Configuration Commands

General Security Commands

description

Syntax **description** *description-string*
no description

Context config>system>security>mgmt-access-filter>ip-filter>entry
config>system>security>mgmt-access-filter>ipv6-filter>entry
config>sys>sec>cpm>ip-filter>entry
config>sys>sec>cpm>ipv6-filter>entry
config>sys>sec>cpm>mac-filter>entry
config>sys>security>keychain>direction>bi>entry
config>system>security>keychain>direction>uni>receive>entry
config>system>security>keychain>direction>uni>send>entry
config>system>security>pki>ca-profile
config>sys>security>cpu-protection>policy
config>system>security>mgmt-access-filter>mac-filter>entry
config>system>security>cpm-filter>mac-filter>entry

Description This command creates a text description stored in the configuration file for a configuration context. This command associates a text string with a configuration context to help identify the context in the configuration file.

The **no** form of the command removes the string.

Default No description associated with the configuration context.

Parameters *string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

shutdown

Syntax [**no**] **shutdown**

Context config>system>security>mgmt-access-filter>ip-filter
config>system>security>mgmt-access-filter>ipv6-filter
config>sys>sec>cpm>ip-filter
config>system>security>keychain>direction>bi>entry
config>system>security>keychain>direction>uni>receive>entry

config>system>security>keychain>direction>uni>send>entry
config>system>security>pki>ca-profile
config>sys>sec>cpm>ipv6-filter
config>sys>sec>cpm>mac-filter>entry

Description The **shutdown** command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of the command puts an entity into the administratively enabled state.

Default no shutdown

security

Syntax **security**

Context config>system

Description This command creates the context to configure security settings.

Security commands manage user profiles and user membership. Security commands also manage user login registrations.

ftp-server

Syntax [**no**] **ftp-server**

Context config>system>security

Description This command enables FTP servers running on the system.

FTP servers are disabled by default. At system startup, only SSH server are enabled.

The **no** form of the command disables FTP servers running on the system.

hash-control

Syntax **hash-control** [**read-version** {**1** | **2** | **all**}] [**write-version** {**1** | **2**}]
no hash-control

Context config>system>security

Description Whenever the user executes a **save** or **info** command, the system will encrypt all passwords, MD5 keys, etc., for security reasons. At present, two algorithms exist.

The first algorithm is a simple, short key that can be copied and pasted in a different location when the user wants to configure the same password. However, because it is the same password and the hash key is limited to the password/key, even the casual observer will notice that it is the same key.

The second algorithm is a more complex key, and cannot be copied and pasted in different locations in the configuration file. In this case, if the same key or password is used repeatedly in different contexts, each encrypted (hashed) version will be different.

Default all — read-version set to accept both versions 1 and 2

Parameters **read-version** {**1** | **2** | **all**} **—** When the read-version is configured as "all," both versions 1 and 2 will be accepted by the system. Otherwise, only the selected version will be accepted when reading configuration or exec files. The presence of incorrect hash versions will abort the script/startup.

write-version {**1** | **2**} **—** Select the hash version that will be used the next time the configuration file is saved (or an info command is executed). Be careful to save the read and write version correctly, so that the file can be properly processed after the next reboot or exec.

per-peer-queuing

Syntax [**no**] **per-peer-queuing**

Context config>system>security

Description This command enables CPM hardware queuing per peer. This means that when a peering session is established, the router will automatically allocate a separate CPM hardware queue for that peer.

The **no** form of the command disables CPM hardware queuing per peer.

Default per-peer-queuing

source-address

Syntax **source-address**

Context config>system>security

Description This command specifies the source address that should be used in all unsolicited packets sent by the application.

This feature only applies on inband interfaces and does not apply on the out of band management interface. Packets going out the management interface will keep using that as source IP address. In other words, when the RADIUS server is reachable through both the management interface and a network interface, the management interface is used despite whatever is configured under the source-address statement.

When a source address is specified for the **ptp** application, the port-based 1588 hardware timestamping assist function will be applied to PTP packets matching the IPv4 address of the router interface used to ingress the SR/ESS or IP address specified in this command. If the IP address is removed, then the port-based 1588 hardware timestamping assist function will only be applied to PTP packets matching the IPv4 address of the router interface.

application

Syntax **application** *app* [*ip-int-name*|*ip-address*]
no application *app*

Context config>system>security>source-address

Description This command specifies the use of the source IP address specified by the **source-address** command.

Parameters *app* — Specify the application name.

Values cflowd, dns, ftp, ntp, ping, ptp, radius, snmptrap, sntp, ssh, syslog, tacplus, telnet, traceroute, mcreporter, icmp-error

ip-int-name | *ip-address* — Specifies the name of the IP interface or IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

application6

Syntax **application6** *app ipv6-address*
no application6

Context config>system>security>source-address

Description This command specifies the application to use the source IPv6 address specified by the **source-address** command.

Parameters *app* — Specify the application name.

Values cflowd, dns, ftp, ntp, ping, radius, snmptrap, syslog, tacplus, telnet, traceroute, icmp6-error

ipv6-address — Specifies the IPv6 address.

telnet-server

Syntax [**no**] **telnet-server**

Context config>system>security

Description This command enables Telnet servers running on the system.

Telnet servers are off by default. At system startup, only SSH servers are enabled.

Telnet servers in networks limit a Telnet clients to three retries to login. The Telnet server disconnects the Telnet client session after three retries.

The **no** form of the command disables Telnet servers running on the system.

telnet6-server

Syntax [**no**] **telnet6-server**

Context config>system>security

Description This command enables Telnet IPv6 servers running on the system.

Telnet servers are off by default. At system startup, only SSH server are enabled.

The **no** form of the command disables Telnet IPv6 servers running on the system.

vprn-network-exceptions

Syntax **vprn-network-exceptions** *number seconds*

Context config>system>security

Description This command configures the rate to limit ICMP replies to packets with label TTL expiry received within all VPRN sentences in the system and from all network IP interfaces. This includes labeled user packets, ping and traceroute packets within VPRN.

This feature currently also limits the same packets when received within the context of an LSP short-cut.

This feature does not rate limit MPLS and service OAM packets such as vprn-ping, vprn-trace, lsp-ping, lsp-trace, vccv-ping, and vccv-trace.

The **no** form of the command disables the rate limiting of the reply to these packets.

Default no security vprn-network-exceptions

Parameters *number* — 10 — 10,000

seconds — 1 — 60

LLDP Commands

lldp

Syntax **lldp**

Context config>system

Description This command enables the context to configure system-wide Link Layer Discovery Protocol parameters.

message-fast-tx

Syntax **message-fast-tx** *time*
no message-fast-tx

Context config>system>lldp

Description This command configures the duration of the fast transmission period.

Parameters *time* — Specifies the fast transmission period in seconds.

Values 1 — 3600

Default 1

message-fast-tx-init

Syntax **message-fast-tx-init** *count*
no message-fast-tx-init

Context config>system>lldp

Description This command configures the number of LLDPDUs to send during the fast transmission period.

Parameters *count* — Specifies the number of LLDPDUs to send during the fast transmission period.

Values 1 — 8

Default 4

notification-interval

Syntax **notification-interval** *time*
no notification-interval

Context config>system>lldp

Description This command configures the minimum time between change notifications.

Parameters *time* — Specifies the minimum time, in seconds, between change notifications.

Values	5 — 3600
Default	5

reinit-delay

Syntax **reinit-delay** *time*
no reinit-delay

Context config>system>lldp

Description This command configures the time before re-initializing LLDP on a port.

Parameters *time* — Specifies the time, in seconds, before re-initializing LLDP on a port.

Values	1 — 10
Default	2

tx-credit-max

Syntax **tx-credit-max** *count*
no tx-credit-max

Context config>system>lldp

Description This command configures the maximum consecutive LLDPDUs transmitted.

Parameters *count* — Specifies the maximum consecutive LLDPDUs transmitted.

Values	1 — 100
Default	5

tx-hold-multiplier

Syntax **tx-hold-multiplier** *multiplier*
no tx-hold-multiplier

Context config>system>lldp

Description This command configures the multiplier of the tx-interval.

Parameters *multiplier* — Specifies the multiplier of the tx-interval.

Values 2 — 10

Default 4

tx-interval

Syntax **tx-interval** *interval*
no tx-interval

Context config>system>lldp

Description This command configures the LLDP transmit interval time.

Parameters *interval* — Specifies the LLDP transmit interval time.

Values 1 — 100

Default 5

Login, Telnet, SSH and FTP Commands

exponential-backoff

Syntax [**no**] **exponential-backoff**

Context config>system>login-control

Description This command enables the exponential-backoff of the login prompt. The exponential-backoff command is used to deter dictionary attacks, when a malicious user can gain access to the CLI by using a script to try **admin** with any conceivable password.

The **no** form of the command disables exponential-backoff.

Default no exponential-backoff

ftp

Syntax **ftp**

Context config>system>login-control

Description This command creates the context to configure FTP login control parameters.

idle-timeout

Syntax **idle-timeout** {*minutes* | **disable**}
no idle-timeout

Context config>system>login-control

Description This command configures the idle timeout for FTP, console, or Telnet sessions before the session is terminated by the system.

By default, an idle FTP, console, SSH or Telnet session times out after 30 minutes of inactivity. This timer can be set per session.

The **no** form of the command reverts to the default value.

Default **30** — Idle timeout set for 30 minutes.

Parameters *minutes* — The idle timeout in minutes. Allowed values are 1 to 1440. 0 implies the sessions never timeout.

Values 1 — 1440

disable — When the **disable** option is specified, a session will never timeout. To re-enable idle timeout, enter the command without the disable option.

inbound-max-sessions

Syntax **inbound-max-sessions** *value*
no inbound-max-sessions

Context config>system>login-control>ftp

Description This command configures the maximum number of concurrent inbound FTP sessions.

This value is the combined total of inbound and outbound sessions.

The **no** form of the command reverts to the default value.

Default 3

Parameters *value* — The maximum number of concurrent FTP sessions on the node.

Values 0 — 5

inbound-max-sessions

Syntax **inbound-max-sessions** *number-of-sessions*
no inbound-max-sessions

Context config>system>login-control>telnet
config>system>login-control>ssh

Description This parameter limits the number of inbound Telnet and SSH sessions. A maximum of 30 telnet and ssh connections can be established to the router. The local serial port cannot be disabled.

Telnet and SSH maximum sessions can also use the combined total of both inbound sessions (ssh+telent). While it is acceptable to continue to internally limit the combined total of SSH and Telnet sessions to N, either SSH or Telnet sessions can use the inbound maximum sessions, if so required by the Operator.

The **no** form of the command reverts to the default value.

Default 5

Parameters *number-of-sessions* — The maximum number of concurrent inbound Telnet sessions, expressed as an integer.

Values 0 — 50 (default = 5)
or 0 — N where N is the new total number of SSH+Telent sessions if they are scaled

login-banner

Syntax [**no**] **login-banner**

Context config>system>login-control

Description This command enables or disables the display of a login banner. The login banner contains the SR OS copyright and build date information for a console login attempt.

The **no** form of the command causes only the configured pre-login-message and a generic login prompt to display.

login-control

Syntax **login-control**

Context config>system

Description This command creates the context to configure the session control for console, Telnet and FTP.

motd

Syntax **motd** {**url** *url-prefix*: *source-url* | **text** *motd-text-string*}
no motd

Context config>system>login-control

Description This command creates the message of the day displayed after a successful console login. Only one message can be configured.

The **no** form of the command removes the message.

Default No **motd** is defined.

Parameters **url** *url-prefix*: *source-url* — When the message of the day is present as a text file, provide both url-prefix and the source-url of the file containing the message of the day. The URL prefix can be local or remote.

text *motd-text-string* — The text of the message of the day. The *motd-text-string* must be enclosed in double quotes. Multiple text strings are not appended to one another.

Some special characters can be used to format the message text. The "\n" character creates multi-line MOTDs and the "\r" character restarts at the beginning of the new line. For example, entering "\n\r" will start the string at the beginning of the new line, while entering "\n" will start the second line below the last character from the first line.

outbound-max-sessions

Syntax **outbound-max-sessions** *value*
no outbound-max-sessions

Context config>system>login-control>telnet

Description This parameter limits the number of outbound Telnet and SSH sessions. A maximum of 15 telnet and ssh connections can be established from the router. The local serial port cannot be disabled.

The **no** form of the command reverts to the default value.

Default 5

Parameters *value* — The maximum number of concurrent outbound Telnet sessions, expressed as an integer.

Values 0 — 15

pre-login-message

Syntax **pre-login-message** *login-text-string* [**name**]
no pre-login-message

Context config>system>login-control

Description This command creates a message displayed prior to console login attempts on the console via Telnet.

Only one message can be configured. If multiple **pre-login-messages** are configured, the last message entered overwrites the previous entry.

It is possible to add the name parameter to an existing message without affecting the current **pre-login-message**.

The **no** form of the command removes the message.

Default No **pre-login-message** is defined.

Parameters *login-text-string* — The string can be up to 900 characters. Any printable, 7-bit ASCII characters can be used. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Some special characters can be used to format the message text. The **\n** character creates multiline messages and the **\r** character restarts at the beginning of the new line. For example, entering **\n\r** will start the string at the beginning of the new line, while entering **\n** will start the second line below the last character from the first line.

name — When the keyword *name* is defined, the configured system name is always displayed first in the login message. To remove the name from the login message, the message must be cleared and a new message entered without the name.

ssh

Syntax **ssh**

Context config>system>login-control

Description This command enables the context to configure the SSH parameters.

client-cipher-list protocol-version

Syntax **client-cipher-list protocol-version** *version*

Context config>system>security>ssh

Description This command enables configuration the list of allowed ciphers by the SSH client.

Parameters *version* — Specifies the SSH version.

Values 1 — Specifies that the SSH server will only accept connections from clients that support SSH protocol version 1
2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 2

cipher

Syntax **cipher** *index* **name** *cipher-name*
no cipher *index*

Context config>system>security>ssh>client-cipher-list
config>system>security>ssh>server-cipher-list

Description This command enables configuration of a cipher. Client-ciphers are used when the SR OS is acting as an SSH client. Server-ciphers are used when the SR OS is acting as an SSH server.

Parameters *index* — Specifies the index of the cipher in the list.

Values 1 — 255

cipher-name — Specifies the algorithm for performing encryption or decryption.

Values For SSHv1:
Client ciphers: des, 3des, blowfish
Server ciphers: 3des, blowfish
The following default ciphers are used for SSHv1:

Cipher index value	Cipher name
10	`3des`
20	`blowfish`
30	`des`

Note: blowfish and des are not permitted in FIPS-140-2 mode.

Values For SSHv2:
Client ciphers: 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc, aes128-ctr, aes192-ctr, aes256-ctr
Server ciphers: 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-

cbc, aes256-cbc, rijndael-cbc, aes128-ctr, aes192-ctr, aes256-ctr

The following default ciphers are used for SSHv2:

Cipher index value	Cipher name
190	`aes256-ctr`
192	`aes192-ctr`
194	`aes128-ctr`
200	`aes128-cbc`
205	`3des-cbc`
210	`blowfish-cbc`
215	`cast128-cbc`
220	`arcfour`
225	`aes192-cbc`
230	`aes256-cbc`
235	`rijndael-cbc`

Note: blowfish-cbc, cast128-cbc, arcfour, and rijndael-cbc are not permitted in FIPS-140-2 mode.

Default no cipher *index*

disable-graceful-shutdown

Syntax [**no**] **disable-graceful-shutdown**

Context config>system>login-control>ssh

Description This command enables graceful shutdown of SSH sessions.

The **no** form of the command disables graceful shutdown of SSH sessions.

preserve-key

Syntax [**no**] **preserve-key**

Context config>system>security>ssh

Description After enabling this command, private keys, public keys, and host key file will be saved by the server. It is restored following a system reboot or the ssh server restart.

The **no** form of the command specifies that the keys will be held in memory by the SSH server and is not restored following a system reboot.

Default no preserve-key

server-cipher-list protocol-version

Syntax **client-cipher-list protocol-version** *version*

Context config>system>security>ssh

Description This command enables configuration the list of allowed ciphers by the SSH server.

Parameters *version* — Specifies the SSH version.

Values 1 — Specifies that the SSH server will only accept connections from clients that support SSH protocol version 1
2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 2

server-shutdown

Syntax [**no**] **server-shutdown**

Context config>system>security>ssh

Description This command enables the SSH servers running on the system.

Default At system startup, only the SSH server is enabled.

version

Syntax **version** *ssh-version*
no version

Context config>system>security>ssh

Description Specifies the SSH protocol version that will be supported by the SSH server.

Default 2

Parameters *ssh-version* — Specifies the SSH version.

Values 1 — Specifies that the SSH server will only accept connections from clients that support SSH protocol version 1
2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 2
1-2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 1, or SSH protocol version 2 or both.

Note: "1" and "1-2" are not permitted in FIPS-140-2 mode.

telnet

Syntax **telnet**

Context config>system>login-control

Description This command creates the context to configure the Telnet login control parameters.

enable-graceful-shutdown

Syntax [**no**] **enable-graceful-shutdown**

Context config>system>login-control>telnet

Description This command enables graceful shutdown of telnet sessions.

The no form of the command disables graceful shutdown of telnet sessions.

Management Access Filter Commands

management-access-filter

Syntax [**no**] **management-access-filter**

Context config>system>security

Description This command creates the context to edit management access filters and to reset match criteria.

Management access filters control all traffic in and out of the CPM. They can be used to restrict management of the router by other nodes outside either specific (sub)networks or through designated ports.

Management filters, as opposed to other traffic filters, are enforced by system software.

The **no** form of the command removes management access filters from the configuration.

