Example

```
no ntp-servers
```

Syntax

```
ntp-update-interval <UINT16>
```

Mode

Time

Description

Set the NTP Update Interval.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
ntp-update-interval 123
```

Syntax

```
license
```

Mode

Config

Description

License configuration.

Example

```
license
```

Syntax

```
synchronize
```

Mode

License

Description

Synchronize licenses with www.mysonicwall.com.

Example

```
synchronize
```

Syntax

```
upgrade { [ key <WORD> ] [ key-set <WORD> ] }
```

Mode

License

Description

Manual upgrade services.

Options

- key** Upgrade by key.
- <WORD>** Word in the form: WORD or "QUOTED STRING".
Example: *abc*
- key-set** Upgrade by key set.
- <WORD>** Word in the form: WORD or "QUOTED STRING".
Example: *abc*

Example

```
upgrade key CARZFDMR
```

Syntax

```
ssh server
```

Mode

Config

Description

Enter SSH server configuration mode.

Example

```
ssh server
```

Syntax

```
port <IPV4_PORT>
```

Mode

SSH Server

Description

Set the SSH port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
port 4022
```

Syntax

```
keygen
```

Mode

SSH Server

Description

Generate authentication keys for SSH.

Example

```
keygen
```

Syntax

```
restart
```

Mode

SSH Server

Description

Restart SSH server.

Example

```
restart
```

Syntax

```
enable
```

Mode

SSH Server

Description

Enable SSH server.

Example

```
enable
```

Syntax

terminate

Mode

SSH Server

Description

Disable SSH access and terminate all SSH sessions.

Example

terminate

Syntax

kill session ip <SSH_SERVER_SESSION_IP> port <SSH_SERVER_SESSION_PORT>

Mode

SSH Server

Description

Terminate specified SSH session.

Options

| | |
|--|--|
| <i>ip</i> | Terminate session at specified ip. |
| <i><SSH_SERVER_SESSION_IP></i> | IPV4: address in the form: D.D.D.D\nIPV6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i> |
| <i>port</i> | Client port. |
| <i><SSH_SERVER_SESSION_PORT></i> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

kill session ip 192.168.168.12 port 52781

Syntax

kill sessions

Mode

SSH Server

Description

Terminate all SSH session.

Example

kill sessions

Syntax

ssh client

Mode

Config

Syntax

server-key <WORD>

Mode

SSH Client

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Syntax

no server-key <WORD>

Mode

SSH Client

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Syntax

no server-keys

Mode

SSH Client

Syntax

fips

Mode

Config

Description

Enable FIPS mode.

Example

fips

Syntax

no fips

Mode

Config

Description

Disable FIPS mode.

Example

no fips

Syntax

ndpp

Mode

Config

Description

Enable NDPP mode.

Example

ndpp

Syntax

no ndpp

Mode

Config

Description

Disable NDPP mode.

Example

no ndpp

Syntax

show administration [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show Administration Configuration and Information.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

show administration

Syntax

show snmp [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show SNMP Configuration and Information.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show snmp
```

Syntax

```
show firmware [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show Firmware configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show firmware
```

Syntax

```
show status
```

Mode

All Modes

Description

Show basic system status and information.

Example

```
show status
```

Syntax

```
show time [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show Time settings or NTP settings.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show time
```

Syntax

```
show version
```

Mode

All Modes

Syntax

```
show license [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

status Show license status.

Syntax

```
show ssh server [ { pending-config | with-pending-config } | sessions ]
```

Mode

All Modes

Description

Show SSH server configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

sessions Show SSH server sessions.

Example

```
show ssh server
```

Syntax

```
show ssh client [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show SSH client configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show ssh client
```

Syntax

```
show fips [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show FIPS configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show fips
```

Syntax

```
show ndpp [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NDPP configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show ndpp
```

Syntax

```
user authentication
```

Mode

Config

Description

Configure user authentication related settings.

Example

```
user authentication
```

Syntax

```
method [ partition <PARTITION_NAME> ] { ldap | ldap-local | local | radius | radius-local }
```

Mode

User Authentication

Description

Set the user authentication method.

Options

| | |
|-------------------------------|--|
| partition | Set user authentication method for the select partition |
| <PARTITION_NAME> | User authentication partition name. Example: <i>CorpSales</i> |
| ldap | Use LDAP user authentication. |
| ldap-local | Use both LDAP and local user authentication. |
| local | Use local user authentication. |
| radius | Use RADIUS user authentication. |
| radius-local | Use both RADIUS and local user authentication. |

Example

```
method local  
method partition myPartition local
```

Syntax

```
sso-method { browser-ntlm [ { after-sso-agent-failed | before-sso-agent | enabled } ] | radius-accounting | sso-agent | terminal-services-agent }
```

Mode

User Authentication Per-partition

Description

Enable the single-sign-on mechanism.

Options

| | |
|-------------------------------|--|
| browser-ntlm | Enable browser NTLM authentication. |
| after-sso-agent-failed | Use NTLM to authenticate HTTP traffic only if SSO via the agent fails. |
| before-sso-agent | Use NTLM to authenticate HTTP traffic before attempting SSO via the agent. |

| | |
|---------------------------------------|--|
| <i>enabled</i> | Enable browser-ntlm option. |
| <i>radius-accounting</i> | Enable RADIUS accounting authentication. |
| <i>sso-agent</i> | Enable SSO agent authentication. |
| <i>terminal-services-agent</i> | Enable terminal services agent authentication. |

Example

```
sso-method sso-agent
```

Syntax

```
no sso-method { browser-ntlm | radius-accounting | sso-agent | terminal-services-agent }
```

Mode

User Authentication Per-partition

Description

Disable the single-sign-on mechanism.

Options

| | |
|---------------------------------------|---|
| <i>browser-ntlm</i> | Disable browser NTLM authentication. |
| <i>radius-accounting</i> | Disable RADIUS accounting authentication. |
| <i>sso-agent</i> | Disable SSO agent authentication. |
| <i>terminal-services-agent</i> | Disable terminal services agent authentication. |

Example

```
no sso-method sso-agent
```

Syntax

```
case-sensitive-names
```

Mode

User Authentication

Description

Enable treating user names as case-sensitive.

Example

```
case-sensitive-names
```

Syntax

```
no case-sensitive-names
```

Mode

User Authentication

Description

Disable treating user names as case-sensitive.

Example

```
no case-sensitive-names
```

Syntax

```
login-uniqueness
```

Mode

User Authentication

Description

Enable enforcing a single login per user name.

Example

```
login-uniqueness
```

Syntax

```
no login-uniqueness
```

Mode

User Authentication

Description

Disable enforcing a single login per user name.

Example

```
no login-uniqueness
```

Syntax

```
relogin-after-password-change
```

Mode

User Authentication

Description

Enable enforcing relogin after password change.

Example

```
relogin-after-password-change
```

Syntax

```
no relogin-after-password-change
```

Mode

User Authentication

Description

Disable enforcing relogin after password change.

Example

```
no relogin-after-password-change
```

Syntax

```
one-time-password format { characters | mixed | numbers }
```

Mode

User Authentication

Description

Set one-time password format.

Options

characters Characters format.

mixed Mixed format.

numbers Numbers format.

Example

```
one-time-password format characters
```

Syntax

```
one-time-password length { [ min <UINT8> ] [ max <UINT8> ] }
```

Mode

User Authentication

Description

Set one-time password length.

Options

min Minimum length.

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

max Maximum length.

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
one-time-password length min 8 max 12
```

Syntax

```
one-time-password email-format { html | plain-text }
```

Mode

User Authentication

Description

Set one-time password e-mail format.

Options

html Html format.

plain-text Plain-text format.

Example

```
one-time-password email-format html
```

Syntax

```
auth-page-timeout <UINT16>
```

Mode

User Authentication

Description

Set the timeout for showing the web login page.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
auth-page-timeout 2
```

Syntax

```
no auth-page-timeout
```

Mode

User Authentication

Description

Clear the timeout for showing the web login page.

Example

```
no auth-page-timeout
```

Syntax

```
browser-redirect-via { host-name | interface-ip | name-from-certificate | reverse-dns }
```

Mode

User Authentication

Description

Set the method for redirect the browser to this appliance.

Options

host-name Redirect the browser via domain name configured for firewall.

interface-ip Redirect the browser via the interface ip address.

name-from-certificate Redirect the browser via name from the administration certificate.

reverse-dns

Redirect the browser via domain name from a reverse DNS lookup of the interface IP address.

Example

```
browser-redirect-via interface-ip
```

Syntax

```
http-redirect-after-login
```

Mode

User Authentication

Description

Enable redirect from HTTPS to HTTP after login.

Example

```
http-redirect-after-login
```

Syntax

```
no http-redirect-after-login
```

Mode

User Authentication

Description

Disable redirect from HTTPS to HTTP after login.

Example

```
no http-redirect-after-login
```

Syntax

```
policy-banner [ content <ROL> ]
```

Mode

User Authentication

Description

Set the policy banner displayed to users before login.

Options

- content*** Set the content for the policy banner.
- <ROL>*** Remaining command line input.
Example: *line...*

Example

```
policy-banner
```

Syntax

```
no policy-banner [ content ]
```

Mode

User Authentication

Description

Clear the policy banner displayed to users before login.

Options

content Clear the policy banner content.

Example

```
no policy-banner
no policy-banner content
```

Syntax

```
radius-chap-http-login
```

Mode

User Authentication

Description

Enable allowing HTTP login with RADIUS CHAP mode when that is available rather than redirecting to HTTPS for web login.

Example

```
radius-chap-http-login
```

Syntax

```
no radius-chap-http-login
```

Mode

User Authentication

Description

Disable allowing HTTP login with RADIUS CHAP mode when that is available rather than redirecting to HTTPS for web login.

Example

```
no radius-chap-http-login
```

Syntax

```
inactivity-timeout <UINT16>
```

Mode

User Authentication

Description

Set the user inactivity timeout(minutes).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
inactivity-timeout 60
```

Syntax

```
prevent-inactivity-logout service { group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN>  
<SVC_PORT_END> }
```

Mode

User Authentication

Description

Set service to prevent user logout on inactivity.

Options

| | |
|-------------------------------|---|
| group | Service group. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
prevent-inactivity-logout service name FTP
```

Syntax

```
no prevent-inactivity-logout service
```

Mode

User Authentication

Description

Clear service of traffic to prevent user logout on inactivity.

Example

```
no prevent-inactivity-logout service
```

Syntax

```
log-user-name { bypass-ss0 <WORD> | originating-externally <WORD> | other-unidentified <WORD> | sso-fail <WORD> }
```

Mode

User Authentication

Description

Set user name for logging of connections on which the user is not identified.

Options

| | |
|---------------------|---|
| bypass-ss0 | For connections that bypass SSO. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

| | |
|--------------------------------------|---|
| <i>originating-externally</i> | For connections originating externally. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>other-unidentified</i> | For other unidentified connections. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>sso-fail</i> | If SSO fails to identify the user. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

Example

```
log-user-name originating-externally oriExternUser
```

Syntax

```
no log-user-name { bypass-sso | originating-externally | other-unidentified | sso-fail }
```

Mode

User Authentication

Description

Set no user name for logging of connections on which the user is not identified.

Options

| | |
|--------------------------------------|--|
| <i>bypass-sso</i> | For connections that bypass SSO. |
| <i>originating-externally</i> | Set no user name for connections originating externally. |
| <i>other-unidentified</i> | Set no user name for other unidentified |
| <i>sso-fail</i> | If SSO fails to identify the user. |

Example

```
no log-user-name originating-externally
```

Syntax

```
user-connections-logout { inactivity | reported } { authentication | other } { keep-alive | terminate [ after <UINT16> | now ] }
```

Mode

User Authentication

Description

Set activity for any remaining user connections on logout.

Options

| | |
|------------------------------|--|
| <i>inactivity</i> | Set activity for any remaining user connections on logout due to inactivity. |
| <i>reported</i> | Set activity for any remaining user connections on active/reported logout. |
| <i>authentication</i> | Set activity for authentication connections. |
| <i>other</i> | Set activity for other connections. |
| <i>keep-alive</i> | Leave the connections alive. |

| | |
|-----------------------|--|
| terminate | Terminate the connections. |
| after | Terminate the connections after specified minutes. |
| <UINT16> | Integer in the form: D OR 0xHHHH. Example: 123 |
| now | Terminate the connections now. |

Example

```
user-connections-logout inactivity authentication keep-alive
user-connections-logout inactivity other terminate
user-connections-logout inactivity other terminate after 15
```

Syntax

```
inactive-user { login | timeout }
```

Mode

User Authentication

Description

Enable make user into an inactive state.

Options

login Enable make the user initially inactive until they send traffic on being notified of a login.

timeout Enable make all users inactive instead of logging out on inactivity timeout.

Example

```
inactive-user login
```

Syntax

```
no inactive-user { login | timeout }
```

Mode

User Authentication

Description

Disable make user into an inactive state.

Options

login Disable make the user initially inactive until they send traffic on being notified of a login.

timeout Disable make all users inactive instead of logging out on inactivity timeout.

Example

```
no inactive-user login
```

Syntax

```
age-out <UINT16>
```

Mode

User Authentication

Description

Set age out inactive users time (minutes).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
age-out 60
```

Syntax

```
web-login-session-limit <UINT16>
```

Mode

User Authentication

Description

Set the maximum login session time for web users.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
web-login-session-limit 60
```

Syntax

```
no web-login-session-limit
```

Mode

User Authentication

Description

Set unlimited login session time for web users.

Example

```
no web-login-session-limit
```

Syntax

```
show-user-status-window
```

Mode

User Authentication

Description

Enable showing the login status window after web login.

Example

```
show-user-status-window
```

Syntax

```
no show-user-status-window
```

Mode

User Authentication

Description

Disable showing the login status window after web login.

Example

```
no show-user-status-window
```

Syntax

```
status-window-heartbeat { period <TEN_SEC_GRANULARITY_PERIOD> | timeout <UINT16> }
```

Mode

User Authentication

Description

Configure heartbeats sent from the user login status window.

Options

| | |
|---|---|
| period | Period in seconds. |
| <TEN_SEC_GRANULARITY_PERIOD> | A number of seconds that must be a multiple of 10. Example: 20 |
| timeout | Time in minutes. |
| <UINT16> | Integer in the form: D OR 0xHHHH. Example: 123 |

Example

```
status-window-heartbeat period 60
```

Syntax

```
disconnected-user-detect
```

Mode

User Authentication

Description

Enable using the login status window heartbeat mechanism for detecting disconnected web users.

Example

```
disconnected-user-detect
```

Syntax

```
no disconnected-user-detect
```

Mode

User Authentication

Description

Disable using the login status window heartbeat mechanism for detecting disconnected web users.

Example

```
no disconnected-user-detect
```

Syntax

```
open-in-same-window
```

Mode

User Authentication

Description

Enable open user's login status window in the same window rather than in a popup.

Example

```
open-in-same-window
```

Syntax

```
no open-in-same-window
```

Mode

User Authentication

Description

Disable open user's login status window in the same window rather than in a popup.

Example

```
no open-in-same-window
```

Syntax

```
rule-auth-bypass-http-url <WORD>
```

Mode

User Authentication

Description

Add a destination URL to be allowed to bypass user authentication in access rules.

Options

<WORD> Word in the form: WORD or "QUOTED STRING".
Example: abc

Example

```
rule-auth-bypass-http-url *.windowsupdate.com...
```

Syntax

```
no rule-auth-bypass-http-url <WORD>
```

Mode

User Authentication

Description

Delete a destination URL to be allowed to bypass user authentication in access rules.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no rule-auth-bypass-http-url *.windowsupdate.com...
```

Syntax

```
acceptable-use-policy
```

Mode

User Authentication

Description

Set the acceptable use policy (AUP) displayed to users during login.

Example

```
acceptable-use-policy
```

Syntax

```
window-size <UINT32> <UINT32>
```

Mode

Acceptable Use Policy

Description

Set the acceptable use policy (AUP) window width and height.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
window-size 460 310
```

Syntax

```
scroll-bars
```

Mode

Acceptable Use Policy

Description

Enable scroll bars on the acceptable use policy (AUP) window.

Example

```
scroll-bars
```

Syntax

no scroll-bars

Mode

Acceptable Use Policy

Description

Disable scroll bars on the acceptable use policy (AUP) window.

Example

no scroll-bars

Syntax

content <ROL>

Mode

Acceptable Use Policy

Description

Set the content for the acceptable use policy (AUP).

Options

<ROL> Remaining command line input.
Example: *line...*

Example

content "example template"

Syntax

no content

Mode

Acceptable Use Policy

Description

Clear the content for the acceptable use policy (AUP).

Example

no content

Syntax

aup-on-zones { *public* | *trusted* | *vpn* | *wan* | *wireless* }

Mode

Acceptable Use Policy

Description

Enable the acceptable use policy (AUP) on login from zones of a given type.

Options

public On login from public zones.

trusted On login from trusted zones.

vpn On login from the VPN zone.

wan On login from the WAN zone.

wireless On login from wireless zones.

Example

```
aup-on-zones trusted
```

Syntax

```
no aup-on-zones { public | trusted | vpn | wan | wireless }
```

Mode

Acceptable Use Policy

Description

Disable the acceptable use policy (AUP) on login from from zones of a given type.

Options

public On login from public zones.

trusted On login from trusted zones.

vpn On login from the VPN zone.

wan On login from the WAN zone.

wireless On login from wireless zones.

Example

```
no aup-on-zones trusted
```

Syntax

```
customize-login-page { access-barred | access-down | access-unavailable | authentication | disallowed | full | guest-status |  
lockout | logged-out | message | password-update | preempt | redirect | sso-failure | status } <ROL>
```

Mode

User Authentication

Description

Customize login pages.

Options

access-barred Customize policy access barred page.

access-down Customize policy access down page.

access-unavailable Customize policy access unavailable page.

authentication Customize login authentication page.

disallowed Customize login disallowed page.

| | |
|------------------------|--|
| full | Customize login full page. |
| guest-status | Customize guest login status page. |
| lockout | Customize login lockout page. |
| logged-out | Customize logged out page. |
| message | Customize user login message page. |
| password-update | Customize user password update page. |
| preempt | Customize admin preempt page. |
| redirect | Customize policy login redirect page. |
| sso-failure | Customize policy SSO probe failure page. |
| status | Customize login status page. |
| <ROL> | Remaining command line input. Example: <i>line...</i> |

Example

```
customize-login-page preempt "Preempt page"
```

Syntax

```
no customize-login-page { access-barred | access-down | access-unavailable | authentication | disallowed | full | guest-status | lockout | logged-out | message | password-update | preempt | redirect | sso-failure | status }
```

Mode

User Authentication

Description

Clear specified customized login page.

Options

| | |
|---------------------------|---|
| access-barred | Customize policy access barred page. |
| access-down | Customize policy access down page. |
| access-unavailable | Customize policy access unavailable page. |
| authentication | Customize login authentication page. |
| disallowed | Customize login disallowed page. |
| full | Customize login full page. |
| guest-status | Customize guest login status page. |
| lockout | Customize login lockout page. |
| logged-out | Customize logged out page. |
| message | Customize user login message page. |
| password-update | Customize user password update page. |
| preempt | Customize admin preempt page. |

| | |
|---------------------------|--|
| <i>redirect</i> | Customize policy login redirect page. |
| <i>sso-failure</i> | Customize policy SSO probe failure page. |
| <i>status</i> | Customize login status page. |

Example

```
no customize-login-page preempt
```

Syntax

```
user local
```

Mode

Config

Description

Configure settings related to local users.

Example

```
user local
```

Syntax

```
apply-password-constraints
```

Mode

Local Users

Description

Enable apply password constraints (configured in `administration_mode`) to all local users (including administrative users, but not the built-in admin account). Note that this command is an alternative to the `administration_mode` command: `constraints-apply-to full-admins limited-admins local-users`.

Example

```
apply-password-constraints
```

Syntax

```
no apply-password-constraints
```

Mode

Local Users

Description

Disable apply password constraints (configured in `administration_mode`) for local users.

Example

```
no apply-password-constraints
```

Syntax

```
prune-on-expiry
```

Mode

Local Users

Description

Enable prune expired local user accounts if a limited lifetime is set.

Example

```
prune-on-expiry
```

Syntax

```
no prune-on-expiry
```

Mode

Local Users

Description

Disable prune expired local user accounts.

Example

```
no prune-on-expiry
```

Syntax

```
user [ uuid ] <LOCAL_USER_USER_NAME> [ domain <LOCAL_USER_DOMAIN_NAME> ] [ password <ENC_PASSWORD> ] [ member-of <LOCAL_USER_MEMBER_OF_GROUP_NAME> ]
```

Mode

Local Users

Description

Add or update a local user account.

Options

| | |
|-----------------------------------|---|
| uuid | Edit a user object by UUID. |
| <LOCAL_USER_USER_NAME> | User object name. Example: <i>John</i> |
| domain | Set the user's domain. |
| <LOCAL_USER_DOMAIN_NAME> | User object domain name. Example: <i>example.com</i> |
| password | Set the user password. |
| <ENC_PASSWORD> | Password. Example: <i>secret</i> |
| member-of | Add membership to a user group for this user. |
| <LOCAL_USER_MEMBER_OF_GROUP_NAME> | User group object name. Example: <i>Limited Administrators</i> |

Example

```
user johndoe  
user johndoe domain example.com
```

Syntax

```
no user [ uuid ] <LOCAL_USER_USER_NAME> [ domain <LOCAL_USER_DOMAIN_NAME> ]
```

Mode

Local Users

Description

Delete a local user account.

Options

| | |
|---------------------------------------|---|
| uuid | Delete a user object by UUID. |
| <LOCAL_USER_USER_NAME> | User object name. Example: <i>John</i> |
| domain | Set the user's domain. |
| <LOCAL_USER_DOMAIN_NAME> | User object domain name. Example: <i>example.com</i> |

Example

```
no user johndoe
no user johndoe domain example.com
```

Syntax

```
no users
```

Mode

Local Users

Description

Delete all local user accounts.

Example

```
no users
```

Syntax

```
group [ uuid ] <LOCAL_GROUP_GROUP_NAME> [ domain <LOCAL_GROUP_DOMAIN_NAME> ]
```

Mode

Local Users

Description

Add or update a local user group.

Options

| | |
|--|---|
| uuid | Edit a user group object by UUID. |
| <LOCAL_GROUP_GROUP_NAME> | User group object name. Example: <i>Limited Administrators</i> |
| domain | Set the user group's domain. |
| <LOCAL_GROUP_DOMAIN_NAME> | User group object domain name. Example: <i>example.com</i> |

Example

```
group "Special Users"
group salesTeam domain example.com
```

Syntax

```
no group [ uuid ] <LOCAL_GROUP_GROUP_NAME> [ domain <LOCAL_GROUP_DOMAIN_NAME> ]
```

Mode

Local Users

Description

Delete a local user group.

Options

| | |
|--|---|
| uuid | Delete a user group object by UUID. |
| <LOCAL_GROUP_GROUP_NAME> | User group object name. Example: <i>Limited Administrators</i> |
| domain | Set the user group's domain. |
| <LOCAL_GROUP_DOMAIN_NAME> | User group object domain name. Example: <i>example.com</i> |

Example

```
no group "Special Users"  
no group salesTeam domain example.com
```

Syntax

```
no groups
```

Mode

Local Users

Description

Delete all local user groups.

Example

```
no groups
```

Syntax

```
name <LOCAL_USER_USER_NAME>
```

Mode

Local User

Description

Set the login name of the user account.

Options

| | |
|-------------------------------------|---|
| <LOCAL_USER_USER_NAME> | User object name. Example: <i>John</i> |
|-------------------------------------|---|

Example

```
name johndoe
```

Syntax

```
uuid <UUID>
```

Mode

Local User

Description

Set user object UUID.

Options

| | |
|---------------------|--|
| <UUID> | Universally Unique Identifier (UUID). Min: 36 |
|---------------------|--|

Max: 36
Example: 138a224d-c4c7-d621-0a00-c0eae49ce84c

Example

```
uuid f40b27d6-b8b9-a4fc-0500-c0eae49ce84c
```

Syntax

```
no uuid <UUID>
```

Mode

Local User

Description

Clear user object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: 138a224d-c4c7-d621-0a00-c0eae49ce84c

Example

```
no uuid
```

Syntax

```
domain <LOCAL_USER_DOMAIN_NAME>
```

Mode

Local User

Description

Set the user's domain, this is for domain user.

Options

<LOCAL_USER_DOMAIN_NAME> User object domain name.
Example: *example.com*

Example

```
domain example.com
```

Syntax

```
no domain
```

Mode

Local User

Description

Clear the user's domain, this is for non-domain user.

Example

```
no domain
```

Syntax

comment <WORD>

Mode

Local User

Description

Set a comment for the user account.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Added 7/26/2010"

Syntax

no comment

Mode

Local User

Description

Clear the comment for the user account.

Example

no comment

Syntax

password <ENC_PASSWORD>

Mode

Local User

Description

Set the user password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

password pwd1234

Syntax

no password

Mode

Local User

Description

Clear user password.

Syntax

force-password-change

Mode

Local User

Description

Force the user to change the password at the next login.

Example

force-password-change

Syntax

no force-password-change

Mode

Local User

Description

Disable make the user change the password at next login.

Example

no force-password-change

Syntax

expiration <DATE_YYYYMMDD> <TIME_HHMM>

Mode

Local User

Description

Set user's expiration time (absolute time).

Options

<DATE_YYYYMMDD> Date in the form: YYYY:MM:DD.
Example: 2010:06:30

<TIME_HHMM> Time in the form: DD:DD.
Example: 12:00

Example

expiration 2013:12:31 23:59

Syntax

account-lifetime <UINT16> { days | expired | hours | minutes }

Mode

Local User

Description

Set a limited lifetime for the user account.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

days Set the lifetime in days.

expired Expired user.

hours Set the lifetime in hours.

minutes Set the lifetime in minutes.

Example

```
account-lifetime 48 hours
```

Syntax

```
no account-lifetime
```

Mode

Local User

Description

Disable the user account to expire.

Example

```
no account-lifetime
```

Syntax

```
prune-on-expiry
```

Mode

Local User

Description

Delete the user account when it expires if a limited lifetime is set.

Example

```
prune-on-expiry
```

Syntax

```
no prune-on-expiry
```

Mode

Local User

Description

Disable prune account on expiration.

Example

```
no prune-on-expiry
```

Syntax

```
one-time-password { otp | totp }
```

Mode

Local User

Description

Set one-time passwords method.

Options

otp OTP via mail.

totp TOTP

Example

```
one-time-password otp  
one-time-password totp
```

Syntax

```
no one-time-password
```

Mode

Local User

Description

Disable one-time password required for the user.

Example

```
no one-time-password
```

Syntax

```
unbind-totp-key
```

Mode

Local User

Description

Unbind totp key.

Example

```
unbind-totp-key
```

Syntax

```
email-address <EMAIL>
```

Mode

Local User

Description

Set the user's e-mail address.

Options

<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: support@sonicwall.com

Example

```
email-address me@myplace.org
```

Syntax

```
no email-address
```

Mode

Local User

Description

Clear the user's e-mail address.

Example

```
no email-address
```

Syntax

```
vpn-client-access { { [ ipv4 | ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }  
| group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Local User

Description

Add a local network to which the user will be given access when connecting via VPN client.

Options

| | |
|--------------------------------------|---|
| ipv4 | IPv6 address object. |
| ipv6 | IPv6 address object. |
| host | Give VPN client access to an IP address. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Give VPN client access to a network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Give VPN client access to an IP address range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group | Select an existing address group by name. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| name | Select an existing address object by name. |
| <ADDR_NAME_MIXED> | Address object name. |

Example: *Web Server*

Example

```
vpn-client-access name "LAN Subnets"
```

Syntax

```
no vpn-client-access { group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Local User

Description

Remove a local network from those to which the user gets access when connecting via VPN client.

Options

| | |
|-------------------------|---|
| <i>group</i> | Group address object name. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| <i>name</i> | Address object name. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
no vpn-client-access name "LAN Subnets"
```

Syntax

```
guest-login-uniqueness
```

Mode

Local User

Description

Enable enforcing a unique guest services login session.

Example

```
guest-login-uniqueness
```

Syntax

```
no guest-login-uniqueness
```

Mode

Local User

Description

Disable enforcing a unique guest services login session.

Example

```
no guest-login-uniqueness
```

Syntax

```
guest-idle-timeout <UINT32> { days | hours | minutes }
```

Mode

Local User

Description

Set the idle timeout for guest services.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

days Set the idle timeout in days.

hours Set the idle timeout in hours.

minutes Set the idle timeout in minutes.

Example

```
guest-idle-timeout 20 minutes
```

Syntax

```
no guest-idle-timeout
```

Mode

Local User

Description

Clear the idle timeout for guest services.

Example

```
no guest-idle-timeout
```

Syntax

```
no quota-cycle
```

Mode

Local User

Description

Set no quota cycle for the user.

Example

```
no quota-cycle
```

Syntax

```
quota-cycle { day | month | week }
```

Mode

Local User

Description

Set a quota cycle for the user.

Options

day Set the quota cycle as one day.

month Set the quota cycle as one month.

week Set the quota cycle as one week.

Example

```
quota-cycle per day
```

Syntax

```
session-lifetime <UINT32> { days | hours | minutes }
```

Mode

Local User

Description

Set a session time limit for the user.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

days Set the session limit in days.

hours Set the session limit in hours.

minutes Set the session limit in minutes.

Example

```
session-lifetime 48 hours
```

Syntax

```
no session-lifetime
```

Mode

Local User

Description

Disable session time limit for the user.

Example

```
no session-lifetime
```

Syntax

```
limit { receive | transmit } <UINT32>
```

Mode

Local User

Description

Set the receive or transmit limit in MB for the user.

Options

receive Set the receive limit in MB for the user.

transmit Set the transmit limit in MB for the user.

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
limit receive 500
limit transmit 300
```

Syntax

```
no limit { receive | transmit }
```

Mode

Local User

Description

Disable receive or transmit limit for the user.

Options

receive Disable receive limit for the user.

transmit Disable transmit limit for the user.

Example

```
no limit receive
no limit transmit
```

Syntax

```
member-of <LOCAL_USER_MEMBER_OF_GROUP_NAME>
```

Mode

Local User

Description

Add membership to a user group for this user.

Options

<LOCAL_USER_MEMBER_OF_GROUP_NAME> User group object name.
Example: Limited Administrators

Example

```
member-of "SonicWALL Administrators"
```

Syntax

```
no member-of <LOCAL_USER_MEMBER_OF_GROUP_NAME>
```

Mode

Local User

Description

Remove a user group membership for this user.

Options

`<LOCAL_USER_MEMBER_OF_GROUP_NAME>` User group object name.
Example: *Limited Administrators*

Example

```
no member-of "SonicWALL Administrators"
```

Syntax

```
name <LOCAL_GROUP_GROUP_NAME>
```

Mode

Local Group

Description

Set the name of the user group.

Options

`<LOCAL_GROUP_GROUP_NAME>` User group object name.
Example: *Limited Administrators*

Example

```
name "Special Users"
```

Syntax

```
domain <LOCAL_GROUP_DOMAIN_NAME>
```

Mode

Local Group

Description

Set the user group's domain, this is for domain user group.

Options

`<LOCAL_GROUP_DOMAIN_NAME>` User group object domain name.
Example: *example.com*

Example

```
domain example.com
```

Syntax

```
no domain
```

Mode

Local Group

Description

Clear the user group's domain, this is for non-domain user group.

Example

no domain

Syntax

comment <WORD>

Mode

Local Group

Description

Set a comment for the user group.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Added 7/26/2010"

Syntax

no comment

Mode

Local Group

Description

Remove the comment for the user group.

Example

no comment

Syntax

ldap-location <WORD>

Mode

Local Group

Description

If memberships set by user's location in the LDAP directory is checked, this gives the location in the LDAP directory tree for that.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

ldap-location domain.com/users

Syntax

no ldap-location

Mode

Local Group

Description

Clear location in LDAP directory tree for the memberships that are set by user's location in the LDAP directory.

Example

```
no ldap-location
```

Syntax

```
memberships-by-ldap-location { at | under-or-at }
```

Mode

Local Group

Description

Enable memberships are set by user's location in the LDAP directory. For users, they can set the location at or under the given location which you can set by ldap-location command.

Options

at Set the location at the given LDAP location for users.

under-or-at Set the location under or at the given LDAP location for users.

Example

```
memberships-by-ldap-location at
memberships-by-ldap-location under-or-at
```

Syntax

```
no memberships-by-ldap-location
```

Mode

Local Group

Description

Disable memberships are set by user's location in the LDAP directory.

Example

```
no memberships-by-ldap-location
```

Syntax

```
refresh-from-ldap-server
```

Mode

Local Users

Description

Refresh from LDAP server.

Example

```
refresh-from-ldap-server
```

Syntax

```
one-time-password { otp | totp }
```

Mode

Local Group

Description

Set one-time passwords method.

Options

otp OTP via mail.

totp TOTP

Example

```
one-time-password otp  
one-time-password totp
```

Syntax

```
no one-time-password
```

Mode

Local Group

Description

Disable one-time password required for the user.

Example

```
no one-time-password
```

Syntax

```
to-management-on-login
```

Mode

Local Group

Description

Members of the group with administrative privilege will go straight to the management UI on web login (only applies for user groups that give administrative privilege).

Example

```
to-management-on-login
```

Syntax

```
no to-management-on-login
```

Mode

Local Group

Description

Disable members of the group go straight to the management UI on web login (only applies for user groups that give administrative privilege).

Example

no to-management-on-login

Syntax

```
vpn-client-access { { [ ipv4 | ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }  
| group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Local Group

Description

Add a local network to which members of the group will be given access when connecting via VPN client.

Options

| | |
|---|---|
| ipv4 | IPv6 address object. |
| ipv6 | IPv6 address object. |
| host <ADDR_HOST> | Give VPN client access to an IP address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network <ADDR_NETWORK> | Give VPN client access to a network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> | Give VPN client access to an IP address range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group <ADDR_GROUP_NAME_MIXED> | Select an existing address group by name. Group address object name. Example: <i>Sales Group</i> |
| name <ADDR_NAME_MIXED> | Select an existing address object by name. Address object name. Example: <i>Web Server</i> |

Example

```
vpn-client-access name "LAN Subnets"
```

Syntax

```
no vpn-client-access { group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Local Group

Description

Remove a local network from those to which members of the group get access when connecting via VPN client.

Options

group Group address object name.
<ADDR_GROUP_NAME_MIXED> Group address object name.
Example: *Sales Group*

name Address object name.
<ADDR_NAME_MIXED> Address object name.
Example: *Web Server*

Example

```
no vpn-client-access name "LAN Subnets"
```

Syntax

```
member <LOCAL_USER_OR_GROUP_NAME>
```

Mode

Local Group

Description

Add membership to this group for the named user or user group.

Options

<LOCAL_USER_OR_GROUP_NAME> Local user or user group object name.
Example: *Limited Administrators*

Example

```
member "All LDAP Users"
```

Syntax

```
no member <LOCAL_USER_OR_GROUP_NAME>
```

Mode

Local Group

Description

Remove a member from the group.

Options

<LOCAL_USER_OR_GROUP_NAME> Local user or user group object name.
Example: *Limited Administrators*

Example

```
no member "All LDAP Users"
```

Syntax

```
uuid <UUID>
```

Mode

Local Group

Description

Set user group object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid f40b27d6-b8b9-a4fc-0600-c0eae49ce84c
```

Syntax

```
no uuid <UUID>
```

Mode

Local Group

Description

Clear user group object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
no uuid
```

Syntax

```
bookmark <SSLVPN_BOOKMARK>
```

Mode

Local User

Description

Add/edit bookmark and enter configuration mode.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
bookmark "Admin Desktop"
```

Syntax

```
no bookmark <SSLVPN_BOOKMARK>
```

Mode

Local User

Description

Delete a specified bookmark.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no bookmark "Admin Work Desktop"
```

Syntax

```
no bookmarks
```

Mode

Local User

Description

Delete all bookmarks.

Example

```
no bookmarks
```

Syntax

```
name <SSLVPN_BOOKMARK>
```

Mode

Bookmark

Description

Set bookmark name.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
name "Admin Work Desktop"
```

Syntax

```
host <HOSTNAME_MIXED>
```

Mode

Bookmark

Description

Set host name or IP address.

Options

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

```
host 192.168.168.57
```

Syntax

```
no host
```

Mode

Bookmark

Description

Clear host name or IP address.

Example

```
no host
```

Syntax

```
service { rdp | sshv2 | telnet | vnc }
```

Mode

Bookmark

Description

Set bookmark service type.

Options

rdp Terminal services (RDP-HTML5).

sshv2 Secure shell version 2 (SSHv2).

telnet Telnet.

vnc Virtual network computing (VNC).

Example

```
service vnc
```

Syntax

```
screen-size { 1024x768 | 1280x1024 | 640x480 | 800x600 | full-screen }
```

Mode

ActiveX
RDP

Description

Set screen size.

Options

1024x768 1024x768.

1280x1024 1280x1024.

640x480 640x480.

800x600 800x600.

full-screen Full screen.

Example

```
screen-size 1024x768
```

Syntax

```
colors { 15bit | 16bit | 24bit | 256 | 32bit }
```

Mode

ActiveX
RDP

Description

Set screen colors.

Options

15bit 15 bit - high color.

16bit 16 bit - high color.

24bit 24 bit - high color.

256 256 bit.

32bit 32 bit - highest quality.

Example

```
colors 24bit
```

Syntax

```
application-path <WORD>
```

Mode

ActiveX
RDP

Description

Set application and path to launch.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
application-path "C:\\\\Remote Applications\\\\myapp.exe"
```

Syntax

```
no application-path
```

Mode

ActiveX
RDP

Description

Clear application and path.

Example

```
no application-path
```

Syntax

```
start-in-folder <WORD>
```

Mode

ActiveX
RDP

Description

Set folder to start in.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
start-in-folder "C:\\Work\\"
```

Syntax

```
no start-in-folder
```

Mode

ActiveX
RDP

Description

Clear folder to start in.

Example

```
no start-in-folder
```

Syntax

```
automatic-login { custom [ name <WORD> ] [ password <ENC_PASSWORD> ] [ domain <WORD> ] | ssl-vpn }
```

Mode

ActiveX
RDP

Description

Enable automatically log in.

Options

| | |
|-----------------|---|
| <i>custom</i> | Use custom account credentials. |
| <i>name</i> | Enter login name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>password</i> | Enter login password. |
| <ENC_PASSWORD> | Password. Example: <i>secret</i> |
| <i>domain</i> | Enter login domain. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>ssl-vpn</i> | Use SSL-VPN account credentials. |

Example

```
automatic-login custom name myuser password mypassword domain mydomain
```

Syntax

```
no automatic-login [ custom { domain | name | password } ]
```

Mode

ActiveX
RDP

Description

Disable automatically log in.

Options

custom Use custom account credentials.

domain Clear login domain.

name Clear login name.

password Clear login password.

Example

```
no automatic-login  
no automatic-login custom name  
no automatic-login custom password  
no automatic-login custom domain
```

Syntax

```
plugin-dlls <WORD>
```

Mode

ActiveX

Description

Enable plugin DLLs.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
plugin-dlls x.dll
```

Syntax

```
no plugin-dlls
```

Mode

ActiveX

Description

Disable plugin DLLs.

Example

no plugin-dlls

Syntax

redirect-clipboard

Mode

ActiveX
RDP

Description

Enable redirect clipboard.

Example

redirect-clipboard

Syntax

no redirect-clipboard

Mode

ActiveX
RDP

Description

Disable redirect clipboard.

Example

no redirect-clipboard

Syntax

redirect-audio

Mode

ActiveX
RDP

Description

Enable redirect audio.

Example

redirect-audio

Syntax

no redirect-audio

Mode

ActiveX
RDP

Description

Disable redirect audio.

Example

no redirect-audio

Syntax

auto-reconnection

Mode

ActiveX
RDP

Description

Enable automatic reconnection.

Example

auto-reconnection

Syntax

no auto-reconnection

Mode

ActiveX
RDP

Description

Disable automatic reconnections.

Example

no auto-reconnection

Syntax

desktop-background

Mode

ActiveX
RDP

Description

Enable desktop background.

Example

desktop-background

Syntax

no desktop-background

Mode

ActiveX
RDP

Description

Disable desktop background.

Example

no desktop-background

Syntax

window-drag

Mode

ActiveX
RDP

Description

Enable window drag.

Example

window-drag

Syntax

no window-drag

Mode

ActiveX
RDP

Description

Disable window drag.

Example

no window-drag

Syntax

animation

Mode

ActiveX
RDP

Description

Enable menu / window animation.

Example

animation

Syntax

no animation

Mode

ActiveX
RDP

Description

Disable menu / window animation.

Example

no animation

Syntax

view-only

Mode

VNC

Description

Enable view only.

Example

view-only

Syntax

no view-only

Mode

VNC

Description

Disable view only.

Example

no view-only

Syntax

share-desktop

Mode

VNC

Description

Enable share desktop.

Example

share-desktop

Syntax

no share-desktop

Mode

VNC

Description

Disable share desktop.

Example

no share-desktop

Syntax

automatic-accept-host-key

Mode

SSHV2

Description

Enable automatically accept host key.

Example

automatic-accept-host-key

Syntax

no automatic-accept-host-key

Mode

SSHV2

Description

Disable automatically accept host key.

Example

no automatic-accept-host-key

Syntax

display-on-mobile

Mode

RDP
SSHV2
VNC
Telnet

Description

Enable display bookmark to mobile connect clients.

Example

display-on-mobile

Syntax

no display-on-mobile

Mode

RDP
SSHV2
VNC
Telnet

Description

Disable display bookmark to mobile connect clients.

Example

no display-on-mobile

Syntax

bookmark <SSLVPN_BOOKMARK>

Mode

Local Group

Description

Add/edit bookmark and enter configuration mode.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

bookmark "Admin Desktop"

Syntax

no bookmark <SSLVPN_BOOKMARK>

Mode

Local Group

Description

Delete a specified bookmark.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no bookmark "Admin Work Desktop"

Syntax

no bookmarks

Mode

Local Group

Description

Delete all bookmarks.

Example

no bookmarks

Syntax

name <SSLVPN_BOOKMARK>

Mode

Bookmark

Description

Set bookmark name.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or "QUOTED STRING".
Example: *abc*

Example

```
name "Admin Work Desktop"
```

Syntax

```
host <HOSTNAME_MIXED>
```

Mode

Bookmark

Description

Set host name or IP address.

Options

<HOSTNAME_MIXED> IPV4: hostname in the form: D.D.D.D or hostname\nIPV6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

```
host 192.168.168.57
```

Syntax

```
no host
```

Mode

Bookmark

Description

Clear host name or IP address.

Example

```
no host
```

Syntax

```
service { rdp | sshv2 | telnet | vnc }
```

Mode

Bookmark

Description

Set bookmark service type.

Options

rdp Terminal services (RDP-HTML5).

sshv2 Secure shell version 2 (SSHv2).

telnet Telnet.

vnc Virtual network computing (VNC).

Example

```
service vnc
```

Syntax

```
screen-size { 1024x768 | 1280x1024 | 640x480 | 800x600 | full-screen }
```

Mode

ActiveX
RDP

Description

Set screen size.

Options

1024x768 1024x768.

1280x1024 1280x1024.

640x480 640x480.

800x600 800x600.

full-screen Full screen.

Example

```
screen-size 1024x768
```

Syntax

```
colors { 15bit | 16bit | 24bit | 256 | 32bit }
```

Mode

ActiveX
RDP

Description

Set screen colors.

Options

15bit 15 bit - high color.

16bit 16 bit - high color.

24bit 24 bit - high color.

256 256 bit.

32bit 32 bit - highest quality.

Example

Syntax

application-path <WORD>

Mode

ActiveX
RDP

Description

Set application and path to launch.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

application-path "C:\\\\Remote Applications\\\\myapp.exe"

Syntax

no application-path

Mode

ActiveX
RDP

Description

Clear application and path.

Example

no application-path

Syntax

start-in-folder <WORD>

Mode

ActiveX
RDP

Description

Set folder to start in.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

start-in-folder "C:\\Work\\"

Syntax

no start-in-folder

Mode

ActiveX
RDP

Description

Clear folder to start in.

Example

```
no start-in-folder
```

Syntax

```
automatic-login { custom [ name <WORD> ] [ password <ENC_PASSWORD> ] [ domain <WORD> ] | ssl-vpn }
```

Mode

ActiveX
RDP

Description

Enable automatically log in.

Options

| | |
|-----------------------------|---|
| custom | Use custom account credentials. |
| name | Enter login name. |
| <WORD> | Word in the form: WORD or "QUOTED STRING". Example: <i>abc</i> |
| password | Enter login password. |
| <ENC_PASSWORD> | Password. Example: <i>secret</i> |
| domain | Enter login domain. |
| <WORD> | Word in the form: WORD or "QUOTED STRING". Example: <i>abc</i> |
| ssl-vpn | Use SSL-VPN account credentials. |

Example

```
automatic-login custom name myuser password mypassword domain mydomain
```

Syntax

```
no automatic-login [ custom { domain | name | password } ]
```

Mode

ActiveX
RDP

Description

Disable automatically log in.

Options

| | |
|-----------------|---------------------------------|
| custom | Use custom account credentials. |
| domain | Clear login domain. |
| name | Clear login name. |
| password | Clear login password. |

Example


```
no automatic-login
no automatic-login custom name
no automatic-login custom password
no automatic-login custom domain
```

Syntax

```
plugin-dlls <WORD>
```

Mode

ActiveX

Description

Enable plugin DLLs.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
plugin-dlls x.dll
```

Syntax

```
no plugin-dlls
```

Mode

ActiveX

Description

Disable plugin DLLs.

Example

```
no plugin-dlls
```

Syntax

```
redirect-clipboard
```

Mode

ActiveX
RDP

Description

Enable redirect clipboard.

Example

```
redirect-clipboard
```

Syntax

```
no redirect-clipboard
```

Mode

ActiveX
RDP

Description

Disable redirect clipboard.

Example

```
no redirect-clipboard
```

Syntax

```
redirect-audio
```

Mode

ActiveX
RDP

Description

Enable redirect audio.

Example

```
redirect-audio
```

Syntax

```
no redirect-audio
```

Mode

ActiveX
RDP

Description

Disable redirect audio.

Example

```
no redirect-audio
```

Syntax

```
auto-reconnection
```

Mode

ActiveX
RDP

Description

Enable automatic reconnection.

Example

```
auto-reconnection
```

Syntax

```
no auto-reconnection
```

Mode

ActiveX
RDP

Description

Disable automatic reconnections.

Example

```
no auto-reconnection
```

Syntax

```
desktop-background
```

Mode

ActiveX
RDP

Description

Enable desktop background.

Example

```
desktop-background
```

Syntax

```
no desktop-background
```

Mode

ActiveX
RDP

Description

Disable desktop background.

Example

```
no desktop-background
```

Syntax

```
window-drag
```

Mode

ActiveX
RDP

Description

Enable window drag.

Example

```
window-drag
```

Syntax

```
no window-drag
```

Mode

ActiveX
RDP

Description

Disable window drag.

Example

```
no window-drag
```

Syntax

```
animation
```

Mode

ActiveX
RDP

Description

Enable menu / window animation.

Example

```
animation
```

Syntax

```
no animation
```

Mode

ActiveX
RDP

Description

Disable menu / window animation.

Example

```
no animation
```

Syntax

```
view-only
```

Mode

VNC

Description

Enable view only.

Example

```
view-only
```

Syntax

```
no view-only
```

Mode

VNC

Description

Disable view only.

Example

no view-only

Syntax

share-desktop

Mode

VNC

Description

Enable share desktop.

Example

share-desktop

Syntax

no share-desktop

Mode

VNC

Description

Disable share desktop.

Example

no share-desktop

Syntax

automatic-accept-host-key

Mode

SSHV2

Description

Enable automatically accept host key.

Example

automatic-accept-host-key

Syntax

no automatic-accept-host-key

Mode

SSHV2

Description

Disable automatically accept host key.

Example

```
no automatic-accept-host-key
```

Syntax

```
display-on-mobile
```

Mode

RDP
SSHV2
VNC
Telnet

Description

Enable display bookmark to mobile connect clients.

Example

```
display-on-mobile
```

Syntax

```
no display-on-mobile
```

Mode

RDP
SSHV2
VNC
Telnet

Description

Disable display bookmark to mobile connect clients.

Example

```
no display-on-mobile
```

Syntax

```
kill-user name <USER_LOGIN_NAME>
```

Mode

Top Level
User Management

Description

Log out users.

Options

<USER_LOGIN_NAME> A connected user's login name.
Example: *jdoe*

Example

```
kill-user name guest1
```

Syntax

```
kill-user at <USER_IPV4_ADDR> [ user <UINT32> ]
```

Mode

Top Level
User Management

Description

Log out users.

Options

<USER_IPV4_ADDR> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

user For Terminal Services users only, selects the user at the IP address.

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
kill-user at 192.168.168.1
```

Syntax

```
unlock <USER_IPV4_ADDR>
```

Mode

Top Level
User Management

Description

Unlock an IP address that has been locked out due to too many failed login attempts.

Options

<USER_IPV4_ADDR> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
unlock 192.168.168.1
```

Syntax

```
user management
```

Mode

Config

Description

User management.

Example

```
user management
```

Syntax

```
include { inactive-users | unauthenticated-users }
```

Mode

User Management

Description

Enable show inactive or unauthenticated users' status.

Options

inactive-users Enable show inactive users' status.

unauthenticated-users Enable show unauthenticated users' status.

Example

```
include inactive-users
include unauthenticated-users
```

Syntax

```
no include { inactive-users | unauthenticated-users }
```

Mode

User Management

Description

Disable show inactive or unauthenticated users' status.

Options

inactive-users Disable show inactive users' status.

unauthenticated-users Disable show unauthenticated users' status.

Example

```
no include inactive-users
no include unauthenticated-users
```

Syntax

```
user radius
```

Mode

Config

Description

Configure RADIUS settings.

Example

```
user radius
```

Syntax

```
clear user radius statistics [ server <RADIUS_SERVER_HOST_NAME> ]
```

Mode

RADIUS

Description

Reset RADIUS statistics.

Options

server Reset a specific RADIUS server statistics.
<RADIUS_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *10.10.10.10\www.radiusServer.com*

Example

```
clear user radius statistics  
clear user radius statistics server 10.10.10.10
```

Syntax

```
local-users-only
```

Mode

RADIUS

Description

Limit login to only RADIUS users with accounts in the local user database.

Example

```
local-users-only
```

Syntax

```
no local-users-only
```

Mode

RADIUS

Description

Don't limit login to only RADIUS users with accounts in the local user database.

Example

```
no local-users-only
```

Syntax

```
default-user-group <LOCAL_USER_GROUP_NAME>
```

Mode

RADIUS

Description

Select a user group to whom all users who are authenticated via RADIUS will be given membership by default (i.e. a group that can be used to set accesses etc. that will apply to all RADIUS users).

Options

<LOCAL_USER_GROUP_NAME> Local user group object name.
Example: *Limited Administrators*

Example

```
default-user-group "Radius Users"
```

Syntax

no default-user-group

Mode

RADIUS

Description

RADIUS will not be given membership to any user group by default.

Example

no default-user-group

Syntax

timeout <UINT32>

Mode

RADIUS

Description

Set the timeout for the RADIUS servers.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

timeout 10

Syntax

retries <UINT32>

Mode

RADIUS

Description

Set the number of retries for the RADIUS servers.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

retries 10

Syntax

user-group-mechanism { *ldap* | *local-only* | *radius-attribute* { *filter-id* | *vendor-specific* } }

Mode

RADIUS

Description

Set the mechanism to use to set user group memberships for users who are authenticated via RADIUS.

Options

| | |
|-------------------------|---|
| ldap | Read user groups via LDAP. |
| local-only | Set using local users that duplicate RADIUS users. |
| radius-attribute | Read user groups via a RADIUS attribute. |
| filter-id | Use the standard RADIUS filter-id attribute. |
| vendor-specific | Use the SonicWall vendor-specific RADIUS attribute. |

Example

```
user-group-mechanism radius-attribute filter-id
```

Syntax

```
server <RADIUS_SERVER_HOST_NAME>
```

Mode

RADIUS

Description

Configure a RADIUS server.

Options

<RADIUS_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
 Example: 10.10.10.10\nwww.radiusServer.com

Example

```
server 192.168.168.16
```

Syntax

```
no server <RADIUS_SERVER_HOST_NAME>
```

Mode

RADIUS

Description

Delete a RADIUS server.

Options

<RADIUS_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
 Example: 10.10.10.10\nwww.radiusServer.com

Example

```
no server 192.168.168.16
```

Syntax

```
no servers
```

Mode

RADIUS

Description

Delete all RADIUS servers.

Example

```
no servers
```

Syntax

```
enable
```

Mode

RADIUS Server

Description

Enable the RADIUS server.

Example

```
enable
```

Syntax

```
no enable
```

Mode

RADIUS Server

Description

Disable the RADIUS server.

Example

```
no enable
```

Syntax

```
host <RADIUS_SERVER_HOST_NAME>
```

Mode

RADIUS Server

Description

Set the RADIUS server's host name or IP address.

Options

<RADIUS_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: `10.10.10.10\www.radiusServer.com`

Example

```
host 192.168.168.1
```

Syntax

```
port <IPV4_PORT>
```

Mode

RADIUS Server

Description

Set the RADIUS server's UDP port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
port 1812
```

Syntax

```
partition <PARTITION_NAME>
```

Mode

RADIUS Server

Description

Set the RADIUS server's user partition.

Options

<PARTITION_NAME> User authentication partition name.
Example: CorpSales

Example

```
partition corpsales
```

Syntax

```
no partition
```

Mode

RADIUS Server

Description

Clear the RADIUS server's user partition.

Example

```
no partition
```

Syntax

```
shared-secret <ENC_PASSWORD>
```

Mode

RADIUS Server

Description

Set the RADIUS server's shared secret.

Options

<ENC_PASSWORD> Password.
Example: secret

Example

shared-secret mysecret

Syntax

no shared-secret

Mode

RADIUS Server

Description

Clear the RADIUS server's shared secret.

Example

no shared-secret

Syntax

send-through-vpn-tunnel

Mode

RADIUS Server

Description

Enable enforce send packet through vpn tunnel.

Example

send-through-vpn-tunnel

Syntax

no send-through-vpn-tunnel

Mode

RADIUS Server

Description

Disable enforce send packet through vpn tunnel.

Example

no send-through-vpn-tunnel

Syntax

user-name-format { any | down-level-logon | name-dot-domain | user-name | user-principle }

Mode

RADIUS Server

Description

Set user name attribute format.

Options

any Set to any format.

down-level-logon Set to \"Domain\\User-name\" format.

name-dot-domain Set to \"User-name.Domain\" format.

user-name Set to \"User-name\" format.

user-principle Set to \"User-name@Domain\" format.

Example

```
user-name-format simple-name
```

Syntax

```
test <RADIUS_SERVER_HOST_NAME> [ user <WORD> <WORD> [ { chap | mschap | mschapv2 } ] ]
```

Mode

RADIUS

Description

Run the RADIUS test using specified server.

Options

| | |
|--|--|
| <RADIUS_SERVER_HOST_NAME> | Hostname in the form: hostname OR a.b.c.d. Example: 10.10.10.10\nwww.radiusServer.com |
| user | Run the RADIUS user test with the given user name/password. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: abc |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: abc |
| chap | Run the test with RADIUS in CHAP mode. |
| mschap | Run the test with RADIUS in MSCHAP mode. |
| mschapv2 | Run the test with RADIUS in MSCHAPv2 mode. |

Example

```
test 192.168.168.16  
test 192.168.168.16 user user1 pwd1234
```

Syntax

```
accounting
```

Mode

RADIUS

Description

Configure RADIUS accounting settings.

Example

```
accounting
```

Syntax

```
server <RADIUS_ACCOUNTING_HOST_NAME>
```

Mode

RADIUS Accounting

Description

Configure a RADIUS accounting server.

Options

<RADIUS_ACCOUNTING_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *10.10.10.10\www.radiusServer.com*

Example

```
server 192.168.168.16
```

Syntax

```
no server <RADIUS_ACCOUNTING_HOST_NAME>
```

Mode

RADIUS Accounting

Description

Delete a RADIUS accounting server.

Options

<RADIUS_ACCOUNTING_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *10.10.10.10\www.radiusServer.com*

Example

```
no server 192.168.168.16
```

Syntax

```
no servers
```

Mode

RADIUS Accounting

Description

Delete all RADIUS accounting servers.

Example

```
no servers
```

Syntax

```
enable
```

Mode

RADIUS Accounting Server

Description

Enable the RADIUS accounting server.

Example

```
enable
```

Syntax

no enable

Mode

RADIUS Accounting Server

Description

Disable the RADIUS accounting server.

Example

no enable

Syntax

host <RADIUS_ACCOUNTING_HOST_NAME>

Mode

RADIUS Accounting Server

Description

Set the RADIUS accounting server's host name or IP address.

Options

<RADIUS_ACCOUNTING_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: 10.10.10.10\www.radiusServer.com

Example

host 192.168.168.1

Syntax

port <IPV4_PORT>

Mode

RADIUS Accounting Server

Description

Set the RADIUS accounting server's UDP port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

port 1812

Syntax

partition <PARTITION_NAME>

Mode

RADIUS Accounting Server

Description

Set the RADIUS accounting server's user partition.

Options

<PARTITION_NAME> User authentication partition name.
Example: *CorpSales*

Example

```
partition corpsales
```

Syntax

```
no partition
```

Mode

RADIUS Accounting Server

Description

Clear the RADIUS accounting server's user partition.

Example

```
no partition
```

Syntax

```
shared-secret <ENC_PASSWORD>
```

Mode

RADIUS Accounting Server

Description

Set the RADIUS accounting server's shared secret.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
shared-secret mysecret
```

Syntax

```
no shared-secret
```

Mode

RADIUS Accounting Server

Description

Clear the RADIUS accounting server's shared secret.

Example

```
no shared-secret
```

Syntax

```
user-name-format { down-level-logon | name-dot-domain | user-name | user-principle }
```

Mode

RADIUS Accounting Server

Description

Set user name attribute format.

Options

down-level-logon Set to \"Domain\\User-name\" format.

name-dot-domain Set to \"User-name.Domain\" format.

user-name Set to \"User-name\" format.

user-principle Set to \"User-name@Domain\" format.

Example

```
user-name-format user-name
```

Syntax

```
test <RADIUS_ACCOUNTING_HOST_NAME> [ user <WORD> <IPV4_HOST> ]
```

Mode

RADIUS Accounting

Description

Run the RADIUS accounting server test using specified server.

Options

<RADIUS_ACCOUNTING_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: 10.10.10.10\nwww.radiusServer.com

user Run the RADIUS user test with the given user name/ip address.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
test 192.168.168.16  
test 192.168.168.16 user user1 192.168.168.1
```

Syntax

```
timeout <UINT32>
```

Mode

RADIUS Accounting

Description

Set the timeout for the RADIUS accounting servers.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
timeout 10
```

Syntax

```
retries <UINT32>
```

Mode

RADIUS Accounting

Description

Set the number of retries for the RADIUS accounting servers.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
retries 10
```

Syntax

```
data { all-servers | guest-users | remote-client-users | sso-authenticated-users | users-authenticated-by-web-login }
```

Mode

RADIUS Accounting

Description

Enable sending accounting data to servers or for users.

Options

| | |
|--|--|
| <i>all-servers</i> | Enable sending accounting data to all servers. |
| <i>guest-users</i> | Enable sending accounting data for guest users. |
| <i>remote-client-users</i> | Enable sending accounting data for remote client users. |
| <i>sso-authenticated-users</i> | Enable sending accounting data for SSO-authenticated users. |
| <i>users-authenticated-by-web-login</i> | Enable sending accounting data for users authenticated by web login. |

Example

```
data all-servers
data users-authenticated-by-web-login
data remote-client-users
data guest-users
data sso-authenticated-users
```

Syntax

```
no data { all-servers | guest-users | remote-client-users | sso-authenticated-users | users-authenticated-by-web-login }
```

Mode

RADIUS Accounting

Description

Disable sending accounting data to servers or for users.

Options

| | |
|--|---|
| <i>all-servers</i> | Disable sending accounting data to all servers. |
| <i>guest-users</i> | Disable sending accounting data for guest users. |
| <i>remote-client-users</i> | Disable sending accounting data for remote client users. |
| <i>sso-authenticated-users</i> | Disable sending accounting data for SSO-authenticated users. |
| <i>users-authenticated-by-web-login</i> | Disable sending accounting data for users authenticated by web login. |

Example

```
no data all-servers
no data users-authenticated-by-web-login
no data remote-client-users
no data guest-users
no data sso-authenticated-users
```

Syntax

```
include { domain-and-local-users | domain-users | local-users | sso-users-identified-via-RADIUS-accounting }
```

Mode

RADIUS Accounting

Description

Include different users in user accounting.

Options

| | |
|--|--|
| <i>domain-and-local-users</i> | Include local and domain users in user accounting. |
| <i>domain-users</i> | Include domain users in user accounting. |
| <i>local-users</i> | Include local users in user accounting. |
| <i>sso-users-identified-via-RADIUS-accounting</i> | Include SSO users identified via RADIUS accounting in user accounting. |

Example

```
include domain-users
include local-users
include domain-and-local-users
```

Syntax

```
no include sso-users-identified-via-RADIUS-accounting
```

Mode

RADIUS Accounting

Description

Do not include users in user accounting.

Options

| | |
|--|---|
| <i>sso-users-identified-via-RADIUS-accounting</i> | Do not include SSO users identified via RADIUS accounting in user accounting. |
|--|---|

Example

no include sso-users-identified-via-RADIUS-accounting

Syntax

interim-updates <UINT8>

Mode

RADIUS Accounting

Description

Set the send interim updates for user accounting.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

interim-updates 15

Syntax

no interim-updates

Mode

RADIUS Accounting

Description

Disable the send interim updates for user accounting.

Example

no interim-updates

Syntax

user ldap

Mode

Config

Description

Configure LDAP settings.

Example

user ldap

Syntax

clear user ldap statistics [global | server <LDAP_SERVER_HOST_NAME>]

Mode

LDAP

Description

Reset LDAP statistics.

Options

| | |
|--------------------------------------|---|
| global | Reset LDAP global statistics. |
| server | Reset a specific LDAP server statistics. |
| <LDAP_SERVER_HOST_NAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>LDAP-Server</i> |

Example

```
clear user ldap statistics
clear user ldap statistics global
clear user ldap statistics server 10.10.10.10
```

Syntax

```
protocol-version <UINT8>
```

Mode

LDAP

Description

Set protocol version of LDAP server.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
protocol-version 3
```

Syntax

```
require-valid-certificate
```

Mode

LDAP

Description

Enable validate the certificate presented by the server during the TLS exchange.

Example

```
require-valid-certificate
```

Syntax

```
no require-valid-certificate
```

Mode

LDAP

Description

Disable validate the certificate presented by the server during the TLS exchange.

Example

```
no require-valid-certificate
```

Syntax

`local-tls-certificate <CERT_NAME>`

Mode

LDAP

Description

Select a local certificate to use with LDAP if using TLS. This is not normally required but may be if the LDAP server is configured to require a valid certificate from the client (e.g. on a server that allows reading back passwords from user objects when bound as an administrator).

Options

`<CERT_NAME>` Certificate name.
Example: `my_cert`

Example

`local-tls-certificate my_ldap_server`

Syntax

`no local-tls-certificate`

Mode

LDAP

Description

Clear local certificate for TLS.

Example

`no local-tls-certificate`

Syntax

`allow-referrals`

Mode

LDAP

Description

Allow following referrals to other LDAP servers.

Example

`allow-referrals`

Syntax

`no allow-referrals`

Mode

LDAP

Description

Ignore referrals to other LDAP servers.

Example

no allow-referrals

Syntax

```
allow-references { auto-configuration | domain-search | other-search | user-authentication }
```

Mode

LDAP

Description

Allow following continuation references to look for more results on other LDAP servers.

Options

- auto-configuration*** Follow continuation references during auto-configuration.
- domain-search*** Follow continuation references when searching for domains.
- other-search*** Follow continuation references in other searches.
- user-authentication*** Follow continuation references during user authentication.

Example

```
allow-references user-authentication  
allow-references auto-configuration  
allow-references domain-search  
allow-references other-search
```

Syntax

```
no allow-references { auto-configuration | domain-search | other-search | user-authentication }
```

Mode

LDAP

Description

Disable follow continuation references to look for more results on other LDAP servers when doing particular operations.

Options

- auto-configuration*** Disable follow references during auto-configuration.
- domain-search*** Disable follow references when searching for domains.
- other-search*** Disable follow references in other searches.
- user-authentication*** Disable follow references during user authentication.

Example

```
no allow-references auto-configuration  
no allow-references user-authentication  
no allow-references domain-search
```

Syntax

```
local-users-only
```

Mode

LDAP

Description

Limit login to only LDAP users with accounts in the local user database.

Example

```
local-users-only
```

Syntax

```
no local-users-only
```

Mode

LDAP

Description

Don't limit login to only LDAP users with accounts in the local user database.

Example

```
no local-users-only
```

Syntax

```
default-user-group <LOCAL_USER_GROUP_NAME>
```

Mode

LDAP

Description

Select a user group to whom all users who are authenticated via LDAP will be given membership by default (i.e. a group that can be used to set accesses etc. that will apply to all LDAP users).

Options

<LOCAL_USER_GROUP_NAME> Local user group object name.
Example: *Limited Administrators*

Example

```
default-user-group "LDAP Users"
```

Syntax

```
no default-user-group
```

Mode

LDAP

Description

LDAP will not be given membership to any user group by default.

Example

```
no default-user-group
```

Syntax

```
mirror-user-groups [ all | have-members | refresh { now | period <UINT32> } ]
```

Mode

LDAP

Description

Enable/config mirror LDAP user groups locally.

Options

| | |
|------------------------------|--|
| <i>all</i> | Mirror all user groups on the LDAP server. |
| <i>have-members</i> | Only mirror groups that have member users or groups. |
| <i>refresh</i> | Refresh mirrored LDAP user groups. |
| <i>now</i> | Refresh now. |
| <i>period</i> | Set refresh period. |
| <i><UINT32></i> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |

Example

```
mirror-user-groups
mirror-user-groups all
mirror-user-groups have-members
mirror-user-groups refresh period 5
mirror-user-groups refresh now
```

Syntax

```
no mirror-user-groups
```

Mode

LDAP

Description

Disable mirror LDAP user groups locally.

Example

```
no mirror-user-groups
```

Syntax

```
exclude-tree <LDAP_EXCLUDE_TREE>
```

Mode

LDAP

Description

Enable exclude user groups in the specified sub-tree from the mirroring.

Options

| | |
|---|------------------------------------|
| <i><LDAP_EXCLUDE_TREE></i> | LDAP exclude tree. Example: abc |
|---|------------------------------------|

Example

```
exclude-tree mydomain.com/groups
```

Syntax

no exclude-tree <LDAP_EXCLUDE_TREE>

Mode

LDAP

Description

Disable exclude user groups in the specified sub-tree from the mirroring.

Options

<LDAP_EXCLUDE_TREE> LDAP exclude tree.
Example: *abc*

Example

no exclude-tree mydomain.com/groups

Syntax

relay

Mode

LDAP

Description

Configure the RADIUS to LDAP relay.

Example

relay

Syntax

enable

Mode

LDAP Relay

Description

Enable RADIUS to LDAP Relay.

Example

enable

Syntax

no enable

Mode

LDAP Relay

Description

Disable RADIUS to LDAP Relay.

Example

no enable

Syntax

```
clients-connect { public-zones | trusted-zones | vpn-zone | wan-zone | wireless-zones }
```

Mode

LDAP Relay

Description

Enable specified zone to allow incoming RADIUS requests.

Options

- public-zones** Allow incoming RADIUS requests from public zones.
- trusted-zones** Allow incoming RADIUS requests from trusted zones.
- vpn-zone** Allow incoming RADIUS requests from vpn zone.
- wan-zone** Allow incoming RADIUS requests from wan zone.
- wireless-zones** Allow incoming RADIUS requests from wireless zones.

Example

```
clients-connect-via wan-zone  
clients-connect-via trusted-zones  
clients-connect-via public-zones
```

Syntax

```
no clients-connect { public-zones | trusted-zones | vpn-zone | wan-zone | wireless-zones }
```

Mode

LDAP Relay

Description

Disable specified zone to discard incoming RADIUS requests.

Options

- public-zones** Discard incoming RADIUS requests from public zones.
- trusted-zones** Discard incoming RADIUS requests from trusted zones.
- vpn-zone** Discard incoming RADIUS requests from vpn zone.
- wan-zone** Discard incoming RADIUS requests from wan zone.
- wireless-zones** Discard incoming RADIUS requests from wireless zones.

Example

```
no clients-connect-via wan-zone  
no clients-connect-via trusted-zones  
no clients-connect-via public-zones
```

Syntax

```
shared-secret <ENC_PASSWORD>
```

Mode

LDAP Relay

Description

Set RADIUS shared secret.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
shared-secret 123abc
```

Syntax

```
no shared-secret
```

Mode

LDAP Relay

Description

Clear RADIUS shared secret.

Example

```
no shared-secret
```

Syntax

```
legacy-user-group { internet <WORD> | l2tp <WORD> | vpn <WORD> | vpn-client <WORD> }
```

Mode

LDAP Relay

Description

Set the user group that corresponds to the legacy access privileges. These settings allow inter-operation with remote SonicWALL running non-enhanced firmware that do not support user groups. When a user in one of the given user groups is authenticated, the remote SonicWALL will be informed that the user is to be given the relevant privilege.

Options

internet Set the user group for users with Internet access.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

l2tp Set the user group for L2TP users.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

vpn Set the user group for VPN users.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

vpn-client Set the user group for VPN client users.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
legacy-user-group vpn "WAN GroupVPN"  
legacy-user-group vpn-client "VPN Services"  
legacy-user-group l2tp "My l2tp group"  
legacy-user-group internet "My internet"
```

Syntax

```
no legacy-user-group { internet | l2tp | vpn | vpn-client }
```

Mode

LDAP Relay

Description

Clear the user group that corresponds to the legacy access privileges.

Options

internet Clear the user group for users with Internet access.

l2tp Clear the user group for L2TP users.

vpn Clear the user group for VPN users.

vpn-client Clear the user group for VPN client users.

Example

```
no legacy-user-group vpn
no legacy-user-group vpn-client
no legacy-user-group l2tp
no legacy-user-group internet
```

Syntax

```
server <LDAP_SERVER_HOST_NAME>
```

Mode

LDAP

Description

Add/edit an LDAP server.

Options

<LDAP_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *LDAP-Server*

Example

```
server 192.168.168.1
```

Syntax

```
no server <LDAP_SERVER_HOST_NAME>
```

Mode

LDAP

Description

Delete an LDAP server.

Options

<LDAP_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *LDAP-Server*

Example

```
no server 192.168.168.1
```

Syntax

```
no servers
```

Mode

LDAP

Description

Delete all LDAP servers.

Example

```
no servers
```

Syntax

```
save dynamic-secondary <LDAP_DYNAMIC_SERVER_NAME>
```

Mode

LDAP

Description

Make dynamically learned secondary servers configuration permanent.

Options

<LDAP_DYNAMIC_SERVER_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *LDAP-Dynamic-Server*

Example

```
save dynamic-secondary 192.168.168.16
```

Syntax

```
enable
```

Mode

LDAP Server

Description

Enable the LDAP server.

Example

```
enable
```

Syntax

```
no enable
```

Mode

LDAP Server

Description

Disable the LDAP server.

Example

```
no enable
```

Syntax

```
host <LDAP_SERVER_HOST_NAME>
```

Mode

LDAP Server

Description

Set the LDAP server's host name or IP address.

Options

<LDAP_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *LDAP-Server*

Example

```
host 192.168.168.1
```

Syntax

```
role { backup | primary | secondary }
```

Mode

LDAP Server

Description

Set the LDAP server's role.

Options

backup Backup/replica LDAP server.

primary Primary LDAP server.

secondary Secondary LDAP server.

Example

```
role primary  
role secondary  
role backup
```

Syntax

```
port <IPV4_PORT>
```

Mode

LDAP Server

Description

Set the LDAP server's UDP port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHHH.
Example: 80

Example

```
port 389
```

Syntax

```
partition <PARTITION_NAME>
```

Mode

LDAP Server

Description

Set the LDAP server's user partition.

Options

<PARTITION_NAME> User authentication partition name.
Example: CorpSales

Example

```
partition corpsales
```

Syntax

```
timeout { operation <UINT32> | server <UINT32> }
```

Mode

LDAP Server

Description

Set the timeout for LDAP server.
 The server timeout is the maximum time to wait for each response from the LDAP server over the network. The overall operation timeout is the maximum time to spend on an LDAP operation (including auto-configuration operations that can involve large numbers of requests sent to multiple LDAP servers).

Options

operation Set the overall timeout on an LDAP operation.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

server Set the server timeout which is the maximum time to wait for each response from the LDAP server over the network.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
timeout operation 5  
timeout server 10
```

Syntax

```
use-tls
```

Mode

LDAP Server

Description

Enable use transport layer security (TLS) when log in to the LDAP server.

Example

```
use-tls
```

Syntax

```
no use-tls
```

Mode

LDAP Server

Description

Disable use transport layer security (TLS) when log in to the LDAP server.

Example

```
no use-tls
```

Syntax

```
send-start-tls-request
```

Mode

LDAP Server

Description

Enable send LDAP 'Start TLS' request. This is an LDAP feature that allows an LDAP server to operate in both TLS and non-TLS modes on the same TCP port. You only need check this if your LDAP server uses the same port number for both TLS and non-TLS.

Example

```
send-start-tls-request
```

Syntax

```
no send-start-tls-request
```

Mode

LDAP Server

Description

Disable send LDAP 'Start TLS' request.

Example

```
no send-start-tls-request
```

Syntax

```
backup-for <LDAP_SERVER_HOST_NAME>
```

Mode

LDAP Server

Description

Set the LDAP server for which this is the backup for.

Options

<LDAP_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *LDAP-Server*

Example

backup-for 192.168.168.15

Syntax

no backup-for

Mode

LDAP Server

Description

Clear the backup LDAP server.

Example

no backup-for

Syntax

same-bind-credentials

Mode

LDAP Server

Description

Enable using same bind credentials as the server that this is the backup for.

Example

same-bind-credentials

Syntax

no same-bind-credentials

Mode

LDAP Server

Description

Disable using same bind credentials as the server that this is the backup for.

Example

no same-bind-credentials

Syntax

schema { custom | inet-org-person | microsoft-active-directory | network-information-service | novell-edirectory | samba-smb }

Mode

LDAP Server

Description

Configure the LDAP schema.

Options

| | |
|------------------------------------|---|
| custom | Configure the schema manually. |
| inet-org-person | Use the pre-configured RFC-2798 InetOrgPerson schema. |
| microsoft-active-directory | Use the pre-configured Microsoft Active Directory schema. |
| network-information-service | Use the pre-configured RFC-2307 Network Information Service schema. |
| novell-edirectory | Use the pre-configured Novell eDirectory schema. |
| samba-smb | Use the pre-configured Samba SMB schema. |

Example

```
schema samba-smb
schema microsoft-active-directory
schema novell-edirectory
```

Syntax

```
read-from-server auto-configure [ servers ]
```

Mode

LDAP Schema

Description

Read the schema from the LDAP server and auto-configure the local schema to match.

Options

servers Automatically update the schema configuration on all servers.

Example

```
read-from-server auto-configure
read-from-server auto-configure servers
```

Syntax

```
read-from-server display
```

Mode

LDAP Schema

Description

Read the schema from the LDAP server and display it.

Example

```
read-from-server display
```

Syntax

```
user-class <WORD>
```

Mode

LDAP Schema

Description

Set the class name of user objects.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-class user
```

Syntax

```
user-attribute { additional-group-id <WORD> | framed-ip-address <WORD> | group-membership <WORD> | logon-name <WORD> | qualified-logon-name <WORD> | use-additional-group-id }
```

Mode

LDAP Schema

Description

Define attributes of user objects.

Options

additional-group-id Set the additional user group ID attribute.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

framed-ip-address Set the framed IP address attribute.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

group-membership Set the user group membership attribute.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

logon-name Set the user logon name attribute.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

qualified-logon-name Set the qualified logon name attribute.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

use-additional-group-id Use the additional user group ID attribute.

Example

```
user-attribute logon-name myuid  
user-attribute qualified-logon-name myUserPrincipalName  
user-attribute group-membership myMemberOf  
user-attribute additional-group-id myPrimaryGroupID  
user-attribute use-additional-group-id  
user-attribute framed-ip-address myFramedIPAddress
```

Syntax

```
no user-attribute { additional-group-id | framed-ip-address | group-membership | logon-name | qualified-logon-name | use-additional-group-id }
```

Mode

LDAP Schema

Description

Remove attributes of user objects.

Options

| | |
|---------------------------------------|--|
| <i>additional-group-id</i> | Remove the additional user group ID attribute. |
| <i>framed-ip-address</i> | Remove the framed IP address attribute. |
| <i>group-membership</i> | Remove the user group membership attribute. |
| <i>logon-name</i> | Remove the user logon name attribute. |
| <i>qualified-logon-name</i> | Remove the qualified logon name attribute. |
| <i>use-additional-group-id</i> | Do not use the additional user group ID attribute. |

Example

```
no user-attribute logon-name
no user-attribute qualified-logon-name
no user-attribute group-membership
no user-attribute additional-group-id
no user-attribute use-additional-group-id
no user-attribute framed-ip-address
```

Syntax

```
user-group-class <WORD>
```

Mode

LDAP Schema

Description

Set the class name of user group objects.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-group-class groupOfNames
```

Syntax

```
user-group-attribute { additional-group-match <WORD> | member { distinguished-name | user-id } <WORD> }
```

Mode

LDAP Schema

Description

Define attributes of user group objects.

Options

| | |
|---|---|
| <i>additional-group-match</i> <WORD> | Set the additional user group match attribute. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>member</i> | Set the name/type of the member attribute. |
| <i>distinguished-name</i> | The member attribute holds a distinguished name. |
| <i>user-id</i> | The member attribute holds a user ID (uid). |

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-group-attribute member user-id memberId  
user-group-attribute member distinguished-name memberId  
user-group-attribute additional-group-match myPrimaryGroupToken
```

Syntax

```
no user-group-attribute { additional-group-match | member }
```

Mode

LDAP Schema

Description

Remove attributes of user group objects.

Options

additional-group-match Remove the additional user group match attribute.

member Remove the name of the member attribute.

Example

```
no user-group-attribute member  
no user-group-attribute additional-group-match
```

Syntax

```
directory
```

Mode

LDAP Server

Description

Configure the LDAP directory.

Example

```
directory
```

Syntax

```
read-trees-from-server [ domain <WORD> ] { append | replace } { add | ignore }
```

Mode

LDAP Directory

Description

Read the directory trees containing users and user groups from the LDAP server.

Options

domain The domain to search under.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

append Append to existing trees.

replace Replace existing trees.

add For append method, we need append trees found on that server to its own configuration, and for replace method, we need to replace the trees in that server's own configuration with those found on it.

ignore Ignore trees found on that server.

Example

```
read-trees-from-server append add
read-trees-from-server append ignore
read-trees-from-server replace add
read-trees-from-server replace ignore
read-trees-from-server domain mydomain.com append add
```

Syntax

```
primary-domain <WORD>
```

Mode

LDAP Directory

Description

Set the primary LDAP domain.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
primary-domain mydomain.com
```

Syntax

```
no primary-domain
```

Mode

LDAP Directory

Description

Remove the primary LDAP domain.

Example

```
no primary-domain
```

Syntax

```
users-tree <LDAP_DIRECTORY_NAME>
```

Mode

LDAP Directory

Description

Add or re-order a directory tree to search in when searching for user objects.

Options

<LDAP_DIRECTORY_NAME> LDAP directory user or group name.
Example: *abc*

Example

```
users-tree mydomain.com/users  
users-tree ou=users,dc=mydomain,dc=com
```

Syntax

```
no users-tree <LDAP_DIRECTORY_NAME>
```

Mode

LDAP Directory

Description

Remove a directory tree to search in when searching for user objects.

Options

<LDAP_DIRECTORY_NAME> LDAP directory user or group name.
Example: *abc*

Example

```
no users-tree mydomain.com/users  
no users-tree ou=users,dc=mydomain,dc=com
```

Syntax

```
user-groups-tree <LDAP_DIRECTORY_NAME>
```

Mode

LDAP Directory

Description

Add or re-order a directory tree to search in when searching for user group objects.

Options

<LDAP_DIRECTORY_NAME> LDAP directory user or group name.
Example: *abc*

Example

```
user-groups-tree mydomain.com/groups  
user-groups-tree ou=groups,dc=mydomain,dc=com
```

Syntax

```
no user-groups-tree <LDAP_DIRECTORY_NAME>
```

Mode

LDAP Directory

Description

Remove a directory tree to search in when searching for user group objects.

Options

<LDAP_DIRECTORY_NAME> LDAP directory user or group name.
Example: *abc*

Example

```
no user-groups-tree mydomain.com/groups
no user-groups-tree ou=groups,dc=mydomain,dc=com
```

Syntax

```
bind { anonymous | distinguished-name <WORD> | name <WORD> { location <WORD> } }
```

Mode

LDAP Server

Description

Set how to bind to the LDAP server, either selecting anonymous bind, giving the full distinguished name to use, or giving the account name to use and its location in the directory tree (the latter can be in either URL or DN format).

Options

| | |
|---------------------------|---|
| anonymous | Bind anonymously. |
| distinguished-name | Set the full distinguished name to use. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| name | Set the account name to use. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| location | Set the account location in the directory tree. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

Example

```
bind name administrator location builtin
bind distinguished-name "cn=name,ou=User,dc=mydomain,dc=com"
bind anonymous
```

Syntax

```
bind-password <ENC_PASSWORD>
```

Mode

LDAP Server

Description

Set the password for binding to the LDAP server.

Options

| | |
|-----------------------------|-------------------------------------|
| <ENC_PASSWORD> | Password. Example: <i>secret</i> |
|-----------------------------|-------------------------------------|

Example

```
bind-password mypassword
```

Syntax

```
no bind-password
```

Mode

LDAP Server

Description

Clear the password for binding to the LDAP server.

Example

```
no bind-password
```

Syntax

```
referred-bind-with-account { local | other-servers }
```

Mode

LDAP Server

Description

Set the bind method when referred to other servers.

Options

local Bind with this account.

other-servers Bind with an equivalent account on that server (same password).

Example

```
referred-bind-with-account local
referred-bind-with-account other-servers
```

Syntax

```
test <LDAP_SERVER_HOST_NAME> type { connectivity-bind | ldap-search [ return-attribute <WORD> ] { { filter <WORD> [ base { other
<WORD> | root-directory | top-domain-tree } scope { base-entry-only | level-below-base | subtree } ] | group { member | name }
<WORD> | user { common-name | login-name | qualified-name } <WORD> } } | user-authentication <WORD> <WORD> [ chap ] }
```

Mode

LDAP

Description

Run the LDAP test to the specified server with one type of test.

Options

<LDAP_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *LDAP-Server*

type Select one test type.

connectivity-bind Connectivity/bind test. This test will simply try to bind to the LDAP server with the configured bind credentials.

ldap-search LDAP search test. This test will have basic and advanced modes.

return-attribute The return attributes will allow specifying a list of the attributes to return and display rather than displaying the entire matched entry.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

filter Set the search filter for advanced mode.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

base Set the search base.

other Other search base.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

root-directory Root of the directory.

top-domain-tree Top of the domain tree.

| | |
|----------------------------|--|
| scope | Set the search scope. |
| base-entry-only | Search the base entry only. |
| level-below-base | Search one level below the base. |
| subtree | Search the sub-tree. |
| group | Search for a group with a given name or member. |
| member | Search for a group with specific member. |
| name | Search for a group with specific group name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| user | Search for a user with a given login name or common name. |
| common-name | Search for a user with specific common name. |
| login-name | Search for a user with specific login name. |
| qualified-name | Search for a user with specific qualified login name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| user-authentication | User authentication test, testing that a given user name and password can be sent to and authenticated by the LDAP server. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| chap | Test LDAP in a CHAP-compatible way. |

Example

```
test 192.168.168.15 type connectivity-bind
test 192.168.168.15 type user-authentication adminUser password
test 192.168.168.15 type user-authentication adminUser password chap
test 192.168.168.15 type ldap-search user login-name adminUser
test 192.168.168.15 type ldap-search group name adminGroup
test 192.168.168.15 type ldap-search filter LDAPTestFilterContent
test 192.168.168.15 type ldap-search filter LDAPTestFilterContent base root-directory scope subtree
test 192.168.168.15 type ldap-search filter LDAPTestFilterContent base other "dc=example,dc=com" scope subtree
test 192.168.168.15 type ldap-search return-attri dn user login-name adminUser
test 192.168.168.15 type ldap-search return-attri cn group name adminGroup
test 192.168.168.15 type ldap-search return-attri cn filter LDAPTestFilterContent
test 192.168.168.15 type ldap-search return-attri dn filter LDAPTestFilterContent base root-directory scope subtree
test 192.168.168.15 type ldap-search return-attri dn filter LDAPTestFilterContent base other "dc=example,dc=com" scope subtree
```

Syntax

```
user partitioning
```

Mode

Config

Description

Configure user authentication partitioning settings.

Example

```
user partitioning
```

Syntax

```
enable
```

Mode

User Partitioning

Description

Enable user partitioning.

Example

```
enable
```

Syntax

```
no enable
```

Mode

User Partitioning

Description

Disable user partitioning.

Example

```
no enable
```

Syntax

```
partition <PARTITION_NAME>
```

Mode

User Partitioning

Description

Add/edit user authentication partition.

Options

<PARTITION_NAME> User authentication partition name.
Example: *CorpSales*

Example

```
partition corpsales
```

Syntax

```
no partition <PARTITION_NAME>
```

Mode

User Partitioning

Description

Delete user authentication partition.

Options

<PARTITION_NAME> User authentication partition name.
Example: *CorpSales*

Example

```
no partition corpsales
```

Syntax

no partitions

Mode

User Partitioning

Description

Delete all user authentication partitions.

Example

no partitions

Syntax

name <PARTITION_NAME>

Mode

User Partition

Description

Set the user partitioning name.

Options

<PARTITION_NAME> User authentication partition name.
Example: *CorpSales*

Example

name corpSales

Syntax

parent-partition <PARTITION_NAME>

Mode

User Partition

Description

Set parent partition.

Options

<PARTITION_NAME> User authentication partition name.
Example: *CorpSales*

Example

parent-partition topPartition

Syntax

no parent-partition

Mode

User Partition

Description

Clear parent partition.

Example

```
no parent-partition
```

Syntax

```
domain <PARTITION_DOMAIN_NAME>
```

Mode

User Partition

Description

Set the user partitioning domain.

Options

<PARTITION_DOMAIN_NAME> User authentication partition domain.
Example: *CorpSales.com*

Example

```
domain corpName.com
```

Syntax

```
no domain <PARTITION_DOMAIN_NAME>
```

Mode

User Partition

Description

Delete one user partitioning domain.

Options

<PARTITION_DOMAIN_NAME> User authentication partition domain.
Example: *CorpSales.com*

Example

```
no domain corpName.com
```

Syntax

```
no domains
```

Mode

User Partition

Description

Delete all partition domains.

Example

```
no domains
```

Syntax

comment <WORD>

Mode

User Partition

Description

Set the user partitioning comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Corperation Sales"
```

Syntax

no comment

Mode

User Partition

Description

Clear the user partitioning comment.

Example

```
no comment
```

Syntax

```
no policy [ for-console-user | for-remote-user ] interface <PARTITION_INTERFACE> [ zone <PARTITION_ZONE_NAME> ] [ address-object { { [ ipv6 ] { network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any | group <PARTITION_ADDR_MIXED_GROUP_NAME> | name <PARTITION_ADDR_MIXED_NAME> } } ]
```

Mode

User Partitioning

Description

Delete the specified partition selection policy.

Options

for-console-user Delete the specified partition selection policy for console port login user.

for-remote-user Delete the specified partition selection policy for remote user.

interface User partition selection policy interface.

<PARTITION_INTERFACE> User authentication interface name.

Example: *X1*

zone User partition selection policy zone.

<PARTITION_ZONE_NAME> User authentication zone name.

Example: *LAN*

address-object User partition selection policy address object.

ipv6 IPv6 addresses.

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n

Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:0:0:0:0:0*

| | |
|--|--|
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| any | Any. |
| group | Address object group. |
| <PARTITION_ADDR_MIXED_GROUP_NAME> | User authentication address-object name. Example: <i>X0 Subnets</i> |
| name | Address object name. |
| <PARTITION_ADDR_MIXED_NAME> | User authentication address-object name. Example: <i>X0 Subnet</i> |

Example

```
no policy interface X0 zone LAN address-object any no policy for-remote-user interface any
no policy for-console-user interface console
```

Syntax

```
no policies
```

Mode

User Partitioning

Description

Delete all partition selection policies.

Example

```
no policies
```

Syntax

```
policy [ for-console-user | for-remote-user ] interface <PARTITION_INTERFACE> [ zone <PARTITION_ZONE_NAME> ] [ address-object { {
{ [ ipv6 ] { network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any | group
<PARTITION_ADDR_MIXED_GROUP_NAME> | name <PARTITION_ADDR_MIXED_NAME> } } ]
```

Mode

User Partitioning

Description

Add/edit user partition selection policy.

Options

| | |
|------------------------------------|--|
| for-console-user | Delete the specified partition selection policy for console port login user. |
| for-remote-user | Set user partition selection policy for remote user. |
| interface | User partition selection policy interface. |
| <PARTITION_INTERFACE> | User authentication interface name. Example: <i>X1</i> |
| zone | User partition selection policy zone. |
| <PARTITION_ZONE_NAME> | User authentication zone name. Example: <i>LAN</i> |
| address-object | User partition selection policy address object. |

| | |
|--|---|
| ipv6 | IPv6 addresses. |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| any | Any. |
| group | Address object group. |
| <PARTITION_ADDR_MIXED_GROUP_NAME> | User authentication address-object name. Example: <i>X0 Subnets</i> |
| name | Address object name. |
| <PARTITION_ADDR_MIXED_NAME> | User authentication address-object name. Example: <i>X0 Subnet</i> |

Example

```
policy interface X0 zone LAN address-object any policy for-remote-user interface X1
policy for-console-user interface console
```

Syntax

```
zone <PARTITION_ZONE_NAME>
```

Mode

User Partition Selection Policy

Description

Add zone to the selection criteria.

Options

<PARTITION_ZONE_NAME> User authentication zone name.
Example: *LAN*

Example

```
zone WAN
```

Syntax

```
interface <PARTITION_INTERFACE>
```

Mode

User Partition Selection Policy

Description

Set network for the selection policy.

Options

<PARTITION_INTERFACE> User authentication interface name.
Example: *X1*

Example

```
interface X2
```

Syntax

```
address-object { { { [ ipv6 ] { network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any | group  
<PARTITION_ADDR_MIXED_GROUP_NAME> | name <PARTITION_ADDR_MIXED_NAME> } }
```

Mode

User Partition Selection Policy

Description

Set network for the selection policy.

Options

| | |
|---|--|
| ipv6 | IPv6 addresses. |
| network <ADDR_NETWORK> | Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> | Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| any | Any. |
| group <PARTITION_ADDR_MIXED_GROUP_NAME> | Address object group. User authentication address-object name. Example: <i>X0 Subnets</i> |
| name <PARTITION_ADDR_MIXED_NAME> | Address object name. User authentication address-object name. Example: <i>X0 Subnet</i> |

Example

```
address-object name "X0 Subnet"  
address-object range 10.10.10.1 10.10.10.10  
address-object group "LAN Subnets"
```

Syntax

```
partition <PARTITION_NAME>
```

Mode

User Partition Selection Policy

Description

Select partition for the policy.

Options

<PARTITION_NAME> User authentication partition name.
Example: *CorpSales*

Example

```
partition Default
```

Syntax

```
comment <WORD>
```

Mode

User Partition Selection Policy

Description

Set the partition selection policy comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Partion for Remote User"
```

Syntax

```
no comment
```

Mode

User Partition Selection Policy

Description

Clear the partition selection policy comment.

Example

```
no comment
```

Syntax

```
auto-assign { partition <PARTITION_NAME> | partitions }
```

Mode

User Partitioning

Description

Auto-assign items to the partition(s).

Options

partition Auto-assign items to the selected partition.
<PARTITION_NAME> User authentication partition name.
Example: *CorpSales*

partitions Auto-assign items to the partitions.

Example

```
auto-assign myPartition  
auto-assign partitions
```

Syntax

```
user sso
```

Mode

Config

Description

Configure SSO settings.

Example

```
user sso
```

Syntax

```
clear user sso statistics [ agent <SSO_AGENT_HOST_NAME> | global | radius-accounting-client <SSO_RAD_ACCT_CLIENT_HOST_NAME> | terminal-services-agent <SSO_TS_AGENT_HOST_NAME> ]
```

Mode

SSO

Description

Reset SSO statistics.

Options

| | |
|--|--|
| agent <SSO_AGENT_HOST_NAME> | Reset SSO agent statistics. Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Agent</i> |
| global | Reset global (non-agent) SSO statistics. |
| radius-accounting-client <SSO_RAD_ACCT_CLIENT_HOST_NAME> | Reset SSO RADIUS accounting client statistics. Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i> |
| terminal-services-agent <SSO_TS_AGENT_HOST_NAME> | Reset SSO terminal services agent statistics. Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Terminal-Services-Agent</i> |

Example

```
clear user sso statistics
```

Syntax

```
method { browser-ntlm [ { after-sso-agent-failed | before-sso-agent | enabled } ] | radius-accounting | sso-agent | terminal-services-agent }
```

Mode

SSO

Description

Enable the single-sign-on mechanism.

Options

| | |
|---------------------|-------------------------------------|
| browser-ntlm | Enable browser NTLM authentication. |
|---------------------|-------------------------------------|

| | |
|---------------------------------------|--|
| <i>after-ss-agent-failed</i> | Use NTLM to authenticate HTTP traffic only if SSO via the agent fails. |
| <i>before-ss-agent</i> | Use NTLM to authenticate HTTP traffic before attempting SSO via the agent. |
| <i>enabled</i> | Enable browser-ntlm option. |
| <i>radius-accounting</i> | Enable RADIUS accounting authentication. |
| <i>ss-agent</i> | Enable SSO agent authentication. |
| <i>terminal-services-agent</i> | Enable terminal services agent authentication. |

Example

```
method sso-agent
```

Syntax

```
no method { browser-ntlm | radius-accounting | sso-agent | terminal-services-agent }
```

Mode

SSO

Description

Disable the single-sign-on mechanism.

Options

| | |
|---------------------------------------|---|
| <i>browser-ntlm</i> | Disable browser NTLM authentication. |
| <i>radius-accounting</i> | Disable RADIUS accounting authentication. |
| <i>ss-agent</i> | Disable SSO agent authentication. |
| <i>terminal-services-agent</i> | Disable terminal services agent authentication. |

Example

```
no method sso-agent
```

Syntax

```
next-agent-on-no-name
```

Mode

SSO

Description

Enable try next agent on getting no name from NetAPI/WMI.

Example

```
next-agent-on-no-name
```

Syntax

```
no next-agent-on-no-name
```

Mode

SSO

Description

Disable try next agent on getting no name from NetAPI/WMI.

Example

```
no next-agent-on-no-name
```

Syntax

```
block-traffic
```

Mode

SSO

Description

Block user traffic while waiting for SSO.

Example

```
block-traffic
```

Syntax

```
no block-traffic
```

Mode

SSO

Description

Disable block user traffic while waiting for SSO.

Example

```
no block-traffic
```

Syntax

```
including-for-access-rules { all | selected }
```

Mode

SSO

Description

Allow through user traffic for all or selected access rules.

Options

all Allow through user traffic for all access rules.

selected Allow through user traffic for all access rules.

Example

```
including-for-access-rules all
```

Syntax

no including-for-access-rules

Mode

SSO

Description

Block user traffic for all access rules.

Example

no including-for-access-rules

Syntax

local-users-only

Mode

SSO

Description

Limit login to only SSO users with accounts in the local user database.

Example

local-users-only

Syntax

no local-users-only

Mode

SSO

Description

Disable limit login to only SSO users with accounts in the local user database.

Example

no local-users-only

Syntax

non-domain-limited-access

Mode

SSO

Description

Allow limited access for users who are identified by SSO but reported by the agent as not logged into the domain. These users will not be given membership to the Trusted Users user group (even when set locally).

Example

non-domain-limited-access

Syntax

no non-domain-limited-access

Mode

SSO

Description

Disable allow any access for users who are reported by the agent as not logged into the domain.

Example

```
no non-domain-limited-access
```

Syntax

```
probe { netapi [ [ over-netbios | over-tcp ] ] | test-mode | timeout <UINT16> | wmi }
```

Mode

SSO

Description

Probe IP addresses to check if they respond to NetAPI or WMI before making an SSO attempt
 Set timeout for probing IP addresses
 Enable probe test-mode.

Options

| | |
|---|---|
| netapi | Probe for NetAPI, default over NetBIOS. |
| over-netbios | Probe for NetAPI over NetBIOS. |
| over-tcp | Probe for NetAPI over TCP. |
| test-mode | Enable probe test-mode. Probe test mode allows testing that SSO probes are functioning correctly during SSO without their interfering with the user authentications |
| timeout <UINT16> | Set timeout for probing IP addresses. Integer in the form: D OR 0xHHHH. Example: 123 |
| wmi | Probe for WMI. |

Example

```
probe netapi over-tcp
probe wmi
probe time-out 5
probe test-mode
```

Syntax

```
no probe [ test-mode ]
```

Mode

SSO

Description

Disable probe IP addresses to check if they respond to NetAPI or WMI before making an SSO attempt.

Options

test-mode Disable probe test-mode.

Example

```
no probe
```

Syntax

```
user-group-mechanism { ldap | local-only }
```

Mode

SSO

Description

Set the mechanism to use to set user group memberships for users who are authenticated via SSO.

Options

ldap Read user groups via LDAP.

local-only Set using local users that duplicate SSO users.

Example

```
user-group-mechanism ldap
```

Syntax

```
poll rate <UINT32>
```

Mode

SSO

Description

Set the polling rate for checking if logged in users who were identified via SSO are still logged in.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
poll rate 10
```

Syntax

```
poll same-agent
```

Mode

SSO

Description

Enable poll the same agent that authenticated the user.

Example

```
poll same-agent
```

Syntax

```
no poll same-agent
```

Mode

SSO

Description

Disable poll the same agent that authenticated the user.

Example

```
no poll same-agent
```

Syntax

```
hold-time after-failure <UINT16>
```

Mode

SSO

Description

Set the time to hold off from trying again to identify the user at an IP address following an SSO failure for it.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
hold-time after-failure 10
```

Syntax

```
hold-time after-no-user <UINT16>
```

Mode

SSO

Description

Set the time to hold off from trying again to identify the user at an IP address following reporting no user for it.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
hold-time after-no-user 10
```

Syntax

```
windows-service-user-name <WINDOWS_SERVICE_USER_NAME>
```

Mode

SSO

Description

Add a name to the list of user names known to be used by Windows services (and so to be ignored by the SSO agent).

Options

<WINDOWS_SERVICE_USER_NAME> The login name of a windows service.
Example: abc

Example

windows-service-user-name someservice

Syntax

no windows-service-user-name <WINDOWS_SERVICE_USER_NAME>

Mode

SSO

Description

Remove a name from the list of user names known to be used by Windows services (and so to be ignored by the SSO agent).

Options

<WINDOWS_SERVICE_USER_NAME> The login name of a windows service.
Example: abc

Example

no windows-service-user-name someservice

Syntax

security-service-bypass address { [ipv6] { { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <SECURITY_SERVICE_BYPASS_IP_NAME> }

Mode

SSO

Description

Add/edit one bypass SSO rule for the specified address(es).

Options

| | |
|--|--|
| ipv6 | IPv6 address object. |
| host <ADDR_HOST> | Host address object. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n |
| network <ADDR_NETWORK> | Network address object. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: IPV4: 255.255.255.0\nIPV6: /64\n |
| range <ADDR_BEGIN> | Range address object. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n |
| group <ADDR_GROUP_NAME_MIXED> | Group address object name. Group address object name. Example: Sales Group |
| name <SECURITY_SERVICE_BYPASS_IP_NAME> | Address object name. Security service bypass IP name. Example: Web Server |

Example

```
security-service-bypass address name "Non-User Addresses"
```

Syntax

```
no security-service-bypass address <SSO_BYPASS_ADDRESS_NAME>
```

Mode

SSO

Description

Delete one bypass rule with specified address.

Options

<SSO_BYPASS_ADDRESS_NAME> SSO bypass rule address name.
Example: *abc*

Example

```
no security-service-bypass address "Non-User Addresses"
```

Syntax

```
security-service-bypass service { built-in <SSO_BYPASS_SERVICE_BUILT_IN_NAME> | group <SVC_GROUP_NAME> | name  
<SSO_BYPASS_SERVICE_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

SSO

Description

Add/edit one bypass SSO rule for the specified service(s).

Options

| | |
|---|---|
| built-in | SSO bypass built-in service object. |
| <SSO_BYPASS_SERVICE_BUILT_IN_NAME> | SSO bypass build-in object name. Example: <i>abc</i> |
| group | Service group name. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SSO_BYPASS_SERVICE_NAME> | SSO bypass rule service name. Example: <i>abc</i> |
| protocol | Service protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
security-service-bypass service name "POP3"
```

Syntax

```
no security-service-bypass service { group <SSO_BYPASS_SERVICE_NAME> | name <SSO_BYPASS_SERVICE_NAME> }
```

Mode

SSO

Description

Delete one bypass rule with specified service.

Options

| | |
|--|--|
| group | Service group name. |
| <SSO_BYPASS_SERVICE_NAME> | SSO bypass rule service name. Example: <i>abc</i> |
| name | Service object name. |
| <SSO_BYPASS_SERVICE_NAME> | SSO bypass rule service name. Example: <i>abc</i> |

Example

```
no security-service-bypass service name "POP3"
```

Syntax

```
address { [ ipv6 ] { { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <SECURITY_SERVICE_BYPASS_IP_NAME> }
```

Mode

SSO Bypass

Description

Set address object or group as bypass rule name.

Options

| | |
|--|--|
| ipv6 | IPv6 address object. |
| host | Host address object. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Network address object. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Range address object. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group | Group address object name. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| name | Address object name. |
| <SECURITY_SERVICE_BYPASS_IP_NAME> | Security service bypass IP name. Example: <i>Web Server</i> |

Example

address name ssoBypassName

Syntax

```
service { built-in <SSO_BYPASS_SERVICE_BUILT_IN_NAME> | group <SVC_GROUP_NAME> | name <SSO_BYPASS_SERVICE_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

SSO Bypass

Description

Set service object or group as bypass rule name.

Options

| | |
|---|---|
| built-in | SSO bypass built-in service object. |
| <SSO_BYPASS_SERVICE_BUILT_IN_NAME> | SSO bypass build-in object name. Example: <i>abc</i> |
| group | Service group name. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SSO_BYPASS_SERVICE_NAME> | SSO bypass rule service name. Example: <i>abc</i> |
| protocol | Service protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
service name ssoBypassName
```

Syntax

```
type { full-bypass | trigger-sso }
```

Mode

SSO Bypass

Description

Set bypass type.

Options

- full-bypass** Set bypass type as full bypass.
- trigger-sso** Set bypass type as trigger SSO but bypass holding packets while waiting for it.

Example

```
type full-bypass
```

Syntax


```
dummy-user [ name <WORD> | timeout <UINT16> ]
```

Mode

SSO

Description

Enable create dummy user entries for SSO bypass and set its configuration.

Options

name Set user name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

timeout Set inactivity timeout.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
dummy-user  
dummy-user name "SSO Bypass"  
dummy-user timeout 15
```

Syntax

```
no dummy-user [ name ]
```

Mode

SSO

Description

Disable create dummy user entries for SSO bypass or clear user name.

Options

name Clear user name.

Example

```
no dummy-user  
no dummy-user name
```

Syntax

```
enforce-on-zone <SSO_ZONE_NAME>
```

Mode

SSO

Description

Select to always enforce SSO on a zone.

Options

<SSO_ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
enforce-on-zone lan
```

Syntax

```
no enforce-on-zone <SSO_ZONE_NAME>
```

Mode

SSO

Description

Select to not always enforce SSO on a zone.

Options

<SSO_ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
no enforce-on-zone lan
```

Syntax

```
tso-services-bypass
```

Mode

SSO

Description

Allow traffic from services on a terminal server running the TS agent to bypass user authentication in access rules.

Example

```
tso-services-bypass
```

Syntax

```
no tso-services-bypass
```

Mode

SSO

Description

Don't Allow traffic from services on a terminal server running the TS agent to bypass user authentication in access rules.

Example

```
no tso-services-bypass
```

Syntax

```
authentication-domain { custom <WORD> | inherit-from-ldap }
```

Mode

SSO

Description

Set the authentication domain.

Options

custom User the custom domain.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

inherit-from-ldap Use the domain from the LDAP configuration.

Example

```
authentication-domain custom "www.mydomain.com"
```

Syntax

```
redirect-browser { certificate-name | domain-name { { configured | reverse-dns-look-up } } | ip-address }
```

Mode

SSO

Description

Set method of redirect browser to SonicWall appliance's own web server.

Options

certificate-name Via the name from the administration certificate

domain-name Via the domain name

configured Via its configured domain name

reverse-dns-look-up Via its domain name from a reverse DNS lookup of the interface IP address

ip-address Via the interface IP address

Example

```
redirect-browser ip-address
```

Syntax

```
retries-on-failure <UINT16>
```

Mode

SSO

Description

Set maximum retries to allow on authentication failure.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
retries-on-failure 3
```

Syntax

```
poll users { linux | macintosh | windows } { { agent | bypass-re-authentication | re-authentication-ntlm } }
```

Mode

SSO

Description

On the poll timer, set polling method for users authenticated via NTLM in different system.

Options

| | |
|---------------------------------|---|
| linux | Set polling method for linux users. |
| macintosh | Set polling method for macintosh users. |
| windows | Set polling method for windows users. |
| agent | Poll via the SSO agent. |
| bypass-re-authentication | Don't re-authenticate. |
| re-authentication-ntlm | Re-authenticate via NTLM. |

Example

```
poll users linux re-authentication-ntlm
```

Syntax

```
forward-lanman
```

Mode

SSO

Description

Enable forward legacy LanMan in NTLM.

Example

```
forward-lanman
```

Syntax

```
no forward-lanman
```

Mode

SSO

Description

Disable forward legacy LanMan in NTLM.

Example

```
no forward-lanman
```

Syntax

```
radius-accounting port <IPV4_PORT>
```

Mode

SSO

Description

Set the RADIUS accounting's UDP port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
radius-accounting port 1813
```

Syntax

```
agent <SSO_AGENT_HOST_NAME>
```

Mode

SSO

Description

Configure an SSO agent.

Options

<SSO_AGENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *SSO-Agent*

Example

```
agent 192.168.168.1
```

Syntax

```
no agent <SSO_AGENT_HOST_NAME>
```

Mode

SSO

Description

Delete an SSO agent.

Options

<SSO_AGENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *SSO-Agent*

Example

```
no agent 192.168.168.1
```

Syntax

```
no agents
```

Mode

SSO

Description

Delete all SSO agents.

Example

```
no agents
```

Syntax

```
host <SSO_AGENT_HOST_NAME>
```

Mode

SSO Agent

Description

Set the SSO agent's host name or IP address.

Options

<SSO_AGENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *SSO-Agent*

Example

```
host 192.168.168.1
```

Syntax

```
port <IPV4_PORT>
```

Mode

SSO Agent

Description

Set the SSO agent's UDP port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
port 389
```

Syntax

```
enable
```

Mode

SSO Agent

Description

Enable the SSO agent.

Example

```
enable
```

Syntax

```
no enable
```

Mode

SSO Agent

Description

Disable the SSO agent.

Example

```
no enable
```

Syntax

```
timeout <UINT16>
```

Mode

SSO Agent

Description

Set the timeout on replies from the agent.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
timeout 10
```

Syntax

```
retries <UINT16>
```

Mode

SSO Agent

Description

Set the maximum number of retries to make after timeouts waiting for replies from the agent.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
retries 10
```

Syntax

```
no shared-key
```

Mode

SSO Agent

Description

Clear the shared key for encrypting messages to/from the agent.

Example

```
no shared-key
```

Syntax

```
shared-key <ENC_HEX_STRING>
```

Mode

SSO Agent

Description

Set the hexadecimal value of the shared key for encrypting messages to/from the SSO agent.

Options

<ENC_HEX_STRING> String of hexadecimal digits.
Example: *0123456989abcdef*

Example

```
shared-key 1234abcd
```

Syntax

```
max-requests <UINT16>
```

Mode

SSO Agent

Description

Set the maximum number of requests to send to the agent at a time.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
max-requests 10
```

Syntax

```
partition <PARTITION_NAME>
```

Mode

SSO Agent

Description

Set the SSO agent's user partition.

Options

<PARTITION_NAME> User authentication partition name.
Example: *CorpSales*

Example

```
partition corpsales
```

Syntax

```
no partition
```

Mode

SSO Agent

Description

Clear the SSO agent's user partition.

Example

```
no partition
```

Syntax

```
terminal-services-agent <SSO_TS_AGENT_HOST_NAME>
```

Mode

SSO

Description

Configure a terminal services agent.

Options

<SSO_TS_AGENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *SSO-Terminal-Services-Agent*

Example

```
terminal-services-agent 192.168.168.1
```

Syntax

```
no terminal-services-agent <SSO_TS_AGENT_HOST_NAME>
```

Mode

SSO

Description

Delete a terminal services agent.

Options

<SSO_TS_AGENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *SSO-Terminal-Services-Agent*

Example

```
no terminal-services-agent 192.168.168.1
```

Syntax

```
no terminal-services-agents
```

Mode

SSO

Description

Delete all terminal services agents.

Example

```
no terminal-services-agents
```

Syntax

host <HOSTNAME>

Mode

SSO Agent

Description

Set the agent's host name or IP address.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

host 192.168.168.1

Syntax

port <IPV4_PORT>

Mode

SSO Agent

Description

Set the agent's UDP port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

port 389

Syntax

enable

Mode

SSO Agent

Description

Enable the terminal services agent.

Example

enable

Syntax

no enable

Mode

SSO Agent

Description

Disable the terminal services agent.

Example

no enable

Syntax

no shared-key

Mode

SSO Agent

Description

Clear the shared key for encrypting messages to/from the agent.

Example

no shared-key

Syntax

shared-key <ENC_HEX_STRING>

Mode

SSO Agent

Description

Set the hexadecimal value of the shared key for encrypting messages to/from the terminal services agent.

Options

<ENC_HEX_STRING> String of hexadecimal digits.
Example: *0123456989abcdef*

Example

shared-key 1234abcd

Syntax

partition <PARTITION_NAME>

Mode

SSO Agent

Description

Set the Terminal Services agent's user partition.

Options

<PARTITION_NAME> User authentication partition name.
Example: *CorpSales*

Example

partition corpsales

Syntax

no partition

Mode

SSO Agent

Description

Clear the Terminal Services agent's user partition.

Example

```
no partition
```

Syntax

```
radius-accounting-client <SSO_RAD_ACCT_CLIENT_HOST_NAME>
```

Mode

SSO

Description

Configure a RADIUS accounting client.

Options

<SSO_RAD_ACCT_CLIENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
radius-accounting-client 192.168.168.11
```

Syntax

```
no radius-accounting-client <SSO_RAD_ACCT_CLIENT_HOST_NAME>
```

Mode

SSO

Description

Delete a RADIUS accounting client.

Options

<SSO_RAD_ACCT_CLIENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
no radius-accounting-client 192.168.168.11
```

Syntax

```
no radius-accounting-clients
```

Mode

SSO

Description

Delete all RADIUS accounting clients.

Example

```
no radius-accounting-clients
```

Syntax

```
host <SSO_RAD_ACCT_CLIENT_HOST_NAME>
```

Mode

SSO RADIUS Accounting Client

Description

Set the RADIUS accounting client's host name or IP address.

Options

<SSO_RAD_ACCT_CLIENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
host 192.168.168.1
```

Syntax

```
shared-secret <ENC_PASSWORD>
```

Mode

SSO RADIUS Accounting Client

Description

Set the value of the shared secret for encrypting messages to/from the client.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
shared-secret 1234abcd
```

Syntax

```
no shared-secret
```

Mode

SSO RADIUS Accounting Client

Description

Clear the shared secret for encrypting messages to/from the client.

Example

```
no shared-secret
```

Syntax

```
user-name-format { canonical | down-level-logon | sonicwall-aventail | user-name | user-principle }
```

Mode

SSO RADIUS Accounting Client

Description

Set user name attribute format.

Options

| | |
|---------------------------|---|
| canonical | Set to pre-defined \"Domain/User-name\" format. |
| down-level-logon | Set to pre-defined \"Domain\\User-name\" format. |
| sonicwall-aventail | Set to pre-defined \"SonicWall Aventail\" format. |
| user-name | Set to pre-defined \"User-name\" format. |
| user-principle | Set to pre-defined \"User-name@Domain\" format. |

Example

```
user-name-format user-name
```

Syntax

```
missing-domain { ldap-look-up | local-user }
```

Mode

SSO RADIUS Accounting Client

Description

Set approach if the domain component is missing in a RADIUS message.

Options

| | |
|---------------------|---------------------------------|
| ldap-look-up | Look up the user name via LDAP. |
| local-user | Assume a non-domain user. |

Example

```
missing-domain ldap-look-up
```

Syntax

```
log-user-out <UINT32>
```

Mode

SSO RADIUS Accounting Client

Description

Log user out if no accounting interim updates are received for the specified minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
log-user-out 5
```

Syntax

```
no log-user-out
```

Mode

Description

Disable log user out.

Example

```
no log-user-out
```

Syntax

```
server <SSO_RAD_ACCT_FORWARD_SERVER_ID> <SSO_RAD_ACCT_PROXY_FWD_SERVER_HOST_NAME> [ port <IPV4_PORT> ] [ shared-secret <ENC_PASSWORD> ]
```

Mode

SSO RADIUS Accounting Client

Description

Configure the server for receiving RADIUS accounting messages forwarded from this client.

Options

| | |
|--|---|
| <SSO_RAD_ACCT_FORWARD_SERVER_ID> | Integer in the form: D OR 0xHH. Example: 1 |
| <SSO_RAD_ACCT_PROXY_FWD_SERVER_HOST_NAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i> |
| port | Set the server's port number. |
| <IPV4_PORT> | Integer in the form: D OR 0xHHHH. Example: 80 |
| shared-secret | Set the shared secret. |
| <ENC_PASSWORD> | Password. Example: <i>secret</i> |

Example

```
server 1 192.168.168.11 port 1813 shared-secret 123abc
```

Syntax

```
no server <SSO_RAD_ACCT_FORWARD_SERVER_ID> [ shared-secret ]
```

Mode

SSO RADIUS Accounting Client

Description

Clear a RADIUS accounting client forwarding server.

Options

| | |
|---|---|
| <SSO_RAD_ACCT_FORWARD_SERVER_ID> | Integer in the form: D OR 0xHH. Example: 1 |
| shared-secret | Clear the shared secret. |

Example

```
no server 1
```

Syntax

```
proxy-forward timeout <UINT16>
```

Mode

SSO RADIUS Accounting Client

Description

Set timeout for each forward.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
proxy-forward timeout 5
```

Syntax

```
proxy-forward retries <UINT16>
```

Mode

SSO RADIUS Accounting Client

Description

Set retries number for each accounting server.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
proxy-forward retries 5
```

Syntax

```
proxy-forward type { forward-to-all | try-next-on-timeout }
```

Mode

SSO RADIUS Accounting Client

Description

Set how to proxy forward to multiple accounting servers.

Options

forward-to-all Proxy forward to all servers.

try-next-on-timeout Try next server when timeout.

Example

```
proxy-forward type try-next-on-timeout
```

Syntax

```
partition <PARTITION_NAME>
```

Mode

SSO RADIUS Accounting Client

Description

Set the Radius Accounting client's user partition.

Options

<PARTITION_NAME> User authentication partition name.
Example: *CorpSales*

Example

```
partition corpsales
```

Syntax

```
no partition
```

Mode

SSO RADIUS Accounting Client

Description

Clear the Radius Accounting client's user partition.

Example

```
no partition
```

Syntax

```
test [ [ agent <SSO_AGENT_HOST_NAME> ] [ user-ip <IPV4_HOST> ] | terminal-services-agent <SSO_TS_AGENT_HOST_NAME> ]
```

Mode

SSO

Description

Run the SSO test with the given user name/password.

Options

| | |
|---------------------------------------|---|
| agent | Specify an agent to test. |
| <SSO_AGENT_HOST_NAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Agent</i> |
| user-ip | The IP address of a user to test. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |
| terminal-services-agent | Specify a terminal services agent to test. |
| <SSO_TS_AGENT_HOST_NAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Terminal-Services-Agent</i> |

Example

```
test agent 192.168.168.1 user-ip 192.168.168.99
```

Syntax

```
user guest
```

Mode

Config

Description

Configure settings related to guest users.

Example

```
user guest
```

Syntax

```
profile <GUEST_PROFILE_NAME>
```

Mode

Guest User

Description

Add or update a guest user profile.

Options

<GUEST_PROFILE_NAME> Guest profile name.
Example: *profile1*

Example

```
profile "Custom Profile"
```

Syntax

```
no profile <GUEST_PROFILE_NAME>
```

Mode

Guest User

Description

Delete a guest user profile.

Options

<GUEST_PROFILE_NAME> Guest profile name.
Example: *profile1*

Example

```
no profile "Custom Profile"
```

Syntax

```
user [ uuid ] <GUEST_USER_NAME> [ password <ENC_PASSWORD> [ hide-password ] ]
```

Mode

Guest User

Description

Add or edit a guest user account.

Options

uuid Edit a user object by UUID.
<GUEST_USER_NAME> Guest user name.
Example: *guest1*
password Set the guest user password.
<ENC_PASSWORD> Password.
Example: *secret*
hide-password Don't show the auto-generated password.

Example

```
user johndoe
user johndoe password password
user johndoe password password hide-password
```

Syntax

```
generate <UINT32> [ profile <GUEST_PROFILE_NAME> ] [ hide-password ]
```

Mode

Guest User

Description

Auto generate some guest users.

Options

| | |
|-----------------------------------|---|
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: 123 |
| profile | Apply the settings from a guest profile. |
| <GUEST_PROFILE_NAME> | Guest profile name. Example: profile1 |
| hide-password | Don't show the auto-generated password. |

Example

```
generate 2 profile Default hide-password
```

Syntax

```
no user [ uuid ] <GUEST_USER_NAME>
```

Mode

Guest User

Description

Delete a guest user account.

Options

| | |
|--------------------------------|-------------------------------------|
| uuid | Delete a user object by UUID. |
| <GUEST_USER_NAME> | Guest user name. Example: guest1 |

Example

```
no user johndoe
```

Syntax

```
no users <WORD>
```

Mode

Guest User

Description

Delete all guest user accounts with a given name prefix.

Options

| | |
|---------------------|--|
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: abc |
|---------------------|--|

Example

```
no users temp-guest
```

Syntax

```
show-guest-status-window
```

Mode

Guest User

Description

Enable showing the login status window after guest login.

Example

```
show-guest-status-window
```

Syntax

```
no show-guest-status-window
```

Mode

Guest User

Description

Disable showing the login status window after guest login.

Example

```
no show-guest-status-window
```

Syntax

```
export guest-accounts { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

Guest User

Description

Export guest accounts' configurations.

Options

ftp Export using the FTP protocol.
<FTP_URL> FTP URL in the form: ftp://username:password@hostname/ Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: ftp://username:password@hostname/ nftp://username@hostname/ nftp://hostname/

scp Export using the SCP protocol.
<SCP_URL> SCP URL in the form: scp://username@host/ Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: scp://username@host/ nscp://host/

Example

```
export guest-accounts ftp ftp://user:password@servername/ guest-accounts.csv
```

Syntax

```
logout user at <GUEST_LOGIN_USER_BY_IP>
```

Mode

Guest User

Description

Logout guest user.

Options

at Logout a guest user by IP.
<GUEST_LOGIN_USER_BY_IP> IPV4: address in the form: D.D.D.D\nIPV6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
logout user at 192.168.168.1
```

Syntax

```
logout users
```

Mode

Guest User

Description

Logout guest users.

Example

```
logout users
```

Syntax

```
name <GUEST_PROFILE_NAME>
```

Mode

Guest Profile

Description

Set the name of the guest user profile.

Options

<GUEST_PROFILE_NAME> Guest profile name.
Example: *profile1*

Example

```
name profile1
```

Syntax

```
generate { name | password }
```

Mode

Guest Profile

Description

Auto generate names or passwords for guest accounts created with this profile.

Options

name Auto-generate names for created guest accounts.

password Auto generate passwords for created guest accounts.

Example

```
generate name
generate password
```

Syntax

```
no generate { name | password }
```

Mode

Guest Profile

Description

Disable auto generate names or passwords for guest accounts created with this profile.

Options

name Disable auto-generate names for created guest accounts.

password Disable auto generate passwords for created guest accounts.

Example

```
no generate name
no generate password
```

Syntax

```
name-prefix <WORD>
```

Mode

Guest Profile

Description

Set a prefix for auto generated names for guest accounts created with this profile.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name-prefix guest
```

Syntax

```
comment <WORD>
```

Mode

Guest Profile

Description

Set comment for guest accounts created with this profile.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Added via profile1"
```

Syntax

```
no comment
```

Mode

Guest Profile

Description

Clear comment for guest accounts created with this profile.

Example

```
no comment
```

Syntax

```
enable
```

Mode

Guest Profile

Description

Enable guest accounts to be created.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Guest Profile

Description

Disable guest accounts to be created.

Example

```
no enable
```

Syntax

```
activate-on-login
```

Mode

Guest Profile

Description

Enable activate account upon first login.

Example

```
activate-on-login
```

Syntax

```
no activate-on-login
```

Mode

Guest Profile

Description

Disable activate account upon first login.

Example

```
no activate-on-login
```

Syntax

```
login-uniqueness
```

Mode

Guest Profile

Description

Enable enforcing unique login sessions.

Example

```
login-uniqueness
```

Syntax

```
no login-uniqueness
```

Mode

Guest Profile

Description

Disable enforcing unique login sessions.

Example

```
no login-uniqueness
```

Syntax

```
prune-on-expiry
```

Mode

Guest Profile

Description

Enable to delete the guest accounts when they are expired if a limited lifetime is set.

Example

```
prune-on-expiry
```

Syntax

```
no prune-on-expiry
```

Mode

Guest Profile

Description

Disable to delete the guest accounts when they are expired.

Example

```
no prune-on-expiry
```

Syntax

```
account-lifetime <UINT32> { days | hours | minutes }
```

Mode

Guest Profile

Description

Set a limited lifetime for the guest accounts.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

days Set the lifetime in days.

hours Set the lifetime in hours.

minutes Set the lifetime in minutes.

Example

```
account-lifetime 48 hours
```

Syntax

```
no quota-cycle
```

Mode

Guest Profile

Description

Set no quota cycle for the guest accounts created with this profile.

Example

```
no quota-cycle
```

Syntax

```
quota-cycle { day | month | week }
```

Mode

Guest Profile

Description

Set a quota cycle for the guest accounts created with this profile.

Options

day Set the quota cycle as one day.

month Set the quota cycle as one month.

week Set the quota cycle as one week.

Example

```
quota-cycle per day
```

Syntax

```
session-lifetime <UINT32> { days | hours | minutes }
```

Mode

Guest Profile

Description

Set a session time limit for the created guest accounts.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

days Set the session limit in days.

hours Set the session limit in hours.

minutes Set the session limit in minutes.

Example

```
session-lifetime 48 hours
```

Syntax

```
idle-timeout <UINT32> { days | hours | minutes }
```

Mode

Guest Profile

Description

Set the session inactivity timeout for created guest accounts.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

days Set the idle timeout in days.

hours Set the idle timeout in hours.

minutes Set the idle timeout in minutes.

Example

```
idle-timeout 20 minutes
```

Syntax

```
limit { receive | transmit } <UINT32>
```

Mode

Guest Profile

Description

Set the receive or transmit limit in MB.

Options

receive Set the receive limit in MB.

transmit Set the transmit limit in MB.

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
limit receive 500  
limit transmit 300
```

Syntax

```
no limit { receive | transmit }
```

Mode

Guest Profile

Description

Disable receive or transmit limit.

Options

receive Disable receive limit.

transmit Disable transmit limit.

Example

```
no limit receive  
no limit transmit
```

Syntax

```
name <GUEST_USER_NAME>
```

Mode

Guest User

Description

Set the login name of the guest account.

Options

<GUEST_USER_NAME> Guest user name.
Example: *guest1*

Example

```
name johndoe
```

Syntax

```
uuid <UUID>
```

Mode

Guest User

Description

Set user object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid f40b27d6-b8b9-a4fc-0500-c0eae49ce84c
```

Syntax

```
no uuid <UUID>
```

Mode

Guest User

Description

Clear user object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
no uuid
```

Syntax

```
generate { name | password [ hide ] }
```

Mode

Guest User

Description

Generate a login name or password for the guest account.

Options

name Generate a login name for the guest account.

password Generate a password for the guest account.

hide Disable showing the generated password.

Example

```
generate name
generate password
```

Syntax

```
profile <GUEST_PROFILE_NAME> [ hide-password ]
```

Mode

Guest User

Description

Enable the settings from a guest profile.

Options

<GUEST_PROFILE_NAME> Guest profile name.
Example: *profile1*

hide-password Disable showing the auto-generated password.

Example

```
profile "Custom Profile"
```

Syntax

```
comment <WORD>
```

Mode

Guest User

Description

Set comment for the guest account.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Added 7/26/2010"
```

Syntax

```
no comment
```

Mode

Guest User

Description

Clear the comment for the guest account.

Example

no comment

Syntax

password <ENC_PASSWORD>

Mode

Guest User

Description

Set the guest account password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

password *pwd1234*

Syntax

no password

Mode

Guest User

Description

Clear the guest account password.

Example

no password

Syntax

enable

Mode

Guest User

Description

Enable the guest account.

Example

enable

Syntax

no enable

Mode

Guest User

Description

Disable the guest account.

Example

```
no enable
```

Syntax

```
activate-on-login
```

Mode

Guest User

Description

Enable activate account upon first login.

Example

```
activate-on-login
```

Syntax

```
no activate-on-login
```

Mode

Guest User

Description

Disable activate account upon first login.

Example

```
no activate-on-login
```

Syntax

```
login-uniqueness
```

Mode

Guest User

Description

Enable enforcing a unique login session with the guest account.

Example

```
login-uniqueness
```

Syntax

```
no login-uniqueness
```

Mode

Guest User

Description

Disable enforcing a unique login session with the guest account.

Example

```
no login-uniqueness
```

Syntax

```
prune-on-expiry
```

Mode

Guest User

Description

Enable delete the guest account when it is expired if a limited lifetime is set.

Example

```
prune-on-expiry
```

Syntax

```
no prune-on-expiry
```

Mode

Guest User

Description

Disable delete the guest account when it is expired.

Example

```
no prune-on-expiry
```

Syntax

```
account-lifetime <UINT32> { days | hours | minutes }
```

Mode

Guest User

Description

Set a limited lifetime for the guest account.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

days Set the lifetime in days.

hours Set the lifetime in hours.

minutes Set the lifetime in minutes.

Example

```
account-lifetime 48 hours
```

Syntax

no quota-cycle

Mode

Guest User

Description

Set no quota cycle for the guest account.

Example

no quota-cycle

Syntax

quota-cycle { day | month | week }

Mode

Guest User

Description

Set a quota cycle for the guest account.

Options

day Set the quota cycle as one day.

month Set the quota cycle as one month.

week Set the quota cycle as one week.

Example

quota-cycle per day

Syntax

session-lifetime <UINT32> { days | hours | minutes }

Mode

Guest User

Description

Set a session time limit for the guest account.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

days Set the session limit in days.

hours Set the session limit in hours.

minutes Set the session limit in minutes.

Example

session-lifetime 48 hours

Syntax

no session-lifetime

Mode

Guest User

Description

Disable session time limit for the guest account.

Example

no session-lifetime

Syntax

idle-timeout <UINT32> { days | hours | minutes }

Mode

Guest User

Description

Set the session inactivity timeout for the guest account.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

days Set the idle timeout in days.

hours Set the idle timeout in hours.

minutes Set the idle timeout in minutes.

Example

idle-timeout 20 minutes

Syntax

limit { receive | transmit } <UINT32>

Mode

Guest User

Description

Set the receive or transmit limit in MB for the guest account.

Options

receive Set the receive limit in MB for the guest account.

transmit Set the transmit limit in MB for the guest account.

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

limit receive 500
limit transmit 300

Syntax

```
no limit { receive | transmit }
```

Mode

Guest User

Description

Disable receive or transmit limit for the guest account.

Options

receive Disable receive limit for the guest account.

transmit Disable transmit limit for the guest account.

Example

```
no limit receive
no limit transmit
```

Syntax

```
show user authentication [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show user authentication related settings.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show user authentication
```

Syntax

```
show user local [ group { name | uuid } <LOCAL_GROUP_GROUP_NAME> [ domain <LOCAL_GROUP_DOMAIN_NAME> ] | groups | user { name | uuid } <LOCAL_USER_USER_NAME> [ domain <LOCAL_USER_DOMAIN_NAME> ] | users ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show settings for local users/groups.

Options

group Show a local user group.

name Show a user group object by name.

uuid Show a user group object by UUID.

<LOCAL_GROUP_GROUP_NAME> User group object name.
Example: *Limited Administrators*

| | |
|--|---|
| domain | Set the user group's domain. |
| <LOCAL_GROUP_DOMAIN_NAME> | User group object domain name. Example: <i>example.com</i> |
| groups | Show all local user groups. |
| user | Show a local user. |
| name | Show a user object by name. |
| uuid | Show a user object by UUID. |
| <LOCAL_USER_USER_NAME> | User object name. Example: <i>John</i> |
| domain | Set the user's domain. |
| <LOCAL_USER_DOMAIN_NAME> | User object domain name. Example: <i>example.com</i> |
| users | Show all local users. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show user local
show user local users
show user local user name jcool
show user local user uuid 00000000-0000-0001-0500-c0eae49ce84c
show user local groups
show user local group uuid 00000000-0000-0001-0600-c0eae49ce84c
show user local group name "Special Users"
```

Syntax

```
show user status [ at <USER_IPV4_ADDR> [ user <UINT32> ] | cli | inactive | name <USER_LOGIN_NAME> | unauthenticated ] [ pending ]
[ logged-in ] [ locked-out ]
```

Mode

All Modes

Description

Show information on current users.

Options

| | |
|--------------------------------|---|
| at | Show detail of a user at a given IP address. |
| <USER_IPV4_ADDR> | IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |
| user | For Terminal Services users only, select the user at the IP address. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i> |
| cli | Show the status of CLI login users. |
| inactive | Show information of inactive users. |
| name | Show information of the users with the given name |
| <USER_LOGIN_NAME> | A connected user's login name. Example: <i>jdoe</i> |
| unauthenticated | Show information of unauthenticated users. |
| pending | Include users currently being authenticated. |
| logged-in | Include logged in users. |
| locked-out | Include locked out users. |

Example

```
show user status
show user status at 192.168.168.1
```

Syntax

```
show user statistics
```

Mode

All Modes

Description

Show current user's statistics information.

Example

```
show user statistics
```

Syntax

```
show user management
```

Mode

All Modes

Description

Show user management configuration.

Example

```
show user management
```

Syntax

```
show user radius [ [ accounting [ [ server <RADIUS_ACCOUNTING_HOST_NAME> | servers ] ] | server <RADIUS_SERVER_HOST_NAME> | servers ] [ { pending-config | with-pending-config } ] | statistics [ server <RADIUS_SERVER_HOST_NAME> ] ]
```

Mode

All Modes

Description

Show RADIUS settings and statistics.

Options

| | |
|---|--|
| accounting | Show settings for RADIUS accounting settings. |
| server <RADIUS_ACCOUNTING_HOST_NAME> | Show RADIUS accounting server settings. Hostname in the form: hostname OR a.b.c.d. Example: 10.10.10.10\www.radiusServer.com |
| servers | Show settings for all RADIUS accounting servers. |
| server <RADIUS_SERVER_HOST_NAME> | Show RADIUS server settings. Hostname in the form: hostname OR a.b.c.d. Example: 10.10.10.10\www.radiusServer.com |
| servers | Show settings for all RADIUS servers. |
| pending-config | Show pending configuration changes. |

| | |
|--|---|
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |
| <i>statistics</i> | Show RADIUS server statistics. |
| <i>server</i> | Show statistics for a specific RADIUS server. |
| <RADIUS_SERVER_HOST_NAME> | Hostname in the form: hostname OR a.b.c.d. Example: 10.10.10.10\www.radiusServer.com |

Example

```
show user radius
show user radius servers
show user radius server 192.168.168.168
show user radius accounting
show user radius accounting servers
show user radius accounting server 192.168.168.1
show user radius statistics
show user radius statistics server 10.10.10.10
```

Syntax

```
show user ldap [ [ relay | server <LDAP_SERVER_HOST_NAME> | servers ] [ { pending-config | with-pending-config } ] | dynamic-
server <LDAP_DYNAMIC_SERVER_NAME> | dynamic-servers | statistics [ { dynamic-server <LDAP_DYNAMIC_SERVER_NAME> | global | server
<LDAP_SERVER_HOST_NAME> | servers } ] ]
```

Mode

All Modes

Description

Show LDAP settings and statistics.

Options

| | |
|---|--|
| <i>relay</i> | Show LDAP relay configuration. |
| <i>server</i> <LDAP_SERVER_HOST_NAME> | Show specified LDAP server settings. Hostname in the form: hostname OR a.b.c.d. Example: <i>LDAP-Server</i> |
| <i>servers</i> | Show all LDAP servers settings. |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |
| <i>dynamic-server</i> <LDAP_DYNAMIC_SERVER_NAME> | Show status for a specific LDAP dynamic server. Hostname in the form: hostname OR a.b.c.d. Example: <i>LDAP-Dynamic-Server</i> |
| <i>dynamic-servers</i> | Show all LDAP dynamic servers status. |
| <i>statistics</i> | Show LDAP server statistics. |
| <i>dynamic-server</i> <LDAP_DYNAMIC_SERVER_NAME> | Show statistics for a specific LDAP dynamic server. Hostname in the form: hostname OR a.b.c.d. Example: <i>LDAP-Dynamic-Server</i> |
| <i>global</i> | Show LDAP servers global statistics. |
| <i>server</i> <LDAP_SERVER_HOST_NAME> | Show statistics for a specific LDAP server. Hostname in the form: hostname OR a.b.c.d. Example: <i>LDAP-Server</i> |
| <i>servers</i> | Show all LDAP servers statistics. |

Example

```

show user ldap show user ldap servers
show user ldap server 192.168.168.2
show user ldap relay
show user ldap statistics
show user ldap statistics global
show user ldap statistics server 10.10.10.10
show user ldap statistics dynamic-server 10.10.10.11
show user ldap statistics servers
show user ldap dynamic-servers
show user ldap dynamic-server 20.20.20.20

```

Syntax

```

show user partitioning [ partition <PARTITION_NAME> | partitions | policies | policy { { [ for-console-user | for-remote-user ]
interface <PARTITION_INTERFACE> [ zone <PARTITION_ZONE_NAME> ] [ address-object { { [ ipv6 ] { network <ADDR_NETWORK>
<ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any | group <PARTITION_ADDR_MIXED_GROUP_NAME> | name <PARTITION_ADDR_MIXED_NAME>
} } ] } ] [ { pending-config | with-pending-config } ]

```

Mode

All Modes

Description

Show user partitioning settings.

Options

| | |
|--|---|
| partition | Show settings for specified user partition. |
| <PARTITION_NAME> | User authentication partition name. Example: <i>CorpSales</i> |
| partitions | Show settings for all user partitions. |
| policies | Show all partition selection policies. |
| policy | Show a specified partition selection policy. |
| for-console-user | Show the specified partition selection policy for console port login user. |
| for-remote-user | Show the partition selection policy for remote user. |
| interface | User partition selection policy interface. |
| <PARTITION_INTERFACE> | User authentication interface name. Example: <i>X1</i> |
| zone | User partition selection policy zone. |
| <PARTITION_ZONE_NAME> | User authentication zone name. Example: <i>LAN</i> |
| address-object | User partition selection policy address object. |
| ipv6 | IPv6 addresses. |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| any | Any. |
| group | Address object group. |
| <PARTITION_ADDR_MIXED_GROUP_NAME> | User authentication address-object name. Example: <i>X0 Subnets</i> |

| | |
|--|---|
| name | Address object name. |
| <PARTITION_ADDR_MIXED_NAME> | User authentication address-object name. Example: <i>X0 Subnet</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show user partitioning
show user partitioning partitions
show user partitioning partition mypartition1
show user partitioning policies
show user partitioning policy for-remote-user interface X3
show user partitioning policy interface X2 zone LAN
show user partitioning policy for-console-user interface console
```

Syntax

```
show user sso [ agent <SSO_AGENT_HOST_NAME> | agents | radius-accounting-client <SSO_RAD_ACCT_CLIENT_HOST_NAME> | radius-
accounting-clients | statistics [ { agent <SSO_AGENT_HOST_NAME> | all | radius-accounting-client <SSO_RAD_ACCT_CLIENT_HOST_NAME> |
terminal-services-agent <SSO_TS_AGENT_HOST_NAME> } ] | status | terminal-services-agent <SSO_TS_AGENT_HOST_NAME> | terminal-
services-agents ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show SSO settings, status or statistics.

Options

| | |
|--|---|
| agent | Show SSO agent settings. |
| <SSO_AGENT_HOST_NAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Agent</i> |
| agents | Show settings for all SSO agents. |
| radius-accounting-client | Show SSO RADIUS accounting client settings. |
| <SSO_RAD_ACCT_CLIENT_HOST_NAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i> |
| radius-accounting-clients | Show settings for all SSO RADIUS accounting clients. |
| statistics | Show SSO statistics. |
| agent | Show statistics for an SSO agent. |
| <SSO_AGENT_HOST_NAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Agent</i> |
| all | Show all SSO statistics. |
| radius-accounting-client | Show statistics for an SSO RADIUS accounting client. |
| <SSO_RAD_ACCT_CLIENT_HOST_NAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i> |
| terminal-services-agent | Show statistics for an SSO terminal services agent. |
| <SSO_TS_AGENT_HOST_NAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Terminal-Services-Agent</i> |
| status | Show SSO agent status. |
| terminal-services-agent | Show SSO terminal services agent settings. |
| <SSO_TS_AGENT_HOST_NAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Terminal-Services-Agent</i> |

| | |
|---------------------------------|---|
| terminal-services-agents | Show settings for all SSO terminal services agents. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show user sso
show user sso agents
show user sso agent 192.168.168.1
```

Syntax

```
show user guest [ [ profile <GUEST_PROFILE_NAME> | profiles | user [ uuid ] <GUEST_USER_NAME> | users ] [ { pending-config | with-pending-config } ] ] | [ detail { { user <GUEST_USER_NAME> | users } } | statistic user <GUEST_LOGIN_USER_BY_IP> | status { { user <GUEST_LOGIN_USER_BY_IP> | users } } ] ]
```

Mode

All Modes

Description

Show settings for guest profiles/users.

Options

| | |
|---|--|
| profile <GUEST_PROFILE_NAME> | Show a guest user profile. Guest profile name. Example: <i>profile1</i> |
| profiles | Show all guest user profiles. |
| user uuid <GUEST_USER_NAME> | Show a guest user. Show a user object by UUID. Guest user name. Example: <i>guest1</i> |
| users | Show all guest users. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| detail | Show guest user(s) detail. |
| user <GUEST_USER_NAME> | Show guest user detail. Guest user name. Example: <i>guest1</i> |
| users | Show guest users detail. |
| statistic user <GUEST_LOGIN_USER_BY_IP> | Show the logged-in guest users' statistic. Show the logged-in guest user's statistic. IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i> |
| status | Show the logged-in guest users' status. |
| user <GUEST_LOGIN_USER_BY_IP> | Show the logged-in guest user's status. IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i> |
| users | Show the logged-in guest users' status. |

Example

```
show user guest
show user guest users
show user guest user uuid 00000000-0000-0001-0500-c0eae49ce84c
show user guest user jcool
```

Syntax

```
appflow
```

Mode

Config

Description

Enter appflow configuration mode.

Example

```
appflow
```

Syntax

```
clear flow-reporting statistics
```

Mode

AppFlow

Description

Clear flow reporting statistics.

Example

```
clear flow-reporting statistics
```

Syntax

```
default
```

Mode

AppFlow

Description

Clear all settings to default configuration.

Example

```
default
```

Syntax

```
report connections { all | interface-based | rules-based }
```

Mode

AppFlow

Description

Set the type of connections to report.

Options

| | |
|-------------------------------|---------------------------|
| <i>all</i> | All connections. |
| <i>interface-based</i> | Interface based. |
| <i>rules-based</i> | Firewall/app rules based. |

Example

```
report connections rules-based
report connections interface-based
report connections all
```

Syntax

```
real-time data-collection
```

Mode

AppFlow

Description

Enable real-time data collection.

Example

```
real-time data-collection
```

Syntax

```
no real-time data-collection
```

Mode

AppFlow

Description

Disable real-time data collection.

Example

```
no real-time data-collection
```

Syntax

```
real-time collect-for { [ top-applications ] [ bits-per-second ] [ packets-per-second ] [ average-packet-size ] [ connections-per-second ] [ core-utilization ] [ memory-utilization ] }
```

Mode

AppFlow

Description

Enable what to collect real-time data for.

Options

| | |
|--------------------------------------|-------------------------|
| <i>top-applications</i> | Top applications. |
| <i>bits-per-second</i> | Bits per second. |
| <i>packets-per-second</i> | Packets per second. |
| <i>average-packet-size</i> | Average packet size. |
| <i>connections-per-second</i> | Connections per second. |

core-utilization Core utilization.
memory-utilization Memory utilization.

Example

```
real-time collect-for top-apps core-utilization
```

Syntax

```
no real-time collect-for { [ top-applications ] [ bits-per-second ] [ packets-per-second ] [ average-packet-size ] [ connections-per-second ] [ core-utilization ] [ memory-utilization ] }
```

Mode

AppFlow

Description

Disable what to collect real-time data for.

Options

top-applications Top applications.
bits-per-second Bits per second.
packets-per-second Packets per second.
average-packet-size Average packet size.
connections-per-second Connections per second.
core-utilization Core utilization.
memory-utilization Memory utilization.

Example

```
no real-time collect-for top-apps core-utilization
```

Syntax

```
aggregate data-collection
```

Mode

AppFlow

Description

Enable aggregate appflow report data collection.

Example

```
aggregate data-collection
```

Syntax

```
no aggregate data-collection
```

Mode

AppFlow

Description

Disable aggregate appflow report data collection.

Example

```
no aggregate data-collection
```

Syntax

```
aggregate collect-for { [ applications ] [ user ] [ ip ] [ threat ] [ geo-ip ] [ url ] }
```

Mode

AppFlow

Description

Enable what to collect aggregate report data for.

Options

| | |
|---------------------|----------------------|
| applications | Applications report. |
| user | User report. |
| ip | Ip report. |
| threat | Threat report. |
| geo-ip | Geo-IP report. |
| url | URL report. |

Example

```
aggregate collect-for applications user
```

Syntax

```
no aggregate collect-for { [ applications ] [ user ] [ ip ] [ threat ] [ geo-ip ] [ url ] }
```

Mode

AppFlow

Description

Disable what to collect aggregate report data for.

Options

| | |
|---------------------|----------------------|
| applications | Applications report. |
| user | User report. |
| ip | Ip report. |
| threat | Threat report. |
| geo-ip | Geo-IP report. |
| url | URL report. |

Example

```
no aggregate collect-for applications user
```

Syntax

```
flows-to local-collector
```

Mode

AppFlow

Description

Enable sending appflow to local collector.

Example

```
flows-to local-collector
```

Syntax

no flows-to local-collector

Mode

AppFlow

Description

Disable sending appflow to local collector.

Example

no flows-to local-collector

Syntax

report dropped

Mode

AppFlow

Description

Enable report dropped connection.

Example

report dropped

Syntax

no report dropped

Mode

AppFlow

Description

Disable report dropped connection.

Example

no report dropped

Syntax

report stack

Mode

AppFlow

Description

Enable report STACK connection.

Example

report stack

Syntax

no report stack

Mode

AppFlow

Description

Skip reporting STACK connection.

Example

```
no report stack
```

Syntax

```
include-url-types { [ gifs ] [ jpegs ] [ pngs ] [ js ] [ xmls ] [ jsons ] [ css ] [ htmls ] [ aspx ] [ cms ] }
```

Mode

AppFlow

Description

Enable inclusion of specified URL types.

Options

| | |
|---------------------|--------|
| <i>gifs</i> | Gifs. |
| <i>jpegs</i> | Jpegs. |
| <i>pngs</i> | Pngs. |
| <i>js</i> | Js. |
| <i>xmls</i> | Xmls. |
| <i>jsons</i> | Jsons. |
| <i>css</i> | Css. |
| <i>htmls</i> | Htmls. |
| <i>aspx</i> | Aspx. |
| <i>cms</i> | Cms. |

Example

```
include-url-types jpegs htmls
```

Syntax

```
no include-url-types { [ gifs ] [ jpegs ] [ pngs ] [ js ] [ xmls ] [ jsons ] [ css ] [ htmls ] [ aspx ] [ cms ] }
```

Mode

AppFlow

Description

Disable inclusion of specified URL types.

Options

| | |
|---------------------|--------|
| <i>gifs</i> | Gifs. |
| <i>jpegs</i> | Jpegs. |
| <i>pngs</i> | Pngs. |
| <i>js</i> | Js. |
| <i>xmls</i> | Xmls. |
| <i>jsons</i> | Jsons. |
| <i>css</i> | Css. |
| <i>htmls</i> | Htmls. |
| <i>aspx</i> | Aspx. |
| <i>cms</i> | Cms. |

Example

```
no include-url-types jpegs htmls
```

Syntax

geo-ip-resolution

Mode

AppFlow

Description

Enable geo-ip and name resolution.

Example

geo-ip-resolution

Syntax

no geo-ip-resolution

Mode

AppFlow

Description

Disable geo-ip and name resolution.

Example

no geo-ip-resolution

Syntax

report ipv6-flows

Mode

AppFlow

Description

Enable reporting IPv6 flows (all).

Example

report ipv6-flows

Syntax

no report ipv6-flows

Mode

AppFlow

Description

Disable reporting IPv6 flows (all).

Example

no report ipv6-flows

Syntax

```
report upload-timeout <UINT8>
```

Mode

AppFlow

Description

Set the appflow report upload timeout in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
report upload-timeout 120
```

Syntax

```
gmsflow-server
```

Mode

AppFlow

Description

Enter GMS flow server configuration mode.

Example

```
gmsflow-server
```

Syntax

```
flows
```

Mode

GMSFlow Server

Description

Enable sending appflow to SonicWALL GMS flow server.

Example

```
flows
```

Syntax

```
no flows
```

Mode

GMSFlow Server

Description

Disable sending appflow to SonicWALL GMS flow server.

Example

```
no flows
```

Syntax

real-time

Mode

GMSFlow Server

Description

Enable sending of real-time data to SonicWALL GMS flow server.

Example

real-time

Syntax

no real-time

Mode

GMSFlow Server

Description

Disable sending of real-time flows to SonicWALL GMS flow server.

Example

no real-time

Syntax

report open

Mode

GMSFlow Server

Description

Enable report on connection OPEN.

Example

report open

Syntax

no report open

Mode

GMSFlow Server

Description

Disable report on connection OPEN.

Example

no report open

Syntax

```
report close
```

Mode

GMSFlow Server

Description

Enable report on connection CLOSE.

Example

```
report close
```

Syntax

```
no report close
```

Mode

GMSFlow Server

Description

Disable report on connection CLOSE.

Example

```
no report close
```

Syntax

```
report update { [ threat ] [ application ] [ user ] [ vpn-tunnel ] [ url ] }
```

Mode

GMSFlow Server

Description

Enable report connections on the specified updates.

Options

| | |
|--------------------|------------------------|
| threat | Threat detection. |
| application | Application detection. |
| user | User detection. |
| vpn-tunnel | VPN tunnel detection. |
| url | URL detection. |

Example

```
report update application user
```

Syntax

```
no report update { [ threat ] [ application ] [ user ] [ vpn-tunnel ] [ url ] }
```

Mode

GMSFlow Server

Description

Disable report connections on the specified updates.

Options

| | |
|--------------------|------------------------|
| threat | Threat detection. |
| application | Application detection. |
| user | User detection. |
| vpn-tunnel | VPN tunnel detection. |
| url | URL detection. |

Example

```
no report update application user
```

Syntax

```
dynamic-flows { [ connections ] [ users ] [ urls ] [ url-ratings ] [ vpns ] [ devices ] [ spams ] [ locations ] [ voips ] }
```

Mode

GMSFlow Server

Description

Enable send dynamic appflow for specified tables.

Options

| | |
|--------------------|--------------|
| connections | Connections. |
| users | Users. |
| urls | URLs. |
| url-ratings | URL ratings. |
| vpns | VPNs. |
| devices | Devices. |
| spams | SPAMs |
| locations | Locations. |
| voips | VOIPs. |

Example

```
dynamic-flows connections users urls
```

Syntax

```
no dynamic-flows { [ connections ] [ users ] [ urls ] [ url-ratings ] [ vpns ] [ devices ] [ spams ] [ locations ] [ voips ] }
```

Mode

GMSFlow Server

Description

Disable send dynamic appflow for specified tables.

Options

| | |
|--------------------|--------------|
| connections | Connections. |
| users | Users. |
| urls | URLs. |
| url-ratings | URL ratings. |
| vpns | VPNs. |
| devices | Devices. |
| spams | SPAMs |
| locations | Locations. |
| voips | VOIPs. |

Example

```
no dynamic-flows connections users urls
```

Syntax

server-ip

Mode

GMSFlow Server

Description

Enter GMS flow server IP configuration mode.

Example

server-ip

Syntax

ip <IPV4_HOST>

Mode

GMSFlow Server IP

Description

Set GMS flow server IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

ip 10.10.10.200

Syntax

vpn-source-ip <IPV4_HOST>

Mode

GMSFlow Server IP

Description

Set source IP to use for GMS flow server on a VPN tunnel.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

vpn-source-ip 10.10.10.110

Syntax

communication-timeout <UINT8>

Mode

GMSFlow Server IP

Description

Set the GMS flow server communication timeout in seconds.

Options

<*UINT8*> Integer in the form: D OR 0xHH.
Example: 123

Example

```
communication-timeout 60
```

Syntax

```
auto-synchronize
```

Mode

GMSFlow Server IP

Description

Enable auto-synchronize for GMS flow server.

Example

```
auto-synchronize
```

Syntax

```
no auto-synchronize
```

Mode

GMSFlow Server IP

Description

Disable auto-synchronize for GMS flow server.

Example

```
no auto-synchronize
```

Syntax

```
synchronize
```

Mode

GMSFlow Server IP

Description

Synchronize GMS flow server.

Example

```
synchronize
```

Syntax

```
test-connectivity
```

Mode

GMSFlow Server IP

Description

Test connectivity of GMS flow server.

Example

```
test-connectivity
```

Syntax

```
appflow-server
```

Mode

AppFlow

Description

Enter appflow server configuration mode.

Example

```
appflow-server
```

Syntax

```
flows
```

Mode

AppFlow Server

Description

Enable sending appflow to SonicWALL appflow server.

Example

```
flows
```

Syntax

```
no flows
```

Mode

AppFlow Server

Description

Disable sending appflow to SonicWALL appflow server.

Example

```
no flows
```

Syntax

```
real-time
```

Mode

AppFlow Server

Description

Enable sending of real-time data to SonicWALL appflow server.

Example

```
real-time
```

Syntax

```
no real-time
```

Mode

AppFlow Server

Description

Disable sending of real-time data to SonicWALL appflow server.

Example

```
no real-time
```

Syntax

```
report open
```

Mode

AppFlow Server

Description

Enable report on connection OPEN.

Example

```
report open
```

Syntax

```
no report open
```

Mode

AppFlow Server

Description

Disable report on connection OPEN.

Example

```
no report open
```

Syntax

```
report close
```

Mode

AppFlow Server

Description

Enable report on connection CLOSE.

Example

```
report close
```

Syntax

```
no report close
```

Mode

AppFlow Server

Description

Disable report on connection CLOSE.

Example

```
no report close
```

Syntax

```
report update { [ threat ] [ application ] [ user ] [ vpn-tunnel ] [ url ] }
```

Mode

AppFlow Server

Description

Enable report connections on the specified updates.

Options

| | |
|--------------------|------------------------|
| threat | Threat detection. |
| application | Application detection. |
| user | User detection. |
| vpn-tunnel | VPN tunnel detection. |
| url | URL detection. |

Example

```
report update application user
```

Syntax

```
no report update { [ threat ] [ application ] [ user ] [ vpn-tunnel ] [ url ] }
```

Mode

AppFlow Server

Description

Disable report connections on the specified updates.

Options

| | |
|--------------------|------------------------|
| threat | Threat detection. |
| application | Application detection. |
| user | User detection. |
| vpn-tunnel | VPN tunnel detection. |
| url | URL detection. |

Example

no report update application user

Syntax

dynamic-flows { [connections] [users] [urls] [url-ratings] [vpns] [devices] [spams] [locations] [voips] }

Mode

AppFlow Server

Description

Enable send dynamic appflow for specified tables.

Options

connections Connections.
users Users.
urls URLs.
url-ratings URL ratings.
vpns VPNs.
devices Devices.
spams SPAMs
locations Locations.
voips VOIPs.

Example

dynamic-flows connections users urls

Syntax

no dynamic-flows { [connections] [users] [urls] [url-ratings] [vpns] [devices] [spams] [locations] [voips] }

Mode

AppFlow Server

Description

Disable send dynamic appflow for specified tables.

Options

connections Connections.
users Users.
urls URLs.
url-ratings URL ratings.
vpns VPNs.
devices Devices.
spams SPAMs
locations Locations.
voips VOIPs.

Example

no dynamic-flows connections users urls

Syntax

server-ip

Mode

AppFlow Server

Description

Enter appflow server IP configuration mode.

Example

```
server-ip
```

Syntax

```
keep-alive
```

Mode

AppFlow Server IP

Description

Enable keep-alive with appflow server.

Example

```
keep-alive
```

Syntax

```
no keep-alive
```

Mode

AppFlow Server IP

Description

Disable keep-alive with appflow server.

Example

```
no keep-alive
```

Syntax

```
ip <IPV4_HOST>
```

Mode

AppFlow Server IP

Description

Set appflow server IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
ip 10.10.10.200
```

Syntax

```
vpn-source-ip <IPV4_HOST>
```

Mode

AppFlow Server IP

Description

Set source IP to use for appflow server on a VPN tunnel.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
vpn-source-ip 10.10.10.110
```

Syntax

```
max-flows <UINT32>
```

Mode

AppFlow Server IP

Description

Set the appflow server maximum flows.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
max-flows 500000
```

Syntax

```
communication-timeout <UINT8>
```

Mode

AppFlow Server IP

Description

Set the appflow server communication timeout in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
communication-timeout 60
```

Syntax

```
firewall-name <WORD>
```

Mode

AppFlow Server IP

Description

Set the appflow server firewall name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
firewall-name "My Sonicwall"
```

Syntax

```
passphrase <ENC_PASSWORD>
```

Mode

AppFlow Server IP

Description

Set the connection passphrase.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
passphrase reveal2noone
```

Syntax

```
no passphrase
```

Mode

AppFlow Server IP

Description

Clear the connection passphrase.

Example

```
no passphrase
```

Syntax

```
auto-synchronize
```

Mode

AppFlow Server IP

Description

Enable auto-synchronize for appflow server.

Example

```
auto-synchronize
```

Syntax

```
no auto-synchronize
```

Mode

AppFlow Server IP

Description

Disable auto-synchronize for appflow server.

Example

```
no auto-synchronize
```

Syntax

```
synchronize
```

Mode

AppFlow Server IP

Description

Synchronize appflow server.

Example

```
synchronize
```

Syntax

```
test-connectivity
```

Mode

AppFlow Server IP

Description

Test connectivity of appflow server.

Example

```
test-connectivity
```

Syntax

```
flush server <IPV4_HOST>
```

Mode

AppFlow Server IP

Description

Flush specified appflow server.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
flush server 192.168.168.166
```

Syntax

flush servers

Mode

AppFlow Server IP

Description

Flush all discovered appflow servers.

Example

flush servers

Syntax

discover <ASSIGNED_INTERFACE>

Mode

AppFlow Server IP

Description

Discover appflow servers.

Options

<ASSIGNED_INTERFACE> Interface name.
Example: *X0*

Example

discover interfaceId

Syntax

external-collector

Mode

AppFlow

Description

Enter external collector configuration mode.

Example

external-collector

Syntax

flows

Mode

External Collector

Description

Enable sending appflow and real-time data to external collector.

Example

flows

Syntax

```
no flows
```

Mode

External Collector

Description

Disable sending appflow and real-time data to external collector.

Example

```
no flows
```

Syntax

```
reporting-format { ipfix | ipfix-with-extensions | netflow-5 | netflow-9 }
```

Mode

External Collector

Description

Set the external appflow reporting format.

Options

| | |
|-------------------------------------|------------------------|
| <i>ipfix</i> | IPFIX. |
| <i>ipfix-with-extensions</i> | IPFIX with extensions. |
| <i>netflow-5</i> | Netflow version 5. |
| <i>netflow-9</i> | Netflow version 9. |

Example

```
reporting-format ipfix
```

Syntax

```
ip <IPV4_HOST>
```

Mode

External Collector

Description

Set external collector IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
ip 10.10.10.200
```

Syntax

```
vpn-source-ip <IPV4_HOST>
```


Mode

External Collector

Description

Set source IP to use for external collector on a VPN tunnel.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
vpn-source-ip 10.10.10.110
```

Syntax

```
port <UINT16>
```

Mode

External Collector

Description

Set external collector UDP port number.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
port 2055
```

Syntax

```
send templates
```

Mode

External Collector

Description

Enable sending of netflow/ipfix templates at regular intervals.

Example

```
send templates
```

Syntax

```
no send templates
```

Mode

External Collector

Description

Disable sending of netflow/ipfix templates at regular intervals.

Example

```
no send templates
```

Syntax

send static-flows

Mode

External Collector

Description

Enable sending of static appflow at regular intervals.

Example

send static-flows

Syntax

no send static-flows

Mode

External Collector

Description

Disable sending of static appflow at regular intervals.

Example

no send static-flows

Syntax

```
static-flows { [ applications ] [ viruses ] [ spyware ] [ intrusions ] [ location-map ] [ services ] [ rating-map ] [ table-map ] [ column-map ] }
```

Mode

External Collector

Description

Enable tables to send static appflows for.

Options

applications Applications.
viruses Viruses.
spyware Spyware.
intrusions Intrusions.
location-map Location map.
services Services.
rating-map Rating map.
table-map Table map.
column-map Column map.

Example

static-flows applications spyware

Syntax

```
no static-flows { [ applications ] [ viruses ] [ spyware ] [ intrusions ] [ location-map ] [ services ] [ rating-map ] [ table-map ] [ column-map ] }
```

Mode

External Collector

Description

Disable tables to send static appflows for.

Options

| | |
|---------------------|---------------|
| applications | Applications. |
| viruses | Viruses. |
| spyware | Spyware. |
| intrusions | Intrusions. |
| location-map | Location map. |
| services | Services. |
| rating-map | Rating map. |
| table-map | Table map. |
| column-map | Column map. |

Example

```
no static-flows applications spyware
```

Syntax

```
dynamic-flows { [ connections ] [ users ] [ urls ] [ url-ratings ] [ vpns ] [ devices ] [ spams ] [ locations ] [ voips ] }
```

Mode

External Collector

Description

Enable tables to send dynamic appflows for.

Options

| | |
|--------------------|--------------|
| connections | Connections. |
| users | Users. |
| urls | URLs. |
| url-ratings | URL ratings. |
| vpns | VPNs. |
| devices | Devices. |
| spams | SPAMs |
| locations | Locations. |
| voips | VOIPs. |

Example

```
dynamic-flows applications spyware
```

Syntax

```
no dynamic-flows { [ connections ] [ users ] [ urls ] [ url-ratings ] [ vpns ] [ devices ] [ spams ] [ locations ] [ voips ] }
```

Mode

External Collector

Description

Disable tables to send dynamic appflows for.

Options

connections Connections.
users Users.
urls URLs.
url-ratings URL ratings.
vpns VPNs.
devices Devices.
spams SPAMs
locations Locations.
voips VOIPs.

Example

```
no dynamic-flows applications spyware
```

Syntax

```
ipfix-reports { [ top-10-apps ] [ interface-statistics ] [ core-utilization ] [ memory-utilization ] }
```

Mode

External Collector

Description

Enable including of specified additional reports via IPFIX.

Options

top-10-apps Top 10 applications.
interface-statistics Interface statistics.
core-utilization Core utilization.
memory-utilization Memory utilization.

Example

```
ipfix-reports top-10-apps memory-utilization
```

Syntax

```
no ipfix-reports { [ top-10-apps ] [ interface-statistics ] [ core-utilization ] [ memory-utilization ] }
```

Mode

External Collector

Description

Disable including of specified additional reports via IPFIX.

Options

top-10-apps Top 10 applications.
interface-statistics Interface statistics.
core-utilization Core utilization.
memory-utilization Memory utilization.

Example

```
no ipfix-reports top-10-apps memory-utilization
```

Syntax

```
report open
```

Mode

External Collector

Description

Enable report on connection OPEN.

Example

```
report open
```

Syntax

```
no report open
```

Mode

External Collector

Description

Disable report on connection OPEN.

Example

```
no report open
```

Syntax

```
report close
```

Mode

External Collector

Description

Enable report on connection CLOSE.

Example

```
report close
```

Syntax

```
no report close
```

Mode

External Collector

Description

Disable report on connection CLOSE.

Example

```
no report close
```

Syntax

```
report active-timeout <UINT8>
```

Mode

External Collector

Description

Enable report connection on active timeout.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
report active-timeout 60
```

Syntax

```
no report active-timeout
```

Mode

External Collector

Description

Disable report connection on active timeout.

Example

```
no report active-timeout
```

Syntax

```
report kilobytes-exchanged [ kilobytes <UINT16> ] [ once ]
```

Mode

External Collector

Description

Enable report connection on kilobytes exchanged.

Options

kilobytes Specify kilobytes.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123
once Report once.

Example

```
report kilobytes-exchanged kilobytes 100  
report kilobytes-exchanged  
report kilobytes-exchanged kilobytes 200 once
```

Syntax

```
no report kilobytes-exchanged [ once ]
```

Mode

External Collector

Description

Disable report connection on kilobytes exchanged.

Options

once Report once.

Example

```
no report kilobytes-exchanged
```

Syntax

```
report update { [ threat ] [ application ] [ user ] [ vpn-tunnel ] [ url ] }
```

Mode

External Collector

Description

Enable report connections on the specified updates.

Options

| | |
|--------------------|------------------------|
| threat | Threat detection. |
| application | Application detection. |
| user | User detection. |
| vpn-tunnel | VPN tunnel detection. |
| url | URL detection. |

Example

```
report update application user
```

Syntax

```
no report update { [ threat ] [ application ] [ user ] [ vpn-tunnel ] [ url ] }
```

Mode

External Collector

Description

Disable report connections on the specified updates.

Options

| | |
|--------------------|------------------------|
| threat | Threat detection. |
| application | Application detection. |
| user | User detection. |
| vpn-tunnel | VPN tunnel detection. |
| url | URL detection. |

Example

```
no report update application user
```

Syntax

```
generate all-templates
```

Mode

External Collector

Description

Generate all templates.

Example

generate all-templates

Syntax

generate static-appflow-data

Mode

External Collector

Description

Generate static appflow data.

Example

generate static-appflow-data

Syntax

```
show appflow [ [ appflow-server | external-collector | gmsflow-server ] [ { pending-config | with-pending-config } ] | statistics  
[ { external | internal | ipfix } ] | status [ { appflow-server | gmsflow-server } ] ]
```

Mode

All Modes

Description

Show appflow configuration.

Options

| | |
|-----------------------------------|---|
| <i>appflow-server</i> | Show appflow server configuration. |
| <i>external-collector</i> | Show external collector configuration. |
| <i>gmsflow-server</i> | Show GMS flow server configuration. |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |
| <i>statistics</i> | Show appflow statistics. |
| <i>external</i> | Show external flow reporting statistics. |
| <i>internal</i> | Show internal appflow reporting statistics. |
| <i>ipfix</i> | Show total IPFIX statistics. |
| <i>status</i> | Show appflow status. |
| <i>appflow-server</i> | Show appflow server status. |
| <i>gmsflow-server</i> | Show GMS flow server status. |

Example

show appflow

Syntax

certificates

Mode

Config

Description

Certificate configuration.

Example

certificates

Syntax

```
export signing-request <CERT_NAME> { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

Certificates

Description

Export certificate signing request.

Options

<CERT_NAME> Certificate name.
Example: *my_cert*

ftp Export using the FTP protocol.

<FTP_URL> FTP URL in the form: ftp://username:password@hostname\n Escape character: '!' -> '\\!', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: *ftp://username:password@hostname\nftp://username@hostname\nftp://hostname/*

scp Export using the SCP protocol.

<SCP_URL> SCP URL in the form: scp://username@host\n Escape character: '!' -> '\\!', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: *scp://username@host\nscp://host/*

Example

```
export signing-request "Corp VPN Cert" ftp ftp://ftp.myserver.local/cert.p10  
export signing-request "Corp VPN Cert" scp scp://myserver.local/cert.p10
```

Syntax

```
export cert-key-pair <CERT_NAME> password <WORD> { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

Certificates

Description

Export certificate signing request or certificate / key pair.

Options

<CERT_NAME> Certificate name.
Example: *my_cert*

password Password of the PKCS#12 (.p12 or .pfx) encoded file.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

ftp Export using the FTP protocol.

<FTP_URL> FTP URL in the form: ftp://username:password@hostname\n Escape character: '!' -> '\\!', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: *ftp://username:password@hostname\nftp://username@hostname\nftp://hostname/*

scp Export using the SCP protocol.

<SCP_URL> SCP URL in the form: scp://username@host\n Escape character: '!' -> '\\!', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: *scp://username@host\nscp://host/*

Example

```
export cert-key-pair "Corp VPN Cert" password pwd ftp ftp://ftp.myserver.local/cert.p12
export cert-key-pair "Corp VPN Cert" password pwd scp scp://myserver.local/cert.p12
```

Syntax

```
import cert-key-pair <WORD> password <WORD> { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

Certificates

Description

Import certificate / key pair.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

password Password of the PKCS#12 (.p12 or .pfx) encoded file.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

ftp Import using the FTP protocol.

<FTP_URL> FTP URL in the form: ftp://username:password@hostname/ Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: *ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/*

scp Import using the SCP protocol.

<SCP_URL> SCP URL in the form: scp://username@host/ Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: *scp://username@host/\\nscp://host/*

Example

```
import cert-key-pair "Corp VPN Cert" password pwd ftp ftp://ftp.myserver.local/cert.p12
import cert-key-pair "Corp VPN Cert" password pwd scp scp://myserver.local/cert.p12
```

Syntax

```
import ca-cert { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

Certificates

Description

Import CA certificate.

Options

ftp Import using the FTP protocol.

<FTP_URL> FTP URL in the form: ftp://username:password@hostname/ Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: *ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/*

scp Import using the SCP protocol.