Default No management access filters are defined.

ip-filter

Syntax [**no**] **ip-filter**

Context config>system>security>mgmt-access-filter

Description This command enables the context to configure management access IP filter parameters.

ipv6-filter

Syntax [**no**] **ipv6-filter**

Context config>system>security>mgmt-access-filter

Description This command enables the context to configure management access IPv6 filter parameters.

mac-filter

Syntax [**no**] **mac-filter**

Context config>system>security>mgmt-access-filter

Description This command configures a management access MAC-filter.

action

Syntax **action** {**permit** | **deny** | **deny-host-unreachable**}
no action

Context config>system>security>mgmt-access-filter>ip-filter>entry
config>system>security>mgmt-access-filter>ipv6-filter>entry
config>system>security>mgmt-access-filter>mac-filter

Description This command creates the action associated with the management access filter match criteria entry.

The **action** keyword is required. If no **action** is defined, the filter is ignored. If multiple action statements are configured, the last one overwrites previous configured actions.

If the packet does not meet any of the match criteria the configured **default action** is applied.

Default none — The action is specified by default-action command.

Parameters *permit* — Specifies that packets matching the configured criteria will be permitted.

deny — Specifies that packets matching the configured selection criteria will be denied and that a ICMP host unreachable message will not be issued.

deny-host-unreachable — Specifies that packets matching the configured selection criteria will be denied and that a host unreachable message will not be issued.
Note: deni-host-unreachable only applies to ip-filter and ipv6filter.

default-action

Syntax **default-action** {**permit** | **deny** | **deny-host-unreachable**}

Context config>system>security>mgmt-access-filter>ip-filter
config>system>security>mgmt-access-filter>ipv6-filter
config>system>security>mgmt-access-filter>mac-filter

Description This command creates the default action for management access in the absence of a specific management access filter match.

The **default-action** is applied to a packet that does not satisfy any match criteria in any of the management access filters. Whenever management access filters are configured, the **default-action** must be defined.

Default No default-action is defined.

Parameters **permit —** Specifies that packets not matching the configured selection criteria in any of the filter entries will be permitted.

deny — Specifies that packets not matching the selection criteria be denied and that an ICMP host unreachable message will not be issued.

deny-host-unreachable — Specifies that packets not matching the selection criteria be denied access and that an ICMP host unreachable message will be issued. **Note:** deni-host-unreachable only applies to ip-filter and ipv6filter.

dst-port

Syntax [**no**] **dst-port** *value* [*mask*]

Context config>system>security>mgmt-access-filter>ip-filter>entry
config>system>security>mgmt-access-filter>ipv6-filter>entry

Description This command configures a source TCP or UDP port number or port range for a management access filter match criterion.

The **no** form of the command removes the source port match criterion.

Default No dst-port match criterion.

Parameters *value* — The source TCP or UDP port number as match criteria.

Values 1 — 65535 (decimal)

mask — Mask used to specify a range of source port numbers as the match criterion.

This 16 bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	`DDDDD`	`63488`
Hexadecimal	`0xHHHH`	`0xF800`
Binary	`0bBBBBBBBBBBBBBBBB`	`0b1111100000000000`

To select a range from 1024 up to 2047, specify 1024 0xFC00 for value and mask.

Default **65535** (exact match)

Values 1 — 65535 (decimal)

entry

Syntax [**no**] **entry** *entry-id*

Context config>system>security>mgmt-access-filter>ip-filter
config>system>security>mgmt-access-filter>ipv6-filter
config>system>security>mgmt-access-filter>mac-filter

Description This command is used to create or edit a management access IP(v4), IPv6, or MAC filter entry. Multiple entries can be created with unique *entry-id* numbers. The OS exits the filter upon the first match found and executes the actions according to the respective action command. For this reason, entries must be sequenced correctly from most to least explicit.

An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword **action** defined to be considered complete. Entries without the **action** keyword are considered incomplete and inactive.

The **no** form of the command removes the specified entry from the management access filter.

Default No entries are defined.

Parameters *entry-id* — An entry ID uniquely identifies a match criteria and the corresponding action. It is recommended that entries are numbered in staggered increments. This allows users to insert a new entry in an existing policy without having to renumber the existing entries.

Values 1 — 9999

flow-label

Syntax **flow-label** *value*
no flow-label

Context config>system>security>mgmt-access-filter>ipv6-filter>entry

Description This command configures flow label match conditions. Flow labeling enables the labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as non-default quality of service or real-time service.

Parameters *value* — Specify the flow identifier in an IPv6 packet header that can be used to discriminate traffic flows (See RFC 3595, *Textual Conventions for IPv6 Flow Label*.)

Values 0 — 1048575

log

Syntax [**no**] log

Context config>system>security>mgmt-access-filter>ip-filter>entry
config>system>security>mgmt-access-filter>ipv6-filter>entry
config>system>security>mgmt-access-filter>mac-filter

Description This command enables match logging. When enabled, matches on this entry will cause the Security event mafEntryMatch to be raised.

Default no log

next-header

Syntax **next-header** *next-header*
no next-header

Context config>system>security>mgmt-access-filter>ipv6-filter>entry

Description This command specifies the next header to match. The protocol type such as TCP / UDP / OSPF is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6), UDP(17). IPv6 Extension headers are identified by the next header IPv6 numbers as per RFC2460.

Parameters *next-header* — Specifies for IPv4 MAF the IP protocol field, and for IPv6 the next header type to be used in the match criteria for this Management Access Filter Entry.

Values next-header: 0 — 255, protocol numbers accepted in DHB
keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-icmp, ipv6-no-nxt, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp

protocol

Syntax [**no**] **protocol** *protocol-id*

Context config>system>security>mgmt-access-filter>ip-filter>entry

Description This command configures an IP protocol type to be used as a management access filter match criterion.

The protocol type, such as TCP, UDP, and OSPF, is identified by its respective protocol number. Well-known protocol numbers include ICMP (1), TCP (6), and UDP (17).

The **no** form the command removes the protocol from the match criteria.

Default No protocol match criterion is specified.

Parameters *protocol* — The protocol number for the match criterion.

Values 1 to 255 (decimal)

port

Syntax **port** *tcp/udp port-number* [*mask*]
port-list *port-list-name*
port range *start end*
no port

Context config>system-security>cpm-filter>ip-filter>entry>match
config>system>security>cpm-filter>ipv6-filter>entry>match

Description This command configures a TCP/UDP source or destination port match criterion in IPv4 and IPv6 CPM filter policies. A packet matches this criterion if packet's TCP/UDP (as configured by protocol/next-header match) source OR destination port matches either the specified port value or a port in the specified port range or port list.

This command is mutually exclusive with **src-port** and **dst-port** commands.

The **no** form of this command deletes the specified port match criterion.

Default **no port**

Parameters *port-number* — A source or destination port to be used as a match criterion specified as a decimal integer.

Values 1 -65535

mask — Specifies the 16 bit mask to be applied when matching the port.

Values [0x0000..0xFFFF] | [0..65535] | [0b0000000000000000..0b1111111111111111]

range *start end* — an inclusive range of source or destination port values to be used as match criteria. *start* of the range and *end* of the range are expressed as decimal integers.

Values start, end, port-number: 1 -65535

port-list *port-list-name* — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

router

Syntax **router service-name** *service-name*
router {*router-instance*}
no router

Context config>system>security>mgmt-access-filter>ip-filter>entry
config>system>security>mgmt-access-filter>ipv6-filter>entry

Description This command configures a router name or service ID to be used as a management access filter match criterion.

The **no** form the command removes the router name or service ID from the match criteria.

Parameters *router-instance* — Specify one of the following parameters for the router instance:

router-name — Specifies a router name up to 32 characters to be used in the match criteria.

service-id — Specifies an existing service ID to be used in the match criteria.

Values 1 — 2147483647

service-name *service-name* — Specifies an existing service name up to 64 characters in length.

renum

Syntax **renum** *old-entry-number new-entry-number*

Context config>system>security>mgmt-access-filter>ip-filter
config>system>security>mgmt-access-filter>ipv6-filter
config>system>security>mgmt-access-filter>mac-filter

Description This command renumbers existing management access filter entries for an IP(v4), IPv6, or MAC filter to re-sequence filter entries.

The exits on the first match found and executes the actions in accordance with the accompanying **action** command. This may require some entries to be re-numbered differently from most to least explicit.

Parameters *old-entry-number* — Enter the entry number of the existing entry.

Values 1 — 9999

new-entry-number — Enter the new entry number that will replace the old entry number.

Values 1 — 9999

shutdown

Syntax [**no**] **shutdown**

Context config>system>security>mgmt-access-filter>ip-filter
config>system>security>mgmt-access-filter>ipv6-filter
config>system>security>mgmt-access-filter>mac-filter

Description This command shutdowns the management-access-filter.

match

Syntax **match** [**frame-type** *frame-type*]
no match

Context config>system>security>mgmt-access-filter>mac-filter>entry

Description This command configures math criteria for this MAC filter entry.

Parameters **frame-type** *frame-type* **—** Specifies the type of MAC frame to use as match criteria.

Values none, 802dot2-llc, ethernet_II

cfm-opcode

Syntax **cfm-opcode** {**lt** | **gt** | **eq**} *opcode*
cfm-opcode range *start end*
no cfm-opcode

Context config>system>security>mgmt-access-filter>mac-filter>entry

Description This command specifies the type of opcode checking to be performed.

If the cfm-opcode match condition is configured then a check must be made to see if the Ethertype is either IEEE802.1ag or Y1731. If the Ethertype does not match then the packet is not CFM and no match to the cfm-opcode is attempted.

The CFM (ieee802.1ag or Y1731) opcode can be assigned as a range with a start and an end number or with a (less than lt, greater than gt, or equal to eq) operator.

If no range with a start and an end or operator (lt, gt, eq) followed by an opcode with the value between 0 and 255 is defined then the command is invalid.

The following table provides opcode values.

Table 10: Opcode Values

CFM PDU or Organization	Acronym	Conflgurable Numeric Value (Range)
Reserved for IEEE 802.1 0		0
Continuity Check Message	CCM	1
Loopback Reply	LBR	2
Loopback Message	LBM	3
Linktrace Reply	LTR	4
Linktrace Message	LTM	5
Reserved for IEEE 802.1		6 – 31
Reserved for ITU		32
	AIS	33
Reserved for ITU		34
	LCK	35
Reserved for ITU		36
	TST	37
Reserved for ITU		38
	APS	39
Reserved for ITU		40
	MCC	41
	LMR	42
	LMM	43
Reserved for ITU		44
	1DM	45
	DMR	46
	DMM	47
Reserved for ITU		48 – 63
Reserved for IEEE 802.1 0		64 - 255

Defined by	ITU-T Y.1731	32 - 63
Defined by	IEEE 802.1.	64 - 255

Default no cfm-opcode

Parameters *opcode* — Specifies the opcode checking to be performed.

start — specifies the start number.

Values 0 — 255

end — Specifies the end number.

Values 0 — 255

lt|gt|eq — keywords

dot1p

Syntax **dot1p** *dot1p-value* [*dot1p-mask*]

Context config>system>security>mgmt-access-filter>mac-filter>entry>match

Description This command configures Dot1p match conditions.

Parameters *dot1p-value* — The IEEE 802.1p value in decimal.

Values 0 — 7

mask — This 3-bit mask can be configured using the following formats:

Values 0 — 7

dsap

Syntax **dsap** *dsap-value* [*dsap-mask*]

Context config>system>security>mgmt-access-filter>mac-filter>entry>match

Description This command configures dsap match conditions.

Format Style	Format Syntax	Example
Decimal	D	4
Hexadecimal	0xH	0x4
Binary	0bBBB	0b100

Parameters *dsap-value* — The 8-bit dsap match criteria value in hexadecimal.

Values 0x00 — 0xFF (hex)

mask — This is optional and may be used when specifying a range of dsap values to use as the match criteria.

This 8 bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	`DDD`	`240`
Hexadecimal	`0xHH`	`0xF0`
Binary	`0bBBBBBBBB`	`0b11110000`

Default FF (hex) (exact match)

Values 0x00 — 0xFF

dst-mac

Syntax **dst-mac** *ieee-address* [*ieee-address-mask*]
no dst-mac

Context config>system>security>mgmt-access-filter>mac-filter>entry>match

Description This command configures the destination MAC match condition.

Parameters *ieee-address* — The MAC address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

mask — A 48-bit mask to match a range of MAC address values.

etype

Syntax **etype** *0x0600xx0xffff*
no etype

Context config>system>security>mgmt-access-filter>mac-filter>entry>match

Description Configures an Ethernet type II Ethertype value to be used as a MAC filter match criterion.

The Ethernet type field is a two-byte field used to identify the protocol carried by the Ethernet frame. For example, 0800 is used to identify the IPv4 packets.

The Ethernet type field is used by the Ethernet version-II frames. IEEE 802.3 Ethernet frames do not use the type field. For IEEE 802.3 frames, use the dsap, ssap or snap-pid fields as match criteria.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. Refer to the Router Configuration Guide for information about MAC Match Criteria Exclusivity Rules fields that are exclusive based on the frame format.

The **no** form of the command removes the previously entered etype field as the match criteria.

Default no etype

Parameters *ethernet-type* — The Ethernet type II frame Ethertype value to be used as a match criterion expressed in hexadecimal.

Values 0x0600 — 0xFFFF

snap-oui

Syntax **snap-oui** {**zero | non-zero**}

Context config>system>security>mgmt-access-filter>mac-filter>entry>match

Description This command configures an IEEE 802.3 LLC SNAP Ethernet Frame OUI zero or non-zero value to be used as a MAC filter match criterion.

The **no** form of the command removes the criterion from the match criteria.

Default no snap-oui

Parameters **zero —** Specifies to match packets with the three-byte OUI field in the SNAP-ID set to zero.

non-zero — Specifies to match packets with the three-byte OUI field in the SNAP-ID not set to zero.

snap-pid

Syntax **snap-pid** *snap-pid*
no snap-pid

Context config>system>security>mgmt-access-filter>mac-filter>entry>match

Description This command configures an IEEE 802.3 LLC SNAP Ethernet Frame PID value to be used as a MAC filter match criterion.

This is a two-byte protocol id that is part of the IEEE 802.3 LLC SNAP Ethernet Frame that follows the three-byte OUI field.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. Refer to the Router Configuration Guide for information about MAC Match Criteria Exclusivity Rules fields that are exclusive based on the frame format.

Note: The snap-pid match criterion is independent of the OUI field within the SNAP header. Two packets with different three-byte OUI fields but the same PID field will both match the same filter entry based on a snap-pid match criteria.

The **no** form of the command removes the snap-pid value as the match criteria.

Default no snap-pid

Parameters *pid-value* — The two-byte snap-pid value to be used as a match criterion in hexadecimal.

Values 0x0000 — 0xFFFF

src-mac

Syntax **src-mac** *ieee-address* [*ieee-address-mask*]
no src-mac

Context config>system>security>mgmt-access-filter>mac-filter>entry>match

Description This command configures a source MAC address or range to be used as a MAC filter match criterion.

The **no** form of the command removes the source mac as the match criteria.

Default no src-mac

Parameters *ieee-address* — Enter the 48-bit IEEE mac address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

ieee-address-mask — This 48-bit mask can be configured using:

Format Style	Format Syntax	Example
Decimal	DDDDDDDDDDDDDD	281474959933440
Hexadecimal	0xHHHHHHHHHHHH	0x0FFFFF000000
Binary	0bBBBBBBB...B	0b11110000...B

To configure so that all packets with a source MAC OUI value of 00-03-FA are subject to a match condition then the entry should be specified as: 003FA000000 0xFFFFFF000000

Default 0xFFFFFFFFFFFF (exact match)

Values 0x00000000000000 — 0xFFFFFFFFFFFF

ssap

Syntax **ssap** *ssap-value* [*ssap-mask*]
no ssap

Context config>system>security>mgmt-access-filter>mac-filter>entry>match

Description This command configures an Ethernet 802.2 LLC SSAP value or range for a MAC filter match criterion.

This is a one-byte field that is part of the 802.2 LLC header of the IEEE 802.3 Ethernet Frame.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. Refer to the Router Configuration Guide for information about MAC Match Criteria Exclusivity Rules fields that are exclusive based on the frame format.

The **no** form of the command removes the ssap match criterion.

Default no ssap

Parameters *ssap-value* — The 8-bit ssap match criteria value in hex.

Values 0x00 — 0xFF

ssap-mask — This is optional and may be used when specifying a range of ssap values to use as the match criteria.

svc-id

Syntax **svc-id** *service-id*
no svc-id

Context config>system>security>mgmt-access-filter>mac-filter>entry>match

Description This command specifies an existing svc-id to use as a match condition.

Parameters *service-id* — Specifies a service-id to match.

Values	*service-id*:	1 — 2147483647
	svc-name:	64 characters maximum

src-port

Syntax **src-port** {*port-id* | **cpm** | **lag** *port-id*}
no src-port

Context config>system>security>mgmt-access-filter>ip-filter>entry
config>system>security>mgmt-access-filter>ipv6-filter>entry

Description This command restricts ingress management traffic to either the CPMCCM Ethernet port or any other logical port (for example LAG) on the device.

When the source interface is configured, only management traffic arriving on those ports satisfy the match criteria.

The **no** form of the command reverts to the default value.

Default any interface

Parameters *port-id* — The port ID in the following format: slot[/mda]/port.

For example: To configure port 3 on MDA 2 on card 1 would be specified as 1/2/3.

Values

port-id	*slot*/*mda*/*port*[.*channel*]	
encap-val	0	for null
	0 — 4094 for dot1q	
aps-id	aps-*group-id*[.*channel*]	
aps	keyword	
group-id	1 — 64	
ccag-idccag-*id*. *path-id*[*cc-type*]		
	ccag	keyword
	id	1 — 8
	path-id	a, b
	cc-type	.sap-net, .net-sap
	cc-id	0 — 4094
lag-id	lag-*id*	
	lag	keyword
	id	1 — 800
cpm	keyword	

cpm — Configure the Ethernet port on the primary to match the criteria.

src-ip

Syntax [**no**] **src-ip** {[*ip-prefixlmask*] | [*ip-prefix*] | **ip-prefix-list** *prefix-list-name*}

Context config>system>security>mgmt-access-filter>ip-filter>entry

Description This command configures a source IP address range prefix to be used as a management access filter match criterion.