<SCP_URL> SCP URL in the form: scp://username@host/ Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: *scp://username@host/\\nscp://host/*

Example

```
import ca-cert ftp ftp://ftp.myserver.local/cacert.crt
import ca-cert scp scp://myserver.local/cacert.crt
```

Syntax

```
import signed-cert <CERT_NAME> { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

Certificates

Description

Import CA signed certificate.

Options

<CERT_NAME> Certificate name.
Example: *my_cert*

ftp Import using the FTP protocol.

<FTP_URL> FTP URL in the form: *ftp://username:password@hostname/* Escape character: *'-' -> '\\\\', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'*.
Example: *ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/*

scp Import using the SCP protocol.

<SCP_URL> SCP URL in the form: *scp://username@host/* Escape character: *'-' -> '\\\\', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'*.
Example: *scp://username@host/\\nscp://host/*

Example

```
import signed-cert "Corp VPN Cert" ftp ftp://ftp.myserver.local/cert.crt
import signed-cert "Corp VPN Cert" scp scp://myserver.local/cert.crt
```

Syntax

```
import crl ca-name <CERT_NAME> { [ disable-invalidate-certificates | invalidate-certificates ] [ directly { ftp <FTP_URL> | scp
<SCP_URL> } | periodically <WEB_URL> ] }
```

Mode

Certificates

Description

Import certificate revocation list or set the location to periodically download via HTTP.

Options

ca-name CA certificate associated with CRL.

<CERT_NAME> Certificate name.
Example: *my_cert*

disable-invalidate-certificates Disable invalidate certificates and security associations if CRL import or processing fails.

invalidate-certificates Invalidate certificates and security associations if CRL import or processing fails.

directly Import CRL directly from a PEM (.pem) or DER (.der or .crl) encoded file.

ftp Import using the FTP protocol.

<FTP_URL> FTP URL in the form: *ftp://username:password@hostname/* Escape character: *'-' -> '\\\\', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'*.
Example: *ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/*

scp Import using the SCP protocol.

<SCP_URL> SCP URL in the form: *scp://username@host/* Escape character: *'-' -> '\\\\', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'*.
Example: *scp://username@host/\\nscp://host/*

periodically Periodically auto-import CRL via HTTP.

<WEB_URL> URL in the form: *http://host/file*.
Example: *http://www.example.com/products/*

Example

```
import crl ca-name "Corp CA Cert" directly ftp ftp://ftp.myserver.local/cert.crl
import crl ca-name "Corp CA Cert" invalidate-certificates
```

Syntax

```
no certificate <CERT_NAME>
```

Mode

Certificates

Description

Delete CA certificate, signing request or certificate / key pair.

Options

<CERT_NAME> Certificate name.
Example: *my_cert*

Example

```
no certificate "Corp VPN Cert"
```

Syntax

```
no certificates
```

Mode

Certificates

Description

Delete all imported CA certificates, signing requests or certificate / key pairs.

Example

```
no certificates
```

Syntax

```
generate-signing-request
```

Mode

Certificates

Description

Enter certificate signing request configuration mode.

Example

```
generate-signing-request
```

Syntax

```
no enrollment
```

Mode

Certificates

Description

Stop enrollment for signing request.

Example

```
no enrollment
```

Syntax

scep

Mode

Certificates

Description

Enter simple certificate enrollment protocol configuration mode.

Example

scep

Syntax

alias <WORD>

Mode

Signing Request

Description

Configure certificate signing request alias.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

alias "MyCertAlias"

Syntax

distinguished-name element1 { country <CERT_COUNTRY> | locality <WORD> | organization <WORD> | state <WORD> }

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

country Country. Adds C=country-name to distinguished name.
<CERT_COUNTRY> Certificate signing request country.
Example: *afghanistan*

locality Locality, City, or County. Adds L=locality-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

organization Company or organization. Adds O=organization-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

state State. Adds ST=state-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
distinguished-name element1 country US
```

Syntax

```
distinguished-name element2 { country <CERT_COUNTRY> | department <WORD> | locality <WORD> | organization <WORD> | state <WORD> }
```

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

| | |
|-----------------------------|--|
| country | Country. Adds C=country-name to distinguished name. |
| <CERT_COUNTRY> | Certificate signing request country. Example: <i>afghanistan</i> |
| department | Department. Adds OU=department-name to distinguished name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| locality | Locality, City, or County. Adds L=locality-name to distinguished name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| organization | Company or organization. Adds O=organization-name to distinguished name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| state | State. Adds ST=state-name to distinguished name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

Example

```
distinguished-name element2 state CA
```

Syntax

```
distinguished-name element3 { department <WORD> | group <WORD> | locality <WORD> | organization <WORD> | team <WORD> }
```

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

| | |
|---------------------|--|
| department | Department. Adds OU=department-name to distinguished name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| group | Group. Adds OU=group-name to distinguished name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| locality | Locality, City, or County. Adds L=locality-name to distinguished name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

organization Company or organization. Adds O=organization-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

team Team. Adds OU=team-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
distinguished-name element3 locality "San Jose"
```

Syntax

```
distinguished-name element4 { common-name <WORD> | department <WORD> | email <WORD> | group <WORD> | organization <WORD> | serial <WORD> | team <WORD> }
```

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

common-name Common Name. Adds CN=common-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

department Department. Adds OU=department-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

email E-mail Address. Adds Email=email-address to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

group Group. Adds OU=group-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

organization Company or organization. Adds O=organization-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

serial Serial Number. Adds SN=serial-number to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

team Team. Adds OU=team-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
distinguished-name element4 organization "My company"
```

Syntax

```
distinguished-name element5 { common-name <WORD> | department <WORD> | email <WORD> | group <WORD> | serial <WORD> | team <WORD> }
```

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

common-name Common Name. Adds CN=common-name to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

department Department. Adds OU=department-name to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

email E-mail Address. Adds Email=email-address to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

group Group. Adds OU=group-name to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

serial Serial Number. Adds SN=serial-number to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

team Team. Adds OU=team-name to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
distinguished-name element5 department "Department"
```

Syntax

```
distinguished-name element6 { common-name <WORD> | email <WORD> | group <WORD> | serial <WORD> | team <WORD> }
```

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

common-name Common Name. Adds CN=common-name to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

email E-mail Address. Adds Email=email-address to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

group Group. Adds OU=group-name to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

serial Serial Number. Adds SN=serial-number to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

team Team. Adds OU=team-name to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example


```
distinguished-name element6 group "Group"
```

Syntax

```
distinguished-name element7 { common-name <WORD> | email <WORD> | serial <WORD> | team <WORD> }
```

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

common-name Common Name. Adds CN=common-name to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

email E-mail Address. Adds Email=email-address to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

serial Serial Number. Adds SN=serial-number to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

team Team. Adds OU=team-name to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
distinguished-name element7 team "Team"
```

Syntax

```
distinguished-name element8 { common-name <WORD> | email <WORD> | serial <WORD> }
```

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

common-name Common Name. Adds CN=common-name to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

email E-mail Address. Adds Email=email-address to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

serial Serial Number. Adds SN=serial-number to distinguished name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
distinguished-name element8 email admin@mycompany.local
```

Syntax

```
alternate-name { domain-name <HOSTNAME> | email-address <EMAIL> | ipv4-address <IPV4_HOST> }
```

Mode

Signing Request

Description

Configure certificate signing request alternate name.

Options

| | |
|--------------------------|--|
| domain-name | Domain name. |
| <HOSTNAME> | Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i> |
| email-address | E-mail address. |
| <EMAIL> | E-mail in the form: aaaa@bbb.com. Example: <i>support@sonicwall.com</i> |
| ipv4-address | IP address. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |

Example

```
alternate-name ipv4-address 10.10.10.10
```

Syntax

```
signature-algorithm { md5 | sha-1 | sha-256 | sha-384 | sha-512 }
```

Mode

Signing Request

Description

Configure certificate signing request signature algorithm.

Options

| | |
|----------------|---------|
| md5 | MD5. |
| sha-1 | SHA1. |
| sha-256 | SHA256. |
| sha-384 | SHA384. |
| sha-512 | SHA512. |

Example

```
signature-algorithm sha-1
```

Syntax

```
key type { ecdsa | rsa }
```

Mode

Signing Request

Description

Configure certificate signing request subject key type.

Options

ecdsa ECDSA.

rsa RSA.

Example

```
key type rsa
```

Syntax

```
key size { 1024 | 1536 | 2048 | 256 | 384 | 4096 | 521 }
```

Mode

Signing Request

Description

Configure certificate signing request subject key size.

Options

1024 1024 bits.

1536 1536 bits.

2048 2048 bits.

256 prime256v1: X9.62/SECG curve over a 256 bit prime field.

384 secp384r1: NIST/SECG curve over a 384 bit prime field.

4096 4096 bits.

521 secp521r1: NIST/SECG curve over a 521 bit prime field.

Example

```
key size rsa 1024
```

Syntax

```
generate
```

Mode

Signing Request

Description

Generate certificate signing request.

Example

```
generate
```

Syntax

```
signing-request <CERT_NAME>
```

Mode

SCEP

Description

Configure simple certificate enrollment protocol signing request.

Options

<CERT_NAME> Certificate name.
Example: *my_cert*

Example

```
signing-request srlocal
```

Syntax

```
ca-url <WEB_URL>
```

Mode

SCEP

Description

Configure simple certificate enrollment protocol certificate authority URL.

Options

<WEB_URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

```
ca-url http://scep.mydomain.local
```

Syntax

```
challenge-password <WORD>
```

Mode

SCEP

Description

Configure simple certificate enrollment protocol certificate authority challenge password.

Options

<WORD> Word in the form: WORD or "QUOTED STRING".
Example: *abc*

Example

```
challenge-password secret
```

Syntax

```
request-count <UINT16>
```

Mode

SCEP

Description

Configure simple certificate enrollment protocol request count.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
request-count 256
```

Syntax

```
polling-interval <UINT16>
```

Mode

SCEP

Description

Configure simple certificate enrollment protocol polling interval.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
polling-interval 30
```

Syntax

```
max-polling-time <UINT16>
```

Mode

SCEP

Description

Configure simple certificate enrollment protocol max polling time.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
max-polling-time 28800
```

Syntax

```
scep
```

Mode

SCEP

Description

Enable simple certificate enrollment protocol.

Example

```
scep
```

Syntax

```
show certificates status [ build-in [ with-expired ] | imported ]
```

Mode

All Modes

Description

Show certificates status.

Options

| | |
|---------------------|--|
| status | Show certificates status. |
| build-in | Show build in certificates. |
| with-expired | Include expired build in certificates. |
| imported | Show imported certificates. |

Example

```
show certificates status
```

Syntax

```
show certificate name <CERT_NAME> status
```

Mode

All Modes

Description

Show certificate status.

Options

| | |
|--------------------------|--|
| name | Certificate name. |
| <CERT_NAME> | Certificate name. Example: <i>my_cert</i> |
| status | Show certificate status. |

Example

```
show certificate name EchoCERT status
```

Syntax

```
high-availability
```

Mode

Config

Description

Enter high availability configuration mode.

Example

```
high-availability
```

Syntax

```
heartbeat-interval <UINT32>
```

Mode

High Availability

Description

Set heartbeat interval in milliseconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
heartbeat-interval 5000
```

Syntax

```
failover-trigger-level <UINT8>
```

Mode

High Availability

Description

Set failover trigger level (missed heartbeats).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
failover-trigger-level 5
```

Syntax

```
probe interval <UINT8>
```

Mode

High Availability

Description

Set probe interval in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
probe interval 20
```

Syntax

```
probe count <UINT8>
```

Mode

High Availability

Description

Set probe count.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
probe count 3
```

Syntax

```
election-delay-time <UINT8>
```

Mode

High Availability

Description

Set election delay time in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
election-delay-time 3
```

Syntax

```
route-hold-down-time <UINT8>
```

Mode

High Availability

Description

Set dynamic route hold-down time in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
route-hold-down-time 3
```

Syntax

```
no route-hold-down-time
```

Mode

High Availability

Description

Clear dynamic route hold-down time.

Example

```
no route-hold-down-time
```

Syntax

```
failover-when-aggregate-down
```

Mode

High Availability

Description

Enable failover only when all aggregate links are down.

Example

```
failover-when-aggregate-down
```

Syntax

```
no failover-when-aggregate-down
```

Mode

High Availability

Description

Disable failover only when all aggregate links are down.

Example

```
no failover-when-aggregate-down
```

Syntax

```
enable node <VIRTUAL_GROUP_ID>
```

Mode

High Availability

Description

Enable specified ha cluster node.

Options

<VIRTUAL_GROUP_ID> Integer in the form: D OR 0xHH.
Example: 1

Example

```
enable node 2
```

Syntax

```
no enable node <VIRTUAL_GROUP_ID>
```

Mode

High Availability

Description

Disable specified ha cluster node.

Options

<VIRTUAL_GROUP_ID> Integer in the form: D OR 0xHH.
Example: 1

Example

```
no enable node 2
```

Syntax

```
include-certificates-keys
```

Mode

High Availability

Description

Enable include certificates and keys.

Example

```
include-certificates-keys
```

Syntax

```
no include-certificates-keys
```

Mode

High Availability

Description

Disable include certificates and keys.

Example

```
no include-certificates-keys
```

Syntax

```
synchronize settings
```

Mode

High Availability

Description

Synchronize settings.

Example

```
synchronize settings
```

Syntax

```
synchronize firmware
```

Mode

High Availability

Description

Synchronize firmware.

Example

```
synchronize firmware
```

Syntax

```
force-failover
```

Mode

High Availability

Description

Force HA active/standby failover.

Example

```
force-failover
```

Syntax

```
no mode
```

Mode

High Availability

Description

Disable high availability.

Example

```
no mode
```

Syntax

```
mode { active-active-clustering | active-active-clustering-dpi | active-active-dpi | active-standby }
```

Mode

High Availability

Description

Enable high availability and set high availability mode.

Options

| | |
|--|---|
| <i>active-active-clustering</i> | Active-active clustering mode. |
| <i>active-active-clustering-dpi</i> | Active-active clustering with DPI mode. |
| <i>active-active-dpi</i> | Active-active DPI mode. |
| <i>active-standby</i> | Active-standby mode. |

Example

```
mode active-standby
```

Syntax

```
primary-serial <MAC>
```

Mode

Active Standby
Active Active Dpi

Description

Set high availability primary serial number.

Options

<MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD

Example

```
primary-serial 0017C5010203
```

Syntax

```
secondary-serial <MAC>
```

Mode

Active Standby
Active Active Dpi

Description

Set high availability secondary serial number.

Options

<MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD

Example

```
secondary-serial 0017C5040506
```

Syntax

```
no secondary-serial
```

Mode

Active Standby
Active Active Dpi

Description

Clear high availability secondary serial number.

Example

```
no secondary-serial
```

Syntax

```
node-num <UINT8>
```

Mode

Active Active Clustering
Active Active Clustering Dpi

Description

Set active-active cluster node number (2-4).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
node-num 3
```

Syntax

```
rank node <VIRTUAL_GROUP_ID> virtual-group <VIRTUAL_GROUP_ID> [ rank ] { none | owner | standby | standby2 | standby3 }
```

Mode

Active Active Clustering
Active Active Clustering Dpi

Description

Set the rank of ownership of virtual group for the node.

Options

<VIRTUAL_GROUP_ID> Integer in the form: D OR 0xHH.
Example: 1

virtual-group Virtual group.

<VIRTUAL_GROUP_ID> Integer in the form: D OR 0xHH.
Example: 1

rank rank.

none No assignment.

owner Owner.

standby Standby.

standby2 Standby2.

standby3 Standby3.

Example

```
rank node 1 virtual-group 1 owner
```

Syntax

```
serial node <VIRTUAL_GROUP_ID> { primary <MAC> | secondary <MAC> }
```

Mode

Active Active Clustering
Active Active Clustering Dpi

Description

Set active-active cluster node serial number..

Options

<VIRTUAL_GROUP_ID> Integer in the form: D OR 0xHH.
Example: 1

primary Primary serial number.

<MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD

secondary Secondary serial number.
<MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
serial node 2 primary 0017C5010203
```

Syntax

```
no serial node <VIRTUAL_GROUP_ID> { primary | secondary }
```

Mode

Active Active Clustering
Active Active Clustering Dpi

Description

Remove active-active cluster node serial number.

Options

<VIRTUAL_GROUP_ID> Integer in the form: D OR 0xHH.
Example: *1*

primary Primary serial number.

secondary Secondary serial number.

Example

```
no serial node 2 primary
```

Syntax

```
stateful-synchronization
```

Mode

Active Standby
Active Active Clustering

Description

Enable stateful synchronization.

Example

```
stateful-synchronization
```

Syntax

```
no stateful-synchronization
```

Mode

Active Standby
Active Active Clustering

Description

Disable stateful synchronization.

Example

```
no stateful-synchronization
```

Syntax

```
dpi-interface <DPI_INTERFACE_ID> <HA_DATA_INTERFACE>
```

Mode

Active Active Dpi
Active Active Clustering Dpi

Description

Configure active/active DPI interface.

Options

<DPI_INTERFACE_ID> Integer in the form: D OR 0xHH.
Example: 1

<HA_DATA_INTERFACE> Interface name.
Example: X0

Example

```
dpi-interface 1 X5
```

Syntax

```
no dpi-interface <DPI_INTERFACE_ID>
```

Mode

Active Active Dpi
Active Active Clustering Dpi

Description

Clear active/active DPI interface.

Options

<DPI_INTERFACE_ID> Integer in the form: D OR 0xHH.
Example: 1

Example

```
no dpi-interface 1
```

Syntax

```
control-interface <HA_LINK_INTERFACE>
```

Mode

Active Standby
Active Active Dpi
Active Active Clustering
Active Active Clustering Dpi

Description

Configure HA control interface.

Options

<HA_LINK_INTERFACE> Interface name.
Example: X0

Example

```
control-interface X5
```

Syntax

no control-interface

Mode

Active Standby
Active Active Dpi
Active Active Clustering
Active Active Clustering Dpi

Description

Clear HA control interface.

Example

no control-interface

Syntax

data-interface <HA_DATA_INTERFACE>

Mode

Active Standby
Active Active Dpi
Active Active Clustering
Active Active Clustering Dpi

Description

Configure HA data interface.

Options

<HA_DATA_INTERFACE> Interface name.
Example: *X0*

Example

data-interface X5

Syntax

no data-interface

Mode

Active Standby
Active Active Dpi
Active Active Clustering
Active Active Clustering Dpi

Description

Clear HA data interface.

Example

no data-interface

Syntax

switched-link

Mode

Description

Enable switched active/active cluster link.

Example

```
switched-link
```

Syntax

```
no switched-link
```

Mode

Active Active Clustering
Active Active Clustering Dpi

Description

Disable switched active/active cluster link.

Example

```
no switched-link
```

Syntax

```
active-active-cluster-link <SVRRP_LINK> <HA_LINK_INTERFACE>
```

Mode

Active Active Clustering
Active Active Clustering Dpi

Description

Configure active/active cluster link.

Options

| | |
|----------------------------------|---|
| <SVRRP_LINK> | Integer in the form: D OR 0xHH. Example: 1 |
| <HA_LINK_INTERFACE> | Interface name. Example: X0 |

Example

```
active-active-cluster-link 2 X5
```

Syntax

```
no active-active-cluster-link <SVRRP_LINK>
```

Mode

Active Active Clustering
Active Active Clustering Dpi

Description

Clear active/active cluster link.

Options

| | |
|---------------------------|---|
| <SVRRP_LINK> | Integer in the form: D OR 0xHH. Example: 1 |
|---------------------------|---|

Example

```
no active-active-cluster-link 2
```

Syntax

```
preempt
```

Mode

Active Standby
Active Active Dpi

Description

Enable preempt mode.

Example

```
preempt
```

Syntax

```
no preempt
```

Mode

Active Standby
Active Active Dpi

Description

Disable preempt mode.

Example

```
no preempt
```

Syntax

```
encryption
```

Mode

Active Standby
Active Active Dpi

Description

Enable encryption for control communication.

Example

```
encryption
```

Syntax

```
no encryption
```

Mode

Active Standby
Active Active Dpi

Description

Disable encryption for control communication.

Example

no encryption

Syntax

generate-backup-firmware

Mode

Active Standby
Active Active Dpi
Active Active Clustering
Active Active Clustering Dpi

Description

Enable generate/overwrite backup firmware and settings when upgrading firmware.

Example

generate-backup-firmware

Syntax

no generate-backup-firmware

Mode

Active Standby
Active Active Dpi
Active Active Clustering
Active Active Clustering Dpi

Description

Disable generate/overwrite backup firmware and settings when upgrading firmware.

Example

no generate-backup-firmware

Syntax

enable-encryption

Mode

Active Standby
Active Active Dpi

Description

Enable encryption for control communication.

Example

enable-encryption

Syntax

no enable-encryption

Mode

Active Standby
Active Active Dpi

Description

Disable encryption for control communication.

Example

```
no enable-encryption
```

Syntax

```
virtual-mac
```

Mode

Active Standby
Active Active Dpi

Description

Enable virtual MAC.

Example

```
virtual-mac
```

Syntax

```
no virtual-mac
```

Mode

Active Standby
Active Active Dpi

Description

Disable virtual MAC.

Example

```
no virtual-mac
```

Syntax

```
monitoring
```

Mode

High Availability

Description

High availability monitoring.

Example

```
monitoring
```

Syntax

```
monitoring interface [ ipv4 | ipv6 ] <HA_MONITOR_INTERFACE>
```

Mode

High Availability

Description

Enter high availability monitoring configuration mode.

Options

| | |
|---|---|
| <code>ipv4</code> | High availability monitoring interface IPv4. |
| <code>ipv6</code> | High availability monitoring interface IPv6. |
| <code><HA_MONITOR_INTERFACE></code> | HA monitoring interface name. Example: <code>X0</code> |

Example

```
monitoring interface X1
```

Syntax

```
svrrp
```

Mode

High Availability

Description

High availability monitoring.

Example

```
svrrp
```

Syntax

```
svrrp monitoring node <VIRTUAL_GROUP_ID> interface <HA_MONITOR_INTERFACE>
```

Mode

High Availability

Description

Enter high availability monitoring configuration mode.

Options

| | |
|---|--|
| <code><VIRTUAL_GROUP_ID></code> | Integer in the form: D OR 0xHH. Example: <code>1</code> |
| <code>interface</code> | High availability monitoring interface. |
| <code><HA_MONITOR_INTERFACE></code> | HA monitoring interface name. Example: <code>X0</code> |

Example

```
monitoring node 1 interface X1
```

Syntax

```
link-monitoring
```

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Enable physical/link monitoring.

Example

```
link-monitoring
```

Syntax

```
no link-monitoring
```

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Disable physical/link monitoring.

Example

```
no link-monitoring
```

Syntax

```
no primary
```

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Clear primary interface monitoring IP address.

Example

```
no primary
```

Syntax

```
primary <HOST_IP>
```

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Set primary interface monitoring IP address.

Options

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

```
primary fe80::1001  
primary 192.168.168.211
```

Syntax

```
no secondary
```

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Clear secondary interface monitoring IP address.

Example

```
no secondary
```

Syntax

```
secondary <HOST_IP>
```

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Set secondary interface monitoring IP address.

Options

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

```
secondary fe80::1001  
secondary 192.168.168.211
```

Syntax

```
allow-management
```

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Enable allow management on primary/secondary IP address.

Example

```
allow-management
```

Syntax

```
no allow-management
```

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Disable allow management on primary/secondary IP address.

Example

```
no allow-management
```

Syntax

logical-probe <HOST_IP>

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Enable logical/probe and set IP address.

Options

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

```
logical-probe fe80::1001
logical-probe 192.168.168.211
```

Syntax

no logical-probe

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Disable logical/probe.

Example

```
no logical-probe
```

Syntax

override-virtual-mac <MAC>

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Enable override virtual MAC and set MAC.

Options

<MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
override-virtual-mac 02:17:c5:01:02:03
```

Syntax

no override-virtual-mac

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Disable override virtual MAC.

Example

```
no override-virtual-mac
```

Syntax

```
link-monitoring
```

Mode

High Availability Clustering Monitoring

Description

Enable physical/link monitoring.

Example

```
link-monitoring
```

Syntax

```
no link-monitoring
```

Mode

High Availability Clustering Monitoring

Description

Disable physical/link monitoring.

Example

```
no link-monitoring
```

Syntax

```
no primary
```

Mode

High Availability Clustering Monitoring

Description

Clear primary interface monitoring IP address.

Example

```
no primary
```

Syntax

```
primary <IPv4_HOST>
```

Mode

High Availability Clustering Monitoring

Description

Set primary interface monitoring IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
primary 192.168.168.211
```

Syntax

```
no secondary
```

Mode

High Availability Clustering Monitoring

Description

Clear secondary interface monitoring IP address.

Example

```
no secondary
```

Syntax

```
secondary <IPV4_HOST>
```

Mode

High Availability Clustering Monitoring

Description

Set secondary interface monitoring IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
secondary 192.168.168.212
```

Syntax

```
allow-management
```

Mode

High Availability Clustering Monitoring

Description

Enable allow management on primary/secondary IP address.

Example

```
allow-management
```

Syntax

no allow-management

Mode

High Availability Clustering Monitoring

Description

Disable allow management on primary/secondary IP address.

Example

no allow-management

Syntax

logical-probe <IPV4_HOST>

Mode

High Availability Clustering Monitoring

Description

Enable logical/probe and set IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

logical-probe 10.10.10.10

Syntax

no logical-probe

Mode

High Availability Clustering Monitoring

Description

Disable logical/probe.

Example

no logical-probe

Syntax

show high-availability [monitoring [ipv4 | ipv6] [interface <HA_MONITOR_INTERFACE>] | status] [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show high availability configuration and status.

Options

| | |
|-------------------------------------|---|
| monitoring | Show high availability monitoring interface. |
| ipv4 | Show only IPv4 high availability monitoring interface. |
| ipv6 | Show only IPv6 high availability monitoring interface. |
| interface | Show high availability monitoring interface. |
| <HA_MONITOR_INTERFACE> | HA monitoring interface name. Example: X0 |
| status | Show high availability status. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show high-availability
```

Syntax

```
export log { csv | txt } { ftp <FTP_URL> | zmodem }
```

Mode

Top Level

Description

Export log from the device using zmodem or FTP.

Options

| | |
|------------------------|---|
| csv | CSV format. |
| txt | Text format. |
| ftp | Use ftp. |
| <FTP_URL> | FTP URL in the form: ftp://username:password@hostname/ Escape character: ' -> '\\', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/ |
| zmodem | Use zmodem. |

Example

```
export log ftp ftp://ftp.myserver.local/log.wri
```

Syntax

```
clear log
```

Mode

All Modes
Top Level

Description

Clear all log entries.

Example

```
clear log
```

Syntax

```
email log
```

Mode

Config

Description

Send log to configured e-mail address.

Example

```
email log
```

Syntax

```
log display { max-number <UINT32> | time-range { all | last <UINT8> { days | hours | minutes } } }
```

Mode

Config

Description

Configure time range and max number for showing log view in CLI.

Options

max-number Max number
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

time-range Time range.

all All entries.

last Last time range.
<UINT8> Integer in the form: D OR 0xHH.
Example: 123

days Days.

hours Hours.

minutes Minutes.

Example

```
log display max-number 100  
log display time-range last 5 minutes
```

Syntax

```
log event-id <LOG_EVENT_ID_FOR_ATTRIBUTES>
```

Mode

Config

Description

Enter log event configuration mode with specified event ID.

Options

<LOG_EVENT_ID_FOR_ATTRIBUTES> Event ID for showing the attributes.
Example: 123

Example

```
log event-id 440
```

Syntax

```
log category <LOG_CATEGORY_NAME> [ group <LOG_GROUP_NAME> [ event <LOG_EVENT_NAME> ] ]
```

Mode

Config

Description

Enter log category configuration mode.

Options

| | |
|----------------------------------|--|
| <LOG_CATEGORY_NAME> | Log category name. Example: <i>Firewall</i> |
| group | Group configuration. |
| <LOG_GROUP_NAME> | Group name. Example: <i>Firewall Event</i> |
| event | Event configuration. |
| <LOG_EVENT_NAME> | Event name. Example: <i>Activate Firewall</i> |

Example

```
log category VPN
log category "Admin System" group GMS
log category Firewall group "Firewall Rule" event "Firewall Add"
```

Syntax

```
log categories
```

Mode

Config

Description

Enter log categories configuration mode.

Example

```
log categories
```

Syntax

```
log syslog
```

Mode

Config

Description

Enter syslog configuration mode.

Example

```
log syslog
```

Syntax

log automation

Mode

Config

Description

Enter log automation configuration mode.

Example

log automation

Syntax

log name-resolution

Mode

Config

Description

Enter log name resolution configuration mode.

Example

log name-resolution

Syntax

log reports

Mode

Config

Description

Enter log reports configuration mode.

Example

log reports

Syntax

log viewpoint

Mode

Config

Description

Enter viewpoint configuration mode.

Example

log viewpoint

Syntax

log analyzer

Mode

Config

Description

Enter analyzer configuration mode.

Example

log analyzer

Syntax

save-template <WORD>

Mode

Log Categories

Description

Save current log event settings in custom template.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

save-template "Current event log company specific default settings"

Syntax

import-template { *analyzer-viewpoint-gms* | *custom* | *default* | *minimal* }

Mode

Log Categories

Description

Set log event settings to what is specified in the template.

Options

analyzer-viewpoint-gms Set event log settings to work well with analyzer / viewpoint / GMS server.

custom Set event log settings to previously saved settings.

default Restore all event log settings to default values.

minimal Set event log settings so that a minimal amount of logs are created.

Example

import-template default

Syntax

reset event-count { *all* | *category* <LOG_CATEGORY_NAME> [*group* <LOG_GROUP_NAME> [*event* <LOG_EVENT_NAME>]] | *event-id* <LOG_EVENT_ID_FOR_ATTRIBUTES> }

Mode

Log Categories

Description

Reset the event counters for specified category.

Options

| | |
|--|--|
| all | All categories. |
| category <LOG_CATEGORY_NAME> | Specify category. Log category name. Example: <i>Firewall</i> |
| group <LOG_GROUP_NAME> | Specify group. Group name. Example: <i>Firewall Event</i> |
| event <LOG_EVENT_NAME> | Specify event. Event name. Example: <i>Activate Firewall</i> |
| event-id <LOG_EVENT_ID_FOR_ATTRIBUTES> | Specify event ID. Event ID for showing the attributes. Example: <i>123</i> |

Example

```
reset event-count all
reset event-count category VPN
```

Syntax

```
logging-level { alert | critical | debug | emergency | error | inform | notice | warning }
```

Mode

Log Categories

Description

Set global logging level.

Options

| | |
|------------------|------------|
| alert | Alert. |
| critical | Critical. |
| debug | Debug. |
| emergency | Emergency. |
| error | Error. |
| inform | Inform. |
| notice | Notice. |
| warning | Warning. |

Example

```
logging-level critical
```

Syntax

```
alert-level { alert | critical | emergency | error | warning }
```

Mode

Log Categories

Description

Set alert level.

Options

alert Alert.

critical Critical.

emergency Emergency.

error Error.

warning Warning.

Example

```
alert-level critical
```

Syntax

```
global-category-attribute
```

Mode

Log Categories

Description

Enter global category attributes configuration mode.

Example

```
global-category-attribute
```

Syntax

```
priority-level { alert | critical | debug | emergency | error | inform | mixed | notice | warning }
```

Mode

Log Categories Global Attributes

Description

Set priority level.

Options

alert Alert.

critical Critical.

debug Debug.

emergency Emergency.

error Error.

inform Inform.

mixed Mixed.

notice Notice.

warning Warning.

Example

```
priority-level critical
```

Syntax

```
log-monitor [ mixed ] [ redundancy-interval <UINT32> ]
```

Mode

Log Categories Global Attributes

Description

Enable display in Log Monitor of categories and optionally set redundancy filter.

Options

| | |
|---|---|
| mixed | Mixed. |
| redundancy-interval <UINT32> | Set the redundancy interval in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |

Example

```
log-monitor redundancy-interval 60
```

Syntax

```
no log-monitor
```

Mode

Log Categories Global Attributes

Description

Disable display in Log Monitor of categories.

Example

```
no log-monitor
```

Syntax

```
email-alert [ mixed ] [ redundancy-interval <UINT32> ]
```

Mode

Log Categories Global Attributes

Description

Enable send events as Email Alerts and optionally set redundancy filter.

Options

| | |
|---|---|
| mixed | Mixed. |
| redundancy-interval <UINT32> | Set the redundancy interval in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |

Example

```
email-alert redundancy-interval 60
```

Syntax

```
no email-alert
```

Mode

Log Categories Global Attributes

Description

Disable send events as Email Alerts.

Example

```
no email-alert
```

Syntax

```
syslog [ mixed ] [ redundancy-interval <UINT32> ]
```

Mode

Log Categories Global Attributes

Description

Enable report events via Syslog and optionally set redundancy filter.

Options

| | |
|----------------------------|--|
| mixed | Mixed. |
| redundancy-interval | Set the redundancy interval in seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |

Example

```
syslog redundancy-interval 60
```

Syntax

```
no syslog
```

Mode

Log Categories Global Attributes

Description

Disable report events via Syslog.

Example

```
no syslog
```

Syntax

```
event-profile { mixed | syslog-server-profile <SYSLOG_SERVER_PROFILE> }
```

Mode

Log Categories Global Attributes

Description

Set syslog server profile of categories.

Options

| | |
|--------------------------------------|------------------------------------|
| <i>mixed</i> | Mixed profile. |
| <i>syslog-server-profile</i> | Specify the syslog server profile. |
| <SYSLOG_SERVER_PROFILE> | Syslog server profile. |

Example

```
event-profile syslog-server-profile 0
```

Syntax

```
ipfix [ mixed ] [ keep-original-redundancy-interval | redundancy-interval <UINT32> ]
```

Mode

Log Categories Global Attributes

Description

Enable ipfix of categories and optionally set redundancy filter.

Options

| | |
|--|--|
| <i>mixed</i> | Mixed. |
| <i>keep-original-redundancy-interval</i> | Keep original redundancy filter interval. |
| <i>redundancy-interval</i> <UINT32> | Set the redundancy interval in seconds. Integer in the form: D OR 0xHHHHHHHH. Example: 123 |

Example

```
ipfix redundancy-interval 60
```

Syntax

```
no ipfix
```

Mode

Log Categories Global Attributes

Description

Disable ipfix of categories.

Example

```
no ipfix
```

Syntax

```
log-digest [ mixed ]
```

Mode

Log Categories Global Attributes

Description

Include events in Log Digest.

Options

mixed Mixed.

Example

```
log-digest
```

Syntax

```
no log-digest
```

Mode

Log Categories Global Attributes

Description

Exclude events in Log Digest.

Example

```
no log-digest
```

Syntax

```
color { black | blue | green | hex <HEX_UINT32> | leave-unchanged | orange | purple | red | rgb <UINT8> <UINT8> <UINT8> | yellow }
```

Mode

Log Categories Global Attributes

Description

Set the color of the category to be displayed in the Log Monitor.

Options

| | |
|---------------------------|--|
| black | Black. |
| blue | Blue. |
| green | Green. |
| hex | Hex representation. |
| <HEX_UINT32> | Hexadecimal integer in the form: 0xHHHHHHHH. Example: <i>0xaa55aa55</i> |
| leave-unchanged | Leave the original color unchanged. |
| orange | Orange. |
| purple | Purple. |
| red | Red. |
| rgb | Red, green, blue scale. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| yellow | Yellow. |

Example

```
color black
color hex 0x00111333
color rgb 3 5 7
```

Syntax

```
log-email { address <EMAIL> | leave-unchanged }
```

Mode

Log Categories Global Attributes

Description

Set Email address of all log events to send log to.

Options

| | |
|----------------------|--|
| address | Specify the log Email address. |
| <EMAIL> | E-mail in the form: aaaa@bbb.com. Example: <i>support@sonicwall.com</i> |

leave-unchanged Leave the original log email address unchanged.

Example

```
log-email address categoriesadmin@utm.local
```

Syntax

```
no log-email
```

Mode

Log Categories Global Attributes

Description

Clear Email address of all log events to send log to.

Example

```
no log-email
```

Syntax

```
alert-email { address <EMAIL> | leave-unchanged }
```

Mode

Log Categories Global Attributes

Description

Set Alert Email address of all log events to send log to.

Options

| | |
|----------------------|--|
| address | Specify the alert Email address. |
| <EMAIL> | E-mail in the form: aaaa@bbb.com. Example: <i>support@sonicwall.com</i> |

leave-unchanged Leave the original alert email address unchanged.

Example

```
alert-email address categoriesadmin@utm.local
```

Syntax

```
no alert-email
```

Mode

Log Categories Global Attributes

Description

Clear Alert Email address of all log events to send alert to.

Example

```
no alert-email
```

Syntax

```
priority-level { alert | critical | debug | emergency | error | inform | mixed | notice | warning }
```

Mode

Log Category

Description

Set priority level.

Options

alert Alert.

critical Critical.

debug Debug.

emergency Emergency.

error Error.

inform Inform.

mixed Mixed.

notice Notice.

warning Warning.

Example

```
priority-level critical
```

Syntax

```
log-monitor [ mixed ] [ redundancy-interval <UINT32> ]
```

Mode

Log Category

Description

Enable display in Log Monitor of category and optionally set redundancy filter.

Options

| | |
|-----------------------------------|--|
| <i>mixed</i> | Events under this are of mixed settings. |
| <i>redundancy-interval</i> | Set the redundancy interval in seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |

Example

```
log-monitor redundancy-interval 60
log-monitor mixed redundancy-interval 90
log-monitor mixed
```

Syntax

```
no log-monitor
```

Mode

Log Category

Description

Disable display in Log Monitor.

Example

```
no log-monitor
```

Syntax

```
email-alert [ mixed ] [ redundancy-interval <UINT32> ]
```

Mode

Log Category

Description

Enable send events as Email Alerts and optionally set redundancy filter.

Options

| | |
|-----------------------------------|--|
| <i>mixed</i> | Events under this are of mixed settings. |
| <i>redundancy-interval</i> | Set the redundancy interval in seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |

Example

```
email-alert redundancy-interval 60
```

Syntax

```
no email-alert
```

Mode

Log Category

Description

Disable send events as Email Alerts.

Example

```
no email-alert
```

Syntax

```
syslog [ mixed ] [ redundancy-interval <UINT32> ]
```

Mode

Log Category

Description

Enable report events via Syslog and optionally set redundancy filter.

Options

| | |
|----------------------------|--|
| mixed | Events under this are of mixed settings. |
| redundancy-interval | Set the redundancy interval in seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |

Example

```
syslog redundancy-interval 60
```

Syntax

```
no syslog
```

Mode

Log Category

Description

Disable report events via Syslog.

Example

```
no syslog
```

Syntax

```
event-profile { mixed | syslog-server-profile <SYSLOG_SERVER_PROFILE> }
```

Mode

Log Category

Description

Set syslog server profile of category.

Options

| | |
|--------------------------------------|------------------------------------|
| mixed | Mixed profile. |
| syslog-server-profile | Specify the syslog server profile. |
| <SYSLOG_SERVER_PROFILE> | Syslog server profile. |

Example

```
event-profile syslog-server-profile 0
```

Syntax

```
ipfix [ mixed ] [ redundancy-interval <UINT32> ]
```

Mode

Log Category

Description

Enable ipfix of category and optionally set redundancy filter.

Options

| | |
|----------------------------|--|
| mixed | Categories under this are of mixed settings. |
| redundancy-interval | Set the redundancy interval in seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |

Example

```
ipfix redundancy-interval 60
```

Syntax

```
no ipfix
```

Mode

Log Category

Description

Disable ipfix of category.

Example

```
no ipfix
```

Syntax

```
log-digest [ mixed ]
```

Mode

Log Category

Description

Include events in Log Digest.

Options

| | |
|--------------|--|
| mixed | Events under this are of mixed settings. |
|--------------|--|

Example

```
log-digest
```

Syntax

```
no log-digest
```

Mode

Log Category

Description

Exclude events in Log Digest.

Example

```
no log-digest
```

Syntax

```
color { black | blue | green | hex <HEX_UINT32> | leave-unchanged | orange | purple | red | rgb <UINT8> <UINT8> <UINT8> | yellow }
```

Mode

Log Category

Description

Set the color of the category to be displayed in the Log Monitor.

Options

| | |
|---------------------------|---|
| black | Black. |
| blue | Blue. |
| green | Green. |
| hex | Hex representation. |
| <HEX_UINT32> | Hexadecimal integer in the form: 0xHHHHHHHH. Example: 0xaa55aa55 |
| leave-unchanged | Leave unchanged. |
| orange | Orange. |
| purple | Purple. |
| red | Red. |
| rgb | Red, green, blue scale. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| yellow | Yellow. |

Example

```
color black
color leave-unchanged
color hex 0x00111333
color rgb 3 5 7
```

Syntax

```
log-email <EMAIL>
```

Mode

Log Category

Description

Set e-mail address to send log of this category to.

Options

<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: support@sonicwall.com

Example

```
log-email categoryadmin@utm.local
```

Syntax

```
no log-email
```

Mode

Log Category

Description

Clear e-mail address to send log of this category to.

Example

```
no log-email
```

Syntax

```
alert-email { address <EMAIL> | leave-unchanged }
```

Mode

Log Category

Description

Set alert e-mail address to send category to.

Options

| | |
|----------------------|--|
| address | Specify the alert e-mail address. |
| <EMAIL> | E-mail in the form: aaaaa@bbb.com. Example: support@sonicwall.com |

leave-unchanged Leave the original setting for children categories unchanged.

Example

```
alert-email address categoryadmin@utm.local
```

Syntax

```
no alert-email
```

Mode

Log Category

Description

Clear e-mail address to send alert of this category to.

Example

```
no alert-email
```

Syntax

```
priority-level { alert | critical | debug | emergency | error | inform | mixed | notice | warning }
```

Mode

Log Group

Description

Set priority level.

Options

| | |
|------------------|------------|
| alert | Alert. |
| critical | Critical. |
| debug | Debug. |
| emergency | Emergency. |
| error | Error. |
| inform | Inform. |
| mixed | Mixed. |
| notice | Notice. |
| warning | Warning. |

Example

```
priority-level critical
```

Syntax

```
log-monitor [ mixed ] [ redundancy-interval <UINT32> ]
```

Mode

Log Group

Description

Enable display in Log Monitor of group and optionally set redundancy filter.

Options

| | |
|----------------------------|--|
| mixed | Events under this are of mixed settings. |
| redundancy-interval | Set the redundancy interval in seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |

Example

```
log-monitor redundancy-interval 60  
log-monitor mixed redundancy-interval 90  
log-monitor mixed
```

Syntax

```
no log-monitor
```

Mode

Log Group

Description

Disable display in Log Monitor.

Example

```
no log-monitor
```

Syntax

```
email-alert [ mixed ] [ redundancy-interval <UINT32> ]
```

Mode

Log Group

Description

Enable send events as Email Alerts and optionally set redundancy filter.

Options

| | |
|----------------------------|--|
| mixed | Events under this are of mixed settings. |
| redundancy-interval | Set the redundancy interval in seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |

Example

```
email-alert redundancy-interval 60
```

Syntax

```
no email-alert
```

Mode

Log Group

Description

Disable send events as Email Alerts.

Example

```
no email-alert
```

Syntax

```
syslog [ mixed ] [ redundancy-interval <UINT32> ]
```

Mode

Log Group

Description

Enable report events via Syslog and optionally set redundancy filter.

Options

| | |
|----------------------------|--|
| mixed | Events under this are of mixed settings. |
| redundancy-interval | Set the redundancy interval in seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |

Example

```
syslog redundancy-interval 60
```

Syntax

```
no syslog
```

Mode

Log Group

Description

Disable report events via Syslog.

Example

```
no syslog
```

Syntax

```
event-profile { mixed | syslog-server-profile <SYSLOG_SERVER_PROFILE> }
```

Mode

Log Group

Description

Set syslog server profile of group.

Options

- mixed** Mixed profile.
- syslog-server-profile** Specify the syslog server profile.
- <SYSLOG_SERVER_PROFILE>** Syslog server profile.

Example

```
event-profile syslog-server-profile 0
```

Syntax

```
ipfix [ mixed ] [ redundancy-interval <UINT32> ]
```

Mode

Log Group

Description

Enable ipfix of group and optionally set redundancy filter.

Options

- mixed** Categories under this are of mixed settings.
- redundancy-interval** Set the redundancy interval in seconds.
- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
ipfix redundancy-interval 60
```

Syntax

no ipfix

Mode

Log Group

Description

Disable ipfix of group.

Example

no ipfix

Syntax

log-digest [mixed]

Mode

Log Group

Description

Include events in Log Digest.

Options

mixed Events under this are of mixed settings.

Example

log-digest

Syntax

no log-digest

Mode

Log Group

Description

Exclude events in Log Digest.

Example

no log-digest

Syntax

color { black | blue | green | hex <HEX_UINT32> | leave-unchanged | orange | purple | red | rgb <UINT8> <UINT8> <UINT8> | yellow }

Mode

Log Group

Description

Set the color of the group to be displayed in the Log Monitor.

Options

black Black.

blue Blue.

| | |
|---------------------------|--|
| green | Green. |
| hex | Hex representation. |
| <HEX_UINT32> | Hexadecimal integer in the form: 0xHHHHHHHH. Example: <i>0xaa55aa55</i> |
| leave-unchanged | Leave unchanged. |
| orange | Orange. |
| purple | Purple. |
| red | Red. |
| rgb | Red, green, blue scale. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| yellow | Yellow. |

Example

```
color black
color hex 0x00111333
color rgb 3 5 7
```

Syntax

```
alert-email { address <EMAIL> | leave-unchanged }
```

Mode

Log Group

Description

Set alert e-mail address to send group to.

Options

| | |
|----------------------|---|
| address | Specify the alert e-mail address. |
| <EMAIL> | E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i> |

leave-unchanged Leave the original setting for children categories unchanged.

Example

```
alert-email address groupadmin@utm.local
```

Syntax

```
no alert-email
```

Mode

Log Group

Description

Clear e-mail address to send alert of this group to.

Example

`no alert-email`

Syntax

`priority-level { alert | critical | debug | emergency | error | inform | notice | warning }`

Mode

Log Event

Description

Set priority level.

Options

alert Alert.

critical Critical.

debug Debug.

emergency Emergency.

error Error.

inform Inform.

notice Notice.

warning Warning.

Example

`priority-level critical`

Syntax

`log-monitor [redundancy-interval <UINT32>]`

Mode

Log Event

Description

Enable display in Log Monitor of event and optionally set redundancy filter.

Options

redundancy-interval Set the redundancy interval in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

`log-monitor redundancy-interval 60`
`log-monitor`

Syntax

`no log-monitor`

Mode

Log Event

Description

Disable display in Log Monitor.

Example

```
no log-monitor
```

Syntax

```
email-alert [ redundancy-interval <UINT32> ]
```

Mode

Log Event

Description

Enable send events as Email Alerts and optionally set redundancy filter.

Options

redundancy-interval Set the redundancy interval in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
email-alert redundancy-interval 60
```

Syntax

```
no email-alert
```

Mode

Log Event

Description

Disable send events as Email Alerts.

Example

```
no email-alert
```

Syntax

```
syslog [ redundancy-interval <UINT32> ]
```

Mode

Log Event

Description

Enable report events via Syslog and optionally set redundancy filter.

Options

redundancy-interval Set the redundancy interval in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
syslog redundancy-interval 60
```

Syntax

no syslog

Mode

Log Event

Description

Disable report events via Syslog.

Example

no syslog

Syntax

event-profile syslog-server-profile <SYSLOG_SERVER_PROFILE>

Mode

Log Event

Description

Set syslog server profile of event.

Options

<SYSLOG_SERVER_PROFILE> Syslog server profile.

Example

event-profile syslog-server-profile 0

Syntax

ipfix [redundancy-interval <UINT32>]

Mode

Log Event

Description

Enable ipfix of event and optionally set redundancy filter.

Options

redundancy-interval Set the redundancy interval in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

ipfix redundancy-interval 60

Syntax

no ipfix

Mode

Log Event

Description

Disable ipfix of event.

Example

```
no ipfix
```

Syntax

```
log-digest
```

Mode

Log Event

Description

Include events in Log Digest.

Example

```
log-digest
```

Syntax

```
no log-digest
```

Mode

Log Event

Description

Exclude events in Log Digest.

Example

```
no log-digest
```

Syntax

```
color { black | blue | green | hex <HEX_UINT32> | orange | purple | red | rgb <UINT8> <UINT8> <UINT8> | yellow }
```

Mode

Log Event

Description

Set the color of the event to be displayed in the Log Monitor.

Options

| | |
|---------------------------|---|
| black | Black. |
| blue | Blue. |
| green | Green. |
| hex | Hex representation. |
| <HEX_UINT32> | Hexadecimal integer in the form: 0xHHHHHHHHH. Example: <i>0xaa55aa55</i> |
| orange | Orange. |

| | |
|----------------------|---|
| purple | Purple. |
| red | Red. |
| rgb | Red, green, blue scale. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| yellow | Yellow. |

Example

```
color black
color hex 0x00111333
color rgb 3 5 7
```

Syntax

```
alert-email address <EMAIL>
```

Mode

Log Event

Description

Set alert e-mail address to send event to.

Options

- address** Specify the alert e-mail address.
- <EMAIL>** E-mail in the form: aaaaa@bbb.com.
Example: support@sonicwall.com

Example

```
alert-email address eventadmin@utm.local
```

Syntax

```
no alert-email
```

Mode

Log Event

Description

Clear e-mail address to send alert of this event to.

Example

```
no alert-email
```

Syntax

```
facility { authpriv-messages | clock-daemon-linux-bsd | clock-daemon-solaris | ftp-daemon | generated-internally | kernel | line-
printer-subsystem | local-use0 | local-use1 | local-use2 | local-use3 | local-use4 | local-use5 | local-use6 | local-use7 | log-
alert | log-audit | mail-system | network-news-subsystem | ntp-subsystem | security-authorization-messages | system-daemons |
user-level-messages | uucp-subsystem }
```

Mode

Syslog

Description

Set syslog facility for all the servers.

Options

| | |
|--|---|
| <i>authpriv-messages</i> | AUTHPRIV security/authorization messages. |
| <i>clock-daemon-linux-bsd</i> | Clock daemon (BSP, Linux). |
| <i>clock-daemon-solaris</i> | Clock daemon (solaris). |
| <i>ftp-daemon</i> | FTP daemon. |
| <i>generated-internally</i> | Messages generated internally by syslogd. |
| <i>kernel</i> | Kernel. |
| <i>line-printer-subsystem</i> | Line printer subsystem. |
| <i>local-use0</i> | Local use 0. |
| <i>local-use1</i> | Local use 1. |
| <i>local-use2</i> | Local use 2. |
| <i>local-use3</i> | Local use 3. |
| <i>local-use4</i> | Local use 4. |
| <i>local-use5</i> | Local use 5. |
| <i>local-use6</i> | Local use 6. |
| <i>local-use7</i> | Local use 7. |
| <i>log-alert</i> | Log alert. |
| <i>log-audit</i> | Log audit. |
| <i>mail-system</i> | Mail system. |
| <i>network-news-subsystem</i> | Network news subsystem. |
| <i>ntp-subsystem</i> | NTP subsystem. |
| <i>security-authorization-messages</i> | Security/authorization messages. |
| <i>system-daemons</i> | System daemons. |
| <i>user-level-messages</i> | User-level messages. |
| <i>uucp-subsystem</i> | UUCP subsystem. |

Example

```
facility local-use0
```

Syntax

```
format { arcSight | default | enhanced-syslog | webtrends }
```

Mode

Syslog

Description

Set syslog format for all the servers.

Options

| | |
|-------------------------------|-------------------------|
| <i>arcSight</i> | Arcsight format. |
| <i>default</i> | Default format. |
| <i>enhanced-syslog</i> | Enhanced syslog format. |
| <i>webtrends</i> | Webtrends format. |

Example

```
format default
```

Syntax

```
id <WORD>
```

Mode

Syslog

Description

Set syslog ID for all the servers.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
id firewall
```

Syntax

```
event-rate-limiting <UINT16>
```

Mode

Syslog

Description

Set maximum events per second for all the servers.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
event-rate-limiting 1000
```

Syntax

```
data-rate-limiting <UINT32>
```

Mode

Syslog

Description

Set maximum bytes per second for all the servers.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
data-rate-limiting 10000000
```

Syntax

```
type { analyzer | syslog-server }
```

Mode

Syslog Server

Description

Syslog server type.

Options

analyzer Analyzer server

syslog-server Syslog server

Example

```
type analyzer
```

Syntax

```
facility { authpriv-messages | clock-daemon-linux-bsd | clock-daemon-solaris | ftp-daemon | generated-internally | kernel | line-printer-subsystem | local-use0 | local-use1 | local-use2 | local-use3 | local-use4 | local-use5 | local-use6 | local-use7 | log-alert | log-audit | mail-system | network-news-subsystem | ntp-subsystem | security-authorization-messages | system-daemons | user-level-messages | uucp-subsystem }
```

Mode

Syslog Server

Description

Syslog server facility.

Options

authpriv-messages AUTHPRIV security/authorization messages.

clock-daemon-linux-bsd Clock daemon (BSP, Linux).

clock-daemon-solaris Clock daemon (solaris).

ftp-daemon FTP daemon.

generated-internally Messages generated internally by syslogd.

kernel Kernel.

line-printer-subsystem Line printer subsystem.

| | |
|--|----------------------------------|
| <i>local-use0</i> | Local use 0. |
| <i>local-use1</i> | Local use 1. |
| <i>local-use2</i> | Local use 2. |
| <i>local-use3</i> | Local use 3. |
| <i>local-use4</i> | Local use 4. |
| <i>local-use5</i> | Local use 5. |
| <i>local-use6</i> | Local use 6. |
| <i>local-use7</i> | Local use 7. |
| <i>log-alert</i> | Log alert. |
| <i>log-audit</i> | Log audit. |
| <i>mail-system</i> | Mail system. |
| <i>network-news-subsystem</i> | Network news subsystem. |
| <i>ntp-subsystem</i> | NTP subsystem. |
| <i>security-authorization-messages</i> | Security/authorization messages. |
| <i>system-daemons</i> | System daemons. |
| <i>user-level-messages</i> | User-level messages. |
| <i>uucp-subsystem</i> | UUCP subsystem. |

Example

```
facility local-use0
```

Syntax

```
format { arcSight | default | enhanced-syslog | webtrends }
```

Mode

Syslog Server

Description

Syslog server format.

Options

| | |
|------------------------|-------------------------|
| <i>arcSight</i> | Arcsight format. |
| <i>default</i> | Default format. |
| <i>enhanced-syslog</i> | Enhanced syslog format. |
| <i>webtrends</i> | Webtrends format. |

Example

```
format default
```

Syntax

id <WORD>

Mode

Syslog Server

Description

Syslog server ID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

id firewall

Syntax

event-rate-limiting <UINT16>

Mode

Syslog Server

Description

Enable syslog event rate limiting and set maximum events per second.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

event-rate-limiting 1000

Syntax

no event-rate-limiting

Mode

Syslog Server

Description

Disable syslog event rate limiting and set maximum events per second.

Example

no event-rate-limiting

Syntax

data-rate-limiting <UINT32>

Mode

Syslog Server

Description

Enable syslog data rate limiting and set maximum events per second.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
data-rate-limiting 10000000
```

Syntax

```
no data-rate-limiting
```

Mode

Syslog Server

Description

Disable syslog data rate limiting and set maximum events per second.

Example

```
no data-rate-limiting
```

Syntax

```
enabled
```

Mode

Syslog Server

Description

Enable syslog server.

Example

```
enabled
```

Syntax

```
no enabled
```

Mode

Syslog Server

Description

Disable syslog server.

Example

```
no enabled
```

Syntax

```
ndpp
```

Mode

Syslog

Description

Enable NDPP enforcement for syslog server.

Example

```
ndpp
```

Syntax

```
no ndpp
```

Mode

Syslog

Description

Disable NDPP enforcement for syslog server.

Example

```
no ndpp
```

Syntax

```
syslog-server server { fqdn <ADDR_FQDN> | host <ADDR_HOST> | name <ADDR_FQDNHOST_ADDR> } port <UINT32> profile <SYSLOG_SERVER_PROFILE>
```

Mode

Syslog
Analyzer
Viewpoint

Description

Add/edit syslog server.

Options

| | |
|---|--|
| fqdn <ADDR_FQDN> | Address object full qualified domain name (FQDN). FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| host <ADDR_HOST> | Address object host IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <ADDR_FQDNHOST_ADDR> | Address object name FQDN/host address object name. Example: <i>Web Server</i> |
| port <UINT32> | server port. Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i> |
| profile <SYSLOG_SERVER_PROFILE> | Syslog server profile. Syslog server profile. |

Example

```
syslog-server server name "Syslog Server Public" port 514 profile 0  
syslog-server server host 10.10.10.10 port 514 profile 0
```

Syntax

```
no syslog-server server name <SYSLOG_SERVER> port <SYSLOG_SERVER_PORT> profile <SYSLOG_SERVER_PROFILE>
```

Mode

Syslog
Analyzer
Viewpoint

Description

Delete syslog server.

Options

| | |
|---|---|
| <i>name</i> | Address object name |
| <i><SYSLOG_SERVER></i> | Syslog custom server in the form: hostname OR a.b.c.d. Example: <i>abc</i> |
| <i>port</i> | server port. |
| <i><SYSLOG_SERVER_PORT></i> | Syslog custom server port. Example: <i>80</i> |
| <i>profile</i> | Syslog server profile. |
| <i><SYSLOG_SERVER_PROFILE></i> | Syslog server profile. |

Example

```
no syslog-server server name "Syslog Server Public" port 514 profile 0
```

Syntax

```
no servers
```

Mode

Syslog
Analyzer
Viewpoint

Description

Delete all syslog servers.

Example

```
no servers
```

Syntax

```
profile <SYSLOG_SERVER_PROFILE>
```

Mode

Syslog Server

Description

configure the syslog server profile.

Options

| | |
|---|------------------------|
| <i><SYSLOG_SERVER_PROFILE></i> | Syslog server profile. |
|---|------------------------|

Example

```
profile 0
```

Syntax

```
server { fqdn <ADDR_FQDN> | host <ADDR_HOST> | name <ADDR_FQDNHOST_ADDR> }
```

Mode

Syslog Server

Description

configure the syslog server name.

Options

| | |
|--|---|
| <i>fqdn</i> <ADDR_FQDN> | Address object full qualified domain name (FQDN). FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| <i>host</i> <ADDR_HOST> | Address object host IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <i>name</i> <ADDR_FQDNHOST_ADDR> | Address object name FQDN/host address object name. Example: <i>Web Server</i> |

Example

```
server name "Syslog Server Public"  
server host 10.10.10.10  
server fqdn "*.example.com"
```

Syntax

```
port <UINT32>
```

Mode

Syslog Server

Description

configure the syslog server port.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
port 514
```

Syntax

```
outbound-interface <SYSLOG_SERVER_OUTBOUND_INTERFACE>
```

Mode

Syslog Server

Description

Set the outbound interface.

Options

<SYSLOG_SERVER_OUTBOUND_INTERFACE> Syslog server outbound interface name.
Example: *vpnTunnelInterface*

Example

```
outbound-interface "Remote Office"
```

Syntax

```
no outbound-interface
```

Mode

Syslog Server

Description

Clear the outbound interface.

Example

```
no outbound-interface
```

Syntax

```
local-interface <NETMON_INTERFACE>
```

Mode

Syslog Server

Description

Set the local interface.

Options

<NETMON_INTERFACE> Interface name.
Example: *X0*

Example

```
local-interface X2
```

Syntax

```
no local-interface
```

Mode

Syslog Server

Description

Clear the local interface.

Example

```
no local-interface
```

Syntax

```
email-address { alert | log | user } <EMAIL>
```

Mode

Log Automation

Description

Set E-mail address.

Options

alert Set E-mail address to send alert to.

- log** Set E-mail address to send log to.
- user** Set E-mail address to send user creation and enablement notification to.
- <EMAIL>** E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

Example

```
email-address log admin@somedomain.com
email-address alert admin@somedomain.com
```

Syntax

```
no email-address { alert | log | user }
```

Mode

Log Automation

Description

Clear E-mail address.

Options

- alert** Clear E-mail address to send alert to.
- log** Clear E-mail address to send log to.
- user** Clear E-mail address to send user creation and enablement notification to.

Example

```
no email-address log
no email-address alert
```

Syntax

```
send-log { { daily hour <UINT8> minute <UINT8> | weekly { fri | mon | sat | sun | thu | tue | wed } hour <UINT8> minute <UINT8> | when-full } }
```

Mode

Log Automation

Description

Specify when to send log.

Options

- daily** Daily.
- hour** Hour.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: *123*
- minute** Minute.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: *123*
- weekly** Weekly.
- fri** Day of the week.
- mon** Day of the week.
- sat** Day of the week.

sun Day of the week.

thu Day of the week.

tue Day of the week.

wed Day of the week.

hour Hour.

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

minute Minute.

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

when-full When full.

Example

```
send-log weekly mon hour 07 minute 30
```

Syntax

```
email-format { attachment csv | html | plain-text }
```

Mode

Log Automation

Description

Specify e-mail format.

Options

attachment Attachment.

csv CSV.

html HTML.

plain-text Plain text.

Example

```
email-format plain-text
```

Syntax

```
include-all-log-information
```

Mode

Log Automation

Description

Include all log information.

Example

```
include-all-log-information
```

Syntax

```
no include-all-log-information
```

Mode

Log Automation

Description

Include default log information.

Example

```
no include-all-log-information
```

Syntax

```
health-check-email { address <EMAIL> | body <WORD> | schedule { days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } | subject <WORD> }
```

Mode

Log Automation

Description

Edit health check E-mail settings.

Options

| | |
|-----------------------------------|--|
| address <EMAIL> | Set the health check E-mail address. E-mail in the form: aaaa@bbb.com. Example: <i>support@sonicwall.com</i> |
| body <WORD> | Set the health check E-mail body. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| schedule | Enable E-mail health check and select a schedule. |
| days <SCHED_DAYS> | Schedule object days. Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time <SCHED_TIME_BEGIN> | Schedule object beginning/ending time. Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name <SCHED_NAME> | Schedule object name. Schedule object name. Example: <i>Work Hours</i> |
| subject <WORD> | Set the health check E-mail subject. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

Example

```
health-check-email schedule name "Work Hours"  
health-check-email address aaa@bbb.com  
health-check-email subject "health check email"  
health-check-email body "health check notification"
```

Syntax

```
no health-check-email { address | body | schedule | subject }
```

Mode

Log Automation

Description

Clear health check E-mail settings.

Options

address Clear the health check E-mail address.

body Clear the health check E-mail body.

schedule Disable E-mail health check.

subject Clear the health check E-mail subject.

Example

```
no health-check-email schedule
```

Syntax

```
mail-server <HOSTNAME>
```

Mode

Log Automation

Description

Set mail server IP address or hostname.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
mail-server 192.168.168.204
```

Syntax

```
no mail-server
```

Mode

Log Automation

Description

Clear mail server IP address or hostname.

Example

```
no mail-server
```

Syntax

```
mail-from <EMAIL>
```

Mode

Log Automation

Description

Set E-mail address to mail from.

Options

<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

Example

```
mail-from admin@nsa5000
```

Syntax

```
no mail-from
```

Mode

Log Automation

Description

Clear E-mail address to mail from.

Example

```
no mail-from
```

Syntax

```
authentication-method { { none | pop-before-smtp } }
```

Mode

Log Automation

Description

Specify e-mail server authentication method.

Options

none No authentication.

pop-before-smtp Pop before SMTP.

Example

```
authentication-method pop-before-smtp
```

Syntax

```
pop3-server <LOG_POP3_SERVER_NAME>
```

Mode

Log Automation

Description

POP3 server IP address or hostname.

Options

<LOG_POP3_SERVER_NAME> Log POP3 server name in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

Syntax

```
no pop3-server
```

Mode

Log Automation

Description

Clear POP3 server IP address or hostname.

Example

```
no pop3-server
```

Syntax

```
pop3-user-name <WORD>
```

Mode

Log Automation

Description

Specify username for authentication.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
pop3-user-name user
```

Syntax

```
no pop3-user-name
```

Mode

Log Automation

Description

Clear specify username for authentication.

Example

```
no pop3-user-name
```

Syntax

```
pop3-password <ENC_PASSWORD>
```

Mode

Log Automation

Description

Specify password for authentication.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
pop3-password 123
```

Syntax

```
no pop3-password
```

Mode

Log Automation

Description

Clear specify password for authentication.

Example

```
no pop3-password
```

Syntax

```
test
```

Mode

Log Automation

Description

Check log automation settings.

Example

```
test
```

Syntax

```
mail-server-advanced
```

Mode

Log Automation

Description

Enter mail server advanced mode.

Example

```
mail-server-advanced
```

Syntax

```
smtp-port <IPV4_PORT>
```

Mode

Mail Server Advanced

Description

Set E-mail server SMTP TCP port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
smtp-port 4025
```

Syntax

```
connection-security-method { ssl-tls | start-tls }
```

Mode

Mail Server Advanced

Description

Select a connection security method.

Options

ssl-tls SSL/TLS.

start-tls STARTTLS.

Example

```
connection-security-method ssl-tls
```

Syntax

```
no connection-security-method
```

Mode

Mail Server Advanced

Description

Disable connection security method.

Example

```
no connection-security-method
```

Syntax

```
smtp-authentication
```

Mode

Mail Server Advanced

Description

Enable SMTP authentication.

Example

```
smtp-authentication
```

Syntax

no smtp-authentication

Mode

Mail Server Advanced

Description

Disable SMTP authentication.

Example

no smtp-authentication

Syntax

user-name <WORD>

Mode

Mail Server Advanced

Description

Specify username for authentication.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

user-name mailadmin

Syntax

no user-name

Mode

Mail Server Advanced

Description

Clear username for authentication.

Example

no user-name

Syntax

password <ENC_PASSWORD>

Mode

Mail Server Advanced

Description

Specify password for authentication.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password mailadmin
```

Syntax

```
no password
```

Mode

Mail Server Advanced

Description

Clear password for authentication.

Example

```
no password
```

Syntax

```
solera server { fqdn <ADDR_FQDN> | host <ADDR_HOST> | name <ADDR_FQDNHOST_ADDR> }
```

Mode

Log Automation

Description

Enable solera capture stack integration, enter configuration mode and set solera server.

Options

| | |
|-------------------------------------|--|
| fqdn <ADDR_FQDN> | Set the solera server to fqdn address. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| host <ADDR_HOST> | Set the solera server to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <ADDR_FQDNHOST_ADDR> | Set the solera server as named address object. FQDN/host address object name. Example: <i>Web Server</i> |

Example

```
solera server host 192.168.168.198
```

Syntax

```
no solera
```

Mode

Log Automation

Description

Disable solera capture stack integration and enter configuration mode.

Example

```
no solera
```

Syntax

```
protocol { http | https }
```

Mode

Solera

Description

Set solera server protocol.

Options

http HTTP.

https HTTPS.

Example

```
protocol https
```

Syntax

```
port <IPV4_PORT>
```

Mode

Solera

Description

Set solera port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
port 54443
```

Syntax

```
user <WORD>
```

Mode

Solera

Description

Set solera user.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
user mysolerauser
```

Syntax

```
password <ENC_PASSWORD> confirm-password <ENC_PASSWORD>
```

Mode

Solera

Description

Set solera password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

confirm-password Confirm solera password.

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password mysolerapassword
```

Syntax

```
deepsee-base-url <URL>
```

Mode

Solera

Description

Set deepsee base URL.

Options

<URL> URL in the form: *http://host/file*.
Example: *http://www.example.com/products/*

Example

```
deepsee-base-url https://$host:$port/ws/pcap?  
user=$usr&password=$pwd&method=deepsee&start=$start&stop=$stop&ipproto=$ipproto&srcip=$srcip&dstip=$dstip&srcport=$srcport&dstport=
```

Syntax

```
pcap-base-url <URL>
```

Mode

Solera

Description

Set PCAP base URL.

Options

<URL> URL in the form: *http://host/file*.
Example: *http://www.example.com/products/*

Example

```
pcap-base-url https://$host:$port/ws/pcap?  
user=$usr&password=$pwd&method=filename&start=$start&stop=$stop&ipproto=$ipproto&srcip=$srcip&dstip=$dstip&srcport=$srcport&dstport=
```

Syntax

```
address-to-link { lan | wan }
```

Mode

Solera

Description

Set default zone for address to link from email alerts.

Options

lan Default LAN

wan Default WAN

Example

```
address-to-link wan
```

Syntax

```
method { dns | dns-then-netbios | netbios | none }
```

Mode

Log Name Resolution

Description

Set name resolution method.

Options

dns DNS.

dns-then-netbios DNS then NetBIOS.

netbios NetBIOS.

none None.

Example

```
method dns
```

Syntax

```
dns { inherit | static { primary <IPV4_HOST> | secondary <IPV4_HOST> | tertiary <IPV4_HOST> } }
```

Mode

Log Name Resolution

Description

Set whether DNS is inherited or set manually with the associated DNS server IP addresses.

Options

inherit Inherit DNS servers.

static Set static DNS server

primary Specify primary DNS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.

Example: 192.168.168.168

secondary Specify secondary DNS server IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.

Example: 192.168.168.168

tertiary Specify tertiary DNS server IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.

Example: 192.168.168.168

Example

```
dns primary 192.168.168.165
```

Syntax

```
no dns static { primary | secondary | tertiary }
```

Mode

Log Name Resolution

Description

Manually clear DNS server IP address.

Options

static Clear static DNS server IP address.

primary Clear primary DNS server IP address.

secondary Clear secondary DNS server IP address.

tertiary Clear tertiary DNS server IP address.

Example

```
no dns primary
```

Syntax

```
start
```

Mode

Log Reports

Description

Start data collection.

Example

```
start
```

Syntax

```
stop
```

Mode

Log Reports

Description

Stop data collection.

Example

```
stop
```

Syntax

```
report-view { bandwidth-usage-by-ip | bandwidth-usage-by-service | web-site-hits }
```

Mode

Log Reports

Description

Set reports view.

Options

bandwidth-usage-by-ip Bandwidth usage by IP address.

bandwidth-usage-by-service Bandwidth usage by service.

web-site-hits Web site hits.

Example

```
report-view web-site-hits
```

Syntax

```
show report
```

Mode

Log Reports

Description

Show log report.

Options

report Show log report.

Example

```
show report
```

Syntax

```
enable
```

Mode

Viewpoint

Description

Enable viewpoint settings.

Example

```
enable
```

Syntax

no enable

Mode

Viewpoint

Description

Disable viewpoint settings.

Example

no enable

Syntax

enable

Mode

Analyzer

Description

Enable analyzer settings.

Example

enable

Syntax

no enable

Mode

Analyzer

Description

Disable analyzer settings.

Example

no enable

Syntax

log audit

Mode

Config

Description

Enter audit configuration mode.

Example

log audit

Syntax

enable

Mode

Configuration Audit

Description

Enable configuration auditing.

Example

enable

Syntax

no enable

Mode

Configuration Audit

Description

Disable configuration auditing.

Example

no enable

Syntax

debug

Mode

Configuration Audit

Description

Show configuration auditing messages to console.

Example

debug

Syntax

no debug

Mode

Configuration Audit

Description

Disable console output of audit messages.

Example

no debug

Syntax

audit-all

Mode

Configuration Audit

Description

Enable configuration auditing for all changes.

Example

```
audit-all
```

Syntax

```
no audit-all
```

Mode

Configuration Audit

Description

Disable configuration auditing for all changes.

Example

```
no audit-all
```

Syntax

```
send audit
```

Mode

Config

Description

E-mail audit records now.

Example

```
send audit
```

Syntax

```
show log [ analyzer | audit [ [ settings | view ] ] | automation | categories [ [ attributes [ [ category <LOG_CATEGORY_NAME> [ group <LOG_GROUP_NAME> [ event <LOG_EVENT_NAME> ] ] ] | event-id <LOG_EVENT_ID_FOR_ATTRIBUTES> ] ] | global-category-attributes | statistics [ category-level <LOG_CATEGORY_BRANCH_LEVEL> ] [ id <INT32> ] [ name <WORD> ] ] ] | display | name-resolution | syslog | view [ id <LOG_EVENT_ID_FOR_ATTRIBUTES> ] [ category <LOG_CATEGORY_NAME> ] [ priority <WORD> ] [ source-interface <LOG_INTERFACE_NAME> ] [ destination-interface <LOG_INTERFACE_NAME> ] [ source-ip <IP_V4V6_HOST> ] [ source-port <UINT16> ] [ destination-ip <IP_V4V6_HOST> ] [ destination-port <UINT16> ] [ ip-protocol <WORD> ] [ user-name <WORD> ] [ application <WORD> ] | view-status | viewpoint ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show device log and configuration.

Options

| | |
|-----------------|---------------------------|
| analyzer | Show analyzer settings. |
| audit | Show configuration audit. |

| | |
|---|---|
| settings | Show configuration audit settings. |
| view | View configuration audit messages. |
| automation | Show log automation settings. |
| categories | Show log categories configuration. |
| attributes | Show log categories event attributes which have been changed. |
| category <LOG_CATEGORY_NAME> | Show log attributes with specified category name. Log category name. Example: <i>Firewall</i> |
| group <LOG_GROUP_NAME> | Show log attributes with specified group name. Group name. Example: <i>Firewall Event</i> |
| event <LOG_EVENT_NAME> | Show log attributes with specified event name. Event name. Example: <i>Activate Firewall</i> |
| event-id <LOG_EVENT_ID_FOR_ATTRIBUTES> | Show log event attributes with specified ID. Event ID for showing the attributes. Example: <i>123</i> |
| global-category-attributes | Show global category attributes. |
| statistics category-level <LOG_CATEGORY_BRANCH_LEVEL> | Show log categories event statistics. Show event statistics of specified category level: category, group or event. Log category branch level. Example: <i>Category</i> |
| id <INT32> | Show event statistics by event ID. Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i> |
| name <WORD> | Show statistics by the name of a category, group or event. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| display | Show time range and max number for showing log view in CLI based current time. |
| name-resolution | Show name resolution settings. |
| syslog | Show syslog settings. |
| view id <LOG_EVENT_ID_FOR_ATTRIBUTES> | Show system log. Show log with specified ID. Event ID for showing the attributes. Example: <i>123</i> |
| category <LOG_CATEGORY_NAME> | Show log with specified category. Log category name. Example: <i>Firewall</i> |
| priority <WORD> | Show log with specified priority. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| source-interface <LOG_INTERFACE_NAME> | Show log with specified source interface. Interface name. Example: <i>X0</i> |
| destination-interface <LOG_INTERFACE_NAME> | Show log with specified destination interface. Interface name. Example: <i>X0</i> |
| source-ip <IP_V4V6_HOST> | Show log with specified source-ip. IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i> |
| source-port <UINT16> | Show log with specified source-port. Integer in the form: D OR 0xHHHH. Example: <i>123</i> |
| destination-ip <IP_V4V6_HOST> | Show log with specified destination-ip. IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i> |
| destination-port <UINT16> | Show log with specified destination-port. Integer in the form: D OR 0xHHHH. Example: <i>123</i> |

| | |
|-----------------------------------|---|
| <i>ip-protocol</i> | Show log with specified IP protocol. |
| <i><WORD></i> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>user-name</i> | Show log with specified user name. |
| <i><WORD></i> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>application</i> | Show log with specified application. |
| <i><WORD></i> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>view-status</i> | Show system log status. |
| <i>viewpoint</i> | Show viewpoint settings. |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |

Example

```
show log
show log view
show log categories
show log categories statistics category-level Category
show log syslog
show log audit view
show log audit settings
```

Syntax

```
voip
```

Mode

Config

Description

Enter VoIP configuration mode.

Example

```
voip
```

Syntax

```
flush-all
```

Mode

VoIP

Description

Flush all VoIP call entry.

Example

```
flush-all
```

Syntax

```
consistent-nat
```

Mode

VoIP

Description

Enable consistent nat.

Example

```
consistent-nat
```

Syntax

```
no consistent-nat
```

Mode

VoIP

Description

Disable consistent nat.

Example

```
no consistent-nat
```

Syntax

```
sip
```

Mode

VoIP

Description

Enable SIP transformations and enter its configuration mode.

Example

```
sip
```

Syntax

```
no sip
```

Mode

VoIP

Description

Disable SIP transformations.

Example

```
no sip
```

Syntax

```
h323
```

Mode

VoIP

Description

Enable H.323 transformations and enter its configuration mode.

Example

```
h323
```

Syntax

```
no h323
```

Mode

VoIP

Description

Disable H.323 transformations.

Example

```
no h323
```

Syntax

```
non-sip-packets
```

Mode

SIP

Description

Enable permit non-SIP packets on signaling port.

Example

```
non-sip-packets
```

Syntax

```
no non-sip-packets
```

Mode

SIP

Description

Disable permit non-SIP packets on signaling port.

Example

```
no non-sip-packets
```

Syntax

```
b2bua-support
```

Mode

SIP

Description

Enable SIP back-to-back user agent (B2BUA) support.

Example

```
b2bua-support
```

Syntax

```
no b2bua-support
```

Mode

SIP

Description

Disable SIP back-to-back user agent (B2BUA) support.

Example

```
no b2bua-support
```

Syntax

```
signaling-timeout <UINT32>
```

Mode

SIP

Description

Set SIP signaling inactivity time out (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
signaling-timeout 1800
```

Syntax

```
media-timeout <UINT16>
```

Mode

SIP

Description

Set SIP media inactivity time out (seconds).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
media-timeout 120
```

Syntax

```
no signaling-port
```


Mode

SIP

Description

Clear additional SIP signaling port (UDP) for transformations (optional).

Example

```
no signaling-port
```

Syntax

```
signaling-port <UINT16>
```

Mode

SIP

Description

Set additional SIP signaling port (UDP) for transformations (optional).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
signaling-port 45060
```

Syntax

```
endpoint-registration-anomaly-tracking
```

Mode

SIP

Description

Enable SIP endpoint registration anomaly tracking.

Example

```
endpoint-registration-anomaly-tracking
```

Syntax

```
no endpoint-registration-anomaly-tracking
```

Mode

SIP

Description

Disable SIP endpoint registration anomaly tracking.

Example

```
no endpoint-registration-anomaly-tracking
```

Syntax

registration-tracking-interval <UINT32>

Mode

SIP

Description

Set SIP registration tracking interval (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

registration-tracking-interval 300

Syntax

failed-registration-threshold <UINT16>

Mode

SIP

Description

Set SIP failed registration threshold.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

failed-registration-threshold 5

Syntax

endpoint-block-interval <UINT16>

Mode

SIP

Description

Set endpoint block interval(seconds).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

endpoint-block-interval 3600

Syntax

only-gatekeeper-calls

Mode

H323

Description

Enable only accept incoming calls from gatekeeper.

Example

```
only-gatekeeper-calls
```

Syntax

```
no only-gatekeeper-calls
```

Mode

H323

Description

Disable only accept incoming calls from gatekeeper.

Example

```
no only-gatekeeper-calls
```

Syntax

```
inactivity-timeout <UINT32>
```

Mode

H323

Description

Set H.323 signaling/media inactivity time out (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
inactivity-timeout 300
```

Syntax

```
no gatekeeper-ip
```

Mode

H323

Description

Clear default wan/dmz gatekeeper IP address.

Example

```
no gatekeeper-ip
```

Syntax

```
gatekeeper-ip <IPV4_HOST>
```

Mode

H323

Description

Set default wan/dmz gatekeeper IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
gatekeeper-ip 172.16.10.10
```

Syntax

```
show voip [ { pending-config | with-pending-config } | call-status ]
```

Mode

All Modes

Description

Show VoIP status or configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

call-status Show VoIP call status.

Example

```
show voip
```

Syntax

```
security-services
```

Mode

Config

Description

Enter security services configuration mode.

Example

```
security-services
```

Syntax

```
synchronize
```

Mode

Security Services

Description

Synchronize licenses with www.mysonicwall.com.

Example

```
synchronize-license
```

Syntax

```
security { maximum | performance-optimized }
```

Mode

Security Services

Description

Set global security services setting.

Options

maximum Use maximum security (recommended).

performance-optimized Use performance optimized.

Example

```
security maximum
```

Syntax

```
reduce-isdn-antivirus-traffic
```

Mode

Security Services

Description

Enable reduce Anti-Virus traffic for ISDN connections.

Example

```
reduce-isdn-antivirus-traffic
```

Syntax

```
no reduce-isdn-antivirus-traffic
```

Mode

Security Services

Description

Disable reduce Anti-Virus traffic for ISDN connections.

Example

```
no reduce-isdn-antivirus-traffic
```

Syntax

```
drop-packets-at-reload
```

Mode

Security Services

Description

Enable drop all packets while IPS, GAV and Anti-Spyware database is reloading.

Example

```
drop-packets-at-reload
```

Syntax

```
no drop-packets-at-reload
```

Mode

Security Services

Description

Disable drop all packets while IPS, GAV and Anti-Spyware database is reloading.

Example

```
no drop-packets-at-reload
```

Syntax

```
http-clientless-notification-timeout <UINT32>
```

Mode

Security Services

Description

Set HTTP clientless notification timeout for gateway AntiVirus and AntiSpyware.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
http-clientless-notification-timeout 86400
```

Syntax

```
proxy-server
```

Mode

Security Services

Description

Enable download signature through a proxy server and enter proxy server configure mode.

Example

```
proxy-server
```

Syntax

```
no proxy-server
```

Mode

Security Services

Description

Disable download signature through a proxy server.

Example

```
no proxy-server
```

Syntax

```
host <HOSTNAME>
```

Mode

Security Services Proxy Server

Description

Set hostname or IP address for proxy server.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
host 10.10.10.10
```

Syntax

```
no host
```

Mode

Security Services Proxy Server

Description

Clear hostname or IP address for proxy server.

Example

```
no host
```

Syntax

```
port <IPV4_PORT>
```

Mode

Security Services Proxy Server

Description

Set proxy server TCP port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
port 8080
```

Syntax

no port

Mode

Security Services Proxy Server

Description

Clear proxy server TCP port.

Example

no port

Syntax

authentication [user-name <WORD>] [password <ENC_PASSWORD>]

Mode

Security Services Proxy Server

Description

Configure proxy server authentication.

Options

| | |
|------------------------------------|---|
| <i>user-name</i> | Set proxy server username. |
| <i><WORD></i> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>password</i> | Set proxy server password. |
| <i><ENC_PASSWORD></i> | Password. Example: <i>secret</i> |

Example

authentication user-name proxyUser password proxyPass

Syntax

no authentication [password | user-name]

Mode

Security Services Proxy Server

Description

Disable proxy server authentication.

Options

| | |
|-------------------------|---|
| <i>password</i> | Clear proxy server authentication password. |
| <i>user-name</i> | Clear proxy server authentication username. |

Example

no authentication
no authentication user-name
no authentication password

Syntax

```
portal [ user-name <WORD> ] [ password <ENC_PASSWORD> ]
```

Mode

Security Services Proxy Server

Description

Configure proxy server portal username and password.

Options

| | |
|-----------------------------|---|
| user-name | Set proxy server portal username. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| password | Set proxy server portal password. |
| <ENC_PASSWORD> | Password. Example: <i>secret</i> |

Example

```
portal user-name portalUser
```

Syntax

```
no portal { password | user-name }
```

Mode

Security Services Proxy Server

Description

Clear proxy server portal username or password.

Options

| | |
|------------------|-------------------------------------|
| password | Clear proxy server portal password. |
| user-name | Clear proxy server portal username. |

Example

```
no portal user-name
```

Syntax

```
dpi-ssh
```

Mode

Config

Description

Enter DPI-SSH configuration mode.

Example

```
dpi-ssh
```

Syntax

```
enable
```

Mode

DPI SSH

Description

Enable SSH inspection.

Example

```
enable
```

Syntax

```
no enable
```

Mode

DPI SSH

Description

Disable SSH inspection.

Example

```
no enable
```

Syntax

```
intrusion-prevention
```

Mode

DPI SSH

Description

Enable intrusion prevention for DPI-SSH.

Example

```
intrusion-prevention
```

Syntax

```
no intrusion-prevention
```

Mode

DPI SSH

Description

Disable intrusion prevention for DPI-SSH.

Example

```
no intrusion-prevention
```

Syntax

```
gateway { anti-spyware | anti-virus }
```

Mode

DPI SSH

Description

Enable gateway anti-virus or anti-spyware for DPI-SSH.

Options

anti-spyware Enable gateway anti-spyware for DPI-SSH.

anti-virus Enable gateway anti-virus for DPI-SSH.

Example

```
gateway anti-virus
gateway anti-spyware
```

Syntax

```
no gateway { anti-spyware | anti-virus }
```

Mode

DPI SSH

Description

Disable gateway anti-virus or anti-spyware for DPI-SSH.

Options

anti-spyware Disable gateway anti-spyware for DPI-SSH.

anti-virus Disable gateway anti-virus for DPI-SSH.

Example

```
no gateway anti-virus
no gateway anti-spyware
```

Syntax

```
application-firewall
```

Mode

DPI SSH

Description

Enable application firewall for DPI-SSH.

Example

```
application-firewall
```

Syntax

```
no application-firewall
```

Mode

DPI SSH

Description

Disable application firewall for DPI-SSH.

Example

```
no application-firewall
```

Syntax

```
block-port-forwarding [ global | local | remote | x11 ]
```

Mode

DPI SSH

Description

Block port forwarding.

Options

global Block port forwarding.

local Block local port forwarding.

remote Block remote port forwarding.

x11 Block X11 forwarding.

Example

```
block-port-forwarding
block-port-forwarding local
block-port-forwarding remote
```

Syntax

```
no block-port-forwarding [ global | local | remote | x11 ]
```

Mode

DPI SSH

Description

Allow port forwarding.

Options

global Block port forwarding.

local Allow local port forwarding.

remote Allow remote port forwarding.

x11 Allow X11 forwarding.

Example

```
no block-port-forwarding
no block-port-forwarding local
no block-port-forwarding remote
```

Syntax

```
include address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | all | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

DPI SSH

Description

Set the DPI-SSH inclusion address object or group.

Options

| | |
|---|--|
| ipv6 | IPv6 address object. |
| host <ADDR_HOST> | Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network <ADDR_NETWORK> | Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> | Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| all | All addresses. |
| fqdn <ADDR_FQDN> | Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group <ADDR_GROUP_NAME_MIXED> | Address group name. Group address object name. Example: <i>Sales Group</i> |
| mac <ADDR_MAC> | Address object MAC. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name <ADDR_NAME_MIXED> | Address object name. Address object name. Example: <i>Web Server</i> |

Example

```
include address name "DPI-SSH Inclusion Object"
```

Syntax

```
exclude address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

DPI SSH

Description

Set the DPI-SSH exclusion address object or group.

Options

| | |
|--------------------------------------|--|
| ipv6 | IPv6 address object. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| mac | Address object MAC. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
exclude address name "DPI-SSH Exclusion Object"
```

Syntax

```
no exclude address
```

Mode

DPI SSH

Description

Clear exclusion address objects or group for DPI-SSH.

Example

```
no exclude address
```

Syntax

```
include service { all | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

DPI SSH

Description

Set the DPI-SSH inclusion service object or group.

Options

| | |
|-------------------------------|---|
| all | All services. |
| group | Service group name. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
include service name "DPI-SSH Inclusion Service"
```

Syntax

```
exclude service { group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

DPI SSH

Description

Set the DPI-SSH exclusion service object or group.

Options

| | |
|-------------------------------|---|
| group | Service group name. |
| <SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Service object name. |
| <SVC_NAME> | Service object name. Example: <i>HTTPS</i> |
| protocol | Service object protocol. |
| <SVC_PROTOCOL> | Service protocol. Example: <i>TCP</i> |
| <SVC_PORT_BEGIN> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <SVC_PORT_END> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
exclude service name "DPI-SSH Exclusion Service"
```

Syntax

```
no exclude service
```

Mode

DPI SSH

Description

Clear exclusion service objects or group for DPI-SSH.

Example

```
no exclude service
```

Syntax

```
include user { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

DPI SSH

Description

Set the DPI-SSH inclusion user object or group.

Options

| | |
|--------------------------------------|---|
| administrator | Administrator. |
| all | All users. |
| group | Group object name. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guest users. |
| name | User object name. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
include user group "DPI-SSH User Group"
```

Syntax

```
exclude user { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

DPI SSH

Description

Set the DPI-SSH exclusion user object or group.

Options

| | |
|--------------------------------------|---|
| administrator | Administrator. |
| group | Group object name. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guest users. |
| name | User object name. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
exclude user group "DPI-SSH User Group"
```

Syntax

no exclude user

Mode

DPI SSH

Description

Clear exclusion user for DPI-SSH.

Example

no exclude user

Syntax

content-filter

Mode

Config

Description

Enter content filter configuration mode.

Example

content-filter

Syntax

filter-type { cfs | websense }

Mode

Content Filter

Description

Set filter type and enter corresponding configuration mode.

Options

cfs SonicWall CFS.

websense Websense enterprise.

Example

filter-type cfs
filter-type websense

Syntax

max-url-caches <UINT32>

Mode

SonicWall CFS

Description

Set CFS max URL caches number.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
max-url-caches 51200
```

Syntax

```
enable
```

Mode

SonicWall CFS

Description

Enable CFS.

Example

```
enable
```

Syntax

```
no enable
```

Mode

SonicWall CFS

Description

Disable CFS.

Example

```
no enable
```

Syntax

```
block-if-server-unavailable
```

Mode

SonicWall CFS

Description

Enable block if CFS server is unavailable.

Example

```
block-if-server-unavailable
```

Syntax

```
no block-if-server-unavailable
```

Mode

SonicWall CFS

Description

Disable block if CFS server is unavailable.

Example

```
no block-if-server-unavailable
```

Syntax

```
server-timeout <UINT16>
```

Mode

SonicWall CFS

Description

Set CFS server timeout.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
server-timeout 5
```

Syntax

```
local-server [ primary <HOSTNAME_MIXED> | secondary <HOSTNAME_MIXED> ]
```

Mode

SonicWall CFS

Description

Enable local CFS server or set server address.

Options

primary Set primary local CFS server.
<HOSTNAME_MIXED> IPV4: hostname in the form: D.D.D.D or hostname\nIPV6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

secondary Set secondary local CFS server.
<HOSTNAME_MIXED> IPV4: hostname in the form: D.D.D.D or hostname\nIPV6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

```
local-server  
local-server primary 1.1.1.1  
local-server secondary localserver.sonicwall.com
```

Syntax

```
no local-server [ primary | secondary ]
```

Mode

SonicWall CFS

Description

Disable local CFS server or clear server address.

Options

primary Clear primary local CFS server.

secondary Clear secondary local CFS server.

Example

```
no local-server
no local-server primary
no local-server secondary
```

Syntax

```
exclude administrator
```

Mode

SonicWall CFS

Description

Enable exclude administrator.

Example

```
exclude administrator
```

Syntax

```
no exclude administrator
```

Mode

SonicWall CFS

Description

Diable exclude administrator.

Example

```
no exclude administrator
```

Syntax

```
exclude address { { [ ipv6 ] { fqdn <ADDR_FQDN> | host <ADDR_HOST> | mac <ADDR_MAC> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

SonicWall CFS

Description

Exclude address.

Options

ipv6 IPv6 Address object.

fqdn Address object full qualified domain name.

| | |
|--------------------------------------|---|
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| mac | Address object MAC Address. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Specify IP range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group | Address object group name. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| name | Address object name. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
exclude address host 192.168.168.168
exclude address network 192.168.168.0 255.255.255.0
exclude address range 192.168.168.1 192.168.168.10
exclude address mac D067E534E99C
exclude address fqdn example.com
exclude address ipv6 host fec0:1::1
exclude address ipv6 network fec0:1:: 64
exclude address ipv6 range fec0:1::1 fec0:1::100
exclude address group "Corp CFS Exclusion Address Group"
exclude address name "Corp CFS Exclusion Address Object"
```

Syntax

```
no exclude address
```

Mode

SonicWall CFS

Description

Clear excluded address.

Example

```
no exclude address
```

Syntax

```
clear policies statistics
```

Mode

SonicWall CFS

Description

Clear all statistics of CFS policies.

Example

```
clear policies statistics
```

Syntax

```
no policies
```

Mode

SonicWall CFS

Description

Delete all CFS policies.

Example

```
no policies
```

Syntax

```
no policy <CFS_POLICY_NAME>
```

Mode

SonicWall CFS

Description

Delete CFS policy.

Options

<CFS_POLICY_NAME> CFS policy name.
Example: *Market policy*

Example

```
no policy "policyName"
```

Syntax

```
policy <CFS_POLICY_NAME>
```

Mode

SonicWall CFS

Description

Add/Edit CFS policy and enter configuration mode.

Options

<CFS_POLICY_NAME> CFS policy name.
Example: *Market policy*

Example

```
policy "CFS default policy"
```

Syntax

```
name <CFS_POLICY_NAME>
```

Mode

CFS Policy

Description

Set policy name.

Options

<CFS_POLICY_NAME> CFS policy name.
Example: *Market policy*

Example

```
name "CFS default policy"
```

Syntax

```
source zone <CFS_POLICY_ZONE>
```

Mode

CFS Policy

Description

Set source zone.

Options

<CFS_POLICY_ZONE> CFS policy zone.
Example: *LAN*

Example

```
source zone LAN
```

Syntax

```
destination zone <CFS_POLICY_ZONE>
```

Mode

CFS Policy

Description

Set destination zone.

Options

<CFS_POLICY_ZONE> CFS policy zone.
Example: *LAN*

Example

```
destination zone WAN
```

Syntax

```
source address included { ( [ ipv6 ] { host <CFS_POLICY_ADDR_HOST> | network <CFS_POLICY_ADDR_NETWORK> <CFS_POLICY_ADDR_MASK> |  
range <CFS_POLICY_ADDR_BEGIN> <CFS_POLICY_ADDR_END> } } | any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC>  
| name <ADDR_NAME_MIXED> }
```

Mode

CFS Policy

Description

Set included source address.

Options

| | |
|--|--|
| ipv6 | IPv6 Address object. |
| host | Address object host. |
| <CFS_POLICY_ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <CFS_POLICY_ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <CFS_POLICY_ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Specify IP range. |
| <CFS_POLICY_ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <CFS_POLICY_ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group object name. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| mac | Address object MAC Address. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
source address included host 192.168.168.168
source address included network 192.168.168.0 255.255.255.0
source address included range 192.168.168.1 192.168.168.10
source address included mac D067E534E99C
source address included fqdn example.com
source address included ipv6 host fec0:1::1
source address included ipv6 network fec0:1:: 64
source address included ipv6 range fec0:1::1 fec0:1::100
source address included any
source address included group "CFS Policy Source Address Group"
source address included name "CFS Policy Source Address Object"
```

Syntax

```
source address excluded { [ { ipv6 ] { host <CFS_POLICY_ADDR_HOST> | network <CFS_POLICY_ADDR_NETWORK> <CFS_POLICY_ADDR_MASK> |
range <CFS_POLICY_ADDR_BEGIN> <CFS_POLICY_ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name
<ADDR_NAME_MIXED> | none }
```

Mode

CFS Policy

Description

Set excluded source address.

Options

| | |
|--|--|
| ipv6 | IPv6 Address object. |
| host | Address object host. |
| <CFS_POLICY_ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <CFS_POLICY_ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <CFS_POLICY_ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Specify IP range. |
| <CFS_POLICY_ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <CFS_POLICY_ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group object name. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| mac | Address object MAC Address. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |
| none | None address. |

Example

```
source address excluded host 192.168.168.168
source address excluded network 192.168.168.0 255.255.255.0
source address excluded range 192.168.168.1 192.168.168.10
source address excluded mac D067E534E99C
source address excluded fqdn example.com
source address excluded ipv6 host fec0:1::1
source address excluded ipv6 network fec0:1:: 64
source address excluded ipv6 range fec0:1::1 fec0:1::100
source address excluded none
source address excluded group "CFS Policy Source Address Group"
source address excluded name "CFS Policy Source Address Object"
```

Syntax

```
user included { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

CFS Policy

Description

Set included users.

Options

| | |
|--------------------------------------|---|
| administrator | Administrator. |
| all | All users. |
| group | User group object name. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests. |
| name | User object name. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
user included all
user included guests
user included administrator
user included name "user1"
user included group "Limited Administrators"
```

Syntax

```
user excluded { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> | none }
```

Mode

CFS Policy

Description

Set excluded users.

Options

| | |
|--------------------------------------|---|
| administrator | Administrator. |
| group | User group object name. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests. |
| name | User object name. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |
| none | None users. |

Example

```
user excluded none
user excluded guests
user excluded administrator
user excluded name "user1"
user excluded group "Limited Administrators"
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

CFS Policy

Description

Set schedule.

Options

| | |
|---------------------------------------|---|
| <code>always-on</code> | Always on. |
| <code>days</code> | Schedule object days. |
| <code><SCHED_DAYS></code> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| <code>time</code> | Schedule object beginning/ending time. |
| <code><SCHED_TIME_BEGIN></code> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <code><SCHED_TIME_END></code> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <code>name</code> | Schedule object name. |
| <code><SCHED_NAME></code> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule always-on
schedule name "Schedule Name"
schedule days "Schedule Days" time "Schedule Time Begin" "Schedule Time End"
```

Syntax

```
profile <CONTENT_FILTER_PROFILE_NAME>
```

Mode

CFS Policy

Description

Set profile.

Options

| | |
|--|---|
| <code><CONTENT_FILTER_PROFILE_NAME></code> | Content filter profile object name. Example: <i>Market profile</i> |
|--|---|

Example

```
profile "CFS Default profile"
```

Syntax

```
action <CONTENT_FILTER_ACTION_NAME>
```

Mode

CFS Policy

Description

Set action.

Options

| | |
|---|---|
| <code><CONTENT_FILTER_ACTION_NAME></code> | Content filter action object name. Example: <i>Market action</i> |
|---|---|

Example

```
action "CFS Default action"
```

Syntax

enable

Mode

CFS Policy

Description

Enable the policy.

Example

enable

Syntax

no enable

Mode

CFS Policy

Description

Disable the policy.

Example

no enable

Syntax

priority <UINT32>

Mode

CFS Policy

Description

Set priority.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

priority 3

Syntax

custom-category

Mode

SonicWall CFS

Description

Enter CFS custom category configuration mode.

Example

custom-category

Syntax

enable

Mode

CFS Custom Category

Description

Enable custom category.

Example

enable

Syntax

no enable

Mode

CFS Custom Category

Description

Disable custom category.

Example

no enable

Syntax

no category-entries

Mode

CFS Custom Category

Description

Delete all custom category entries.

Example

no category-entries

Syntax

no category-entry <CFS_CUSTOM_CATEGORY_DOMAIN>

Mode

CFS Custom Category

Description

Delete custom category entry.

Options

<CFS_CUSTOM_CATEGORY_DOMAIN> CFS custom category domain.
Example: *google.com*

Example

no category-entry yahoo.com

Syntax

category-entry <CFS_CUSTOM_CATEGORY_DOMAIN>

Mode

CFS Custom Category

Description

Add/Edit custom category entry and enter configuration mode.

Options

<CFS_CUSTOM_CATEGORY_DOMAIN> CFS custom category domain.
Example: *google.com*

Example

category-entry www.google.com

Syntax

domain <CFS_CUSTOM_CATEGORY_DOMAIN>

Mode

Content Filter Custom Category Entry

Description

Set custom category entry domain.

Options

<CFS_CUSTOM_CATEGORY_DOMAIN> CFS custom category domain.
Example: *google.com*

Example

domain www.google.com

Syntax

no ratings

Mode

Content Filter Custom Category Entry

Description

Delete all ratings of category entry.

Example

no ratings

Syntax

rating <CONTENT_FILTER_CATEGORY_ID_NAME>

Mode

Content Filter Custom Category Entry

Description

Add rating for category entry.

Options

<CONTENT_FILTER_CATEGORY_ID_NAME> Content filter category number and name.
Example: 1. Violence/Hate/Racism

Example

```
rating "1.Violence/Hate/Racism"
```

Syntax

```
no rating <CFS_CUSTOM_CATEGORY_RATING>
```

Mode

Content Filter Custom Category Entry

Description

Delete rating of category entry.

Options

<CFS_CUSTOM_CATEGORY_RATING> CFS custom category rating number and name.
Example: 1. Violence/Hate/Racism

Example

```
no rating "1.Violence/Hate/Racism"
```

Syntax

```
no uri-list-objects
```

Mode

Content Filter

Description

Delete all content filter URI list objects.

Example

```
no uri-list-objects
```

Syntax

```
no uri-list-groups
```

Mode

Content Filter

Description

Delete all content filter URI list groups.

Example

```
no uri-list-groups
```

Syntax

```
no uri-list-object <CONTENT_FILTER_URI_LIST_OBJ_NAME>
```

Mode

Content Filter

Description

Delete content filter URI list object.

Options

<CONTENT_FILTER_URI_LIST_OBJ_NAME> Content filter URI list object name.
Example: *White URI list object*

Example

```
no uri-list-object "uriListObjName"
```

Syntax

```
no uri-list-group <CONTENT_FILTER_URI_LIST_GRP_NAME>
```

Mode

Content Filter

Description

Delete content filter URI list group.

Options

<CONTENT_FILTER_URI_LIST_GRP_NAME> Content filter URI list group name.
Example: *White URI list group*

Example

```
no uri-list-group "uriListGrpName"
```

Syntax

```
uri-list-object <CONTENT_FILTER_URI_LIST_OBJ_NAME>
```

Mode

Content Filter

Description

Add/Edit content filter URI list object and enter configuration mode.

Options

<CONTENT_FILTER_URI_LIST_OBJ_NAME> Content filter URI list object name.
Example: *White URI list object*

Example

```
uri-list-object "Uri List Object Name"
```

Syntax

```
uri-list-group <CONTENT_FILTER_URI_LIST_GRP_NAME>
```

Mode

Content Filter

Description

Add/Edit content filter URI list group and enter configuration mode.

Options

<CONTENT_FILTER_URI_LIST_GRP_NAME> Content filter URI list group name.
Example: *White URI list group*

Example

```
uri-list-group "Uri List Group Name"
```

Syntax

```
name <CONTENT_FILTER_URI_LIST_OBJ_NAME>
```

Mode

Content Filter URI List Object

Description

Set URI list object name.

Options

<CONTENT_FILTER_URI_LIST_OBJ_NAME> Content filter URI list object name.
Example: *White URI list object*

Example

```
name "default URI List"
```

Syntax

```
name <CONTENT_FILTER_URI_LIST_GRP_NAME>
```

Mode

Content Filter URI List Group

Description

Set URI list group name.

Options

<CONTENT_FILTER_URI_LIST_GRP_NAME> Content filter URI list group name.
Example: *White URI list group*

Example

```
name "default URI List"
```

Syntax

```
uri <CONTENT_FILTER_URI_LIST_URI>
```

Mode

Content Filter URI List Object

Description

Add URI into URI list object.

Options

<CONTENT_FILTER_URI_LIST_URI> Content filter URI list URI.
Example: *google.com*

Example

```
uri www.google.com
```

Syntax

```
no uri <CONTENT_FILTER_URI_LIST_URI>
```

Mode

Content Filter URI List Object

Description

Remove URI from URI list.

Options

<CONTENT_FILTER_URI_LIST_URI> Content filter URI list URI.
Example: *google.com*

Example

```
no uri www.google.com
```

Syntax

```
no uris
```

Mode

Content Filter URI List Object

Description

Remove all URIs from URI list.

Example

```
no uris
```

Syntax

```
keyword <CONTENT_FILTER_URI_LIST_KEYWORD>
```

Mode

Content Filter URI List Object

Description

Add keyword into URI list.

Options

<CONTENT_FILTER_URI_LIST_KEYWORD> Content filter URI list keyword.
Example: *news*

Example

```
keyword news
```

Syntax

```
no keyword <CONTENT_FILTER_URI_LIST_KEYWORD>
```

Mode

Content Filter URI List Object

Description

Remove keyword from URI list.

Options

<CONTENT_FILTER_URI_LIST_KEYWORD> Content filter URI list keyword.
Example: *news*

Example

```
no keyword news
```

Syntax

```
no keywords
```

Mode

Content Filter URI List Object

Description

Remove all keywords from URI list.

Example

```
no keywords
```

Syntax

```
uri-list-object <CONTENT_FILTER_URI_LIST_OBJ_NAME>
```

Mode

Content Filter URI List Group

Description

Assign URI list object to group.

Options

<CONTENT_FILTER_URI_LIST_OBJ_NAME> Content filter URI list object name.
Example: *White URI list object*

Example

```
uri-list-object "allowed uri list object"
```

Syntax

```
no uri-list-object <CONTENT_FILTER_URI_LIST_OBJ_NAME>
```

Mode

Content Filter URI List Group

Description

Remove URI list object from group.

Options

<CONTENT_FILTER_URI_LIST_OBJ_NAME> Content filter URI list object name.
Example: *White URI list object*

Example

```
no uri-list-object "white list object"
```

Syntax

```
uri-list-group <CONTENT_FILTER_URI_LIST_GRP_NAME>
```

Mode

Content Filter URI List Group

Description

Assign URI list group to group.

Options

<CONTENT_FILTER_URI_LIST_GRP_NAME> Content filter URI list group name.
Example: *White URI list group*

Example

```
uri-list-group "white list group"
```

Syntax

```
no uri-list-group <CONTENT_FILTER_URI_LIST_GRP_NAME>
```

Mode

Content Filter URI List Group

Description

Remove URI list group from group.

Options

<CONTENT_FILTER_URI_LIST_GRP_NAME> Content filter URI list group name.
Example: *White URI list group*

Example

```
no uri-list-group "white list group"
```

Syntax

```
no actions
```

Mode

Content Filter

Description

Delete all content filter action objects.

Example

```
no actions
```

Syntax

```
no action <CONTENT_FILTER_ACTION_NAME>
```

Mode

Content Filter

Description

Delete content filter action object.

Options

<CONTENT_FILTER_ACTION_NAME> Content filter action object name.
Example: *Market action*

Example

```
no action "actionName"
```

Syntax

```
action <CONTENT_FILTER_ACTION_NAME>
```

Mode

Content Filter

Description

Add/Edit content filter action object and enter configuration mode.

Options

<CONTENT_FILTER_ACTION_NAME> Content filter action object name.
Example: *Market action*

Example

```
action "actionName"
```

Syntax

```
name <CONTENT_FILTER_ACTION_NAME>
```

Mode

Content Filter Action Object

Description

Set action object name.

Options

<CONTENT_FILTER_ACTION_NAME> Content filter action object name.
Example: *Market action*

Example

```
name "actionName"
```

Syntax

```
wipe-cookies
```

Mode

Content Filter Action Object

Description

Enable wipe cookies.

Example

wipe-cookies

Syntax

no wipe-cookies

Mode

Content Filter Action Object

Description

Disable wipe cookies.

Example

no wipe-cookies

Syntax

flow-reporting

Mode

Content Filter Action Object

Description

Enable flow reporting.

Example

flow-reporting

Syntax

no flow-reporting

Mode

Content Filter Action Object

Description

Disable flow reporting.

Example

no flow-reporting

Syntax

block page { custom <WORD> | default }

Mode

Content Filter Action Object

Description

Set block page.

Options

- custom** Use custom defined page.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- default** Use default page.

Example

```
block page custom "<html> ... </html>"  
block page default
```

Syntax

```
passphrase page { custom <WORD> | default }
```

Mode

Content Filter Action Object

Description

Set passphrase page.

Options

- custom** Use custom defined page.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- default** Use default page.

Example

```
passphrase page custom "<html> ... </html>"  
passphrase page default
```

Syntax

```
passphrase password <ENC_PASSWORD>
```

Mode

Content Filter Action Object

Description

Set passphrase password.

Options

- <ENC_PASSWORD>** Password.
Example: *secret*

Example

```
passphrase password 123456
```

Syntax

```
no passphrase password
```

Mode

Content Filter Action Object

Description

Clear passphrase password.

Example

```
no passphrase password
```

Syntax

```
passphrase active-time <UINT32>
```

Mode

Content Filter Action Object

Description

Set passphrase active time.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
passphrase active-time 60
```

Syntax

```
confirm page { custom <WORD> | default }
```

Mode

Content Filter Action Object

Description

Set confirm page.

Options

custom Use custom defined page.

<WORD> Word in the form: WORD or "QUOTED STRING".
Example: abc

default Use default page.

Example

```
confirm page custom "<html> ... </html>
```

```
confirm page default
```

Syntax

```
confirm active-time <UINT32>
```


Mode

Content Filter Action Object

Description

Set confirm active time.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
confirm active-time 60
```

Syntax

```
bandwidth-management aggregation-method { action | policy }
```

Mode

Content Filter Action Object

Description

Set bandwidth management aggregation method.

Options

action Use per action aggregation method.

policy Use per policy aggregation method.

Example

```
bandwidth-management aggregation-method policy
```

Syntax

```
bandwidth-management egress [ name <BANDWIDTH_RULE_NAME> ]
```

Mode

Content Filter Action Object

Description

Enable egress bandwidth management or set egress object.

Options

name Set egress bandwidth management object.
<BANDWIDTH_RULE_NAME> Bandwidth object name.
Example: `"Corp High Priority"`

Example

```
bandwidth-management egress  
bandwidth-management egress name "Egress BWM Object"
```

Syntax

```
no bandwidth-management egress [ name ]
```

Mode

Content Filter Action Object

Description

Disable egress bandwidth management or clear egress object.

Options

name Clear egress bandwidth management object.

Example

```
no bandwidth-management egress
no bandwidth-management egress name
```

Syntax

```
bandwidth-management ingress [ name <BANDWIDTH_RULE_NAME> ]
```

Mode

Content Filter Action Object

Description

Enable ingress bandwidth management or set ingress object.

Options

name Set ingress bandwidth management object.
<BANDWIDTH_RULE_NAME> Bandwidth object name.
Example: `\\"Corp High Priority\\"`

Example

```
bandwidth-management ingress
bandwidth-management ingress name "Ingress BWM Object"
```

Syntax

```
no bandwidth-management ingress [ name ]
```

Mode

Content Filter Action Object

Description

Disable ingress bandwidth management or clear ingress object.

Options

name Clear ingress bandwidth management object.

Example

```
no bandwidth-management ingress
no bandwidth-management ingress name
```

Syntax

```
bandwidth-management usage-tracking
```

Mode

Content Filter Action Object

Description

Enable bandwidth usage tracking.

Example

```
bandwidth-management usage-tracking
```

Syntax

```
no bandwidth-management usage-tracking
```

Mode

Content Filter Action Object

Description

Disable bandwidth usage tracking.

Example

```
no bandwidth-management usage-tracking
```

Syntax

```
no profiles
```

Mode

Content Filter

Description

Delete all content filter profile objects.

Example

```
no profiles
```

Syntax

```
no profile <CONTENT_FILTER_PROFILE_NAME>
```

Mode

Content Filter

Description

Delete content filter profile object.

Options

<CONTENT_FILTER_PROFILE_NAME> Content filter profile object name.
Example: *Market profile*

Example

```
no profile profileName
```

Syntax

```
profile <CONTENT_FILTER_PROFILE_NAME>
```

Mode

Content Filter

Description

Add/Edit content filter profile object and enter configuration mode.

Options

<CONTENT_FILTER_PROFILE_NAME> Content filter profile object name.
Example: *Market profile*

Example

```
profile profileName
```

Syntax

```
name <CONTENT_FILTER_PROFILE_NAME>
```

Mode

Content Filter Profile Object

Description

Set profile object name.

Options

<CONTENT_FILTER_PROFILE_NAME> Content filter profile object name.
Example: *Market profile*

Example

```
name profileName
```

Syntax

```
uri-list allowed <CONTENT_FILTER_URI_LIST_NAME>
```

Mode

Content Filter Profile Object

Description

Set allowed uri list.

Options

<CONTENT_FILTER_URI_LIST_NAME> Content filter URI list object/group name.
Example: *White URI list*

Example

```
uri-list allowed allowedUriListName
```

Syntax

```
no uri-list allowed
```

Mode

Content Filter Profile Object

Description

Clear allowed uri list.

Example

no uri-list allowed

Syntax

uri-list forbidden <CONTENT_FILTER_URI_LIST_NAME>

Mode

Content Filter Profile Object

Description

Set forbidden uri list.

Options

<CONTENT_FILTER_URI_LIST_NAME> Content filter URI list object/group name.
Example: *White URI list*

Example

uri-list forbidden forbiddenUriListName

Syntax

no uri-list forbidden

Mode

Content Filter Profile Object

Description

Clear forbidden uri list.

Example

no uri-list forbidden

Syntax

uri-list search-order { allowed-first | forbidden-first }

Mode

Content Filter Profile Object

Description

Set uri list search order.

Options

allowed-first Search allowed URI list first.

forbidden-first Search forbidden URI list first.

Example

uri-list search-order allowed-first

Syntax

uri-list forbidden-operation <CONTENT_FILTER_FORBIDDEN_LIST_OPERATION_NAME>

Mode

Content Filter Profile Object

Description

Set operation of forbidden uri list.

Options

<CONTENT_FILTER_FORBIDDEN_LIST_OPERATION_NAME> Content filter operation for forbidden URI list.
Example: *block*

Example

```
uri-list operation-for-forbidden block
```

Syntax

```
category <CONTENT_FILTER_CATEGORY_ID_NAME> <CONTENT_FILTER_OPERATION_NAME>
```

Mode

Content Filter Profile Object

Description

Set operation of category.

Options

<CONTENT_FILTER_CATEGORY_ID_NAME> Content filter category number and name.
Example: *1. Violence/Hate/Racism*

<CONTENT_FILTER_OPERATION_NAME> Content filter operation.
Example: *block*

Example

```
category "1. Violence/Hate/Racism" block
```

Syntax

```
categories <CONTENT_FILTER_OPERATION_HAVING_DEFAULT_NAME>
```

Mode

Content Filter Profile Object

Description

Set operation for all categories.

Options

<CONTENT_FILTER_OPERATION_HAVING_DEFAULT_NAME> Content filter operation with additional \"default\".
Example: *default*

Example

```
categories default  
categories block
```

Syntax

```
https-filtering
```

Mode

Content Filter Profile Object

Description

Enable CFS HTTPS filtering.

Example

```
https-filtering
```

Syntax

```
no https-filtering
```

Mode

Content Filter Profile Object

Description

Disable CFS HTTPS filtering.

Example

```
no https-filtering
```

Syntax

```
smart-filter
```

Mode

Content Filter Profile Object

Description

Enable smart filtering for embedded URI.

Example

```
smart-filter
```

Syntax

```
no smart-filter
```

Mode

Content Filter Profile Object

Description

Disable smart filtering for embedded URI.

Example

```
smart-filter
```

Syntax

```
safe-search
```

Mode

Content Filter Profile Object

Description

Enable safe search enforcement.

Example

```
safe-search
```

Syntax

```
no safe-search
```

Mode

Content Filter Profile Object

Description

Disable safe search enforcement.

Example

```
no safe-search
```

Syntax

```
google-force-safe-search
```

Mode

Content Filter Profile Object

Description

Enable Google force safe search.

Example

```
google-force-safe-search
```

Syntax

```
no google-force-safe-search
```

Mode

Content Filter Profile Object

Description

Disable Google force safe search.

Example

```
no google-force-safe-search
```

Syntax

```
youtube-restrict-mode
```

Mode

Content Filter Profile Object

Description

Enable YouTube restrict mode.

Example

youtube-restrict-mode

Syntax

no youtube-restrict-mode

Mode

Content Filter Profile Object

Description

Disable YouTube restrict mode.

Example

no youtube-restrict-mode

Syntax

bing-force-safe-search

Mode

Content Filter Profile Object

Description

Enable Bing force safe search.

Example

bing-force-safe-search

Syntax

no bing-force-safe-search

Mode

Content Filter Profile Object

Description

Disable Bing force safe search.

Example

no bing-force-safe-search

Syntax

consent required

Mode

Content Filter Profile Object

Description

Enable consent.

Example

consent required

Syntax

no consent required

Mode

Content Filter Profile Object

Description

Disable consent.

Example

no consent required

Syntax

consent user-idle-timeout <UINT32>

Mode

Content Filter Profile Object

Description

Set consent user idle timeout.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

consent user-idle-timeout 15

Syntax

consent optional page-url <WORD>

Mode

Content Filter Profile Object

Description

Set consent optional page URL.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

consent optional page-url 1.1.1.1/consentOptional.html

Syntax

no consent optional page-url

Mode

Content Filter Profile Object

Description

Clear consent optional page URL.

Example

```
no consent optional page-url
```

Syntax

```
consent mandatory page-url <WORD>
```

Mode

Content Filter Profile Object

Description

Set consent mandatory page URL.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
consent mandatory page-url 1.1.1.1/consentMandatory.html
```

Syntax

```
no consent mandatory page-url
```

Mode

Content Filter Profile Object

Description

Clear consent mandatory page URL.

Example

```
no consent mandatory page-url
```

Syntax

```
consent mandatory address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }  
| any | group <ADDR_HNR_GROUP_MIXED> | name <ADDR_HNR_NAME_MIXED> }
```

Mode

Content Filter Profile Object

Description

Set consent mandatory filtering address.

Options

ipv6 IPv6 Address object.

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

| | |
|-------------------------------------|--|
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Specify IP range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| any | All address. |
| group | Address object group name. |
| <ADDR_HNR_GROUP_MIXED> | Host/network/range group address object name. Example: <i>Sales & Marketing Network Access Points</i> |
| name | Address object name. |
| <ADDR_HNR_NAME_MIXED> | Host/network/range address object name. Example: <i>Web Server</i> |

Example

```
consent mandatory address host 192.168.168.168
consent mandatory address network 192.168.168.0 255.255.255.0
consent mandatory address range 192.168.168.1 192.168.168.10
consent mandatory address ipv6 host fec0:1::1
consent mandatory address ipv6 network fec0:1:: 64
consent mandatory address ipv6 range fec0:1::1 fec0:1::100
consent mandatory address any
consent mandatory address group "Consent Mandatory Address Group"
consent mandatory address name "Consent Mandatory Address Object"
```

Syntax

```
no consent mandatory address
```

Mode

Content Filter Profile Object

Description

Clear consent mandatory filtering address.

Example

```
no consent mandatory address
```

Syntax

```
custom-header insertion
```

Mode

Content Filter Profile Object

Description

Enable custom header insertion.

Example

```
custom-header insertion
```

Syntax

```
no custom-header insertion
```

Mode

Content Filter Profile Object

Description

Disable custom header insertion.

Example

```
no custom-header insertion
```

Syntax

```
custom-header entry <CONTENT_FILTER_CUSTOM_HEADER_DOMAIN> <CONTENT_FILTER_CUSTOM_HEADER_KEY> <CONTENT_FILTER_CUSTOM_HEADER_VALUE>
```

Mode

Content Filter Profile Object

Description

Add new custom header entry into custom header list.

Options

| | |
|--|---|
| <CONTENT_FILTER_CUSTOM_HEADER_DOMAIN> | Content filter custom header domain. Example: <code>\ "YouTube.com\"</code> |
| <CONTENT_FILTER_CUSTOM_HEADER_KEY> | Content filter custom header key. Example: <code>\ "YouTube-Restrict-Mode\"</code> |
| <CONTENT_FILTER_CUSTOM_HEADER_VALUE> | Content filter custom header value. Example: <code>\ "Strict\"</code> |

Example

```
custom-header entry "YouTube.com" "YouTube-Restrict-Mode" "Strict"
```

Syntax

```
no custom-header entry <CONTENT_FILTER_CUSTOM_HEADER_DOMAIN> <CONTENT_FILTER_CUSTOM_HEADER_KEY>  
<CONTENT_FILTER_CUSTOM_HEADER_VALUE>
```

Mode

Content Filter Profile Object

Description

Delete custom header entry from custom header list.

Options

| | |
|--|---|
| <CONTENT_FILTER_CUSTOM_HEADER_DOMAIN> | Content filter custom header domain. Example: <code>\ "YouTube.com\"</code> |
| <CONTENT_FILTER_CUSTOM_HEADER_KEY> | Content filter custom header key. Example: <code>\ "YouTube-Restrict-Mode\"</code> |
| <CONTENT_FILTER_CUSTOM_HEADER_VALUE> | Content filter custom header value. Example: <code>\ "Strict\"</code> |

Example

```
no custom-header entry "YouTube.com" "YouTube-Restrict-Mode" "Strict"
```

Syntax

no custom-header entries

Mode

Content Filter Profile Object

Description

Remove all custom header entries from custom header list.

Example

no custom-header entries

Syntax

```
server <HOSTNAME>
```

Mode

Websense enterprise

Description

Set Websense server address.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
server 192.168.168.100
```

Syntax

```
no server
```

Mode

Websense enterprise

Description

Clear Websense server address.

Example

```
no server
```

Syntax

```
port <IPV4_PORT>
```

Mode

Websense enterprise

Description

Set Websense server port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

port 15868

Syntax

user-name <WORD>

Mode

Websense enterprise

Description

Set user name of Websense.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

user-name *userName*

Syntax

no user-name

Mode

Websense enterprise

Description

Clear user name of Websense.

Example

no user-name

Syntax

max-url-caches <UINT32>

Mode

Websense enterprise

Description

Set maximum URL cache entries that can be added.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

max-url-caches *5120*

Syntax

https-content-filtering

Mode

Websense enterprise

Description

Enable https content filtering.

Example

```
https-content-filtering
```

Syntax

```
no https-content-filtering
```

Mode

Websense enterprise

Description

Disable https content filtering.

Example

```
no https-content-filtering
```

Syntax

```
probe monitoring
```

Mode

Websense enterprise

Description

Enable Websense probe monitoring.

Example

```
probe monitoring
```

Syntax

```
no probe monitoring
```

Mode

Websense enterprise

Description

Disable Websense probe monitoring.

Example

```
no probe monitoring
```

Syntax

```
probe interval <UINT16>
```

Mode

Websense enterprise

Description

Set check server interval in seconds of Websense probe monitoring.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
probe interval 10
```

Syntax

```
probe deactivate-after <UINT8>
```

Mode

Websense enterprise

Description

Set deactivation condition of Websense.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
probe deactivate-after 3
```

Syntax

```
probe reactivate-after <UINT8>
```

Mode

Websense enterprise

Description

Set reactivation condition of Websense.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
probe reactivate-after 2
```

Syntax

```
block-if-server-unavailable
```

Mode

Websense enterprise

Description

Enable block if Websense server is unavailable.

Example

block-if-server-unavailable

Syntax

no block-if-server-unavailable

Mode

Websense enterprise

Description

Disable block if Websense server is unavailable.

Example

no block-if-server-unavailable

Syntax

server-timeout <UINT16>

Mode

Websense enterprise

Description

Set Websense server timeout.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

server-timeout 5

Syntax

block activex

Mode

Websense enterprise

Description

Enable block ActiveX feature.

Example

block activex

Syntax

no block activex

Mode

Websense enterprise

Description

Disable block ActiveX feature.

Example

```
no block activex
```

Syntax

```
block java
```

Mode

Websense enterprise

Description

Enable block Java feature.

Example

```
block java
```

Syntax

```
no block java
```

Mode

Websense enterprise

Description

Disable block Java feature.

Example

```
no block java
```

Syntax

```
block flash
```

Mode

Websense enterprise

Description

Enable block Flash feature.

Example

```
block flash
```

Syntax

```
no block flash
```

Mode

Websense enterprise

Description

Disable block Flash feature.

Example

no block flash

Syntax

block cookies

Mode

Websense enterprise

Description

Enable block cookies feature.

Example

block cookies

Syntax

no block cookies

Mode

Websense enterprise

Description

Disable block cookies feature.

Example

no block cookies

Syntax

block http-proxy-access

Mode

Websense enterprise

Description

Enable block access to HTTP proxy feature.

Example

block http-proxy-access

Syntax

no block http-proxy-access

Mode

Websense enterprise

Description

Disable block Access to HTTP Proxy feature.

Example

no block http-proxy-access

Syntax

`exclude web-features-domains <CONTENT_FILTER_URI_LIST_NAME>`

Mode

Websense enterprise

Description

Set excluded domains of block web features.

Options

`<CONTENT_FILTER_URI_LIST_NAME>` Content filter URI list object/group name.
Example: `White URI list`

Example

`exclude web-features-domains uriListName`

Syntax

`no exclude web-features-domains`

Mode

Websense enterprise

Description

Clear excluded domains of block web features.

Example

`no exclude web-features-domains`

Syntax

`exclude administrator`

Mode

Websense enterprise

Description

Enable exclude administrator.

Example

`exclude administrator`

Syntax

`no exclude administrator`

Mode

Websense enterprise

Description

Disable exclude administrator.

Example

no exclude administrator

Syntax

```
exclude address { { [ ipv6 ] { fqdn <ADDR_FQDN> | host <ADDR_HOST> | mac <ADDR_MAC> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Websense enterprise

Description

Exclude address.

Options

| | |
|---|---|
| ipv6 | IPv6 Address object. |
| fqdn <ADDR_FQDN> | Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| host <ADDR_HOST> | Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i> |
| mac <ADDR_MAC> | Address object MAC Address. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| network <ADDR_NETWORK> | Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> | Specify IP range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group <ADDR_GROUP_NAME_MIXED> | Address object group name. Group address object name. Example: <i>Sales Group</i> |
| name <ADDR_NAME_MIXED> | Address object name. Address object name. Example: <i>Web Server</i> |

Example

```
exclude address host 192.168.168.168
exclude address network 192.168.168.0 255.255.255.0
exclude address range 192.168.168.1 192.168.168.10
exclude address mac D067E534E99C
exclude address fqdn example.com
exclude address ipv6 host fec0:1::1
exclude address ipv6 network fec0:1:: 64
exclude address ipv6 range fec0:1::1 fec0:1::100
exclude address group "Corp Websense Exclusion Group"
exclude address name "Corp Websense Exclusion Object"
```

Syntax

no exclude address

Mode

Websense enterprise

Description

Clear excluded address.

Example

```
no exclude address
```

Syntax

```
blocking-page { custom <WORD> | default }
```

Mode

Websense enterprise

Description

Set Websense blocking page.

Options

custom Use custom defined page.
<WORD> Word in the form: WORD or "QUOTED STRING".
Example: *abc*

default Use default page.

Example

```
blocking-page custom "<html> ... </html>"  
blocking-page default
```

Syntax

```
anti-spam
```

Mode

Config

Description

Enter anti-spam configuration mode.

Example

```
anti-spam
```

Syntax

```
start capture
```

Mode

Anti-Spam

Description

Start e-mail stream packet capture.

Example

```
start capture
```

Syntax

stop capture

Mode

Anti-Spam

Description

Stop e-mail stream packet capture.

Example

stop capture

Syntax

clear capture

Mode

Anti-Spam

Description

Clear the e-mail stream packet capture buffer.

Example

clear capture

Syntax

export capture { ftp <FTP_URL> | scp <SCP_URL> }

Mode

Anti-Spam

Description

Download e-mail stream capture data.

Options

ftp Export using the FTP protocol.

<FTP_URL> FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/

scp Export using the SCP protocol.

<SCP_URL> SCP URL in the form: scp://username@host/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: scp://username@host/\nscp://host/

Example

export capture ftp ftp://user:password@servername/packet-hd.html
export capture scp scp://user@server/packet-hd.html

Syntax

grid-ip-check <IPV4_HOST>

Mode

Anti-Spam

Description

Do the IP reputation check with the SonicWall GRID network with the given ip address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
grid-ip-check 10.10.10.10
```

Syntax

```
enable
```

Mode

Anti-Spam

Description

Enable anti-spam service.

Example

```
enable
```

Syntax

```
destination-mail-server public <IPV4_HOST> private <IPV4_HOST> zone <ANTI_SPAM_DMS_ZONE> port <IPV4_PORT>
```

Mode

Anti-Spam

Description

Set the destination mail server configuration.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

private Set the destination mail server public IP.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

zone Set the destination mail server zone assignment.

<ANTI_SPAM_DMS_ZONE> Zone object name.
Example: *DMZ*

port Set the destination mail server inbound e-mail port.

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
destination-mail-server public 192.168.168.110 private 192.168.1.2 zone LAN port 25
```

Syntax

```
no enable
```

Mode

Anti-Spam

Description

Disable anti-spam service.

Example

```
no enable
```

Syntax

```
action likely-spam { delete | filtering-off | store | tag }
```

Mode

Anti-Spam

Description

Set the action for the likely spam category.

Options

delete Permanently delete.

filtering-off Filtering off.

store Store in junk box.

tag Tag the email.

Example

```
action likely-spam filtering-off
```

Syntax

```
action definite-spam { delete | filtering-off | store | tag }
```

Mode

Anti-Spam

Description

Set the action for the definite spam category.

Options

delete Permanently delete.

filtering-off Filtering off.

store Store in junk box.

tag Tag the email.

Example

```
action definite-spam tag
```

Syntax

```
action likely-phishing { delete | filtering-off | store | tag }
```

Mode

Anti-Spam

Description

Set the action for the likely phishing category.

Options

delete Permanently delete.

filtering-off Filtering off.

store Store in junk box.

tag Tag the email.

Example

```
action likely-phishing tag
```

Syntax

```
action definite-phishing { delete | filtering-off | store | tag }
```

Mode

Anti-Spam

Description

Set the action for the definite phishing category.

Options

delete Permanently delete.

filtering-off Filtering off.

store Store in junk box.

tag Tag the email.

Example

```
action definite-phishing delete
```

Syntax

```
action likely-virus { delete | filtering-off | store | tag }
```

Mode

Anti-Spam

Description

Set the action for the likely spam category.

Options

delete Permanently delete.

filtering-off Filtering off.

store Store in junk box.

tag Tag the email.

Example

```
action likely-virus tag
```

Syntax

```
action definite-virus { delete | filtering-off | store | tag }
```

Mode

Anti-Spam

Description

Set the action for the definite virus category.

Options

delete Permanently delete.

filtering-off Filtering off.

store Store in junk box.

tag Tag the email.

Example

```
action definite-virus delete
```

Syntax

```
allow-list { fqdn <ANTI_SPAM_ADDR_FQDN> | host <ANTI_SPAM_ADDR_HOST> | name <ANTI_SPAM_ADDR_NAME> | range <ANTI_SPAM_ADDR_BEGIN>  
<ANTI_SPAM_ADDR_END> }
```

Mode

Anti-Spam

Description

Add address object to the allow client list.

Options

fqdn Address object full qualified domain name (FQDN).
<ANTI_SPAM_ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

host Address object host.
<ANTI_SPAM_ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ANTI_SPAM_ADDR_NAME> Address object name.
Example: *Web Server*

range Address object range.
<ANTI_SPAM_ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.

Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ANTI_SPAM_ADDR_END>

IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n

Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
allow-list host 168.226.49.15
allow-list name "X3 IP"
allow-list range 192.168.1.100 192.168.1.150
allow-list fqdn "www.sonicwall.com"
```

Syntax

```
no allow-list { fqdn <ANTI_SPAM_ADDR_FQDN> | host <ANTI_SPAM_ADDR_HOST> | name <ANTI_SPAM_ADDR_NAME> | range
<ANTI_SPAM_ADDR_BEGIN> <ANTI_SPAM_ADDR_END> }
```

Mode

Anti-Spam

Description

Remove address object from the allow client list.

Options

| | |
|-------------------------------------|--|
| fqdn | Address object full qualified domain name (FQDN). |
| <ANTI_SPAM_ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| host | Address object host. |
| <ANTI_SPAM_ADDR_HOST> | IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ANTI_SPAM_ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| range | Address object range. |
| <ANTI_SPAM_ADDR_BEGIN> | IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ANTI_SPAM_ADDR_END> | IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
no allow-list host 168.226.49.15
no allow-list name "X3 IP"
no allow-list range 192.168.1.100 192.168.1.150
no allow-list fqdn "www.sonicwall.com"
```

Syntax

```
reject-list { fqdn <ANTI_SPAM_ADDR_FQDN> | host <ANTI_SPAM_ADDR_HOST> | name <ANTI_SPAM_ADDR_NAME> | range <ANTI_SPAM_ADDR_BEGIN>
<ANTI_SPAM_ADDR_END> }
```

Mode

Anti-Spam

Description

Add address object to the reject client list.

Options

| | |
|-------------------------------------|---|
| <i>fqdn</i> | Address object full qualified domain name (FQDN). |
| <ANTI_SPAM_ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| <i>host</i> | Address object host. |
| <ANTI_SPAM_ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <i>name</i> | Address object name. |
| <ANTI_SPAM_ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| <i>range</i> | Address object range. |
| <ANTI_SPAM_ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ANTI_SPAM_ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
reject-list host 168.226.49.15
reject-list name "X3 IP"
reject-list range 192.168.1.100 192.168.1.150
reject-list fqdn "www.sonicwall.com"
```

Syntax

```
no reject-list { fqdn <ANTI_SPAM_ADDR_FQDN> | host <ANTI_SPAM_ADDR_HOST> | name <ANTI_SPAM_ADDR_NAME> | range <ANTI_SPAM_ADDR_BEGIN> <ANTI_SPAM_ADDR_END> }
```

Mode

Anti-Spam

Description

Remove address object from the reject client list.

Options

| | |
|-------------------------------------|---|
| <i>fqdn</i> | Address object full qualified domain name (FQDN). |
| <ANTI_SPAM_ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| <i>host</i> | Address object host. |
| <ANTI_SPAM_ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <i>name</i> | Address object name. |
| <ANTI_SPAM_ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| <i>range</i> | Address object range. |
| <ANTI_SPAM_ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ANTI_SPAM_ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
no reject-list host 168.226.49.15
no reject-list name "X3 IP"
no reject-list range 192.168.1.100 192.168.1.150
no reject-list fqdn "www.sonicwall.com"
```

Syntax

```
service-down { allow | reject }
```

Mode

Anti-Spam

Description

Set action of delivery of unprocessed mail when SonicWall anti-spam service is unavailable.

Options

allow Allow.

reject Reject.

Example

```
service-down reject  
service-down allow
```

Syntax

```
junk-box down { delete | tag-deliver }
```

Mode

Anti-Spam

Description

Set action for e-mails when junk box is unavailable.

Options

delete Delete.

tag-deliver Tag and deliver.

Example

```
junk-box down tag-deliver  
junk-box down delete
```

Syntax

```
junk-box secure-http
```

Mode

Anti-Spam

Description

Enable use secure HTTP for junk box messaging.

Example

```
junk-box secure-http
```

Syntax

```
no junk-box secure-http
```

Mode

Anti-Spam

Description

Disable use secure HTTP for junk box messaging.

Example

```
no junk-box secure-http
```

Syntax

```
junk-box port <IPV4_PORT>
```

Mode

Anti-Spam

Description

Set the junk box messaging port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
junk-box port 80
```

Syntax

```
no junk-box port
```

Mode

Anti-Spam

Description

Clear the junk box messaging port.

Example

```
no junk-box port
```

Syntax

```
probe interval <UINT8>
```

Mode

Anti-Spam

Description

Set the monitoring service probe interval in minutes.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
probe interval 5
```

Syntax

```
probe timeout <UINT16>
```

Mode

Anti-Spam

Description

Set the monitoring service probe timeout in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
probe timeout 30
```

Syntax

```
success-threshold <UINT8>
```

Mode

Anti-Spam

Description

Set the monitoring service probe success count threshold.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
success-threshold 1
```

Syntax

```
failure-threshold <UINT8>
```

Mode

Anti-Spam

Description

Set the monitoring service probe failure count threshold.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
failure-threshold 3
```

Syntax

```
mail-server { port <IPV4_PORT> | private <IPV4_HOST> | public <IPV4_HOST> }
```

Mode

Anti-Spam

Description

Set the destination mail server public IP address, private IP address and inbound e-mail port.

Options

port Set the destination mail server inbound e-mail port.
<IPV4_PORT> Integer in the form: D OR 0xHHHHH.
Example: 80

private Set the destination mail server private IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

public Set the destination mail server public IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
mail-server private 192.168.168.10  
mail-server public 192.168.168.110  
mail-server port 25
```

Syntax

```
no mail-server { port | private | public }
```

Mode

Anti-Spam

Description

Clear the destination mail server public or private IP address or inbound e-mail port.

Options

port Clear the destination mail server inbound e-mail port.

private Clear the destination mail server private IP address.

public Clear the destination mail server public IP address.

Example

```
no mail-server ip private  
no mail-server ip public  
no mail-server port
```

Syntax

```
destination-mail-address-as-junk-store
```

Mode

Anti-Spam

Description

Enable use destination mail server private address as junk store IP address.

Example

```
destination-mail-address-as-junk-store
```

Syntax

```
no destination-mail-address-as-junk-store
```

Mode

Anti-Spam

Description

Disable use destination mail server private address as junk store IP address.

Example

```
no destination-mail-address-as-junk-store
```

Syntax

```
junk-store-ip <IPV4_HOST>
```

Mode

Anti-Spam

Description

Set junk store ip address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
junk-store-ip 192.168.168.168
```

Syntax

```
system-detection
```

Mode

Anti-Spam

Description

Enable e-mail system detection.

Example

```
system-detection
```

Syntax

```
no system-detection
```

Mode

Anti-Spam

Description

Disable e-mail system detection.

Example

```
no system-detection
```

Syntax

```
intrusion-prevention
```

Mode

Config

Description

Enter intrusion prevention configuration mode.

Example

```
intrusion-prevention
```

Syntax

```
update-signatures
```

Mode

IPS

Description

Update signature database.

Example

```
update-signatures
```

Syntax

```
enable
```

Mode

IPS

Description

Enable intrusion prevention.

Example

```
enable
```

Syntax

```
no enable
```

Mode

IPS

Description

Disable intrusion prevention.

Example

```
no enable
```

Syntax

```
signature-group high-priority { detect-all | log-redundancy <UINT32> | prevent-all }
```

Mode

IPS

Description

Enable signature group high priority detection and log redundancy.

Options

detect-all Detect all.

log-redundancy Set log redundancy in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

prevent-all Prevent all.

Example

```
signature-group high-priority prevent-all  
signature-group high-priority log-redundancy 60
```

Syntax

```
signature-group medium-priority { detect-all | log-redundancy <UINT32> | prevent-all }
```

Mode

IPS

Description

Enable signature group medium priority detection and log redundancy.

Options

detect-all Detect all.

log-redundancy Set log redundancy in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

prevent-all Prevent all.

Example

```
signature-group medium-priority prevent-all  
signature-group medium-priority log-redundancy 60
```

Syntax

```
signature-group low-priority { detect-all | log-redundancy <UINT32> | prevent-all }
```

Mode

IPS

Description

Enable signature group low priority detection and log redundancy.

Options

| | |
|------------------------------|---|
| <i>detect-all</i> | Detect all. |
| <i>log-redundancy</i> | Set log redundancy in seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: 123 |
| <i>prevent-all</i> | Prevent all. |

Example

```
signature-group low-priority prevent-all
signature-group low-priority log-redundancy 60
```

Syntax

```
no signature-group high-priority { detect-all | log-redundancy | prevent-all }
```

Mode

IPS

Description

Disable signature group high priority detection and log redundancy.

Options

| | |
|------------------------------|-----------------------|
| <i>detect-all</i> | Detect all. |
| <i>log-redundancy</i> | Clear log redundancy. |
| <i>prevent-all</i> | Prevent all. |

Example

```
no signature-group high-priority prevent-all
no signature-group high-priority log-redundancy
```

Syntax

```
no signature-group medium-priority { detect-all | log-redundancy | prevent-all }
```

Mode

IPS

Description

Disable signature group medium priority detection and log redundancy.

Options

| | |
|------------------------------|-----------------------|
| <i>detect-all</i> | Detect all. |
| <i>log-redundancy</i> | Clear log redundancy. |
| <i>prevent-all</i> | Prevent all. |

Example

```
no signature-group medium-priority prevent-all
no signature-group medium-priority log-redundancy
```

Syntax

```
no signature-group low-priority { detect-all | log-redundancy | prevent-all }
```

Mode

IPS

Description

Disable signature group low priority detection and log redundancy.

Options

detect-all Detect all.

log-redundancy Clear log redundancy.

prevent-all Prevent all.

Example

```
no signature-group low-priority prevent-all
no signature-group low-priority log-redundancy
```

Syntax

```
reset
```

Mode

IPS

Description

Reset intrusion prevention settings to default.

Example

```
reset
```

Syntax

```
category { id <IPS_CATEGORY_ID> | name <IPS_CATEGORY_NAME> } [ policy { id <IPS_POLICY_ID> | name <IPS_POLICY_NAME> } ]
```

Mode

IPS

Description

Enter configuration mode for the specified IPS category.

Options

id IPS category ID.

<IPS_CATEGORY_ID> Category ID.
Example: 1234

name IPS category name.

<IPS_CATEGORY_NAME> Category name.
Example: ACTIVEX

policy Configure the IPS policy and enter its configure mode.

id IPS policy ID.
<IPS_POLICY_ID> Policy ID.
 Example: 1234

name IPS policy name.
<IPS_POLICY_NAME> Policy name.
 Example: ActivePDF WebGrabber ActiveX Instantiation

Example

```
category name "BACKDOOR"
category id 2 policy id 6483
category id 61 policy name "ActivePDF WebGrabber ActiveX Instantiation"
```

Syntax

```
exclusion { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | entry
<IPS_EXCLUSION_BEGIN_IPV4_HOST> <IPS_EXCLUSION_END_IPV4_HOST> | group <ADDR_GROUP_NAME_MIXED> | list | name <ADDR_NAME_MIXED> }
```

Mode

IPS

Description

Configure IPS exclusion list.

Options

ipv6 Excluded IPv6 addresses.

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
 Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
 Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
 Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*
<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
 Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

entry IPS exclusion list entry.
<IPS_EXCLUSION_BEGIN_IPV4_HOST> IPS Exclusion List entry begin IPv4 in the form: D.D.D.D.
 Example: *192.168.168.168*
<IPS_EXCLUSION_END_IPV4_HOST> IPS Exclusion List entry end IPv4 in the form: D.D.D.D.
 Example: *192.168.168.168*

group Address object group
<ADDR_GROUP_NAME_MIXED> Group address object name.
 Example: *Sales Group*

list Enable IPS exclusion list.

name Address object name
<ADDR_NAME_MIXED> Address object name.
 Example: *Web Server*

Example


```
exclusion list
exclusion name "WLAN Subnets"
exclusion entry 10.10.10.1 10.10.10.10
```

Syntax

```
no exclusion { entries | entry <IPS_EXCLUSION_BEGIN_IPV4_HOST> <IPS_EXCLUSION_END_IPV4_HOST> | list }
```

Mode

IPS

Description

Disable IPS exclusion list.

Options

| | |
|--|---|
| entries | Delete all IPS exclusion list entries. |
| entry | Delete one IPS exclusion list entry. |
| <IPS_EXCLUSION_BEGIN_IPV4_HOST> | IPS Exclusion List entry begin IPv4 in the form: D.D.D.D. Example: 192.168.168.168 |
| <IPS_EXCLUSION_END_IPV4_HOST> | IPS Exclusion List entry end IPv4 in the form: D.D.D.D. Example: 192.168.168.168 |
| list | Disable IPS exclusion list. |

Example

```
no exclusion list
no exclusion entries
no exclusion entry 10.10.10.1 10.10.10.10
```

Syntax

```
name <WORD>
```

Mode

IPS Category
IPS Policy

Description

Category name or policy name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
name ACTIVEX
```

Syntax

```
id <UINT32>
```

Mode

IPS Category
IPS Policy

Description

Category ID or policy ID.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

id 8

Syntax

prevention [enable | global]

Mode

IPS Category

Description

Set prevention for IPS category.

Options

enable Enable IPS category prevention.

global Use global setting.

Example

prevention global

Syntax

no prevention

Mode

IPS Category

Description

Disable prevention for IPS category.

Example

no prevention

Syntax

detection [enable | global]

Mode

IPS Category

Description

Set detection for IPS category.

Options

enable Enable IPS category detection.

global Use global setting.

Example

```
detection global
```

Syntax

```
no detection
```

Mode

IPS Category

Description

Disable detection for IPS category.

Example

```
no detection
```

Syntax

```
included users { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

IPS Category

Description

Set included users/groups.

Options

| | |
|--------------------------------------|---|
| administrator | Built-in administrator. |
| all | All. |
| group | Specify local user group. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests. |
| name | Specify local user. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
included users all
```

Syntax

```
excluded users { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

IPS Category

Description

Set excluded users/groups.

Options

| | |
|--------------------------------------|---|
| administrator | Built-in administrator. |
| group | Specify local user group. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests. |
| name | Specify local user. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

excluded users guests

Syntax

```
included ip { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | all | group
<ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

IPS Category

Description

Set included IP address range.

Options

| | |
|--------------------------------------|---|
| ipv6 | Included IPv6 addresses. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Specify IP range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| all | All. |
| group | Address object group. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| name | Specify name of range address object. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

included ip range 10.10.10.1 10.10.10.10

Syntax

```
excluded ip { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

IPS Category

Description

Set excluded IP address range.

Options

| | |
|---|--|
| ipv6 | Excluded IPv6 addresses. |
| host <ADDR_HOST> | Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network <ADDR_NETWORK> | Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> | Specify IP range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group <ADDR_GROUP_NAME_MIXED> | Address object group. Group address object name. Example: <i>Sales Group</i> |
| name <ADDR_NAME_MIXED> | Specify name of range address object. Address object name. Example: <i>Web Server</i> |

Example

```
excluded ip range 10.10.10.1 10.10.10.10
```

Syntax

```
no excluded { ip | users }
```

Mode

IPS Category

Description

Don't excluded any users/groups or IP addresses.

Options

| | |
|--------------|----------------------------------|
| ip | Don't excluded any IP addresses. |
| users | Don't excluded any users/groups. |

Example

```
no excluded users  
no excluded ip
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

IPS Category

Description

Set IPS category schedule.

Options

| | |
|---------------------------------|---|
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule always-on
```

Syntax

```
log-redundancy { filter <UINT16> | global }
```

Mode

IPS Category

Description

Set IPS category log redundancy filter.

Options

| | |
|-----------------------|--|
| filter | Set log redundancy filter in seconds. |
| <UINT16> | Integer in the form: D OR 0xHHHH. Example: <i>123</i> |
| global | Use global setting. |

Example

```
log-redundancy filter 45
```

Syntax

```
category <WORD>
```

Mode

IPS Policy

Description

IPS policy's category name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
category ACTIVEX
```

Syntax

```
prevention [ category | enable ]
```

Mode

IPS Policy

Description

Set prevention for IPS policy.

Options

category Use category setting.

enable Enable IPS policy prevention.

Example

```
prevention category
```

Syntax

```
no prevention
```

Mode

IPS Policy

Description

Disable prevention for IPS policy.

Example

```
no prevention
```

Syntax

```
detection [ category | enable ]
```

Mode

IPS Policy

Description

Set detection for IPS policy.

Options

category Use category setting.

enable Enable IPS policy detection.

Example

```
detection category
```

Syntax

```
no detection
```

Mode

IPS Policy

Description

Disable detection for IPS policy.

Example

```
no detection
```

Syntax

```
included users { administrator | all | category | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

IPS Policy

Description

Set included users/groups.

Options

| | |
|--------------------------------------|---|
| administrator | Built-in administrator. |
| all | All. |
| category | Use category setting. |
| group | Specify local user group. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests. |
| name | Specify local user. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
included users all
```

Syntax

```
excluded users { administrator | category | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

IPS Policy

Description

Set excluded users/groups.

Options

| | |
|--------------------------------------|---|
| administrator | Built-in administrator. |
| category | Use category setting. |
| group | Specify local user group. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests. |
| name | Specify local user. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
excluded users guests
```

Syntax

```
included ip { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | all | category | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

IPS Policy

Description

Set included IP address range.

Options

| | |
|--------------------------------------|---|
| ipv6 | Included IPv6 addresses. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\nExample: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| all | All. |
| category | Use category setting. |
| group | Address object group. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |

name Address object name.
<ADDR_NAME_MIXED> Address object name.
Example: *Web Server*

Example

```
included ip range 10.10.10.1 10.10.10.10
```

Syntax

```
excluded ip { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | category | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

IPS Policy

Description

Set excluded IP address range.

Options

ipv6 Excluded IPv6 addresses.

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

category Use category setting.

group Address object group.
<ADDR_GROUP_NAME_MIXED> Group address object name.
Example: *Sales Group*

name Address object name.
<ADDR_NAME_MIXED> Address object name.
Example: *Web Server*

Example

```
excluded ip range 10.10.10.1 10.10.10.10
```

Syntax

```
no excluded { ip | users }
```

Mode

IPS Policy

Description

Don't excluded any users/groups or IP addresses.

Options

ip Don't excluded any IP addresses.

users Don't excluded any users/groups.

Example

```
no excluded users
no excluded ip
```

Syntax

```
schedule { always-on | category | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

IPS Policy

Description

Set IPS policy schedule.

Options

| | |
|---------------------------------|---|
| always-on | Always on. |
| category | Use category setting. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule always-on
```

Syntax

```
log-redundancy { category | filter <UINT16> }
```

Mode

IPS Policy

Description

Set IPS policy log redundancy filter.

Options

category Use category setting.

filter Set log redundancy filter in seconds.
<UINT16> Integer in the form: D OR 0xHHHH.

Example

```
log-redundancy filter 45
```

Syntax

```
priority { high | low | medium }
```

Mode

IPS Policy

Description

Set IPS policy priority.

Options

high High priority.

low Low priority.

medium Medium priority.

Example

```
priority high
```

Syntax

```
direction { both | incoming | outgoing } [ to-client ] [ to-server ]
```

Mode

IPS Policy

Description

Set IPS policy direction.

Options

both Both.

incoming Incoming.

outgoing Outgoing.

to-client To client.

to-server To server.

Example

```
direction both
```

Syntax

```
gateway-antivirus
```

Mode

Config

Description

Enter Gateway Anti-Virus Configuration Mode.

Example

```
gateway-antivirus
```

Syntax

```
update-signatures
```

Mode

Gateway Anti-Virus

Description

Update signature database.

Example

```
update-signatures
```

Syntax

```
enable
```

Mode

Gateway Anti-Virus

Description

Enable Gateway Anti-Virus service.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Gateway Anti-Virus

Description

Disable Gateway Anti-Virus service.

Example

```
no enable
```

Syntax

```
signature { id <GAV_SIG_ID> | name <GAV_SIG_NAME> }
```

Mode

Gateway Anti-Virus

Description

Enable signature.

Options

| | |
|-----------------------------|---|
| <i>id</i> | Signature ID. |
| <GAV_SIG_ID> | Signature ID. Example: 1234 |
| <i>name</i> | Signature name. |
| <GAV_SIG_NAME> | Signature name. Example: 007SpySoft.G (Trojan) |

Example

```
signature name "180Solutions_6 (Adware)"
```

Syntax

```
no signature { id <GAV_SIG_ID> | name <GAV_SIG_NAME> }
```

Mode

Gateway Anti-Virus

Description

Disable signature.

Options

| | |
|-----------------------------|---|
| <i>id</i> | Signature ID. |
| <GAV_SIG_ID> | Signature ID. Example: 1234 |
| <i>name</i> | Signature name. |
| <GAV_SIG_NAME> | Signature name. Example: 007SpySoft.G (Trojan) |

Example

```
no signature name "180Solutions_6 (Adware)"
```

Syntax

```
inbound-inspection { cifs-netbios | ftp | http | imap | pop3 | smtp | tcp-stream }
```

Mode

Gateway Anti-Virus

Description

Enable inbound inspection for the specified protocols.

Options

| | |
|----------------------------|---------------|
| <i>cifs-netbios</i> | CIFS/NetBIOS. |
| <i>ftp</i> | FTP. |
| <i>http</i> | HTTP. |
| <i>imap</i> | IMAP. |
| <i>pop3</i> | POP3. |

smtp SMTP.

tcp-stream TCP Stream.

Example

```
inbound-inspection http
```

Syntax

```
no inbound-inspection { cifs-netbios | ftp | http | imap | pop3 | smtp | tcp-stream }
```

Mode

Gateway Anti-Virus

Description

Disable inbound inspection for the specified protocols.

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

http HTTP.

imap IMAP.

pop3 POP3.

smtp SMTP.

tcp-stream TCP Stream.

Example

```
no inbound-inspection http
```

Syntax

```
outbound-inspection { ftp | http | smtp | tcp-stream }
```

Mode

Gateway Anti-Virus

Description

Enable outbound inspection for the specified protocols.

Options

ftp FTP.

http HTTP.

smtp SMTP.

tcp-stream TCP Stream.

Example

```
outbound-inspection http
```

Syntax

```
no outbound-inspection { ftp | http | smtp | tcp-stream }
```

Mode

Gateway Anti-Virus

Description

Disable outbound inspection for the specified protocols.

Options

| | |
|-------------------|-------------|
| <i>ftp</i> | FTP. |
| <i>http</i> | HTTP. |
| <i>smtp</i> | SMTP. |
| <i>tcp-stream</i> | TCP Stream. |

Example

```
no outbound-inspection http
```

Syntax

```
restrict password-protected-zip { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Enable restricting transfer of password-protected ZIP files for the specified protocols.

Options

| | |
|---------------------|---------------|
| <i>cifs-netbios</i> | CIFS/NetBIOS. |
| <i>ftp</i> | FTP. |
| <i>http</i> | HTTP. |
| <i>imap</i> | IMAP. |
| <i>pop3</i> | POP3. |
| <i>smtp</i> | SMTP. |

Example

```
restrict password-protected-zip http
```

Syntax

```
no restrict password-protected-zip { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Disable restricting transfer of password-protected ZIP files for the specified protocols.

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

http HTTP.

imap IMAP.

pop3 POP3.

smtp SMTP.

Example

```
no restrict password-protected-zip http
```

Syntax

```
restrict ms-office-macros { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Enable restricting transfer of MS-Office type files containing macros (VBA 5 and above).

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

http HTTP.

imap IMAP.

pop3 POP3.

smtp SMTP.

Example

```
restrict ms-office-macros http
```

Syntax

```
no restrict ms-office-macros { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Disable restricting transfer of MS-Office type files containing macros (VBA 5 and above) for the specified protocols.

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

http HTTP.

imap IMAP.

pop3 POP3.

smtp SMTP.

Example

```
no restrict ms-office-macros http
```

Syntax

```
restrict packed-executables { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Enable restricting transfer of packed executable files (UPX, FSG, etc.) for the specified protocols.

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

http HTTP.

imap IMAP.

pop3 POP3.

smtp SMTP.

Example

```
restrict packed-executables http
```

Syntax

```
no restrict packed-executables { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Disable restricting transfer of packed executable files (UPX, FSG, etc.) for the specified protocols.

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

| | |
|-------------|-------|
| http | HTTP. |
| imap | IMAP. |
| pop3 | POP3. |
| smtp | SMTP. |

Example

```
no restrict packed-executables http
```

Syntax

```
exclusion-object http { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Gateway Anti-Virus

Description

Configure gateway AV protocol exclusion address objects.

Options

| | |
|---|---|
| ipv6 | Excluded IPv6 addresses. |
| host <ADDR_HOST> | Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network <ADDR_NETWORK> | Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> | Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group <ADDR_GROUP_NAME_MIXED> | Address object group Group address object name. Example: <i>Sales Group</i> |
| name <ADDR_NAME_MIXED> | Address object name Address object name. Example: <i>Web Server</i> |

Example

```
exclusion-object http name "WLAN Subnets"
```

Syntax

```
exclusion-object ftp { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Description

Configure gateway AV protocol exclusion address objects.

Options

| | |
|--------------------------------------|--|
| ipv6 | Excluded IPv6 addresses. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group | Address object group |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| name | Address object name |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
exclusion-object ftp name "WLAN Subnets"
```

Syntax

```
exclusion-object imap { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Gateway Anti-Virus

Description

Configure gateway AV protocol exclusion address objects.

Options

| | |
|-----------------------------|--|
| ipv6 | Excluded IPv6 addresses. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |

| | |
|--------------------------------------|--|
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group | Address object group |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| name | Address object name |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
exclusion-object imap name "WLAN Subnets"
```

Syntax

```
exclusion-object smtp { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Gateway Anti-Virus

Description

Configure gateway AV protocol exclusion address objects.

Options

| | |
|--------------------------------------|--|
| ipv6 | Excluded IPv6 addresses. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group | Address object group |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| name | Address object name |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
exclusion-object smtp name "WLAN Subnets"
```

Syntax

```
exclusion-object pop3 { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Gateway Anti-Virus

Description

Configure gateway AV protocol exclusion address objects.

Options

| | |
|---|---|
| ipv6 | Excluded IPv6 addresses. |
| host <ADDR_HOST> | Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network <ADDR_NETWORK> | Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> | Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group <ADDR_GROUP_NAME_MIXED> | Address object group Group address object name. Example: <i>Sales Group</i> |
| name <ADDR_NAME_MIXED> | Address object name Address object name. Example: <i>Web Server</i> |

Example

```
exclusion-object pop3 name "WLAN Subnets"
```

Syntax

```
exclusion-object cifs-netbios { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Gateway Anti-Virus

Description

Configure gateway AV protocol exclusion address objects.

Options

| | |
|----------------------------|--|
| ipv6 | Excluded IPv6 addresses. |
| host <ADDR_HOST> | Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |

| | |
|--------------------------------------|--|
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group | Address object group |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| name | Address object name |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
exclusion-object cifs-netbios name "WLAN Subnets"
```

Syntax

```
no exclusion-object { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Clear gateway AV protocol exclusion address objects.

Options

| | |
|---------------------|---|
| cifs-netbios | Clear CIFS/NetBIOS protocol exclusion address object. |
| ftp | Clear FTP protocol exclusion address object. |
| http | Clear HTTP protocol exclusion address object. |
| imap | Clear IMAP protocol exclusion address object. |
| pop3 | Clear POP3 protocol exclusion address object. |
| smtp | Clear SMTP protocol exclusion address object. |

Example

```
no exclusion-object http
```

Syntax

```
reset-settings
```

Mode

Gateway Anti-Virus

Description

Reset Gateway Anti-Virus Settings to default.

Example

```
reset-settings
```

Syntax

```
cloud anti-virus-database
```

Mode

Gateway Anti-Virus

Description

Enable Cloud Anti-Virus Database.

Example

```
cloud anti-virus-database
```

Syntax

```
no cloud anti-virus-database
```

Mode

Gateway Anti-Virus

Description

Disable Cloud Anti-Virus Database.

Example

```
no cloud anti-virus-database
```

Syntax

```
cloud exclusion { id <GAV_SIG_ID> | name <GAV_SIG_NAME> }
```

Mode

Gateway Anti-Virus

Description

Add a Cloud Anti-Virus Database exclusion.

Options

| | |
|-----------------------------|---|
| id | Signature ID. |
| <GAV_SIG_ID> | Signature ID. Example: 1234 |
| name | Signature name. |
| <GAV_SIG_NAME> | Signature name. Example: 007SpySoft.G (Trojan) |

Example

```
cloud exclusion id 1345342
```

Syntax


```
no cloud exclusion { id <GAV_SIG_ID> | name <GAV_SIG_NAME> }
```

Mode

Gateway Anti-Virus

Description

Remove a Cloud Anti-Virus Database exclusion.

Options

| | |
|-----------------------------|---|
| id | Signature ID. |
| <GAV_SIG_ID> | Signature ID. Example: 1234 |
| name | Signature name. |
| <GAV_SIG_NAME> | Signature name. Example: 007SpySoft.G (Trojan) |

Example

```
no cloud exclusion id 1345342
```

Syntax

```
no cloud exclusions
```

Mode

Gateway Anti-Virus

Description

Delete all Cloud Anti-Virus Database exclusions.

Example

```
no cloud exclusions
```

Syntax

```
smtp-responses
```

Mode

Gateway Anti-Virus

Description

Enable SMTP responses.

Example

```
smtp-responses
```

Syntax

```
no smtp-responses
```

Mode

Gateway Anti-Virus

Description

Disable SMTP responses.

Example

no smtp-responses

Syntax

eicar-detection

Mode

Gateway Anti-Virus

Description

Enable detection of EICAR test virus.

Example

eicar-detection

Syntax

no eicar-detection

Mode

Gateway Anti-Virus

Description

Disable detection of EICAR test virus.

Example

no eicar-detection

Syntax

http-byte-range

Mode

Gateway Anti-Virus

Description

Enable HTTP Byte-Range requests with Gateway AV.

Example

http-byte-range

Syntax

no http-byte-range

Mode

Gateway Anti-Virus

Description

Disable HTTP Byte-Range requests with Gateway AV.

Example

no http-byte-range

Syntax

ftp-rest

Mode

Gateway Anti-Virus

Description

Enable FTP 'REST' requests with Gateway AV.

Example

ftp-rest

Syntax

no ftp-rest

Mode

Gateway Anti-Virus

Description

Disable FTP 'REST' requests with Gateway AV.

Example

no ftp-rest

Syntax

scan-high-compression

Mode

Gateway Anti-Virus

Description

Scan parts of files with high compression ratios.

Example

scan-high-compression

Syntax

no scan-high-compression

Mode

Gateway Anti-Virus

Description

Do not scan parts of files with high compression ratios.

Example

no scan-high-compression

Syntax

block-multiple-compress-files

Mode

Gateway Anti-Virus

Description

Enable to block files with multiple levels of zip/gzip compression.

Example

block-multiple-compress-files

Syntax

no block-multiple-compress-files

Mode

Gateway Anti-Virus

Description

Disable to block files with multiple levels of zip/gzip compression.

Example

no block-multiple-compress-files

Syntax

detection-only

Mode

Gateway Anti-Virus

Description

Enable detection only mode.

Example

detection-only

Syntax

no detection-only

Mode

Gateway Anti-Virus

Description

Disable detection only mode.

Example

no detection-only

Syntax

http-clientless-notification

Mode

Gateway Anti-Virus

Description

Enable HTTP Clientless Notification Alerts.

Example

http-clientless-notification

Syntax

no http-clientless-notification

Mode

Gateway Anti-Virus

Description

Disable HTTP Clientless Notification Alerts.

Example

no http-clientless-notification

Syntax

no notification-message

Mode

Gateway Anti-Virus

Description

Clear HTTP Clientless Notification Message to display when blocking.

Example

no notification-message

Syntax

notification-message <WORD>

Mode

Gateway Anti-Virus

Description

Set HTTP Clientless Notification Message to display when blocking.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

notification-message "This request is blocked by the SonicWall Gateway Anti-Virus Service."

Syntax

```
exclusion { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | entry <GAV_EXCLUSION_BEGIN_IPV4_HOST> <GAV_EXCLUSION_END_IPV4_HOST> | group <ADDR_GROUP_NAME_MIXED> | list | name <ADDR_NAME_MIXED> }
```

Mode

Gateway Anti-Virus

Description

Configure gateway AV exclusion list.

Options

| | |
|---|--|
| ipv6 | Excluded IPv6 addresses. |
| host <ADDR_HOST> | Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network <ADDR_NETWORK> | Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> | Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| entry <GAV_EXCLUSION_BEGIN_IPV4_HOST> | Gateway AV exclusion list entry. Gateway AV Exclusion List entry begin IPv4 in the form: D.D.D.D. Example: <i>192.168.168.168</i> |
| <GAV_EXCLUSION_END_IPV4_HOST> | Gateway AV Exclusion List entry end IPv4 in the form: D.D.D.D. Example: <i>192.168.168.168</i> |
| group <ADDR_GROUP_NAME_MIXED> | Address object group Group address object name. Example: <i>Sales Group</i> |
| list | Enable gateway AV exclusion list. |
| name <ADDR_NAME_MIXED> | Address object name. Address object name. Example: <i>Web Server</i> |

Example

```
exclusion list  
exclusion name "WLAN Subnets"  
exclusion entry 10.10.10.1 10.10.10.10
```

Syntax

```
no exclusion { entries | entry <GAV_EXCLUSION_BEGIN_IPV4_HOST> <GAV_EXCLUSION_END_IPV4_HOST> | list }
```

Mode

Gateway Anti-Virus

Description

Disable gateway AV exclusion list.

Options

| | |
|--|---|
| entries | Delete all gateway AV exclusion list entries. |
| entry | Delete gateway AV exclusion list entry. |
| <GAV_EXCLUSION_BEGIN_IPV4_HOST> | Gateway AV Exclusion List entry begin IPv4 in the form: D.D.D.D. Example: <i>192.168.168.168</i> |
| <GAV_EXCLUSION_END_IPV4_HOST> | Gateway AV Exclusion List entry end IPv4 in the form: D.D.D.D. Example: <i>192.168.168.168</i> |
| list | Disable gateway AV exclusion list. |

Example

```
no exclusion list
no exclusion entry 10.10.10.1 10.10.10.10
```

Syntax

```
capture-atp
```

Mode

Config

Description

Enter capture ATP mode and configure settings.

Example

```
capture-atp
```

Syntax

```
enable
```

Mode

Capture ATP

Description

Enable the capture ATP services.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Capture ATP

Description

Disable the capture ATP services.

Example

```
no enable
```

Syntax

```
file-type { archives | exe | office | officex | pdf }
```

Mode

Capture ATP

Description

Enable the file types that maybe transferred to capture ATP for analysis.

Options

archives Archives (.jar, .apk, .rar, .gz, and .zip).

exe Executables (PE, Mach-O, and DMG).

office Office 97-2003(.doc , .xls ,...).

officex Office(.docx , .xlsx ,...).

pdf PDF.

Example

```
file-type exe
file-type pdf
file-type office
file-type officex
file-type archives
```

Syntax

```
no file-type { archives | exe | office | officex | pdf }
```

Mode

Capture ATP

Description

Disable the file types that maybe transferred to capture ATP for analysis.

Options

archives Archives (.jar, .apk, .rar, .gz, and .zip).

exe Executables (PE, Mach-O, and DMG).

office Office 97-2003(.doc , .xls ,...).

officex Office(.docx , .xlsx ,...).

pdf PDF.

Example

```
no file-type exe
no file-type pdf
no file-type office
no file-type officex
no file-type archives
```

Syntax


```
file-size { default | restrict <UINT32> }
```

Mode

Capture ATP

Description

Specify the maximum file size that may be transferred to capture ATP for analysis.

Options

default Use the default file size specified by the capture service.

restrict Restrict to specific value in KB.

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
file-size default
file-size restrict 1000
```

Syntax

```
exclude address for-capture-atp { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Capture ATP

Description

Set an address object to exclude from capture ATP.

Options

ipv6 IPv6 address object.

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

fqdn Address object full qualified domain name.

<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address group name.

<ADDR_GROUP_NAME_MIXED> Group address object name.
Example: *Sales Group*

mac Address object mac.

<ADDR_MAC> Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.

name Address object name.
<ADDR_NAME_MIXED> Address object name.
Example: *Web Server*

Example

```
exclude address for-capture-atp name "X0 IP"
```

Syntax

```
no exclude address for-capture-atp
```

Mode

Capture ATP

Description

Clear the address object to exclude from capture ATP.

Example

```
no exclude address for-capture-atp
```

Syntax

```
exclude md5-entry <EXCLUDE_MD5_ENTRY>
```

Mode

Capture ATP

Description

Add an entry to the capture ATP MD5 exclusion list.

Options

<EXCLUDE_MD5_ENTRY> MD5 exclusion entry in 32 hexadecimal digits.
Example: *11223344556677889900aabbccddeeff*

Example

```
exclude md5-entry 11223344556677889900aabbccddeeff
```

Syntax

```
no exclude md5-entry <EXCLUDE_MD5_ENTRY>
```

Mode

Capture ATP

Description

Delete an entry from the capture ATP MD5 exclusion list.

Options

<EXCLUDE_MD5_ENTRY> MD5 exclusion entry in 32 hexadecimal digits.
Example: *11223344556677889900aabbccddeeff*

Example

```
no exclude md5-entry 11223344556677889900aabbccddeeff
```

Syntax

```
no exclude md5-entries
```

Mode

Capture ATP

Description

Clear the capture ATP MD5 exclusion list.

Example

```
no exclude md5-entries
```

Syntax

```
await-verdict { allow | block }
```

Mode

Capture ATP

Description

Set the custom block behavior for files that are not identified as malicious by other security services on the firewall and will be sent to capture ATP cloud service.

Options

allow Allow file download while awaiting a verdict.

block Block file download until a verdict is returned.

Example

```
await-verdict allow
```

Syntax

```
exclude address for-block-until-verdict { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Capture ATP

Description

Set an address object to exclude from blocking the file download until verdict is reached by the capture service.

Options

ipv6 IPv6 address object.

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.

| | |
|--------------------------------------|--|
| <ADDR_BEGIN> | IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
exclude address for-block-until-verdict name "X0 IP"
```

Syntax

```
no exclude address for-block-until-verdict
```

Mode

Capture ATP

Description

Clear the address object to exclude from blocking the file download until verdict is reached by the capture service.

Example

```
no exclude address for-block-until-verdict
```

Syntax

```
exclude file-type { archives | exe | office | officex | pdf }
```

Mode

Capture ATP

Description

Set the file types to exclude from blocking the file download until verdict is reached by the capture service.

Options

archives Archives (.jar, .apk, .rar, .gz, and .zip).

exe Executables (PE, Mach-O, and DMG).

office Office 97-2003(.doc, .xls, ...).

officex Office(.docx, .xlsx, ...).

pdf PDF.

Example

```
exclude file-type exe
exclude file-type pdf
exclude file-type office
exclude file-type officex
exclude file-type archives
```

Syntax

```
no exclude file-type { archives | exe | office | officex | pdf }
```

Mode

Capture ATP

Description

Clear the file types to exclude from blocking the file download until verdict is reached by the capture service.

Options

archives Archives (.jar, .apk, .rar, .gz, and .zip).

exe Executables (PE, Mach-O, and DMG).

office Office 97-2003(.doc, .xls, ...).

officex Office(.docx, .xlsx, ...).

pdf PDF.

Example

```
no exclude file-type exe
no exclude file-type pdf
no exclude file-type office
no exclude file-type officex
no exclude file-type archives
```

Syntax

```
no match-object <MATCH_OBJ_NAME>
```

Mode

Config

Description

Delete a match object.

Options

<MATCH_OBJ_NAME> Match object name.
Example: *Match FTP*

Example

```
no match-object "myMatchObject"
```

Syntax

```
no match-objects
```

Mode

Config

Description

Delete all match objects.

Example

```
no match-objects
```

Syntax

```
match-object <MATCH_OBJ_NAME>
```

Mode

Config

Description

Add/edit match object and enter configuration mode.

Options

<MATCH_OBJ_NAME> Match object name.
Example: *Match FTP*

Example

```
match-object "Denied File Extensions"
```

Syntax

```
no type
```

Mode

Match Object

Example

```
no type
```

Syntax

```
type { activex-class-id | application-category-list | application-list | application-signature-list | custom | email-body | email-cc | email-from | email-size | email-subject | email-to | file-content | file-extension | file-name | ftp-command | ftp-command-value | http-cookie | http-host | http-referer | http-request-custom-header | http-response-custom-header | http-set-cookie | http-uri-content | http-url | http-user-agent | ips-signature-category-list | ips-signature-list | log-email-user | mime-custom-header | web-browser }
```

Mode

Match Object

Description

Match object type.

Options

| | |
|-----------------------------------|-----------------------------|
| activex-class-id | Active X class ID. |
| application-category-list | Application category list. |
| application-list | Application list. |
| application-signature-list | Application signature list. |

| | |
|------------------------------------|------------------------------|
| <i>custom</i> | Custom object. |
| <i>email-body</i> | E-mail body. |
| <i>email-cc</i> | E-mail CC. |
| <i>email-from</i> | E-mail from. |
| <i>email-size</i> | E-mail size. |
| <i>email-subject</i> | E-mail subject. |
| <i>email-to</i> | E-mail to. |
| <i>file-content</i> | File content. |
| <i>file-extension</i> | File extension. |
| <i>file-name</i> | File name. |
| <i>ftp-command</i> | FTP command. |
| <i>ftp-command-value</i> | FTP command and value. |
| <i>http-cookie</i> | HTTP cookie. |
| <i>http-host</i> | Http host. |
| <i>http-referer</i> | HTTP referer. |
| <i>http-request-custom-header</i> | HTTP request custom header. |
| <i>http-response-custom-header</i> | HTTP response custom header. |
| <i>http-set-cookie</i> | HTTP set cookie. |
| <i>http-uri-content</i> | HTTP URI content. |
| <i>http-url</i> | HTTP URL. |
| <i>http-user-agent</i> | Http user agent. |
| <i>ips-signature-category-list</i> | IPS signature category list. |
| <i>ips-signature-list</i> | IPS signature list. |
| <i>log-email-user</i> | Log e-mail user. |
| <i>mime-custom-header</i> | MIME custom header. |
| <i>web-browser</i> | Web browser. |

Example

```
type email-body
```

Syntax

```
name <MATCH_OBJ_NAME>
```

Mode

Match Object

Description

Set match object name.

Options

<MATCH_OBJ_NAME> Match object name.
Example: *Match FTP*

Example

```
name "Denied File Extensions "
```

Syntax

```
match-type { exact | partial | prefix | regex | suffix }
```

Mode

Match Object

Description

Set match object match type.

Options

exact Exact match.

partial Partial match.

prefix Prefix match.

regex Regular expression match.

suffix Suffix match.

Example

```
match-type exact
```

Syntax

```
no match-type
```

Mode

Match Object

Description

Clear match object match type.

Example

```
no match-type
```

Syntax

```
enable
```

Mode

Match Object

Description

Enable custom settings.

Example

enable

Syntax

no enable

Mode

Match Object

Description

Disable custom settings.

Example

no enable

Syntax

offset <UINT32>

Mode

Match Object

Description

Set offset.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

offset 1

Syntax

no offset

Mode

Match Object

Description

Clear offset.

Example

no offset

Syntax

depth <UINT32>

Mode

Match Object

Description

Set depth.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

depth 1

Syntax

no depth

Mode

Match Object

Description

Clear depth.

Example

no depth

Syntax

min-size <UINT32>

Mode

Match Object

Description

Set min size.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

min-size 1

Syntax

no min-size

Mode

Match Object

Description

Clear min size.

Example

no min-size

Syntax

max-size <UINT32>

Mode

Match Object

Description

Set max size.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

max-size 1

Syntax

no max-size

Mode

Match Object

Description

Clear max size.

Example

no max-size

Syntax

negative-matching

Mode

Match Object

Description

Enable negative matching.

Example

negative-matching

Syntax

no negative-matching

Mode

Match Object

Description

Disable negative matching.

Example

no negative-matching

Syntax

```
no input-representation
```

Mode

Match Object

Description

Clear match object input representation.

Example

```
no input-representation
```

Syntax

```
input-representation { alphanumeric | hexadecimal }
```

Mode

Match Object

Description

Set match object input representation.

Options

alphanumeric Alphanumeric.

hexadecimal Hexadecimal.

Example

```
input-representation alphanumeric
```

Syntax

```
content-entry <WORD>
```

Mode

Match Object

Description

Add match object content.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
content-entry mpg
```

Syntax

```
no content-entry <MATCH_OBJ_CONTENT_ENTRY>
```

Mode

Match Object

Description

Delete match object content.

Options

<MATCH_OBJ_CONTENT_ENTRY> Match object content.
Example: *mpg*

Example

```
no content-entry mpg
```

Syntax

```
no content-entries
```

Mode

Match Object

Description

Delete all match object content.

Example

```
no content-entries
```

Syntax

```
pre-defined-regex { aba-routing-number | amex-cc | canadian-sin | discover-cc | mastercard-cc | us-ssn | visa-cc }
```

Mode

Match Object

Description

Add a pre-defined regular expression.

Options

aba-routing-number American bankers association (ABA) routing number.

amex-cc American express credit card.

canadian-sin Canadian social insurance number (SIN).

discover-cc Discover card credit card.

mastercard-cc Master card credit card.

us-ssn United states social security number (SSN).

visa-cc Visa credit card.

Example

```
pre-defined-regex visa-cc
```

Syntax

```
no pre-defined-regex { aba-routing-number | amex-cc | canadian-sin | discover-cc | mastercard-cc | us-ssn | visa-cc }
```

Mode

Match Object

Description

Remove a pre-defined regular expression.

Options

aba-routing-number American bankers association (ABA) routing number.

amex-cc American express credit card.

canadian-sin Canadian social insurance number (SIN).

discover-cc Discover card credit card.

mastercard-cc Master card credit card.

us-ssn United states social security number (SSN).

visa-cc Visa credit card.

Example

```
no pre-defined-regex visa-cc
```

Syntax

```
browser { chrome | firefox | msie | netscape | safari }
```

Mode

Match Object

Description

Add match object browser.

Options

chrome Chrome.

firefox Firefox.

msie Internet explorer.

netscape Netscape.

safari Safari.

Example

```
browser safari
```

Syntax

```
no browser { chrome | firefox | msie | netscape | safari }
```

Mode

Match Object

Description

Delete match object browser.

Options

chrome Chrome.

firefox Firefox.

msie Internet explorer.

netscape Netscape.

safari Safari.

Example

```
no browser safari
```

Syntax

```
no browsers
```

Mode

Match Object

Description

Delete all match object browsers.

Example

```
no browsers
```

Syntax

```
custom-header <WORD>
```

Mode

Match Object

Description

Set custom header name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
custom-header "TBD "
```

Syntax

```
no custom-header
```

Mode

Match Object

Description

Clear custom header name.

Example

no custom-header

Syntax

email-size <UIN32>

Mode

Match Object

Description

Specify e-mail size in bytes.