The **no** form of the command removes the source IP address match criterion.

Default No source IP match criterion is specified.

Parameters *ip-prefix’mask* — The IP prefix for the IP match criterion in dotted decimal notation.

ip-prefix-list — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

ip-prefix-list-name — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

mask — Specifies the subnet mask length expressed as a decimal integer.

Values 1 — 32 (mask length), 0.0.0.0 — 255.255.255.255 (dotted decimal)

src-ip

Syntax [**no**] **src-ip** {[*ip-prefixlmask*] | [*ip-prefix*] | **ip-prefix-list** *prefix-list-name*}

Context config>system>security>mgmt-access-filter>ipv6-filter>entry

Description This command configures a source IPv6 address range prefix to be used as a management access filter match criterion.

The **no** form of the command removes the source IPv6 address match criterion.

Default No source IP match criterion is specified.

Parameters *ip-prefix'mask* — The IP prefix for the IP match criterion in dotted decimal notation.

ip-prefix-list — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

ipv6-prefix-list-name — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

mask — Specifies the subnet mask length expressed as a decimal integer.

Values 1 — 32 (mask length), 0.0.0.0 — 255.255.255.255 (dotted decimal)

Password Commands

password

Syntax **password**

Context config>system>security

Description This command creates the context to configure password management parameters.

admin-password

Syntax **admin-password** *password* [**hash** | **hash2**]
no admin-password

Context config>system>security>password

Description This command allows a user (with admin permissions) to configure a password which enables a user to become an administrator.

This password is valid only for one session. When enabled, no authorization to TACACS+ or RADIUS is performed and the user is locally regarded as an admin user.

This functionality can be enabled in two contexts:

config>system>security>password>admin-password

<global> enable-admin

NOTE: See the description for the **enable-admin** on the next page. If the admin-password is configured in the config>system>security>password context, then any user can enter the special mode by entering the **enable-admin** command.

enable-admin is in the default profile. By default, all users are given access to this command.

Once the **enable-admin** command is entered, the user is prompted for a password. If the password matches, user is given unrestricted access to all the commands.

The minimum length of the password is determined by the **minimum-length** command. The complexity requirements for the password is determined by the **complexity** command.

NOTE: The *password* argument of this command is not sent to the servers. This is consistent with other commands which configure secrets.

Also note that usernames and passwords in the FTP and TFTP URLs will not be sent to the authorization or accounting servers when the **file>copy** *source-url dest-url* command is executed.

For example:

```
file copy ftp://test:secret@131.12.31.79/test/srcfile cf1:\destfile
```

In this example, the username 'test' and password 'secret' will not be sent to the AAA servers (or to any logs). They will be replaced with '****'.

The **no** form of the command removes the admin password from the configuration.

Default no admin-password

Parameters *password* — Configures the password which enables a user to become a system administrator. The maximum length can be up to 20 characters if unhashed, 32 characters if hashed, 54 characters if the hash2 keyword is specified.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

enable-admin

Syntax **enable-admin**

Context <global>

Description **NOTE:** See the description for the **admin-password** on the previous page. If the **admin-password** is configured in the config>system>security>password context, then any user can enter the special administrative mode by entering the **enable-admin** command.

enable-admin is in the default profile. By default, all users are given access to this command.

Once the **enable-admin** command is entered, the user is prompted for a password. If the password matches, user is given unrestricted access to all the commands.

The minimum length of the password is determined by the **minimum-length** command. The complexity requirements for the password is determined by the **complexity** command.

There are two ways to verify that a user is in the enable-admin mode:

- show users — Administrator can know which users are in this mode.
- Enter the enable-admin command again at the root prompt and an error message will be returned.

```
A:ALA-1# show users
===============================================================================
User Type From Login time Idle time
===============================================================================
admin Console -- 10AUG2006 13:55:24 0d 19:42:22
admin Telnet 10.20.30.93 09AUG2006 08:35:23 0d 00:00:00 A
-------------------------------------------------------------------------------
Number of users : 2
'A' indicates user is in admin mode
===============================================================================
A:ALA-1#
A:ALA-1# enable-admin
MINOR: CLI Already in admin mode.
A:ALA-1#
```

aging

Syntax **aging** *days*
no aging

Context config>system>security>password

Description This command configures the number of days a user password is valid before the user must change their password. This parameter can be used to force the user to change the password at the configured interval.

The **no** form of the command reverts to the default value.

Default No aging is enforced.

Parameters *days* — The maximum number of days the password is valid.

Values 1 — 500

attempts

Syntax **attempts** *count* [**time** *minutes1* [**lockout** *minutes2*]
no attempts

Context config>system>security>password

Description This command configures a threshold value of unsuccessful login attempts allowed in a specified time frame.

If the threshold is exceeded, the user is locked out for a specified time period.

If multiple **attempts** commands are entered, each command overwrites the previously entered command.

The **no attempts** command resets all values to default.

Default **count**: **3**
time *minutes*: **5**
lockout *minutes*: **10**

Parameters *count* — The number of unsuccessful login attempts allowed for the specified **time**. This is a mandatory value that must be explicitly entered.

Values 1 — 64

time *minutes* **—** The period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out.

Values 0 — 60

lockout *minutes* **—** The lockout period in minutes where the user is not allowed to login. Allowed values are decimal integers.

Values 0 — 1440 | infinite

When the user exceeds the attempted count times in the specified time, then that user is locked out from any further login attempts for the configured time period.

Default 10

Values 0 — 1440

Values infinite; user is locked out and must wait until manually unlocked before any further attempts.

authentication-order

Syntax **authentication-order** [*method-1*] [*method-2*] [*method-3*] [**exit-on-reject**]
no authentication-order

Context config>system>security>password

Description This command configures the sequence in which password authentication, authorization, and accounting is attempted among RADIUS, TACACS+, and local passwords.

The order should be from the most preferred authentication method to the least preferred. The presence of all methods in the command line does not guarantee that they are all operational. Specifying options that are not available delays user authentication.

If all (operational) methods are attempted and no authentication for a particular login has been granted, then an entry in the security log register the failed attempt. Both the attempted login identification and originating IP address is logged with the a timestamp.

The **no** form of the command reverts to the default authentication sequence.

Default **authentication-order radius tacplus local** - The preferred order for password authentication is 1. RADIUS, 2. TACACS+ and 3. local passwords.

Parameters *method-1* — The first password authentication method to attempt.

Default radius

Values radius, tacplus, local

method-2 — The second password authentication method to attempt.

Default tacplus

Values radius, tacplus, local

method-3 — The third password authentication method to attempt.

Default local

Values radius, tacplus, local

radius — RADIUS authentication.

tacplus — TACACS+ authentication.

local — Password authentication based on the local password database.

exit-on-reject — When enabled and if one of the AAA methods configured in the authentication order sends a reject, then the next method in the order will not be tried. If the **exit-on-reject** keyword is not specified and if one AAA method sends a reject, the next AAA method will be attempted. If in this process, all the AAA methods are exhausted, it will be considered as a reject.

Note that a rejection is distinct from an unreachable authentication server. When the **exit-on-reject** keyword is specified, authorization and accounting will only use the method that provided an affirmation authentication; only if that method is no longer readable or is removed from the configuration will other configured methods be attempted. If the local keyword is the first authentication and:

- **exit-on-reject** is configured and the user does not exist, the user will not be authenticated.
- The user is authenticated locally, then other methods, if configured, will be used for authorization and accounting.
- The user is configured locally but without console access, login will be denied.

complexity-rules

Syntax **complexity**-rules

Context config>system>security>password

Description This defines a list of rules for configurable password options.

allow-user-name

Syntax [**no**] **allow-user-name**

Context config>system>security>password>complexity-rules

Description The user name is allowed to be used as part of the password.

The **no** form of the command does not allow user name to be used as password

credits

Syntax **credits** [**lowercase** *credits*] [**uppercase** *credits*] [**numeric** *credits*] [**special-character** *credits*]
no credits

Context config>system>security>password>complexity-rules

Description The maximum credits given for usage of the different character classes in the local passwords.

The **no** form of the command resets to default.

Default no credits

Parameters *credits* — The number of credits that can be used for each characters class.

Values 0-10

minimum-classes

Syntax **minimum-classes** *minimum*
no minimum-classes

Context config>system>security>password>complexity-rules

Description Force the use of at least this many different character classes

The no form of the command resets to default.

Default no minimum-classes

Parameters *minmum* — The minimum number of classes to be configured.

Values 2-4

minimum-length

Syntax **minimum-length** *length*
no minimum-length

Context config>system>security>password

Description This command configures the minimum number of characters required for locally administered passwords, HMAC-MD5-96, HMAC-SHA-96, and des-keys configured in the system security section.

If multiple minimum-length commands are entered each command overwrites the previous entered command.

The **no** form of the command reverts to default value.

Default **minimum-length 6**

Parameters *value* — The minimum number of characters required for a password.

Values 1 — 8

repeated-characters

Syntax **repeated-characters** *count*
no repeated-characters

Context config>system>security>password>complexity-rules

Description The number of times a characters can be repeated consecutively.

The **no** form of the command resets to default.

Default no repeated-characters

Parameters *count* — The minimum count of consecutively repeated characters.

Values 2-8

required

Syntax **required** [**lowercase** *count*] [**uppercase** *count*] [**numeric** *count*] [**special-character** *count*]
no required

Context config>system>security>password>complexity-rules

Description Force the minimum number of different character classes required.

The **no** form of the command resets to default.

Default no required

Parameters *count* — The minimum count of characters classes.

Values 0-10

dynsvc-password

Syntax **dynsvc-password** *password* [**hash|hash2**]
no dynsvc-password

Context config>system>security>password

Description Configure the password which enables the user to configure dynamic services.

Default no dynsvc-password

Parameters *password* — Configures the password which enables a user to become a system administrator. The maximum length can be up to 20 characters if unhashed, 32 characters if hashed, 54 characters if the hash2 keyword is specified.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

enable-admin-control

Syntax **enable-admin-control**

Context config>system>security>password

Description Enable the user to become a system administrator.

tacplus-map-to-priv-lvl

Syntax **tacplus-map-to-priv-lvl** [*admin-priv-lvl*]
no tacplus-map-to-priv-lvl

Context config>system>security>password>enable-admin-control

Description When **tacplus-map-to-priv-lvl** is enabled, and tacplus authorization is enabled with the *use-priv-lvl* option, typing **enable-admin** starts an interactive authentication exchange from the SR OS node to the TACACS+ server. The start message (service=enable) contains the user-id and the requested admin-priv-lvl. Successful authentication results in the use of a new profile (as configured under **config>system>security>tacplus>priv-lvl-map**).

health-check

Syntax [**no**] **health-check** [**interval** *interval*]

Context config>system>security>password

Description This command specifies that RADIUS and TACACS+ servers are monitored for 3 seconds each at 30 second intervals. Servers that are not configured will have 3 seconds of idle time. If in this process a server is found to be unreachable, or a previously unreachable server starts responding, based on the type of the server, a trap will be sent.

The **no** form of the command disables the periodic monitoring of the RADIUS and TACACS+ servers. In this case, the operational status for the active server will be up if the last access was successful.

Default health-check 30

Parameters **interval** *interval* **—** Specifies the polling interval for RADIUS servers.

Values 6 — 1500

history

Syntax **history** *size*
no history

Context config>system>security>password

Description Configure how many previous passwords a new password is matched against.

Default no history

Parameters *size* — Specifies how many previous passwords a new password is matched against.

Values 1—20

minimum-age

Syntax **minimum-age** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no minimum-age

Context config>system>security>password

Description Configure the minimum required age of a password before it can be changed again.

Default no minimum-age

Parameters *days* — Specifies the minimum required days of a password before it can be changed again.

Values 0—1

hours — Specifies the minimum required hours of a password before it can be changed again.

Values 0—23

minutes — Specifies the minimum required minutes of a password before it can be changed again.

Values 0—59

seconds — Specifies the minimum required seconds of a password before it can be changed again.

Values 0—59

minimum-change

Syntax **minimum-change** *length*
no minimum-change

Context config>system>security>password

Description This command configures the minimum number of characters required to be different in the new password from a previous password.

The **no** form of the command reverts to default value.

Default no min-change

Parameters *length* — Specifies how many characters must be different in the new password from the old password.

Values 2—20

Public Key Infrastructure (PKI) Commands

pki

Syntax **pki**

Context config>system>security

Description This command enables the context to configure certificate parameters.

Default none

ca-profile

Syntax **ca-profile** *name* [**create**]
no ca-profile *name*

Context config>system>security>pki

Description This command creates a new **ca-profile** or enter the configuration context of an existing **ca-profile**. Up to 128 ca-profiles could be created in the system. A **shutdown** the ca-profile will not affect the current up and running **ipsec-tunnel** or **ipsec-**gw that associated with the **ca-profile**. But authentication afterwards will fail with a **shutdown ca-profile**.

Executing a **no shutdown** command in this context will cause system to reload the configured cert-file and crl-file.

A **ca-profile** can be applied under the **ipsec-tunnel** or **ipsec-gw** configuration.

The **no** form of the command removes the name parameter from the configuration. A ca-profile can not be removed until all the association(ipsec-tunnel/gw) have been removed.

Parameters *name* — Specifies the name of the **ca-profile**, a string up to 32 characters.

create — Keyword used to create a new **ca-profile**. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

cert-file

Syntax **cert-file** *filename*
no cert-file

Context config>system>security>pki>ca-profile

Description Specifies the filename of a file in cf3:\system-pki\cert as the CA’s certificate of the ca-profile.

Notes:

- The system will perform following checks against configured cert-file when a **no shutdown** command is issued:
  - → Configured cert-file must be a DER formatted X.509v3 certificate file.
  - → All non-optional fields defined in section 4.1 of RFC5280 must exist and conform to the RFC 5280 defined format.
  - → Check the version field to see if its value is 0x2.
  - → Check The Validity field to see that if the certificate is still in validity period.
  - → X509 basic constraints extension must exists, and CA Boolean must be True.
  - → If Key Usage extension exists, then at least keyCertSign and cRLSign should be asserted.
  - → If the certificate is not a self-signing certificate , then system will try to look for issuer's CA's certificate to verify if this certificate is signed by issuer's CA; but if there is no such CA-profile configured, then system will just proceed with a warning message.
  - → If the certificate is not a self-signing certificate, then system will try to look for issuer's CA's CRL to verify that it has not been revoked; but if there is no such CA-profile configured or there is no such CRL, then system will just proceed with a warning message.

  If any of above checks fails, then the **no shutdown** command will fail.
- Changing or removing of **cert-file** is only allowed when the **ca-profile** is in a **shutdown** state.

The **no** form of the command removes the filename from the configuration.

Parameters *filename* — Specifies a local CF card file URL.

accept-unprotected-errormsg

Syntax [**no**] **accept-unprotected-errormsg**

Context config>system>security>pki>ca-profile>cmpv2

Description This command enables the system to accept both protected and unprotected CMPv2 error message. Without this command, system will only accept protected error messages.

The **no** form of the command causes the system to only accept protected PKI confirmation message.

Default no

accept-unprotected-pkiconf

Syntax [**no**] **accept-unprotected-pkiconf**

Context config>system>security>pki>ca-profile>cmpv2

Description This command enables the system to accept both protected and unprotected CMPv2 PKI confirmation messages. Without this command, system will only accept protected PKI confirmation message.

The **no** form of the command causes the system to only accept protected PKI confirmation message.

Default none

key-list

Syntax **cmp-key-list**

Context config>system>security>pki>ca-profile>cmp2

Description This command enables the context to configure pre-shared key list parameters.

key

Syntax **key** *password* [**hash**|**hash2**] **reference** *reference-number*
no key reference *reference-number*

Context config>system>security>pki>ca-profile>cmp2>key-list

Description This command specifies a pre-shared key used for CMPv2 initial registration. Multiples of key commands are allowed to be configured under this context.

The password and reference-number is distributed by the CA via out-of-band means.

The configured password is stored in configuration file in an encrypted form by using SR OS hash2 algorithm.

The **no** form of the command removes the parameters from the configuration.

Default none

Parameters *password* — Specifies a printable ASCII string, up to 64 characters in length.

hash — Specifies that the given password is already hashed using hashing algorithm version 1. A semantic check is performed on the given password field to verify if it is a valid hash 1 key to store in the database.

hash2 — Specifies that the given password is already hashed using hashing algorithm version 2. A semantic check is performed on the given password field to verify if it is a valid hash 2 key to store in the database.

reference *reference-number* — Specifies a printable ASCII string, up to 64 characters in length.

url

Syntax **cmp-url** *url-string* [**service-id** *service-id*]
no cmp-url

Context config>system>security>pki>ca-profile>cmp2

Description This command specifies HTTP URL of the CMPv2 server. The URL must be unique across all configured ca-profiles.

The URL will be resolved by the DNS server configured (if configured) in the corresponding router context.

If the *service-id* is 0 or omitted, then system will try to resolve the FQDN via DNS server configured in bof.cfg. After resolution, the system will connect to the address in management routing instance first, then base routing instance.

Note that if the service is VPRN, then the system only allows HTTP ports 80 and 8080.

Default none

Parameters *url-string* — Specifies the HTTP URL of the CMPv2 server up to 180 characters in length.

service-id *service-id* **—** Specifies the service instance that used to reach CMPv2 server.

Values service-id: 1..2147483647
base-router: 0

http-response-timeout

Syntax **http-response-timeout** *timeout*
no http-response-timeout

Context config>system>security>pki>ca-profile>cmp2

Description This command specifies the timeout value for HTTP response that is used by CMPv2.

The **no** form of the command reverts to the default.

Default 30 seconds

Parameters *timeout* — Specifies the HTTP response timeout in seconds.