Options

<UIN32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

email-size 1000000

Syntax

no email-size

Mode

Match Object

Description

Clear e-mail size.

Example

no email-size

Syntax

ftp-command { *abort* | *account* | *allocate* | *append* | *ascii* | *binary* | *cd* | *cdup* | *delete* | *get* | *help* | *ls* | *mkdir* | *mode* | *modified-time* | *nlist* | *noop* | *passive* | *password* | *port* | *put* | *pwd* | *quit* | *reinitialize* | *rename-from* | *rename-to* | *restart* | *rmdir* | *site* | *size* | *status* | *structure* | *structure-mount* | *structure-unique* | *system* | *type* | *user* }

Mode

Match Object

Description

Add match object FTP command.

Options

| | |
|------------------------|-----------|
| <i>abort</i> | ABORT. |
| <i>account</i> | ACCOUNT. |
| <i>allocate</i> | ALLOCATE. |
| <i>append</i> | APPEND. |
| <i>ascii</i> | ASCII. |

| | |
|-------------------------|-------------------|
| <i>binary</i> | BINARY. |
| <i>cd</i> | CD. |
| <i>cdup</i> | CDUP. |
| <i>delete</i> | DELETE. |
| <i>get</i> | GET. |
| <i>help</i> | HELP. |
| <i>ls</i> | LS. |
| <i>mkdir</i> | MKDIR. |
| <i>mode</i> | MODE. |
| <i>modified-time</i> | MODIFIED_TIME. |
| <i>nlist</i> | NLIST. |
| <i>noop</i> | NOOP. |
| <i>passive</i> | PASSIVE. |
| <i>password</i> | PASSWORD. |
| <i>port</i> | PORT. |
| <i>put</i> | PUT. |
| <i>pwd</i> | PWD. |
| <i>quit</i> | QUIT. |
| <i>reinitialize</i> | REINITIALIZE. |
| <i>rename-from</i> | RENAME_FROM. |
| <i>rename-to</i> | RENAME_TO. |
| <i>restart</i> | RESTART. |
| <i>rmdir</i> | RMDIR. |
| <i>site</i> | SITE. |
| <i>size</i> | SIZE. |
| <i>status</i> | STATUS. |
| <i>structure</i> | STRUCTURE. |
| <i>structure-mount</i> | STRUCTURE_MOUNT. |
| <i>structure-unique</i> | STRUCTURE_UNIQUE. |
| <i>system</i> | SYSTEM. |
| <i>type</i> | TYPE. |
| <i>user</i> | USER. |

Example

Syntax

no ftp-command { *abort* | *account* | *allocate* | *append* | *ascii* | *binary* | *cd* | *cdup* | *delete* | *get* | *help* | *ls* | *mkdir* | *mode* | *modified-time* | *nlist* | *noop* | *passive* | *password* | *port* | *put* | *pwd* | *quit* | *reinitialize* | *rename-from* | *rename-to* | *restart* | *rmdir* | *site* | *size* | *status* | *structure* | *structure-mount* | *structure-unique* | *system* | *type* | *user* }

Mode

Match Object

Description

Delete match object FTP command.

Options

| | |
|----------------------|----------------|
| <i>abort</i> | ABORT. |
| <i>account</i> | ACCOUNT. |
| <i>allocate</i> | ALLOCATE. |
| <i>append</i> | APPEND. |
| <i>ascii</i> | ASCII. |
| <i>binary</i> | BINARY. |
| <i>cd</i> | CD. |
| <i>cdup</i> | CDUP. |
| <i>delete</i> | DELETE. |
| <i>get</i> | GET. |
| <i>help</i> | HELP. |
| <i>ls</i> | LS. |
| <i>mkdir</i> | MKDIR. |
| <i>mode</i> | MODE. |
| <i>modified-time</i> | MODIFIED_TIME. |
| <i>nlist</i> | NLIST. |
| <i>noop</i> | NOOP. |
| <i>passive</i> | PASSIVE. |
| <i>password</i> | PASSWORD. |
| <i>port</i> | PORT. |
| <i>put</i> | PUT. |
| <i>pwd</i> | PWD. |
| <i>quit</i> | QUIT. |
| <i>reinitialize</i> | REINITIALIZE. |

| | |
|-------------------------|-------------------|
| rename-from | RENAME_FROM. |
| rename-to | RENAME_TO. |
| restart | RESTART. |
| rmdir | RMDIR. |
| site | SITE. |
| size | SIZE. |
| status | STATUS. |
| structure | STRUCTURE. |
| structure-mount | STRUCTURE_MOUNT. |
| structure-unique | STRUCTURE_UNIQUE. |
| system | SYSTEM. |
| type | TYPE. |
| user | USER. |

Example

no ftp-command put

Syntax

no ftp-commands

Mode

Match Object

Description

Delete all match object FTP commands.

Example

no ftp-commands

Syntax

argument <WORD>

Mode

Match Object

Description

Add FTP command argument.

Options

<WORD> Word in the form: WORD or "QUOTED STRING".
Example: *abc*

Example

argument file1

Syntax

no argument <MATCH_OBJ_CONTENT_ENTRY>

Mode

Match Object

Description

Delete FTP command argument.

Options

<MATCH_OBJ_CONTENT_ENTRY> Match object content.
Example: *mpg*

Example

no argument file1

Syntax

no arguments

Mode

Match Object

Description

Delete all FTP command arguments.

Example

no arguments

Syntax

ips category { *id* <IPS_CATEGORY_ID> | *name* <IPS_CATEGORY_NAME> }

Mode

Match Object

Description

Add an IPS category.

Options

id Category ID.
<IPS_CATEGORY_ID> Category ID.
Example: *1234*

name Category name.
<IPS_CATEGORY_NAME> Category name.
Example: *ACTIVEX*

Example

ips category name ACTIVEX

Syntax

```
no ips category { id <IPS_CATEGORY_ID> | name <IPS_CATEGORY_NAME> }
```

Mode

Match Object

Description

Delete an IPS category.

Options

| | |
|---|------------------------------------|
| <i>id</i> | Category ID. |
| <i><IPS_CATEGORY_ID></i> | Category ID. Example: 1234 |
| <i>name</i> | Category name. |
| <i><IPS_CATEGORY_NAME></i> | Category name. Example: ACTIVEX |

Example

```
no ips category name ACTIVEX
```

Syntax

```
no ips categories
```

Mode

Match Object

Description

Delete all IPS categories.

Example

```
no ips categories
```

Syntax

```
ips policy category { id <IPS_CATEGORY_ID> | name <IPS_CATEGORY_NAME> } signature { id <IPS_POLICY_ID> | name <IPS_POLICY_NAME> }
```

Mode

Match Object

Description

Add an IPS policy.

Options

| | |
|---|------------------------------------|
| <i>category</i> | Category. |
| <i>id</i> | Category ID. |
| <i><IPS_CATEGORY_ID></i> | Category ID. Example: 1234 |
| <i>name</i> | Category name. |
| <i><IPS_CATEGORY_NAME></i> | Category name. Example: ACTIVEX |
| <i>signature</i> | Signature. |
| <i>id</i> | Signature ID. |
| <i><IPS_POLICY_ID></i> | Policy ID. Example: 1234 |

name Signature name.
<IPS_POLICY_NAME> Policy name.
Example: *ActivePDF WebGrabber ActiveX Instantiation*

Example

```
ips category name ACTIVEEX signature name "Free Tetris Executable (Adware)"
```

Syntax

```
no ips policy category { id <IPS_CATEGORY_ID> | name <IPS_CATEGORY_NAME> } signature { id <IPS_POLICY_ID> | name <IPS_POLICY_NAME> }
```

Mode

Match Object

Description

Delete an IPS policy.

Options

category Category.

id Category ID.
<IPS_CATEGORY_ID> Category ID.
Example: *1234*

name Category name.
<IPS_CATEGORY_NAME> Category name.
Example: *ACTIVEEX*

signature Signature.

id Signature ID.
<IPS_POLICY_ID> Policy ID.
Example: *1234*

name Signature name.
<IPS_POLICY_NAME> Policy name.
Example: *ActivePDF WebGrabber ActiveX Instantiation*

Example

```
no ips category name ACTIVEEX signature name "Free Tetris Executable (Adware)"
```

Syntax

```
no ips policies
```

Mode

Match Object

Description

Delete all IPS policies.

Example

```
no ips policies
```

Syntax

```
category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> }
```

Mode

Match Object

Description

Add an application category.

Options

| | |
|---------------------------------|--|
| <i>id</i> | Category ID. |
| <i><AC_CATEGORY_ID></i> | Category ID. Example: <i>123</i> |
| <i>name</i> | Category name. |
| <i><AC_CATEGORY_NAME></i> | Category name. Example: <i>APP-UPDATE</i> |

Example

```
category name APP-UPDATE
category id 22
```

Syntax

```
no category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> }
```

Mode

Match Object

Description

Delete an application category.

Options

| | |
|---------------------------------|--|
| <i>id</i> | Category ID. |
| <i><AC_CATEGORY_ID></i> | Category ID. Example: <i>123</i> |
| <i>name</i> | Category name. |
| <i><AC_CATEGORY_NAME></i> | Category name. Example: <i>APP-UPDATE</i> |

Example

```
no category name APP-UPDATE
no category id 22
```

Syntax

```
no categories
```

Mode

Match Object

Description

Delete all application categories.

Example

```
no categories
```

Syntax

```
application category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> } app { id <AC_APP_ID> | name <AC_APP_NAME> }
```

Mode

Match Object

Description

Add an application.

Options

| | |
|---------------------------------|--|
| category | Application category. |
| id | Category ID. |
| <AC_CATEGORY_ID> | Category ID. Example: 123 |
| name | Category name. |
| <AC_CATEGORY_NAME> | Category name. Example: APP-UPDATE |
| app | Application. |
| id | Application ID. |
| <AC_APP_ID> | Application ID. Example: 123 |
| name | Application name. |
| <AC_APP_NAME> | Application name. Example: APP-UPDATE |

Example

```
application category name BACKUP-APPS app name Dropbox  
application category id 56 app id 604
```

Syntax

```
no application category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> } app { id <AC_APP_ID> | name <AC_APP_NAME> }
```

Mode

Match Object

Description

Delete an application.

Options

| | |
|---------------------------------|--|
| category | Application category. |
| id | Category ID. |
| <AC_CATEGORY_ID> | Category ID. Example: 123 |
| name | Category name. |
| <AC_CATEGORY_NAME> | Category name. Example: APP-UPDATE |
| app | Application. |
| id | Application ID. |
| <AC_APP_ID> | Application ID. Example: 123 |
| name | Application name. |
| <AC_APP_NAME> | Application name. Example: APP-UPDATE |

Example


```
no application category name BACKUP-APPS app name Dropbox
no application category id 56 app id 604
```

Syntax

```
no applications
```

Mode

Match Object

Description

Delete all applications.

Example

```
no applications
```

Syntax

```
signature category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> } app { id <AC_APP_ID> | name <AC_APP_NAME> } sig { id <AC_SIG_ID> | name <AC_SIG_NAME> }
```

Mode

Match Object

Description

Add a signature.

Options

| | |
|---------------------------------|--|
| category | Application category. |
| id | Category ID. |
| <AC_CATEGORY_ID> | Category ID. Example: 123 |
| name | Category name. |
| <AC_CATEGORY_NAME> | Category name. Example: APP-UPDATE |
| app | Application. |
| id | Application ID. |
| <AC_APP_ID> | Application ID. Example: 123 |
| name | Application name. |
| <AC_APP_NAME> | Application name. Example: APP-UPDATE |
| sig | Signature. |
| id | Signature ID. |
| <AC_SIG_ID> | Signature ID. Example: 123 |
| name | Signature name. |
| <AC_SIG_NAME> | Signature name. |

Example

```
signature category name BACKUP-APPS app name Dropbox sig name "SSL Traffic"
signature category id 56 app id 604 sig id 1736
```

Syntax

```
no signature category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> } app { id <AC_APP_ID> | name <AC_APP_NAME> } sig { id <AC_SIG_ID> | name <AC_SIG_NAME> }
```

Mode

Match Object

Description

Delete a signature.

Options

| | |
|---------------------------------|--|
| category | Application category. |
| id | Category ID. |
| <AC_CATEGORY_ID> | Category ID. Example: 123 |
| name | Category name. |
| <AC_CATEGORY_NAME> | Category name. Example: APP-UPDATE |
| app | Application. |
| id | Application ID. |
| <AC_APP_ID> | Application ID. Example: 123 |
| name | Application name. |
| <AC_APP_NAME> | Application name. Example: APP-UPDATE |
| sig | Signature. |
| id | Signature ID. |
| <AC_SIG_ID> | Signature ID. Example: 123 |
| name | Signature name. |
| <AC_SIG_NAME> | Signature name. |

Example

```
no signature category name BACKUP-APPS app name Dropbox sig name "SSL Traffic"  
no signature category id 56 app id 604 sig id 1736
```

Syntax

```
no signatures
```

Mode

Match Object

Description

Delete all signatures.

Example

```
no signatures
```

Syntax

```
action-object <ACTION_OBJ_NAME>
```

Mode

Config

Description

Create/edit specified action object and enter its configuration mode.

Options

<ACTION_OBJ_NAME> Action object name.
Example: *HTTP Block Page*

Example

```
action-object "Corp E-mail Message"
```

Syntax

```
no action-object <ACTION_OBJ_NAME>
```

Mode

Config

Description

Delete specified action object.

Options

<ACTION_OBJ_NAME> Action object name.
Example: *HTTP Block Page*

Example

```
no action-object "Corp E-mail Message"
```

Syntax

```
no action-objects
```

Mode

Config

Description

Delete all action objects.

Example

```
no action-objects
```

Syntax

```
name <ACTION_OBJ_NAME>
```

Mode

Action Object

Description

Action object name.

Options

<ACTION_OBJ_NAME> Action object name.
Example: *HTTP Block Page*

Example

```
name "Corp Mail Message"
```

Syntax

```
action { bandwidth-management | block-smtp-error-reply | disable-email-attachment | email-add-text | ftp-notification-reply | http-block-page | http-redirect }
```

Mode

Action Object

Description

Set action.

Options

| | |
|---------------------------------|---|
| <i>bandwidth-management</i> | Bandwidth management. |
| <i>block-smtp-error-reply</i> | Block SMTP e-mail and send error reply. |
| <i>disable-email-attachment</i> | Disable e-mail attachment and add text. |
| <i>email-add-text</i> | E-mail - add text. |
| <i>ftp-notification-reply</i> | FTP notification reply. |
| <i>http-block-page</i> | HTTP block page. |
| <i>http-redirect</i> | HTTP redirect. |

Example

```
action block-smtp-email error-reply
```

Syntax

```
no content
```

Mode

Action Object

Description

Clear action object content.

Example

```
no content
```

Syntax

```
content <WORD>
```

Mode

Action Object

Description

Action object content.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
content "Corporate does not allow attachments to Emails."
```

Syntax

```
no color
```

Mode

Action Object

Description

Clear HTTP block page color.

Example

```
no color
```

Syntax

```
color { blue | red | white | yellow }
```

Mode

Action Object

Description

HTTP block page color.

Options

blue Blue.

red Red.

white White.

yellow Yellow.

Example

```
color white
```

Syntax

```
bandwidth-management
```

Mode

Action Object

Description

Configure bandwidth management.

Example

```
bandwidth-management
```

Syntax

```
aggregation-method { per-action | per-policy }
```

Mode

Bandwidth Management

Description

Set the bandwidth aggregation method.

Options

per-action Per action.

per-policy Per policy.

Example

```
aggregation-method per-policy
```

Syntax

```
no egress [ bandwidth-object ]
```

Mode

Bandwidth Management

Description

Disable egress bandwidth management.

Options

bandwidth-object Clear bandwidth object.

Example

```
no egress
```

Syntax

```
egress priority { high | highest | low | lowest | medium | medium-high | medium-low | realtime }
```

Mode

Bandwidth Management

Description

Enable egress bandwidth management and set priority.

Options

high High 2.

highest Highest 1.

low Low 6.

lowest Lowest 7.

medium Medium 4.

medium-high Medium-high 3.

medium-low Medium-low 5.

realtime Realtime 0.

Example

```
egress priority highest
```

Syntax

```
egress bandwidth-object <BANDWIDTH_RULE_NAME>
```

Mode

Bandwidth Management

Description

Enable egress bandwidth management and configure.

Options

<BANDWIDTH_RULE_NAME> Bandwidth object name.
Example: `\\"Corp High Priority\\"`

Example

```
egress bandwidth-object "Corp High Priority"
```

Syntax

```
no ingress [ bandwidth-object ]
```

Mode

Bandwidth Management

Description

Disable ingress bandwidth management.

Options

bandwidth-object Clear bandwidth object.

Example

```
no ingress
```

Syntax

```
ingress priority { high | highest | low | lowest | medium | medium-high | medium-low | realtime }
```

Mode

Bandwidth Management

Description

Enable ingress bandwidth management and set priority.

Options

high High 2.

| | |
|--------------------|----------------|
| highest | Highest 1. |
| low | Low 6. |
| lowest | Lowest 7. |
| medium | Medium 4. |
| medium-high | Medium-high 3. |
| medium-low | Medium-low 5. |
| realtime | Realtime 0. |

Example

```
ingress priority highest
```

Syntax

```
ingress bandwidth-object <BANDWIDTH_RULE_NAME>
```

Mode

Bandwidth Management

Description

Enable ingress bandwidth management and configure.

Options

<BANDWIDTH_RULE_NAME> Bandwidth object name.
Example: `\\"Corp High Priority\\"`

Example

```
ingress bandwidth-object "Corp High Priority"
```

Syntax

```
usage-tracking
```

Mode

Bandwidth Management

Description

Enable tracking bandwidth usage.

Example

```
usage-tracking
```

Syntax

```
no usage-tracking
```

Mode

Bandwidth Management

Description

Disable tracking bandwidth usage.

Example

```
no usage-tracking
```

Syntax

```
no email-object <EMAIL_OBJ_NAME>
```

Mode

Config

Description

Delete an e-mail address object.

Options

<EMAIL_OBJ_NAME> E-mail object name.
Example: *Marketing E-mail Object*

Example

```
no email-object "Client E-mail Addresses"
```

Syntax

```
no email-objects
```

Mode

Config

Description

Delete all e-mail address objects.

Example

```
no email-objects
```

Syntax

```
email-object <EMAIL_OBJ_NAME>
```

Mode

Config

Description

Add/edit e-mail address object and enter configuration mode.

Options

<EMAIL_OBJ_NAME> E-mail object name.
Example: *Marketing E-mail Object*

Example

```
email-object "Client E-mail Addresses"
```

Syntax

```
name <EMAIL_OBJ_NAME>
```

Mode

E-mail Address Object

Description

Set e-mail address object name.

Options

<EMAIL_OBJ_NAME> E-mail object name.
Example: *Marketing E-mail Object*

Example

```
name "Client E-mail Addresses "
```

Syntax

```
no match-type
```

Mode

E-mail Address Object

Description

Clear e-mail address object match type.

Example

```
no match-type
```

Syntax

```
match-type { exact | partial | regex }
```

Mode

E-mail Address Object

Description

Set e-mail address object match type.

Options

exact Exact match.

partial Partial match.

regex Regular expression match.

Example

```
match-type exact
```

Syntax

```
content-entry <EMAIL_OBJ_CONTENT_ENTRY>
```

Mode

E-mail Address Object

Description

Add e-mail address object content entry.

Options

<EMAIL_OBJ_CONTENT_ENTRY> E-mail object content.
Example: *administrator@corp.local*

Example

```
content-entry administrator@corp.local
```

Syntax

```
no content-entry <EMAIL_OBJ_CONTENT_ENTRY>
```

Mode

E-mail Address Object

Description

Delete e-mail address object content entry.

Options

<EMAIL_OBJ_CONTENT_ENTRY> E-mail object content.
Example: *administrator@corp.local*

Example

```
no content-entry administrator@corp.local
```

Syntax

```
no content-entries
```

Mode

E-mail Address Object

Description

Delete all e-mail address object content entries.

Example

```
no content-entries
```

Syntax

```
app-rules
```

Mode

Config

Description

Enter app rules configuration mode.

Example

```
app-rules
```

Syntax

enable

Mode

App Rules

Description

Enable app rules.

Example

enable

Syntax

no enable

Mode

App Rules

Description

Disable app rules.

Example

no enable

Syntax

log-redundancy <UINT32>

Mode

App Rules

Description

Set the global log redundancy filter interval(seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

log-redundancy 60

Syntax

no log-redundancy

Mode

App Rules

Description

Clear the global log redundancy filter interval.

Example

no log-redundancy

Syntax

```
no policy <APP_RULES_POLICY_NAME>
```

Mode

App Rules

Description

Delete specified app rule policy.

Options

<APP_RULES_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no policy "Deny Sensitive Download"
```

Syntax

```
no policies
```

Mode

App Rules

Description

Delete all app rule policies.

Example

```
no policies
```

Syntax

```
policy <APP_RULES_POLICY_NAME>
```

Mode

App Rules

Description

Create/edit specified app rule policy and enter its configuration mode.

Options

<APP_RULES_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
policy "Deny Sensitive Download"
```

Syntax

```
name <APP_RULES_POLICY_NAME>
```

Mode

App Rules Policy

Description

App rule name.

Options

<APP_RULES_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name "Deny Sensitive Emails"
```

Syntax

```
type { app-control | cfs | custom | ftp { { client [ [ download | upload ] ] | data-transfer } } | http { { client | server } } |  
ips | pop3 { { client | server } } | smtp-client }
```

Mode

App Rules Policy

Description

Set app rule policy type.

Options

| | |
|----------------------|---------------------------|
| app-control | App control content. |
| cfs | CFS. |
| custom | Custom policy. |
| ftp | FTP. |
| client | FTP client. |
| download | FTP client file download. |
| upload | FTP client file upload. |
| data-transfer | FTP data transfer. |
| http | HTTP. |
| client | HTTP client. |
| server | HTTP server. |
| ips | IPS content. |
| pop3 | POP3. |
| client | Pop3 client. |
| server | Pop3 server. |
| smtp-client | SMTP client. |

Example

```
type http client
```

Syntax

```
source address { { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any |  
fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | mac <ADDR_MAC> | name <ADDR_NAME> } }
```

Mode

App Rules Policy

Description

Set the source address for the app rule policy.

Options

| | |
|--------------------------------|--|
| ipv6 | IPv6 address object. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| mac | Address object MAC. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |

Example

```
source address name "Corporate IT Administration"
```

Syntax

```
destination address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | mac <ADDR_MAC> | name <ADDR_NAME> } }
```

Mode

App Rules Policy

Description

Set the destination address for the app rule policy.

Options

| | |
|-------------|----------------------|
| ipv6 | IPv6 address object. |
|-------------|----------------------|

| | |
|--------------------------------|--|
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| mac | Address object MAC. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |

Example

```
destination address name "Corporate IT Administration"
```

Syntax

```
address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | mac <ADDR_MAC> | name <ADDR_NAME> } }
```

Mode

App Rules Policy

Description

Set the address for the app rule policy.

Options

| | |
|-----------------------------|--|
| ipv6 | IPv6 address object. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |

| | |
|--------------------------------|--|
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| mac | Address object MAC. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |

Example

```
address name "Corporate IT Administration"
```

Syntax

```
exclusion address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME> | mac <ADDR_MAC> | name <ADDR_NAME> } }
```

Mode

App Rules Policy

Description

Set the exclusion address for the app rule policy.

Options

| | |
|-----------------------------|--|
| ipv6 | IPv6 address object. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| any | Any address. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |

| | |
|--------------------------------|---|
| group | Address group name. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| mac | Address object MAC. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |

Example

```
exclusion address name "Corporate IT Administration"
```

Syntax

```
no exclusion address
```

Mode

App Rules Policy

Description

Clear exclusion address for the app rule policy.

Example

```
no exclusion address
```

Syntax

```
source service { any | group <APP_RULES_POLICY_SVC_GROUP_NAME> | name <APP_RULES_POLICY_SVC_NAME> }
```

Mode

App Rules Policy

Description

Set the source service for the app rule policy.

Options

| | |
|--|--|
| any | Any source service. |
| group | Source service group name. |
| <APP_RULES_POLICY_SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| name | Source service object name. |
| <APP_RULES_POLICY_SVC_NAME> | Service object name. Example: <i>HTTPS</i> |

Example

```
source service name "IT Maintenance"
```

Syntax

```
destination service { any | group <APP_RULES_POLICY_SVC_GROUP_NAME> | name <APP_RULES_POLICY_SVC_NAME> }
```

Mode

App Rules Policy

Description

Set the destination service for the app rule policy.

Options

| | |
|--|--|
| <i>any</i> | Any destination service. |
| <i>group</i> | Destination service group name. |
| <APP_RULES_POLICY_SVC_GROUP_NAME> | Service object group name. Example: <i>VOIP</i> |
| <i>name</i> | Destination service object name. |
| <APP_RULES_POLICY_SVC_NAME> | Service object name. Example: <i>HTTPS</i> |

Example

```
destination service name "Corporate Servers"
```

Syntax

```
match-object { excluded <APP_RULES_POLICY_MATCH_OBJECT> | included <APP_RULES_POLICY_MATCH_OBJECT> | object  
<APP_RULES_POLICY_MATCH_OBJECT> }
```

Mode

App Rules Policy

Description

Set match object for this app rule policy.

Options

| | |
|--|---|
| <i>excluded</i> | Exclude match object. |
| <APP_RULES_POLICY_MATCH_OBJECT> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>included</i> | Include match object. |
| <APP_RULES_POLICY_MATCH_OBJECT> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>object</i> | Include match object. |
| <APP_RULES_POLICY_MATCH_OBJECT> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

Example

```
match-object object "mpg extension"
```

Syntax

```
action-object <APP_RULES_POLICY_ACTION_OBJECT>
```

Mode

App Rules Policy

Description

Set action object for this app rule policy.

Options

| | |
|---|--|
| <APP_RULES_POLICY_ACTION_OBJECT> | Word in the form: WORD or \"QUOTED STRING\". |
|---|--|

Example: *abc*

Example

```
action-object "Bypass DPI"
```

Syntax

```
users { excluded | included } { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

App Rules Policy

Description

Set users to this app rule policy.

Options

| | |
|---|---|
| <i>excluded</i> | Set excluded users. |
| <i>included</i> | Set included users. |
| <i>administrator</i> | Administrator. |
| <i>all</i> | All users. |
| <i>group</i> | Group object name. |
| <i><LOCAL_USER_GROUP_NAME></i> | Local user group object name. Example: <i>Limited Administrators</i> |
| <i>guests</i> | Guest users. |
| <i>name</i> | User object name. |
| <i><LOCAL_USER_NAME></i> | Local user object name. Example: <i>user1</i> |

Example

```
users included name "Corporate IT Administrators"
```

Syntax

```
no users excluded
```

Mode

App Rules Policy

Description

Clear excluded users for the app rule policy.

Options

excluded Clear excluded users for the app rule policy.

Example

```
no users excluded
```

Syntax

```
mail-from included <APP_RULES_POLICY_EMAIL_OBJECT>
```

Mode

App Rules Policy

Description

Set the included from e-mail object for the app rules policy.

Options

<APP_RULES_POLICY_EMAIL_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
mail-from included any mail-from included "John Doe"
```

Syntax

```
mail-from excluded <APP_RULES_POLICY_EMAIL_OBJECT>
```

Mode

App Rules Policy

Description

Set the excluded from e-mail object for the app rules policy.

Options

<APP_RULES_POLICY_EMAIL_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
mail-from excluded "Jane Doe"
```

Syntax

```
no mail-from excluded
```

Mode

App Rules Policy

Description

Clear the excluded from e-mail object for the app rules policy.

Options

excluded Clear the excluded from e-mail object for the app rules policy.

Example

```
no mail-from excluded
```

Syntax

```
rcpt-to included <APP_RULES_POLICY_EMAIL_OBJECT>
```

Mode

App Rules Policy

Description

Set the included RCPT to e-mail address object for the app rule policy.

Options

<APP_RULES_POLICY_EMAIL_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
rcpt-to included any rcpt-to included "John Doe"
```

Syntax

```
rcpt-to excluded <APP_RULES_POLICY_EMAIL_OBJECT>
```

Mode

App Rules Policy

Description

Set the excluded RCPT to e-mail address object for the app rule policy.

Options

<APP_RULES_POLICY_EMAIL_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
rcpt-to excluded "Jane Doe"
```

Syntax

```
no rcpt-to excluded
```

Mode

App Rules Policy

Description

Clear the excluded RCPT to e-mail object for the app rules policy.

Options

excluded Clear the excluded RCPT to e-mail object for the app rules policy.

Example

```
no rcpt-to excluded
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

App Rules Policy

Description

Specify a schedule for this app rule policy.

Options

always-on Always on.

days Schedule object days.

| | |
|---------------------------------|---|
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule name "IT Maintenance"
```

Syntax

```
flow-reporting
```

Mode

App Rules Policy

Description

Enable flow reporting.

Example

```
flow-reporting
```

Syntax

```
no flow-reporting
```

Mode

App Rules Policy

Description

Disable flow reporting.

Example

```
no flow-reporting
```

Syntax

```
logging
```

Mode

App Rules Policy

Description

Enable logging when this app rule is used.

Example

```
logging
```

Syntax

no logging

Mode

App Rules Policy

Description

Disable logging when this app rule is used.

Example

no logging

Syntax

log individual

Mode

App Rules Policy

Description

Enable log individual object content.

Example

log individual

Syntax

no log individual

Mode

App Rules Policy

Description

Disable log individual object content.

Example

no log individual

Syntax

ips-message-format

Mode

App Rules Policy

Description

Enable log using IPS message format.

Example

ips-message-format

Syntax

no ips-message-format

Mode

App Rules Policy

Description

Disable log using IPS message format.

Example

```
no ips-message-format
```

Syntax

```
app-control-message-format
```

Mode

App Rules Policy

Description

Enable log using app control message format.

Example

```
app-control-message-format
```

Syntax

```
no app-control-message-format
```

Mode

App Rules Policy

Description

Disable log using app control message format.

Example

```
no app-control-message-format
```

Syntax

```
cfs-message-format
```

Mode

App Rules Policy

Description

Enable log using CFS message format.

Example

```
cfs-message-format
```

Syntax

```
no cfs-message-format
```

Mode

App Rules Policy

Description

Disable log using CFS message format.

Example

```
no cfs-message-format
```

Syntax

```
log redundancy { global | interval <UINT32> }
```

Mode

App Rules Policy

Description

Set log redundancy filter interval.

Options

global Use the global app rules redundancy filter setting.

interval Set the redundancy interval in seconds.

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
log-redundancy global  
log-redundancy interval 60
```

Syntax

```
connection-side { both | client | server }
```

Mode

App Rules Policy

Description

Set connection side.

Options

both Both sides.

client Client side.

server Server side.

Example

```
connection-side server
```

Syntax

```
direction { advanced [ [ from { any | zone <APP_RULES_POLICY_ZONE> } ] ] [ [ to { any | zone <APP_RULES_POLICY_ZONE> } ] ] ] | basic  
[ [ both | incoming | outgoing ] ] }
```

Mode

App Rules Policy

Description

Set direction.

Options

| | |
|---|--|
| <i>advanced</i> | Advanced. |
| <i>from</i> | From. |
| <i>any</i> | From any zone. |
| <i>zone</i> | Set the source zone. |
| <i><APP_RULES_POLICY_ZONE></i> | Zone object name. Example: <i>DMZ</i> |
| <i>to</i> | To. |
| <i>any</i> | To any zone. |
| <i>zone</i> | Set the destination zone. |
| <i><APP_RULES_POLICY_ZONE></i> | Zone object name. Example: <i>DMZ</i> |
| <i>basic</i> | Basic. |
| <i>both</i> | Both directions. |
| <i>incoming</i> | Incoming. |
| <i>outgoing</i> | Outgoing. |

Example

```
direction incoming
```

Syntax

```
zone { any | name <APP_RULES_POLICY_ZONE> }
```

Mode

App Rules Policy

Description

Set zone.

Options

| | |
|---|--|
| <i>any</i> | Set zone as any. |
| <i>name</i> | Set zone name. |
| <i><APP_RULES_POLICY_ZONE></i> | Zone object name. Example: <i>DMZ</i> |

Example

```
zone any  
zone name LAN
```

Syntax

```
cfs-list allow <APP_RULES_POLICY_CFS_LIST>
```

Mode

App Rules Policy

Description

Set CFS allow/included list for this app rules policy.

Options

<APP_RULES_POLICY_CFS_LIST> Word in the form: WORD or "QUOTED STRING".
Example: *abc*

Example

```
cfs-list allow "CFSAllowList"
```

Syntax

```
no cfs-list allow
```

Mode

App Rules Policy

Description

Clear CFS allow/included list for the app rules policy.

Example

```
no cfs-list allow
```

Syntax

```
cfs-list forbidden <APP_RULES_POLICY_CFS_LIST>
```

Mode

App Rules Policy

Description

Set CFS forbidden/excluded list for this app rules policy.

Options

<APP_RULES_POLICY_CFS_LIST> Word in the form: WORD or "QUOTED STRING".
Example: *abc*

Example

```
cfs-list forbidden "CFSForbiddenList"
```

Syntax

```
no cfs-list forbidden
```

Mode

App Rules Policy

Description

Clear CFS forbidden/excluded list for the app rules policy.

Example

```
no cfs-list forbidden
```

Syntax

safe-search

Mode

App Rules Policy

Description

Enable safe search enforcement.

Example

safe-search

Syntax

no safe-search

Mode

App Rules Policy

Description

Disable safe search enforcement.

Example

no safe-search

Syntax

youtube-for-schools

Mode

App Rules Policy

Description

Enable YouTube for schools.

Example

youtube-for-schools

Syntax

no youtube-for-schools

Mode

App Rules Policy

Description

Disbale YouTube for schools.

Example

no youtube-for-schools

Syntax

school-id <WORD>

Mode

App Rules Policy

Description

Set CFS school id.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

school-id HUST

Syntax

no school-id

Mode

App Rules Policy

Description

Clear CFS school id.

Example

no school-id

Syntax

app-control

Mode

Config

Description

Enter app control configuration mode.

Example

app-control

Syntax

update-signatures

Mode

App Control

Description

Update signature database.

Example

update-signatures

Syntax

enable

Mode

App Control

Description

Enable app control.

Example

enable

Syntax

no enable

Mode

App Control

Description

Disable app control.

Example

no enable

Syntax

log-all

Mode

App Control

Description

Enable logging for all apps.

Example

log-all

Syntax

no log-all

Mode

App Control

Description

Disable logging for all apps.

Example

no log-all

Syntax

log-filename

Mode

App Control

Description

Enable filename logging.

Example

log-filename

Syntax

no log-filename

Mode

App Control

Description

Disable filename logging.

Example

no log-filename

Syntax

log-redundancy filter <UINT16>

Mode

App Control

Description

Set app control log redundancy filter.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

log-redundancy filter 45

Syntax

reset

Mode

App Control

Description

Reset app control settings to default.

Example

reset

Syntax

```
category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> } [ [ application { id <AC_APP_ID> | name <AC_APP_NAME> } [ signature { id <AC_SIG_ID> | name <AC_SIG_NAME> } ] ] ]
```

Mode

App Control

Description

Enter configuration mode for the specified app control category, application or signature.

Options

| | |
|---------------------------------|---|
| id | Category ID. |
| <AC_CATEGORY_ID> | Category ID. Example: 123 |
| name | Category name. |
| <AC_CATEGORY_NAME> | Category name. Example: APP-UPDATE |
| application | Enter configuration mode for the specified app control application. |
| id | Application ID. |
| <AC_APP_ID> | Application ID. Example: 123 |
| name | Application name. |
| <AC_APP_NAME> | Application name. Example: APP-UPDATE |
| signature | Enter configuration mode for the specified app control signature. |
| id | Signature ID. |
| <AC_SIG_ID> | Signature ID. Example: 123 |
| name | Signature name. |
| <AC_SIG_NAME> | Signature name. |

Example

```
category name "GAMING"  
category name GAMING application name "Build-A-Bearville Online"  
category name APP-UPDATE application name 360Safe signature name "Update Traffic 6"
```

Syntax

```
exclusion list { ips | object { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK>  
<ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

App Control

Description

Enable and configure application control exclusion list.

Options

| | |
|--------------------------------|--|
| ips | Use IPS exclusion list. |
| object | Use specified address object for exclusion list. |
| group | Address object group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: Sales Group |
| host | Address object host. |

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Specify name of address object.

<ADDR_NAME_MIXED> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Specify IP range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
exclusion list ips
exclusion list object name "Corp App Control Exclusion List"
exclusion list object range 10.10.10.1 10.10.10.10
```

Syntax

```
no exclusion list
```

Mode

App Control

Description

Disable application control exclusion list.

Example

```
no exclusion list
```

Syntax

```
name <WORD>
```

Mode

App Control Category
App Control Application
App Control Signature

Description

Policy name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name GAMING
```

Syntax

id <UINT32>

Mode

App Control Category
App Control Application
App Control Signature

Description

Policy ID.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

id 8

Syntax

block

Mode

App Control Category

Description

Set blocking for app control category.

Example

block

Syntax

no block

Mode

App Control Category

Description

Disable blocking for app control category.

Example

no block

Syntax

log [enable | global]

Mode

App Control Category

Description

Set logging for app control category.

Options

enable Enable app control category logging.

global Use global setting.

Example

```
log global
```

Syntax

```
no log
```

Mode

App Control Category

Description

Disable logging for app control category.

Example

```
no log
```

Syntax

```
included users { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

App Control Category

Description

Set included users/groups.

Options

| | |
|--------------------------------------|---|
| administrator | Built-in administrator. |
| all | All. |
| group | Specify local user group. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests. |
| name | Specify local user. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
included users all
```

Syntax

```
excluded users { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

App Control Category

Description

Set excluded users/groups.

Options

| | |
|--------------------------------------|---|
| administrator | Built-in administrator. |
| group | Specify local user group. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests. |
| name | Specify local user. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
excluded users guests
```

Syntax

```
included ip { all | group <ADDR_GROUP_NAME_MIXED> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

App Control Category

Description

Set included IP address range.

Options

| | |
|--------------------------------------|--|
| all | All. |
| group | Address object group. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i> |
| name | Specify name of range address object. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Specify IP range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
included ip range 10.10.10.1 10.10.10.10
```

Syntax

```
excluded ip { group <ADDR_GROUP_NAME_MIXED> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

App Control Category

Description

Set excluded IP address range.

Options

| | |
|--------------------------------------|---|
| group | Address object group. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Specify name of range address object. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Specify IP range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
excluded ip range 10.10.10.1 10.10.10.10
```

Syntax

```
no excluded { ip | users }
```

Mode

App Control Category

Description

Disable exclude users/groups or IP addresses.

Options

| | |
|--------------|-------------------------------|
| ip | Disable exclude IP addresses. |
| users | Disable exclude users/groups. |

Example

```
no excluded users  
no excluded ip
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

App Control Category

Description

Set app control category schedule.

Options

| | |
|---------------------------------|---|
| <i>always-on</i> | Always on. |
| <i>days</i> | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| <i>time</i> | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <i>name</i> | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule always-on
```

Syntax

```
log-redundancy { filter <UINT16> | global }
```

Mode

App Control Category

Description

Set app control category log redundancy filter.

Options

| | |
|-----------------------|--|
| <i>filter</i> | Set log redundancy filter in seconds. |
| <UINT16> | Integer in the form: D OR 0xHHHH. Example: <i>123</i> |
| <i>global</i> | Use global setting. |

Example

```
log-redundancy filter 45
```

Syntax

```
block [ category | enable ]
```

Mode

App Control Application

Description

Set blocking for app control application.

Options

category Use category setting.

enable Enable app control application blocking.

Example

```
block category
```

Syntax

```
no block
```

Mode

App Control Application

Description

Disable blocking for app control application.

Example

```
no block
```

Syntax

```
log [ category | enable ]
```

Mode

App Control Application

Description

Set logging for app control application.

Options

category Use category setting.

enable Enable app control application logging.

Example

```
log category
```

Syntax

```
no log
```

Mode

App Control Application

Description

Disable logging for app control application.

Example

```
no log
```

Syntax

```
included users { administrator | all | category | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

App Control Application

Description

Set included users/groups.

Options

| | |
|--------------------------------------|---|
| administrator | Built-in administrator. |
| all | All. |
| category | Use category setting. |
| group | Specify local user group. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests. |
| name | Specify local user. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
included users all
```

Syntax

```
excluded users { administrator | category | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

App Control Application

Description

Set excluded users/groups.

Options

| | |
|--------------------------------------|---|
| administrator | Built-in administrator. |
| category | Use category setting. |
| group | Specify local user group. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests. |
| name | Specify local user. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
excluded users guests
```

Syntax

```
included ip { all | category | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK>  
<ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

App Control Application

Description

Set included IP address range.

Options

| | |
|-----------------------------------|--|
| all | All. |
| category | Use category setting. |
| group <ADDR_GROUP_NAME> | Address object group. Group address object name. Example: <i>Sales Group</i> |
| host <ADDR_HOST> | Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <ADDR_NAME_MIXED> | Address object name. Address object name. Example: <i>Web Server</i> |
| network <ADDR_NETWORK> | Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> | Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
included ip range 10.10.10.1 10.10.10.10
```

Syntax

```
excluded ip { category | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK>  
| range <ADDR_BEGIN> <ADDR_END> }
```

Mode

App Control Application

Description

Set excluded IP address range.

Options

| | |
|-----------------------------------|--|
| category | Use category setting. |
| group <ADDR_GROUP_NAME> | Address object group. Group address object name. Example: <i>Sales Group</i> |

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME_MIXED> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
excluded ip range 10.10.10.1 10.10.10.10
```

Syntax

```
no excluded { ip | users }
```

Mode

App Control Application

Description

Disable exclude users/groups or IP addresses.

Options

ip Disable exclude IP addresses.

users Disable exclude users/groups.

Example

```
no excluded users
no excluded ip
```

Syntax

```
schedule { always-on | category | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

App Control Application

Description

Set app control application schedule.

Options

always-on Always on.

| | |
|---------------------------------|---|
| category | Use category setting. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule always-on
```

Syntax

```
log-redundancy { category | filter <UINT16> }
```

Mode

App Control Application

Description

Set app control application log redundancy filter.

Options

category Use category setting.

filter Set log redundancy filter in seconds.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
log-redundancy filter 45
```

Syntax

```
category <WORD>
```

Mode

App Control Signature
App Control Application

Description

App control signature or application's category name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
category WEBMAIL
```

Syntax

application <WORD>

Mode

App Control Signature

Description

App control signature's application name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

application Cox

Syntax

block [*app* | *enable*]

Mode

App Control Signature

Description

Set blocking for app control signature.

Options

app Use app setting.

enable Enable app control signature blocking.

Example

block app

Syntax

no block

Mode

App Control Signature

Description

Disable blocking for app control signature.

Example

no block

Syntax

log [*app* | *enable*]

Mode

App Control Signature

Description

Set logging for app control signature.

Options

app Use app setting.

enable Enable app control signature logging.

Example

```
log app
```

Syntax

```
no log
```

Mode

App Control Signature

Description

Disable logging for app control signature.

Example

```
no log
```

Syntax

```
included users { administrator | all | app | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

App Control Signature

Description

Set included users/groups.

Options

| | |
|--------------------------------------|---|
| administrator | Built-in administrator. |
| all | All. |
| app | Use app setting. |
| group | Specify local user group. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests. |
| name | Specify local user. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
included users all
```

Syntax

```
excluded users { administrator | app | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

App Control Signature

Description

Set excluded users/groups.

Options

| | |
|--------------------------------------|---|
| administrator | Built-in administrator. |
| app | Use app setting. |
| group | Specify local user group. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests. |
| name | Specify local user. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
excluded users guests
```

Syntax

```
included ip { all | app | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

App Control Signature

Description

Set included IP address range.

Options

| | |
|--------------------------------|--|
| all | All. |
| app | Use app setting. |
| group | Address object group |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\nExample: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
included ip range 10.10.10.1 10.10.10.10
```

Syntax

```
excluded ip { app | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

App Control Signature

Description

Set excluded IP address range.

Options

app Use app setting.

group Address object group
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_NAME_MIXED> Address object name.
Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range Address object range.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
excluded ip range 10.10.10.1 10.10.10.10
```

Syntax

```
no excluded { ip | users }
```

Mode

App Control Signature

Description

Disable exclude users/groups or IP addresses.

Options

ip Disable exclude IP addresses.

users Disable exclude users/groups.

Example

```
no excluded users
no excluded ip
```

Syntax

```
schedule { always-on | app | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

App Control Signature

Description

Set app control signature schedule.

Options

| | |
|---------------------------------|---|
| always-on | Always on. |
| app | Use app setting. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule always-on
```

Syntax

```
log-redundancy { app | filter <UINT16> }
```

Mode

App Control Signature

Description

Set app control signature log redundancy filter.

Options

app Use app setting.

filter Set log redundancy filter in seconds.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
log-redundancy filter 45
```

Syntax

```
rbl
```

Mode

Config

Description

Enter Real-Time Blacklist Configuration Mode.

Example

```
rbl
```

Syntax

```
enable
```

Mode

RBL

Description

Enable Real-Time Blacklist Blocking.

Example

```
enable
```

Syntax

```
no enable
```

Mode

RBL

Description

Disable Real-Time Blacklist Blocking.

Example

```
no enable
```

Syntax

```
dns { inherit | static { primary <IPV4_HOST> | secondary <IPV4_HOST> | tertiary <IPV4_HOST> } }
```

Mode

RBL

Description

Set whether RBL DNS is inherited from WAN Zone or set manually with the associated DNS server IP addresses.

Options

| | |
|--------------------------|---|
| <i>inherit</i> | Inherit DNS servers. |
| <i>static</i> | Set static DNS server |
| <i>primary</i> | Specify primary DNS server IP address. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |
| <i>secondary</i> | Specify secondary DNS server IP address. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |
| <i>tertiary</i> | Specify tertiary DNS server IP address. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |

Example

```
dns primary 192.168.168.165
```

Syntax

```
no dns static { primary | secondary | tertiary }
```

Mode

RBL

Description

Manually Clear DNS server IP address.

Options

| | |
|-------------------------|--|
| <i>static</i> | Set static DNS server |
| <i>primary</i> | Clear primary DNS server IP address. |
| <i>secondary</i> | Clear secondary DNS server IP address. |
| <i>tertiary</i> | Clear tertiary DNS server IP address. |

Example

```
no dns primary
```

Syntax

```
service { domain <RBL_SERVICE_NAME> | enable <RBL_SERVICE_NAME> }
```

Mode

RBL

Description

Enable/Add/Edit Real-Time Blacklist Service.

Options

| | |
|---------------------------------|---|
| <i>domain</i> | Real-Time Blacklist Service Name. |
| <RBL_SERVICE_NAME> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

enable Enable specified parameter.
<RBL_SERVICE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
service domain avidspamsender.local
```

Syntax

```
no service { domain <RBL_SERVICE_NAME> | enable <RBL_SERVICE_NAME> }
```

Mode

RBL

Description

Delete Real-Time Blacklist Service.

Options

domain Real-Time Blacklist Service Name.
<RBL_SERVICE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

enable Enable specified parameter.
<RBL_SERVICE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no service enable xxx.org
```

Syntax

```
no services
```

Mode

RBL

Description

Delete all RBL services.

Example

```
no services
```

Syntax

```
clear statistics [ name <RBL_SERVICE_NAME> ]
```

Mode

RBL

Description

Clear all or specified RBL service statistics.

Options

name RBL service name.
<RBL_SERVICE_NAME> Word in the form: WORD or \"QUOTED STRING\".

Example: *abc*

Example

```
clear statistics
clear statistics name "dnsbl.sorbs.net"
```

Syntax

```
blacklist { fqdn <ADDR_FQDN> | host <ADDR_HOST> | name <RBL_ADDR_NAME> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

RBL

Description

Add SMTP server to blacklist.

Options

| | |
|------------------------------|--|
| fqdn | SMTP server Full Qualified Domain Name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| host | SMTP server host address. |
| <ADDR_HOST> | IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | SMTP server named host address object. |
| <RBL_ADDR_NAME> | Address object name. Example: <i>Web Server</i> |
| range | SMTP server Range. |
| <ADDR_BEGIN> | IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
blacklist host 168.226.49.15
```

Syntax

```
no blacklist { fqdn <RBL_ADDR_FQDN> | host <RBL_ADDR_HOST> | name <RBL_ADDR_NAME> | range <RBL_ADDR_BEGIN> <RBL_ADDR_END> }
```

Mode

RBL

Description

Remove SMTP server from blacklist.

Options

| | |
|------------------------------|--|
| fqdn | SMTP server Full Qualified Domain Name. |
| <RBL_ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| host | SMTP server host address. |
| <RBL_ADDR_HOST> | IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |

name SMTP server named host address object.
<RBL_ADDR_NAME> Address object name.
 Example: *Web Server*

range SMTP server Range.
<RBL_ADDR_BEGIN> IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:3257:9652\n*

<RBL_ADDR_END> IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:3257:effe\n*

Example

```
no blacklist host 168.226.49.15
```

Syntax

```
whitelist { fqdn <ADDR_FQDN> | host <ADDR_HOST> | name <RBL_ADDR_NAME> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

RBL

Description

Add SMTP server to whitelist.

Options

fqdn SMTP server Full Qualified Domain Name.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
 Example: *example.com*

host SMTP server host address.
<ADDR_HOST> IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:3257:9652\n*

name SMTP server named host address object.
<RBL_ADDR_NAME> Address object name.
 Example: *Web Server*

range SMTP server Range.
<ADDR_BEGIN> IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:3257:9652\n*

<ADDR_END> IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:3257:effe\n*

Example

```
whitelist host 168.226.49.15
```

Syntax

```
no whitelist { fqdn <RBL_ADDR_FQDN> | host <RBL_ADDR_HOST> | name <RBL_ADDR_NAME> | range <RBL_ADDR_BEGIN> <RBL_ADDR_END> }
```

Mode

RBL

Description

Remove SMTP server from whitelist.

Options

fqdn SMTP server Full Qualified Domain Name.
<RBL_ADDR_FQDN> FQDN in the form: example.com or *.example.com.
 Example: *example.com*

host SMTP server host address.
<RBL_ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name SMTP server named host address object.
<RBL_ADDR_NAME> Address object name.
 Example: *Web Server*

range SMTP server Range.
<RBL_ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*
<RBL_ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
 Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
no whitelist host 168.226.49.15
```

Syntax

```
enable
```

Mode

RBL Service

Description

Enable Real-Time Blacklist Domain.

Example

```
enable
```

Syntax

```
no enable
```

Mode

RBL Service

Description

Disable Real-Time Blacklist Domain.

Example

```
no enable
```

Syntax

```
domain <RBL_SERVICE_NAME>
```

Mode

RBL Service

Description

Set Real-Time Blacklist Service Domain Name.

Options

<RBL_SERVICE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
domain avidspamsender.local
```

Syntax

```
blocked-responses [ open-relay ] [ dialup-spam-source ] [ spam-source ] [ smart-host ] [ spamware-site ] [ bad-list-server ] [ insecure-script ] [ open-proxy-server ] [ block-all ]
```

Mode

RBL Service

Description

Enable specified RBL Blocked Responses.

Options

| | |
|---------------------------|---------------------------------|
| open-relay | 127.0.0.2 - Open Relay. |
| dialup-spam-source | 127.0.0.3 - Dialup Spam Source. |
| spam-source | 127.0.0.4 - Spam Source. |
| smart-host | 127.0.0.5 - Smart Host. |
| spamware-site | 127.0.0.6 - Spamware Site. |
| bad-list-server | 127.0.0.7 - Bad List Server. |
| insecure-script | 127.0.0.8 - Insecure Script. |
| open-proxy-server | 127.0.0.9 - Open Proxy Server. |
| block-all | Block All Responses. |

Example

```
blocked-responses open-relay spamware-site
```

Syntax

```
no blocked-responses [ open-relay ] [ dialup-spam-source ] [ spam-source ] [ smart-host ] [ spamware-site ] [ bad-list-server ] [ insecure-script ] [ open-proxy-server ] [ block-all ]
```

Mode

RBL Service

Description

Disable specified RBL Blocked Responses.

Options

| | |
|---------------------------|---------------------------------|
| open-relay | 127.0.0.2 - Open Relay. |
| dialup-spam-source | 127.0.0.3 - Dialup Spam Source. |
| spam-source | 127.0.0.4 - Spam Source. |
| smart-host | 127.0.0.5 - Smart Host. |
| spamware-site | 127.0.0.6 - Spamware Site. |
| bad-list-server | 127.0.0.7 - Bad List Server. |
| insecure-script | 127.0.0.8 - Insecure Script. |
| open-proxy-server | 127.0.0.9 - Open Proxy Server. |
| block-all | Block All Responses. |

Example

```
no blocked-responses open-relay spamware-site
```

Syntax

```
dpi-ssl { client | server }
```

Mode

Config

Description

Enter DPI-SSL configuration mode.

Options

client Enter client DPI-SSL configuration mode.

server Enter server DPI-SSL configuration mode.

Example

```
dpi-ssl server  
dpi-ssl client
```

Syntax

```
enable
```

Mode

Client DPI-SSL

Description

Enable SSL client inspection.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Client DPI-SSL

Description

Disable SSL client inspection.

Example

```
no enable
```

Syntax

```
intrusion-prevention
```

Mode

Client DPI-SSL

Description

Enable intrusion prevention for client DPI-SSL.

Example

```
intrusion-prevention
```

Syntax

```
no intrusion-prevention
```

Mode

Client DPI-SSL

Description

Disable intrusion prevention for client DPI-SSL.

Example

```
no intrusion-prevention
```

Syntax

```
gateway { anti-spyware | anti-virus }
```

Mode

Client DPI-SSL

Description

Enable gateway anti-virus or anti-spyware for client DPI-SSL.

Options

anti-spyware Enable gateway anti-spyware for client DPI-SSL.

anti-virus Enable gateway anti-virus for client DPI-SSL.

Example

```
gateway anti-virus
```

Syntax

```
no gateway { anti-spyware | anti-virus }
```

Mode

Client DPI-SSL

Description

Disable gateway anti-virus or anti-spyware for client DPI-SSL.

Options

anti-spyware Disable gateway anti-spyware for client DPI-SSL.

anti-virus Disable gateway anti-virus for client DPI-SSL.

Example

```
no gateway anti-virus
```

Syntax

application-firewall

Mode

Client DPI-SSL

Description

Enable application firewall for client DPI-SSL.

Example

application-firewall

Syntax

no application-firewall

Mode

Client DPI-SSL

Description

Disable application firewall for client DPI-SSL.

Example

no application-firewall

Syntax

content-filter

Mode

Client DPI-SSL

Description

Enable content filter for client DPI-SSL.

Example

content-filter

Syntax

no content-filter

Mode

Client DPI-SSL

Description

Disable content filter for client DPI-SSL.

Example

no content-filter

Syntax

authenticate-server-for-decrypted-connections

Mode

Client DPI-SSL

Description

Enable always authenticate server for decrypted connections for client DPI-SSL.

Example

authenticate-server-for-decrypted-connections

Syntax

no authenticate-server-for-decrypted-connections

Mode

Client DPI-SSL

Description

Disable always authenticate server for decrypted connections for client DPI-SSL.

Example

no authenticate-server-for-decrypted-connections

Syntax

expired-ca

Mode

Client DPI-SSL

Description

Enable allow expired CA.

Example

expired-ca

Syntax

no expired-ca

Mode

Client DPI-SSL

Description

Disable allow expired CA.

Example

no expired-ca

Syntax

deployment-server-domains

Mode

Client DPI-SSL

Description

Enable deployment wherein the firewall sees a single server IP for different server domains, ex: proxy setup.

Example

deployment-server-domains

Syntax

no deployment-server-domains

Mode

Client DPI-SSL

Description

Disable deployment wherein the firewall sees a single server IP for different server domains, ex: proxy setup.

Example

no deployment-server-domains

Syntax

bypass-decryption

Mode

Client DPI-SSL

Description

Enable allow SSL without decryption (bypass) when connection limit exceeded.

Example

bypass-decryption

Syntax

no bypass-decryption

Mode

Client DPI-SSL

Description

Disable allow SSL without decryption (bypass) when connection limit exceeded.

Example

no bypass-decryption

Syntax

audit-built-in-exclusion

Mode

Client DPI-SSL

Description

Enable audit new built-in exclusion domain names prior to being added for exclusion.

Example

```
audit-built-in-exclusion
```

Syntax

```
no audit-built-in-exclusion
```

Mode

Client DPI-SSL

Description

Disable audit new built-in exclusion domain names prior to being added for exclusion.

Example

```
no audit-built-in-exclusion
```

Syntax

```
authenticate-server
```

Mode

Client DPI-SSL

Description

Enable always authenticate server before applying exclusion policy.

Example

```
authenticate-server
```

Syntax

```
no authenticate-server
```

Mode

Client DPI-SSL

Description

Disable always authenticate server before applying exclusion policy.

Example

```
no authenticate-server
```

Syntax

```
open-failed-connections
```

Mode

Client DPI-SSL

Description

Open failed connections (that are not deemed a security threat).

Example

```
open-failed-connections
```

Syntax

```
no open-failed-connections
```

Mode

Client DPI-SSL

Description

Fail-open failed connections (that are not deemed a security threat).

Example

```
no open-failed-connections
```

Syntax

```
resigning-authority { certificate <CERT_NAME> | default [ 2048-bit | none-2048-bit ] }
```

Mode

Client DPI-SSL

Description

Set the re-signing authority certificate.

Options

certificate Specify DPI-SSL CA certificate.

<CERT_NAME> Certificate name.
Example: *my_cert*

default Default SonicWall DPI-SSL CA certificate.

2048-bit Default SonicWall DPI-SSL 2048 bit CA certificate.

none-2048-bit Default SonicWall DPI-SSL CA certificate.

Example

```
resigning-authority certificate "Corp CA Certificate"
```

Syntax

```
include address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | all | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Client DPI-SSL

Description

Set the DPI-SSL inclusion address object or group.

Options

| | |
|--------------------------------------|--|
| ipv6 | IPv6 address object. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| all | All addresses. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| mac | Address object mac. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
include address name "DPI Inclusion Object"
```

Syntax

```
exclude address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Client DPI-SSL

Description

Set the DPI-SSL exclusion address object or group.

Options

| | |
|-----------------------------|--|
| ipv6 | IPv6 address object. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: |

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n

Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK>

IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n

Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range

Address object range.

<ADDR_BEGIN>

IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n

Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END>

IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n

Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

fqdn

Address object full qualified domain name.

<ADDR_FQDN>

FQDN in the form: example.com or *.example.com.

Example: *example.com*

group

Address group name.

<ADDR_GROUP_NAME_MIXED>

Group address object name.

Example: *Sales Group*

mac

Address object mac.

<ADDR_MAC>

Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.

name

Address object name.

<ADDR_NAME_MIXED>

Address object name.

Example: *Web Server*

Example

```
exclude address name "DPI Exclusion Object"
```

Syntax

```
no exclude address
```

Mode

Client DPI-SSL

Description

Clear exclusion address objects or group for DPI-SSL client.

Example

```
no exclude address
```

Syntax

```
include service { all | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

Client DPI-SSL

Description

Set the DPI-SSL inclusion service object or group.

Options

all

All services.

group

Service group name.

<SVC_GROUP_NAME>

Service object group name.

Example: *VOIP*

| | |
|--------------------------------------|---|
| <i>name</i> | Service object name. |
| <i><SVC_NAME></i> | Service object name. Example: <i>HTTPS</i> |
| <i>protocol</i> | Service object protocol. |
| <i><SVC_PROTOCOL></i> | Service protocol. Example: <i>TCP</i> |
| <i><SVC_PORT_BEGIN></i> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <i><SVC_PORT_END></i> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
include service name "DPI Inclusion Service"
```

Syntax

```
exclude service { group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

Client DPI-SSL

Description

Set the DPI-SSL exclusion service object or group.

Options

| | |
|--------------------------------------|---|
| <i>group</i> | Service group name. |
| <i><SVC_GROUP_NAME></i> | Service object group name. Example: <i>VOIP</i> |
| <i>name</i> | Service object name. |
| <i><SVC_NAME></i> | Service object name. Example: <i>HTTPS</i> |
| <i>protocol</i> | Service object protocol. |
| <i><SVC_PROTOCOL></i> | Service protocol. Example: <i>TCP</i> |
| <i><SVC_PORT_BEGIN></i> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| <i><SVC_PORT_END></i> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |

Example

```
exclude service name "DPI Exclusion Service"
```

Syntax

```
no exclude service
```

Mode

Client DPI-SSL

Description

Clear exclusion service objects or group for DPI-SSL client.

Example

```
no exclude service
```

Syntax

```
include user { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

Client DPI-SSL

Description

Set the DPI-SSL inclusion user object or group.

Options

| | |
|--------------------------------------|---|
| administrator | Administrator. |
| all | All users. |
| group | Group object name. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guest users. |
| name | User object name. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
include user group "DPI User Group"
```

Syntax

```
exclude user { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

Client DPI-SSL

Description

Set the DPI-SSL exclusion user object or group.

Options

| | |
|--------------------------------------|---|
| administrator | Administrator. |
| group | Group object name. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guest users. |
| name | User object name. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
exclude user group "DPI User Group"
```

Syntax

```
no exclude user
```

Mode

Client DPI-SSL

Description

Clear exclusion user for DPI-SSL client.

Example

```
no exclude user
```

Syntax

```
reject <DPI_SSL_CLIENT_COMMON_NAME>
```

Mode

Client DPI-SSL

Description

Reject DPI-SSL client build-in common name.

Options

<DPI_SSL_CLIENT_COMMON_NAME> Client DPI-SSL common name.
Example: `update.software.local`

Example

```
reject .livemeeting.com
```

Syntax

```
accept <DPI_SSL_CLIENT_COMMON_NAME>
```

Mode

Client DPI-SSL

Description

Accept DPI-SSL client build-in common names.

Options

<DPI_SSL_CLIENT_COMMON_NAME> Client DPI-SSL common name.
Example: `update.software.local`

Example

```
accept .livemeeting.com
```

Syntax

```
no common-name <DPI_SSL_CLIENT_COMMON_NAME> [ action { exclude [ { authenticate-server | disable-authenticate-server } ] | skip-authentication | skip-content-filter-exclusion } ]
```

Mode

Client DPI-SSL

Description

Delete a DPI-SSL common name.

Options

<DPI_SSL_CLIENT_COMMON_NAME> Client DPI-SSL common name.
Example: `update.software.local`

| | |
|--------------------------------------|---|
| action | Set the action for client DPI-SSL common name. |
| exclude | Set action as exclude. |
| authenticate-server | Enable always authenticate server before applying exclusion policy |
| disable-authenticate-server | Disable always authenticate server before applying exclusion policy |
| skip-authentication | Set action as skip authentication. |
| skip-content-filter-exclusion | Set action as skip CFS category-based exclusion. |

Example

```
no common-name update.software.local
```

Syntax

```
no common-names [ exclude | skip-authentication | skip-content-filter-exclusion ]
```

Mode

Client DPI-SSL

Description

Delete all DPI-SSL common names.

Options

| | |
|--------------------------------------|---|
| exclude | Delete DPI-SSL exclusion common names. |
| skip-authentication | Delete DPI-SSL client skip authentication common names. |
| skip-content-filter-exclusion | Delete DPI-SSL client skip CFS category-based exclusion common names. |

Example

```
no common-names
no common-names exclude
no common-names skip-content-filter-exclusion
no common-names skip-authentication
```

Syntax

```
common-name <WORD> action { exclude [ { authenticate-server | disable-authenticate-server } ] | skip-authentication | skip-content-filter-exclusion }
```

Mode

Client DPI-SSL

Description

Add client DPI-SSL common name.

Options

| | |
|------------------------------------|---|
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: abc |
| action | Set the action for client DPI-SSL common name. |
| exclude | Set action as exclude. |
| authenticate-server | Enable always authenticate server before applying exclusion policy |
| disable-authenticate-server | Disable always authenticate server before applying exclusion policy |

skip-authentication Set action as skip authentication.

skip-content-filter-exclusion Set action as skip CFS category-based exclusion.

Example

```
common-name .sonicwall.com action skip-authentication
```

Syntax

```
cfs-categories { category <CONTENT_FILTER_CATEGORY_ID_NAME_HAVING_ALL> | exclude | include }
```

Mode

Client DPI-SSL

Description

Set content filter categories inclusion/exclusion.

Options

| | |
|---|---|
| category | Set inclusion/exclusion categories |
| <CONTENT_FILTER_CATEGORY_ID_NAME_HAVING_ALL> | Content filter category number and name with additional \"all\". Example: <i>all</i> |
| exclude | Enable exclude CFS categories. |
| include | Enable include CFS categories. |

Example

```
cfs-categories category "1. Violence/Hate/Racism"  
cfs-categories category all  
cfs-categories include  
cfs-categories exclude
```

Syntax

```
no cfs-categories category <CONTENT_FILTER_CATEGORY_ID_NAME_HAVING_ALL>
```

Mode

Client DPI-SSL

Description

Clear content filter categories inclusion/exclusion.

Options

| | |
|---|---|
| category | Clear inclusion/exclusion categories |
| <CONTENT_FILTER_CATEGORY_ID_NAME_HAVING_ALL> | Content filter category number and name with additional \"all\". Example: <i>all</i> |

Example

```
no cfs-categories category all  
no cfs-categories category "1. Violence/Hate/Racism"
```

Syntax

```
exclude cfs-category-unavailable
```

Mode

Client DPI-SSL

Description

Enable exclude connection if content filter category is not available.

Example

```
exclude cfs-category-unavailable
```

Syntax

```
no exclude cfs-category-unavailable
```

Mode

Client DPI-SSL

Description

Disable exclude connection if content filter category is not available.

Example

```
no exclude cfs-category-unavailable
```

Syntax

```
enable
```

Mode

Server DPI-SSL

Description

Enable SSL server inspection.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Server DPI-SSL

Description

Disable SSL server inspection.

Example

```
no enable
```

Syntax

```
intrusion-prevention
```

Mode

Server DPI-SSL

Description

Enable intrusion prevention for server DPI-SSL.

Example

```
intrusion-prevention
```

Syntax

```
no intrusion-prevention
```

Mode

Server DPI-SSL

Description

Disable intrusion prevention for server DPI-SSL.

Example

```
no intrusion-prevention
```

Syntax

```
gateway { anti-spyware | anti-virus }
```

Mode

Server DPI-SSL

Description

Enable gateway anti-virus or anti-spyware for server DPI-SSL.

Options

anti-spyware Enable gateway anti-spyware for server DPI-SSL.

anti-virus Enable gateway anti-virus for server DPI-SSL.

Example

```
gateway anti-virus
```

Syntax

```
no gateway { anti-spyware | anti-virus }
```

Mode

Server DPI-SSL

Description

Disable gateway anti-virus or anti-spyware for server DPI-SSL.

Options

anti-spyware Disable gateway anti-spyware for server DPI-SSL.

anti-virus Disable gateway anti-virus for server DPI-SSL.

Example

no gateway anti-virus

Syntax

application-firewall

Mode

Server DPI-SSL

Description

Enable application firewall for server DPI-SSL.

Example

application-firewall

Syntax

no application-firewall

Mode

Server DPI-SSL

Description

Disable application firewall for server DPI-SSL.

Example

no application-firewall

Syntax

```
include address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | all | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Server DPI-SSL

Description

Set the DPI-SSL inclusion address object or group.

Options

| | |
|-----------------------------|--|
| ipv6 | IPv6 address object. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\nExample: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |

| | |
|--------------------------------------|--|
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| all | All addresses. |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| mac | Address object MAC. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
include address name "DPI Inclusion Object"
```

Syntax

```
exclude address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Server DPI-SSL

Description

Set the DPI-SSL exclusion address object or group.

Options

| | |
|--------------------------------------|--|
| ipv6 | IPv6 address object. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| fqdn | Address object full qualified domain name. |
| <ADDR_FQDN> | FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group | Address group name. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |

| | |
|--------------------------------|---|
| mac | Address object MAC. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | Address object name. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |

Example

```
exclude address name "DPI Exclusion Object"
```

Syntax

```
include user { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

Server DPI-SSL

Description

Set the DPI-SSL inclusion user object or group.

Options

| | |
|--------------------------------------|---|
| administrator | Administrator. |
| all | All users. |
| group | Group object name. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guest users. |
| name | User object name. |
| <LOCAL_USER_NAME> | Local user object name. Example: <i>user1</i> |

Example

```
include user group "DPI User Group"
```

Syntax

```
exclude user { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

Server DPI-SSL

Description

Set the DPI-SSL exclusion user object or group.

Options

| | |
|--------------------------------------|---|
| administrator | Administrator. |
| group | Group object name. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guest users. |
| name | User object name. |

<LOCAL_USER_NAME> Local user object name.
Example: *user1*

Example

```
exclude user group "DPI User Group"
```

Syntax

```
no exclude { address | user }
```

Mode

Server DPI-SSL

Description

Clear exclusion for DPI-SSL server.

Options

address Clear exclusion address object or group for DPI-SSL server.

user Clear exclusion user or group for DPI-SSL server.

Example

```
no exclude address
```

Syntax

```
ssl-server [ ipv6 ] { fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name  
<ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } certificate <CERT_NAME> [ cleartext ]
```

Mode

Server DPI-SSL

Description

Add a DPI-SSL SSL server.

Options

ipv6 IPv6 address object.

fqdn Address object full qualified domain name.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address group name.
<ADDR_GROUP_NAME_MIXED> Group address object name.
Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

mac Address object MAC.
<ADDR_MAC> Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.

name Address object name.
<ADDR_NAME_MIXED> Address object name.
Example: *Web Server*

network Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n

Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK>

IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n

Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range

Address object range.

<ADDR_BEGIN>

IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n

Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END>

IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n

Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

certificate

Set the DPI-SSL SSL server certificate.

<CERT_NAME>

Certificate name.

Example: *my_cert*

cleartext

Enable clear text on the back end.

Example

```
ssl-server host 192.168.168.172 certificate "Corp SSL Server Certificate" cleartext
```

```
ssl-server name mySSLServerAo certificate "Corp SSL Server Certificate"
```

```
ssl-server group sslServerGroup certificate "Corp SSL Server Certificate"
```

Syntax

```
no ssl-server <DPI_SSL_SSL_SERVER_NAME>
```

Mode

Server DPI-SSL

Description

Delete a DPI-SSL SSL server.

Options

<DPI_SSL_SSL_SERVER_NAME> SSL server name.

Example: *DPI-SSL Server Name*

Example

```
no ssl-server sslServerGroup
```

Syntax

```
no ssl-servers
```

Mode

Server DPI-SSL

Description

Delete all DPI-SSL SSL servers.

Example

```
no ssl-servers
```

Syntax

```
client-enforcement anti-virus
```

Mode

Config

Description

Enter client anti-virus enforcement configuration mode.

Example

```
client-enforcement anti-virus
```

Syntax

```
policing
```

Mode

Client AV Enforcement

Description

Enable policing from trusted to public.

Example

```
policing
```

Syntax

```
no policing
```

Mode

Client AV Enforcement

Description

Disable policing from trusted to public.

Example

```
no policing
```

Syntax

```
force interval <UINT8>
```

Mode

Client AV Enforcement

Description

Set the number of days before forcing update.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
force interval 5
```

Syntax

```
no force interval
```

Mode

Client AV Enforcement

Description

Clear forcing update interval.

Example

```
no force interval
```

Syntax

```
force update { high | low | medium }
```

Mode

Client AV Enforcement

Description

Set risk levels for forcing update.

Options

high High risk.

low Low risk.

medium Medium risk.

Example

```
force update medium
force update high
force update low
```

Syntax

```
no force update { high | low | medium }
```

Mode

Client AV Enforcement

Description

Disable force update on alert for the set risk levels.

Options

high High risk.

low Low risk.

medium Medium risk.

Example

```
no force update medium
no force update high
no force update low
```

Syntax

```
enforcement-list { capture-client-exclusion | capture-client-inclusion | mcafee-exclusion | mcafee-inclusion } { host <ADDR_HOST>
| name <ADDR_HOST_RANGE_NAME> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

Client AV Enforcement

Description

Add host or range address object to enforcement lists.

Options

| | |
|-------------------------------------|--|
| capture-client-exclusion | Excluded from capture client enforcement list. |
| capture-client-inclusion | Capture client enforcement list. |
| mcafee-exclusion | Excluded from McAfee client AV enforcement list. |
| mcafee-inclusion | McAfee client AV enforcement list. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name | Address object name. |
| <ADDR_HOST_RANGE_NAME> | Host or range address object name. Example: <i>Web Server</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
enforcement-list mcafee-inclusion name "Gamers LAN"  
enforcement-list mcafee-exclusion host 10.10.10.10
```

Syntax

```
no enforcement-list { capture-client-exclusion name <CLIENT_NGAV_ENFORCEMENT_SENTINELONE_EXC_NAME> | capture-client-inclusion name <CLIENT_NGAV_ENFORCEMENT_SENTINELONE_INC_NAME> | mcafee-exclusion name <CLIENT_AV_ENFORCEMENT_MCAFFEE_EXC_NAME> | mcafee-inclusion name <CLIENT_AV_ENFORCEMENT_MCAFFEE_INC_NAME> }
```

Mode

Client AV Enforcement

Description

Delete host or range address objects from enforcement lists.

Options

| | |
|---|--|
| capture-client-exclusion | Excluded from capture client enforcement list. |
| name | Address object name. |
| <CLIENT_NGAV_ENFORCEMENT_SENTINELONE_EXC_NAME> | Excluded from capture client enforcement list member name. Example: <i>Web Server</i> |
| capture-client-inclusion | Capture client enforcement list. |
| name | Address object name. |
| <CLIENT_NGAV_ENFORCEMENT_SENTINELONE_INC_NAME> | Capture client enforcement list member name. Example: <i>Web Server</i> |
| mcafee-exclusion | Excluded from McAfee client AV enforcement list. |
| name | Address object name. |

<CLIENT_AV_ENFORCEMENT_MCAFFEE_EXC_NAME>

Excluded from McAfee client AV enforcement list member name.
Example: *Web Server*

mcafee-inclusion

McAfee client AV enforcement list.

name

Address object name.

<CLIENT_AV_ENFORCEMENT_MCAFFEE_INC_NAME>

McAfee client AV enforcement list member name.
Example: *Web Server*

Example

```
no enforcement-list mcafee-exclusion name "McAfee Exclusion Name"  
no enforcement-list mcafee-inclusion name "Gamers LAN"
```

Syntax

```
client-enforcement content-filtering
```

Mode

Config

Description

Enter client content filtering enforcement configuration mode.

Example

```
client-enforcement content-filtering
```

Syntax

```
grace-period <UINT8>
```

Mode

Client CFS Enforcement

Description

Set the number of days for the grace period.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
grace-period 5
```

Syntax

```
no grace-period
```

Mode

Client CFS Enforcement

Description

Set the grace period to 0 days.

Example

```
no grace-period
```

Syntax

```
enforcement-list { exclusion | inclusion } { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Client CFS Enforcement

Description

Add address object to enforcement lists.

Options

| | |
|---|---|
| exclusion | Excluded from client CF enforcement list. |
| inclusion | Add address object to client CF enforcement list. |
| ipv6 | IPv6 address object. |
| host <ADDR_HOST> | Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network <ADDR_NETWORK> | Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> | Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| fqdn <ADDR_FQDN> | Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| group <ADDR_GROUP_NAME_MIXED> | Address group name. Group address object name. Example: <i>Sales Group</i> |
| mac <ADDR_MAC> | Address object mac. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name <ADDR_NAME_MIXED> | Address object name. Address object name. Example: <i>Web Server</i> |

Example

```
enforcement-list inclusion name "Corp LAN"  
enforcement-list inclusion ipv6 host 1001::1002  
enforcement-list exclusion host 10.10.10.10  
enforcement-list exclusion ipv6 host fe80::1001
```

Syntax

```
no enforcement-list { exclusion | inclusion } { group <CLIENT_CF_ENFORCEMENT_GROUP_NAME> | name <CLIENT_CF_ENFORCEMENT_NAME> }
```

Mode

Client CFS Enforcement

Description

Delete address object from enforcement lists.

Options

| | |
|--|--|
| <i>exclusion</i> | Excluded from client CF enforcement list. |
| <i>inclusion</i> | Delete address object from client CF enforcement list. |
| <i>group</i> | Address group name. |
| <i><CLIENT_CF_ENFORCEMENT_GROUP_NAME></i> | Address object name. Example: <i>Web Server</i> |
| <i>name</i> | Address object name. |
| <i><CLIENT_CF_ENFORCEMENT_NAME></i> | Address object name. Example: <i>Web Server</i> |

Example

```
no enforcement-list inclusion name "Corp LAN"  
no enforcement-list exclusion name "Exclusion Name"
```

Syntax

```
default-enforcement { client-cf-enforcement | none }
```

Mode

Client CFS Enforcement

Description

Set the default enforcement for computers whose addresses do not fall in any of the lists.

Options

| | |
|-------------------------------------|--|
| <i>client-cf-enforcement</i> | Use client content filtering enforcement by default. |
| <i>none</i> | Clear the default enforcement. |

Example

```
default-enforcement client-cf-enforcement
```

Syntax

```
no default-enforcement
```

Mode

Client CFS Enforcement

Description

Clear the default enforcement.

Example

```
no default-enforcement
```

Syntax

```
geo-ip
```

Mode

Config

Description

Enter Geo-IP configuration mode.

Example

```
geo-ip
```

Syntax

```
custom-list
```

Mode

Geo-IP

Description

Enter custom list configuration mode.

Example

```
custom-list
```

Syntax

```
enable
```

Mode

Custom List

Description

Enable Geo-IP custom list.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Custom List

Description

Disable Geo-IP custom list.

Example

```
no enable
```

Syntax

```
override-countries
```

Mode

Custom List

Description

Override firewall countries by custom list.

Example

```
override-countries
```

Syntax

```
no override-countries
```

Mode

Custom List

Description

Disable override firewall countries by custom list.

Example

```
no override-countries
```

Syntax

```
address { group <ADDR_GROUP_NAME> | name <ADDR_NAME> }
```

Mode

Custom List

Description

Set Geo-IP custom list IP address and enter address configuration mode.

Options

| | |
|--------------------------------|---|
| group | Set address group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |

| | |
|--------------------------|--|
| name | Set address object name. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |

Example

```
address name "X5 Subnet"  
address group "WLAN Subnets"
```

Syntax

```
no address { group <GEO_IP_ADDR_GROUP> | name <GEO_IP_ADDR_NAME> }
```

Mode

Custom List

Description

Delete a Geo-IP custom list IP address object.

Options

group Address object group.
<GEO_IP_ADDR_GROUP> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

name Address object name.
<GEO_IP_ADDR_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no address name "X5 Subnet"  
no address group "WLAN Subnets"
```

Syntax

```
no addresses
```

Mode

Custom List

Description

Delete all address objects from Geo-IP custom list.

Example

```
no addresses
```

Syntax

```
country <GEO_IP_BLOCKED_COUNTRY>
```

Mode

Geo IP Custom Country Entry

Description

Set the country.

Options

<GEO_IP_BLOCKED_COUNTRY> Geo-IP blocked country name.
Example: *Angola*

Example

```
country Antartica
```

Syntax

```
comment <WORD>
```

Mode

Geo IP Custom Country Entry

Description

Set the comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "USServer".
```

Syntax

```
no comment
```

Mode

Geo IP Custom Country Entry

Description

Clear the comment.

Example

```
no comment
```

Syntax

```
block connections [ all | firewall-rule-based ]
```

Mode

Geo-IP

Description

Set block connection method for Geo-IP.

Options

all All connections.

firewall-rule-based Firewall rule based connections.

Example

```
block connections firewall-rule-based
block connections all
block connections
```

Syntax

```
no block connections
```

Mode

Geo-IP

Description

Disable blocking connections to/from configured country list.

Example

```
no block connections
```

Syntax

```
block database-not-downloaded
```

Mode

Geo-IP

Description

Enable blocking all connections to public IPs if Geo-IP database is not downloaded.

Example

```
block database-not-downloaded
```

Syntax

```
no block database-not-downloaded
```

Mode

Geo-IP

Description

Disable blocking all connections to public IPs if Geo-IP database is not downloaded.

Example

```
no block database-not-downloaded
```

Syntax

```
logging
```

Mode

Geo-IP

Description

Enable Geo-IP filter logging.

Example

```
logging
```

Syntax

```
no logging
```

Mode

Geo-IP

Description

Disable Geo-IP filter logging.

Example

```
no logging
```

Syntax

```
block country <GEO_IP_BLOCKED_COUNTRY>
```

Mode

Geo-IP

Description

Enable the country in the configured country list.

Options

<GEO_IP_BLOCKED_COUNTRY> Geo-IP blocked country name.
Example: *Angola*

Example

```
block country Antartica
```

Syntax

```
no block country <GEO_IP_BLOCKED_COUNTRY>
```

Mode

Geo-IP

Description

Disable the country in the configured country list.

Options

<GEO_IP_BLOCKED_COUNTRY> Geo-IP blocked country name.
Example: *Angola*

Example

```
no block country Canada
```

Syntax

```
block countries [ unknown ]
```

Mode

Geo-IP

Description

Set block countries for Geo-IP.

Options

unknown Enable block all unknown countries.

Example

```
block countries  
block countries unknown
```

Syntax

```
no block countries [ unknown ]
```

Mode

Geo-IP

Description

Set block countries for Geo-IP.

Options

unknown Disable block all unknown countries.

Example

```
no block countries
no block countries unknown
```

Syntax

```
no exclude
```

Mode

Geo-IP

Description

Clear Geo-IP exclusion objects.

Example

```
no exclude
```

Syntax

```
exclude { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group
<ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Geo-IP

Description

Set Geo-IP exclusion object.

Options

| | |
|---|---|
| ipv6 | IPv6 |
| host <ADDR_HOST> | Geo-IP exclusion host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network <ADDR_NETWORK> | Geo-IP exclusion network IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <ADDR_BEGIN> | Geo-IP exclusion range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group <ADDR_GROUP_NAME_MIXED> | Geo-IP exclusion named address group. Group address object name. Example: <i>Sales Group</i> |
| name <ADDR_NAME_MIXED> | Geo-IP exclusion named address object. Address object name. Example: <i>Web Server</i> |

Example

```
exclude name "X5 Subnet"
exclude group "WLAN Subnets"
```

```
exclude host 192.168.168.168
exclude network 192.168.168.1 255.255.255.0
exclude range 192.168.168.10 192.168.168.100
exclude ipv6 host fe80::1001
exclude ipv6 network fe80::1 /64
exclude ipv6 range fe80::1001 fe80::1010
```

Syntax

```
include block-details
```

Mode

Geo-IP

Description

Enable inclusion of Geo-IP block details.

Example

```
include block-details
```

Syntax

```
no include block-details
```

Mode

Geo-IP

Description

Disable inclusion of Geo-IP block details.

Example

```
no include block-details
```

Syntax

```
alert-text <WORD>
```

Mode

Geo-IP

Description

Set the Geo-IP alert text.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
alert-text "This site had been blocked by the network administrator."
```

Syntax

```
no alert-text
```

Mode

Geo-IP

Description

Clear the Geo-IP alert text.

Example

```
no alert-text
```

Syntax

```
logo-icon { data <GEO_IP_LOGO_ICON_DATA> | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Geo-IP

Description

Set/Upload the Botnet Base64 encoded logo icon.

Options

| | |
|--------------------------------------|--|
| data | Set the Geo-IP Base64 encoded logo icon with user input. |
| <GEO_IP_LOGO_ICON_DATA> | Geo-IP logo icon data. Example: <code>data:image/gif;base64,GEOIP/BOTNETLOGOICONDATA</code> |
| ftp | Import using the FTP protocol. |
| <FTP_URL> | FTP URL in the form: <code>ftp://username:password@hostname/</code> Escape character: <code>'-' -> '\\\\', '@' -> '\\\\@', '/' -> '\\\\/', '\\-' -> '\\\\\\\\'</code> . Example: <code>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</code> |
| scp | Export using the SCP protocol. |
| <SCP_URL> | SCP URL in the form: <code>scp://username@host/</code> Escape character: <code>'-' -> '\\\\', '@' -> '\\\\@', '/' -> '\\\\/', '\\-' -> '\\\\\\\\'</code> . Example: <code>scp://username@host/\\nscp://host/</code> |
| port | SCP port. |
| <IPV4_PORT> | Integer in the form: D OR 0xHHHH. Example: <code>80</code> |

Example

```
logo-icon data "data:image/gif;base64,base64 encoded text goes here"
```

Syntax

```
default blocked-page
```

Mode

Geo-IP

Description

Set the blocked page settings to default.

Example

```
default blocked-page
```

Syntax

```
botnet
```

Mode

Config

Description

Enter botnet filter configuration mode.

Example

```
botnet
```

Syntax

```
custom-list
```

Mode

Botnet

Description

Enter custom list configuration mode.

Example

```
custom-list
```

Syntax

```
dynamic-list
```

Mode

Botnet

Description

Enter dynamic list configuration mode.

Example

```
dynamic-list
```

Syntax

```
block connections { all | firewall-rule-based }
```

Mode

Botnet

Description

Enable blocking connections to/from botnet command and control centers.

Options

all All connections.

firewall-rule-based Firewall rule based connections.

Example

```
block connections firewall-rule-based
```

Syntax

```
no block connections
```

Mode

Botnet

Description

Disable blocking connections to/from botnet command and control centers.

Example

```
no block connections
```

Syntax

```
block database-not-downloaded
```

Mode

Botnet

Description

Enable blocking all connections to public IPs if botnet database is not downloaded.

Example

```
block database-not-downloaded
```

Syntax

```
no block database-not-downloaded
```

Mode

Botnet

Description

Disable blocking all connections to public IPs if botnet database is not downloaded.

Example

```
no block database-not-downloaded
```

Syntax

```
enable
```

Mode

Custom List

Description

Enable botnet custom list.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Custom List

Description

Disable botnet custom list.

Example

```
no enable
```

Syntax

```
address { group <ADDR_GROUP_NAME> | name <ADDR_NAME> }
```

Mode

Custom List

Description

Set botnet custom list IP address and enter address configuration mode.

Options

group Set address group.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

name Set address object name.
<ADDR_NAME> Address object name.
Example: *Web Server*

Example

```
address name "X5 Subnet"  
address group "WLAN Subnets"
```

Syntax

```
no address { group <BOTNET_ADDR_GROUP> | name <BOTNET_ADDR_NAME> }
```

Mode

Custom List

Description

Delete a botnet custom list IP address object.

Options

group Group address object.
<BOTNET_ADDR_GROUP> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

name Name address object.
<BOTNET_ADDR_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no address name "X5 Subnet"  
no address group "WLAN Subnets"
```

Syntax

no addresses

Mode

Custom List

Description

Delete all address objects from botnet custom list.