Values 1 — 3600

response-signing-cert

Syntax **response-signing-cert** *filename*
no response-signing-cert

Context config>system>security>pki>ca-profile>cmp2

Description This command specifies a imported certificate that is used to verify the CMP response message if they are protected by signature. If this command is not configured, then CA’s certificate will be used.

Default none

Parameters *filename* — Specifies the filename of the imported certificate.

same-recipnonce-for-pollreq

Syntax [**no**] **same-recipnonce-for-pollreq**

Context config>system>security>pki>ca-profile>cmp2

Description This command enables the system to use same recipNonce as the last CMPv2 response for poll request.

Default none

crl-file

Syntax **crl-file** *filename*
no crl-file

Context config>system>security>pki>ca-profile

Description This command specifies the name of a file in cf3:\system-pki\crl as the Certification Revoke List file of the **ca-profile**.

Notes:

- The system will perform following checks against configured crl-file when a **no shutdown** command is issued:
  - → A valid cert-file of the ca-profile must be already configured.
  - → Configured crl-file must be a DER formatted CRLv2 file.
  - → All non-optional fields defined in section 5.1 of RFC5280 must exist and conform to the RFC5280 defined format.
  - → Check the version field to see if its value is 0x1.
  - → Delta CRL Indicator must NOT exists (delta CRL is not supported).
  - → CRL's signature must be verified by using the cert-file of ca-profile.

  If any of above checks fail, the **no shutdown** command will fail.
- Changing or removing the **crl-file** is only allowed when the **ca-profile** is in a **shutdown** state.

The **no** form of the command removes the filename from the configuration.

Default none

Parameters *filename* — Specifies the name of CRL file stored in cf3:\system-pki\crl.

ocsp

Syntax **ocsp**

Context config>system>security>pki>ca-profile

Description This command enables the context to configure OCSP parameters.

responder-url

Syntax **responder-url** *url-string*
no responder-url

Context config>system>security>pki>ca-profile>ocsp

Description This command specifies HTTP URL of the OCSP responder for the CA, this URL will only be used if there is no OCSP responder defined in the AIA extension of the certificate to be verified.

Default no responder-url

Parameters *url-string* — Specifies the HTTP URL of the OCSP responder

service

Syntax **service** *service-id*
no service

Context config>system>security>pki>ca-profile>ocsp

Description This command specifies the service or routing instance that used to contact OCSP responder. This applies to OCSP responders that either configured in CLI or defined in AIA extension of the certificate to be verified.

The responder-url will also be resolved by using the DNS server configured in the configured routing instance.

In case of VPRN service, system will check if the specified service-id or service-name is an existing VPRN service at the time of CLI configuration. Otherwise the configuration will fail.

Parameters *service-id* — Specifies an existing service ID to be used in the match criteria.

Values service-id: 1 — 2147483647
base-router: 0

certificate-display-format

Syntax **certificate-display-format** {**ascii|utf8**}

Context config>system>security>pki

Description This command specifies the display format used for the Certificates and Certificate Revocation Lists.

Default ascii

Parameters **ascii —** Specifies the ASCII format to use for the Certificates and Certificate Revocation Lists.

utf8 — Specifies the UTF8 format to use for the Certificates and Certificate Revocation Lists.

certificate-expiration-warning

Syntax **certificate-expiration-warning** *hours* [**repeat** *repeat-hours*]
no certificate-expiration-warning

Context config>system>security>pki

Description With this command configured, the system will issues two types of warnings related to certificate expiration:

- **BeforeExp —** A warning message issued before certificate expire
- **AfterExp —** A warning message issued when certificate expire

This command specifies when system will issue **BeforeExp** message before a certificate expires. For example, with c**ertificate-expiration-warning 5**, the system will issue a **BeforeExp** message 5 hours before a certificate expires. An optional **repeat** <*repeat-hour*> parameter will enable the system to repeat the **BeforeExp** message every hour until the certificate expires.

If the user only wants **AfterExp**, then **certificate-expiration-warning 0** can be used to achieve this.

BeforeExp and **AfterExp** warnings can be cleared in following cases:

- The certificate is reloaded by the **admin certificate reload** command. In this case, if the reloaded file is not expired, then **AfterExp** is cleared. And, if the reloaded file is outside of configured warning window, then the **BeforeExp** is also cleared.
- When the **ca-profile/ipsec-gw/ipsec-tunnel/cert-profile** is shutdown, then **BeforeExp** and **AfterExp** of corresponding certificates are cleared.
- When **no certificate-expiration-warning** command is configured, then all existing **BeforeExp** and **AfterExp** are cleared.
- Users may change the configuration of the **certificate-expiration-warning** so that certain certificates are no longer in the warning window. **BeforeExp** of corresponding certificates are cleared.
- If the system time changes so that the new time causes the certificates to no longer be in the warning window, then **BeforeExp** is cleared. If the new time causes an expired certificate to come non-expired, then **AfterExp** is cleared.

Default no certificate-expiration-warning

Parameters *hours* — Specfies the amount of time before a certificate expires when system issues BeforeExp.

Values 0 — 8760

repeat *repeat-hours* **—** The system will repeat BeforeExp every repeat-hour.

Values 0 — 8760

crl-expiration-warning

Syntax **crl-expiration-warning** *hours* [**repeat** *repeat-hours*]
no crl-expiration-warning

Context config>system>security>pki

Description This command specifies when system will issue **BeforeExp** message before a CRL expires. For example, with **certificate-expiration-warning 5**, the system will issue a **BeforeExp** message 5 hours before a CRL expires. An optional **repeat** <*repeat-hour*> parameter will enable the system to repeat the **BeforeExp** message every hour until the CRL expires.

If the user only wants **AfterExp**, then **certificate-expiration-warning 0** can be used to achieve this.

BeforeExp and **AfterExp** warnings can be cleared in following cases:

- The CRL is reloaded by the **admin certificate reload** command. In this case, if the reloaded file is not expired, then **AfterExp** is cleared. And, if the reloaded file is outside of configured warning window, then the **BeforeExp** is also cleared.
- When the **ca-profile** is shutdown, then **BeforeExp** and **AfterExp** of corresponding certificates are cleared.
- When **no crl-expiration-warning** command is configured, then all existing **BeforeExp** and **AfterExp** are cleared.
- Users may change the configuration of the **crl-expiration-warning** so that certain CRL are no longer in the warning window. **BeforeExp** of corresponding CRL are cleared.
- If the system time changes so that the new time causes the CRL to no longer be in the warning window, then **BeforeExp** is cleared. If the new time causes an expired CRL to come non-expired, then **AfterExp** is cleared.

Default no crl-expiration-warning

Parameters *hours* — Specifies the amount of time before a CRL expires when system issues **BeforeExp**.

Values 0 — 8760

repeat-hour — Specifies that the system will repeat **BeforeExp** every repeat-hour.

Values 0 — 8760

maximum-cert-chain-depth

Syntax **maximum-cert-chain-depth** *level*

no maximum-cert-chain-depth

Context config>system>security>pki

Description This command defines the maximum depth of certificate chain verification. This number is applied system wide.

The **no** form of the command reverts to the default.

Default 7

Parameters *level* — Specifies the maximum depth level of certificate chain verification, range from 1 to 7. the certificate under verification is not counted in. for example, if this parameter is set to 1, then the certificate under verification must be directly signed by trust anchor CA.

Values 1 — 7

shutdown

Syntax [**no**] **shutdown**

Context config>system>security>pki>ca-profile>

Description Use this command to enable or disable the ca-profile. The system will verify the configured cert-file and crl-file. If the verification fails, then the **no shutdown** command will fail.

The ca-profile in a **shutdown** state cannot be used in certificate authentication.

Default shutdown

certificate[1]

Syntax **certificate**

Context admin

Description This command enables the context to configure X.509 certificate related operational parameters.

clear-ocsp-cache

Syntax **clear-ocsp-cache** [*entry-id*]

Context admin>certificate

Description This command clears the current OCSP response cache. If optional issuer and serial-number are not specified, then all current cached results are cleared.

[1] For information about CMPv6 admin certificate commands, see the *7450 ESS and 7750 SR Multiservice Integrated Service Adapter Guide*.

Parameters *entry-id* — Specifies the local cache entry identifier of the certificate to clear.

Values 1 — 2000

crl-update

Syntax **crl-update ca** *ca-profile-name*

Context admin>certificate

Description This command manually triggers the Certificate Revocation List file (CRL) update for the specified ca-profile.

Using this command requires shutting down the auto-crl-update.

Default None

Parameters **ca** *ca-profile-name* — Specifies the name of the Certificate Authority profile.

display

Syntax **display type** {**cert**|**key**|**crl**|**cert-request**} *url-string* **format** {**pkcs10**|**pkcs12**|**pkcs7-der**|**pkcs7-pem**|**pem**|**der**} [**password** [*32 chars max*]]

Context admin>certificate

Description This command displays the content of an input file in plain text. Note that when displaying the key file content, only the key size and type are displayed.

The following list summarizes the formats supported by this command:

Default

- Certificate
  - → system format
  - → PKCS #12
  - → PKCS #7 PEM encoded
  - → PKCS #7 DER encoded
  - → RFC4945
- Certificate Request
  - → PKCS #10
- Key
  - → system format
  - → PKCS #12
- CRL
  - → system format
  - → PKCS #7 PEM encoded

→ PKCS #7 DER encoded

→ RFC4945

Default none

Parameters *file-url* — Specifies the local CF card url of the input file.

Values	url-string	<local-url> - [99 chars max]
	local-url	<cflash-id>/<file-path>
	cflash-id	cf1:|cf2:|cf3:

type — Specifies the type of input file, possible values are cert/key/crl/cert-request.

Values cert, key, crl, cert-request

format — Specifies the format of input file.

Values pkcs10, pkcs12, pkcs7-der, pkcs7-pem, pem, der

password — Specifies the password to decrypt the input file in case that it is a encrypted PKCS#12 file, up to 99 characters in length.

export

Syntax **export type** {**cert|key|crl**} **input** *filename* **output** *url-string* **format** *output-format* [**password** [*32 chars max*]] [**pkey** *filename*]

Context admin>certificate

Description This command performs certificate operations.

gen-keypair

Syntax **gen-keypair** *url-string* [**size** {**512|1024|2048**}] [**type** {**rsa|dsa**}]

Context admin>certificate

Description This command generatse a RSA or DSA private key/public key pairs and store them in a local file in cf3:\system-pki\key

Parameters *url-string* — Specifies the name of the key file.

Values	url-string	<local-url> - [99 chars max]
	local-url	<cflash-id>/<file-path>
	cflash-id	cf1:|cf2:|cf3:

size — Specifies the key size in bits.
Note: The minimum key-size is 1024 when running in FIPS-140-2 mode.

Values 512/1024/2048

Default 2048

type — Specifies the type of key.

Default rsa

gen-local-cert-req

Syntax **gen-local-cert-req keypair** *url-string* **subject-dn** *subject-dn* [**domain-name** [*255 chars max*]] [**ip-addr** *ip-address*] **file** *url-string* **[hash-alg hash-algorithm]**

Context admin>certificate

Description This command generates a PKCS#10 formatted certificate request by using a local existing key pair file.

Default none

Parameters *url-string* — Specifies the name of the keyfile in cf3:\system-pki\key that is used to generate a certificate request.

Values	url-string	<local-url> - [99 chars max]
	local-url	<cflash-id>/<file-path>
	cflash-id	cf1:|cf2:|cf3:

subject-dn — Specifies the distinguish name that is used as the subject in a certificate request, including:

- C-Country
- ST-State
- O-Organization name
- OU-Organization Unit name
- CN-common name

This parameter is formatted as a text string including any of the above attributes. The attribute and its value is linked by using "=", and "," is used to separate different attributes.

For example: C=US,ST=CA,O=ALU,CN=SR12

Values attr1=val1,attr2=val2... where: attrN={C|ST|O|OU|CN}, 256 chars max

domain-name — Optionally, a domain name string can be specified and included as the dNSName in the Subject Alternative Name extension of the certificate request.

ip-address — Optionally, an IPv4 address string can be specified and included as the ipAddress in the Subject Alternative Name extension of the certificate request.

cert-req-file-url — This URL could be either a local CF card path and filename to save the certificate request; or an FTP URL to upload the certificate request.

hash-alg *hash-algorithm* **—** Specifies the hash algorithm to be used in a certificate request.

Values sha1, sha224, sha256, sha384, sha512

import

Syntax **import type** {**cert|key|crl**} **input** *url-string* **output** *filename* **format** *input-format* [**password** [*32 chars max*]]

Context admin>certificate#

Description This command converts an input file(key/certificate/CRL) to a system format file. The following list summarizes the formats supported by this command:

- Certificate
  - → PKCS #12
  - → PKCS #7 PEM encoded
  - → PKCS #7 DER encoded
  - → PEM
  - → DER
- Key
  - → PKCS #12
  - → PEM
  - → DER
- CRL
  - → PKCS #7 PEM encoded
  - → PKCS #7 DER encoded
  - → PEM
  - → DER

Note that if there are multiple objects with same type in the input file, only first object will be extracted and converted.

Default none

Parameters **input** *url-string* — Specifies the URL for the input file. This URL could be either a local CF card URL file or a FP URL to download the input file.

output *url-string* — Specifies the name of output file up to 95 characters in length. The output directory depends on the file type like following:

- Key: cf3:\system-pki\key
- Cert: cf3:\system-pki\cert
- CRL: cf3:\system-pki\CRL

Values		
	url-string	<local-url> - [99 chars max]
	local-url	<cflash-id>/<file-path>
	cflash-id	cf1:|cf2:|cf3:

type — The type of input file.

Values cert, key, crl

format — Specifies the format of input file.

Values pkcs12, pkcs7-der, pkcs7-pem, pem, der

password — Specifies the password to decrypt the input file in case that it is a encrypted PKCS#12 file.

reload

Syntax **reload type** {**cert**|**key**|**cert-key-pair**} *filename* [**key-file** *filename*]

Context admin>certificate

Description This command reloads imported certificate or key file or both at the same time. This command is typically used to update certificate/key file without shutting down **ipsec-tunne/ipsec-gw/cert-profile/ca-profile**. Note that **type cert** and **type key** will be deprecated in a future release. Use **type cert-key-pair** instead. Instead of **type cert** use **type key** instead.

- If the new file exists and valid, then for each tunnel using it:
  - → If the key matches the certificate, then the new file will be downloaded to the MS-ISA to be used the next time. Tunnels currently up are not affected.
  - → If the key does not match the certificate:
    - → If **cert** and **key** configuration is used instead of **cert-profile** then the tunnel will be brought down.
    - → If **cert-profile** is used, then **cert-profile** will be brought down. The next authentication will fail while the established tunnels are not affected.

If the new file does not exists or somehow invalid (bad format, does not contain right extension, etc.), then this command will abort.

In the case of **type cert-key-pair**, if the new file doesn't exist or is invalid or **cert** and **key** do not match, then this command will abort with an error message.

Default none

Parameters **cert —** Specifies to reload a certificate file.

key — Specifies to reload a key file.

cert-key-pair — Specifies to reload a certificate file and its key file at the same time.

file-name — Specifies the file name of imported certificate or key.

key-filename — In case of cert-key-pair, filename is the imported filename of certificate, key-filename is the imported key file.

secure-nd-export

Syntax **secure-nd-export**

Context admin>certificate

Description This command exports IPv6 Secure Neighbor Discovery (SeND) certificates to the file cf[1..3]:\system-pki\secureNdKey in PKCS #7 DER format.

secure-nd-import

Syntax **secure-nd-import input** *url-string* **format** *input-format* [**password** *password*] [**key-rollover**]

Context admin>certificate

Description This command imports IPv6 Secure Neighbor Discovery (SeND) certificates from a file, and saves them to cf[1..3]:\system-pki\secureNdKey in PKCS #7 DER format.

Parameters **input** *url-string* **—** Specifies the name of an input file up to 99 characters in length.

Values	local-url	<cflash-id>\<file-path>
	cflash-id	cf1:|cf2:|cf3:

format *input-format* — Specifies the input file format.

Values pkcs12, pem, or der

password *password* — Specifies the password to decrypt the input file if it is an encrypted PKCS#12 file.

Values 32 characters maximum

Profile Management Commands

action

Syntax **action** {**deny** | **permit**}

Context config>system>security>profile *user-profile-name*>entry *entry-id*

Description This command configures the action associated with the profile entry.

Parameters **deny —** Specifies that commands matching the entry command match criteria are to be denied.

permit — Specifies that commands matching the entry command match criteria will be permitted.

match

Syntax **match** *command-string*
no match

Context config>system>security>profile *user-profile-name*>entry *entry-id*

Description This command configures a command or subtree commands in subordinate command levels are specified.

Because the OS exits when the first match is found, subordinate levels cannot be modified with subsequent action commands. More specific action commands should be entered with a lower entry number or in a profile that is evaluated prior to this profile.

All commands below the hierarchy level of the matched command are denied.

The **no** form of this command removes a match condition

Default none

Parameters *command-string* — The CLI command or CLI tree level that is the scope of the profile entry.

copy

Syntax **copy** {**user** *source-user* | **profile** *source-profile*} **to** *destination* [**overwrite**]

Context config>system>security

Description This command copies a profile or user from a source profile to a destination profile.

Parameters *source-profile* — The profile to copy. The profile must exist.

dest-profile — The copied profile is copied to the destination profile.

overwrite — Specifies that the destination profile configuration will be overwritten with the copied source profile configuration. A profile will not be overwritten if the **overwrite** command is not specified.

default-action

Syntax **default-action {deny-all | permit-all | none}**

Context config>system>security>profile *user-profile-name*

Description This command specifies the default action to be applied when no match conditions are met.

Default none

Parameters **deny-all —** Sets the default of the profile to deny access to all commands.

permit-all — Sets the default of the profile to permit access to all commands.

Note: permit-all does not change access to security commands. Security commands are only and always available to members of the super-user profile.

none — Sets the default of the profile to no-action. This option is useful to assign multiple profiles to a user.

For example, if a user is a member of two profiles and the default action of the first profile is **permit-all**, then the second profile will never be evaluated because the **permit-all** is executed first. Set the first profile default action to **none** and if no match conditions are met in the first profile, then the second profile will be evaluated. If the default action of the last profile is **none** and no explicit match is found, then the default **deny-all** takes effect.

description

Syntax **description** *description-string*
no description

Context config>system>security>profile *user-profile-name*>entry *entry-id*

Description This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the context in the configuration file.

The **no** form of the command removes the string from the context.

Default No description is configured.

Parameters *string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

entry

Syntax [**no**] **entry** *entry-id*

Context config>system>security>profile *user-profile-name*

Description This command is used to create a user profile entry.

More than one entry can be created with unique *entry-id* numbers. Exits when the first match is found and executes the actions according to the accompanying **action** command. Entries should be sequenced from most explicit to least explicit.

An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword **action** for it to be considered complete.

The **no** form of the command removes the specified entry from the user profile.

Default No entry IDs are defined.

Parameters *entry-id* — An entry-id uniquely identifies a user profile command match criteria and a corresponding action. If more than one entry is configured, the *entry-ids* should be numbered in staggered increments to allow users to insert a new entry without requiring renumbering of the existing entries.

Values 1 — 9999

profile

Syntax [**no**] **profile** *user-profile-name*

Context config>system>security

Description This command creates a context to create user profiles for CLI command tree permissions.

Profiles are used to either deny or permit user console access to a hierarchical branch or to specific commands.

Once the profiles are created, the **user** command assigns users to one or more profiles. You can define up to 16 user profiles but a maximum of 8 profiles can be assigned to a user. The *user-profile-name* can consist of up to 32 alphanumeric characters.

The **no** form of the command deletes a user profile.

Default user-profile default

Parameters *user-profile-name* — The user profile name entered as a character string. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

renum

Syntax **renum** *old-entry-number new-entry-number*

Context config>system>security>profile *user-profile-name*

Description This command renumbers profile entries to re-sequence the entries.

Since the OS exits when the first match is found and executes the actions according to accompanying action command, re-numbering is useful to rearrange the entries from most explicit to least explicit.

Parameters *old-entry-number* — Enter the entry number of an existing entry.

Values 1 — 9999

new-entry-number — Enter the new entry number.

Values 1 — 9999

User Management Commands

access

Syntax [**no**] **access** [**ftp**] [**snmp**] [**console**] [**li**] [**netconf**]

Context config>system>security>user
config>system>security>user-template

Description This command grants a user permission for FTP, SNMP, console or lawful intercept (LI) access.

If a user requires access to more than one application, then multiple applications can be specified in a single command. Multiple commands are treated additively.

The **no** form of command removes access for a specific application.
no access denies permission for all management access methods. To deny a single access method, enter the **no** form of the command followed by the method to be denied, for example, **no access FTP** denies FTP access.

Default No access is granted to the user by default.

Parameters **ftp —** Specifies FTP permission.

snmp — Specifies SNMP permission. This keyword is only configurable in the **config>system>security>user** context.

console — Specifies console access (serial port or Telnet) permission.

li — Allows user to access CLI commands in the lawful intercept (LI) context.

netconf — Allows the user defined in the specified user context to access NETCONF sessions. The user must also have console access permissions configured to operate with NETCONF.

authentication

Syntax **authentication** {[**none**] | [[**hash**] {**md5** *key-1* | **sha** *key-1*} **privacy** {**none|des-key|aes-128-cfb-key** *key-2*}]

Context config>system>security>user>snmp

Description This command configures the authentication and encryption method the user must use in order to be validated by the router. SNMP authentication allows the device to validate the managing node that issued the SNMP message and determine if the message has been tampered.

The keys configured in this command must be localized keys (MD5 or DES hash of the configured SNMP engine-ID and a password).   The password is not directly entered in this command (only the localized key).

Default **authentication none** - No authentication is configured and privacy cannot be configured.

Parameters **none —** Do not use authentication. If **none** is specified, then privacy cannot be configured.

hash — When **hash** is not specified, then non-encrypted characters can be entered. When **hash** is configured, then all specified keys are stored in an encrypted format in the configuration file. The password must be entered in encrypted form when the **hash** parameter is used.

md5 *key* **—** The authentication protocol can either be HMAC-MD5-96 or HMAC-SHA-96.

The MD5 authentication key is stored in an encrypted format. The minimum key length is determined by the **config>system>security>password>minimum-length** value. The maximum length is 16 octets (32 printable characters).

The complexity of the key is determined by the **complexity-rules** command.

sha *key* **—** The authentication protocol can be either HMAC-MD5-96 or HMAC-SHA-96.

The **sha** authentication key is stored in an encrypted format. The minimum key length is determined by the **config>system>security>password>minimum-length** value. The maximum length is 20 octets (40 printable characters).

The complexity of the key is determined by the **complexity-rules** command.

privacy none — Do not perform SNMP packet encryption.

Default privacy none

privacy des-key key-2 — Use DES for SNMP payload encryption and configure the key. The key must be a 32 hex-character string and is stored in an encrypted format.

Note: des-key is not available in FIPS-140-2 mode.

privacy aes-128-cfb-key key-2 — Use 128 bit CFB mode AES for SNMP payload encryption and configure the key. The key must be a 32 hex-character string and is stored in an encrypted format.

Default privacy none

group

Syntax **group** *group-name*
no group

Context config>system>security>user>snmp

Description This command associates (or links) a user to a group name. The group name must be configured with the **config>system>security>user >snmp>group** command. The **access** command links the group with one or more views, security model (s), security level (s), and read, write, and notify permissions

Default No group name is associated with a user.

Parameters *group-name* — Enter the group name (between 1 and 32 alphanumeric characters) that is associated with this user. A user can be associated with one group-name per security model.

cannot-change-password

Syntax [**no**] **cannot-change-password**

Context config>system>security>user>console

Description This command allows a user the privilege to change their password for both FTP and console login.

To disable a user's privilege to change their password, use the **cannot-change-password** form of the command.

Note that the cannot-change-password flag is not replicated when a user copy is performed. A new-password-at-login flag is created instead.

Default no cannot-change-password

console

Syntax **console**

Context config>system>security>user
config>system>security>user-template

Description This command creates the context to configure user profile membership for the console (either Telnet or CPM serial port user).

copy

Syntax **copy** {**user** *source-user* **|** **profile** *source-profile*} **to** *destination* [**overwrite**]

Context config>system>security

Description This command copies a specific user's configuration parameters to another (destination) user.

The password is set to a carriage return and a new password at login must be selected.

Parameters *source-user* — The user to copy. The user must already exist.

dest-user — The copied profile is copied to a destination user.

overwrite — Specifies that the destination user configuration will be overwritten with the copied source user configuration. A configuration will not be overwritten if the **overwrite** command is not specified.

home-directory

Syntax **home-directory** *url-prefix* [*directory*] [*directory/directory…*]
no home-directory

Context config>system>security>user
config>system>security>user-template

Description This command configures the local home directory for the user for both console (file commands and '>' redirection) and FTP access.

If the URL or the specified URL/directory structure is not present, then a warning message is issued and the default is assumed.

The **no** form of the command removes the configured home directory.

Default no home-directory

NOTE: If restrict-to-home has been configured no file access is granted and no home-directory is created, if restrict-to-home is not applied then root becomes the user's home-directory.

Parameters *local-url-prefix* [*directory*] [*directory/directory*…] — The user's local home directory URL prefix and directory structure up to 190 characters in length.

profile

Syntax **profile** *user-profile-name*
no profile

Context config>system>security>user-template

Description This command configures the profile for the user based on this template.

Parameters *user-profile-name* — The user profile name entered as a character string. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

login-exec

Syntax [**no**] **login-exec** *url-prefix***:** *source-url*

Context config>system>security>user>console
config>system>security>user-template>console

Description This command configures a user's login exec file which executes whenever the user successfully logs in to a console session.

Only one exec file can be configured. If multiple **login-exec** commands are entered for the same user, each subsequent entry overwrites the previous entry.

The **no** form of the command disables the login exec file for the user.

Default No login exec file is defined.

Parameters *url-prefix: source-url* — Enter either a local or remote URL, up to 200 characters in length, that identifies the exec file that will be executed after the user successfully logs in.

member

Syntax **member** *user-profile-name* [*user-profile-name…*]
no member *user-profile-name*

Context config>system>security>user>console

Description This command is used to allow the user access to a profile.

A user can participate in up to eight profiles.

The **no** form of this command deletes access user access to a profile.

Default default

Parameters *user-profile-name* — The user profile name.

new-password-at-login

Syntax [**no**] **new-password-at-login**

Context config>system>security>user>console

Description This command forces the user to change a password at the next console login. The new password applies to FTP but the change can be enforced only by the console, SSH, or Telnet login.

The **no** form of the command does not force the user to change passwords.

Default no new-password-at-login

password

Syntax **password** [*password*]

Context config>system>security>user

Description This command configures the user password for console and FTP access.

The password is stored in an encrypted format in the configuration file when specified. Passwords should be encased in double quotes (“ “) at the time of the password creation. The double quote character (“) is not accepted inside a password. It is interpreted as the start or stop delimiter of a string.

The password can be entered as plain text or a hashed value. SR OS can distinguish between hashed passwords and plain text passwords and take the appropriate action to store the password correctly.

```
config>system>security>user# password testuser1
```

The password is hashed by default.

For example:

```
config>system>security# user testuser1
config>system>security>user$ password xyzabcd1
config>system>security>user# exit


config>system>security# info
```

```
-------------------------------------
...
            user "testuser1"
                password "$2y$10$pFoehOg/tCbBMPDJ/kqpu.8af0AoVGY2xsR7WFqyn5fVTnwR-
zGmOK"
            exit
...
-------------------------------------
config>system>security#
```

The **password** command allows you also to enter the password as a hashed value.

For example:

```
config>system>security# user testuser1
config>system>security>user$ password "$2y$10$pFoehOg/tCbBMPDJ/
kqpu.8af0AoVGY2xsR7WFqyn5fVTnwRzGmOK"
config>system>security>user# exit
config>system>security# info
-------------------------------------
...
user "testuser1"
password "$2y$10$pFoehOg/tCbBMPDJ/kqpu.8af0AoVGY2xsR7WFqyn5fVTnwRzGmOK"
exit
...
-------------------------------------
config>system>security#
```

Parameters *password* — This is the password for the user that must be entered by this user during the login procedure. The minimum length of the password is determined by the **minimum-length** command. The maximum length can be up to 20 chars if unhashed, 32 characters if hashed. The complexity requirements for the password is determined by the **complexity** command.

A password value that does not conform to the minimum-length or other password complexity rules can be configured using the **config**>**system**>**security**>**user**>**password** command, but a warning is provided in the CLI. This allows, for example, an administrator to configure a non-conformant password for a user. A user cannot configure a non-conformant password for themselves using the global **password** command.

All password special characters (#, $, spaces, etc.) must be enclosed within double quotes.

For example: config>system>security>user# password “south#bay?”

The question mark character (?) cannot be directly inserted as input during a telnet connection because the character is bound to the **help** command during a normal Telnet/console connection.

To insert a # or ? characters, they must be entered inside a notepad or clipboard program and then cut and pasted into the Telnet session in the password field that is encased in the double quotes as delimiters for the password.

If a password is entered without any parameters, a password length of zero is implied: (carriage return).

restricted-to-home

Syntax **[no] restricted-to-home**

Context config>system>security>user
config>system>security>user-template

Description This command prevents users from navigating above their home directories for file access (either by means of CLI sessions with the file command, '>' redirection, or by means of FTP). A user is not allowed to navigate to a directory higher in the directory tree on the home directory device. The user is allowed to create and access subdirectories below their home directory.

If a home-directory is not configured or the home directory is not available, then the user has no file access.

The **no** form of the command allows the user access to navigate to directories above their home directory.

Default no restricted-to-home

rsa-key

Syntax **rsa-key** *public-key-value key-id*
rsa-key *key-id*

Context config>system>security>user

Description This command allows the user to associate an RSA public key with the user-name. The public key must be enclosed in quotation marks. This command may be used several times since a user may have multiple public keys. The key is a 1024-bit key.

Default none

Parameters *public-key-value* — Specifies the public key up to 255 characters in length. The key is a 1024-bit key.

key-id — Specifies the key identifier name.

Values 1 — 32

snmp

Syntax **snmp**

Context config>system>security>user

Description This command creates the context to configure SNMP group membership for a specific user and defines encryption and authentication parameters.

All SNMPv3 users must be configured with the commands available in this CLI node.

The OS always uses the configured SNMPv3 user name as the security user name.

user-template

Syntax **user-template** {**tacplus_default** | **radius_default**}

Context config>system>security

Description This command configures default security user template parameters.

Parameters **tacplus_default —** Specifies the default TACACS+ user template. All parameters of the tacplus_default template except the “profile” are actively applied to all TACACS+ users if tacplus use-default-template is enabled. The “profile” parameters are applied to all TACACS+ users if tacplus authorization is enabled (without the use-priv-lvl option) and tacplus use-default-template is enabled.

radius_default — Specifies the default RADIUS user template. The radius_default template is actively applied to a RADIUS user if radius authorization is enabled, radius use-default-template is enabled, and no VSAs are returned with the auth-accept from the RADIUS server.

user

Syntax [**no**] **user** *user-name*

Context config>system>security

Description This command creates a local user and a context to edit the user configuration.

If a new *user-name* is entered, the user is created. When an existing *user-name* is specified, the user parameters can be edited.

When creating a new user and then entering the **info** command, the system displays a password in the output. This is expected behavior in the hash2 scenario. However, when using that user name, there will be no password required. The user can login to the system and then <ENTER> at the password prompt, the user will be logged in.

Unless an administrator explicitly changes the password, it will be null. The hashed value displayed uses the username and null password field, so when the username is changed, the displayed hashed value will change.

The **no** form of the command deletes the user and all configuration data. Users cannot delete themselves.

Default none

Parameters *user-name* — The name of the user up to 32 characters.

CLI Session Management Commands

cli-session-group

Syntax [**no**] **cli-session-group** *session-group-name* [**create**]

Context config>system>security

Description This command is used to configure a session group that can be used to limit the number of CLI sessions available to members of the group.

Parameters *session-group-name* — Specifies a particualr session group.

ssh-max-sessions

Syntax **ssh-max-sessions** *session-limit*
no ssh-max-sessions

Context config>system>security>cli-session-group
config>system>security>profile

Description This command is used to limit the number of SSH-based CLI sessions available to all users that are part of a particular profile, or to all users of all profiles that are part of the same cli-session-group.

The no form of this command disables the command and the profile/group limit is not applied on the number of sessions.

Default no ssh-max-sessions

Parameters *session-limit* — Specifies the maximum number of allowed SSH-based CLI sessions.

Values 0 — 50

telnet-max-sessions

Syntax **telnet-max-sessions** *session-limit*
no telnet-max-sessions

Context config>system>security>cli-session-group
config>system>security>profile

Description This command is used to limit the number of Telnet-based CLI sessions available to all users that are part of a particular profile, or to all users of all profiles that are part of the same cli-session-group.

The no form of this command disables the command and the profile/group limit is not applied on the number of sessions.

Default no telnet-max-sessions

Parameters *session-limit* — Specifies the maximum number of allowed Telnet-based CLI sessions.

Values 0 — 50

combined-max-sessions

Syntax **combined-max-sessions** *session-limit*
no combined-max-sessions

Context config>system>security>cli-session-group
config>system>security>profile

Description This command is used to limit the number of combined SSH/TELENT based CLI sessions available to all users that are part of a particular profile, or to all users of all profiles that are part of the same cli-session-group.

The **no** form of this command disables the command and the profile/group limit is not applied to the number of combined sessions.

Default no combined-max-sessions

Parameters *session-limit* — Specifies the maximum number of allowed combined SSH/TELNET based CLI sessions.

Values 0 — 50

RADIUS Client Commands

access-algorithm

Syntax **access-algorithm** {**direct** | **round-robin**}
no access-algorithm

Context config>system>security>radius

Description This command indicates the algorithm used to access the set of RADIUS servers.

Default direct

Parameters **direct —** The first server will be used as primary server for all requests, the second as secondary and so on.

round-robin — The first server will be used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.

accounting

Syntax [**no**] **accounting**

Context config>system>security>radius

Description This command enables RADIUS accounting.

The **no** form of this command disables RADIUS accounting.

Default no accounting

accounting-port

Syntax **accounting-port** *port*
no accounting-port

Context config>system>security>radius

Description This command specifies a UDP port number on which to contact the RADIUS server for accounting requests.

Parameters *port* — Specifies the UDP port number.

Values 1 — 65535

Default 1813

authorization

Syntax [**no**] **authorization**

Context config>system>security>radius

Description This command configures RADIUS authorization parameters for the system.

Default no authorization

interactive-authentication

Syntax [**no**] **authorization**

Context config>system>security>radius

Description This command enables RADIUS interactive authentication for the system. Enabling interactive-authentication forces RADIUS to fall into challenge/response mode.

Default no authentication

port

Syntax **port** *port*
no port

Context config>system>security>radius

Description This command configures the TCP port number to contact the RADIUS server.

The **no** form of the command reverts to the default value.

Default **1812** (as specified in RFC 2865, *Remote Authentication Dial In User Service* (*RADIUS*))

Parameters *port* — The TCP port number to contact the RADIUS server.

Values 1 — 65535

radius

Syntax [**no**] **radius**

Context config>system>security

Description This command creates the context to configure RADIUS authentication on the router.

Implement redundancy by configuring multiple server addresses for each router.

The **no** form of the command removes the RADIUS configuration.

retry

Syntax **retry** *count*
no retry

Context config>system>security>radius
config>system>security>dot1x>radius-plcy

Description This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server.