Example

no addresses

Syntax

name <WORD>

Mode

Custom List Botnet Entry

Description

Botnet custom list name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name "X5 Subnet"

Syntax

group <WORD>

Mode

Custom List Botnet Entry

Description

Botnet custom list group.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

group "WLAN Subnets"

Syntax

enable

Mode

Custom List Botnet Entry

Description

Enable custom list botnet.

Example

enable

Syntax

no enable

Mode

Custom List Botnet Entry

Description

Disable custom list botnet.

Example

no enable

Syntax

comment <WORD>

Mode

Custom List Botnet Entry

Description

Set comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Remote USServer"

Syntax

no comment

Mode

Custom List Botnet Entry

Description

Clear comment.

Example

no comment

Syntax

enable

Mode

Dynamic List

Description

Enable botnet dynamic list.

Example

enable

Syntax

no enable

Mode

Dynamic List

Description

Disable botnet dynamic list.

Example

no enable

Syntax

flush

Mode

Dynamic List

Description

Flush the IPs downloaded from dynamic botnet servers.

Example

flush

Syntax

download

Mode

Dynamic List

Description

Download the IPs downloaded from dynamic botnet servers.

Example

download

Syntax

periodical-download

Mode

Dynamic List

Description

Enable botnet list download periodically.

Example

periodical-download

Syntax

no periodical-download

Mode

Dynamic List

Description

Disable botnet list download periodically.

Example

no periodical-download

Syntax

download-interval { 15minutes | 1hour | 24hours | 5minutes }

Mode

Dynamic List

Description

Set a download interval for the dynamic botnet list server.

Options

15minutes Set the download interval as 15 minutes.

1hour Set the download interval as 1 hour.

24hours Set the download interval as 24 hours.

5minutes Set the download interval as 5 minutes.

Example

download-interval 5minutes

Syntax

protocol { FTP | HTTPS }

Mode

Dynamic List

Description

Set botnet server protocol type.

Options

FTP FTP protocol.

HTTPS HTTPS protocol.

Example

protocol HTTPS

Syntax

server-ip-address <IPV4_HOST>

Mode

Dynamic List

Description

Set server IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

server-ip-address 2.2.2.2

Syntax

no server-ip-address

Mode

Dynamic List

Description

Clear server IP address.

Example

no server-ip-address

Syntax

login <WORD>

Mode

Dynamic List

Description

Set login ID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

login admin

Syntax

no login

Mode

Dynamic List

Description

Clear login ID.

Example

```
no login
```

Syntax

```
password <WORD>
```

Mode

Dynamic List

Description

Set password.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
password mypassword
```

Syntax

```
no password
```

Mode

Dynamic List

Description

Clear password.

Example

```
no password
```

Syntax

```
directory-path <WORD>
```

Mode

Dynamic List

Description

Set server directory path.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
directory-path "server/botnet"
```

Syntax

no directory-path

Mode

Dynamic List

Description

Clear server directory path.

Example

no directory-path

Syntax

file-name <WORD>

Mode

Dynamic List

Description

Set server file name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

file-name aaa

Syntax

no file-name

Mode

Dynamic List

Description

Clear server file name.

Example

no file-name

Syntax

url-name <WORD>

Mode

Dynamic List

Description

Set server url name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
url-name www.SonicWall.com
```

Syntax

```
no url-name
```

Mode

Dynamic List

Description

Clear server url name.

Example

```
no url-name
```

Syntax

```
logging
```

Mode

Botnet

Description

Enable botnet filter logging.

Example

```
logging
```

Syntax

```
no logging
```

Mode

Botnet

Description

Disable botnet filter logging.

Example

```
no logging
```

Syntax

```
exclude { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group  
<ADDR_GROUP_NAME> | name <ADDR_NAME> }
```

Mode

Botnet

Description

Set botnet exclusion object.

Options

| | |
|--------------------------------|--|
| ipv6 | IPv6 |
| host | Botnet exclusion host address. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Botnet exclusion network |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Botnet exclusion range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| group | Botnet exclusion named address group. |
| <ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| name | Botnet exclusion named address object. |
| <ADDR_NAME> | Address object name. Example: <i>Web Server</i> |

Example

```
exclude name "X5 Subnet"
exclude group "WLAN Subnets"
exclude host 192.168.168.168
exclude network 192.168.168.1 255.255.255.0
exclude range 192.168.168.10 192.168.168.100
exclude ipv6 host fe80::1001
exclude ipv6 network fe80::1 /64
exclude ipv6 range fe80::1001 fe80::1010
```

Syntax

```
no exclude
```

Mode

Botnet

Description

Clear botnet exclusion objects.

Example

```
no exclude
```

Syntax

```
include block-details
```

Mode

Botnet

Description

Enable inclusion of botnet block details.

Example

`include block-details`

Syntax

`no include block-details`

Mode

Botnet

Description

Disable inclusion of botnet block details.

Example

`no include block-details`

Syntax

`alert-text <WORD>`

Mode

Botnet

Description

Set the botnet alert text.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: `abc`

Example

`alert-text "This site had been blocked by the network administrator"`

Syntax

`no alert-text`

Mode

Botnet

Description

Set the botnet alert text.

Example

`no alert-text`

Syntax

`logo-icon { data <GEO_IP_LOGO_ICON_DATA> | ftp <FTP_URL> | scp <SCP_URL> }`

Mode

Botnet

Description

Set/Upload the botnet Base64 encoded logo icon.

Options

| | |
|--------------------------------------|--|
| data | Set the botnet base64 encoded logo icon data. |
| <GEO_IP_LOGO_ICON_DATA> | Geo-IP logo icon data. Example: <code>data:image/gif;base64,GEOIP/BOTNETLOGOICONDATA</code> |
| ftp | Set base64 encoded logo icon data using the FTP protocol. |
| <FTP_URL> | FTP URL in the form: <code>ftp://username:password@hostname/</code> Escape character: <code>'-' -> '\\\\', '@' -> '\\\\@', '/' -> '\\\\/', '\\\\' -> '\\\\\\\\'</code> . Example: <code>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</code> |
| scp | Set base64 encoded logo icon data using the SCP protocol. |
| <SCP_URL> | SCP URL in the form: <code>scp://username@host/</code> Escape character: <code>'-' -> '\\\\', '@' -> '\\\\@', '/' -> '\\\\/', '\\\\' -> '\\\\\\\\'</code> . Example: <code>scp://username@host/\\nscp://host/</code> |

Example

```
logo-icon data "data:image/gif;base64,base64 encoded text goes here"
```

Syntax

```
default blocked-page
```

Mode

Botnet

Description

Set the blocked page settings to default.

Example

```
default blocked-page
```

Syntax

```
anti-spyware
```

Mode

Config

Description

Enter anti-spyware configuration mode.

Example

```
anti-spyware
```

Syntax

```
update-signatures
```

Mode

Anti-spyware

Description

Update signature database.

Example

```
update-signatures
```

Syntax

enable

Mode

Anti-spyware

Description

Enable anti-spyware.

Example

enable

Syntax

no enable

Mode

Anti-spyware

Description

Disable anti-spyware.

Example

no enable

Syntax

```
signature-group { high-danger [ prevent-all ] [ detect-all ] [ log-redundancy <UINT32> ] | low-danger [ prevent-all ] [ detect-all ] [ log-redundancy <UINT32> ] | medium-danger [ prevent-all ] [ detect-all ] [ log-redundancy <UINT32> ] }
```

Mode

Anti-spyware

Description

Set signature group detection and log redundancy.

Options

| | |
|-----------------------|--|
| high-danger | High danger attacks. |
| prevent-all | Prevent all. |
| detect-all | Detect all. |
| log-redundancy | Set log redundancy in seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |
| low-danger | Low danger attacks. |
| prevent-all | Prevent all. |
| detect-all | Detect all. |
| log-redundancy | Set log redundancy in seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |
| medium-danger | Medium danger attacks. |
| prevent-all | Prevent all. |
| detect-all | Detect all. |
| log-redundancy | Set log redundancy in seconds. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |

Example

```
signature-group high-danger prevent-all log-redundancy 1
```

Syntax

```
no signature-group { high-danger [ prevent-all ] [ detect-all ] [ log-redundancy ] | low-danger [ prevent-all ] [ detect-all ] [ log-redundancy ] | medium-danger [ prevent-all ] [ detect-all ] [ log-redundancy ] }
```

Mode

Anti-spyware

Description

Clear signature group detection.

Options

high-danger High danger attacks.
prevent-all Prevent all.
detect-all Detect all.
log-redundancy Set log redundancy in seconds.

low-danger Low danger attacks.
prevent-all Prevent all.
detect-all Detect all.
log-redundancy Set log redundancy in seconds.

medium-danger Medium danger attacks.
prevent-all Prevent all.
detect-all Detect all.
log-redundancy Set log redundancy in seconds.

Example

```
no signature-group high-danger prevent-all
```

Syntax

```
reset
```

Mode

Anti-spyware

Description

Reset anti-spyware settings and policies to default.

Example

```
reset
```

Syntax

```
inspection inbound [ http ] [ ftp ] [ imap ] [ smtp ] [ pop3 ]
```

Mode

Anti-spyware

Description

Enable inbound inspection for the specified protocols.

Options

http HTTP.
ftp FTP.
imap IMAP.
smtp SMTP.
pop3 POP3.

Example

```
inspection inbound http smtp
```

Syntax

```
no inspection inbound [ http ] [ ftp ] [ imap ] [ smtp ] [ pop3 ]
```

Mode

Anti-spyware

Description

Disable inbound inspection for the specified protocols.

Options

http HTTP.
ftp FTP.
imap IMAP.
smtp SMTP.
pop3 POP3.

Example

```
no inspection inbound http smtp
```

Syntax

```
inspection outbound
```

Mode

Anti-spyware

Description

Enable inspection of outbound spyware communication.

Example

```
inspection outbound
```

Syntax

```
no inspection outbound
```

Mode

Anti-spyware

Description

Disable inspection of outbound spyware communication.

Example

```
no inspection outbound
```

Syntax

smtp-responses

Mode

Anti-spyware

Description

Enable SMTP responses.

Example

smtp-responses

Syntax

no smtp-responses

Mode

Anti-spyware

Description

Disable SMTP responses.

Example

no smtp-responses

Syntax

http-clientless-notification

Mode

Anti-spyware

Description

Enable HTTP clientless notification alerts.

Example

http-clientless-notification

Syntax

no http-clientless-notification

Mode

Anti-spyware

Description

Disable HTTP clientless notification alerts.

Example

no http-clientless-notification

Syntax

message <WORD>

Mode

Anti-spyware

Description

Set HTTP clientless notification message to display when blocking.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
message "This request is blocked by the SonicWall Gateway Anti-Spyware Service."
```

Syntax

```
no message
```

Mode

Anti-spyware

Description

Clear the notification message when blocking.

Example

```
no message
```

Syntax

```
exclusion { address-object { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }  
} | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> } | entry  
<ANTI_SPYWARE_EXCLUSION_BEGIN_IP> <ANTI_SPYWARE_EXCLUSION_END_IP> | list }
```

Mode

Anti-spyware

Description

Set anti-spyware exclusion list and enable.

Options

| | |
|-----------------------------|---|
| address-object | Set exclusion list with address object. |
| ipv6 | IPv6 address. |
| host | Address object host. |
| <ADDR_HOST> | IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| network | Address object network. |
| <ADDR_NETWORK> | IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> |
| <ADDR_MASK> | IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range | Address object range. |
| <ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: |

| | |
|--|---|
| <ADDR_END> | <pre> HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n </pre> |
| fqdn <ADDR_FQDN> | <pre> Address object FQDN. FQDN in the form: example.com or *.example.com. Example: example.com </pre> |
| group <ADDR_GROUP_NAME_MIXED> | <pre> Address group. Group address object name. Example: Sales Group </pre> |
| mac <ADDR_MAC> | <pre> Address object MAC. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. </pre> |
| name <ADDR_NAME_MIXED> | <pre> Address object name. Address object name. Example: Web Server </pre> |
| entry <ANTI_SPYWARE_EXCLUSION_BEGIN_IP> | <pre> Set exclusion list entry. The from IP of anti-spyware exclusion range list. Example: 192.168.168.168 </pre> |
| <ANTI_SPYWARE_EXCLUSION_END_IP> | <pre> The end IP of anti-spyware exclusion range list. Example: 192.168.168.168 </pre> |
| list | <pre> Enable anti-spyware exclusion list. </pre> |

Example

```

exclusion list
exclusion address-object name "All Interface IP"
exclusion entry 10.10.10.10 10.10.10.100

```

Syntax

```
no exclusion list
```

Mode

Anti-spyware

Description

Disable anti-spyware exclusion list.

Example

```
no exclusion list
```

Syntax

```
no exclusion entry <ANTI_SPYWARE_EXCLUSION_BEGIN_IP> <ANTI_SPYWARE_EXCLUSION_END_IP>
```

Mode

Anti-spyware

Description

Delete anti-spyware exclusion list entry.

Options

| | |
|--|---|
| <ANTI_SPYWARE_EXCLUSION_BEGIN_IP> | <pre> The from IP of anti-spyware exclusion range list. Example: 192.168.168.168 </pre> |
| <ANTI_SPYWARE_EXCLUSION_END_IP> | <pre> The end IP of anti-spyware exclusion range list. Example: 192.168.168.168 </pre> |

Example

```
no exclusion entry 10.10.10.1 10.10.10.10
```

Syntax

```
no exclusion entries
```

Mode

Anti-spyware

Description

Delete all anti-spyware exclusion list entries.

Example

```
no exclusion entries
```

Syntax

```
product { id <ANTI_SPYWARE_PRODUCT_ID> | name <ANTI_SPYWARE_PRODUCT_NAME> } [ policy id <ANTI_SPYWARE_POLICY_ID> ]
```

Mode

Anti-spyware

Description

Enter configuration mode for the specified anti-spyware product.

Options

| | |
|--|--|
| id | Product ID. |
| <ANTI_SPYWARE_PRODUCT_ID> | The ID of anti-spyware product. Example: 123 |
| name | Anti-spyware product name. |
| <ANTI_SPYWARE_PRODUCT_NAME> | The name of anti-spyware product. Example: abc |
| policy | Configure the anti-spyware policy and enter its configure mode. |
| id | Anti-spyware policy ID. |
| <ANTI_SPYWARE_POLICY_ID> | The policy ID of the specified anti-spyware product. Example: 123 |

Example

```
product name "123mania"  
product id 940  
product name "180solutions" policy id 837
```

Syntax

```
name <WORD>
```

Mode

Anti-spyware Product
Anti-spyware Policy

Description

Anti-spyware product name or policy name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name 123minia

Syntax

id <UINT32>

Mode

Anti-spyware Product
Anti-spyware Policy

Description

Anti-spyware product ID or policy ID.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

id 3364

Syntax

prevention [enable | global]

Mode

Anti-spyware Product

Description

Set prevention for anti-spyware product.

Options

enable Enable anti-spyware product prevention.

global Use global setting.

Example

prevention global

Syntax

no prevention

Mode

Anti-spyware Product

Description

Disable prevention for anti-spyware product.

Example

no prevention

Syntax

detection [enable | global]

Mode

Anti-spyware Product

Description

Set detection for anti-spyware product.

Options

enable Enable anti-spyware product detection.

global Use global setting.

Example

detection

Syntax

no detection

Mode

Anti-spyware Product

Description

Disable detection for anti-spyware product.

Example

no detection

Syntax

included { ip { all | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> } | users { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <USER_NAME> } }

Mode

Anti-spyware Product

Description

Set included users or IP address ranges.

Options

ip Set included IP address ranges.

all All IP address ranges.

group Group of IP address ranges.
<ADDR_GROUP_NAME_MIXED> Group address object name.
Example: *Sales Group*

name Name of IP address range.
<ADDR_NAME_MIXED> Address object name.
Example: *Web Server*

users Set included users or groups.

| | |
|--------------------------------------|---|
| administrator | Administrator. |
| all | All users and groups. |
| group | Group of users. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests users. |
| name | Name of users. |
| <USER_NAME> | User object name. Example: <i>user1</i> |

Example

```
included users all
included users name user1
included ip all
included ip name aol
```

Syntax

```
excluded { ip { all | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> } | users { administrator | all | group
<LOCAL_USER_GROUP_NAME> | guests | name <USER_NAME> } }
```

Mode

Anti-spyware Product

Description

Set excluded users/groups or IP address ranges.

Options

| | |
|--------------------------------------|---|
| ip | Set excluded IP address ranges. |
| all | All IP address ranges. |
| group | Group of IP address ranges. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| name | Name of IP address range. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |
| users | Set excluded users or groups. |
| administrator | Administrator. |
| all | All users and groups. |
| group | Group of users. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests users. |
| name | Name of users. |
| <USER_NAME> | User object name. Example: <i>user1</i> |

Example

```
excluded users administrator
excluded ip name aol
```

Syntax

```
no excluded { ip | users }
```

Mode

Anti-spyware Product

Description

Set no excluded users or IP address.

Options

ip Set no excluded IP address.

users Set no excluded users.

Example

```
no excluded users
no excluded ip
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

Anti-spyware Product

Description

Set anti-spyware product schedule.

Options

always-on Always on.

days Schedule object days.

<SCHED_DAYS> Days of the week in the form: SU-M-T-W-TH-F-SA.
Example: *SU-M-TH-SA*

time Schedule object beginning/ending time.

<SCHED_TIME_BEGIN> Time in the form: DD:DD.
Example: *12:00*

<SCHED_TIME_END> Time in the form: DD:DD.
Example: *12:00*

name Schedule object name.

<SCHED_NAME> Schedule object name.
Example: *Work Hours*

Example

```
schedule always-on
```

Syntax

```
log-redundancy { filter <UINT16> | global }
```

Mode

Anti-spyware Product

Description

Set anti-spyware product log redundancy filter.

Options

filter Set log redundancy filter in seconds.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

global Use global setting.

Example

```
log-redundancy filter 45
```

Syntax

```
product <WORD>
```

Mode

Anti-spyware Policy

Description

Anti-spyware policy's product name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
product 123mania
```

Syntax

```
danger-level { high | low | medium }
```

Mode

Anti-spyware Policy

Description

Anti-spyware policy's danger level.

Options

high Anti-spyware policy high danger level.

low Anti-spyware policy low danger level.

medium Anti-spyware policy medium danger level.

Example

```
danger-level medium
```

Syntax

```
prevention [ enable | product ]
```

Mode

Anti-spyware Policy

Description

Set prevention for anti-spyware policy.

Options

enable Enable anti-spyware policy prevention.

product Use product setting.

Example

```
prevention product
```

Syntax

```
no prevention
```

Mode

Anti-spyware Policy

Description

Disable prevention for anti-spyware policy.

Example

```
no prevention
```

Syntax

```
detection [ enable | product ]
```

Mode

Anti-spyware Policy

Description

Set detection for anti-spyware policy.

Options

enable Enable anti-spyware policy detection.

product Use product setting.

Example

```
detection product
```

Syntax

```
no detection
```

Mode

Anti-spyware Policy

Description

Disable detection for anti-spyware policy.

Example

```
no detection
```

Syntax

```
included { ip { { { all | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> } } | product } } | users { { { administrator  
| all | group <LOCAL_USER_GROUP_NAME> | guests | name <USER_NAME> } } | product } } }
```

Mode

Anti-spyware Policy

Description

Set included users or IP address ranges.

Options

| | |
|---|--|
| ip | Set included IP address ranges. |
| all | All IP address ranges. |
| group <ADDR_GROUP_NAME_MIXED> | Group of IP address ranges. Group address object name. Example: <i>Sales Group</i> |
| name <ADDR_NAME_MIXED> | Name of IP address range. Address object name. Example: <i>Web Server</i> |
| product | Set included IP address ranges as product setting. |
| users | Set included users or groups. |
| administrator | Administrator. |
| all | All users and groups. |
| group <LOCAL_USER_GROUP_NAME> | Group of users. Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests users. |
| name <USER_NAME> | Name of users. User object name. Example: <i>user1</i> |
| product | Set included users as product setting. |

Example

```
included users all  
included users name user1  
included ip all  
included ip name aol
```

Syntax

```
excluded { ip { { { all | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> } } | product } } | users { { { administrator  
| all | group <LOCAL_USER_GROUP_NAME> | guests | name <USER_NAME> } } | product } } }
```


Mode

Anti-spyware Policy

Description

Set excluded users/groups or IP address ranges.

Options

| | |
|--------------------------------------|---|
| ip | Set excluded IP address ranges. |
| all | All IP address ranges. |
| group | Group of IP address ranges. |
| <ADDR_GROUP_NAME_MIXED> | Group address object name. Example: <i>Sales Group</i> |
| name | Name of IP address range. |
| <ADDR_NAME_MIXED> | Address object name. Example: <i>Web Server</i> |
| product | Set excluded IP address as product setting. |
| users | Set excluded users or groups. |
| administrator | Administrator. |
| all | All users and groups. |
| group | Group of users. |
| <LOCAL_USER_GROUP_NAME> | Local user group object name. Example: <i>Limited Administrators</i> |
| guests | Guests users. |
| name | Name of users. |
| <USER_NAME> | User object name. Example: <i>user1</i> |
| product | Set excluded users as product setting. |

Example

```
excluded users administrator  
excluded ip name aol
```

Syntax

```
no excluded { ip | users }
```

Mode

Anti-spyware Policy

Description

Set no excluded users or IP address.

Options

| | |
|--------------|-----------------------------|
| ip | Set no excluded IP address. |
| users | Set no excluded users. |

Example

no excluded users
no excluded ip

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> | product }
```

Mode

Anti-spyware Policy

Description

Set anti-spyware product schedule.

Options

| | |
|---------------------------------|---|
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |
| product | Use product setting. |

Example

```
schedule always-on
```

Syntax

```
log-redundancy { filter <UINT16> | product }
```

Mode

Anti-spyware Policy

Description

Set anti-spyware product log redundancy filter.

Options

| | |
|-----------------------|--|
| filter | Set log redundancy filter in seconds. |
| <UINT16> | Integer in the form: D OR 0xHHHH. Example: <i>123</i> |
| product | Use product setting. |

Example

```
log-redundancy filter 45
```

Syntax

```
show security-services [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show security services configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show security-services
```

Syntax

```
show dpi-ssh [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show DPI-SSH configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show dpi-ssh
```

Syntax

```
show content-filter [ action <CONTENT_FILTER_ACTION_NAME> | actions | cfs [ { custom-category [ { category-entries | category-entry <CFS_CUSTOM_CATEGORY_DOMAIN> } ] | policies | policy <CFS_POLICY_NAME> } ] | profile <CONTENT_FILTER_PROFILE_NAME> | profiles | uri-list-group <CONTENT_FILTER_URI_LIST_GRP_NAME> | uri-list-groups | uri-list-object <CONTENT_FILTER_URI_LIST_OBJ_NAME> | uri-list-objects | websense ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show content filter configuration and status.

Options

action Content filter action object.
<CONTENT_FILTER_ACTION_NAME> Content filter action object name.
Example: *Market action*

actions All content filter action objects.

cfs CFS configuration.

| | |
|---|---|
| custom-category | CFS custom category configuration. |
| category-entries | All CFS custom category entries. |
| category-entry | CFS custom category entry. |
| <CFS_CUSTOM_CATEGORY_DOMAIN> | CFS custom category domain. Example: <i>google.com</i> |
| policies | All CFS policies. |
| policy | CFS policy. |
| <CFS_POLICY_NAME> | CFS policy name. Example: <i>Market policy</i> |
| profile | Content filter profile object. |
| <CONTENT_FILTER_PROFILE_NAME> | Content filter profile object name. Example: <i>Market profile</i> |
| profiles | All content filter profile objects. |
| uri-list-group | Content filter URI list group. |
| <CONTENT_FILTER_URI_LIST_GRP_NAME> | Content filter URI list group name. Example: <i>White URI list group</i> |
| uri-list-groups | All content filter URI list groups. |
| uri-list-object | Content filter URI list object. |
| <CONTENT_FILTER_URI_LIST_OBJ_NAME> | Content filter URI list object name. Example: <i>White URI list object</i> |
| uri-list-objects | All content filter URI list objects. |
| websense | Websense. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show content-filter
```

Syntax

```
show anti-spam [ [ allow-list | reject-list ] [ { pending-config | with-pending-config } ] | statistics [ { capture | general | probe | threats } ] | status [ { monitoring | service } ] ]
```

Mode

All Modes

Description

Show anti-spam configuration and status.

Options

| | |
|----------------------------|---|
| allow-list | Show anti-spam allow client list. |
| reject-list | Show anti-spam reject client list. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| statistics | Show anti-spam statistics. |

| | |
|-------------------|---|
| capture | Show anti-spam packets capture statistics. |
| general | Show anti-spam general statistics. |
| probe | Show anti-spam monitoring probe statistics. |
| threats | Show anti-spam threats statistics. |
| status | Show anti-spam status. |
| monitoring | Show anti-spam monitoring status. |
| service | Show anti-spam service status. |

Example

```
show anti-spam
show anti-spam allow-list
show anti-spam reject-list
show anti-spam status
show anti-spam status monitoring
show anti-spam statistics probe
show anti-spam statistics
```

Syntax

```
show intrusion-prevention [ categories | category { id <IPS_CATEGORY_ID> | name <IPS_CATEGORY_NAME> } [ [ policies | policy { id <IPS_POLICY_ID> | name <IPS_POLICY_NAME> } ] ] | exclusion-list | global | policies | policy { id <IPS_POLICY_ID> | name <IPS_POLICY_NAME> } | status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show intrusion prevention configuration.

Options

| | |
|----------------------------------|---|
| categories | Show intrusion prevention categories. |
| category | Show intrusion prevention category. |
| id | Category ID. |
| <IPS_CATEGORY_ID> | Category ID. Example: 1234 |
| name | Category name. |
| <IPS_CATEGORY_NAME> | Category name. Example: ACTIVEX |
| policies | Show all policies of the specified IPS product. |
| policy | Show policy of the IPS category. |
| id | Show IPS policy by ID. |
| <IPS_POLICY_ID> | Policy ID. Example: 1234 |
| name | Show IPS policy by name. |
| <IPS_POLICY_NAME> | Policy name. Example: ActivePDF WebGrabber ActiveX Instantiation |
| exclusion-list | Show intrusion prevention exclusion list. |
| global | Show intrusion prevention global configuration. |

| | |
|---------------------------------------|--|
| <i>policies</i> | Show intrusion prevention policies. |
| <i>policy</i> | Show intrusion prevention policy. |
| <i>id</i> | Show IPS policy by ID. |
| <i><IPS_POLICY_ID></i> | Policy ID. Example: <i>1234</i> |
| <i>name</i> | Show IPS policy by name. |
| <i><IPS_POLICY_NAME></i> | Policy name. Example: <i>ActivePDF WebGrabber ActiveX Instantiation</i> |
| <i>status</i> | Show intrusion prevention status. |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |

Example

```
show intrusion-prevention
```

Syntax

```
show gateway-antivirus [ exclusion-list | signatures | status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show Gateway Anti-Virus configuration.

Options

| | |
|-----------------------------------|---|
| <i>exclusion-list</i> | Show Gateway Anti-Virus exclusion list. |
| <i>signatures</i> | Show Gateway Anti-Virus signatures. |
| <i>status</i> | Show Gateway Anti-Virus status. |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |

Example

```
show gateway-antivirus
```

Syntax

```
show capture-atp [ [ { pending-config | with-pending-config } ] | status ]
```

Mode

All Modes

Description

Show capture ATP configuration and status.

Options

| | |
|------------------------------|-------------------------------------|
| <i>pending-config</i> | Show pending configuration changes. |
|------------------------------|-------------------------------------|

with-pending-config View current configuration with pending changes included in the output.

status Show capture ATP status

Example

```
show capture-atp
```

Syntax

```
show match-objects [ status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all match objects.

Options

status Show match objects status.

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show match-objects
```

Syntax

```
show match-object <MATCH_OBJ_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show a match object.

Options

<MATCH_OBJ_NAME> Match object name.
Example: *Match FTP*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show match-object "Match FTP"
```

Syntax

```
show action-objects [ status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all action objects.

Options

- status*** Show action objects status.
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show action-objects
```

Syntax

```
show action-object <ACTION_OBJ_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show action object configuration.

Options

- <ACTION_OBJ_NAME>*** Action object name.
Example: *HTTP Block Page*
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show action-object CorpMailMessage
```

Syntax

```
show email-objects [ status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all e-mail address objects.

Options

- status*** Show e-mail user objects status.
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show email-objects
```

Syntax


```
show email-object <EMAIL_OBJ_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show an e-mail address Object.

Options

- <EMAIL_OBJ_NAME>** E-mail object name.
Example: *Marketing E-mail Object*
- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.

Example

```
show email-object "Client E-mail Addresses"
```

Syntax

```
show app-rules [ [ [ policies | policy <APP_RULES_POLICY_NAME> ] ] [ { pending-config | with-pending-config } ] | status ]
```

Mode

All Modes

Description

Show app rule configuration.

Options

- policies** Show app rule policies.
- policy** Show app rule policy configuration.
- <APP_RULES_POLICY_NAME>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.
- status** Show app rule status.

Example

```
show app-rules
```

Syntax

```
show app-control [ application { { id <AC_APP_ID> | name <AC_APP_NAME> } } [ [ signature { { id <AC_SIG_ID> | name <AC_SIG_NAME> } } | signatures ] ] | applications | categories | category { { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> } } [ [ application { { id <AC_APP_ID> | name <AC_APP_NAME> } } [ [ signature { { id <AC_SIG_ID> | name <AC_SIG_NAME> } } | signatures ] ] | applications ] ] | exclusion-list | signature { { id <AC_SIG_ID> | name <AC_SIG_NAME> } } | signatures | status ] [ { custom | default } ] [ { pending-config | with-pending-config } ] ]
```

Mode

All Modes

Description

Show app control configuration.

Options

| | |
|---------------------------------|---|
| application | Show app control application. |
| id | Application ID. |
| <AC_APP_ID> | Application ID. Example: 123 |
| name | Application name. |
| <AC_APP_NAME> | Application name. Example: APP-UPDATE |
| signature | Show app control signature of the specified application. |
| id | Signature ID. |
| <AC_SIG_ID> | Signature ID. Example: 123 |
| name | Signature name. |
| <AC_SIG_NAME> | Signature name. |
| signatures | Show app control signatures of the specified application. |
| applications | Show app control applications. |
| categories | Show app control categories. |
| category | Show app control category. |
| id | Category ID. |
| <AC_CATEGORY_ID> | Category ID. Example: 123 |
| name | Category name. |
| <AC_CATEGORY_NAME> | Category name. Example: APP-UPDATE |
| application | Show app control application of the specified category. |
| id | Application ID. |
| <AC_APP_ID> | Application ID. Example: 123 |
| name | Application name. |
| <AC_APP_NAME> | Application name. Example: APP-UPDATE |
| signature | Show app control signature of the specified application. |
| id | Signature ID. |
| <AC_SIG_ID> | Signature ID. Example: 123 |
| name | Signature name. |
| <AC_SIG_NAME> | Signature name. |
| signatures | Show app control signatures of the specified application. |
| applications | Show app control applications of the specified category. |
| exclusion-list | Show app control exclusion list. |
| signature | Show app control signature. |
| id | Signature ID. |
| <AC_SIG_ID> | Signature ID. Example: 123 |

| | |
|-----------------------------------|---|
| <i>name</i> | Signature name. |
| <i><AC_SIG_NAME></i> | Signature name. |
| <i>signatures</i> | Show app control signatures. |
| <i>status</i> | Show app control status. |
| <i>custom</i> | Show custom configuration. |
| <i>default</i> | Show system/factory default configuration. |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |

Example

```
show app-control
```

Syntax

```
show rbl [ blacklist | service <RBL_SERVICE_NAME> | services | statistics | whitelist ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show Real-Time Blacklist configuration.

Options

| | |
|--|---|
| <i>blacklist</i> | Show RBL blacklist. |
| <i>service</i> | Show Real-Time Blacklist service. |
| <i><RBL_SERVICE_NAME></i> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>services</i> | Show Real-Time Blacklist services. |
| <i>statistics</i> | Show Real-Time Blacklist service statistics. |
| <i>whitelist</i> | Show RBL whitelist. |
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |

Example

```
show rbl
```

Syntax

```
show dpi-ssl [ client | server ] [ [ { pending-config | with-pending-config } ] ] | connection-failures ]
```

Mode

All Modes

Description

Show DPI-SSL configuration and status.

Options

| | |
|----------------------------|---|
| client | Show client DPI-SSL configuration. |
| server | Show server DPI-SSL configuration. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| connection-failures | Show client DPI-SSL connection failures list. |

Example

```
show dpi-ssl
show dpi-ssl client
show dpi-ssl server
show dpi-ssl client connection-failures
```

Syntax

```
show client-enforcement anti-virus [ list | policy | status ]
```

Mode

All Modes

Description

Show client anti-virus enforcement configuration.

Options

| | |
|---------------|--|
| list | Show client anti-virus enforcement exclusion/inclusion list. |
| policy | Show client anti-virus enforcement policy settings. |
| status | Show client anti-virus enforcement license status. |

Example

```
show client-enforcement anti-virus policy
show client-enforcement anti-virus list
show client-enforcement anti-virus status
```

Syntax

```
show client-enforcement content-filtering [ exclusion | list ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show client cfs enforcement configuration.

Options

| | |
|-----------------------|---|
| exclusion | Show client cfs enforcement exclusion list. |
| list | Show client cfs enforcement list. |
| pending-config | Show pending configuration changes. |

with-pending-config View current configuration with pending changes included in the output.

Example

```
show client-enforcement content-filtering list
show client-enforcement content-filtering exclusion
show client-enforcement content-filtering
```

Syntax

```
show geo-ip [ [ { pending-config | with-pending-config } ] | cache-statistics | resolved-locations | status ]
```

Mode

All Modes

Description

Show Geo-IP configuration.

Options

| | |
|-----------------------------------|---|
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |
| <i>cache-statistics</i> | Show Geo-IP cache statistics. |
| <i>resolved-locations</i> | Show Geo-IP resolved locations. |
| <i>status</i> | Show Geo-IP database status. |

Example

```
show geo-ip
show geo-ip status
show geo-ip cache-statistics
show geo-ip resolved-locations
```

Syntax

```
show botnet [ [ { pending-config | with-pending-config } ] | cache-statistics | resolved-locations | status ]
```

Mode

All Modes

Description

Show Botnet configuration.

Options

| | |
|-----------------------------------|---|
| <i>pending-config</i> | Show pending configuration changes. |
| <i>with-pending-config</i> | View current configuration with pending changes included in the output. |
| <i>cache-statistics</i> | Show Botnet cache statistics. |
| <i>resolved-locations</i> | Show Botnet resolved locations. |
| <i>status</i> | Show Botnet database status. |

Example

```
show botnet
show botnet status
show botnet cache-statistics
show botnet resolved-locations
```

Syntax

```
show anti-spyware [ [ exclusion-list | global | policies | policy id <ANTI_SPYWARE_POLICY_ID> | product { id
<ANTI_SPYWARE_PRODUCT_ID> | name <ANTI_SPYWARE_PRODUCT_NAME> } [ [ policies | policy id <ANTI_SPYWARE_POLICY_ID> ] ] | products ]
[ { pending-config | with-pending-config } ] | status ]
```

Mode

All Modes

Description

Show anti-spyware configuration or status.

Options

| | |
|--|---|
| exclusion-list | Show anti-spyware exclusion list. |
| global | Show anti-spyware global configuration. |
| policies | Show all anti-spyware policies. |
| policy | Show anti-spyware policy. |
| id | Show anti-spyware policy by ID. |
| <ANTI_SPYWARE_POLICY_ID> | The policy ID of the specified anti-spyware product. Example: <i>123</i> |
| product | Show anti-spyware product. |
| id | Show anti-spyware product by id. |
| <ANTI_SPYWARE_PRODUCT_ID> | The ID of anti-spyware product. Example: <i>123</i> |
| name | Show anti-spyware product by name. |
| <ANTI_SPYWARE_PRODUCT_NAME> | The name of anti-spyware product. Example: <i>abc</i> |
| policies | Show all policies of the specified anti-spyware product. |
| policy | Show policy of the anti-spyware product. |
| id | Show anti-spyware policy by ID. |
| <ANTI_SPYWARE_POLICY_ID> | The policy ID of the specified anti-spyware product. Example: <i>123</i> |
| products | Show anti-spyware products. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |
| status | Show anti-spyware status. |

Example

```
show anti-spyware
```

Syntax

sonicpoint

Mode

Config

Description

Enter SonicPoint configuration mode.

Example

sonicpoint

Syntax

synchronize

Mode

SonicPoint

Description

Synchronize SonicPoints and SonicPointNs.

Example

synchronize

Syntax

reboot { sonicpoint [ac | n | ndr | wave2] <SONICPOINT_N_NAME> | sonicpoints } [factory-default]

Mode

SonicPoint

Description

Reboot specified SonicPoint or all SonicPoints.

Options

| | |
|---|--|
| <i>sonicpoint</i> | Specify SonicPoint. |
| <i>ac</i> | SonicPoint ACe/ACi/N2/W2. |
| <i>n</i> | SonicPoint N. |
| <i>ndr</i> | SonicPoint NDR. |
| <i>wave2</i> | SonicPoint ACWave2 |
| <i><SONICPOINT_N_NAME></i> | SonicPointN name. Example: <i>mySonicpointn</i> |
| <i>sonicpoints</i> | Reboot all SonicPoints. |
| <i>factory-default</i> | Reboot to factory default. |

Example

reboot sonicpoint "SonicPointN 2e57e"

Syntax

no sonicpoint [ac | n | ndr | wave2] <SONICPOINT_N_NAME>

Mode

SonicPoint

Description

Delete or disable the specified SonicPoint.

Options

| | |
|----------------------------------|--|
| ac | SonicPoint ACe/ACi/N2/W2. |
| n | SonicPoint N. |
| ndr | SonicPoint NDR. |
| wave2 | SonicPoint ACWave2 |
| <SONICPOINT_N_NAME> | SonicPointN name. Example: <i>mySonicpointn</i> |

Example

```
no sonicpoint n "SonicPointN 2e57e"  
no sonicpoint "SonicPointN 2e57e"
```

Syntax

```
no profile [ ac | n | ndr | wave2 ] <SONICPOINT_N_PROFILE_NAME>
```

Mode

SonicPoint

Description

Delete SonicPoint provisioning profile.

Options

| | |
|--|--|
| ac | SonicPoint ACe/ACi/N2/W2. |
| n | SonicPoint N. |
| ndr | SonicPoint NDR. |
| wave2 | SonicPoint ACWave2 profile. |
| <SONICPOINT_N_PROFILE_NAME> | SonicPointN provisioning profile name. Example: <i>mySonicpointnProfile</i> |

Example

```
no profile n CorpSonic  
no profile CorpSonic
```

Syntax

```
no sonicpoints [ { ac | n | ndr | wave2 } ]
```

Mode

SonicPoint

Description

Delete all SonicPoints.

Options

ac SonicPoint ACe/ACi/N2/W2.

n SonicPoint N.

ndr SonicPoint NDR.

wave2 SonicPoint ACWave2.

Example

```
no sonicpoints
no sonicpoints n
```

Syntax

```
no profiles [ { ac | n | ndr | wave2 } ]
```

Mode

SonicPoint

Description

Delete all SonicPoint provisioning profiles.

Options

ac SonicPoint ACe/ACi/N2/W2.

n SonicPoint N.

ndr SonicPoint NDR.

wave2 SonicPoint ACWave2.

Example

```
no profiles
no profiles n
```

Syntax

```
sonicpoint { ac | n | ndr | wave2 } <SONICPOINT_N_NAME>
```

Mode

SonicPoint

Description

Edit SonicPoint and enter its configuration mode.

Options

ac SonicPoint ACe/ACi/N2/W2.

n SonicPoint N.

ndr SonicPoint NDR.

wave2 SonicPoint ACWave2.

<SONICPOINT_N_NAME> SonicPointN name.
Example: *mySonicpointn*

Example

```
sonicpoint n "SonicPointN 2e57e"
```

Syntax

```
profile { ac | n | ndr | wave2 } <SONICPOINT_N_PROFILE_NAME>
```

Mode

SonicPoint

Description

Add/edit SonicPoint provisioning profile and enter its configuration mode.

Options

| | |
|--|--|
| ac | SonicPoint ACe/ACi/N2/W2. |
| n | SonicPoint N. |
| ndr | SonicPoint NDR. |
| wave2 | SonicPoint ACWave2. |
| <SONICPOINT_N_PROFILE_NAME> | SonicPointN provisioning profile name. Example: <i>mySonicpointnProfile</i> |

Example

```
profile n CorpSonic
```

Syntax

```
enable
```

Mode

SonicPointN

Description

Enable SonicPointN.

Example

```
enable
```

Syntax

```
no enable
```

Mode

SonicPointN

Description

Disable SonicPointN.

Example

```
no enable
```

Syntax

rf-monitoring

Mode

SonicPointN

Description

Enable RF monitoring.

Example

rf-monitoring

Syntax

no rf-monitoring

Mode

SonicPointN

Description

Disable RF monitoring.

Example

no rf-monitoring

Syntax

poe-out

Mode

SonicPointN

Description

Enable POE out.

Example

poe-out

Syntax

no poe-out

Mode

SonicPointN

Description

Disable POE out.

Example

no poe-out

Syntax

low-power

Mode

SonicPointN

Description

Enable low power mode.

Example

```
low-power
```

Syntax

```
no low-power
```

Mode

SonicPointN

Description

Disable low power mode.

Example

```
no low-power
```

Syntax

```
retain [ all | led | radio [ 2400mhz | 5000mhz | single-radio ] [ { access-list | advanced | radio-settings | virtual-access-point | wireless-security } ] | retain | rf-monitoring | sonicpoint [ { ip | name-and-country-code } ] | widp-sensor ]
```

Mode

SonicPointN

Description

Enable retain settings.

Options

| | |
|-----------------------------|---------------------------------------|
| all | Retain all settings. |
| led | Retain enable LED(Ni/Ne only). |
| radio | Retain radio settings. |
| 2400mhz | Retain 2.4GHz radio settings. |
| 5000mhz | Retain 5GHz radio settings. |
| single-radio | Retain radio settings. |
| access-list | Retain access list enforcement. |
| advanced | Retain advanced radio settings. |
| radio-settings | Retain radio settings. |
| virtual-access-point | Retain virtual access point settings. |
| wireless-security | Retain wireless security settings. |
| retain | Retain enable retain settings |

| | |
|-------------------------------------|--|
| <i>rf-monitoring</i> | Retain enable RF monitoring. |
| <i>sonicpoint</i> | Retain enable SonicPoint. |
| <i>ip</i> | Retain SonicPoint IP information. |
| <i>name-and-country-code</i> | Retain SonicPoint name and country code. |
| <i>widp-sensor</i> | Retain DIDP sensor. |

Example

```
retain all
retain retain
retain sonicpoint
retain sonicpoint name-and-country-code
retain radio
retain radio advanced
```

Syntax

```
no retain [ all | led | radio [ 2400mhz | 5000mhz | single-radio ] [ { access-list | advanced | radio-settings | virtual-access-point | wireless-security } ] ] | retain | rf-monitoring | sonicpoint [ { ip | name-and-country-code } ] | widp-sensor ]
```

Mode

SonicPointN

Description

Disable SonicPointN retain settings.

Options

| | |
|-------------------------------------|--|
| <i>all</i> | Retain all settings. |
| <i>led</i> | Retain enable LED(Ni/Ne only). |
| <i>radio</i> | Retain radio settings. |
| <i>2400mhz</i> | Retain 2.4GHz radio settings. |
| <i>5000mhz</i> | Retain 5GHz radio settings. |
| <i>single-radio</i> | Retain radio settings. |
| <i>access-list</i> | Retain access list enforcement. |
| <i>advanced</i> | Retain advanced radio settings. |
| <i>radio-settings</i> | Retain radio settings. |
| <i>virtual-access-point</i> | Retain virtual access point settings. |
| <i>wireless-security</i> | Retain wireless security settings. |
| <i>retain</i> | Retain enable retain settings |
| <i>rf-monitoring</i> | Retain enable RF monitoring. |
| <i>sonicpoint</i> | Retain enable SonicPoint. |
| <i>ip</i> | Retain SonicPoint IP information. |
| <i>name-and-country-code</i> | Retain SonicPoint name and country code. |
| <i>widp-sensor</i> | Retain DIDP sensor. |

Example

```
no retain
no retain retain
no retain sonicpoint
no retain sonicpoint name-and-country-code
no retain radio
no retain radio advanced
```

Syntax

```
led
```

Mode

SonicPointN

Description

Enable SonicPointN LED.

Example

```
led
```

Syntax

```
no led
```

Mode

SonicPointN

Description

Disable SonicPointN LED.

Example

```
no led
```

Syntax

```
name-prefix <WORD>
```

Mode

SonicPointN

Description

Set provisioning profile name prefix.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
name-prefix CorpSonicPointN
```

Syntax

```
name <WORD>
```

Mode

SonicPointN

Description

Set SonicPointN name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name CorpSonicPointN-1234
```

Syntax

```
country-code <SONICPOINT_N_COUNTRY_CODE>
```

Mode

SonicPointN

Description

Set SonicPointN country code.

Options

<SONICPOINT_N_COUNTRY_CODE> SonicPointN country code.
Example: *United States*

Example

```
country-code "United States"
```

Syntax

```
eapol-version { v1 | v2 }
```

Mode

SonicPointN

Description

Set EAPOL version (v2 provides better security).

Options

v1 Version 1.

v2 Version 2.

Example

```
eapol-version v2
```

Syntax

```
band-steering { auto | force-5ghz | prefer-5ghz }
```

Mode

SonicPointN

Description

Set band steering.

Options

- auto** Auto.
- force-5ghz** Force 5GHz.
- prefer-5ghz** Prefer 5GHz.

Example

```
band-steering auto
```

Syntax

```
no band-steering
```

Mode

SonicPointN

Description

Disable band steering.

Example

```
no band-steering
```

Syntax

```
sslvpn { auto-reconnect | domain <HOSTNAME_MIXED> | password <ENC_PASSWORD> | server <WORD> | user-name <WORD> }
```

Mode

SonicPointN

Description

Set SonicPoint L3 SSLVPN tunnel.

Options

- auto-reconnect** Enable SonicPoint L3 SSLVPN tunnel auto reconnect.
- domain** Set SonicPoint L3 SSLVPN tunnel user domain.
<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: `2001:cdba:0000:0000:0000:0000:3257:9652\n`
- password** Set SonicPoint L3 SSLVPN tunnel user password.
<ENC_PASSWORD> Password.
Example: `secret`
- server** Set SonicPoint L3 SSLVPN tunnel server.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: `abc`
- user-name** Set SonicPoint L3 SSLVPN tunnel user name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: `abc`

Example


```
sslvpn server 172.168.12.4
sslvpn user-name jshone
sslvpn password password
sslvpn domain mySonicPoint.com
sslvpn auto-reconnect
```

Syntax

```
no sslvpn { auto-reconnect | domain | password | server | user-name }
```

Mode

SonicPointN

Description

Clear SonicPoint L3 SSLVPN tunnel settings.

Options

| | |
|-----------------------|---|
| auto-reconnect | Disable SonicPoint L3 SSLVPN tunnel auto reconnect. |
| domain | Clear SonicPoint L3 SSLVPN tunnel user domain. |
| password | Clear SonicPoint L3 SSLVPN tunnel user password. |
| server | Clear SonicPoint L3 SSLVPN tunnel server. |
| user-name | Clear SonicPoint L3 SSLVPN tunnel user name. |

Example

```
no sslvpn server
no sslvpn user-name
no sslvpn password
no sslvpn domain
no sslvpn auto-reconnect
```

Syntax

```
radius { accounting { server1 | server2 } { { ip <IPV4_HOST> | port <IPV4_PORT> | secret <ENC_PASSWORD> } } | nas { { identifier { sonicpoint-mac-address | sonicpoint-name | sonicpoint-ssid } | ip <IPV4_HOST> } } | retries <UINT8> | retry-interval <UINT8> | server { server1 | server2 } { { ip <IPV4_HOST> | port <IPV4_PORT> | secret <ENC_PASSWORD> } } }
```

Mode

SonicPointN

Description

Set radius server for SonicPoint radio.

Options

| | |
|---|--|
| accounting | Set radius accounting server. |
| server1 | Radius accounting server 1. |
| server2 | Radius accounting server 2. |
| ip <IPV4_HOST> | Radius accounting server IP. IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| port <IPV4_PORT> | Radius accounting server port. Integer in the form: D OR 0xHHHH. Example: 80 |

| | |
|-------------------------------|---|
| secret | Radius accounting server secret. |
| <ENC_PASSWORD> | Password. Example: <i>secret</i> |
| nas | Nas settings to radius server. |
| identifier | Nas identifier to radius server. |
| sonicpoint-mac-address | SonicPoint's MAC address. |
| sonicpoint-name | SonicPoint's name. |
| sonicpoint-ssid | SonicPoint's SSID. |
| ip | Nas IP to radius server. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |
| retries | Set radius server retries. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| retry-interval | Set radius server retry interval (seconds). |
| <UINT8> | Integer in the form: D OR 0xHH. Example: <i>123</i> |
| server | Set radius server. |
| server1 | Radius server 1. |
| server2 | Radius server 2. |
| ip | Radius server IP. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |
| port | Radius server port. |
| <IPV4_PORT> | Integer in the form: D OR 0xHHHH. Example: <i>80</i> |
| secret | Radius server secret. |
| <ENC_PASSWORD> | Password. Example: <i>secret</i> |

Example

```
radius retries 1
radius retry-interval 20
radius server server1 ip 192.168.168.1
radius server server1 port 1812
radius server server1 secret radsecret
radius server server2 ip 192.168.168.2
radius server server2 port 1812
radius server server2 secret radsecret2
radius accounting server1 ip 192.168.168.1
radius accounting server1 port 1812
radius accounting server1 secret radsecret
radius accounting server2 ip 192.168.168.2
radius accounting server2 port 1812
radius accounting server2 secret radsecret2
radius nas identifier sonicpoint-name
radius nas identifier sonicpoint-mac-address
radius nas ip 192.168.168.1
```

Syntax

```
no radius { accounting { server1 | server2 } { { ip | port | secret } } | nas { identifier | ip } | retries | retry-interval |
server { server1 | server2 } { { ip | port | secret } } }
```

Mode

SonicPointN

Description

Clear radius server settings for SonicPoint radio.

Options

| | |
|------------------------------|---|
| <i>accounting</i> | Clear radius accounting server settings. |
| <i>server1</i> | Clear radius accounting server 1 settings. |
| <i>server2</i> | Clear radius accounting server 2 settings. |
| <i>ip</i> | Clear radius accounting server IP. |
| <i>port</i> | Clear radius accounting server port. |
| <i>secret</i> | Clear radius accounting server secret. |
| <i>nas</i> | Clear nas settings to radius server. |
| <i>identifier</i> | Nas identifier to radius server not included. |
| <i>ip</i> | Clear nas IP to radius server. |
| <i>retries</i> | Clear radius server retries. |
| <i>retry-interval</i> | Clear radius server retry interval. |
| <i>server</i> | Clear radius server settings. |
| <i>server1</i> | Clear radius server 1 settings. |
| <i>server2</i> | Clear radius server 2 settings. |
| <i>ip</i> | Clear radius server IP. |
| <i>port</i> | Clear radius server port. |
| <i>secret</i> | Clear radius server secret. |

Example

```
no radius retries
no radius retry-interval
no radius server server1 ip
no radius server server1 port
no radius server server1 secret
no radius server server2 ip
no radius server server2 port
no radius server server2 secret
no radius accounting server1 ip
no radius accounting server1 port
no radius accounting server1 secret
no radius accounting server2 ip
no radius accounting server2 port
no radius accounting server2 secret
no radius nas identifier
no radius nas ip
```

Syntax

```
administrator { name <WORD> | password <ENC_PASSWORD> }
```

Mode

SonicPointN

Description

Set SonicPoint administrator name or password.

Options

| | |
|------------------------------------|---|
| <i>name</i> | Set SonicPoint administrator name. |
| <i><WORD></i> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| <i>password</i> | Set SonicPoint administrator password. |
| <i><ENC_PASSWORD></i> | Password. Example: <i>secret</i> |

Example

```
administrator name admin
administrator password password
```

Syntax

```
no administrator { name | password }
```

Mode

SonicPointN

Description

Clear SonicPoint administrator name or password.

Options

| | |
|------------------------|--|
| <i>name</i> | Clear SonicPoint administrator name. |
| <i>password</i> | Clear SonicPoint administrator password. |

Example

```
no administrator name
no administrator password
```

Syntax

```
widp-sensor schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

SonicPointN

Description

Enable WIDP sensor and set WIDP sensor schedule.

Options

| | |
|--|---|
| <i>schedule</i> | Set WIDP sensor schedule. |
| <i>always-on</i> | Always on. |
| <i>days</i> | Schedule object days. |
| <i><SCHED_DAYS></i> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| <i>time</i> | Schedule object beginning/ending time. |
| <i><SCHED_TIME_BEGIN></i> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <i><SCHED_TIME_END></i> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <i>name</i> | Schedule object name. |
| <i><SCHED_NAME></i> | Schedule object name. |

Example

```
widp-sensor schedule name "Work Hours"
```

Syntax

```
no widp-sensor
```

Mode

SonicPointN

Description

Disable WIDP sensor.

Example

```
no widp-sensor
```

Syntax

```
wwan [ bound-to <SONICPOINT_WWAN_VLAN_INTERFACE> ]
```

Mode

SonicPointN

Description

Set SonicPoint 3G/4G WWAN.

Options

| | |
|---|--|
| bound-to | Set SonicPoint 3G/4G WWAN bound to WAN VLAN interface. |
| <SONICPOINT_WWAN_VLAN_INTERFACE> | SonicPoint WWAN VLAN interface name. Example: <i>X2:253</i> |

Example

```
wwan  
wwan bound-to X2:V33
```

Syntax

```
no wwan [ bound-to ]
```

Mode

SonicPointN

Description

Set SonicPoint 3G/4G WWAN.

Options

bound-to clear SonicPoint 3G/4G WWAN bound to WAN VLAN interface.

Example

```
no wwan  
no wwan bound-to
```

Syntax

```
mesh { 2400mhz | 5000mhz } [ enable | psk <ENC_PASSWORD> | rssi-threshold <INT16> | ssid <WORD> ]
```

Mode

SonicPointN

Description

Set sonicwave MESH network.

Options

| | |
|-----------------------------|---|
| 2400mhz | Set sonicwave MESH in radio 2.4GHz. |
| 5000mhz | Set sonicwave MESH in radio 5GHz. |
| enable | Enable sonicwave MESH |
| psk | Set sonicwave MESH psk. |
| <ENC_PASSWORD> | Password. Example: <i>secret</i> |
| rssi-threshold | Set sonicwave MESH rssi-threshold. |
| <INT16> | Integer in the form: D OR 0xHHHH. Example: <i>123</i> |
| ssid | Set sonicwave MESH ssid. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

Example

```
mesh 2400mhz
mesh 2400mhz ssid SonicWave_Mesh
mesh 2400mhz psk password
mesh 2400mhz rssi-threshold -80
```

Syntax

```
no mesh { 2400mhz | 5000mhz } [ enable | psk | ssid ]
```

Mode

SonicPointN

Description

Clear sonicwave MESH network.

Options

| | |
|----------------|---|
| 2400mhz | Disable sonicwave MESH in radio 2.4GHz. |
| 5000mhz | Disable sonicwave MESH in radio 5GHz. |
| enable | Disable sonicwave MESH. |
| psk | Clear sonicwave MESH psk. |
| ssid | Clear sonicwave MESH ssid. |

Example

```
no mesh 2400mhz
no mesh 2400mhz ssid
no mesh 2400mhz psk
```

Syntax

```
ble { advertisement | ibeacon [ major <UINT16> | minor <UINT16> | uuid <SONICPOINT_BLE_IBEACON_UUID> ] }
```

Mode

SonicPointN

Description

Set SonicWave Bluetooth Low Energy.

Options

| | |
|--|---|
| advertisement | Enable SonicWave Bluetooth Advertisement. |
| ibeacon | Enable SonicWave Bluetooth Low Energy iBeacon. |
| major <UINT16> | Set SonicWave BLE iBeacon major. Integer in the form: D OR 0xHHHH. Example: 123 |
| minor <UINT16> | Set SonicWave BLE iBeacon minor. Integer in the form: D OR 0xHHHH. Example: 123 |
| uuid <SONICPOINT_BLE_IBEACON_UUID> | Set SonicWave BLE iBeacon UUID. SonicWave BLE iBeacon UUID. Example: 51b9d455-6a32-426c-b5cc-524181c24df3 |

Example

```
ble advertisement
ble ibeacon
ble ibeacon uuid 51b9d455-6a32-426c-b5cc-524181c24df3
ble ibeacon major 4
ble ibeacon minor 3
```

Syntax

```
no ble { advertisement | ibeacon [ major | minor | uuid ] }
```

Mode

SonicPointN

Description

Disable SonicWave Bluetooth Low Energy.

Options

| | |
|----------------------|--------------------------------------|
| advertisement | Disable SonicWave BLE Advertisement. |
| ibeacon | Disable SonicWave BLE iBeacon. |
| major | Clear SonicWave BLE iBeacon major. |
| minor | Clear SonicWave BLE iBeacon minor. |
| uuid | Clear SonicWave BLE iBeacon UUID. |

Example

```
no ble ibeacon
```

Syntax

packet-capture

Mode

SonicPointN

Description

Configuration SonicPoint packet capture and enter its configuration mode.

Example

packet-capture

Syntax

```
mode { 2400mhz { { ngb-mixed } } | 5000mhz { { ac-na-mixed | na-mixed } } }
```

Mode

Capture Radio

Description

Set the capture radio mode.

Options

| | |
|--------------------|---------------------------|
| 2400mhz | 2.4GHz. |
| ngb-mixed | 2.4GHz 802.11n/b/g mixed. |
| 5000mhz | 5GHz. |
| ac-na-mixed | 5GHz 802.11ac/n/a mixed. |
| na-mixed | 5GHz 802.11n/a mixed. |

Example

```
mode 2400mhz ngb-mixed  
mode 5000mhz na-mixed
```

Syntax

```
band { 20 | 40 | 80 }
```

Mode

Capture Radio

Description

Set the capture radio band.

Options

| | |
|-----------|---------------------------|
| 20 | Standard - 20mhz channel. |
| 40 | Wide - 40mhz channel. |
| 80 | Wide - 80mhz channel. |

Example

```
band 20
```

Syntax

```
channel { primary <SONICPOINT_N_CAPTURE_CHANNEL> | secondary <SONICPOINT_N_CAPTURE_CHANNEL> | standard <SONICPOINT_N_CAPTURE_CHANNEL> }
```

Mode

Capture Radio

Description

Set the capture radio channel.

Options

| | |
|---|--|
| primary | Set the radio primary channel. |
| <SONICPOINT_N_CAPTURE_CHANNEL> | SonicPointN capture channel. Example: 6 |
| secondary | Set the radio secondary channel. |
| <SONICPOINT_N_CAPTURE_CHANNEL> | SonicPointN capture channel. Example: 6 |
| standard | Set the radio standard channel. |
| <SONICPOINT_N_CAPTURE_CHANNEL> | SonicPointN capture channel. Example: 6 |

Example

```
channel auto
```

Syntax

```
capture [ bidirectional | exclude [ { beacon | control | data | probe [ { request | response } ] } ] | packet-capture | wrap-buffer ]
```

Mode

Capture Radio

Description

Enable capture settings.

Options

| | |
|-----------------------|--|
| bidirectional | Enable bidirectional address matching. |
| exclude | EXCLUDE. |
| beacon | Exclude beacon. |
| control | Exclude control. |
| data | Exclude data. |
| probe | PROBE. |
| request | Exclude probe request. |
| response | Exclude probe response. |
| packet-capture | Enable packet capture. |
| wrap-buffer | Wrap capture buffer once full. |

Example

```
capture wrap-buffer
capture bidirectional
capture exclude beacon
capture exclude probe request
capture exclude probe response
capture exclude control
capture exclude data
```

Syntax

```
no capture [ bidirectional | exclude [ { beacon | control | data | probe [ { request | response } ] ] ] | packet-capture | wrap-buffer ]
```

Mode

Capture Radio

Description

Disable capture settings.

Options

| | |
|------------------------------|--|
| <i>bidirectional</i> | Enable bidirectional address matching. |
| <i>exclude</i> | EXCLUDE. |
| <i>beacon</i> | Exclude beacon. |
| <i>control</i> | Exclude control. |
| <i>data</i> | Exclude data. |
| <i>probe</i> | PROBE. |
| <i>request</i> | Exclude probe request. |
| <i>response</i> | Exclude probe response. |
| <i>packet-capture</i> | Enable packet capture. |
| <i>wrap-buffer</i> | Wrap capture buffer once full. |

Example

```
no capture
no capture wrap-buffer
no capture bidirectional
no capture exclude beacon
no capture exclude probe request
no capture exclude probe response
no capture exclude control
no capture exclude data
```

Syntax

```
ssid <WORD>
```

Mode

Capture Radio

Description

Set the capture ESSID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ssid sonicwall
```

Syntax

```
no ssid
```

Mode

Capture Radio

Description

Clear capture ESSID.

Example

```
no ssid
```

Syntax

```
bssid <ADDR_MAC>
```

Mode

Capture Radio

Description

Set the capture BSSID.

Options

<ADDR_MAC> Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.

Example

```
bssid 18:b1:69:4d:28:c0
```

Syntax

```
no bssid
```

Mode

Capture Radio

Description

Clear capture BSSID.

Example

```
no bssid
```

Syntax

```
mac { destination <SONICPOINT_CAPTURE_MAC> | source <SONICPOINT_CAPTURE_MAC> }
```

Mode

Capture Radio

Description

Set the capture source or destination MAC address(es).

Options

destination Set the capture destination MAC address(es).
<SONICPOINT_CAPTURE_MAC> SonicPoint capture filter MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.\n You can enter up to five MAC at most with separated by commas or space.

source Set the capture source MAC address(es).
<SONICPOINT_CAPTURE_MAC> SonicPoint capture filter MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.\n You can enter up to five MAC at most with separated by commas or space.

Example

```
mac source 18:b1:69:4d:28:c0,c0:ea:e4:a7:57:c4
```

Syntax

```
no mac { destination | source }
```

Mode

Capture Radio

Description

Clear capture source or destination MAC address(es).

Options

destination Clear the capture destination MAC address(es).

source Clear the capture source MAC address(es).

Example

```
no mac source
```

Syntax

```
radio
```

Mode

SonicPointN

Description

Configuration SonicPoint radio and enter its configuration mode.

Example

```
radio
```

Syntax

```
radio-2400mhz
```

Mode

SonicPointN

Description

Configuration SonicPoint radio 2.4GHz and enter its configuration mode.

Example

```
radio-2400mhz
```

Syntax

```
radio-5000mhz
```

Mode

SonicPointN

Description

Configuration SonicPoint radio 5GHz and enter its configuration mode.

Example

```
radio-5000mhz
```

Syntax

```
virtual-access-point group <VAP_GROUP>
```

Mode

Radio N
Radio 2.4GHz

Description

Set virtual access point group name.

Options

<VAP_GROUP> VAP group name in the form: WORD or \"QUOTED STRING\".
Example: vapGroup

Example

```
virtual-access-point group CorpAccess
```

Syntax

```
no virtual-access-point group
```

Mode

Radio N
Radio 2.4GHz

Description

Clear virtual access point group name.

Example

```
no virtual-access-point group
```

Syntax

```
dynamic-vlan
```

Mode

Radio N
Radio 2.4GHz

Description

Enable SonicPoint dynamic vlan assignment id for radio.

Example

```
dynamic-vlan
```

Syntax

```
no dynamic-vlan
```

Mode

Radio N
Radio 2.4GHz

Description

Disable SonicPoint dynamic vlan assignment id for radio.

Example

```
no dynamic-vlan
```

Syntax

```
vlan <VAP_VLAN_ID>
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicPoint dynamic VLAN ID.

Options

<VAP_VLAN_ID> VLAN ID.
Example: 100

Example

```
vlan 4
```

Syntax

```
no vlan <VAP_VLAN_ID>
```

Mode

Radio N
Radio 2.4GHz

Description

Clear SonicPoint dynamic VLAN ID.

Options

<VAP_VLAN_ID> VLAN ID.
Example: 100

Example

```
no vlan 4
```

Syntax

```
no vlans
```

Mode

Radio N
Radio 2.4GHz

Description

Clear SonicPoint dynamic VLAN IDs.

Example

```
no vlans
```

Syntax

```
enable
```

Mode

Radio N
Radio 2.4GHz

Description

Enable SonicPoint radio.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Radio N
Radio 2.4GHz

Description

Disable SonicPoint radio.

Example

```
no enable
```

Syntax

```
schedule [ always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> ]
```

Mode

Radio N
Radio 2.4GHz

Description

Set schedule for radio.

Options

| | |
|---------------------------------|---|
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule name "Work Hours"
```

Syntax

```
mode { 5000mhz { { a-only | ac-na-mixed | ac-only | n-only | na-mixed } } | g-only | n-only | ngb-mixed }
```

Mode

Radio N
Radio 2.4GHz

Description

Set the radio mode.

Options

| | |
|--------------------|---------------------------|
| 5000mhz | 5GHz. |
| a-only | 5GHz 802.11a only. |
| ac-na-mixed | 5GHz 802.11ac/n/a mixed. |
| ac-only | 5GHz 802.11ac only. |
| n-only | 5GHz 802.11n only. |
| na-mixed | 5GHz 802.11n/a mixed. |
| g-only | 2.4GHz 802.11g only. |
| n-only | 2.4GHz 802.11n only. |
| ngb-mixed | 2.4GHz 802.11n/b/g mixed. |

Example

```
mode ngb-mixed
mode 5000mhz na-mixed
```

Syntax

```
dfs-channel
```

Mode

Radio N

Description

Enable DFS channel.

Example

```
dfs-channel
```

Syntax

```
no dfs-channel
```

Mode

Radio N

Description

Disable DFS channel.

Example

```
no dfs-channel
```

Syntax

```
ssid <WORD>
```

Mode

Radio N
Radio 2.4GHz

Description

Set the radio SSID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
ssid sonicwall
```

Syntax

```
no ssid
```

Mode

Radio N
Radio 2.4GHz

Description

Clear the radio SSID.

Example

```
no ssid
```

Syntax

```
channel { primary <SONICPOINT_N_CHANNEL> | secondary <SONICPOINT_N_CHANNEL> | standard <SONICPOINT_N_CHANNEL> }
```

Mode

Radio N
Radio 2.4GHz

Description

Set the radio channel.

Options

| | |
|-------------------------------------|--|
| primary | Set the radio primary channel. |
| <SONICPOINT_N_CHANNEL> | SonicPointN channel. Example: <i>auto</i> |
| secondary | Set the radio secondary channel. |
| <SONICPOINT_N_CHANNEL> | SonicPointN channel. Example: <i>auto</i> |
| standard | Set the radio standard channel. |
| <SONICPOINT_N_CHANNEL> | SonicPointN channel. Example: <i>auto</i> |

Example

```
channel primary auto
```

Syntax

```
band { 20 | 40 | 80 | auto }
```

Mode

Radio N
Radio 2.4GHz

Description

Set the radio band.

Options

| | |
|-------------|---------------------------|
| 20 | Standard - 20mhz channel. |
| 40 | Wide - 40mhz channel. |
| 80 | Wide - 80mhz channel. |
| auto | Auto. |

Example

```
band standard
```

Syntax

```
short-guard-interval
```

Mode

Radio N
Radio 2.4GHz

Description

Enable short guard interval.

Example

short-guard-interval

Syntax

no short-guard-interval

Mode

Radio N
Radio 2.4GHz

Description

Disable short guard interval.

Example

no short-guard-interval

Syntax

aggregation

Mode

Radio N
Radio 2.4GHz

Description

Enable aggregation.

Example

aggregation

Syntax

no aggregation

Mode

Radio N
Radio 2.4GHz

Description

Disable aggregation.

Example

no aggregation

Syntax

mimo

Mode

Radio N
Radio 2.4GHz

Description

Enable MIMO.

Example

mimo

Syntax

no mimo

Mode

Radio N
Radio 2.4GHz

Description

Disable MIMO.

Example

no mimo

Syntax

no access-list [deny]

Mode

Radio N
Radio 2.4GHz

Description

Disable MAC filter list or set no deny access list.

Options

deny Set no deny access list.

Example

no access-list
no access-list deny

Syntax

access-list [allow { all | default | group <ADDR_CUSTOM_GROUP_NAME_MIXED> }] [deny { default | group <ADDR_CUSTOM_GROUP_NAME_MIXED> }]

Mode

Radio N
Radio 2.4GHz

Description

Enable/configure MAC filter lists.

Options

| | |
|---|--|
| allow | Set MAC filter allow list. |
| all | All MAC addresses. |
| default | Default SonicPoint ACL allow group. |
| group | Name of ACL allow group. |
| <ADDR_CUSTOM_GROUP_NAME_MIXED> | Custom group address object name. Example: <i>Sales Group</i> |
| deny | Set MAC filter deny list. |

default Default SonicPoint ACL deny group.

group Name of ACL deny group.

<ADDR_CUSTOM_GROUP_NAME_MIXED> Custom group address object name.
Example: *Sales Group*

Example

```
access-list allow all deny default
```

Syntax

```
mic-failure acl-blacklist
```

Mode

Radio N
Radio 2.4GHz

Description

Enable MIC failure ACL blacklist.

Example

```
mic-failure acl-blacklist
```

Syntax

```
no mic-failure acl-blacklist
```

Mode

Radio N
Radio 2.4GHz

Description

Disable MIC failure ACL blacklist.

Example

```
no mic-failure acl-blacklist
```

Syntax

```
mic-failure frequency <UINT8>
```

Mode

Radio N
Radio 2.4GHz

Description

Set MIC failure frequency threshold (times / minute).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
mic-failure frequency 3
```

Syntax

```
virtual-access-point wep-key { { key1 | key2 | key3 | key4 } { { type { 128 | 152 | 64 } value <ENC_PASSWORD> } } | default { { 1 | 2 | 3 | 4 } } | method { { alphanumeric | hexadecimal } } }
```

Mode

Radio N
Radio 2.4GHz

Description

Set virtual access point WEP key configuration.

Options

| | |
|-----------------------------|---|
| key1 | Key 1. |
| key2 | Key 2. |
| key3 | Key 3. |
| key4 | Key 4. |
| type | Set WEP key type. |
| 128 | 128 bits. |
| 152 | 152 bits. |
| 64 | 64 bits. |
| value | Set WEP key value. |
| <ENC_PASSWORD> | Password. Example: <i>secret</i> |
| default | Set virtual access point WEP default key. |
| 1 | Key 1. |
| 2 | Key 2. |
| 3 | Key 3. |
| 4 | Key 4. |
| method | Set virtual access point WEP key method. |
| alphanumeric | Alphanumeric. |
| hexadecimal | Hexadecimal. |

Example

```
virtual-access-point wep-key method alphanumeric  
virtual-access-point wep-key default 1  
virtual-access-point wep-key 1 type 64 value wepke
```

Syntax

```
no virtual-access-point wep-key { key1 | key2 | key3 | key4 }
```

Mode

Radio N
Radio 2.4GHz

Description

Clear virtual access point WEP key type.

Options

key1 Key 1.

key2 Key 2.

key3 Key 3.

key4 Key 4.

Example

```
no virtual-access-point wep-key key 1 type
```

Syntax

```
authentication-type { wep { { both | open-system | shared-key } } | wpa { { eap | psk } } | wpa2 { { auto { { eap | psk } } | eap | psk } } }
```

Mode

Radio N
Radio 2.4GHz

Description

Set WEP/WPA authentication type.

Options

| | |
|--------------------|--|
| wep | WEP. |
| both | WEP - both (open system and shared key). |
| open-system | WEP - open system. |
| shared-key | WEP - shared key. |
| wpa | WPA. |
| eap | WPA - EAP. |
| psk | WPA - PSK. |
| wpa2 | WPA2. |
| auto | WPA2 - AUTO. |
| eap | WPA2 - AUTO - EAP. |
| psk | WPA2 - AUTO - PSK. |
| eap | WPA2 - EAP. |
| psk | WPA2 - PSK. |

Example

```
authentication-type wep both
```

Syntax

```
no wep-key { { key1 | key2 | key3 | key4 } value | type }
```

Mode

Radio N
Radio 2.4GHz

Description

Clear WEP key type.

Options

key1 Key 1.
key2 Key 2.
key3 Key 3.
key4 Key 4.
value Clear WEP key value.
type Clear WEP key type.

Example

```
no wep-key type
```

Syntax

```
wep-key { { key1 | key2 | key3 | key4 } value <ENC_PASSWORD> | default { { 1 | 2 | 3 | 4 } } | method { { alphanumeric | hexadecimal } } | type { { 128 | 152 | 64 | none } } }
```

Mode

Radio N
Radio 2.4GHz

Description

Set WEP key configuration.

Options

key1 Key 1.
key2 Key 2.
key3 Key 3.
key4 Key 4.
value Set WEP key value.
<ENC_PASSWORD> Password.
Example: *secret*
default Set WEP default key.
1 Key 1.
2 Key 2.
3 Key 3.
4 Key 4.
method Set WEP key method.

| | |
|---------------------|---------------------|
| alphanumeric | Alphanumeric. |
| hexadecimal | Hexadecimal. |
| type | Set WEP key type. |
| 128 | 128 bits. |
| 152 | 152 bits. |
| 64 | 64 bits. |
| none | Clear WEP key type. |

Example

```
wep-key method alphaNumeric
wep-key default 1
wep-key type 64
wep-key 1 value wepKeyValue1
```

Syntax

```
wpa auth-balance-method { local-radius-first | local-radius-only | remote-radius-first | remote-radius-only }
```

Mode

Radio N
Radio 2.4GHz

Description

Set authentication balance method.

Options

| | |
|----------------------------|--|
| local-radius-first | Local radius server first. |
| local-radius-only | Only local radius server. |
| remote-radius-first | Local radius server as failover mechanism. |
| remote-radius-only | Only remote radius server. |

Example

```
wpa auth-balance-method local-radius-first
```

Syntax

```
wpa cipher-type { aes | auto | tkip }
```

Mode

Radio N
Radio 2.4GHz

Description

Set WPA cipher type.

Options

| | |
|-------------|-------|
| aes | AES. |
| auto | Auto. |

tkip TKIP.

Example

```
wpa cipher-type aes
```

Syntax

```
wpa group-key-interval <UINT32>
```

Mode

Radio N
Radio 2.4GHz

Description

Set WPA group key interval in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
wpa group-key-interval 86400
```

Syntax

```
wpa passphrase <ENC_PASSWORD>
```

Mode

Radio N
Radio 2.4GHz

Description

Set WPA passphrase.

Options

<ENC_PASSWORD> Password.
Example: secret

Example

```
wpa passphrase mywppassphrase
```

Syntax

```
no wpa passphrase
```

Mode

Radio N
Radio 2.4GHz

Description

Clear WPA passphrase.

Example

```
no wpa passphrase
```

Syntax

```
wpa pmf [ enabled | required ]
```

Mode

Radio N
Radio 2.4GHz

Description

Set WPA PMF(Protected Management Frame) option.

Options

enabled Enable PMF(Protected Management Frame) option.

required Clients must enable the service to connect the AP.

Example

```
wpa pmf
```

Syntax

```
no wpa pmf
```

Mode

Radio N
Radio 2.4GHz

Description

Disable PMF(Protected Management Frame) option.

Example

```
no wpa pmf
```

Syntax

```
remote-mac-access-control
```

Mode

Radio N
Radio 2.4GHz

Description

Enable enforce radio wireless access control based on MAC-based authentication policy in remote radius server.

Example

```
remote-mac-access-control
```

Syntax

```
no remote-mac-access-control
```

Mode

Radio N
Radio 2.4GHz

Description

Disable enforce radio wireless access control based on MAC-based authentication policy in remote radius server.

Example

```
no remote-mac-access-control
```

Syntax

```
hide-ssid
```

Mode

Radio N
Radio 2.4GHz

Description

Enable hide SSID in beacon.

Example

```
hide-ssid
```

Syntax

```
no hide-ssid
```

Mode

Radio N
Radio 2.4GHz

Description

Disable hide SSID in beacon.

Example

```
no hide-ssid
```

Syntax

```
ids-scan schedule { days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

Radio N
Radio 2.4GHz

Description

Set schedule for IDS scan.

Options

| | |
|---------------------------------|---|
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
ids-scan schedule name "Weekend Hours"
```

Syntax

```
no ids-scan schedule
```

Mode

Radio N
Radio 2.4GHz

Description

Disable IDS scan schedule.

Example

```
no ids-scan schedule
```

Syntax

```
data-rate <SONICPOINT_RADIO_DATA_RATE>
```

Mode

Radio N
Radio 2.4GHz

Description

Set data rate.

Options

<SONICPOINT_RADIO_DATA_RATE> SonicPoint radio data rate.
Example: *best*

Example

```
data-rate best
```

Syntax

```
transmit-power { eighth | full | half | minimum | quarter }
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio transmit power.

Options

eighth Eighth (-9 dB).

full Full power.

half Half (-3 dB).

minimum Minimum.

quarter Quarter (-6 dB).

Example

```
transmit-power half
```

Syntax

```
antennae-diversity best
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio antennae diversity.

Options

best Best.

Example

```
antennae-diversity best
```

Syntax

```
interval { beacon <UINT16> | dtim <UINT8> }
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio interval.

Options

beacon Set radio beacon interval in milliseconds.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

dtim Set radio DTIM interval.
<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
interval beacon 100  
interval dtim 1
```

Syntax

```
threshold { fragmentation <UINT16> | rts <UINT16> }
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio threshold in bytes.

Options

fragmentation Set radio fragmentation threshold in bytes.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

rts Set radio RTS threshold in bytes.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
threshold fragmentation 2346  
threshold rts 2346
```

Syntax

```
max-clients <UINT8>
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio maximum client associations.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
max-clients 32
```

Syntax

```
station-inactivity-timeout <UINT16>
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio station inactivity timeout in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
station-inactivity-timeout 300
```

Syntax

```
preamble-length { long | short }
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio preamble length.

Options

long Long.

short Short.

Example

```
preamble-length long
```

Syntax

```
protection mode { always | auto }
```

Mode

Radio N
Radio 2.4GHz

Description

Set the radio protection mode.

Options

always Always.

auto Auto.

Example

```
protection mode always
```

Syntax

```
no protection mode
```

Mode

Radio N
Radio 2.4GHz

Description

Set no radio protection mode.

Example

```
no protection mode
```

Syntax

```
protection rate { 1 | 11 | 2 | 5 }
```

Mode

Radio N
Radio 2.4GHz

Description

Set the radio protection rate in Mbps.

Options

1 Data rate.

11 Data rate.

2 Data rate.

5 Data rate.

Example

```
protection rate 5
```

Syntax

```
protection type { cts-only | rts-cts }
```

Mode

Radio N
Radio 2.4GHz

Description

Set the radio protection type.

Options

cts-only CTS-only.

rts-cts RTS-CTS.

Example

```
protection type cts-only
```

Syntax

```
short-slot-time
```

Mode

Radio N
Radio 2.4GHz

Description

Enable short slot time.

Example

```
short-slot-time
```

Syntax

```
no short-slot-time
```

Mode

Radio N
Radio 2.4GHz

Description

Disable short slot time.

Example

```
no short-slot-time
```

Syntax

```
deny-b
```

Mode

Radio N
Radio 2.4GHz

Description

Enable does not allow 802.11b clients to connect.

Example

```
deny-b
```

Syntax

```
no deny-b
```

Mode

Radio N
Radio 2.4GHz

Description

Disable does not allow 802.11b clients to connect.

Example

```
no deny-b
```

Syntax

```
wds-ap
```

Mode

Radio N
Radio 2.4GHz

Description

Enable WDS AP.

Example

```
wds-ap
```

Syntax

```
no wds-ap
```

Mode

Radio N
Radio 2.4GHz

Description

Disable WDS AP.

Example

```
no wds-ap
```

Syntax

```
wmm <WMM_PROFILE>
```

Mode

Radio N
Radio 2.4GHz

Description

Set WMM (Wi-Fi multimedia).

Options

<WMM_PROFILE> WiFi multimedia profile name.
Example: *abc*

Example

```
wmm wmmprofile
```

Syntax

```
no wmm
```

Mode

Radio N
Radio 2.4GHz

Description

Disable WMM (Wi-Fi multimedia).

Example

```
no wmm
```

Syntax

```
green-ap [ timeout <UINT16> ]
```

Mode

Radio N
Radio 2.4GHz

Description

Enable SonicPoint green AP and set timeout.

Options

timeout Set SonicPoint green AP timeout.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
greep-ap  
green-ap timeout 20
```

Syntax

```
no green-ap
```

Mode

Radio N
Radio 2.4GHz

Description

Disable SonicPoint green AP.

Example

```
no greep-ap
```

Syntax

```
rsii [ threshold <INT16> ]
```

Mode

Radio N
Radio 2.4GHz

Description

Enable SonicPoint rsii and set threshold.

Options

threshold Set SonicPoint rssi threshold.
<INT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
rsii  
rsii threshold -95
```

Syntax

```
no rssi
```

Mode

Radio N
Radio 2.4GHz

Description

Disable SonicPoint rssi.

Example

```
no rssi
```

Syntax

```
airtime-fairness
```

Mode

Radio N
Radio 2.4GHz

Description

Enable SonicPoint airtime fairness.

Example

```
airtime-fairness
```

Syntax

```
no airtime-fairness
```

Mode

Radio N
Radio 2.4GHz

Description

Disable SonicPoint airtime fairness.

Example

```
no airtime-fairness
```

Syntax

```
80211r [ ft-over-ds | mix-mode ]
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicWave IEEE80211r.

Options

ft-over-ds Enable IEEE802.11r FT over DS.

mix-mode Enable IEEE802.11r mix mode.

Example

```
80211r  
80211r ft-over-ds 80211r mix-mode
```

Syntax

```
no 80211r [ ft-over-ds | mix-mode ]
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicWave IEEE80211r.

Options

ft-over-ds Disable IEEE802.11r FT over DS.

mix-mode Disable IEEE802.11r mix mode.

Example

```
no 80211r  
no 80211r ft-over-ds no 80211r mix-mode
```

Syntax

```
80211k neighbour-report
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicWave IEEE80211k.

Example

```
80211k neighbour-report
```

Syntax

```
no 80211k neighbour-report
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicWave IEEE80211k.

Example

```
no 80211k neighbour-report
```

Syntax

```
80211v { bss-trans-mgmt | wnm-sleep }
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicWave IEEE80211v.

Options

bss-trans-mgmt Enable IEEE802.11v BSS transition management.

wnm-sleep Enable IEEE802.11v WNM sleep mode.

Example

```
80211v bss-trans-mgmt
```

Syntax

```
no 80211v { bss-trans-mgmt | wnm-sleep }
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicWave IEEE80211v.

Options

bss-trans-mgmt Disable IEEE802.11v BSS transition management.

wnm-sleep Disable IEEE802.11v WNM sleep mode.

Example

```
no 80211v bss-trans-mgmt
```

Syntax

```
ids
```

Mode

SonicPoint

Description

Enter SonicPoint IDS mode.

Example

```
ids
```

Syntax

```
scan sonicpoint <SONICPOINT_IDS_SCAN_NAME> { both | radio { 2400mhz | 5000mhz } }
```

Mode

SonicPoint IDS

Description

Perform SonicPoint scan.

Options

<SONICPOINT_IDS_SCAN_NAME> SonicPoint IDS scan name.
Example: *mySonicpointn*

both 802.11 both 2.4G and 5G radio.

radio 802.11n 2.4G radio or 5G radio.

2400mhz 802.11n 2.4G radio.

5000mhz 802.11n 5G radio.

Example

```
scan sonicpoint mySP both
scan sonicpoint mySP radio 2400mhz
scan sonicpoint mySP radio 5000mhz
```

Syntax

```
scan all
```

Mode

SonicPoint IDS

Description

Perform SonicPoints scan all.

Example

```
scan all
```

Syntax

```
authorizing-access-point mac <SONICPOINT_DETECTED_AP_MAC>
```

Mode

SonicPoint IDS

Description

Authorizing the access point.

Options

| | |
|---|---|
| mac | Detected by the SonicPoint. |
| <SONICPOINT_DETECTED_AP_MAC> | Detected access point MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: 00:0C:F1:56:98:AD |

Example

```
authorizing-access-point mac 01:02:03:04:05:06
```

Syntax

```
widp
```

Mode

SonicPoint

Description

Enter SonicPoint wireless intrusion detection and prevention mode.

Example

```
widp
```

Syntax

```
no widp
```

Mode

SonicPoint

Description

Disable wireless intrusion detection and prevention.

Example

```
no widp
```

Syntax

```
authorized-access-point { all | group <ADDR_CUSTOM_GROUP_NAME_MIXED> }
```

Mode

SonicPoint WIDP

Description

Set authorized access points.

Options

| | |
|---|--|
| all | All authorized access points. |
| group | Specify MAC address object group for authorized access points. |
| <ADDR_CUSTOM_GROUP_NAME_MIXED> | Custom group address object name. Example: <i>Sales Group</i> |

Example

```
authorized-access-point all
```

Syntax

```
rogue-access-point { all | group <ADDR_CUSTOM_GROUP_NAME_MIXED> }
```

Mode

SonicPoint WIDP

Description

Set rogue access points.

Options

| | |
|---|--|
| all | All rogue access points. |
| group | Specify MAC address object group for rogue access points. |
| <ADDR_CUSTOM_GROUP_NAME_MIXED> | Custom group address object name. Example: <i>Sales Group</i> |

Example

```
rogue-access-point all
```

Syntax

```
unauthorized-access-point { any | connected }
```

Mode

SonicPoint WIDP

Description

Enable add any unauthorized AP or connected unauthorized AP into rogue AP list.