The **no** form of the command reverts to the default value.

Default 3

Parameters *count* — The retry count.

Values 1 — 10

priv-lvl-map

Syntax [**no**] **priv-lvl-map**

Context config>system>security>tacplus

Description This command is used to specify a series of mappings between TACACS+ priv-lvl and locally configured profiles for authorization. These mappings are used when the use-priv-lvl option is specified for tacplus authorization.

priv-lvl

Syntax **priv-lvl** *priv-lvl user-profile-name*
no priv-lvl *priv-lvl*

Context config>system>security>tacplus>priv-lvl-map

Description This command maps a specific TACACS+ priv-lvl to a locally configured profile for authorization. This mapping is used when the **use-priv-lvl** option is specified for TACPLUS authorization.

Parameters *priv-lvl* — Specifies the privilege level used when sending a TACACS+ ENABLE request.

Values 0 — 15

user-profile-name — Specifies the user profile for this mapping.

server

Syntax **server** *index* **address** *ip-address* **secret** *key* [**hash** | **hash2**]
no server *index*

Context config>system>security>radius

Description This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values.

Up to five RADIUS servers can be configured at any one time. RADIUS servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried. It is assumed that there are multiple identical servers configured as backups and that the servers do not have redundant data.

The **no** form of the command removes the server from the configuration.

Default No RADIUS servers are configured.

Parameters *index* — The index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 — 5

address *ip-address* **—** The IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

Values	ipv4-address	a.b.c.d (host bits must be 0)
	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x: [0..FFFF]H
		d: [0..255]D

secret *key* **—** The secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.

Values Up to 128 characters in length.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

shutdown

Syntax [**no**] **shutdown**

Context config>system>security>radius

Description This command administratively disables the RADIUS protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of the command administratively enables the protocol which is the default state.

Default no shutdown

timeout

Syntax **timeout** *seconds*
no timeout

Context config>system>security>radius

Description This command configures the number of seconds the router waits for a response from a RADIUS server.

The **no** form of the command reverts to the default value.

Default 3 seconds

Parameters *seconds* — The number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer.

Values 1 — 90

use-default-template

Syntax [**no**] **use-default-template**

Context config>system>security>radius

Description This command specifies whether the radius_default user-template is actively applied to the RADIUS user if no VSAs are returned with the auth-accept from the RADIUS server. When enabled, the radius_default user-template is actively applied if no VSAs are returned with the auth-accept from the RADIUS server and radius authorization is enabled.

TACACS+ Client Commands

server

Syntax **server** *index* **address** *ip-address* **secret** *key* [**port** *port*]
no server *index*

Context config>system>security>tacplus

Description This command adds a TACACS+ server and configures the TACACS+ server IP address, index, and key values.

Up to five TACACS+ servers can be configured at any one time. TACACS+ servers are accessed in order from lowest index to the highest index for authentication requests.

The **no** form of the command removes the server from the configuration.

Default No TACACS+ servers are configured.

Parameters *index* — The index for the TACACS+ server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from the lowest index to the highest index.

Values 1 — 5

address *ip-address* **—** The IP address of the TACACS+ server. Two TACACS+ servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

Values	ipv4-address	a.b.c.d (host bits must be 0)
	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x: [0..FFFF]H
		d: [0..255]D

secret *key* **—** The secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.

Values Up to 128 characters in length.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

port *port* **—** Specifies the port ID.

Values 0 — 65535

shutdown

Syntax [**no**] **shutdown**

Context config>system>security>tacplus

Description This command administratively disables the TACACS+ protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of the command administratively enables the protocol which is the default state.

Default no shutdown

tacplus

Syntax [**no**] **tacplus**

Context config>system>security

Description This command creates the context to configure TACACS+ authentication on the router.

Configure multiple server addresses for each router for redundancy.

The **no** form of the command removes the TACACS+ configuration.

accounting

Syntax **accounting** [**record-type** {**start-stop** | **stop-only**}]
no accounting

Context config>system>security>tacplus

Description This command configures the type of accounting record packet that is to be sent to the TACACS+ server. The **record-type** parameter indicates whether TACACS+ accounting start and stop packets be sent or just stop packets be sent.

Default record-type stop-only

Parameters **record-type start-stop —** Specifies that a TACACS+ start packet is sent whenever the user executes a command.

record-type stop-only — Specifies that a stop packet is sent whenever the command execution is complete.

authorization

Syntax [**no**] **authorization** [**use-priv-lvl**]

Context config>system>security>tacplus

Description This command configures TACACS+ authorization parameters for the system.

Default no authorization

use-priv-lvl — Automatically performs a single authorization request to the TACACS+ server for cmd* (all commands) immediately after login, and then use the local profile associated (via the priv-lvl-map) with the priv-lvl returned by the TACACS+ server for all subsequent authorization (except enable-admin). After the initial authorization for cmd*, no further authorization requests will be sent to the TACACS+ server (except enable-admin).

interactive-authentication

Syntax **[no] interactive-authentication**

Context config>system>security>tacplus

Description This configuration instructs SR OS to send no username nor password in the TACACS+ start message, and to display the *server_msg* in the GETUSER and GETPASS response from the TACACS+ server. Interactive authentication can be used to support a One Time Password scheme (e.g. S/Key). An example flow (e.g. with a telnet connection) is as follows:

- SR OS will send an authentication start request to the TACACS+ server with no username nor password.
- TACACS+ server replies with TAC_PLUS_AUTHEN_STATUS_GETUSER and a *server_msg*.
- SR OS displays the *server_msg*, and collects the user name.
- SR OS sends a continue message with the user name.
- TACACS+ server replies with TAC_PLUS_AUTHEN_STATUS_GETPASS and a *server_msg*.
- SR OS displays the *server_msg* (which may contain, for example, an S/Key for One Time Password operation), and collects the password.
- SR OS sends a continue message with the password.
- TACACS+ server replies with PASS or FAIL.

When interactive-authentication is disabled SR OS will send the username and password in the *tacplus* start message. An example flow (e.g. with a telnet connection) is as follows:

- TAC_PLUS_AUTHEN_TYPE_ASCII.
  - → the login username in the “user” field.
  - → the password in the *user_msg* field (note: this is non-standard but doesn’t cause interoperability problems).
- TACACS+ server ignores the password and replies with TAC_PLUS_AUTHEN_STATUS_GETPASS.
- SR OS sends a continue packet with the password in the *user_msg* field.
- TACACS+ server replies with PASS or FAIL.

When interactive-authentication is enabled, tacplus must be the first method specified in the authentication-order configuration.

Default no interactive-authentication

timeout

Syntax **timeout** *second*s
no timeout

Context config>system>security>tacplus

Description This command configures the number of seconds the router waits for a response from a TACACS+ server.

The **no** form of the command reverts to the default value.

Default **3**

Parameters *seconds* — The number of seconds the router waits for a response from a TACACS+ server, expressed as a decimal integer.

Values 1 — 90

shutdown

Syntax [**no**] **shutdown**

Context config>system>security>tacplus

Description This command administratively disables the TACACS+ protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of the command administratively enables the protocol which is the default state.

Default no shutdown

use-default-template

Syntax [**no**] **use-default-template**

Context config>system>security>tacplus

Description This command specifies whether the tacplus_default user-template is actively applied to the TACACS+ user. When enabled, the tacplus_default user-template is actively applied if tacplus authorization is enabled (without the use-priv-lvl option).

Generic 802.1x COMMANDS

dot1x

Syntax [**no**] **dot1x**

Context config>system>security

Description This command creates the context to configure 802.1x network access control on the router.

The **no** form of the command removes the 802.1x configuration.

radius-plcy

Syntax [**no**] **radius-plcy**

Context config>system>security> dot1x

Description This command creates the context to configure RADIUS server parameters for 802.1x network access control on the router.

NOTE: The RADIUS server configured under the config>system>security>dot1x>radius-plcy context authenticates clients who get access to the data plane of the router as opposed to the RADIUS server configured under the **config>system>radius** context which authenticates CLI login users who get access to the management plane of the router.

The **no** form of the command removes the RADIUS server configuration for 802.1x.

retry

Syntax **retry** *count*
no retry

Context config>system>security> dot1x

Description This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server.

The **no** form of the command reverts to the default value.

Default 3

Parameters *count* — The retry count.

Values 1 — 10

server (dot1x)

Syntax **server** *server-index* **address** *ip-address* **secret** *key* [**hash | hash2**] [**auth-port** *auth-port*] [**acct-port** *acct-port*] [**type** *server-type*]
no server *index*

Context config>system>security> dot1x>radius-plcy

Description This command adds a Dot1x server and configures the Dot1x server IP address, index, and key values.

Up to five Dot1x servers can be configured at any one time. Dot1x servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other Dot1x servers are queried. It is assumed that there are multiple identical servers configured as backups and that the servers do not have redundant data.

The **no** form of the command removes the server from the configuration.

Default No Dot1x servers are configured.

Parameters *server-index* — The index for the Dot1x server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 — 5

address *ip-address* **—** The IP address of the Dot1x server. Two Dot1x servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

secret *key* **—** The secret key to access the Dot1x server. This secret key must match the password on the Dot1x server.

Values Up to 128 characters in length.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

acct-port *acct-port* **—** The UDP port number on which to contact the RADIUS server for accounting requests.

auth-port *auth-port* **—** specifies a UDP port number to be used as a match criteria.

Values 1 — 65535

type *server-type* **—** Specifies the server type.

Values authorization, accounting, combined

source-address

Syntax **source-address** *ip-address*
no source-address

Context config>system>security> dot1x>radius-plcy

Description This command configures the NAS IP address to be sent in the RADIUS packet.

The **no** form of the command reverts to the default value.

Default By default the System IP address is used in the NAS field.

Parameters *ip-address* — The IP prefix for the IP match criterion in dotted decimal notation.

Values 0.0.0.0 — 255.255.255.255

shutdown

Syntax [**no**] **shutdown**

Context config>system>security>dot1x
config>system>security>dot1x>radius-plcy

Description This command administratively disables the 802.1x protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.

The operational state of the entity is disabled as well as the operational state of any entities contained within.

The **no** form of the command administratively enables the protocol which is the default state.

Default shutdown

timeout

Syntax **timeout** *seconds*
no timeout

Context config>system>security> dot1x>radius-plcy

Description This command configures the number of seconds the router waits for a response from a RADIUS server.

The **no** form of the command reverts to the default value.

Default 3 seconds

Parameters *seconds* — The number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer.

Values 1 — 90

Keychain Authentication

keychain

Syntax [**no**] **keychain** *keychain-name*

Context config>system>security

Description This command enables the context to configure keychain parameters. A keychain must be configured on the system before it can be applied to a session.

The **no** form of the command removes the keychain nodal context and everything under it from the configuration. If the keychain to be removed is in use when the no keychain command is entered, the command will not be accepted and an error indicating that the keychain is in use will be printed.

Default none

Parameters *keychain-name* — Specifies a keychain name which identifies this particular keychain entry.

Values An ASCII string up to 32 characters.

direction

Syntax **direction**

Context config>system>security>keychain

Description This command specifies the data type that indicates the TCP stream direction to apply the keychain.

Default none

bi

Syntax **bi**

Context config>system>security>keychain>direction

Description This command configures keys for both send and receive stream directions.

Default none

uni

Syntax **uni**

Context config>system>security>keychain>direction

Description This command configures keys for send or receive stream directions.

Default none

receive

Syntax **receive**

Context config>system>security>keychain>direction>uni

Description This command enables the receive nodal context. Entries defined under this context are used to authenticate TCP segments that are being received by the router.

Default none

send

Syntax **send**

Context config>system>security>keychain>direction>uni

Description This command specifies the send nodal context to sign TCP segments that are being sent by the router to another device.

Default none

entry

Syntax **entry** *entry-id* **key** [*authentication-key* | *hash-key* | *hash2-key*] [**hash** | **hash2**] **algorithm** *algorithm*
no entry *entry-id*

Context config>system>security>keychain>direction>bi
config>system>security>keychain>direction>uni>receive
config>system>security>keychain>direction>uni>send

Description This command defines a particular key in the keychain. Entries are defined by an entry-id. A keychain must have valid entries for the TCP Enhanced Authentication mechanism to work.

The **no** form of the command removes the entry from the keychain. If the entry is the active entry for sending, then this will cause a new active key to be selected (if one is available using the youngest key rule). If it is the ONLY possible send key, then the system will reject the command with an error indicating the configured key is the only available send key.

If the key is one of the eligible keys for receiving, it will be removed. If the key is the ONLY possible eligible key, then the command will not be accepted, and an error indicating that this is the only eligible key will be output.

The **no** form of the command deletes the entry.

Default There are no default entries.

Parameters *entry-id* — Specifies an entry that represents a key configuration to be applied to a keychain.

Values 0 — 63

key — Specifies a key ID which is used along with *keychain-name* and **direction** to uniquely identify this particular key entry.

authentication-key — Specifies the *authentication-key* that will be used by the encryption algorithm. The key is used to sign and authenticate a protocol packet.

The *authentication-key* can be any combination of letters or numbers. .

Values A key must be 160 bits for algorithm hmac-sha-1-96 and must be 128 bits for algorithm aes-128-cmac-96. If the key given with the entry command amounts to less than this number of bits, then it is padded internally with zero bits up to the correct length.

algorithm-*algorithm* — Specifies an enumerated integer that indicates the encryption algorithm to be used by the key defined in the keychain.

Values aes-128-cmac-96 — Specifies an algorithm based on the AES standard for TCP authentication..
hmac-sha-1-96 — Specifies an algorithm based on SHA-1 for RSVP-TE and TCP authentication.
message-digest — MD5 hash used for TCP authentication.
hmac-md5 — MD5 hash used for IS-IS and RSVP-TE.
password – Specifies a simple password authentication for OSPF, IS-IS, and RSVP-TE.
hmac-sha-1 — Specifies the sha-1 algorithm for OSPF, IS-IS, and RSVP-TE.
hmac-sha-256 — Specifies the sha-256 algorithm for OSPF and IS-IS.

hash-key | *hash2-key* — The hash key. The key can be any combination of ASCII characters up to 33 for the *hash-key* and 96 characters for the *hash2-key* in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form.

begin-time

Syntax **begin-time** [*date] [hours-minutes*] [**UTC**] [**now**] [**forever**]

Context config>system>security>keychain>direction>bi>entry
config>system>security>keychain>direction>uni>receive>entry
config>system>security>keychain>direction>uni>send>entry

Description This command specifies the calendar date and time after which the key specified by the keychain authentication key is used to sign and/or authenticate the protocol stream.

If no date and time is set, the begin-time is represented by a date and time string with all NULLs and the key is not valid by default.

Parameters *date hours-minutes* — Specifies the date and time for the key to become active.

Values date: YYYY/MM/DD
hours-minutes: hh:mm[:ss]

now — Specifies the the key should become active immediately.

forever — Specifies that the key should always be active.

end-time

Syntax **end-time** [*date] [hours-minutes*] [**UTC**] [**now**] [**forever**]

Context config>system>security>keychain>direction>uni>receive>entry
config>system>security>keychain>direction>uni>send>entry

Description This command specifies the calendar date and time after which the key specified by the authentication key is no longer eligible to sign and/or authenticate the protocol stream.

Default forever

Parameters *date* — Specifies the calendar date after which the key specified by the authentication key is no longer eligible to sign and/or authenticate the protocol stream in the YYYY/MM/DD format. When no year is specified the system assumes the current year.

hours-minutes — Specifies the time after which the key specified by the authentication key is no longer eligible to sign and/or authenticate the protocol stream in the hh:mm[:ss] format. Seconds are optional, and if not included, assumed to be 0.

UTC — Indicates that time is given with reference to Coordinated Universal Time in the input.

now — Specifies a time equal to the current system time.

forever — Specifies a time beyond the current epoch.

tolerance

Syntax **tolerance** [*seconds* **| forever**]

Context config>system>security>keychain>direction>bi>entry
config>system>security>keychain>direction>uni>receive>entry
config>system>security>keychain>direction>uni>send>entry

Description This command configures the amount of time that an eligible receive key should overlap with the active send key or to never expire.

Parameters *seconds* — Specifies the duration that an eligible receive key overlaps with the active send key.

Values 0 — 4294967294 seconds

forever — Specifies that an eligible receive key overlap with the active send key forever.

option

Syntax **option** {**basic** | **isis-enhanced**}

Context config>system>security>keychain>direction>bi>entry
config>system>security>keychain>direction>uni>send>entry

Description This command configures allows options to be associated with the authentication key.

Parameters **basic —** Specifies that IS-IS should use RFC 5304 encoding of the authentication information. It is only applicable if used with the IS-IS protocol. All other protocols should ignore this configuration command.

isis-enhanced — Specifies that IS-IS should use RFC 5310 encoding of the authentication information. It is only applicable if used with the IS-IS protocol. All other protocols should ignore this configuration command.

tcp-option-number

Syntax **tcp-option-number**

Context config>system>security>keychain

Description This command enables the context to configure the TCP option number to be placed in the TCP packet header.

receive

Syntax **receive** *option-number*

Context config>system>security>keychain>tcp-option-number

Description This command configures the TCP option number accepted in TCP packets received.

Default 254

Parameters *option-number* — Specifies an enumerated integer that indicates the TCP option number to be used in the TCP header.

Values 253, 254, 253&254

send

Syntax **send** *option-number*

Context config>system>security>keychain>tcp-option-number

Description This command configures the TCP option number accepted in TCP packets sent.

Default 254

Parameters *option-number* — Specifies an enumerated integer that indicates the TCP option number to be used in the TCP header.

Values 253, 254

CLI Script Commands

cli-script

Syntax **cli-script**

Context config>system>security

Description This command enables the context to configure CLI scripts.

authorization

Syntax **authorization**

Context config>system>security>cli-script

Description This command enables the context to authorize CLI script execution.

cron

Syntax **cron**

Context config>system>security>cli-script>authorization

Description This command enables the context to configure authorization for the Cron job-scheduler.

vsd

Syntax [**no**] **vsd**

Context config>system>security>cli-script>authorization

Description This command enables the context to configure authorization for the VSD server.