Options

any Enable add any unauthorized AP into rogue AP list.

connected Enable add connected unauthorized AP into rogue AP list.

Example

```
unauthorized-access-point any
unauthorized-access-point connected
```

Syntax

```
no unauthorized-access-point { any | connected }
```

Mode

SonicPoint WIDP

Description

Disable add any unauthorized AP or connected unauthorized AP into rogue AP list.

Options

any Disable add any unauthorized AP into rogue AP list.

connected Disable add connected unauthorized AP into rogue AP list.

Example

```
no unauthorized-access-point any
no unauthorized-access-point connected
```

Syntax

```
arp-cache-lookup
```

Mode

SonicPoint WIDP

Description

Enable ARP cache lookup to detect connected rogue AP.

Example

```
arp-cache-lookup
```

Syntax

```
no arp-cache-lookup
```

Mode

SonicPoint WIDP

Description

Disable ARP cache lookup to detect connected rogue AP.

Example

```
no arp-cache-lookup
```

Syntax

active-probe

Mode

SonicPoint WIDP

Description

Enable active probe to detect connected rogue AP.

Example

active-probe

Syntax

no active-probe

Mode

SonicPoint WIDP

Description

Disable active probe to detect connected rogue AP.

Example

no active-probe

Syntax

evil-twin

Mode

SonicPoint WIDP

Description

Enable add evil twin into rogue AP list.

Example

evil-twin

Syntax

no evil-twin

Mode

SonicPoint WIDP

Description

Disable add evil twin into rogue AP list.

Example

no evil-twin

Syntax

```
block-traffic { all | group <ADDR_CUSTOM_GROUP_NAME_MIXED> }
```

Mode

SonicPoint WIDP

Description

Enable block traffic from rogue AP and its associated clients.

Options

| | |
|---|--|
| all | All rogue devices. |
| group | Specify IP address object group for rogue devices. |
| <ADDR_CUSTOM_GROUP_NAME_MIXED> | Custom group address object name. Example: <i>Sales Group</i> |

Example

```
block-traffic all
```

Syntax

```
no block-traffic
```

Mode

SonicPoint WIDP

Description

Disable block traffic from rogue AP and its associated clients.

Example

```
no block-traffic
```

Syntax

```
disassociate rogue
```

Mode

SonicPoint WIDP

Description

Enable disassociate rogue AP and its associated clients.

Example

```
disassociate rogue
```

Syntax

```
no disassociate rogue
```

Mode

SonicPoint WIDP

Description

Disable disassociate rogue AP and its associated clients.

Example

no disassociate rogue

Syntax

disassociate krack

Mode

SonicPoint WIDP

Description

Enable disassociate client from KRACK MITM AP.

Example

disassociate krack

Syntax

no disassociate krack

Mode

SonicPoint WIDP

Description

Disable disassociate client from KRACK MITM AP.

Example

no disassociate krack

Syntax

rf-monitoring

Mode

SonicPoint

Description

Enter SonicPoint RF monitoring configuration mode.

Example

rf-monitoring

Syntax

measurement-interval <UINT16>

Mode

RF Monitoring

Description

Set the RF monitoring measurement interval.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
measurement-interval 300
```

Syntax

```
management-frame-flood
```

Mode

RF Monitoring

Description

Enable management frame flood threat detection.

Example

```
management-frame-flood
```

Syntax

```
no management-frame-flood
```

Mode

RF Monitoring

Description

Disable management frame flood threat detection.

Example

```
no management-frame-flood
```

Syntax

```
null-probe-response
```

Mode

RF Monitoring

Description

Enable null probe response threat detection.

Example

```
null-probe-response
```

Syntax

```
no null-probe-response
```

Mode

RF Monitoring

Description

Disable null probe response threat detection.

Example

no null-probe-response

Syntax

broadcasting-deauthentication

Mode

RF Monitoring

Description

Enable broadcasting deauthentication threat detection.

Example

broadcasting-deauthentication

Syntax

no broadcasting-deauthentication

Mode

RF Monitoring

Description

Disable broadcasting deauthentication threat detection.

Example

no broadcasting-deauthentication

Syntax

station-with-invalid-ssid

Mode

RF Monitoring

Description

Enable valid station with invalid SSID threat detection.

Example

station-with-invalid-ssid

Syntax

no station-with-invalid-ssid

Mode

RF Monitoring

Description

Disable valid station with invalid SSID threat detection.

Example

no station-with-invalid-ssid

Syntax

wellenreiter

Mode

RF Monitoring

Description

Enable wellenreiter detection threat detection.

Example

wellenreiter

Syntax

no wellenreiter

Mode

RF Monitoring

Description

Disable wellenreiter detection threat detection.

Example

no wellenreiter

Syntax

ad-hoc-station

Mode

RF Monitoring

Description

Enable AD-Hoc station threat detection.

Example

ad-hoc-station

Syntax

no ad-hoc-station

Mode

RF Monitoring

Description

Disable AD-Hoc station threat detection.

Example

no ad-hoc-station

Syntax

long-duration

Mode

RF Monitoring

Description

Enable long duration threat detection.

Example

long-duration

Syntax

no long-duration

Mode

RF Monitoring

Description

Disable long duration threat detection.

Example

no long-duration

Syntax

unassociated-station

Mode

RF Monitoring

Description

Enable unassociated station threat detection.

Example

unassociated-station

Syntax

no unassociated-station

Mode

RF Monitoring

Description

Disable unassociated station threat detection.

Example

no unassociated-station

Syntax

netstumbler

Mode

RF Monitoring

Description

Enable netstumbler threat detection.

Example

netstumbler

Syntax

no netstumbler

Mode

RF Monitoring

Description

Disable netstumbler threat detection.

Example

no netstumbler

Syntax

eapol-packet-flood

Mode

RF Monitoring

Description

Enable EAPOL packet flood threat detection.

Example

eapol-packet-flood

Syntax

no eapol-packet-flood

Mode

RF Monitoring

Description

Disable EAPOL packet flood threat detection.

Example

no eapol-packet-flood

Syntax

weak-wep-iv

Mode

RF Monitoring

Description

Enable weak WEP IV threat detection.

Example

```
weak-wep-iv
```

Syntax

```
no weak-wep-iv
```

Mode

RF Monitoring

Description

Disable weak WEP IV threat detection.

Example

```
no weak-wep-iv
```

Syntax

```
watch station <RFM_DETECTED_STATION_MAC>
```

Mode

RF Monitoring

Description

Add station into watch list.

Options

<RFM_DETECTED_STATION_MAC> Rf monitoring detected station MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD

Example

```
watch station 01:02:03:04:05:06
```

Syntax

```
no watch station <RFM_DETECTED_STATION_MAC>
```

Mode

RF Monitoring

Description

Remove station from watch list.

Options

<RFM_DETECTED_STATION_MAC> Rf monitoring detected station MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD

Example

```
no watch station 01:02:03:04:05:06
```

Syntax

```
clear rf-monitoring statistics
```

Mode

RF Monitoring

Description

Clear RF monitoring statistics information.

Example

```
clear rf-monitoring statistics
```

Syntax

```
fairnet enable
```

Mode

SonicPoint

Description

Enable FairNet.

Example

```
fairnet enable
```

Syntax

```
no fairnet enable
```

Mode

SonicPoint

Description

Disable FairNet.

Example

```
no fairnet enable
```

Syntax

```
fairnet policy direction { both | downlink | uplink } range <IPV4_HOST> <IPV4_HOST> interface <FAIRNET_INTERFACE> [ rate min <UINT32> max <UINT32> ]
```

Mode

SonicPoint

Description

Add/edit FairNet policy and enter its configuration mode.

Options

direction Specify direction.

| | |
|----------------------------------|--|
| both | Both. |
| downlink | Downlink (AP to client). |
| uplink | Uplink (client to AP). |
| range | Specify IP range. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| interface | Specify interface. |
| <FAIRNET_INTERFACE> | Fairnet interface name. Example: X0 |
| rate | Specify rate of FairNet policy in kbps. |
| min | Specify min rate of FairNet policy in kbps. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: 123 |
| max | Specify maximum rate of FairNet policy in kbps. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: 123 |

Example

```
fairnet policy direction both range 192.168.168.100 192.168.168.200 interface X2
```

Syntax

```
no fairnet policy direction { both | downlink | uplink } range <IPV4_HOST> <IPV4_HOST> interface <FAIRNET_INTERFACE>
```

Mode

SonicPoint

Description

Delete FairNet policy.

Options

| | |
|----------------------------------|--|
| direction | Specify direction. |
| both | Both. |
| downlink | Downlink (AP to client). |
| uplink | Uplink (client to AP). |
| range | Specify IP range. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| interface | Specify interface. |
| <FAIRNET_INTERFACE> | Fairnet interface name. Example: X0 |

Example

```
no fairnet policy direction both range 192.168.168.100 192.168.168.200 interface X2
```

Syntax

```
no fairnet policies
```

Mode

SonicPoint

Description

Delete all FairNet policies.

Example

```
no fairnet policies
```

Syntax

```
enable
```

Mode

FairNet Policy

Description

Enable this FairNet policy.

Example

```
enable
```

Syntax

```
no enable
```

Mode

FairNet Policy

Description

Disable this FairNet policy.

Example

```
no enable
```

Syntax

```
direction { both | downlink | uplink }
```

Mode

FairNet Policy

Description

Set direction of FairNet policy.

Options

both Both.

downlink Downlink (AP to client).

uplink Uplink (client to AP).

Example

```
direction both
```

Syntax

```
range <IPV4_HOST> <IPV4_HOST>
```

Mode

FairNet Policy

Description

Set IP range of FairNet policy.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
range 192.168.168.100 192.168.168.200
```

Syntax

```
interface <FAIRNET_INTERFACE>
```

Mode

FairNet Policy

Description

Set interface of FairNet policy.

Options

<FAIRNET_INTERFACE> Fairnet interface name.
Example: *X0*

Example

```
interface X2
```

Syntax

```
rate min <UINT32> max <UINT32>
```

Mode

FairNet Policy

Description

Set rate of FairNet policy in kbps.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

max Specify maximum rate of FairNet policy in kbps.

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
rate min 1000 max 2000
```

Syntax

```
wmm profile <WMM_PROFILE>
```

Mode

SonicPoint

Description

Add/edit WiFi multimedia profile and enter its configuration mode.

Options

<WMM_PROFILE> WiFi multimedia profile name.
Example: *abc*

Example

```
wmm profile corpwifiwmm
```

Syntax

```
no wmm profile <WMM_PROFILE>
```

Mode

SonicPoint

Description

Delete the specified WiFi multimedia profile.

Options

<WMM_PROFILE> WiFi multimedia profile name.
Example: *abc*

Example

```
no wmm profile corpwifiwmm
```

Syntax

```
no wmm profiles
```

Mode

SonicPoint

Description

Delete all WiFi multimedia profiles.

Example

```
no wmm profiles
```

Syntax

```
name <WMM_PROFILE>
```

Mode

WiFi Multimedia Profile

Description

Set the WiFi multimedia profile name.

Options

<WMM_PROFILE> WiFi multimedia profile name.

Example: *abc*

Example

```
name corpwifiwmm
```

Syntax

```
no access-point { ac-be | ac-bk | ac-vi | ac-vo } { [ cwmin ] [ cymax ] }
```

Mode

WiFi Multimedia Profile

Description

Set the WMM parameter for access point category.

Options

ac-be Set the WMM parameters for access point category AC_BE (0).

ac-bk Set the WMM parameters for access point category AC_BK (1).

ac-vi Set the WMM parameters for access point category AC_VI (2).

ac-vo Set the WMM parameters for access point category AC_VO (3).

cwmin Clear the CW min value.

cymax Clear the CW max value.

Example

```
no access-point ac-be cwmin cymax
no access-point ac-be cwmin
no access-point ac-be cymax
```

Syntax

```
access-point { ac-be | ac-bk | ac-vi | ac-vo } { [ cwmin <UINT8> ] [ cymax <UINT8> ] [ aifs <UINT8> ] }
```

Mode

WiFi Multimedia Profile

Description

Set the WMM parameter for access point category.

Options

ac-be Set the WMM parameters for access point category AC_BE (0).

ac-bk Set the WMM parameters for access point category AC_BK (1).

ac-vi Set the WMM parameters for access point category AC_VI (2).

ac-vo Set the WMM parameters for access point category AC_VO (3).

cwmin Set the CW min value.

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

cymax Set the CW max value.

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

aifs Set the AIFS value.

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
access-point ac-be cwmín 4 cwmáx 6 aifs 3
access-point ac-be cwmín 4 cwmáx 6
access-point ac-be cwmín 4
access-point ac-be cwmáx 6
access-point ac-be aifs 3
```

Syntax

```
no station { ac-be | ac-bk | ac-vi | ac-vo } { [ cwmín ] [ cwmáx ] }
```

Mode

WiFi Multimedia Profile

Description

Set the WMM parameter for station category.

Options

ac-be Set the WMM parameters for station category AC_BE (0).

ac-bk Set the WMM parameters for station category AC_BK (1).

ac-vi Set the WMM parameters for station category AC_VI (2).

ac-vo Set the WMM parameters for station category AC_VO (3).

cwmín Clear the CW min value.

cwmáx Clear the CW max value.

Example

```
no station ac-be cwmín cwmáx
no station ac-be cwmín
no station ac-be cwmáx
```

Syntax

```
station { ac-be | ac-bk | ac-vi | ac-vo } { [ cwmín <UINT8> ] [ cwmáx <UINT8> ] [ aifs <UINT8> ] }
```

Mode

WiFi Multimedia Profile

Description

Set the WMM parameter for station category.

Options

ac-be Set the WMM parameters for station category AC_BE (0).

ac-bk Set the WMM parameters for station category AC_BK (1).

ac-vi Set the WMM parameters for station category AC_VI (2).

ac-vo Set the WMM parameters for station category AC_VO (3).

cwmín Set the CW min value.

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

cwmáx Set the CW max value.

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

aifs Set the AIFS value.

<UINT8> Integer in the form: D OR 0xHH.

Example

```
station ac-be cwmmin 4 cwmax 10 aifs 3
station ac-be cwmmin 4 cwmax 10
station ac-be cwmmin 4
station ac-be cwmax 10
station ac-be aifs 3
```

Syntax

```
no mapping { ac-be | ac-bk | ac-vi | ac-vo }
```

Mode

WiFi Multimedia Profile

Description

Clear the WMM DSCP mapping.

Options

ac-be Clear the WMM DSCP mapping for category AC_BE (0).

ac-bk Clear the WMM DSCP mapping for category AC_BK (1).

ac-vi Clear the WMM DSCP mapping for category AC_VI (2).

ac-vo Clear the WMM DSCP mapping for category AC_VO (3).

Example

```
no mapping ac-bk
```

Syntax

```
mapping { ac-be <UINT8> | ac-bk <UINT8> | ac-vi <UINT8> | ac-vo <UINT8> }
```

Mode

WiFi Multimedia Profile

Description

Set the WMM DSCP mapping.

Options

ac-be Set the WMM DSCP mapping for category AC_BE (0).
<UINT8> Integer in the form: D OR 0xHH.
Example: 123

ac-bk Set the WMM DSCP mapping for category AC_BK (1).
<UINT8> Integer in the form: D OR 0xHH.
Example: 123

ac-vi Set the WMM DSCP mapping for category AC_VI (2).
<UINT8> Integer in the form: D OR 0xHH.
Example: 123

ac-vo Set the WMM DSCP mapping for category AC_VO (3).
<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

Syntax

```
virtual-access-point group <VAP_GROUP>
```

Mode

SonicPoint

Description

Add/edit virtual access point group and enter its configuration mode.

Options

<VAP_GROUP> VAP group name in the form: WORD or \"QUOTED STRING\".
Example: *vapGroup*

Example

```
virtual-access-point group CorpVAP
```

Syntax

```
virtual-access-point profile <VAP_PROFILE>
```

Mode

SonicPoint

Description

Add/edit virtual access point profile and enter its configuration mode.

Options

<VAP_PROFILE> VAP profile name in the form: WORD or \"QUOTED STRING\".
Example: *vapProfile*

Example

```
virtual-access-point profile CorpVAP
```

Syntax

```
virtual-access-point object <VAP_NAME>
```

Mode

SonicPoint

Description

Add/edit virtual access point object and enter its configuration mode.

Options

<VAP_NAME> VAP NAME in the form: WORD or \"QUOTED STRING\".
Example: *vapObject*

Example

```
virtual-access-point object CorpVAP
```

Syntax

```
no virtual-access-point { group <VAP_GROUP> | groups | object <VAP_NAME> | objects | profile <VAP_PROFILE> | profiles }
```

Mode

SonicPoint

Description

Delete the specified virtual access point object, profile or group.

Options

| | |
|----------------------------|--|
| group | Delete virtual access point group and enter its configuration mode. |
| <VAP_GROUP> | VAP group name in the form: WORD or \"QUOTED STRING\". Example: <i>vapGroup</i> |
| groups | Delete all virtual access point groups. |
| object | Delete virtual access point object and enter its configuration mode. |
| <VAP_NAME> | VAP NAME in the form: WORD or \"QUOTED STRING\". Example: <i>vapObject</i> |
| objects | Delete all virtual access point objects. |
| profile | Delete virtual access point profile and enter its configuration mode. |
| <VAP_PROFILE> | VAP profile name in the form: WORD or \"QUOTED STRING\". Example: <i>vapProfile</i> |
| profiles | Delete all virtual access point profiles. |

Example

```
no virtual-access-point object CorpVAP
no virtual-access-point groups
```

Syntax

```
name <VAP_GROUP>
```

Mode

SonicPoint Virtual Access Point Group

Description

Set virtual access point group name.

Options

| | |
|--------------------------|--|
| <VAP_GROUP> | VAP group name in the form: WORD or \"QUOTED STRING\". Example: <i>vapGroup</i> |
|--------------------------|--|

Example

```
name CorpVAPGroup
```

Syntax

```
virtual-access-point <VAP_NAME>
```

Mode

SonicPoint Virtual Access Point Group

Description

Add virtual access point object to this group.

Options

<VAP_NAME> VAP NAME in the form: WORD or \"QUOTED STRING\".
Example: *vapObject*

Example

```
virtual-access-point CorpVAPSSID
```

Syntax

```
group <VAP_GROUP>
```

Mode

SonicPoint Virtual Access Point Group

Description

Add virtual access point group to this group.

Options

<VAP_GROUP> VAP group name in the form: WORD or \"QUOTED STRING\".
Example: *vapGroup*

Example

```
group CorpVAPGroup
```

Syntax

```
no virtual-access-point <VAP_NAME>
```

Mode

SonicPoint Virtual Access Point Group

Description

Remove the specified virtual access point from this group.

Options

<VAP_NAME> VAP NAME in the form: WORD or \"QUOTED STRING\".
Example: *vapObject*

Example

```
no virtual-access-point CorpVAPSSid
```

Syntax

```
no group <VAP_GROUP>
```

Mode

SonicPoint Virtual Access Point Group

Description

Remove the specified virtual access point group from this group.

Options

<VAP_GROUP> VAP group name in the form: WORD or \"QUOTED STRING\".
Example: *vapGroup*

Example

```
no group CorpVAPGroup
```

Syntax

```
name <VAP_EDIT_NAME>
```

Mode

VAP Profile
Virtual Access Point

Description

Set virtual access point object or profile name.

Options

<VAP_EDIT_NAME> VAP object or profile name in the form: WORD or "QUOTED STRING".
Example: *vapName*

Example

```
name CorpVAP
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

VAP Profile
Virtual Access Point

Description

Set the schedule.

Options

| | |
|---------------------------------|---|
| always-on | Always on. |
| days | Schedule object days. |
| <SCHED_DAYS> | Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i> |
| time | Schedule object beginning/ending time. |
| <SCHED_TIME_BEGIN> | Time in the form: DD:DD. Example: <i>12:00</i> |
| <SCHED_TIME_END> | Time in the form: DD:DD. Example: <i>12:00</i> |
| name | Schedule object name. |
| <SCHED_NAME> | Schedule object name. Example: <i>Work Hours</i> |

Example

```
schedule name "Work Hours"
```

Syntax

```
access-list [ [ allow { { all | default | group <ADDR_CUSTOM_GROUP_NAME_MIXED> } } | deny { { default | group <ADDR_CUSTOM_GROUP_NAME_MIXED> } } | mac-filter-list [ use-global-access-list ] ] ]
```

Mode

Description

Enable/configure MAC filter list for this VAP.

Options

| | |
|---|--|
| allow | Set MAC filter allow list. |
| all | All MAC addresses. |
| default | Default ACL allow group. |
| group | Name of ACL allow group. |
| <ADDR_CUSTOM_GROUP_NAME_MIXED> | Custom group address object name. Example: <i>Sales Group</i> |
| deny | Set MAC filter deny list. |
| default | Default ACL deny group. |
| group | Name of ACL deny group. |
| <ADDR_CUSTOM_GROUP_NAME_MIXED> | Custom group address object name. Example: <i>Sales Group</i> |
| mac-filter-list | Enable MAC filter list. |
| use-global-access-list | Enable this VAP to use global ACL settings. |

Example

```
access-list allow all deny default
access-list allow default
access-list deny group wirelessAclDenyList
```

Syntax

```
no access-list [ deny | mac-filter-list | use-global-access-list ]
```

Mode

VAP Profile
Virtual Access Point

Description

Disable MAC filter list to use global ACL settings for this VAP.

Options

| | |
|-------------------------------|--|
| deny | Disable MAC filter deny list. |
| mac-filter-list | Disable MAC filter list. |
| use-global-access-list | Disable this VAP to use global ACL settings. |

Example

```
no access-list
no access-list deny
no access-list use-global-access-list
```

Syntax


```
radio-type { sonicpoint | wireless }
```

Mode

VAP Profile

Description

Set virtual access point profile radio type.

Options

sonicpoint Sonicpoint.

wireless Wireless.

Example

```
radio-type sonicpoint
```

Syntax

```
max-clients <UINT8>
```

Mode

VAP Profile

Virtual Access Point

Description

Set maximum client associations.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
max-clients 16
```

Syntax

```
wep-key default { 1 | 2 | 3 | 4 }
```

Mode

VAP Profile

Virtual Access Point

Description

Set WEP encryption default key index.

Options

default Set WEP encryption default key index.

1 Key 1.

2 Key 2.

3 Key 3.

4 Key 4.

Example

wep-key default 1

Syntax

```
authentication-type { wep { { both | open-system | shared-key } } | wpa { { eap | psk } } | wpa2 { { auto { { eap | psk } } | eap | psk } } }
```

Mode

VAP Profile
Virtual Access Point

Description

Set WEP/WPA authentication type.

Options

| | |
|--------------------|--|
| wep | WEP. |
| both | WEP - both (open system and shared key). |
| open-system | WEP - open system. |
| shared-key | WEP - shared key. |
| wpa | WPA. |
| eap | WPA - EAP. |
| psk | WPA - PSK. |
| wpa2 | WPA2. |
| auto | WPA2 - AUTO. |
| eap | WPA2 - AUTO - EAP. |
| psk | WPA2 - AUTO - PSK. |
| eap | WPA2 - EAP. |
| psk | WPA2 - PSK. |

Example

```
authentication-type wep both
```

Syntax

```
wpa auth-balance-method { local-radius-first | local-radius-only | remote-radius-first | remote-radius-only }
```

Mode

VAP Profile
Virtual Access Point

Description

Set authentication balance method.

Options

| | |
|---------------------------|----------------------------|
| local-radius-first | Local radius server first. |
|---------------------------|----------------------------|

local-radius-only Only local radius server.

remote-radius-first Local radius server as failover mechanism.

remote-radius-only Only remote radius server.

Example

```
wpa auth-balance-method local-radius-first
```

Syntax

```
cipher-type { aes | auto | tkip | wep }
```

Mode

VAP Profile
Virtual Access Point

Description

Set cipher type.

Options

aes AES.

auto Auto.

tkip TKIP.

wep WEP.

Example

```
cipher-type aes
```

Syntax

```
no cipher-type
```

Mode

VAP Profile
Virtual Access Point

Description

Set no cipher.

Example

```
no cipher-type
```

Syntax

```
wpa passphrase <ENC_PASSWORD>
```

Mode

VAP Profile
Virtual Access Point

Description

Set WPA passphrase.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
wpa passphrase mywpapassphrase
```

Syntax

```
no wpa passphrase
```

Mode

VAP Profile
Virtual Access Point

Description

Clear WPA passphrase.

Example

```
no wpa passphrase
```

Syntax

```
wpa group-key-interval <UINT32>
```

Mode

VAP Profile
Virtual Access Point

Description

Set WPA group key interval in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
wpa group-key-interval 86400
```

Syntax

```
wpa pmf [ enabled | required ]
```

Mode

VAP Profile
Virtual Access Point

Description

Set WPA PMF(Protected Management Frame) option.

Options

enabled Enable PMF(Protected Management Frame) option.

required Clients must enable the service to connect the AP.

Example

```
wpa pmf
```

Syntax

```
no wpa pmf
```

Mode

VAP Profile
Virtual Access Point

Description

Disable PMF(Protected Management Frame) option.

Example

```
no wpa pmf
```

Syntax

```
radius { accounting { server1 | server2 } { { ip <IPV4_HOST> | port <IPV4_PORT> | secret <ENC_PASSWORD> } } | nas { { identifier { sonicpoint-mac-address | sonicpoint-name | sonicpoint-ssid } | ip <IPV4_HOST> } } | retries <UINT8> | retry-interval <UINT8> | server { server1 | server2 } { { ip <IPV4_HOST> | port <IPV4_PORT> | secret <ENC_PASSWORD> } } }
```

Mode

VAP Profile
Virtual Access Point

Description

Set radius server for virtual access point.

Options

| | |
|--|--|
| accounting | Set radius accounting server. |
| server1 | Radius accounting server 1. |
| server2 | Radius accounting server 2. |
| ip <IPV4_HOST> | Radius accounting server IP. IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| port <IPV4_PORT> | Radius accounting server port. Integer in the form: D OR 0xHHHH. Example: 80 |
| secret <ENC_PASSWORD> | Radius accounting server secret. Password. Example: secret |
| nas | Nas settings to radius server. |
| identifier | Nas identifier to radius server. |
| sonicpoint-mac-address | SonicPoint's MAC address. |
| sonicpoint-name | SonicPoint's name. |
| sonicpoint-ssid | SonicPoint's SSID. |
| ip | Nas IP to radius server. |

| | |
|-----------------------------|--|
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| retries | Set radius server retries. |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| retry-interval | Set radius server retry interval (seconds). |
| <UINT8> | Integer in the form: D OR 0xHH. Example: 123 |
| server | Set radius server. |
| server1 | Radius server 1. |
| server2 | Radius server 2. |
| ip | Radius server IP. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| port | Radius server port. |
| <IPV4_PORT> | Integer in the form: D OR 0xHHHH. Example: 80 |
| secret | Radius server secret. |
| <ENC_PASSWORD> | Password. Example: secret |

Example

```
radius retries 1
radius retry-interval 20
radius server server1 ip 192.168.168.1
radius server server1 port 1812
radius server server1 secret radsecret
radius server server2 ip 192.168.168.2
radius server server2 port 1812
radius server server2 secret radsecret2
```

Syntax

```
no radius { accounting { server1 | server2 } { { ip | port | secret } } | nas { identifier | ip } | retries | retry-interval |
server { server1 | server2 } { { ip | port | secret } } }
```

Mode

VAP Profile
Virtual Access Point

Description

Clear radius server settings for virtual access point.

Options

| | |
|-------------------|--|
| accounting | Clear radius accounting server settings. |
| server1 | Clear radius accounting server 1 settings. |
| server2 | Clear radius accounting server 2 settings. |
| ip | Clear radius accounting server IP. |
| port | Clear radius accounting server port. |
| secret | Clear radius accounting server secret. |
| nas | Clear nas settings to radius server. |

| | |
|-----------------------|---|
| identifier | Nas identifier to radius server not included. |
| ip | Clear nas IP to radius server. |
| retries | Clear radius server retries. |
| retry-interval | Clear radius server retry interval. |
| server | Clear radius server setting. |
| server1 | Clear radius server 1 settings. |
| server2 | Clear radius server 2 settings. |
| ip | Clear radius server IP. |
| port | Clear radius server port. |
| secret | Clear radius server secre. |

Example

```
no radius retries
no radius retry-interval
no server server1 ip
no server server1 port
no server server1 secret
no server server2 ip
no server server2 port
no server server2 secret
```

Syntax

```
remote-mac-access-control
```

Mode

VAP Profile
Virtual Access Point

Description

Enable enforce radio wireless access control based on MAC-based authentication policy in remote radius server.

Example

```
remote-mac-access-control
```

Syntax

```
no remote-mac-access-control
```

Mode

VAP Profile
Virtual Access Point

Description

Disable enforce radio wireless access control based on MAC-based authentication policy in remote radius server.

Example

```
no remote-mac-access-control
```

Syntax

wds

Mode

VAP Profile
Virtual Access Point

Description

Enable virtual access point wireless distribution system.

Example

wds

Syntax

no wds

Mode

VAP Profile
Virtual Access Point

Description

Disable virtual access point wireless distribution system.

Example

no wds

Syntax

radio-type { sonicpoint | wireless }

Mode

Virtual Access Point

Description

Set virtual access point radio type.

Options

sonicpoint Sonicpoint.

wireless Wireless.

Example

radio-type sonicpoint

Syntax

ssid <WORD>

Mode

Virtual Access Point

Description

Set virtual access point SSID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ssid CorpSSID
```

Syntax

```
no ssid
```

Mode

Virtual Access Point

Description

Clear virtual access point SSID.

Example

```
no ssid
```

Syntax

```
no vlan-id
```

Mode

Virtual Access Point

Description

Clear virtual access point vlan id.

Example

```
no vlan-id
```

Syntax

```
vlan-id <VAP_VLAN_ID>
```

Mode

Virtual Access Point

Description

Set virtual access point vlan id.

Options

<VAP_VLAN_ID> VLAN ID.
Example: *100*

Example

```
vlan-id 100
```

Syntax

```
suppress-ssid
```

Mode

Virtual Access Point

Description

Enable suppress SSID.

Example

```
suppress-ssid
```

Syntax

```
no suppress-ssid
```

Mode

Virtual Access Point

Description

Disable suppress SSID.

Example

```
no suppress-ssid
```

Syntax

```
enable
```

Mode

Virtual Access Point

Description

Enable virtual access point.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Virtual Access Point

Description

Disable virtual access point.

Example

```
no enable
```

Syntax

```
dynamic-vlan
```

Mode

Virtual Access Point

Description

Enable VAP dynamic vlan assignment id.

Example

```
dynamic-vlan
```

Syntax

```
no dynamic-vlan
```

Mode

Virtual Access Point

Description

Disable VAP dynamic vlan assignment id.

Example

```
no dynamic-vlan
```

Syntax

```
vlan <VAP_VLAN_ID>
```

Mode

Virtual Access Point

Description

Set SonicPoint dynamic VLAN ID.

Options

<VAP_VLAN_ID> VLAN ID.
Example: 100

Example

```
vlan 4
```

Syntax

```
no vlan <VAP_VLAN_ID>
```

Mode

Virtual Access Point

Description

Clear SonicPoint dynamic VLAN ID.

Options

<VAP_VLAN_ID> VLAN ID.
Example: 100

Example

```
no vlan 4
```

Syntax

```
no vlans
```

Mode

Virtual Access Point

Description

Clear SonicPoint dynamic VLAN IDs.

Example

```
no vlans
```

Syntax

```
profile { sonicpoint <VAP_PROFILE> }
```

Mode

Virtual Access Point

Description

Set virtual access point profile used.

Options

sonicpoint Specify profile name.
<VAP_PROFILE> VAP profile name in the form: WORD or "QUOTED STRING".
Example: *vapProfile*

Example

```
profile sonicpoint CorpVAPProfile
```

Syntax

```
no profile
```

Mode

Virtual Access Point

Description

Clear virtual access point profile.

Example

```
no profile
```

Syntax

```
80211r [ ft-over-ds | mix-mode ]
```

Mode

VAP Profile
Virtual Access Point

Description

Set SonicWave IEEE80211r.

Options

ft-over-ds Enable IEEE802.11r FT over DS.

mix-mode Enable IEEE802.11r mix mode.

Example

```
80211r  
80211r ft-over-ds 80211r mix-mode
```

Syntax

```
no 80211r [ ft-over-ds | mix-mode ]
```

Mode

VAP Profile
Virtual Access Point

Description

Set SonicWave IEEE80211r.

Options

ft-over-ds Disable IEEE802.11r FT over DS.

mix-mode Disable IEEE802.11r mix mode.

Example

```
no 80211r  
no 80211r ft-over-ds no 80211r mix-mode
```

Syntax

```
80211k neighbour-report
```

Mode

VAP Profile
Virtual Access Point

Description

Set SonicWave IEEE80211k.

Example

```
80211k neighbour-report
```

Syntax

```
no 80211k neighbour-report
```

Mode

VAP Profile
Virtual Access Point

Description

Set SonicWave IEEE80211k.

Example

```
no 80211k neighbour-report
```

Syntax

```
80211v { bss-trans-mgmt | wnm-sleep }
```

Mode

VAP Profile
Virtual Access Point

Description

Set SonicWave IEEE80211v.

Options

bss-trans-mgmt Enable IEEE802.11v BSS transition management.

wnm-sleep Enable IEEE802.11v WNM sleep mode.

Example

```
80211v bss-trans-mgmt
```

Syntax

```
no 80211v { bss-trans-mgmt | wnm-sleep }
```

Mode

VAP Profile
Virtual Access Point

Description

Set SonicWave IEEE80211v.

Options

bss-trans-mgmt Disable IEEE802.11v BSS transition management.

wnm-sleep Disable IEEE802.11v WNM sleep mode.

Example

```
no 80211v bss-trans-mgmt
```

Syntax

```
show sonicpoint [ discovered-access-points [ sonicpoint <SONICPOINT_N_NAME> ] | fairnet [ { policies | policy { direction { both | downlink | uplink } range <IPV4_HOST> <IPV4_HOST> interface <FAIRNET_INTERFACE> } } ] | profile [ ac | n | ndr | wave2 ] <SONICPOINT_N_PROFILE_NAME> | profiles [ { ac | n | ndr | wave2 } ] | rf { analysis [ { channel { { highly-interfered | overloaded } } | score } ] | monitoring [ { discovered-threat-stations [ watch-list ] | statistics } ] ] | sonicpoint [ ac | n | ndr | wave2 ] <SONICPOINT_N_NAME> | sonicpoints [ { ac | n | ndr | wave2 } ] | station { statistics [ { radio [ sonicpoint <SONICPOINT_N_NAME> ] | sonicpoint <SONICPOINT_N_NAME> | traffic [ sonicpoint <SONICPOINT_N_NAME> ] } ] | status [ sonicpoint <SONICPOINT_N_NAME> ] } ] | statistics [ { radio [ sonicpoint <SONICPOINT_N_NAME> ] | sonicpoint <SONICPOINT_N_NAME> | traffic [ sonicpoint <SONICPOINT_N_NAME> ] } ] | status [ sonicpoint <SONICPOINT_N_NAME> ] | virtual-access-point { { group <VAP_GROUP> | groups | object <VAP_NAME> | objects | profile <VAP_PROFILE> | profiles } } | widp [ sensor-unit ] | wmm [ profile <WMM_PROFILE> ] } ] [ { pending-config | with-pending-config } ] ]
```

Mode

All Modes

Description

Show SonicPoint configuration.

Options

| | |
|---|--|
| <i>discovered-access-points</i> | Show all SonicPoints discovered access points. |
| <i>sonicpoint</i> | Show a specified SonicPoint discovered access points. |
| <i><SONICPOINT_N_NAME></i> | SonicPointN name. Example: <i>mySonicpointn</i> |
| <i>fairnet</i> | Show FairNet configuration. |
| <i>policies</i> | Show all FairNet policies. |
| <i>policy</i> | Show one specific FairNet policy. |
| <i>direction</i> | Specify direction. |
| <i>both</i> | Both. |
| <i>downlink</i> | Downlink (AP to client). |
| <i>uplink</i> | Uplink (client to AP). |
| <i>range</i> | Specify IP range. |
| <i><IPV4_HOST></i> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |
| <i><IPV4_HOST></i> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |
| <i>interface</i> | Specify interface. |
| <i><FAIRNET_INTERFACE></i> | Fairnet interface name. Example: <i>X0</i> |
| <i>profile</i> | Show the specified SonicPointNs provisioning profiles. |
| <i>ac</i> | SonicPoint ACe/ACi/N2/W2. |
| <i>n</i> | SonicPoint N. |
| <i>ndr</i> | SonicPoint NDR. |
| <i>wave2</i> | SonicPoint ACWave2 profile. |
| <i><SONICPOINT_N_PROFILE_NAME></i> | SonicPointN provisioning profile name. Example: <i>mySonicpointnProfile</i> |
| <i>profiles</i> | Show available SonicPointNs provisioning profiles. |
| <i>ac</i> | SonicPoint ACe/ACi/N2/W2. |
| <i>n</i> | SonicPointN. |
| <i>ndr</i> | SonicPointNDR. |
| <i>wave2</i> | SonicPoint ACWave2. |
| <i>rf</i> | Show SonicPoint RF monitoring and RF analysis information. |
| <i>analysis</i> | Show all SonicPoints RF analysis. |
| <i>channel</i> | Show SonicPoint each channel details. |
| <i>highly-interfered</i> | Show SonicPoint channel highly interfered by APs operating in the same channel as well as adjacent channels. |
| <i>overloaded</i> | Show SonicPoint channel overloaded by APs operating in the same channel. |
| <i>score</i> | Show all SonicPoints RF score. |
| <i>monitoring</i> | Show SonicPoint RF monitoring status or configuration. |
| <i>discovered-threat-stations</i> | Show discovered RF threat stations. |
| <i>watch-list</i> | Only stations in watch list group. |

| | |
|----------------------------------|---|
| statistics | Show SonicPoint RF monitoring statistics information, including total data threats, total management threats, etc.. |
| sonicpoint | Show the specified SonicPointNs. |
| ac | SonicPoint ACe/ACi/N2/W2. |
| n | SonicPoint N. |
| ndr | SonicPoint NDR. |
| wave2 | SonicPoint ACWave2 |
| <SONICPOINT_N_NAME> | SonicPointN name. Example: <i>mySonicpointn</i> |
| sonicpoints | Show available SonicPointNs. |
| ac | SonicPoint ACe/ACi/N2/W2. |
| n | SonicPointN. |
| ndr | SonicPointNDR. |
| wave2 | SonicPoint ACWave2. |
| station | Show all SonicPoints station status and statistics, status means some general information, including IP, SSID, AID, etc., statistics means statistical information, including radio and traffic statistics information. |
| statistics | Show all SonicPoints station statistics, including radio statistics and traffic statistics. |
| radio | Show all SonicPoints station's radio statistics information, including radio, channel, associations, disassociations, etc.. |
| sonicpoint | Show a specified SonicPoint station's radio statistics information. |
| <SONICPOINT_N_NAME> | SonicPointN name. Example: <i>mySonicpointn</i> |
| sonicpoint | Show a specified SonicPoint station statistics. |
| <SONICPOINT_N_NAME> | SonicPointN name. Example: <i>mySonicpointn</i> |
| traffic | Show all SonicPoints station's traffic statistics information, including good packets, control packets, management packets, etc.. |
| sonicpoint | Show a specified SonicPoint station's traffic statistics information. |
| <SONICPOINT_N_NAME> | SonicPointN name. Example: <i>mySonicpointn</i> |
| status | Show all SonicPoints station status, including IP address, mac address, type, SSID, AID, etc.. |
| sonicpoint | Show a specified SonicPoint station status. |
| <SONICPOINT_N_NAME> | SonicPointN name. Example: <i>mySonicpointn</i> |
| statistics | Show all SonicPoints statistics information, including radio statistics and traffic statistics. |
| radio | Show all SonicPoints radio statistics information, including radio, channel, associations, disassociations, etc.. |
| sonicpoint | Show a specified SonicPoint radio statistics information. |
| <SONICPOINT_N_NAME> | SonicPointN name. Example: <i>mySonicpointn</i> |
| sonicpoint | Show a specified SonicPoint statistics. |
| <SONICPOINT_N_NAME> | SonicPointN name. Example: <i>mySonicpointn</i> |
| traffic | Show all SonicPoints traffic statistics information, including good packets, control packets, management packets, etc.. |
| sonicpoint | Show a specified SonicPoint traffic statistics information. |
| <SONICPOINT_N_NAME> | SonicPointN name. Example: <i>mySonicpointn</i> |
| status | Show all SonicPoints status, including mac, IP, interface, zone, status, etc.. |
| sonicpoint | Show a specified SonicPoint status. |
| <SONICPOINT_N_NAME> | SonicPointN name. Example: <i>mySonicpointn</i> |

| | |
|--|--|
| virtual-access-point | Show virtual access point(s), profile(s) or group(s). |
| group <VAP_GROUP> | Show specified virtual access point group. VAP group name in the form: WORD or \"QUOTED STRING\". Example: <i>vapGroup</i> |
| groups | Show all virtual access point groups. |
| object <VAP_NAME> | Show specified virtual access point. VAP NAME in the form: WORD or \"QUOTED STRING\". Example: <i>vapObject</i> |
| objects | Show all virtual access points. |
| profile <VAP_PROFILE> | Show specified virtual access point profile configuration. VAP profile name in the form: WORD or \"QUOTED STRING\". Example: <i>vapProfile</i> |
| profiles | Show all virtual access point profiles configuration. |
| widp sensor-unit | Show SonicPoint wireless intrusion detection and prevention configuration. Show SonicPoint WIDP sensor units information. |
| wmm profile <WMM_PROFILE> | Show WiFi multimedia configuration. Show WiFi multimedia profile configuration. WiFi multimedia profile name. Example: <i>abc</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show sonicpoint
show sonicpoint profiles
show sonicpoint sonicpoints
show sonicpoint widp
show sonicpoint fairnet
show sonicpoint wmm
show sonicpoint rf monitoring
show sonicpoint rf analysis
show sonicpoint discovered-access-points
show sonicpoint station status
show sonicpoint station statistics
show sonicpoint status
show sonicpoint statistics
```

Syntax

```
virtual-assist
```

Mode

Config

Description

Enter virtual assist configuration mode.

Example

```
virtual-assist
```

Syntax

```
logout <CUSTOMER_ID>
```

Mode

Virtual Assist

Description

Logout specified virtual assist customer.

Options

<CUSTOMER_ID> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
logout myuser@acme.com
```

Syntax

```
assistance-code <WORD>
```

Mode

Virtual Assist

Description

Set virtual assist assistance code.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
assistance-code keyi0123
```

Syntax

```
no assistance-code
```

Mode

Virtual Assist

Description

Clear virtual assist assistance code.

Example

```
no assistance-code
```

Syntax

```
support-without-invitation
```

Mode

Virtual Assist

Description

Enable support without invitation.

Example

```
support-without-invitation
```

Syntax

no support-without-invitation

Mode

Virtual Assist

Description

Disable support without invitation.

Example

no support-without-invitation

Syntax

disclaimer <ROL>

Mode

Virtual Assist

Description

Set virtual assist disclaimer.

Options

<ROL> Remaining command line input.
Example: *line...*

Example

disclaimer "Disclaimer message."

Syntax

no disclaimer

Mode

Virtual Assist

Description

Clear virtual assist disclaimer.

Example

no disclaimer

Syntax

customer-access-link <WORD>

Mode

Virtual Assist

Description

Set virtual assist customer access link.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
customer-access-link www.virtualassistaccess.com
```

Syntax

```
no customer-access-link
```

Mode

Virtual Assist

Description

Clear virtual assist customer access link.

Example

```
no customer-access-link
```

Syntax

```
link-on-portal-login
```

Mode

Virtual Assist

Description

Enable display virtual assist link from portal login.

Example

```
link-on-portal-login
```

Syntax

```
no link-on-portal-login
```

Mode

Virtual Assist

Description

Disable display virtual assist link from portal login.

Example

```
no link-on-portal-login
```

Syntax

```
technician-email-list <ROL>
```

Mode

Virtual Assist

Description

Set virtual assist technician e-mail list.

Options

<ROL> Remaining command line input.
Example: *line...*

Example

```
technician-email-list myuser@acme.com
```

Syntax

```
no technician-email-list
```

Mode

Virtual Assist

Description

Clear virtual assist technician e-mail list.

Example

```
no technician-email-list
```

Syntax

```
invitation-subject <WORD>
```

Mode

Virtual Assist

Description

Set technician subject of invitation.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
invitation-subject \"%EXPERTNAME% has sent you a support invitation\"
```

Syntax

```
no invitation-subject
```

Mode

Virtual Assist

Description

Clear technician subject of invitation.

Example

```
no invitation-subject
```

Syntax

```
invitation-message <ROL>
```

Mode

Virtual Assist

Description

Set technician invitation message.

Options

<ROL> Remaining command line input.
Example: *line...*

Example

```
invitation-message "An assistance invitation has been generated for you"
```

Syntax

```
no invitation-message
```

Mode

Virtual Assist

Description

Clear technician invitation message.

Example

```
no invitation-message
```

Syntax

```
max-requests <UINT8>
```

Mode

Virtual Assist

Description

Set maximum requests.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
max-requests 10
```

Syntax

```
limit-message <WORD>
```

Mode

Virtual Assist

Description

Set technician limit message.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
limit-message "Maximum queue size reached, please try again later"
```

Syntax

```
no limit-message
```

Mode

Virtual Assist

Description

Clear technician limit message.

Example

```
no limit-message
```

Syntax

```
max-requests-one-ip <UINT16>
```

Mode

Virtual Assist

Description

Set maximum requests allowed from one IP.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
max-requests-one-ip 5
```

Syntax

```
no max-requests-one-ip
```

Mode

Virtual Assist

Description

Set no limit requests allowed from one IP.

Example

```
no max-requests-one-ip
```

Syntax

```
pending-request-expiration <UINT16>
```

Mode

Virtual Assist

Description

Set time (in minutes) customers are allowed to remain in queue before being removed without being assisted by technician.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
pending-request-expiration 10
```

Syntax

```
no pending-request-expiration
```

Mode

Virtual Assist

Description

Clear expiration time customers are allowed to remain in queue before being removed without being assisted by technician.

Example

```
no pending-request-expiration
```

Syntax

```
deny-requests { host <IPV4_HOST> | network <IPV4_HOST> <IPV4_MASK> }
```

Mode

Virtual Assist

Description

Add address from which to deny requests from.

Options

host IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

network Network address and subnet mask.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

<IPV4_MASK> IPV4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: 255.255.255.0

Example

```
deny-requests host 10.10.10.1  
deny-requests network 10.10.10.0 255.255.255.0
```

Syntax

```
no deny-requests { host <VIRTUAL_ASSIST_DENY_REQUESTS_HOST> | network <VIRTUAL_ASSIST_DENY_REQUESTS_HOST>  
<VIRTUAL_ASSIST_DENY_REQUESTS_NETMASK> }
```

Mode

Virtual Assist

Description

Delete address from which to deny requests from.

Options

| | |
|---|---|
| host | IP address. |
| <VIRTUAL_ASSIST_DENY_REQUESTS_HOST> | IPv4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| network | Network address and subnet mask. |
| <VIRTUAL_ASSIST_DENY_REQUESTS_HOST> | IPv4 Address in the form: a.b.c.d. Example: 192.168.168.168 |
| <VIRTUAL_ASSIST_DENY_REQUESTS_NETMASK> | IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D. Example: 255.255.255.0 |

Example

```
no deny-requests host 10.10.10.1
```

Syntax

```
show virtual-assist [ sessions ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show virtual assist configuration.

Options

| | |
|----------------------------|---|
| sessions | Show virtual assist active customer sessions. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show virtual-assist
```

Syntax

```
vpn [ policy { [ ipv4 ] { { group-vpn <VPN_GROUP_POLICY_NAME> | site-to-site <VPN_SITE_POLICY_NAME> | tunnel-interface <VPN_TUNNEL_POLICY_NAME> } } | enable <VPN_POLICY_NAME> | ipv6 { site-to-site <VPN_SITE_POLICY_V6_NAME> } } ]
```

Mode

Config

Description

Configure VPN.

Options

| | |
|--------------------------------------|---|
| policy | Add, edit or enable a VPN policy. |
| ipv4 | IPv4 vpn policy. |
| group-vpn | Edit group VPN policy. |
| <VPN_GROUP_POLICY_NAME> | Group VPN policy name. Example: WAN GroupVPN |
| site-to-site | Add or edit site-to-site VPN policy. |
| <VPN_SITE_POLICY_NAME> | Site-to-site VPN policy name. Example: Remote Office |

| | |
|--|---|
| tunnel-interface | Add or edit tunnel interface VPN policy. |
| <VPN_TUNNEL_POLICY_NAME> | Tunnel interface VPN policy name. Example: <i>Remote Office</i> |
| enable | Enable a VPN policy. |
| <VPN_POLICY_NAME> | VPN policy name. Example: <i>Remote Office</i> |
| ipv6 | IPv6 vpn policy. |
| site-to-site | Add or edit IPv6 site-to-site VPN policy. |
| <VPN_SITE_POLICY_V6_NAME> | IPv6 Site-to-site VPN policy name. Example: <i>Remote Office</i> |

Example

```
vpn
vpn policy site-to-site "Remote Office"
vpn policy group-vpn "WAN GroupVPN"
vpn policy enable "Remote Office"
```

Syntax

```
no vpn policy { [ ipv4 ] { { site-to-site <VPN_SITE_POLICY_NAME> | tunnel-interface <VPN_TUNNEL_POLICY_NAME> } } | enable <VPN_POLICY_NAME> | ipv6 { site-to-site <VPN_SITE_POLICY_V6_NAME> } }
```

Mode

Config

Description

Delete or disable a VPN policy.

Options

| | |
|--|---|
| ipv4 | IPv4 vpn policy. |
| site-to-site | Delete site-to-site VPN policy. |
| <VPN_SITE_POLICY_NAME> | Site-to-site VPN policy name. Example: <i>Remote Office</i> |
| tunnel-interface | Delete tunnel interface VPN policy. |
| <VPN_TUNNEL_POLICY_NAME> | Tunnel interface VPN policy name. Example: <i>Remote Office</i> |
| enable | Enable a VPN policy. |
| <VPN_POLICY_NAME> | VPN policy name. Example: <i>Remote Office</i> |
| ipv6 | IPv6 vpn policy. |
| site-to-site | Delete IPv6 site-to-site VPN policy. |
| <VPN_SITE_POLICY_V6_NAME> | IPv6 Site-to-site VPN policy name. Example: <i>Remote Office</i> |

Example

```
no vpn policy site-to-site "Remote Office"
no vpn policy enable "Remote Office"
```

Syntax

```
no vpn policies
```

Mode

Config

Description

Delete all VPN policies.

Example

```
no vpn policies
```

Syntax

```
enable
```

Mode

VPN

Description

Enable VPN.

Example

```
enable
```

Syntax

```
no enable
```

Mode

VPN

Description

Disable VPN.

Example

```
no enable
```

Syntax

```
firewall-identifier <WORD>
```

Mode

VPN

Description

Configure unique firewall identifier.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
firewall-identifier CorpFirewall
```

Syntax

```
no ike-dpd
```

Mode

VPN

Description

Disable IKE dead peer detection.

Example

```
no ike-dpd
```

Syntax

```
ike-dpd
```

Mode

VPN

Description

Configure IKE dead peer detection.

Example

```
ike-dpd
```

Syntax

```
interval <UINT8>
```

Mode

IKE Dead Peer Detection

Description

Configure dead peer detection interval.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
interval 60
```

Syntax

```
trigger <UINT8>
```

Mode

IKE Dead Peer Detection

Description

Configure failure trigger level in number of heartbeats.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
trigger 3
```

Syntax

```
idle-dpd [ interval <UINT16> ]
```

Mode

IKE Dead Peer Detection

Description

Enable dead peer detection for idle VPN sessions.

Options

interval Dead peer detection interval for idle VPN sessions in seconds.
<UINT16> Integer in the form: D OR 0xHHHHH.
Example: 123

Example

```
idle-dpd interval 600
```

Syntax

```
no idle-dpd
```

Mode

IKE Dead Peer Detection

Description

Disable dead peer detection for idle VPN sessions.

Example

```
no idle-dpd
```

Syntax

```
frag-packets
```

Mode

VPN

Description

Enable and configure fragmented packet handling for VPN.

Example

```
frag-packets
```

Syntax

```
no frag-packets
```

Mode

VPN

Description

Disable fragmented packet handling for VPN.

Example

```
no frag-packets
```

Syntax

ignore-df-bit

Mode

Fragmented Packet Handling

Description

Ignore DF (don't fragment) bit.

Example

ignore-df-bit

Syntax

no ignore-df-bit

Mode

Fragmented Packet Handling

Description

Disable ignore DF (don't fragment) bit.

Example

no ignore-df-bit

Syntax

nat-traversal

Mode

VPN

Description

Enable NAT traversal.

Example

nat-traversal

Syntax

no nat-traversal

Mode

VPN

Description

Disable NAT traversal.

Example

no nat-traversal

Syntax

cleanup-tunnels

Mode

VPN

Description

Enable clean up active tunnels when peer gateway DNS name resolves to a different IP address.

Example

cleanup-tunnels

Syntax

no cleanup-tunnels

Mode

VPN

Description

Disable clean up active tunnels when peer gateway DNS name resolves to a different IP address.

Example

no cleanup-tunnels

Syntax

preserve-ike-port

Mode

VPN

Description

Enable preserve IKE port for pass through connections.

Example

preserve-ike-port

Syntax

no preserve-ike-port

Mode

VPN

Description

Disable preserve IKE port for pass through connections.

Example

no preserve-ike-port

Syntax

*no ocs**sp-checking*

Mode

VPN

Description

Disable OCSP checking.

Example

*no ocs**sp-checking*

Syntax

*ocs**sp-checking*

Mode

VPN

Description

Enable and configure OCSP checking.

Example

*ocs**sp-checking*

Syntax

responder-url <*WEB_URL*>

Mode

OCSP Checking

Description

Configure responder URL.

Options

<*WEB_URL*> URL in the form: *http://host/file*.
Example: *http://www.example.com/products/*

Example

responder-url *http://www.sonicwall.com/ocsp*

Syntax

no responder-url

Mode

OCSP Checking

Description

Clear responder URL.

Example

no responder-url

Syntax

traps-on-change

Mode

VPN

Description

Enable VPN tunnel traps only when tunnel status changes.

Example

traps-on-change

Syntax

no traps-on-change

Mode

VPN

Description

Disable VPN tunnel traps only when tunnel status changes.

Example

no traps-on-change

Syntax

use-radius { mschap | mschapv2 }

Mode

VPN

Description

Enable use RADIUS in specified mode for XAUTH.

Options

mschap Use MSCHAP for RADIUS.

mschapv2 Use MSCHAPv2 for RADIUS.

Example

use-radius mschapv2

Syntax

no use-radius

Mode

VPN

Description

Disable use RADIUS for XAUTH.

Example

`no use-radius`

Syntax

```
dns server { inherit | static { primary <IPV4_HOST> | secondary <IPV4_HOST> | tertiary <IPV4_HOST> } }
```

Mode

VPN

Description

Manually set DNS settings or inherit DNS settings dynamically from the SonicWall's DNS settings.

Options

inherit Inherit DNS servers.

static Static DNS server.

primary Specify primary DNS server IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: `192.168.168.168`

secondary Specify secondary DNS server IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: `192.168.168.168`

tertiary Specify ternary DNS server IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: `192.168.168.168`

Example

```
dns server static primary 192.168.168.165  
dns server inherit
```

Syntax

```
no dns server static { primary | secondary | tertiary }
```

Mode

VPN

Description

Manually clear DNS server IP address.

Options

static Static DNS server.

primary Primary DNS server IP address.

secondary Secondary DNS server IP address.

tertiary Ternary DNS server IP address.

Example

```
no dns server primary
```

Syntax

```
wins { primary <IPV4_HOST> | secondary <IPV4_HOST> }
```

Mode

VPN

Description

Set the WINS server IP address.

Options

primary Primary WINS server IP address.
<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

secondary Secondary WINS server IP address.
<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
wins primary 192.168.168.169
```

Syntax

```
no wins { primary | secondary }
```

Mode

VPN

Description

Manually clear WINS server IP address.

Options

primary Primary WINS server IP address.

secondary Secondary WINS server IP address.

Example

```
no wins primary
```

Syntax

```
ikev2
```

Mode

VPN

Description

Configure IKEv2.

Example

```
ikev2
```

Syntax

```
send-cookie
```

Mode

IKEv2

Description

Enable send IKEv2 cookie notify.

Example

```
send-cookie
```

Syntax

```
no send-cookie
```

Mode

IKEv2

Description

Disable send IKEv2 cookie notify.

Example

```
no send-cookie
```

Syntax

```
send-invalid-spi
```

Mode

IKEv2

Description

Enable send IKEv2 invalid spi notify.

Example

```
send-invalid-spi
```

Syntax

```
no send-invalid-spi
```

Mode

IKEv2

Description

Disable send IKEv2 invalid spi notify.

Example

```
no send-invalid-spi
```

Syntax

```
proposal dh-group { 1 | 14 | 19 | 2 | 20 | 21 | 25 | 26 | 5 }
```

Mode

IKEv2

Description

Configure IKEv2 DH group.

Options

- 1** Group 1 modp768.
- 14** Group 14 modp2048.
- 19** Group 19 ECP random 256-bit.
- 2** Group 2 modp1024.
- 20** Group 20 ECP random 384-Bit.
- 21** Group 21 ECP random 521-Bit.
- 25** Group 25 ECP random 192-Bit.
- 26** Group 26 ECP random 224-Bit.
- 5** Group 5 modp1536.

Example

```
proposal dh-group 2
```

Syntax

```
proposal encryption { aes-128 | aes-192 | aes-256 | des | triple-des }
```

Mode

IKEv2

Description

Configure IKEv2 encryption algorithm.

Options

- aes-128** Advanced encryption standard (AES) - 128 bit.
- aes-192** Advanced encryption standard (AES) - 192 bit.
- aes-256** Advanced encryption standard (AES) - 256 bit.
- des** Data encryption standard (DES).
- triple-des** Triple data encryption standard (3DES).

Example

```
proposal encryption aes-128
```

Syntax

```
proposal authentication { md5 | sha-1 | sha-256 | sha-384 | sha-512 }
```

Mode

IKEv2

Description

Configure IKEv2 authentication hashing algorithm.

Options

- md5** Message-digest algorithm 5 (MD5).
- sha-1** Secure hash algorithm 1 (SHA-1).
- sha-256** Secure hash algorithm 256 (SHA-256).
- sha-384** Secure hash algorithm 384 (SHA-384).
- sha-512** Secure hash algorithm 512 (SHA-512).

Example

```
proposal authentication md5
```

Syntax

```
policy { [ ipv4 ] { { group-vpn <VPN_GROUP_POLICY_NAME> | site-to-site <VPN_SITE_POLICY_NAME> | tunnel-interface <VPN_TUNNEL_POLICY_NAME> } } | enable <VPN_POLICY_NAME> | ipv6 { site-to-site <VPN_SITE_POLICY_V6_NAME> } }
```

Mode

VPN

Description

Add, edit or enable a VPN policy.

Options

- ipv4** IPv4 vpn policy.
- group-vpn** Edit group VPN policy.
<VPN_GROUP_POLICY_NAME> Group VPN policy name.
Example: *WAN GroupVPN*
- site-to-site** Add or edit site-to-site VPN policy.
<VPN_SITE_POLICY_NAME> Site-to-site VPN policy name.
Example: *Remote Office*
- tunnel-interface** Add or edit tunnel interface VPN policy.
<VPN_TUNNEL_POLICY_NAME> Tunnel interface VPN policy name.
Example: *Remote Office*
- enable** Enable a VPN policy.
<VPN_POLICY_NAME> VPN policy name.
Example: *Remote Office*
- ipv6** IPv6 vpn policy.
- site-to-site** Delete IPv6 site-to-site VPN policy.
<VPN_SITE_POLICY_V6_NAME> IPv6 Site-to-site VPN policy name.
Example: *Remote Office*

Example

```
policy site-to-site "Remote Office"  
policy group-vpn "WAN GroupVPN"  
policy enable "Remote Office"
```

Syntax

```
no policy { [ ipv4 ] { { site-to-site <VPN_SITE_POLICY_NAME> | tunnel-interface <VPN_TUNNEL_POLICY_NAME> } } | enable <VPN_POLICY_NAME> | ipv6 { site-to-site <VPN_SITE_POLICY_V6_NAME> } }
```

Mode

VPN

Description

Delete or disable a VPN policy.

Options

| | |
|--|---|
| ipv4 | IPv4 vpn policy. |
| site-to-site <VPN_SITE_POLICY_NAME> | Delete site-to-site VPN policy. Site-to-site VPN policy name. Example: <i>Remote Office</i> |
| tunnel-interface <VPN_TUNNEL_POLICY_NAME> | Delete tunnel interface VPN policy. Tunnel interface VPN policy name. Example: <i>Remote Office</i> |
| enable <VPN_POLICY_NAME> | Enable a VPN policy. VPN policy name. Example: <i>Remote Office</i> |
| ipv6 site-to-site <VPN_SITE_POLICY_V6_NAME> | IPv6 vpn policy. Delete IPv6 site-to-site VPN policy. IPv6 Site-to-site VPN policy name. Example: <i>Remote Office</i> |

Example

```
no policy site-to-site "Remote Office"  
no policy enable "Remote Office"
```

Syntax

```
no policies
```

Mode

VPN

Description

Delete all VPN policies.

Example

```
no policies
```

Syntax

```
name <VPN_POLICY_NAME>
```

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN

Description

Configure policy name.

Options

<VPN_POLICY_NAME> VPN policy name.

Example

```
name "Remote Office"
```

Syntax

```
name <VPN_SITE_POLICY_V6_NAME>
```

Mode

Site to Site VPN IPv6 Policy

Description

Configure policy name.

Options

<VPN_SITE_POLICY_V6_NAME> IPv6 Site-to-site VPN policy name.
Example: *Remote Office*

Example

```
name "Remote Office"
```

Syntax

```
enable
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN

Description

Enable VPN policy.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN

Description

Disable VPN policy.

Example

```
no enable
```

Syntax


```
gateway primary <HOSTNAME_MIXED>
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Configure the IPsec gateway name or address.

Options

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

```
gateway primary 10.10.10.1
```

Syntax

```
no gateway primary
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Clear the IPsec gateway name or address.

Example

```
no gateway primary
```

Syntax

```
gateway secondary <HOSTNAME_MIXED>
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Configure the IPsec gateway name or address.

Options

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

```
gateway secondary 10.10.10.1
```

Syntax

```
no gateway secondary
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Clear the IPsec gateway name or address.

Example

```
no gateway secondary
```

Syntax

```
auth-method { certificate | manual-key | shared-secret }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Configure VPN policy authentication method.

Options

certificate IKE using 3rd party certificates.

manual-key Manual key.

shared-secret IKE using pre-shared secret.

Example

```
auth-method shared-secret
```

Syntax

```
auth-method { certificate | shared-secret }
```

Mode

Group VPN

Description

Configure VPN policy authentication method.

Options

certificate IKE using 3rd party certificates.

shared-secret IKE using pre-shared secret.

Example

```
auth-method shared-secret
```

Syntax

```
export group-vpn <VPN_GROUP_POLICY_ENABLE_NAME> { rcf { network { group <VPN_ADDR_GROUP_NAME> | name <VPN_ADDR_NAME> } [ password <WORD> ] { ftp <FTP_URL> } } | spd ftp <FTP_URL> }
```

Mode

VPN

Description

Export a group VPN client policy file to FTP server.

Options

| | |
|---|---|
| <VPN_GROUP_POLICY_ENABLE_NAME> | Group VPN policy name. Example: <i>WAN GroupVPN</i> |
| rcf | Ref format is required for Global VPN Clients. |
| network | Configure the client access network(s) you wish to export. |
| group | Select the network to named address object group. |
| <VPN_ADDR_GROUP_NAME> | Group address object name. Example: <i>Sales Group</i> |
| name | Select the network to named address object. |
| <VPN_ADDR_NAME> | Host/network/range address object name. Example: <i>Web Server</i> |
| password | You may encrypt the exported file using a chosen password. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| ftp | Export using the FTP protocol. |
| <FTP_URL> | FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/nftp://username@hostname/nftp://hostname/</i> |
| spd | Spd format is required for VPN Clients 8.x and earlier. |
| ftp | Export using the FTP protocol. |
| <FTP_URL> | FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/nftp://username@hostname/nftp://hostname/</i> |

Example

```
export group-vpn WAN\\ GroupVPN rcf network name LANSubnets ftp ftp://user:password@servername/WAN\\ GroupVPN.rcf
```

Syntax

```
shared-secret <ENC_PASSWORD>
```

Mode

IKE Preshared Secret

Description

Configure the pre-shared secret.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
shared-secret mysecret
```

Syntax

```
no shared-secret
```

Mode

IKE Preshared Secret

Description

Clear the pre-shared secret.

Example

no shared-secret

Syntax

```
ike-id local { domain-name <VPN_FQDN> | email-address <EMAIL> | firewall-id <WORD> | ipv4 <IPV4_HOST> | ipv6 <IPV6_HOST> | key-id <WORD> }
```

Mode

IKE Preshared Secret

Description

Configure local IKE authentication associated identifiers.

Options

| | |
|--------------------------|---|
| domain-name | Domain name identifier. |
| <VPN_FQDN> | Domain name in the form: aaa.aa. Example: <i>example.com</i> |
| email-address | E-mail address identifier. |
| <EMAIL> | E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i> |
| firewall-id | Firewall identifier. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| ipv4 | IP address identifier. |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |
| ipv6 | IPv6 address identifier. |
| <IPV6_HOST> | IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i> |
| key-id | Key ID identifier. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

Example

```
ike-id local email-address user@domain.com
```

Syntax

```
no ike-id local { domain-name | email-address | firewall-id | ipv4 | ipv6 | key-id }
```

Mode

IKE Preshared Secret

Description

Clear local IKE authentication associated identifiers.

Options

| | |
|----------------------|----------------------------------|
| domain-name | Clear domain name identifier. |
| email-address | Clear e-mail address identifier. |
| firewall-id | Clear Firewall ID identifier. |
| ipv4 | Clear IPv4 address identifier. |

ipv6 Clear IPv6 address identifier.

key-id Clear key ID identifier.

Example

```
no ike-id local email-address
```

Syntax

```
ike-id peer { domain-name <VPN_FQDN> | email-address <EMAIL> | firewall-id <WORD> | ipv4 <IPV4_HOST> | ipv6 <IPV6_HOST> | key-id <WORD> }
```

Mode

IKE Preshared Secret

Description

Configure peer IKE authentication associated identifiers.

Options

domain-name Domain name identifier.

<VPN_FQDN> Domain name in the form: aaa.aa.
Example: *example.com*

email-address E-mail address identifier.

<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

firewall-id Firewall ID identifier.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

ipv4 IP address identifier.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

ipv6 IPv6 address identifier.

<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

key-id Key ID identifier.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ike-id peer email-address user@domain.com
```

Syntax

```
no ike-id peer { domain-name | email-address | firewall-id | ipv4 | ipv6 | key-id }
```

Mode

IKE Preshared Secret

Description

Clear peer IKE authentication associated identifiers.

Options

domain-name Clear domain name identifier.

email-address Clear e-mail address identifier.

firewall-id Clear Firewall ID identifier.

ipv4 Clear IPv4 address identifier.

ipv6 Clear IPv6 address identifier.

key-id Clear key ID identifier.

Example

```
no ike-id peer email-address
```

Syntax

```
certificate <CERT_NAME>
```

Mode

IKE 3rd Party Certificate
IKE 3rd Party Certificate

Description

Configure the local certificate name.

Options

<CERT_NAME> Certificate name.
Example: *my_cert*

Example

```
certificate mycertificate
```

Syntax

```
no certificate
```

Mode

IKE 3rd Party Certificate
IKE 3rd Party Certificate

Description

Clear the local certificate name.

Example

```
no certificate
```

Syntax

```
ike-id local { default-id | distinguished-name | domain-name | email-id | ip }
```

Mode

IKE 3rd Party Certificate

Description

Configure the local identifier.

Options

| | |
|---------------------------|----------------------------------|
| default-id | Default ID from the certificate. |
| distinguished-name | Distinguished name (DN). |
| domain-name | Domain name (FQDN). |
| email-id | E-mail ID (userFQDN). |
| ip | IP address (IPV4). |

Example

```
ike-id local default-id
```

Syntax

```
ike-id peer { distinguished-name <DISTINGUISHED_NAME> | domain-name <VPN_FQDN> | email-id <EMAIL> | ip <IPV4_HOST> }
```

Mode

IKE 3rd Party Certificate

Description

Configure the peer identifier.

Options

| | |
|-----------------------------------|---|
| distinguished-name | Distinguished name (DN). |
| <DISTINGUISHED_NAME> | Distinguished name filter in the form: c=*,cn=*,o=*,ou=*, or *. Example: <i>ou=aaa;c=a;*</i> |
| domain-name | Domain name (FQDN). |
| <VPN_FQDN> | Domain name in the form: aaa.aa. Example: <i>example.com</i> |
| email-id | E-mail ID (userFQDN). |
| <EMAIL> | E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i> |
| ip | IP address (IPV4). |
| <IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |

Example

```
ike-id peer distinguished-name
```

Syntax

```
no ike-id peer { distinguished-name | domain-name | email-id | ip }
```

Mode

IKE 3rd Party Certificate

Description

Clear the peer identifier.

Options

| | |
|---------------------------|--------------------------------|
| distinguished-name | Clear distinguished name (DN). |
| domain-name | Clear domain name (FQDN). |

email-id Clear e-mail ID (userFQDN).

ip Clear IP address (IPv4).

Example

```
no ike-id peer distinguished-name
```

Syntax

```
peer id { distinguished-name <DISTINGUISHED_NAME> | domain-name <VPN_FQDN_FILTER> | email-id <VPN_EMAIL_FILTER> }
```

Mode

IKE 3rd Party Certificate

Description

Configure the peer identifier type.

Options

distinguished-name Distinguished name.
<DISTINGUISHED_NAME> Distinguished name filter in the form: c=*;cn=*;o=*;ou=*; or *.
Example: *ou=aaa;c=a;**

domain-name Domain name.
<VPN_FQDN_FILTER> Domain name filter in the form: aabb?*-aa.
Example: *example.com*

email-id E-mail ID.
<VPN_EMAIL_FILTER> E-mail filter in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

Example

```
peer id-type domain-name example.com
```

Syntax

```
peer match-issuer
```

Mode

IKE 3rd Party Certificate

Description

Enable allow only peer certificates signed by gateway issuer.

Example

```
peer match-issuer
```

Syntax

```
no peer match-issuer
```

Mode

IKE 3rd Party Certificate

Description

Disable allow only peer certificates signed by gateway issuer.

Example

```
no peer match-issuer
```

Syntax

```
network local { any | dhcp | group <VPN_ADDR_GROUP_NAME> | host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Configure the local network.

Options

| | |
|---|--|
| any | Any local network. |
| dhcp | Obtain IP addresses using DHCP through this VPN tunnel. |
| group <VPN_ADDR_GROUP_NAME> | Configure the local network to named address object group. Group address object name. Example: <i>Sales Group</i> |
| host <VPN_ADDR_HOST> | Configure the local network to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <VPN_ADDR_NAME> | Configure the local network to named address object. Host/network/range address object name. Example: <i>Web Server</i> |
| network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | Configure the local network to network address. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <VPN_ADDR_BEGIN> <VPN_ADDR_END> | Configure the local network to range of addresses. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
network local name LANSubnets
```

Syntax

```
no network local
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Clear the local network.

Example

```
no network local
```

Syntax

```
network remote { any | dhcp | group <VPN_ADDR_GROUP_NAME> | host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Configure the remote network.

Options

| | |
|---|---|
| any | Use this VPN tunnel as default route for all internet traffic. |
| dhcp | Destination network obtains IP addresses using DHCP through this VPN tunnel. |
| group <VPN_ADDR_GROUP_NAME> | Configure the remote network to named address object group. Group address object name. Example: <i>Sales Group</i> |
| host <VPN_ADDR_HOST> | Configure the remote network to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <VPN_ADDR_NAME> | Configure the remote network to named address object. Host/network/range address object name. Example: <i>Web Server</i> |
| network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | Configure the remote network to network address. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| range <VPN_ADDR_BEGIN> <VPN_ADDR_END> | Configure the remote network to range of addresses. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |

Example

```
network remote name RemoteSubnets
```

Syntax

```
no network remote
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Clear the remote network.

Example

```
no network remote
```

Syntax

```
proposal ike { authentication { { md5 | sha-1 | sha-256 | sha-384 | sha-512 } } | dh-group { { 1 | 14 | 19 | 2 | 20 | 21 | 25 | 26 | 5 } } | encryption { { aes-128 | aes-192 | aes-256 | des | triple-des } } | exchange { { aggressive | ikev2 | main } } | lifetime <UINT32> }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN

Description

Configure VPN policy IKE (phase 1) proposal.

Options

authentication Authentication hashing encryption algorithm.

md5 Message-digest algorithm 5 (MD5).

sha-1 Secure hash algorithm 1 (SHA-1).

sha-256 Secure hash algorithm 256 (SHA-256).

sha-384 Secure hash algorithm 384 (SHA-384).

sha-512 Secure hash algorithm 512 (SHA-512).

dh-group DH group.

1 Group 1 modp768.

14 Group 14 modp2048.

19 Group 19 ECP random 256-bit.

2 Group 2 modp1024.

20 Group 20 ECP random 384-Bit.

21 Group 21 ECP random 521-Bit.

25 Group 25 ECP random 192-Bit.

26 Group 26 ECP random 224-Bit.

5 Group 5 modp1536.

encryption Encryption algorithm.

aes-128 Advanced encryption standard (AES) - 128 bit.

aes-192 Advanced encryption standard (AES) - 192 bit.

aes-256 Advanced encryption standard (AES) - 256 bit.

des Data encryption standard (DES).

triple-des Triple data encryption standard (3DES).

| | |
|-----------------------|---|
| exchange | Exchange. |
| aggressive | Aggressive mode. |
| ikev2 | IKEv2 mode. |
| main | Main mode. |
| lifetime | Life time (seconds). |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: 123 |

Example

```
proposal ike encryption aes-256
proposal ike authentication sha-1
proposal ike dh-group 2
proposal ike lifetime 3000
```

Syntax

```
proposal ipsec { authentication { { aes-xcbc | md5 | sha-1 | sha-256 | sha-384 | sha-512 } } | authentication-key
<VPN_HEX_STRING128> | encryption { { aes-128 | aes-192 | aes-256 | aes-gcm16-128 | aes-gcm16-192 | aes-gcm16-256 | aes-gmac-128 |
aes-gmac-192 | aes-gmac-256 | des | triple-des } } | encryption-key <VPN_HEX_STRING128> | in-authentication-key
<VPN_HEX_STRING128> | in-encryption-key <VPN_HEX_STRING128> | in-spi <VPN_HEX_UINT32> | lifetime <UINT32> | out-authentication-key
<VPN_HEX_STRING128> | out-encryption-key <VPN_HEX_STRING128> | out-spi <VPN_HEX_UINT32> | perfect-forward-secrecy dh-group { { 1 |
14 | 19 | 2 | 20 | 21 | 25 | 26 | 5 } } | protocol { { ah | esp } } }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN

Description

Configure VPN policy IPsec (phase 2) proposal.

Options

| | |
|---|--|
| authentication | Authentication hashing encryption algorithm. |
| aes-xcbc | Secure hash algorithm AES (AES-XCBC). |
| md5 | Message-digest algorithm 5 (MD5). |
| sha-1 | Secure hash algorithm 1 (SHA-1). |
| sha-256 | Secure hash algorithm 256 (SHA-256). |
| sha-384 | Secure hash algorithm 384 (SHA-384). |
| sha-512 | Secure hash algorithm 512 (SHA-512). |
| authentication-key <VPN_HEX_STRING128> | Configure authentication key. String of hexadecimal (16-128) digits. Example: 0123456989abcdef |
| encryption | Encryption algorithm. |
| aes-128 | Advanced encryption standard (AES) - 128 bit. |
| aes-192 | Advanced encryption standard (AES) - 192 bit. |
| aes-256 | Advanced encryption standard (AES) - 256 bit. |
| aes-gcm16-128 | Advanced encryption standard (AES) - GCM16 128 bit. |

| | |
|----------------------------------|---|
| aes-gcm16-192 | Advanced encryption standard (AES) - GCM16 192 bit. |
| aes-gcm16-256 | Advanced encryption standard (AES) - GCM16 256 bit. |
| aes-gmac-128 | Advanced encryption standard (AES) - GMAC 128 bit. |
| aes-gmac-192 | Advanced encryption standard (AES) - GMAC 192 bit. |
| aes-gmac-256 | Advanced encryption standard (AES) - GMAC 256 bit. |
| des | Data encryption standard (DES). |
| triple-des | Triple data encryption standard (3DES). |
| encryption-key | Configure encryption key. |
| <VPN_HEX_STRING128> | String of hexadecimal (16-128) digits. Example: <i>0123456989abcdef</i> |
| in-authentication-key | Configure incoming authentication key. |
| <VPN_HEX_STRING128> | String of hexadecimal (16-128) digits. Example: <i>0123456989abcdef</i> |
| in-encryption-key | Configure incoming encryption key. |
| <VPN_HEX_STRING128> | String of hexadecimal (16-128) digits. Example: <i>0123456989abcdef</i> |
| in-spi | Configure incoming SPI. |
| <VPN_HEX_UINT32> | Hexadecimal integer in the form: 0xHHHHHHHHH. Example: <i>0xaa55aa55</i> |
| lifetime | Life time (seconds). |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i> |
| out-authentication-key | Configure outgoing authentication key. |
| <VPN_HEX_STRING128> | String of hexadecimal (16-128) digits. Example: <i>0123456989abcdef</i> |
| out-encryption-key | Configure outgoing encryption key. |
| <VPN_HEX_STRING128> | String of hexadecimal (16-128) digits. Example: <i>0123456989abcdef</i> |
| out-spi | Configure outgoing SPI. |
| <VPN_HEX_UINT32> | Hexadecimal integer in the form: 0xHHHHHHHHH. Example: <i>0xaa55aa55</i> |
| perfect-forward-secrecy | Enable perfect forward secrecy. |
| dh-group | DH group. |
| 1 | Group 1 modp768. |
| 14 | Group 14 modp2048. |
| 19 | Group 19 ECP random 256-bit. |
| 2 | Group 2 modp1024. |
| 20 | Group 20 ECP random 384-Bit. |
| 21 | Group 21 ECP random 521-Bit. |
| 25 | Group 25 ECP random 192-Bit. |
| 26 | Group 26 ECP random 224-Bit. |
| 5 | Group 5 modp1536. |
| protocol | Protocol. |

ah Configure AH.
esp Configure ESP.

Example

```
proposal ipsec encryption aes-256  
proposal ipsec authentication sha-1  
proposal ipsec perfect-forward-secrecy dh-group 2  
proposal ipsec lifetime 3000
```

Manual Key Only:

```
proposal ipsec in-spi 0x5dlb19a1  
proposal ipsec out-spi 0x88f24984  
proposal ipsec encryption-key 5f7cd04166523fd78e56ca9920d9c870d53ed63d92001d4f  
proposal ipsec authentication-key 3b1db664fe578ae5fd38d7042e7a106f4c23408a
```

Syntax

```
no proposal ipsec { authentication | authentication-key | encryption | encryption-key | perfect-forward-secrecy }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN

Description

Clear VPN policy IPsec (phase 2) proposal.

Options

authentication None authentication hashing encryption algorithm.
authentication-key Configure authentication key.
encryption None encryption algorithm.
encryption-key Configure encryption key.
perfect-forward-secrecy Disable perfect forward secrecy.

Example

```
no proposal ipsec encryption-key  
no proposal ipsec authentication-key  
no proposal ipsec encryption  
no proposal ipsec authentication  
no proposal ipsec perfect-forward-secrecy
```

Syntax

```
client cache-xauth { always | never | single-session }
```

Mode

Group VPN

Description

Configure cache XAUTH user name and password on client.

Options

always Always cache.
never No caching.

single-session Cache for single session.

Example

```
client cache-xauth single-session
```

Syntax

```
client virtual-adaptor { dhcp-and-manual | dhcp-only | none }
```

Mode

Group VPN

Description

Configure virtual adaptor lease settings.

Options

dhcp-and-manual Use DHCP lease or manual configuration.

dhcp-only Use DHCP lease.

none None.

Example

```
client virtual-adaptor dhcp-only
```

Syntax

```
client allow-connections-to { all-secured-gateways | split-tunnels | this-gateway-only }
```

Mode

Group VPN

Description

Configure what connections to allow to.

Options

all-secured-gateways All secured gateways.

split-tunnels Split tunnels.

this-gateway-only This gateway only.

Example

```
client allow-connections-to this-gateway-only
```

Syntax

```
client default-route { access-list | disable-acl }
```

Mode

Group VPN

Description

Configure default route as this gateway.

Options

access-list Enable apply VPN access control list.

disable-acl Disable apply VPN access control list.

Example

```
client default-route access-list
```

Syntax

```
no client default-route
```

Mode

Group VPN

Description

Clear default route as this gateway.

Example

```
no client default-route
```

Syntax

```
client simple-provisioning
```

Mode

Group VPN

Description

Enable use default key for simple client provisioning.

Example

```
client simple-provisioning
```

Syntax

```
no client simple-provisioning
```

Mode

Group VPN

Description

Disable use default key for simple client provisioning.

Example

```
no client simple-provisioning
```

Syntax

```
keep-alive
```


Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Enable VPN policy keep alive.

Example

```
keep-alive
```

Syntax

```
no keep-alive
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Disable VPN policy keep alive.

Example

```
no keep-alive
```

Syntax

```
suppress-auto-add-rule
```

Mode

Site to Site VPN Policy

Description

Enable suppress automatic access rules creation for VPN policy.

Example

```
suppress-auto-add-rule
```

Syntax

```
no suppress-auto-add-rule
```

Mode

Site to Site VPN Policy

Description

Disable suppress automatic access rules creation for VPN policy.

Example

```
no suppress-auto-add-rule
```

Syntax

```
require-xauth <LOCAL_USER_GROUP_NAME>
```

Mode

Site to Site VPN Policy

Description

Enable XAUTH checking for VPN policy.

Options

`<LOCAL_USER_GROUP_NAME>` Local user group object name.
Example: *Limited Administrators*

Example

```
require-xauth "Everyone"
```

Syntax

```
no require-xauth
```

Mode

Site to Site VPN Policy

Description

Disable require authentication of VPN clients by XAUTH.

Example

```
no require-xauth
```

Syntax

```
anti-replay
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN

Description

Enable anti replay.

Example

```
anti-replay
```

Syntax

```
no anti-replay
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN

Description

Disable anti replay.

Example

```
no anti-replay
```

Syntax

advanced-routing

Mode

Tunnel Interface VPN Policy

Description

Enable allow advanced routing.

Example

advanced-routing

Syntax

no advanced-routing

Mode

Tunnel Interface VPN Policy

Description

Disable allow advanced routing.

Example

no advanced-routing

Syntax

transport-mode

Mode

Tunnel Interface VPN Policy

Description

Enable transport mode.

Example

transport-mode

Syntax

no transport-mode

Mode

Tunnel Interface VPN Policy

Description

Disable transport mode.

Example

no transport-mode

Syntax

netbios

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy

Description

Enable VPN policy NetBIOS.

Example

netbios

Syntax

no netbios

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy

Description

Disable VPN policy NetBIOS.

Example

no netbios

Syntax

multicast

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN

Description

Enable VPN policy multicast.

Example

multicast

Syntax

no multicast

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN

Description

Disable VPN policy multicast.

Example

no multicast

Syntax

permit-acceleration

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN

Description

Enable permit acceleration.

Example

permit-acceleration

Syntax

no permit-acceleration

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN

Description

Disable permit acceleration.

Example

no permit-acceleration

Syntax

wxa-group <WXA_GROUP_NAME>

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy

Description

Configure WXA group.

Options

<WXA_GROUP_NAME> WXA group name.
Example: *Group One*

Example

wxa-group "Group One"

Syntax

no wxa-group

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy

Description

Clear WXA group.

Example

```
no wxa-group
```

Syntax

```
apply-nat [ translated-local { group <VPN_ADDR_GROUP_NAME> | host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | original | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> } ] [ translated-remote { group <VPN_ADDR_GROUP_NAME> | host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | original | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> } ]
```

Mode

Site to Site VPN Policy

Description

Enable VPN policy NAT translation.

Options

| | |
|---|--|
| translated-local | Translated local network. |
| group <VPN_ADDR_GROUP_NAME> | Configure the local network to named address object group. Group address object name. Example: <i>Sales Group</i> |
| host <VPN_ADDR_HOST> | Host IP. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <VPN_ADDR_NAME> | Address object name. Host/network/range address object name. Example: <i>Web Server</i> |
| network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | Network address. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i> |
| original | Original translated local network. |
| range <VPN_ADDR_BEGIN> <VPN_ADDR_END> | Network range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| translated-remote | Translated remote network. |
| group <VPN_ADDR_GROUP_NAME> | Configure the local network to named address object group. Group address object name. Example: <i>Sales Group</i> |
| host <VPN_ADDR_HOST> | Host IP. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <VPN_ADDR_NAME> | Address object name. Host/network/range address object name. Example: <i>Web Server</i> |
| network | Network address. |

<VPN_ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<VPN_ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

original Original translated remote network.

range Network range.

<VPN_ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<VPN_ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
apply-nat translated-local name "TranslatedLocalAddrs"
apply-nat translated-remote name "TranslatedRemoteAddrs"
```

Syntax

```
no apply-nat
```

Mode

Site to Site VPN Policy

Description

Disable VPN policy NAT parameters.

Example

```
no apply-nat
```

Syntax

```
no oosp-checking
```

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN

Description

Disable OSCP checking.

Example

```
no oosp-checking
```

Syntax

```
oosp-checking
```

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN

Description

Enable and configure OSCP checking.

Example

```
ocsp-checking
```

Syntax

```
responder-url <WEB_URL>
```

Mode

OCSP Checking

Description

Configure responder URL.

Options

<WEB_URL> URL in the form: http://host/file.
Example: http://www.example.com/products/

Example

```
responder-url http://www.sonicwall.com/ocsp
```

Syntax

```
no responder-url
```

Mode

OCSP Checking

Description

Clear responder URL.

Example

```
no responder-url
```

Syntax

```
management { http | https | snmp | ssh }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN

Description

Enable management for VPN policy.

Options

http Enable HTTP management for VPN policy.

https Enable HTTPS management for VPN policy.

snmp Enable SNMP management for VPN policy.

ssh Enable SSH management for VPN policy.

Example

management https

Syntax

```
no management { http | https | snmp | ssh }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN

Description

Disable management for VPN policy.

Options

http Disable HTTP management for VPN policy.

https Disable HTTPS management for VPN policy.

snmp Disable SNMP management for VPN policy.

ssh Disable SSH management for VPN policy.

Example

```
no management https
```

Syntax

```
user-login { http | https }
```

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy

Description

Enable VPN policy for user login.

Options

http Enable VPN policy for HTTP user login.

https Enable VPN policy for HTTPS user login.

Example

```
user-login http
```

Syntax

```
no user-login { http | https }
```

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy

Description

Disable VPN policy for user login.

Options

http Disable VPN policy for HTTP user login.

https Disable VPN policy for HTTPS user login.

Example

```
no user-login http
```

Syntax

```
default-lan-gateway <IPV4_HOST>
```

Mode

Site to Site VPN Policy
Group VPN

Description

Configure LAN default gateway.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
default-lan-gateway 192.168.168.1
```

Syntax

```
no default-lan-gateway
```

Mode

Site to Site VPN Policy
Group VPN

Description

Clear LAN default gateway.

Example

```
no default-lan-gateway
```

Syntax

```
bound-to { interface <VPN_BOUND_TO_INTERFACE> | zone <ZONE_WAN_NAME> }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Configure VPN policy bound to.

Options

interface Bound to interface.

<VPN_BOUND_TO_INTERFACE> Interface name.
Example: *X0*

zone Bound to zone.
<ZONE_WAN_NAME> Zone object name.
Example: *DMZ*

Example

```
bound-to interface X1
```

Syntax

```
local-ip { custom <IPV6_HOST> | primary }
```

Mode

Site to Site VPN IPv6 Policy

Description

Set the local gateway ip address.

Options

custom Specify the Local Gateway IP address.
<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

primary Using Primary IP address.

Example

```
local-ip custom 4::5
```

Syntax

```
group { 1 | 2 | 3 | 4 }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Configure VPN policy group.

Options

1 Bound to group 1.

2 Bound to group 2.

3 Bound to group 3.

4 Bound to group 4.

Example

```
group 1
```

Syntax

`preempt-secondary-gateway <UINT32>`

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Enable preempt secondary gateway and set primary gateway detection interval (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
preempt-secondary-gateway 28800
```

Syntax

```
no preempt-secondary-gateway
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Disable preempt secondary gateway.

Example

```
no preempt-secondary-gateway
```

Syntax

```
client-authentication { allow-unauthenticated { { group <VPN_ADDR_GROUP_NAME> | host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> |  
network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> } } | require-xauth <LOCAL_USER_GROUP_NAME> }
```

Mode

Group VPN

Description

Enable XAUTH checking for VPN policy.

Options

allow-unauthenticated Enable unauthenticated access for VPN policy.

group Configure the remote network to named address object group.

<VPN_ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Host IP.

<VPN_ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<VPN_ADDR_NAME> Host/network/range address object name.
Example: *Web Server*

network Network address.

<VPN_ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.

Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<VPN_ADDR_MASK> IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n.
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range Network range.

<VPN_ADDR_BEGIN> IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<VPN_ADDR_END> IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

require-xauth Enable XAUTH checking for VPN policy.

<LOCAL_USER_GROUP_NAME> Local user group object name.
Example: *Limited Administrators*

Example

```
client-authentication require-xauth "Everyone"
```

Syntax

```
suppress-trigger-packet
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Do not send trigger packet during IKE SA negotiation for IKEv2.

Example

```
suppress-trigger-packet
```

Syntax

```
no suppress-trigger-packet
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Send trigger packet during IKE SA negotiation for IKEv2.

Example

```
no suppress-trigger-packet
```

Syntax

```
accept-hash
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Accept hash & URL certificate type for IKEv2.

Example

accept-hash

Syntax

no accept-hash

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Do not accept hash & URL certificate type for IKEv2.

Example

no accept-hash

Syntax

send-hash <WEB_URL>

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Enable send hash & URL certificate type for IKEv2 and specify url.

Options

<WEB_URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

send-hash <ikev2CertUrl>

Syntax

no send-hash

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Do not send hash & URL certificate type for IKEv2.

Example

no send-hash

Syntax

accept-multiple-proposals

Mode

Group VPN

Description

Enable accept multiple proposals for clients.

Example

```
accept-multiple-proposals
```

Syntax

```
no accept-multiple-proposals
```

Mode

Group VPN

Description

Disable accept multiple proposals for clients.

Example

```
no accept-multiple-proposals
```

Syntax

```
ike-mode-configuration { expiry-time <UINT32> | ip-pool { host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> } }
```

Mode

Group VPN

Description

Enable IKE Mode Configuration.

Options

| | |
|--------------------------------------|--|
| expiry-time <UINT32> | Address Expiry Time(seconds). Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |
| ip-pool | IP Pool for Clients. |
| host <VPN_ADDR_HOST> | Host IP. IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n |
| name <VPN_ADDR_NAME> | Address Object name. Host/network/range address object name. Example: Web Server |
| network <VPN_ADDR_NETWORK> | Network Address. IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.168.0\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n |
| <VPN_ADDR_MASK> | IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n. Example: IPV4: 255.255.255.0\nIPV6: /64\n |
| range <VPN_ADDR_BEGIN> | Network Range. IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n |
| <VPN_ADDR_END> | IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. |

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n

Example

```
ike-mode-configuration ip-pool name "IpPoolClientAddr"  
ike-mode-configuration expiry-time 3600
```

Syntax

```
no ike-mode-configuration
```

Mode

Group VPN

Description

Disable IKE Mode Configuration.

Example

```
no ike-mode-configuration
```

Syntax

```
allow-sonicpointn-layer3
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Allow SonicPointN layer 3 management.

Example

```
allow-sonicpointn-layer3
```

Syntax

```
no allow-sonicpointn-layer3
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Disallow SonicPointN layer 3 management.

Example

```
no allow-sonicpointn-layer3
```

Syntax

```
l2tp-server
```

Mode

VPN

Description

Enable/Configure L2TP Server.

Example

```
l2tp-server
```

Syntax

```
no l2tp-server
```

Mode

VPN

Description

Disable l2tp-server.

Example

```
no l2tp-server
```

Syntax

```
keep-alive <UINT32>
```

Mode

L2TP Server

Description

Set the Keep alive time (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
keep-alive 10
```

Syntax

```
dns { primary <IPV4_HOST> | secondary <IPV4_HOST> }
```

Mode

L2TP Server

Description

Set the primary and secondary DNS server IP address.

Options

primary Primary DNS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

secondary Secondary DNS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
dns primary 192.168.168.169
```

Syntax

```
no dns { primary | secondary }
```

Mode

L2TP Server

Description

Manually Clear DNS server IP address.

Options

primary Clear primary DNS server IP address.

secondary Clear secondary DNS server IP address.

Example

```
no dns primary
```

Syntax

```
wins { primary <IPV4_HOST> | secondary <IPV4_HOST> }
```

Mode

L2TP Server

Description

Set the WINS server IP address.

Options

primary Primary WINS server IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

secondary Secondary WINS server IP address.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
wins primary 192.168.168.169
```

Syntax

```
no wins { primary | secondary }
```

Mode

L2TP Server

Description

Clear the WINS server IP address.

Options

primary Primary WINS server IP address.

secondary Secondary WINS server IP address.

Example

```
no wins primary
```

Syntax

```
ip-pool { local <IPV4_HOST> <IPV4_HOST> | provided }
```

Mode

L2TP Server

Description

Set the IP address pool.

Options

local Use local L2TP IP pool.

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

provided IP address provided by RADIUS/LDAP Server.

Example

```
ip-pool local 192.168.168.10 192.168.168.20
```

Syntax

```
no user-group
```

Mode

L2TP Server

Description

No L2TP user group.

Example

```
no user-group
```

Syntax

```
user-group <LOCAL_USER_GROUP_NAME>
```

Mode

L2TP Server

Description

Set user group for L2TP users.

Options

<LOCAL_USER_GROUP_NAME> Local user group object name.
Example: *Limited Administrators*

Example

```
user-group l2tpUsers
```

Syntax

```
dhcp-over-vpn { central | remote }
```

Mode

VPN

Description

Configure DHCP over VPN.

Options

central Configure DHCP over VPN for central gateway.

remote Configure DHCP over VPN for remote gateway.

Example

```
dhcp-over-vpn central
```

Syntax

```
internal-dhcp
```

Mode

Central

Description

Enable use internal DHCP server.

Example

```
internal-dhcp
```

Syntax

```
no internal-dhcp
```

Mode

Central

Description

Disable use internal DHCP server.

Example

```
no internal-dhcp
```

Syntax

```
global-vpn
```

Mode

Central

Description

Enable use internal DHCP server for global VPN client.

Example

```
global-vpn
```

Syntax

```
no global-vpn
```

Mode

Central

Description

Disable use internal DHCP server for global VPN client.

Example

```
no global-vpn
```

Syntax

```
remote
```

Mode

Central

Description

Enable use internal DHCP server for remote firewall.

Example

```
remote
```

Syntax

```
no remote
```

Mode

Central

Description

Disable use internal DHCP server for remote firewall.

Example

```
no remote
```

Syntax

```
send-requests
```

Mode

Central

Description

Enable send DHCP requests to the server addresses in the server list.

Example

```
send-requests
```

Syntax

```
no send-requests
```

Mode

Central

Description

Disable send DHCP requests to the server addresses in the server list.

Example

```
no send-requests
```

Syntax

```
dhcp-server <DHCP_SERVER_IPV4_HOST>
```

Mode

Central

Description

Add a DHCP server to the server list.

Options

<DHCP_SERVER_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
dhcp-server 192.168.168.170
```

Syntax

```
no dhcp-server <DHCP_SERVER_IPV4_HOST>
```

Mode

Central

Description

Remove a DHCP server from the server list.

Options

<DHCP_SERVER_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
no dhcp-server 192.168.168.170
```

Syntax

no dhcp-servers

Mode

Central

Description

Remove all DHCP servers from the server list.

Example

no dhcp-servers

Syntax

no relay-ip

Mode

Central

Description

Clear DHCP relay IP address.

Example

no relay-ip

Syntax

relay-ip <IPV4_HOST>

Mode

Central

Description

Configure DHCP relay IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

relay-ip 192.168.168.170

Syntax

bound-to <DHCP_OVER_VPN_INTERFACE>

Mode

Remote

Description

DHCP lease bound to.

Options

<DHCP_OVER_VPN_INTERFACE> Interface name.
Example: *X0*

Example

bound-to X2

Syntax

accept-bridged-wlan-request

Mode

Remote

Description

Accept DHCP request from bridged WLAN interface.

Example

accept-bridged-wlan-request

Syntax

no accept-bridged-wlan-request

Mode

Remote

Description

Reject DHCP request from bridged WLAN interface.

Example

no accept-bridged-wlan-request

Syntax

no relay-ip

Mode

Remote

Description

Clear DHCP relay IP address.

Example

no relay-ip

Syntax

relay-ip <IPV4_HOST>

Mode

Remote

Description

Configure DHCP relay IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
relay-ip 192.168.168.170
```

Syntax

```
no management-ip
```

Mode

Remote

Description

Clear remote management IP address.

Example

```
no management-ip
```

Syntax

```
management-ip <IPV4_HOST>
```

Mode

Remote

Description

Configure remote management IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
management-ip 192.168.168.170
```

Syntax

```
block-spoof
```

Mode

Remote

Description

Enable block traffic through tunnel when IP spoof detected.

Example

```
block-spoof
```

Syntax

```
no block-spoof
```

Mode

Remote

Description

Disable block traffic through tunnel when IP spoof detected.

Example

```
no block-spoof
```

Syntax

```
temp-lease
```

Mode

Remote

Description

Enable obtain temporary lease from local DHCP server if tunnel is down.

Example

```
temp-lease
```

Syntax

```
no temp-lease
```

Mode

Remote

Description

Disable obtain temporary lease from local DHCP server if tunnel is down.

Example

```
no temp-lease
```

Syntax

```
lease-time <UINT8>
```

Mode

Remote

Description

Set the temporary lease time (minutes).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
lease-time 10
```

Syntax

```
static-device <STATIC_DEVICE_IPV4_HOST> <STATIC_DEVICE_MAC>
```

Mode

Remote

Description

Add a static devices on LAN.

Options

<STATIC_DEVICE_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

<STATIC_DEVICE_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
static-device 192.168.168.170 01:02:03:04:05:06
```

Syntax

```
no static-device <STATIC_DEVICE_IPV4_HOST>
```

Mode

Remote

Description

Remove a static device on LAN.

Options

<STATIC_DEVICE_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
no static-device 192.168.168.170
```

Syntax

```
no static-devices
```

Mode

Remote

Description

Remove all static devices on LAN.

Example

```
no static-devices
```

Syntax

```
excluded-device <EXCLUDE_DEVICE_MAC>
```

Mode

Remote

Description

Add an excluded LAN device.

Options

<EXCLUDE_DEVICE_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
excluded-device 01:02:03:04:05:06
```

Syntax

```
no excluded-device <EXCLUDE_DEVICE_MAC>
```

Mode

Remote

Description

Remove an excluded LAN device.

Options

<EXCLUDE_DEVICE_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
no excluded-device 01:02:03:04:05:06
```

Syntax

```
no excluded-devices
```

Mode

Remote

Description

Remove all excluded LAN devices.

Example

```
no excluded-devices
```

Syntax

```
show vpn [ { { tunnel <VPN_POLICY_NAME> | tunnels } [ ike | ipsec | summary ] } | dhcp-over-vpn [ leases ] | l2tp-server | policies [ { ipv4 [ { group-vpn | site-to-site | tunnel-interface } ] | ipv6 [ site-to-site ] } ] | policy { ipv4 { { group-vpn <VPN_GROUP_POLICY_NAME> | site-to-site <VPN_SITE_POLICY_NAME> | tunnel-interface <VPN_TUNNEL_POLICY_NAME> } } | ipv6 { site-to-site <VPN_SITE_POLICY_V6_NAME> } } | settings ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show VPN status or configuration.

Options

tunnel Show an active VPN tunnel.
<VPN_POLICY_NAME> VPN policy name.
Example: *Remote Office*

tunnels Show all currently active VPN tunnels.

| | |
|--|---|
| ike | Show ike sa. |
| ipsec | Show ipsec sa. |
| summary | Show vpn sa number. |
| dhcp-over-vpn | Show DHCP over VPN status or configuration. |
| leases | Show DHCP over VPN leases. |
| l2tp-server | Show L2TP server configuration. |
| policies | Show all VPN policies. |
| ipv4 | Show only IPv4 VPN policies. |
| group-vpn | Show only IPv4 group VPN policies. |
| site-to-site | Show only IPv4 site to site VPN policies. |
| tunnel-interface | Show only IPv4 tunnel interface VPN policies. |
| ipv6 | Show only IPv6 VPN policies. |
| site-to-site | Show only IPv6 site to site VPN policies. |
| policy | Show a VPN policy. |
| ipv4 | IPv4 VPN policy. |
| group-vpn | Show IPv4 group VPN policy. |
| <VPN_GROUP_POLICY_NAME> | Group VPN policy name. Example: <i>WAN GroupVPN</i> |
| site-to-site | Show IPv4 site to site VPN policy. |
| <VPN_SITE_POLICY_NAME> | Site-to-site VPN policy name. Example: <i>Remote Office</i> |
| tunnel-interface | Show IPv4 tunnel interface VPN policy. |
| <VPN_TUNNEL_POLICY_NAME> | Tunnel interface VPN policy name. Example: <i>Remote Office</i> |
| ipv6 | IPv6 VPN policy. |
| site-to-site | IPv6 site-to-site VPN policy. |
| <VPN_SITE_POLICY_V6_NAME> | IPv6 Site-to-site VPN policy name. Example: <i>Remote Office</i> |
| settings | Show VPN settings configuration. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show vpn
show vpn tunnels
show vpn tunnel "Remote Office"
show vpn tunnels ipsec
show vpn statistics 0x23ab3456
show vpn dhcp-over-vpn
show vpn dhcp-over-vpn leases
show vpn l2tp-server
show vpn policy ipv4 tunnel-interface "Remote Office"
show vpn policies
```

Syntax

```
ssl-vpn server
```

Mode

Config

Description

Configure SSL VPN server settings.

Example

```
ssl-vpn server
```

Syntax

```
logout <SSLVPN_LOGOUT_IPV4_HOST>
```

Mode

SSL VPN Server

Description

Logout specified NetExtender virtual IP.

Options

<SSLVPN_LOGOUT_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
logout 1.1.1.1
```

Syntax

```
access <SSLVPN_ZONE_NAME>
```

Mode

SSL VPN Server

Description

Enable SSL VPN access on specified zone.

Options

<SSLVPN_ZONE_NAME> Zone object name.
Example: DMZ

Example

```
access WAN
```

Syntax

```
no access <SSLVPN_ZONE_NAME>
```

Mode

SSL VPN Server

Description

Disable SSL VPN access on specified zone.

Options

<SSLVPN_ZONE_NAME> Zone object name.

Example: *DMZ*

Example

```
no access WAN
```

Syntax

```
port <IPV4_PORT>
```

Mode

SSL VPN Server

Description

Set SSL VPN server port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
port 4433
```

Syntax

```
certificate { name <CERT_NAME> | use-self-signed }
```

Mode

SSL VPN Server

Description

Select SSL certificate to use for SSL VPN.

Options

name Specify certificate.
<CERT_NAME> Certificate name.
Example: *my_cert*

use-self-signed Use self signed certificate.

Example

```
certificate name CorpSSLVPNCert
```

Syntax

```
use-radius { mschap | mschapv2 }
```

Mode

SSL VPN Server

Description

Enable use RADIUS in specified mode for XAUTH.

Options

mschap Use MSCHAP for RADIUS.

mschapv2 Use MSCHAPv2 for RADIUS.

Example

```
use-radius mschapv2
```

Syntax

```
no use-radius
```

Mode

SSL VPN Server

Description

Disable use RADIUS for XAUTH.

Example

```
no use-radius
```

Syntax

```
user-domain <HOSTNAME>
```

Mode

SSL VPN Server

Description

Set user domain.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
user-domain LocalDomain
```

Syntax

```
no user-domain
```

Mode

SSL VPN Server

Description

Clear user domain.

Example

```
no user-domain
```

Syntax

```
management web
```

Mode

SSL VPN Server

Description

Enable web management over SSL VPN.

Example

```
management web
```

Syntax

```
no management web
```

Mode

SSL VPN Server

Description

Disable web management over SSL VPN.

Example

```
no management web
```

Syntax

```
management ssh
```

Mode

SSL VPN Server

Description

Enable SSH management over SSL VPN.

Example

```
management ssh
```

Syntax

```
no management ssh
```

Mode

SSL VPN Server

Description

Disable SSH management over SSL VPN.

Example

```
no management ssh
```

Syntax

```
session-timeout <UINT32>
```

Mode

SSL VPN Server

Description

Set the default session timeout in minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
session-timeout 10
```

Syntax

```
download-url { custom <WORD> | default }
```

Mode

SSL VPN Server

Description

Set SSL VPN client download URL.

Options

custom Manually specify SSL VPN image URL.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

default Enable use default SSL VPN image URL.

Example

```
download-url default
```

Syntax

```
ssl-vpn portal
```

Mode

Config

Description

Configure SSL VPN portal settings.

Example

```
ssl-vpn portal
```

Syntax

```
site-title <WORD>
```

Mode

SSL VPN Portal

Description

Set SSL VPN portal site title.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
site-title "Corp - Virtual Office"
```

Syntax

```
banner-title <WORD>
```

Mode

SSL VPN Portal

Description

Set SSL VPN portal banner title.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
banner-title "Virtual Office"
```

Syntax

```
home-page-message { custom <ROL> | default }
```

Mode

SSL VPN Portal

Description

Set SSL VPN portal home page message.

Options

custom Use customized home page message.

<ROL> Remaining command line input.
Example: *line...*

default Use default home page message example template.

Example

```
home-page-message custom "TBD"
```

Syntax

```
login-message { custom <ROL> | default }
```

Mode

SSL VPN Portal

Description

Set SSL VPN portal login message.

Options

custom Use customized login message.
<ROL> Remaining command line input.
Example: *line...*

default Use default login message example template.

Example

```
login-message custom "TBD"
```

Syntax

```
auto-launch
```

Mode

SSL VPN Portal

Description

Enable launch NetExtender after login.

Example

```
auto-launch
```

Syntax

```
no auto-launch
```

Mode

SSL VPN Portal

Description

Disable launch NetExtender after login.

Example

```
no auto-launch
```

Syntax

```
cache-control
```

Mode

SSL VPN Portal

Description

Enable HTTP meta tags for cache control (recommended).

Example

```
cache-control
```

Syntax

```
no cache-control
```

Mode

SSL VPN Portal

Description

Disable HTTP meta tags for cache control (recommended).

Example

```
no cache-control
```

Syntax

```
display-link
```

Mode

SSL VPN Portal

Description

Enable display UTM management link on SSL VPN portal(not recommended).

Example

```
display-link
```

Syntax

```
no display-link
```

Mode

SSL VPN Portal

Description

Disable display UTM management link on SSL VPN portal(not recommended).

Example

```
no display-link
```

Syntax

```
logo { custom <WORD> | default }
```

Mode

SSL VPN Portal

Description

Set SSL VPN portal logo.

Options

- custom** Enable use custom sonicwall logo.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- default** Enable use default sonicwall logo.

Example

```
logo default
```

Syntax

ssl-vpn epc-profile

Mode

Config

Description

Configure SSL VPN EPC profile.

Example

ssl-vpn epc-profile

Syntax

ssl-vpn profile

Mode

Config

Description

Configure SSL VPN default device profile.

Example

ssl-vpn profile

Syntax

enable-epc

Mode

EPC Profile

Description

Enable EPC.

Example

enable-epc

Syntax

no enable-epc

Mode

EPC Profile

Description

Disable EPC.

Example

no enable-epc

Syntax

```
fallback-options { default | quarantine }
```

Mode

EPC Profile

Description

Device profile fallback options.

Options

default Place into default device profile.

quarantine Place into quarantine device profile.

Example

```
fallback-options default
```

Syntax

```
device-profile <EPC_DEVICE_NAME>
```

Mode

Default Device Profile

Description

Configure default device profile.

Options

<EPC_DEVICE_NAME> Device name in the form: WORD or "QUOTED STRING".
Example: *Default Device Profile*

Example

```
device-profile "Default Device Profile"  
device-profile "Default Device Profile for SonicPointN"
```

Syntax

```
device-profile { linux | macos | windows } name <EPC_DEVICE_NAME>
```

Mode

EPC Profile

Description

Configure device profile.

Options

linux The operation system type of profile is linux

macos The operation system type of profile is macos

windows The operation system type of profile is windows

name Name of the profile.

<EPC_DEVICE_NAME> Device name in the form: WORD or "QUOTED STRING".
Example: *Default Device Profile*

Example

```
device-profile windows name "Default Device Profile for Windows"
```

Syntax

```
no device-profile { linux | macos | windows } name <EPC_DEVICE_NAME>
```

Mode

EPC Profile

Description

Delete the device profile.

Options

| | |
|--------------------------------|---|
| linux | OsType of device is linux |
| macos | OsType of device is macos |
| windows | OsType of device is windows |
| name | Name of the device profile. |
| <EPC_DEVICE_NAME> | Device name in the form: WORD or "QUOTED STRING". Example: <i>Default Device Profile</i> |

Example

```
no device-profile windows name "Default Device Profile for Windows"
```

Syntax

```
no device-profiles { linux | macos | windows }
```

Mode

EPC Profile

Description

Delete all device profiles which os type is window, linux or macos.

Options

| | |
|----------------|-----------------------------|
| linux | OsType of device is linux |
| macos | OsType of device is macos |
| windows | OsType of device is windows |

Example

```
no device-profiles windows
```

Syntax

```
name <WORD>
```

Mode

Device Profile

Description

Configure name for the device profile.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name device1
```

Syntax

```
description <WORD>
```

Mode

Device Profile

Description

Configure description for the device profile.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
description "device desc1-desc"
```

Syntax

```
no description
```

Mode

Device Profile

Description

Clear device description.

Example

```
no description
```

Syntax

```
enable
```

Mode

Device Profile

Description

Enable the device profile.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Device Profile

Description

Disable the device profile.

Example

```
no enable
```

Syntax

```
action { allow | deny }
```

Mode

Device Profile

Description

Configure action for the device profile.

Options

allow Device is allowed.

deny Device is denied.

Example

```
action allow
```

Syntax

```
network-address { ipv4 | ipv6 } { host <SSLVPN_ADDR_HOST> | name <SSLVPN_ADDR_NAME> | network <SSLVPN_ADDR_NETWORK> <SSLVPN_ADDR_MASK> | range <SSLVPN_ADDR_BEGIN> <SSLVPN_ADDR_END> } [ zone <SSLVPN_ADDR_ZONE_NAME> ]
```

Mode

Device Profile

Description

Setting network address for the client device.

Options

ipv4 Set IPv4 address object for the device profile.

ipv6 Set IPv6 address object for the device profile.

host Configure address object using host name.

<SSLVPN_ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<SSLVPN_ADDR_NAME> Host/network/range address object name.
Example: *Web Server*

network Configure address object using network.

<SSLVPN_ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<SSLVPN_ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Configure address object using range.

| | |
|--------------------------------------|--|
| <SSLVPN_ADDR_BEGIN> | IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| <SSLVPN_ADDR_END> | IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> |
| zone | Set SSL VPN zone object. |
| <SSLVPN_ADDR_ZONE_NAME> | Zone object name. Example: <i>SSLVPN</i> |

Example

```
network-address ipv4 name addr
network-address ipv4 host 192.168.168.33
network-address ipv4 range 192.168.100.50 192.168.100.60
network-address ipv4 network 192.168.100.0 /24
network-address ipv4 network 192.168.100.0 255.255.255.0
network-address ipv6 name addr
network-address ipv6 host fe10::1001
network-address ipv6 range fe10::1001 fe10::1100
network-address ipv6 network fe10::1001 /64
```

Syntax

```
no network-address { ipv4 | ipv6 }
```

Mode

Device Profile

Description

Clear network address for client device.

Options

ipv4 Clear IPv4 network address for the device profile.

ipv6 Clear IPv6 network address for the device profile.

Example

```
no network-address ipv4
no network-address ipv6
```

Syntax

```
deny-message <WORD>
```

Mode

Device Profile

Description

Configure message for the deny device.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
deny-message "some msg"
```

Syntax

no deny-message

Mode

Device Profile

Description

Clear message for the deny device.

Example

no deny-message

Syntax

```
quarantine-message { custom <WORD> | default }
```

Mode

Device Profile

Description

Configure message for a quarantine device.

Options

custom Set message customer value.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

default Set message default value.

Example

```
quarantine-message custom "some msg"
```

Syntax

```
no quarantine-message
```

Mode

Device Profile

Description

Clear quarantine message for the quarantine device.

Example

```
no quarantine-message
```

Syntax

```
wlan-tunnel-interface <WLAN_TUNNEL_INTERFACE>
```

Mode

Device Profile

Description

Configure wlan tunnel interface for SonicPointN L3 profile.

Options

<WLAN_TUNNEL_INTERFACE> WLAN tunnel interface name.
Example: *WTO*

Example

```
wlan-tunnel-interface X1
```

Syntax

```
no wlan-tunnel-interface
```

Mode

Device Profile

Description

Clear wlan tunnel interface for SonicPointN L3 profile.

Example

```
no wlan-tunnel-interface
```

Syntax

```
security
```

Mode

Device Profile

Description

Security related config for the device profile.

Example

```
security
```

Syntax

```
routes
```

Mode

Device Profile

Description

Routes related config for the device profile.

Example

```
routes
```

Syntax

```
client
```

Mode

Device Profile

Description

Client related config for the device profile.

Example

```
client
```

Syntax

```
no all-attributes
```

Mode

Device Profile Security

Description

Delete all security attribute.

Example

```
no all-attributes
```

Syntax

```
type { anti-spyware | anti-virus } { vendor <SSLVPN_SECURITY_VENDOR> [ product <SSLVPN_SECURITY_PRODUCT> [ [ version-operator <OPERAND> version <SSLVPN_SECURITY_PRODUCT_VER> ] [ updated-operator <OPERAND> updated-days <UINT32> ] [ scanned-operator <OPERAND> scanned-days <UINT32> ] [ realtime ] ] ] }
```

Mode

Device Profile Security

Description

Add a security attribute of type antivirus program or antispyware program.

Options

| | |
|--|---|
| anti-spyware | Add a security attribute of type antispyware program. |
| anti-virus | Add a security attribute of type antivirus program. |
| vendor | The vendor of antivirus program or antispyware program. |
| <SSLVPN_SECURITY_VENDOR> | Antivirus Program. Example: <i>Kaspersky Labs</i> |
| product | The product name of antivirus program or antispyware program. |
| <SSLVPN_SECURITY_PRODUCT> | Antivirus Program Product. Example: <i>Kaspersky Anti-Virus 2009</i> |
| version-operator | Product version. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| version | Product version. |
| <SSLVPN_SECURITY_PRODUCT_VER> | Antivirus Program Product Version. Example: <i>2.x</i> |
| updated-operator | Signature updated date. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| updated-days | Signature updated date. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i> |
| scanned-operator | File system scanned date. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| scanned-days | File system scanned date. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i> |
| realtime | Realtime protection required. |

Example

```
type anti-virus vendor "firewall name" product "product name" version-operator > version 4.0 updated-operator > updated-days 30 scanned-operator < scanned-days 25 realtime
```

Syntax

```
no type { anti-spyware | anti-virus } { vendor <SSLVPN_SECURITY_VENDOR> [ product <SSLVPN_SECURITY_PRODUCT> [ [ version-operator <OPERAND> version <SSLVPN_SECURITY_PRODUCT_VER> ] [ updated-operator <OPERAND> updated-days <UINT32> ] [ scanned-operator <OPERAND> scanned-days <UINT32> ] [ realtime ] ] ] }
```

Mode

Device Profile Security

Description

Delete a security attribute of type antivirus program or antispyware program.

Options

| | |
|--|---|
| anti-spyware | Delete a security attribute of type antispyware program. |
| anti-virus | Delete a security attribute of type antivirus program. |
| vendor | The vendor of antivirus program or antispyware program. |
| <SSLVPN_SECURITY_VENDOR> | Antivirus Program. Example: <i>Kaspersky Labs</i> |
| product | The product name of antivirus program ,antispyware program or firewall. |
| <SSLVPN_SECURITY_PRODUCT> | Antivirus Program Product. Example: <i>Kaspersky Anti-Virus 2009</i> |
| version-operator | Product version. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| version | Product version. |
| <SSLVPN_SECURITY_PRODUCT_VER> | Antivirus Program Product Version. Example: <i>2.x</i> |
| updated-operator | Signature updated date. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| updated-days | Signature updated date. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i> |
| scanned-operator | File system scanned date. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| scanned-days | File system scanned date. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i> |
| realtime | Realtime protection required. |

Example

```
no anti-virus vendor "firewall name" product "product name" version-operator > version 4.0 updated-operator > updated-days 30 scanned-operator < scanned-days 25 realtime
```

Syntax

```
firewall { vendor <SSLVPN_SECURITY_VENDOR> [ product <SSLVPN_SECURITY_PRODUCT> [ version-operator <OPERAND> version <SSLVPN_SECURITY_PRODUCT_VER> ] ] }
```

Mode

Device Profile Security

Description

Add a security attribute of type personal firewall program.

Options

| | |
|---------------------------------------|---|
| vendor | The vendor of antivirus program ,antispyware program or firewall. |
| <SSLVPN_SECURITY_VENDOR> | Antivirus Program. Example: <i>Kaspersky Labs</i> |

| | |
|--|---|
| product | The product of antivirus program ,antispysware program or firewall. |
| <SSLVPN_SECURITY_PRODUCT> | Antivirus Program Product. Example: <i>Kaspersky Anti-Virus 2009</i> |
| version-operator | Product version. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| version | Product version. |
| <SSLVPN_SECURITY_PRODUCT_VER> | Antivirus Program Product Version. Example: <i>2.x</i> |

Example

```
firewall vendor "firewall name" product "product name" version-operator > version 4.0
```

Syntax

```
no firewall { vendor <SSLVPN_SECURITY_VENDOR> [ product <SSLVPN_SECURITY_PRODUCT> [ version-operator <OPERAND> version <SSLVPN_SECURITY_PRODUCT_VER> ] ] }
```

Mode

Device Profile Security

Description

Delete a security attribute of type personal firewall program.

Options

| | |
|--|---|
| vendor | The vendor of antivirus program, antispysware program or firewall. |
| <SSLVPN_SECURITY_VENDOR> | Antivirus Program. Example: <i>Kaspersky Labs</i> |
| product | The product of antivirus program, antispysware program or firewall. |
| <SSLVPN_SECURITY_PRODUCT> | Antivirus Program Product. Example: <i>Kaspersky Anti-Virus 2009</i> |
| version-operator | Configure SSL VPN. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| version | Product version. |
| <SSLVPN_SECURITY_PRODUCT_VER> | Antivirus Program Product Version. Example: <i>2.x</i> |

Example

```
no firewall vendor "firewall name" product "product name" version-operator > version 4.0
```

Syntax

```
certification <SSLVPN_SECURITY_CERT> search { system-only | system-user }
```

Mode

Device Profile Security

Description

Add a security attribute of type certification.

Options

| | |
|-------------------------------------|---|
| <SSLVPN_SECURITY_CERT> | Client Certification. Example: <i>Certification xxx.</i> |
| search | Look for the certification. |
| system-only | Look in system store only. |
| system-user | Look in system store and user store. |

Example

certification certName search system-only

Syntax

no certification

Mode

Device Profile Security

Description

Delete a security attribute of type certification.

Example

no certification

Syntax

application <WORD>

Mode

Device Profile Security

Description

Add a security attribute of type application.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

application app-name

Syntax

no application <WORD>

Mode

Device Profile Security

Description

Delete a security attribute of type application.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no application app-name

Syntax

directory <WORD>

Mode

Device Profile Security

Description

Add a security attribute of type directory name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
directory dir-name
```

Syntax

```
no directory <WORD>
```

Mode

Device Profile Security

Description

Delete a security attribute of type directory name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no directory dir-name
```

Syntax

```
equipment <WORD>
```

Mode

Device Profile Security

Description

Add a security attribute of type equipment identifier.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
equipment equip-id
```

Syntax

```
no equipment
```

Mode

Device Profile Security

Description

Delete a security attribute of type equipment identifier.

Example

no equipment

Syntax

domain <WORD>

Mode

Device Profile Security

Description

Add a security attribute of type windows domain.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

domain domain-name

Syntax

no domain

Mode

Device Profile Security

Description

Delete a security attribute of type windows domain.

Example

no domain

Syntax

file file-name <WORD> [size-operator <OPERAND> bytes <UINT32>] [date-operator <OPERAND> [date { absolute <DATE_YYYYMMDD> | relative days <UINT32> }] [time <TIME_HHMMSS>]] [validate { md5 <WORD> | windows }]

Mode

Device Profile Security

Description

Add a security attribute of type file name.

Options

| | |
|------------------------|---|
| file-name | File name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| size-operator | File size is bigger or less .etc. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| bytes | File size. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i> |
| date-operator | Operand. |
| <OPERAND> | Operand. Example: = != >= > <= < |

| | |
|------------------------------|--|
| date | Last modified. |
| absolute | Absolute date. |
| <DATE_YYYYMMDD> | Date in the form: YYYY:MM:DD. Example: 2010:06:30 |
| relative | Relative date. |
| days | |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |
| time | Set relative time. |
| <TIME_HHMMSS> | Time in the form: DD:DD:DD. Example: 12:00:00 |
| validate | Validate file integrity. |
| md5 | Use MD5 or SHA-1 hash. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: abc |
| windows | Use windows catalog file. |

Example

```
file file-name fileName1 size-operator > bytes 2 date-operator < date absolute 2011/11/11 time 11:11:11 validate windows
```

Syntax

```
no file file-name <WORD> [ size-operator <OPERAND> bytes <UINT32> ] [ date-operator <OPERAND> [ date { absolute <DATE_YYYYMMDD> | relative days <UINT32> } ] [ time <TIME_HHMMSS> ] ] [ validate { md5 <WORD> | windows } ]
```

Mode

Device Profile Security

Options

| | |
|------------------------------|--|
| file-name | File name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: abc |
| size-operator | File size is bigger or less .etc. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| bytes | File size. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |
| date-operator | Operand. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| date | Last modified. |
| absolute | Absolute date. |
| <DATE_YYYYMMDD> | Date in the form: YYYY:MM:DD. Example: 2010:06:30 |
| relative | Relative date. |
| days | |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHHH. Example: 123 |
| time | Set relative time. |
| <TIME_HHMMSS> | Time in the form: DD:DD:DD. Example: 12:00:00 |
| validate | Validate file integrity. |
| md5 | Use MD5 or SHA-1 hash. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: abc |
| windows | Use windows catalog file. |

Example

```
no file file-name fileName1 size-operator > bytes 2 date-operator < date absolute 2011/11/11 time 11:11:11 validate windows
```

Syntax

```
registry key <WORD> [ value <WORD> ] [ data-operator <OPERAND> data <WORD> ]
```

Mode

Device Profile Security

Description

Add a security attribute of type windows registry entry.

Options

| | |
|------------------------|---|
| key | Key of the registry entry. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| value | Value of the registry entry. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| data-operator | Registry entry. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| data | Data of the registry entry. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

Example

```
registry key keyname value valuenam data-operator > data abcd
```

Syntax

```
no registry key <WORD> [ value <WORD> ] [ data-operator <OPERAND> data <WORD> ]
```

Mode

Device Profile Security

Description

Delete a security attribute of type windows registry entry.

Options

| | |
|------------------------|---|
| key | Key of the registry entry. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| value | Value of the registry entry. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| data-operator | Registry entry. |
| <OPERAND> | Operand. Example: = != >= > <= < |
| data | Data of the registry entry. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |

Example

```
no registry key keyname value valuenam data-operator = data abcd
```

Syntax

```
os-version <OS_VERSION> [ build <UINT32> ] [ version-operator <OPERAND> ]
```

Mode

Device Profile Security

Description

Add a security attribute of type windows version.

Options

| | |
|---------------------------|--|
| <OS_VERSION> | Operation System Version. Example: <i>windows 7</i> |
| build | Build of windows version. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i> |
| version-operator | |
| <OPERAND> | Operand. Example: = != >= > <= < |

Example

```
os-version windows-xp build 2345 version-operator >
```

Syntax

```
no os-version <OS_VERSION> [ build <UINT32> ] [ version-operator <OPERAND> ]
```

Mode

Device Profile Security

Description

Delete a security attribute of type windows version.

Options

| | |
|---------------------------|--|
| <OS_VERSION> | Operation System Version. Example: <i>windows 7</i> |
| build | Build of windows version. |
| <UINT32> | Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i> |
| version-operator | |
| <OPERAND> | Operand. Example: = != >= > <= < |

Example

```
no os-version windows-xp build 2345 version-operator >
```

Syntax

```
dns inherit
```

Mode

Device Profile Client

Description

Set DNS server IP address for NetExtender client.

Example

```
dns inherit
```

Syntax

```
dns primary <IP_V4V6_HOST>
```

Mode

Device Profile Client

Description

Set the primary DNS server IP address for NetExtender client.

Options

<IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
dns primary 192.168.168.170  
dns primary fe80::1002
```

Syntax

```
no dns primary
```

Mode

Device Profile Client

Description

Clear the primary DNS server IP address for NetExtender client.

Example

```
no dns primary
```

Syntax

```
dns secondary <IP_V4V6_HOST>
```

Mode

Device Profile Client

Description

Set the secondary DNS server IP address for NetExtender client.

Options

<IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
dns secondary 192.168.168.170  
dns secondary fe80::1002
```

Syntax

```
no dns secondary
```

Mode

Device Profile Client

Description

Clear the secondary DNS server IP address for NetExtender client.

Example

```
no dns secondary
```

Syntax

```
dns search-list <HOSTNAME>
```

Mode

Device Profile Client

Description

Add a dns to the dns search list.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
dns search-list 192.168.168.169
```

Syntax

```
no dns search-list <HOSTNAME>
```

Mode

Device Profile Client

Description

Clear a dns from the dns search list.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
no dns search-list 192.168.168.169
```

Syntax

```
no dns search-lists
```

Mode

Device Profile Client

Description

Clear all dns from the dns search list.

Example

```
no dns search-lists
```

Syntax

```
wins primary <IPV4_HOST>
```


Mode

Device Profile Client

Description

Set the primary WINS server IP address for NetExtender clients.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
wins primary 192.168.168.169
```

Syntax

```
no wins primary
```

Mode

Device Profile Client

Description

Clear the primary WINS server IP address for NetExtender clients.

Example

```
no wins primary
```

Syntax

```
wins secondary <IPV4_HOST>
```

Mode

Device Profile Client

Description

Set the secondary WINS server IP address for NetExtender clients.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
wins secondary 192.168.168.170
```

Syntax

```
no wins secondary
```

Mode

Device Profile Client

Description

Clear the secondary WINS server IP address for NetExtender clients.

Example

```
no wins secondary
```

Syntax

auto-update

Mode

Device Profile Client

Description

Enable client auto update.

Example

auto-update

Syntax

no auto-update

Mode

Device Profile Client

Description

Disable client auto update.

Example

no auto-update

Syntax

exit-after-disconnect

Mode

Device Profile Client

Description

Enable exit client after disconnect.

Example

exit-after-disconnect

Syntax

no exit-after-disconnect

Mode

Device Profile Client

Description

Disable exit client after disconnect.

Example

no exit-after-disconnect

Syntax

netbios-over-sslvpn

Mode

Device Profile Client

Description

Enable NetBIOS over SSL VPN.

Example

netbios-over-sslvpn

Syntax

no netbios-over-sslvpn

Mode

Device Profile Client

Description

Disable NetBIOS over SSL VPN.

Example

no netbios-over-sslvpn

Syntax

touch-id-authentication

Mode

Device Profile Client

Description

Allow Touch ID on IOS devices.

Example

touch-id-authentication

Syntax

no touch-id-authentication

Mode

Device Profile Client

Description

Disable allow Touch ID on IOS devices.

Example

no touch-id-authentication

Syntax

fingerprint-authentication

Mode

Device Profile Client

Description

Allow fingerprint authentication on Android devices.

Example

fingerprint-authentication

Syntax

no fingerprint-authentication

Mode

Device Profile Client

Description

Disable allow fingerprint authentication on Android devices.

Example

no fingerprint-authentication

Syntax

uninstall-after-exit

Mode

Device Profile Client

Description

Enable uninstall client after exit.

Example

uninstall-after-exit

Syntax

no uninstall-after-exit

Mode

Device Profile Client

Description

Disable uninstall client after exit.

Example

no uninstall-after-exit

Syntax

create-connection-profile

Mode

Device Profile Client

Description

Enable create client connection profile.

Example

```
create-connection-profile
```

Syntax

```
no create-connection-profile
```

Mode

Device Profile Client

Description

Disable create client connection profile.

Example

```
no create-connection-profile
```

Syntax

```
cache { credentials | user-name-only }
```

Mode

Device Profile Client

Description

Set user name and password caching.

Options

credentials Allow saving of user name and password.

user-name-only Allow saving of user name only.

Example

```
cache user-name-only
```

Syntax

```
no cache
```

Mode

Device Profile Client

Description

Prohibit saving of user name and password.

Example

```
no cache
```

Syntax

```
tunnel-all
```

Mode

Device Profile Routes

Description

Enable tunnel all.

Example

```
tunnel-all
```

Syntax

```
no tunnel-all
```

Mode

Device Profile Routes

Description

Disable tunnel all.

Example

```
no tunnel-all
```

Syntax

```
route [ ipv4 | ipv6 ] { group <SSLVPN_ROUTES_ADDR_GROUP_NAME> | name <SSLVPN_ROUTES_ADDR_NAME> }
```

Mode

Device Profile Routes

Description

Add a client route.

Options

| | |
|---|---|
| ipv4 | IPv4. |
| ipv6 | IPv6. |
| group <SSLVPN_ROUTES_ADDR_GROUP_NAME> | Add an address group to client route. SSLVPN Route Address Group name. Example: <i>Sales Group</i> |
| name <SSLVPN_ROUTES_ADDR_NAME> | Add an address object to client route. SSLVPN Route Address Object name. Example: <i>Web Server</i> |

Example

```
route name "Corp SSL-VPN Servers"  
route ipv6 name myV6AddrObj
```

Syntax

```
no route [ ipv4 | ipv6 ] { group <SSLVPN_ROUTES_ADDR_GROUP_NAME> | name <SSLVPN_ROUTES_ADDR_NAME> }
```

Mode

Device Profile Routes

Description

Delete a client route.

Options

| | |
|--|---|
| <code>ipv4</code> | IPv4. |
| <code>ipv6</code> | IPv6. |
| <code>group</code> | Delete an address group to client route. |
| <code><SSLVPN_ROUTES_ADDR_GROUP_NAME></code> | SSLVPN Route Address Group name. Example: <i>Sales Group</i> |
| <code>name</code> | Delete an address object to client route. |
| <code><SSLVPN_ROUTES_ADDR_NAME></code> | SSLVPN Route Address Object name. Example: <i>Web Server</i> |

Example

```
no route name "Corp SSL-VPN Servers"  
no route ipv6 name myV6AddrObj
```

Syntax

```
no routes
```

Mode

Device Profile Routes

Description

Delete all client routes.

Example

```
no routes
```

Syntax

```
ssl-vpn virtual-office
```

Mode

Config

Description

Configure SSL VPN virtual office settings.

Example

```
ssl-vpn virtual-office
```

Syntax

```
ssl-vpn logout <SSLVPN_LOGOUT_IPV4_HOST>
```

Mode

Config

Description

Logout specified NetExtender virtual IP.

Options

<SSLVPN_LOGOUT_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
ssl-vpn logout 1.1.1.1
```

Syntax

```
bookmark <SSLVPN_BOOKMARK>
```

Mode

Virtual Office

Description

Add/edit bookmark and enter configuration mode.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
bookmark "Admin Desktop"
```

Syntax

```
no bookmark <SSLVPN_BOOKMARK>
```

Mode

Virtual Office

Description

Delete a specified bookmark.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no bookmark "Admin Work Desktop"
```

Syntax

```
no bookmarks
```

Mode

Virtual Office

Description

Delete all bookmarks.

Example

no bookmarks

Syntax

name <SSLVPN_BOOKMARK>

Mode

Bookmark

Description

Set bookmark name.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name "Admin Work Desktop"

Syntax

host <HOSTNAME_MIXED>

Mode

Bookmark

Description

Set host name or IP address.

Options

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *2001:cdba:0000:0000:0000:3257:9652\n*

Example

host 192.168.168.57

Syntax

no host

Mode

Bookmark

Description

Clear host name or IP address.

Example

no host

Syntax

service { rdp | sshv2 | telnet | vnc }

Mode

Bookmark

Description

Set bookmark service type.

Options

rdp Terminal services (RDP-HTML5).

sshv2 Secure shell version 2 (SSHv2).

telnet Telnet.

vnc Virtual network computing (VNC).

Example

```
service vnc
```

Syntax

```
screen-size { 1024x768 | 1280x1024 | 640x480 | 800x600 | full-screen }
```

Mode

ActiveX
RDP

Description

Set screen size.

Options

1024x768 1024x768.

1280x1024 1280x1024.

640x480 640x480.

800x600 800x600.

full-screen Full screen.

Example

```
screen-size 1024x768
```

Syntax

```
colors { 15bit | 16bit | 24bit | 256 | 32bit }
```

Mode

ActiveX
RDP

Description

Set screen colors.

Options

15bit 15 bit - high color.

16bit 16 bit - high color.

24bit 24 bit - high color.

256 256 bit.

32bit 32 bit - highest quality.

Example

```
colors 24bit
```

Syntax

```
application-path <WORD>
```

Mode

ActiveX
RDP

Description

Set application and path to launch.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
application-path "C:\\\\Remote Applications\\\\myapp.exe"
```

Syntax

```
no application-path
```

Mode

ActiveX
RDP

Description

Clear application and path.

Example

```
no application-path
```

Syntax

```
start-in-folder <WORD>
```

Mode

ActiveX
RDP

Description

Set folder to start in.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
start-in-folder "C:\\Work\\"
```

Syntax

```
no start-in-folder
```

Mode

ActiveX
RDP

Description

Clear folder to start in.

Example

```
no start-in-folder
```

Syntax

```
automatic-login { custom [ name <WORD> ] [ password <ENC_PASSWORD> ] [ domain <WORD> ] | ssl-vpn }
```

Mode

ActiveX
RDP

Description

Enable automatically log in.

Options

| | |
|-----------------------------|---|
| custom | Use custom account credentials. |
| name | Enter login name. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| password | Enter login password. |
| <ENC_PASSWORD> | Password. Example: <i>secret</i> |
| domain | Enter login domain. |
| <WORD> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| ssl-vpn | Use SSL-VPN account credentials. |

Example

```
automatic-login custom name myuser password mypassword domain mydomain
```

Syntax

```
no automatic-login [ custom { domain | name | password } ]
```

Mode

ActiveX
RDP

Description

Disable automatically log in.

Options

custom Use custom account credentials.

domain Clear login domain.

name Clear login name.

password Clear login password.

Example

```
no automatic-login
no automatic-login custom name
no automatic-login custom password
no automatic-login custom domain
```

Syntax

```
plugin-dlls <WORD>
```

Mode

ActiveX

Description

Enable plugin DLLs.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
plugin-dlls x.dll
```

Syntax

```
no plugin-dlls
```

Mode

ActiveX

Description

Disable plugin DLLs.

Example

```
no plugin-dlls
```

Syntax

```
redirect-clipboard
```

Mode

ActiveX
RDP

Description

Enable redirect clipboard.

Example

```
redirect-clipboard
```

Syntax

no redirect-clipboard

Mode

ActiveX
RDP

Description

Disable redirect clipboard.

Example

no redirect-clipboard

Syntax

redirect-audio

Mode

ActiveX
RDP

Description

Enable redirect audio.

Example

redirect-audio

Syntax

no redirect-audio

Mode

ActiveX
RDP

Description

Disable redirect audio.

Example

no redirect-audio

Syntax

auto-reconnection

Mode

ActiveX
RDP

Description

Enable automatic reconnection.

Example

auto-reconnection

Syntax

no auto-reconnection

Mode

ActiveX
RDP

Description

Disable automatic reconnections.

Example

no auto-reconnection

Syntax

desktop-background

Mode

ActiveX
RDP

Description

Enable desktop background.

Example

desktop-background

Syntax

no desktop-background

Mode

ActiveX
RDP

Description

Disable desktop background.

Example

no desktop-background

Syntax

window-drag

Mode

ActiveX
RDP

Description

Enable window drag.

Example

window-drag

Syntax

no window-drag

Mode

ActiveX
RDP

Description

Disable window drag.

Example

no window-drag

Syntax

animation

Mode

ActiveX
RDP

Description

Enable menu / window animation.

Example

animation

Syntax

no animation

Mode

ActiveX
RDP

Description

Disable menu / window animation.

Example

no animation

Syntax

view-only

Mode

VNC

Description

Enable view only.

Example

view-only

Syntax

no view-only

Mode

VNC

Description

Disable view only.

Example

no view-only

Syntax

share-desktop

Mode

VNC

Description

Enable share desktop.

Example

share-desktop

Syntax

no share-desktop

Mode

VNC

Description

Disable share desktop.

Example

no share-desktop

Syntax

automatic-accept-host-key

Mode

SSHV2

Description

Enable automatically accept host key.

Example

automatic-accept-host-key

Syntax

no automatic-accept-host-key

Mode

SSHV2

Description

Disable automatically accept host key.

Example

no automatic-accept-host-key

Syntax

display-on-mobile

Mode

RDP
SSHV2
VNC
Telnet

Description

Enable display bookmark to mobile connect clients.

Example

display-on-mobile

Syntax

no display-on-mobile

Mode

RDP
SSHV2
VNC
Telnet

Description

Disable display bookmark to mobile connect clients.

Example

no display-on-mobile

Syntax

show ssl-vpn [bookmark <SSLVPN_BOOKMARK> | bookmarks [sessions] | device-profile <EPC_DEVICE_NAME> | device-profiles | epc-profile { linux | macos | windows } name <EPC_DEVICE_NAME> | epc-profiles | portal | server | sessions | statistics <SSLVPN_LOGOUT_IPV4_HOST>] [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show SSL VPN status or configuration.

Options

| | |
|--|---|
| bookmark | Show a specified virtual office bookmark. |
| <SSLVPN_BOOKMARK> | Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i> |
| bookmarks | Show all virtual office bookmarks. |
| sessions | Show all active bookmark sessions. |
| device-profile | Show default device profile configuration. |
| <EPC_DEVICE_NAME> | Device name in the form: WORD or \"QUOTED STRING\". Example: <i>Default Device Profile</i> |
| device-profiles | Show all default device profiles configuration. |
| epc-profile | Show EPC profile configuration. |
| linux | Show linux EPC profile configuration. |
| macos | Show macos EPC profile configuration. |
| windows | Show windows EPC profile configuration. |
| name | Show EPC profile configuration. |
| <EPC_DEVICE_NAME> | Device name in the form: WORD or \"QUOTED STRING\". Example: <i>Default Device Profile</i> |
| epc-profiles | Show all EPC profiles configuration. |
| portal | Show portal configuration. |
| server | Show server configuration. |
| sessions | Show all active sslvpn sessions. |
| statistics | Show statistics for the session associated with the specified netextender virtual IP. |
| <SSLVPN_LOGOUT_IPV4_HOST> | IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i> |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show ssl-vpn
```

Syntax

```
switch
```

Mode

Config

Description

Enter switch configuration mode.

Example

```
switch
```

Syntax

```
trunk port <TRUNK_PORT_INTERFACE>
```

Mode

Switch

Description

Add/edit trunk port.

Options

port Configure port.
<TRUNK_PORT_INTERFACE> Interface name.
Example: X0

Example

```
trunk port X3
```

Syntax

```
vlan <VLAN_TAG>
```

Mode

Trunk Port

Description

Add VLAN to trunk port.

Options

<VLAN_TAG> VLAN tag.
Example: 23

Example

```
vlan 2100
```

Syntax

```
no vlan <TRUNK_PORT_VLAN_TAG>
```

Mode

Trunk Port

Description

Remove VLAN from trunk port.

Options

<TRUNK_PORT_VLAN_TAG> VLAN tag.
Example: 23

Example

```
no vlan 2100
```

Syntax

```
no trunk port <TRUNK_PORT_NAME>
```

Mode

Switch

Description

Delete trunk port.

Options

<TRUNK_PORT_NAME> Interface name.
Example: *X0*

Example

```
no trunk port X3
```

Syntax

```
no trunk ports
```

Mode

Switch

Description

Delete all trunk ports.

Example

```
no trunk ports
```

Syntax

```
portshield port <PORTSHIELD_INTERFACE>
```

Mode

Switch

Description

Edit portshield port.

Options

port Configure port.
<PORTSHIELD_INTERFACE> Interface name.
Example: *X0*

Example

```
portshield port X3
```

Syntax

```
vlan <VLAN_TAG>
```

Mode

Portshield Port

Description

Edit VLAN for the portshield port.

Options

<VLAN_TAG> VLAN tag.
Example: *23*

Example

```
vlan 2100
```

Syntax

```
no vlan
```

Mode

Portshield Port

Description

Clear VLAN for the portshield port.

Example

```
no vlan
```

Syntax

```
trunked
```

Mode

Portshield Port

Description

Enable trunked for the portshield port.

Example

```
trunked
```

Syntax

```
no trunked
```

Mode

Portshield Port

Description

Disable trunked for the portshield port.

Example

```
no trunked
```

Syntax

```
refresh l2-discovery [ interface <L2_DISCOVERY_INTERFACE> ]
```

Mode

Switch

Description

Refresh L2 discovery.

Options

interface Refresh L2 discovery interface information.
<L2_DISCOVERY_INTERFACE> Interface name.
Example: X0

Example

```
refresh l2-discovery interface X3
```

Syntax

```
link-aggregation port <LINK_AGGREGATION_INTERFACE_NAME>
```

Mode

Switch

Description

Add/Edit link aggregation.

Options

port Configure port.
<LINK_AGGREGATION_INTERFACE_NAME> Interface name.
Example: X0

Example

```
link-aggregation port X3
```

Syntax

```
key { id <UINT8> }
```

Mode

Link Aggregation

Description

Set the link aggregation key.

Options

id Set the link aggregation key ID.
<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
key id 11
```

Syntax

```
member <LAG_MEMBER_INTERFACE_NAME>
```

Mode

Link Aggregation

Description

Add a member to the link aggregation.

Options

<LAG_MEMBER_INTERFACE_NAME> Interface name.
Example: X0

Example

```
member X4
```

Syntax

```
no member <LAG_NO_MEMBER_INTERFACE_NAME>
```

Mode

Link Aggregation

Description

Delete a member from the link aggregation.

Options

<LAG_NO_MEMBER_INTERFACE_NAME> Interface name.
Example: X0

Example

```
no member X4
```

Syntax

```
lacp
```

Mode

Link Aggregation

Description

Enable LACP.

Example

```
lacp
```

Syntax

```
no lacp
```

Mode

Link Aggregation

Description

Disable LACP.

Example

```
no lacp
```

Syntax

```
load-balance-type source ip
```

Mode

Link Aggregation

Description

Set link aggregation load balance type as source ip.

Example

```
load-balance-type source ip
```

Syntax

```
load-balance-type source mac
```

Mode

Link Aggregation

Description

Set link aggregation load balance type as source mac.

Example

```
load-balance-type source mac
```

Syntax

```
load-balance-type source destination { ip | mac }
```

Mode

Link Aggregation

Description

Set link aggregation load balance type as source destination ip or mac.

Options

ip SRC_IP, SRC_PORT, DST_IP, DST_PORT.

mac SRC_MAC, DST_MAC, ETH_TYPE, VLAN, INTF.

Example

```
load-balance-type source destination mac
```

Syntax

```
load-balance-type destination { ip | mac }
```

Mode

Link Aggregation

Description

Set link aggregation load balance type as destination ip or mac.

Options

ip DST_IP, DST_PORT.

mac DST_MAC, ETH_TYPE, VLAN, INTF.

Example

```
load-balance-type destination mac
```

Syntax

no link-aggregation port <LAG_PORT_NAME>

Mode

Switch

Description

Delete link aggregation or member.

Options

port Configure port.
<LAG_PORT_NAME> Interface name.
 Example: *X0*

Example

no link-aggregation port X3

Syntax

port mirror <PORT_MIRROR_GROUP_NAME>

Mode

Switch

Description

Add/edit port mirror.

Options

<PORT_MIRROR_GROUP_NAME> Port mirror group name.
 Example: *Port Mirror group*

Example

port mirror "CorpMirror"

Syntax

name <PORT_MIRROR_GROUP_NAME>

Mode

Port Mirror

Description

Edit the port mirror group name.

Options

<PORT_MIRROR_GROUP_NAME> Port mirror group name.
 Example: *Port Mirror group*

Example

name CorpMirror

Syntax

```
direction { both | egress | ingress }
```

Mode

Port Mirror

Description

Set port mirror direction.

Options

both Both.

egress Egress.

ingress Ingress.

Example

```
direction egress
```

Syntax

```
enable
```

Mode

Port Mirror

Description

Enable port mirror.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Port Mirror

Description

Disable port mirror.

Example

```
no enable
```

Syntax

```
mirror-port <MIRROR_PORT_NAME>
```

Mode

Port Mirror

Description

Set the port to mirror traffic to.

Options

<MIRROR_PORT_NAME> Interface name.
Example: X0

Example

```
mirror-port X4
```

Syntax

```
no mirror-port
```

Mode

Port Mirror

Description

Clear the port to mirror traffic to.

Example

```
no mirror-port
```

Syntax

```
mirrored-port <MIRROR_PORT_NAME>
```

Mode

Port Mirror

Description

Add a port to mirror traffic from.

Options

<MIRROR_PORT_NAME> Interface name.
Example: X0

Example

```
mirrored-port X1
```

Syntax

```
no mirrored-port <MIRRORED_NO_PORT_NAME>
```

Mode

Port Mirror

Description

Delete a port used to mirror traffic from.

Options

<MIRRORED_NO_PORT_NAME> Interface name.
Example: X0

Example

```
no mirrored-port X1
```

Syntax

```
no port mirror <PORT_MIRROR_GROUP_NAME>
```

Mode

Switch

Description

Delete port mirror.

Options

<PORT_MIRROR_GROUP_NAME> Port mirror group name.
Example: *Port Mirror group*

Example

```
no port mirror "CorpMirror"
```

Syntax

```
no port mirrors
```

Mode

Switch

Description

Delete all port mirrors.

Example

```
no port mirrors
```

Syntax

```
rapid-spanning-tree
```

Mode

Switch

Description

Enter rapid spanning tree configuration mode.

Example

```
rapid-spanning-tree
```

Syntax

```
version { rstp | stp-only }
```

Mode

Rapid Spanning Tree

Description

Set spanning tree forced version.

Options

rstp RSTP operation.

stp-only STP only.

Example

```
version rstp
```

Syntax

```
bridge-priority <UINT16>
```

Mode

Rapid Spanning Tree

Description

Set the bridge priority.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
bridge-priority 32768
```

Syntax

```
no bridge-priority
```

Mode

Rapid Spanning Tree

Description

Clear the bridge priority.

Example

```
no bridge-priority
```

Syntax

```
hello-time <UINT8>
```

Mode

Rapid Spanning Tree

Description

Set the bridge hello time in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
hello-time 3
```

Syntax

```
forward-delay <UINT8>
```

Mode

Rapid Spanning Tree

Description

Set the bridge forward delay in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
forward-delay 15
```

Syntax

```
interface <LAG_PORT_NAME>
```

Mode

Rapid Spanning Tree

Description

Edit interface RSTP settings.

Options

<LAG_PORT_NAME> Interface name.
Example: X0

Example

```
interface X3
```

Syntax

```
enable
```

Mode

Port

Description

Enable RSTP for this interface.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Port

Description

Disable RSTP for this interface.

Example

```
no enable
```

Syntax

```
cost { auto | value <UINT32> }
```

Mode

Port

Description

Set port path cost.

Options

auto Enable auto set port path cost.

value Set the port path cost.

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
cost value 20000  
cost auto
```

Syntax

```
priority
```

Mode

Port

Description

Set port priority.

Example

```
priority
```

Syntax

```
no priority
```

Mode

Port

Description

Clear port priority.

Example

```
no priority
```

Syntax

```
dscp-remap value <UINT8> priority { high | highest | low | normal }
```


Mode

Switch

Description

Set the priority for the DSCP values.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

priority Priority.

high High.

highest Highest.

low Low.

normal Normal.

Example

```
dscp-remap value 4 priority high
```

Syntax

```
dscp-remap restore-defaults
```

Mode

Switch

Description

Set DSCP remap to default values.

Example

```
dscp-remap restore-defaults
```

Syntax

```
qos output-scheduling { strict-priority-queue | weighted-round-robin }
```

Mode

Switch

Description

Set the L2 QoS output scheduling method.

Options

strict-priority-queue Strict priority queue.

weighted-round-robin Weighted round robin.

Example

```
qos output-scheduling weighted-round-robin
```

Syntax

```
qos interface <L2_DISCOVERY_INTERFACE>
```

Mode

Switch

Description

Enter QoS configuration mode for the specified interface.

Options

<L2_DISCOVERY_INTERFACE> Interface name.
Example: X0

Example

```
qos interface X3
```

Syntax

```
fixed-priority
```

Mode

Switch Interface QoS

Description

Enable fixed priority.

Example

```
fixed-priority
```

Syntax

```
no fixed-priority
```

Mode

Switch Interface QoS

Description

Disable fixed priority.

Example

```
no fixed-priority
```

Syntax

```
trust cos
```

Mode

Switch Interface QoS

Description

Enable trust CoS.

Example

```
trust cos
```

Syntax

no trust cos

Mode

Switch Interface QoS

Description

Disable trust CoS.

Example

no trust cos

Syntax

trust dscp

Mode

Switch Interface QoS

Description

Enable trust DSCP.

Example

trust dscp

Syntax

no trust dscp

Mode

Switch Interface QoS

Description

Disable trust DSCP.

Example

no trust dscp

Syntax

prefer cos

Mode

Switch Interface QoS

Description

Enable prefer CoS.

Example

prefer cos

Syntax

no prefer cos

Mode

Switch Interface QoS

Description

Disable prefer cos.

Example

no prefer cos

Syntax

default-priority { high | highest | low | normal }

Mode

Switch Interface QoS

Description

Set QoS default priority.

Options

high High.

highest Highest.

low Low.

normal Normal.

Example

default-priority high

Syntax

rate-control interface <L2_DISCOVERY_INTERFACE>

Mode

Switch

Description

Enter rate control configuration mode for the specified interface.

Options

<L2_DISCOVERY_INTERFACE> Interface name.
Example: *X0*

Example

rate-control interface X3

Syntax

flow-control

Mode

Switch Rate Control

Description

Enable flow control.

Example

```
flow-control
```

Syntax

```
no flow-control
```

Mode

Switch Rate Control

Description

Disable flow control.

Example

```
no flow-control
```

Syntax

```
ingress limit { all | broadcast-multicast broadcast | broadcast-multicast-flood }
```

Mode

Switch Rate Control

Description

Set ingress limit type of traffic.

Options

| | |
|----------------------------------|--|
| all | All. |
| broadcast-multicast | Broadcast, and multicast. |
| broadcast | Only broadcast. |
| broadcast-multicast-flood | Broadcast, multicast, and flooded unicast. |

Example

```
ingress-limit broadcast-multicast
```

Syntax

```
ingress rate <UINT32>
```

Mode

Switch Rate Control

Description

Set the ingress rate in kbits/sec.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
ingress rate 256
```

Syntax

```
no ingress rate
```

Mode

Switch Rate Control

Description

Clear ingress rate.

Example

```
no ingress rate
```

Syntax

```
egress rate <UINT32>
```

Mode

Switch Rate Control

Description

Set the egress rate in kbits/sec.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
egress rate 256
```

Syntax

```
no egress rate
```

Mode

Switch Rate Control

Description

Clear egress rate.

Example

```
no egress rate
```

Syntax

```
rate-control restore-defaults
```

Mode

Switch

Description

Set rate control to default values.

Example

```
rate-control restore-defaults
```

Syntax

```
port security <PORT_SECURITY_INTERFACE_NAME>
```

Mode

Switch

Description

Enter port security configuration mode for the specified interface.

Options

<PORT_SECURITY_INTERFACE_NAME> Interface name.
Example: *X0*

Example

```
port security X3
```

Syntax

```
discard
```

Mode

Switch Port Security

Description

Enable discard.

Example

```
discard
```

Syntax

```
no discard
```

Mode

Switch Port Security

Description

Disable discard.

Example

```
no discard
```

Syntax

```
mac-address { group <ADDR_MAC_GROUP> | mac <ADDR_MAC> | name <ADDR_MAC_NAME> }
```

Mode

Switch Port Security

Description

Add MAC address object to port security for interface.

Options

| | |
|-------------------------------|---|
| group | Address group name. |
| <ADDR_MAC_GROUP> | MAC group address object name. Example: <i>Sales & Marketing Network Access Points</i> |
| mac | MAC address. |
| <ADDR_MAC> | Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH. |
| name | MAC address object name. |
| <ADDR_MAC_NAME> | MAC address object name. Example: <i>Sales Network Access Point</i> |

Example

```
mac-address mac 00:01:02:03:04:05
```

Syntax

```
no mac-address { group <ADDR_MAC_GROUP> | name <ADDR_MAC_NAME> }
```

Mode

Switch Port Security

Description

Delete MAC address object from port security for interface.

Options

| | |
|-------------------------------|---|
| group | Address group name. |
| <ADDR_MAC_GROUP> | MAC group address object name. Example: <i>Sales & Marketing Network Access Points</i> |
| name | MAC address object name. |
| <ADDR_MAC_NAME> | MAC address object name. Example: <i>Sales Network Access Point</i> |

Example

```
no mac-address name macAddress
```

Syntax

```
no mac-addresses
```

Mode

Switch Port Security

Description

Delete all MAC address objects from port security for interface.

Example

```
no mac-addresses
```

Syntax


```
show switch [ cos-remap | dscp-remap | l2-discovery [ interface <L2_DISCOVERY_INTERFACE> ] | link-aggregation [ port
<LAG_PORT_NAME> ] [ { statistics | status } ] | port { { mirror <PORT_MIRROR_GROUP_NAME> | mirrors | security [ interface
<INTERFACE_NAME> ] } } | portshield { { port <PORTSHIELD_INTERFACE> | ports } } | qos [ interface <INTERFACE_NAME> ] | rapid-
spanning-tree [ bridge ] | rate-control [ interface <L2_DISCOVERY_INTERFACE> ] | trunk { port <TRUNK_PORT_NAME> | ports } ] [ {
pending-config | with-pending-config } ] ]
```

Mode

All Modes

Description

Show switch configuration and information.

Options

| | |
|---------------------------------------|--|
| cos-remap | Show CoS remap table. |
| dscp-remap | Show DSCP remap table configuration. |
| l2-discovery | Show L2 discovery information. |
| interface | Show L2 discovery interface information |
| <L2_DISCOVERY_INTERFACE> | Interface name. Example: <i>X0</i> |
| link-aggregation | Show link aggregation configuration. |
| port | Show link aggregation port configuration. |
| <LAG_PORT_NAME> | Interface name. Example: <i>X0</i> |
| statistics | Show link-aggregation interface statistics. |
| status | Show link aggregation status. |
| port | Show port configuration. |
| mirror | Show port mirror group configuration. |
| <PORT_MIRROR_GROUP_NAME> | Port mirror group name. Example: <i>Port Mirror group</i> |
| mirrors | Show all port mirror groups configuration. |
| security | Show port security configuration. |
| interface | Show port security configuration for specified interface. |
| <INTERFACE_NAME> | Interface name. Example: <i>X0</i> |
| portshield | Show portshield port configuration. |
| port | Show specified portshield port configuration. |
| <PORTSHIELD_INTERFACE> | Interface name. Example: <i>X0</i> |
| ports | Show all portshield ports configuration. |
| qos | Show QoS configuration. |
| interface | Show QoS configuration for specified interface. |
| <INTERFACE_NAME> | Interface name. Example: <i>X0</i> |
| rapid-spanning-tree | Show rapid spanning tree configuration. |
| bridge | Show rapid spanning tree bridge information |
| rate-control | Show rate control configuration. |
| interface | Show rate control configuration for specified interface. |
| <L2_DISCOVERY_INTERFACE> | Interface name. Example: <i>X0</i> |
| trunk | Show trunk port configuration. |
| port | Show specified trunk port configuration. |

| | |
|--------------------------------|---|
| <TRUNK_PORT_NAME> | Interface name. Example: X0 |
| ports | Show all trunk ports configuration. |
| pending-config | Show pending configuration changes. |
| with-pending-config | View current configuration with pending changes included in the output. |

Example

```
show switch
show switch trunk ports
show switch trunk port X3
show switch portshield ports
show switch portshield port X4
show switch l2-discovery
show switch l2-discovery interface X2
show switch link-aggregation
show switch link-aggregation port X5
show switch link-aggregation statistics
show switch link-aggregation status
show switch port mirros
show switch port mirror X6
```

Syntax

```
performance-class-object <SDWAN_PERFORMANCE_CLASS_OBJECT_NAME>
```

Mode

SD-WAN

Description

Add/edit SD-WAN performance class object.

Options

<SDWAN_PERFORMANCE_CLASS_OBJECT_NAME> Atom Object name.
Example: *Lowest Jitter*

Example

```
performance-class-object "VoIP"
```

Syntax

```
no performance-class-object <SDWAN_PERFORMANCE_CLASS_OBJECT_NAME>
```

Mode

SD-WAN

Description

Delete a SD-WAN performance class object.

Options

<SDWAN_PERFORMANCE_CLASS_OBJECT_NAME> Atom Object name.
Example: *Lowest Jitter*

Example

```
no performance-class-object "Best of All"
```

Syntax

no performance-class-objects

Mode

SD-WAN

Description

Delete all SD-WAN performance class objects.

Example

no performance-class-objects

Syntax

name <SDWAN_PERFORMANCE_CLASS_OBJECT_NAME>

Mode

SD-WAN Performance Class Object

Description

Set SD-WAN performance class object name.

Options

<SDWAN_PERFORMANCE_CLASS_OBJECT_NAME> Atom Object name.
Example: *Lowest Jitter*

Example

name "Best of All"

Syntax

include { jitter | latency | packet-loss }

Mode

SD-WAN Performance Class Object

Description

Include latency/jitter/packet-loss.

Options

jitter Include jitter.

latency Include latency.

packet-loss Include packet loss.

Example

include jitter

Syntax

no include { jitter | latency | packet-loss }

Mode

SD-WAN Performance Class Object

Description

Disable include latency/jitter/packet-loss.

Options

jitter Include jitter.

latency Include latency.

packet-loss Include packet loss.

Example

```
no include jitter
```

Syntax

```
latency <DECIMAL>
```

Mode

SD-WAN Performance Class Object

Description

Set latency in millisecond.

Options

<DECIMAL> Decimal in the form: n+.n+.
Example: 0.999

Example

```
latency 8
```

Syntax

```
no latency
```

Mode

SD-WAN Performance Class Object

Description

Clear latency.

Example

```
no latency
```

Syntax

```
jitter <DECIMAL>
```

Mode

SD-WAN Performance Class Object

Description

Set jitter in millisecond.

Options

<DECIMAL> Decimal in the form: n+.n+.
Example: 0.999

Example

```
jitter 10
```

Syntax

```
no jitter
```

Mode

SD-WAN Performance Class Object

Description

Clear jitter.

Example

```
no jitter
```

Syntax

```
packet-loss <DECIMAL>
```

Mode

SD-WAN Performance Class Object

Description

Set packet loss in percentage.

Options

<DECIMAL> Decimal in the form: n+.n+.
Example: 0.999

Example

```
packet-loss 20
```

Syntax

```
no packet-loss
```

Mode

SD-WAN Performance Class Object

Description

Clear packet loss.

Example

```
packet-loss 20
```

Syntax

```
comment <WORD>
```

Mode

SD-WAN Performance Class Object

Description

Set comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment myObject
```

Syntax

```
no comment
```

Mode

SD-WAN Performance Class Object

Description

Clear comment.

Example

```
no comment
```

Syntax

```
performance-probe <SDWAN_PROBE_NAME>
```

Mode

SD-WAN

Description

Add/edit a SD-WAN Performance Probe.

Options

<SDWAN_PROBE_NAME> Atom Object name.
Example: *Web Services Monitor*

Example

```
performance-probe "Remote Servers"
```

Syntax

```
no performance-probe <SDWAN_PROBE_NAME>
```

Mode

SD-WAN

Description

Delete SD-WAN Performance Probe.

Options

<SDWAN_PROBE_NAME> Atom Object name.
Example: *Web Services Monitor*

Example

```
no performance-probe "Remote Servers"
```

Syntax

```
no performance-probes
```

Mode

SD-WAN

Description

Delete all SD-WAN Performance Probes.

Example

```
no performance-probes
```

Syntax

```
name <SDWAN_PROBE_NAME>
```

Mode

SD-WAN Performance Probe

Description

Edit a SD-WAN Performance Probe name.

Options

<SDWAN_PROBE_NAME> Atom Object name.
Example: *Web Services Monitor*

Example

```
name "Remote Servers"
```

Syntax

```
sdwan-group <SDWAN_PROBE_GROUP_NAME>
```

Mode

SD-WAN Performance Probe

Description

Edit a SD-WAN Performance Probe interface group.

Options

<SDWAN_PROBE_GROUP_NAME> SD-WAN Group Name.
Example: *Social Networking*

Example

```
group "VoIP"
```

Syntax

```
no probe target
```

Mode

SD-WAN Performance Probe

Description

Clear the probe target.

Example

```
no probe target
```

Syntax

```
probe target { fqdn <ADDR_FQDN> | host <ADDR_HOST> | name <ADDR_FQDNHOST_ADDR> }
```

Mode

SD-WAN Performance Probe

Description

Set the probe target.

Options

| | |
|-------------------------------------|--|
| fqdn <ADDR_FQDN> | Set the probe target to FQDN address. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i> |
| host <ADDR_HOST> | Set the probe target to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> |
| name <ADDR_FQDNHOST_ADDR> | Set the probe target to named address object. FQDN/host address object name. Example: <i>Web Server</i> |

Example

```
probe target name "Remote Target"
```

Syntax

```
probe type { ping explicit | tcp explicit port <IPV4_PORT> }
```

Mode

SD-WAN Performance Probe

Description

Set SD-WAN Performance Probe type.

Options

| | |
|--------------------------|--|
| ping | Ping probe. |
| explicit | Ping probe using explicit route. |
| tcp | TCP probe. |
| explicit | TCP probe using explicit route. |
| port | Set TCP probe port. |
| <IPV4_PORT> | Integer in the form: D OR 0xHHHHH. Example: <i>80</i> |

Example


```
probe type ping explicit
probe type tcp explicit port 80
```

Syntax

```
probe interval <UINT16>
```

Mode

SD-WAN Performance Probe

Description

Set probe host interval.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
probe interval 5
```

Syntax

```
reply-timeout <UINT8>
```

Mode

SD-WAN Performance Probe

Description

Set probing reply timeout.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
reply-timeout 2
```

Syntax

```
interval missed <UINT8>
```

Mode

SD-WAN Performance Probe

Description

Probe state is set to DOWN after specified number of missed intervals.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
interval missed 3
```

Syntax

```
interval successful <UINT8>
```

Mode

SD-WAN Performance Probe

Description

Probe state is set to UP after specified number of successful intervals.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
interval successful 3
```

Syntax

```
rst-as-miss
```

Mode

SD-WAN Performance Probe

Description

Enable RST response counts as miss.

Example

```
rst-as-miss
```

Syntax

```
no rst-as-miss
```

Mode

SD-WAN Performance Probe

Description

Disable RST response counts as miss.

Example

```
no rst-as-miss
```

Syntax

```
comment <WORD>
```

Mode

SD-WAN Performance Probe

Description

Set SD-WAN Performance Probe comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
comment "Remote Servers"
```

Syntax

```
no comment
```

Mode

SD-WAN Performance Probe

Description

Clear SD-WAN Performance Probe comment.

Example

```
no comment
```

Syntax

```
sdwan
```

Mode

Config

Description

Enter SD-WAN configuration mode.

Example

```
sdwan
```

Syntax

```
no group <SDWAN_GROUP_NAME>
```

Mode

SD-WAN

Description

Delete a SD-WAN Group.

Options

<SDWAN_GROUP_NAME> SD-WAN Group Name.
Example: *Social Networking*

Example

```
no group "VoIP"
```

Syntax

```
no groups
```

Mode

SD-WAN

Description

Delete all SD-WAN groups.

Example

```
no groups
```

Syntax

```
group <SDWAN_GROUP_NAME>
```

Mode

SD-WAN

Description

Add/edit SD-WAN Group.

Options

<SDWAN_GROUP_NAME> SD-WAN Group Name.
Example: *Social Networking*

Example

```
group "VoIP"
```

Syntax

```
name <SDWAN_GROUP_NAME>
```

Mode

SD-WAN Group

Description

Set SD-WAN group name.

Options

<SDWAN_GROUP_NAME> SD-WAN Group Name.
Example: *Social Networking*

Example

```
name "VoIP"
```

Syntax

```
interface <SDWAN_GROUP_MEMBER>
```

Mode

SD-WAN Group

Description

Add/Edit group member.

Options

<SDWAN_GROUP_MEMBER> WAN interface name.
Example: *abc*

Example

```
interface X2
```

Syntax

```
no interface <SDWAN_CURRENT_GROUP_MEMBER>
```

Mode

SD-WAN Group

Description

Remove group member.

Options

<SDWAN_CURRENT_GROUP_MEMBER> Group Member Name.
Example: *abc*

Example

```
no interface X1
```

Syntax

```
priority <UINT8>
```

Mode

SD-WAN Group Member

Description

Member Priority in the group.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
priority 2
```

Syntax

```
path-selection-profile <SDWAN_PATH_SELECTION_PROFILE_NAME>
```

Mode

SD-WAN

Description

Add/edit SD-WAN path selection profile.

Options

<SDWAN_PATH_SELECTION_PROFILE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
path-selection-profile "VoIP"
```

Syntax

```
no path-selection-profile <SDWAN_PATH_SELECTION_PROFILE_NAME>
```

Mode

SD-WAN

Description

Delete a SD-WAN path selection profile.

Options

<SDWAN_PATH_SELECTION_PROFILE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no path-selection-profile "Best of All"
```

Syntax

```
no path-selection-profiles
```

Mode

SD-WAN

Description

Delete all SD-WAN path selection profiles.

Example

```
no path-selection-profiles
```

Syntax

```
name <SDWAN_PATH_SELECTION_PROFILE_NAME>
```

Mode

SD-WAN Path Selection Profiles.

Description

Set SD-WAN Path Selection Profile name.

Options

<SDWAN_PATH_SELECTION_PROFILE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name "Best of All"
```

Syntax

```
sdwan-group <SDWAN_PATH_SELECTION_PROFILE_GROUP_NAME>
```

Mode

SD-WAN Path Selection Profiles.

Description

Set SD-WAN group.

Options

<SDWAN_PATH_SELECTION_PROFILE_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".

Example: *abc*

Example

```
sdwan-group "Interface Group 1"
```

Syntax

```
no sdwan-group
```

Mode

SD-WAN Path Selection Profiles.

Description

Clear SD-WAN group.

Example

```
no sdwan-group
```

Syntax

```
performance-probe <SDWAN_PATH_SELECTION_PROFILE_PERFORMANCE_PROBE_NAME>
```

Mode

SD-WAN Path Selection Profiles.

Description

Set performance probe.

Options

<SDWAN_PATH_SELECTION_PROFILE_PERFORMANCE_PROBE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
performance-probe "Ping Probe"
```

Syntax

```
no performance-probe
```

Mode

SD-WAN Path Selection Profiles.

Description

Clear performance probe.

Example

```
no performance-probe
```

Syntax

```
performance-class <SDWAN_PATH_SELECTION_PROFILE_PERFORMANCE_CLASS_NAME>
```

Mode

SD-WAN Path Selection Profiles.

Description

Set performance class.

Options

`<SDWAN_PATH_SELECTION_PROFILE_PERFORMANCE_CLASS_NAME>` Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
performance-class "Lowest Jitter"
```

Syntax

```
no performance-class
```

Mode

SD-WAN Path Selection Profiles.

Description

Clear performance class.

Example

```
no performance-class
```

Syntax

```
backup-interface <SDWAN_PATH_SELECTION_PROFILE_BACKUP_INTERFACE>
```

Mode

SD-WAN Path Selection Profiles.

Description

Set backup interface.

Options

`<SDWAN_PATH_SELECTION_PROFILE_BACKUP_INTERFACE>` Backup interface name.
Example: *X0*

Example

```
backup-interface X5
```

Syntax

```
no backup-interface
```

Mode

SD-WAN Path Selection Profiles.

Description

Clear backup interface.

Example

```
no backup-interface
```

Syntax

probe-default-up

Mode

SD-WAN Path Selection Profiles.

Description

Enable performance probe default state is UP.

Example

probe-default-up

Syntax

no probe-default-up

Mode

SD-WAN Path Selection Profiles.

Description

Disable performance probe default state is UP.

Example

no probe-default-up

Syntax

reset-connections

Mode

SD-WAN Path Selection Profiles.

Description

Enable reset connections if path does not meet the performance criteria.

Example

reset-connections

Syntax

no reset-connections

Mode

SD-WAN Path Selection Profiles.

Description

Disable reset connections if path does not meet the performance criteria.

Example

no reset-connections

Syntax

```
show sdwan performance-class-objects
```

Mode

All Modes

Description

Show all SD-WAN performance class objects.

Example

```
show sdwan performance-class-objects
```

Syntax

```
show sdwan performance-class-object <SDWAN_PERFORMANCE_CLASS_OBJECT_NAME>
```

Mode

All Modes

Description

Show SD-WAN performance class object.

Options

<SDWAN_PERFORMANCE_CLASS_OBJECT_NAME> Atom Object name.
Example: *Lowest Jitter*

Example

```
show sdwan performance-class-object "Best of All"
```

Syntax

```
show sdwan performance-probes [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show all SD-WAN Performance Probes.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

status Show all SD-WAN Performance Probes status.

Example

```
show sdwan-probe performance-probes
```

Syntax

```
show sdwan performance-probe <SDWAN_PROBE_NAME> [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show SD-WAN Performance Probe.

Options

<SDWAN_PROBE_NAME> Atom Object name.
Example: *Web Services Monitor*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

status Show a specific SD-WAN Performance Probe status.

Example

```
show sdwan-probe performance-probe "Remote Servers"
```

Syntax

```
show sdwan group <SDWAN_GROUP_NAME> [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show SD-WAN configuration or status.

Options

<SDWAN_GROUP_NAME> SD-WAN Group Name.
Example: *Social Networking*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

status Show SD-WAN group status.

Example

```
show sdwan group "WAN Group"
```

Syntax

```
show sdwan groups [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show SD-WAN configuration or status.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

status Show SD-WAN groups status.

Example

```
show sdwan groups
```

Syntax

```
show sdwan path-selection-profiles
```

Mode

All Modes

Description

Show all SD-WAN path selection profiles.

Example

```
show sdwan path-selection-profiles
```

Syntax

```
show sdwan path-selection-profile <SDWAN_PATH_SELECTION_PROFILE_NAME>
```

Mode

All Modes

Description

Show SD-WAN path selection profile.

Options

<SDWAN_PATH_SELECTION_PROFILE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
show sdwan path-selection-profile "Best of All"
```

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

About This Document

Legend



WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.



CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.



IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

SonicOS 6.5 E-CLI Reference Guide
Updated - September 2019
Software Version - 6.5
232-005110-00 Rev A

Copyright © 2019 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/en-us/legal/license-agreements>. Select the language based on your geographic location to see the EUPA that applies to your region.

Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035