The **no** form of the command removes all authorizations for the VSD server.

event-handler

Syntax **event-handler**

Context config>system>security>cli-script>authorization

Description This command enables the context to configure authorization for the Event Handling System (EHS). EHS allows user-controlled programmatic exception handling by allowing a CLI script to be executed upon the detection of a log event.

cli-user

Syntax **cli-user** *user-name*
no cli-user

Context config>system>security>cli-script>authorization>event-handler
config>system>security>cli-script>authorization>cron
config>system>security>cli-script>authorization>vsd

Description This command configures The user context under which various types of CLI scripts should execute in order to authorize the script commands. TACACS+ and RADIUS users and authorization are not permitted for **cli-script** authorization.

The **no** form of this command configures scripts to execute with no restrictions and without performing authorization.

Default **no cli-user**

Parameters *user-name* — The name of a user in the local node database. TACACS+ or RADIUS users can not be used. The user configuration should reference a valid local profile for authorization.

CPM Filter Commands

cpm-filter

Syntax **cpm-filter**

Context config>system>security

Description This command enables the context to configure a CPM filter. A CPM filter is a hardware filter done by the P chip on the CPMCFM that applies to all the traffic going to the CPM CPU. It can be used to drop, accept packets, as well as allocate dedicated hardware queues for the traffic.

The **no** form of the command disables the CPM filter.

default-action

Syntax **default-action** {**accept** | **drop**}

Context config>system>security>cpm-filter

Description This command specifies the action to take on the traffic when the filter entry matches. If there are no filter entry defined, the packets received will either be dropped or forwarded based on that default action.

Default accept

Parameters **accept —** Specfies that packets matching the filter entry are forwarded.

drop — Specifies that packets matching the filter entry are dropped.

ip-filter

Syntax [**no**] **ip-filter**

Context config>system>security>cpm-filter

Description This command enables the context to configure CPM IP filter parameters.

Default shutdown

ipv6-filter

Syntax [**no**] **ipv6-filter**

Context config>system>security>cpm-filter

Description

Description This command enables the context to configure CPM IPv6 filter parameters.

Default shutdown

mac-filter

Syntax [**no**] **mac-filter**

Context config>system>security>cpm-filter

Description This command enables the context to configure CPM MAC-filter parameters.

Default shutdown

entry

Syntax **entry** *entry-id*

Context config>sys>sec>cpm>ip-filter
config>sys>sec>cpm>ipv6-filter
config>sys>sec>cpm>mac-filter

Description This command specifies a particular CPM filter match entry. Every CPM filter must have at least one filter match entry. Entries are created and deleted by user.

The default match criteria is match none.

Parameters *entry-id* — Identifies a CPM filter entry as configured on this system.

Values 1 — 2048

action

Syntax **action** [**accept | drop | queue** *queue-id*]
no action

Context config>sys>sec>cpm>ip-filter>entry
config>sys>sec>cpm>ipv6-filter>entry
config>sys>sec>cpm>mac-filter>entry

Description This command specifies the action to take for packets that match this filter entry.

Default drop

Parameters **accept —** Specifies packets matching the entry criteria will be forwarded.

drop — Specifies packets matching the entry criteria will be dropped.

queue *queue-id* **—** Specifies packets matching the entry criteria will be forward to the specified CPM hardware queue.

log

Syntax **log** *log-id*

Context config>sys>sec>cpm>ip-filter>entry
config>sys>sec>cpm>ipv6-filter>entry
config>sys>sec>cpm>mac-filter>entry

Description This command specifies the log in which packets matching this entry should be entered. The value zero indicates that logging is disabled.

The **no** form of the command deletes the log ID.

Parameters *log-id* — Specifies the log ID where packets matching this entry should be entered.

match

Syntax **match** [**protocol** *protocol-id*]
no match

Context config>sys>sec>cpm>ip-filter>entry

Description This command enables the context to enter match criteria for the filter entry. When the match criteria have been satisfied the action associated with the match criteria is executed. If more than one match criteria (within one match statement) are configured then all criteria must be satisfied (AND function) before the action associated with the match is executed.

A **match** context may consist of multiple match criteria, but multiple **match** statements cannot be entered per entry.

The **no** form of the command removes the match criteria for the *entry-id*.

Parameters **protocol —** Configures an IP protocol to be used as an IP filter match criterion. The protocol type such as TCP or UDP is identified by its respective protocol number.

protocol-id — Configures the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP(1), TCP(6), UDP(17). The **no** form the command removes the protocol from the match criteria.

Values 1 — 255 (values can be expressed in decimal, hexidecimal, or binary)
keywords - none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp , * — udp/tcp wildcard

Table 11: IP Protocol Names

Protocol	Protocol ID	Description
icmp	1	Internet Control Message
igmp	2	Internet Group Management
ip	4	IP in IP (encapsulation)
tcp	6	Transmission Control
egp	8	Exterior Gateway Protocol
igp	9	any private interior gateway (used by Cisco for their IGRP)
udp	17	User Datagram
rdp	27	Reliable Data Protocol
ipv6	41	IPv6
ipv6-route	43	Routing Header for IPv6
ipv6-frag	44	Fragment Header for IPv6
idrp	45	Inter-Domain Routing Protocol
rsvp	46	Reservation Protocol
gre	47	General Routing Encapsulation
ipv6-icmp	58	ICMP for IPv6
ipv6-no-nxt	59	No Next Header for IPv6
ipv6-opts	60	Destination Options for IPv6
iso-ip	80	ISO Internet Protocol
eigrp	88	EIGRP
ospf-igp	89	OSPFIGP
ether-ip	97	Ethernet-within-IP Encapsulation
encap	98	Encapsulation Header
pnni	102	PNNI over IP
pim	103	Protocol Independent Multicast
vrrp	112	Virtual Router Redundancy Protocol
l2tp	115	Layer Two Tunneling Protocol
stp	118	Spanning Tree Protocol
ptp	123	Performance Transparency Protocol
isis	124	ISIS over IPv4
crtp	126	Combat Radio Transport Protocol
crudp	127	Combat Radio User Datagram

match

Syntax **match** [**next-header** *next-header*]
no match

Context config>sys>sec>cpm>ipv6-filter>entry

Description This command specifies match criteria for the IP filter entry.

The **no** form of this command removes the match criteria for the *entry-id*.

Parameters **next-header** *next-header* — Specifies the next header to match.

The protocol type such as TCP / UDP / OSPF is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6), UDP(17).

Values next-header: 1 — 42, 45— 49, 52— 59, 61— 255 protocol numbers accepted in DHB
keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-icmp, ipv6-no-nxt, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp
* — udp/tcp wildcard

action

Syntax **action** {**permit** | **deny**}
no action

Context config>system>security>mgmt-access-filter>mac-filter

Description This command creates the action associated with the management access filter match criteria entry.

The **action** keyword is required. If no **action** is defined, the filter is ignored. If multiple action statements are configured, the last one overwrites previous configured actions.

If the packet does not meet any of the match criteria the configured **default action** is applied.

Default none — The action is specified by default-action command.

Parameters *permit* — Specifies that packets matching the configured criteria will be permitted.

deny — Specifies that packets matching the configured selection criteria will be denied and that a ICMP host unreachable message will not be issued.

default-action

Syntax **default-action** {**permit** | **deny**}

Context config>system>security>mgmt-access-filter>mac-filter

Description This command creates the default action for management access in the absence of a specific management access filter match.

The **default-action** is applied to a packet that does not satisfy any match criteria in any of the management access filters. Whenever management access filters are configured, the **default-action** must be defined.

Default No default-action is defined.

Parameters **permit —** Specifies that packets not matching the configured selection criteria in any of the filter entries will be permitted.

deny — Specifies that packets not matching the selection criteria be denied and that an ICMP host unreachable message will not be issued.

dscp

Syntax **dscp** *dscp-name*
no dscp

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match
config>sys>sec>cpm>mac-filter>entry>match

Description This command configures a DiffServ Code Point (DSCP) name to be used as an IP filter match criterion.

The **no** form of the command removes the DSCP match criterion.

Default **no dscp** — No dscp match criterion.

Parameters *dscp-name* — Configures a dscp name that has been previously mapped to a value using the **dscp-name** command. The DiffServ code point may only be specified by its name.

dst-ip

Syntax **dst-ip** *ipv6-address/prefix-length*
dst-ip ipv6-prefix-list *ipv6-prefix-list-name*
no dst-ip

Context config>sys>sec>cpm>ip-filter>entry>match

Description This command configures a destination IP address range to be used as an IP filter match criterion.

To match on the destination IP address, specify the address and its associated mask, for example, 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.

The **no** form of the command removes the destination IP address match criterion.

Default No destination IP match criterion

Parameters *ip-address* — Specifies the IP address for the IP match criterion in dotted decimal notation.

Values 0.0.0.0 — 255.255.255.255

ip-prefix-list — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

ip-prefix-list-name — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

mask — Specifies the subnet mask length expressed as a decimal integer.

Values 1 — 32

netmask — Specifies the dotted quad equivalent of the mask length.

Values 0.0.0.0 — 255.255.255.255

dst-ip

Syntax **dst-ip** [*ipv6-address /prefix-length*] [**ipv6-prefix-list** ipv6-*prefix-list-name*]
no dst-ip

Context config>sys>sec>cpm>ipv6-filter>entry>match

Description This command configures a destination IPv6 address range to be used as an IPv6 filter match criterion.

To match on the destination IPv6 address, specify the address.

The **no** form of the command removes the destination IP address match criterion.

Default No destination IP match criterion

Parameters *ipv6-address/prefix-length* — Specifies the IPv6 address for the IPv6 match criterion in dotted decimal notation. An IPv6 IP address is written as eight 4-digit (16-bit) hexadecimal numbers separated by colons. One string of zeros per address can be left out, so that 1010::700:0:217A is the same as 1010:0:0:0:0:700:0:217A.

Values	x:x:x:x:x:x:x:x (eight 16-bit pieces)		
	x:x:x:x:x:x:d.d.d.d		
		x:	[0 — .FFFF]H
		d:	[0 — 255]D
	prefix-length:	1 — 128	

ipv6-prefix-list — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

ipv6-prefix-list-name — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

dst-port

Syntax **dst-port** [**tcp/udp** *port-number*] [*mask*]
dst-port port-list *port-list-name*
dst-port range *tcp/udp port-number tcp/udp port-number*

no dst-port

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command specifies the TCP/UDP port or port name to match the destination-port of the packet. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The **no** form of the command removes the destination port match criterion.

Parameters *tcp/udp port-numb-number* — Specifies the destination port number to be used as a match criteria expressed as a decimal integer.

Values 0 — 65535 (accepted in decimal hex or binary)

port-list-name — Specifies the port list name to be used as a match criteria for the destination port.

mask — Specifies the 16 bit mask to be applied when matching the destination port.

Values [0x0000..0xFFFF] | [0..65535] | [0b0000000000000000..0b1111111111111111]

flow-label

Syntax **flow-label** *value*
no flow-label

Context config>sys>sec>cpm>ipv6-filter>entry>match

Description This command configures flow label match conditions. Flow labeling enables the labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as non-default quality of service or real-time service.

Parameters *value* — Specify the flow identifier in an IPv6 packet header that can be used to discriminate traffic flows (See RFC 3595, *Textual Conventions for IPv6 Flow Label*.)

Values 0 — 1048575

fragment

Syntax **fragment** {**true** | **false**}
no fragment

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command specifies fragmented or non-fragmented IP packets as an IP filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

This command enables match on existence of IPv6 Fragmentation Extension Header in the IPv6 filter policy. To match first fragment of an IP fragmented packet, specify additional Layer 4 matching criteria in a filter policy entry. The no version of this command ignores IPv6 Fragmentation Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

The **no** form of the command removes the match criterion.

This command enables match on existence of IPv6 Fragmentation Extension Header in the IPv6 filter policy. To match first fragment of an IP fragmented packet, specify additional Layer 4 matching criteria in a filter policy entry. The no version of this command ignores IPv6 Fragmentation Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

Default **no fragment**

Parameters **true —** Specifies to match on all fragmented IP packets. A match will occur for all packets that have either the MF (more fragment) bit set or have the Fragment Offset field of the IP header set to a non-zero value. For IPv6, packet matches if it contains IPv6 Fragmentation Extension Header.

false — Specifies to match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero. For IPv6, packet matches if it does not contain IPv6 Fragmentation Extension Header.

hop-by-hop-opt

Syntax **hop-by-hop-opt** {**true** | **false**}
no hop-by-hop-opt

Context config>sys>sec>cpm>ipv6-filter>entry>match

Description This command enables match on existence of Hop-by-Hop Options Extension Header in the IPv6 filter policy.

The **no** form of this command ignores Hop-by-Hop Options Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

Default no hop-by-hop-opt

Parameters **true —** Match if a packet contains Hop-by-Hop Options Extension Header.

false — Match if a packet does not contain Hop-by-Hop Options Extension Header.

icmp-code

Syntax **icmp-code** *icmp-code*
no icmp-code

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command configures matching on ICMP code field in the ICMP header of an IP packet as an IP filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The behavior of the **icmp-code** value is dependent on the configured **icmp-type** value, thus a configuration with only an **icmp-code** value specified will have no effect. To match on the **icmp-code**, an associated **icmp-type** must also be specified.

The **no** form of the command removes the criterion from the match entry.

Default **no icmp-code** - no match criterion for the ICMP code.

Parameters *icmp-code* — Specifies the ICMP code values that must be present to match.

Values 0 — 255

icmp-type

Syntax **icmp-type** *icmp-type*
no icmp-type

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command configures matching on ICMP type field in the ICMP header of an IP packet as an IP filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The **no** form of the command removes the criterion from the match entry.

Default **no icmp-type** — No match criterion for the ICMP type.

Parameters *icmp-type* — Specifies the ICMP type values that must be present to match.

Values 0 — 255

ip-option

Syntax **ip-option** *ip-option-value ip-option-mask*
no ip-option

Context config>sys>sec>cpm>ip-filter>entry>match

Description This command configures matching packets with a specific IP option or a range of IP options in the IP header as an IP filter match criterion.

The option-type octet contains 3 fields:

- 1 bit copied flag (copy options in all fragments)
- 2 bits option class,
- 5 bits option number.

The **no** form of the command removes the match criterion.

Default No IP option match criterion

Parameters *ip-option-value* — Enter the 8 bit option-type as a decimal integer. The mask is applied as an AND to the option byte, the result is compared with the option-value.

The decimal value entered for the match should be a combined value of the eight bit option type field and not just the option number. Thus to match on IP packets that contain the Router Alert option (option number =20), enter the option type of 148 (10010100).

Values 0 — 255

ip-option-mask — Specifies a range of option numbers to use as the match criteria.

This 8 bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	`DDD`	`20`
Hexadecimal	`0xHH`	`0x14`
Binary	`0bBBBBBBBB`	`0b0010100`

Default 255 (decimal) (exact match)

Values 1 — 255 (decimal)

multiple-option

Syntax **multiple-option** {**true** | **false**}
no multiple-option

Context config>sys>sec>cpm>ip-filter>entry>match

Description This command configures matching packets that contain more than one option fields in the IP header as an IP filter match criterion.

The **no** form of the command removes the checking of the number of option fields in the IP header as a match criterion.

Default **no multiple-option** — No checking for the number of option fields in the IP header

Parameters **true —** Specifies matching on IP packets that contain more that one option field in the header.

false — Specifies matching on IP packets that do not contain multiple option fields present in the header.

option-present

Syntax **option-present** {**true** | **false**}
no option-present

Context config>sys>sec>cpm>ip-filter>entry>match

Description This command configures matching packets that contain the option field or have an option field of zero in the IP header as an IP filter match criterion.

The **no** form of the command removes the checking of the option field in the IP header as a match criterion.

Parameters **true —** Specifies matching on all IP packets that contain the option field in the header. A match will occur for all packets that have the option field present. An option field of zero is considered as no option present.

false — Specifies matching on IP packets that do not have any option field present in the IP header (an option field of zero). An option field of zero is considered as no option present.

router

Syntax **router service-name** *service-name*
router *router-instance*
no router

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command specifies a router name or a service-id to be used in the match criteria.

Parameters *router-instance* — Specify one of the following parameters for the router instance:

router-name — Specifies a router name up to 32 characters to be used in the match criteria.

service-id — Specifies an existing service ID to be used in the match criteria.

Values 1 — 2147483647

service-name *service-name* — Specifies an existing service name up to 64 characters in length.

src-ip

Syntax **src-ip** [*ip-address*/*mask* | **ip-prefix-list** *prefix-list-name*]
no src-ip

Context config>sys>sec>cpm>ip-filter>entry>match

Description This command specifies the IP address to match the source IP address of the packet.

To match on the source IP address, specify the address and its associated mask, such as 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.

The **no** form of the command removes the source IP address match criterion.

Default **no src-ip** — No source IP match criterion.

Parameters *ip-address/mask* — Specifies the IP address for the match criterion in dotted decimal notation. An IP address is written as eight 4-digit (16-bit) hexadecimal numbers separated by colons. One string of zeros per address can be left out, so that 1010::700:0:217A is the same as 1010:0:0:0:0:700:0:217A.

Values	ipv4-address	a.b.c.d (host bits must be 0) x:x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H d: [0..255]D interface: 32 characters maximum, mandatory for link local addresses
	mask:	Specifies the 16 bit mask to be applied when matching the source IP address. 1 — 32

ip-prefix-list — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

ip-prefix-list-name — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

src-ip

Syntax **src-ip** [*ip-address*/*mask* **| ipv6-prefix-list** *ipv6-prefix-list-name*]
no src-ip

Context config>sys>sec>cpm>ipv6-filter>entry>match

Description This command specifies the IPv6 address to match the source IPv6 address of the packet.

To match on the source IP address, specify the address and its associated mask, such as 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.

The **no** form of the command removes the source IP address match criterion.

Default **no src-ip** — No source IP match criterion.

Parameters *ip-address/mask* — Specifies the IP address for the match criterion in dotted decimal notation. An IP address is written as eight 4-digit (16-bit) hexadecimal numbers separated by colons. One string of zeros per address can be left out, so that 1010::700:0:217A is the same as 1010:0:0:0:0:700:0:217A.

Values	ipv6-address	x:x:x:x:x:x:x:x[-interface] x:x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H d: [0..255]D interface: 32 characters maximum, mandatory for link local addresses
	mask:	Specifies eight 16-bit hexadecimal pieces representing bit match criteria. Values x:x:x:x:x:x:x:x (eight 16-bit pieces)

ipv6-prefix-list — Creates a list of IPv6 prefixes for match criteria in IPv6 ACL and CPM filter policies.

ipv6-prefix-list-name — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

src-port

Syntax **src-port** *src-port-number* [*mask*]

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command specifies the TCP/UDP port to match the source port of the packet. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

Parameters *src-port-number* — The source port number to be used as a match criteria expressed as a decimal integer.

Values 0 — 65535

mask — Specifies the 16 bit mask to be applied when matching the source port.

Values 0 — 128

tcp-ack

Syntax **tcp-ack** {**true** | **false**}
no tcp-ack

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command configures matching on the ACK bit being set or reset in the control bits of the TCP header of an IP or IPv6 packet as an IP filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The **no** form of the command removes the criterion from the match entry.

Default No match criterion for the ACK bit

Parameters **true** — Specifies matching on IP or IPv6 packets that have the ACK bit set in the control bits of the TCP header of an IP or IPv6 packet.

false — Specifies matching on IP or IPv6 packets that do not have the ACK bit set in the control bits of the TCP header of the IP or IPv6 packet.

tcp-syn

Syntax **tcp-syn** {**true** | **false**}
no tcp-syn

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command configures matching on the SYN bit being set or reset in the control bits of the TCP header of an IP or IPv6 packet as an IP filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The SYN bit is normally set when the source of the packet wants to initiate a TCP session with the specified destination IP or IPv6 address.

The **no** form of the command removes the criterion from the match entry.

Default No match criterion for the SYN bit

Parameters **true —** Specifies matching on IP or IPv6 packets that have the SYN bit set in the control bits of the TCP header.

false — Specifies matching on IP or IPv6 packets that do not have the SYN bit set in the control bits of the TCP header.

renum

Syntax **renum** *old-entry-id new-entry-id*

Context config>sys>sec>cpm>ip-filter
config>sys>sec>cpm>ipv6-filter>entry>match
config>sys>sec>cpm>mac-filter>entry>match

Description

Description This command renumbers existing IP(IPv4), IPv6, or MAC filter entries to re-sequence filter entries.

This may be required in some cases since the OS exits when the first match is found and execute the actions according to the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

Parameters *old-entry-id* — Enter the entry number of an existing entry.

Values 1 — 2048

new-entry-id — Enter the new entry-number to be assigned to the old entry.

Values 1 — 2048

shutdown

Syntax **shutdown**

Context config>sys>sec>cpm>ip-filter
config>sys>sec>cpm>ipv6-filter
config>sys>sec>cpm>mac-filter

Description This command enables IP(v4), IPv6 or MAC CPM filter.

The **no** form of this command disable the filter.

Default shutdown

CPM Queue Commands

cpm-queue

Syntax **cpm-queue**

Context config>system>security

Description This command enables the context to configure a CPM queue.

queue

Syntax **queue** *queue-id*

Context config>system>security>cpm-queue

Description This command allows users to allocate dedicated CPM.

cbs

Syntax **cbs** *cbs*
no cbs

Context config>system>cpm-queue>queue

Description This command specifies the amount of buffer that can be drawn from the reserved buffer portion of the queue's buffer pool.

Parameters *cbs* — Specifies the commited burst size in kbytes.

mbs

Syntax **mbs** *mbs*
no mbs

Context config>system>security>cpm-queue>queue

Description This command specifies the maximum queue depth to which a queue can grow.

Parameters *mbs* — Specifies the maximum burst size in kbytes.

rate

Syntax **rate** *rate* [**cir** *cir*]
no rate

Context config>system>security>cpm-queue>queue

Description This command specifies the maximum bandwidth that will be made available to the queue in kilobits per second (kbps).

Parameters *rate* — Specifies the administrative Peak Information Rate (PIR) for the queue.

cir *cir* **—** Specifies the amount of bandwidth committed to the queue.

TTL Security Commands

ttl-security

Syntax **ttl-security** *min-ttl-value*
no ttl-security

Context config>router>bgp>group
config>router>bgp>group>neighbor
configure>router>ldp>peer-parameters>peer
config>system>login-control>ssh
config>system>login-control>telnet

Description This command configures TTL security parameters for incoming packets. When the feature is enabled, LDP will accept incoming IP packets from a peer only if the TTL value in the packet is greater than or equal to the minimum TTL value configured for that peer. Per-peer-queueing must be enabled in order for TTL protection to operate.

The **no** form of the command disables TTL security.

Parameters *min-ttl-value* — Specify the minimum TTL value for an incoming BGP packet.

Values 1 — 255

ttl-security

Syntax **ttl-security** *min-ttl-value*
no ttl-security

Context config>router>ldp>peer-parameters>peer

Description This command configures TTL security parameters for incoming packets. When the feature is enabled, BGP will accept incoming IP packets from a peer only if the TTL value in the packet is greater than or equal to the minimum TTL value configured for that peer. Per-peer-queueing must be enabled in order for TTL protection to operate.

The **no** form of the command disables TTL security.

Default no ttl-security

Parameters *min-ttl-value* — Specifies the minimum TTL value for an incoming LDP packet.

Values 1 — 255

ttl-security

Syntax **ttl-security** *min-ttl-value*

no ttl-security

Context config>system>login-control>ssh
config>system>login-control>telnet

Description This command configures TTL security parameters for incoming packets. When the feature is enabled, SSH/Telnet will accept incoming IP packets from a peer only if the TTL value in the packet is greater than or equal to the minimum TTL value configured for that peer. Per-peer-queueing must be enabled in order for TTL protection to operate.

The **no** form of the command disables TTL security.

Parameters *min-ttl-value* — Specify the minimum TTL value for an incoming BGP packet.

Values 1 — 255

CPU Protection Commands

cpu-protection

Syntax **cpu-protection**

Context config>sys>security

Description This command enters the context to configure CPU protection parameters.

included-protocols

Syntax **included-protocols**

Context config>sys>security>cpu-protection> ip>included-protocols

Description This context allows configuration of which protocols are included for ip-src-monitoring.   This is system-wide configuration that applies to cpu protection globally.

dhcp

Syntax **[no] dhcp**

Context config>sys>security>cpu-protection> ip>included-protocols

Description Include extracted IPv4 DHCP packets for ip-src-monitoring. IPv4 DHCP packets will be subject to the per-source-rate of cpu protection policies.

Default dhcp   (note this is different than the other protocols)

gtp

Syntax **[no] gtp**

Context config>sys>security>cpu-protection> ip>included-protocols

Description Include extracted IPV4 GTP packets for ip-src-monitoring. IPv4 GTP packets will be subject to the per-source-rate of cpu protection policies.

Default no gtp

icmp

Syntax **[no] icmp**

Context config>sys>security>cpu-protection> ip>included-protocols

Include extracted IPv4 ICMP packets for ip-src-monitoring. IPv4 ICMP packets will be subject to the per-source-rate of cpu protection policies.

Default no icmp

igmp

Syntax **[no] igmp**

Context config>sys>security>cpu-protection> ip>included-protocols

Description Include extracted IPv4 IGMP packets for ip-src-monitoring. IPv4 IGMP packets will be subject to the per-source-rate of cpu protection policies.

Default no igmp

link-specific-rate

Syntax **link-specific-rate** *packet-rate-limit*
no link-specific-rate

Context config>sys>security>cpu-protection

Description This command configures a link-specific rate for CPU protection. This limit is applied to all ports within the system. The CPU will receive no more than the configured packet rate for all link level protocols such as LACP from any one port. The measurement is cleared each second and is based on the ingress port.

Default max (no limit)

Parameters *packet-rate-limit* — Specifies a packet arrival rate limit, in packets per second, for link level protocols.

Values 1 — 65535, max (no limit)

Default 15000

policy

Syntax **policy** *cpu-protection-policy-id* [**create**]
no policy *cpu-protection-policy-id*

Context config>sys>security>cpu-protection

Description This command configures CPU protection policies.

The **no** form of the command deletes the specified policy from the configuration.

Policies 254 and 255 are reserved as the default access and network interface policies, and cannot de deleted. The parameters within these policies can be modified. An event will be logged (warning) when the default policies are modified.

Default Policy 254 (default access interface policy):

per-source-rate: max (no limit)

overall-rate : 6000

out-profile–rate: 6000

alarm

Policy 255 (default network interface policy):

per-source-rate: max (no limit)

overall-rate : max (no limit)

out-profile-rate: 3000

alarm

Parameters *cpu-protection-policy-id* — Assigns a policy ID to the specific CPU protection policy.

Values 1 — 255

create — Keyword used to create CPU protection policy. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

alarm

Syntax [**no**] **alarm**

Context config>sys>security>cpu-protection>policy

Description This command enables the generation of an event when a rate is exceed. The event includes information about the offending source. Only one event is generated per monitor period.

The **no** form of the command disables the notifications.

Default no alarm

eth-cfm

Syntax **eth-cfm**
no eth-cfm

Context config>sys>security>cpu-protection>policy

Description Provides the construct under which the different entries within CPU policy can define the match criteria and overall arrival rate of the Ethernet Configuration and Fault Management (ETH-CFM) packets at the CPU.

Default None

entry

Syntax **entry** <*entry*> **levels** <*levels*> **opcodes** <*opcodes*> **rate** <*packet-rate-limit*>
no entry

Context config>sys>security>cpu-protection>eth-cfm>

Description Builds the specific match and rate criteria. Up to ten entries may exist in up to four CPU protection policies.

The **no** form of the command reverses the match and rate criteria configured.

Default no entry

Parameters **rate —** Specifies a packet rate limit in frames per second, where a ‘0’ means drop all.

Values 1 —100

level — Specifies a domain level.

Values	all	Wildcard entry level
	range	0 —7: within specified range, multiple ranges allowed
	number	0 ... 7: specific level number, may be combined with range

opcode — Specifies an operational code that identifies the application.

Values	range	0 —255: within specified range, multiple ranges allowed
	number	0 .. .255: specific level number, may be combined with range

out-profile-rate

Syntax **out-profile-rate** *packet-rate-limit* [**log-event**]
no out-profile-rate

Context config>sys>security>cpu-protection>policy

Description This command applies a packet arrival rate limit for the entire SAP/interface, above which packets will be market as discard eligible. The rate defined is a global rate limit for the interface regardless of the number of traffic flows. It is a per-SAP/interface rate.

The **no** form of the command sets out-profile-rate parameter back to the default value.

Default **3000** for cpu-protection-policy-id 1-253

6000 for cpu-protection-policy-id 254 (default access interface policy)

3000 for cpu-protection-policy-id 255 (default network interface policy)

Parameters *packet-rate-limit* — Specifies a packet arrival rate limit in packets per second.

Values 1 — 65535, max (max indicates no limit)

log-events — issues a tmnxCpmProtViolSapOutProf, tmnxCpmProtViolIfOutProf, or tmnxCpmProtViolSdpBindOutProf log event and tracks violating interfaces when the out-profile-rate is exceeded. Supported on CPM3 and above only.

overall-rate

Syntax **overall-rate** *packet-rate-limit*
no overall-rate

Context config>sys>security>cpu-protection>policy

Description This command applies a maximum packet arrival rate limit (applied per SAP/interface) for the entire SAP/interface, above which packets will be discarded immediately. The rate defined is a global rate limit for the interface regardless of how many traffic flows are present on the SAP/interface. It is a per-SAP/interface rate.

The **no** form of the command sets overall-rate parameter back to the default value.

Default **max** for cpu-protection-policy-id 1 — 253

6000 for cpu-protection-policy-id 254 (default access interface policy)

max for cpu-protection-policy-id 255 (default network interface policy)

Parameters *packet-rate-limit* — Specifies a packet arrival rate limit in packets per second.

Values 1 — 65535, max (max indicates no limit)

per-source-rate

Syntax **per-source-rate** *packet-rate-limit*
no per-source-rate

Context config>sys>security>cpu-protection>policy

Description This command configures a per-source packet arrival rate limit. Use this command to apply a packet arrival rate limit on a per source basis. A source is defined as a unique combination of SAP and MAC source address (mac-monitoring) or SAP and source IP address (ip-src-monitoring). The CPU will receive no more than the configured packet rate from each source (only certain protocols are rate limited for ip-src-monitoring as configured under 'include-protocols' in the cpu protection policy). The measurement is cleared each second.

This parameter is only applicable if the policy is assigned to an interface (some examples include saps, subscriber-interfaces, and spoke-sdps), and the **mac-monitor** or **ip-src-monitor** keyword is specified in the **cpu-protection** configuration of that interface.

The ip-src-monitoring is useful in subscriber management architectures that have routers between the subscriber and the BNG (router). In layer-3 aggregation scenarios, all packets from all subscribers behind the same aggregation router will arrive with the same source MAC address and as such the mac-monitoring functionality can not differentiate traffic from different subscribers.

Default max, no limit

Parameters *packet-rate-limit* — Specifies a per-source packet (per SAP/MAC source address or per SAP/IP source address) arrival rate limit in packets per second.

Values 1 — 65535, max (max indicates no limit)

port-overall-rate

Syntax **port-overall-rate** *packet-rate-limit* [**low-action-priority]**
no port-overall-rate

Context config>sys>security>cpu-protection

Description This command configures a per-port overall rate limit for CPU protection.

Parameters *packet-rate-limit* — Specifies an overall per-port packet arrival rate limit in packets per second.

Values 1 — 65535, max (indicates no limit)

action-low-priority — Marks packets that exceed the rate as low-priority (for preferential discard later if there is congestion in the control plane) instead of discarding them immediately.

Default max

protocol-protection

Syntax **protocol-protection** [**allow-sham-links**] [**block-pim-tunneled**]
no protocol-protection

Context config>sys>security>cpu-protection

Description This command causes the network processor on the CPM to discard all packets received for protocols that are not configured on the particular interface. This helps mitigate DoS attacks by filtering invalid control traffic before it hits the CPU. For example, if an interface does not have IS-IS configured, then protocol protection will discard any IS-IS packets received on that interface.

Default no protocol-protection

Parameters **allow-sham-links —** Allows sham links. As OSPF sham links form an adjacency over the MPLS-VPRN backbone network, when protocol-protection is enabled, the tunneled OSPF packets to be received over the backbone network must be explicitly allowed.

block-pim-tunneled — - Blocks extraction and processing of PIM packets arriving at the SR-OS node inside a tunnel (for example, MPLS or GRE) on a network interface. With protocol-protection enabled and tunneled pim blocked, PIM in an mVPN on the egress DR will not switch traffic from the (*,G) to the (S,G) tree.

cpu-protection

Syntax **cpu-protection** *policy-id*
no cpu-protection

Context config>router>interface
config>service>ies>interface
config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>interface
config>service>vprn>network-interface
config>service>vprn>video-interface

Description Use this command to apply a specific CPU protection policy to the associated interface. For these interface types, the per-source rate limit is not applicable.

If no CPU-protection policy is assigned to an interface, then the default policy is used to limit the overall-rate. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

The **no** form of the command reverts to the default values.

Default cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

none (for video-interfaces, shown as no cpu-protection in CLI)

The configuration of **no cpu-protection** returns the interface to the default policies as shown above.

cpu-protection

Syntax **cpu-protection policy-id** [**mac-monitoring**] [**ip-src-monitoring**]
no cpu-protection

Context config>subscriber-mgmt>msap-policy

Description Use this command to apply a specific CPU protection policy to the associated msap-policy. The specified cpu-protection policy will automatically be applied to any MSAPs that are create using the msap-policy.

If no CPU-protection policy is assigned to a SAP, then a default policy is used to limit the overall-rate according to the default policy. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

The **no** form of the command reverts to the default values.

Default cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

The configuration of no cpu-protection returns the msap-policy to the default policies as shown above.

Parameters **mac-monitoring** — Enables per SAP + source MAC address rate limiting using the per-source-rate from the associated cpu-protection policy.

ip-src-monitoring — Enables per SAP + IP source address rate limiting for certain protocol packets using the per-source-rate and included-protocols from the associated cpu-protection policy. The ip-src-monitoring is useful in subscriber management architectures that have routers between the subscriber and the BNG (router). In layer-3 aggregation scenarios all packets from all subscribers behind the same aggregation router will arrive with the same source MAC address and as such the mac-monitoring functionality can not differentiate traffic from different subscribers.

cpu-protection

Syntax **cpu-protection** *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]] |[**ip-src-monitoring**]
no cpu-protection

Context config>service>ies>interface>sap
config>service>ies>interface>spoke-sdp
config>service>ies>sub-if>grp-if>sap
config>service>vprn>interface>sap
config>service>vprn>interface>spoke-sdp
config>service>vprn>sub-if>grp-if>sap

Description Use this command to apply a specific CPU protection policy to the associated msap-policy. The specified cpu-protection policy will automatically be applied to any MSAPs that are create using the msap-policy.

If no CPU-protection policy is assigned to a SAP, then a default policy is used to limit the overall-rate according to the default policy. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

The **no** form of the command reverts to the default values.

Default cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

The configuration of no cpu-protection returns the msap-policy to the default policies as shown above.

Parameters **mac-monitoring** — Enables per SAP + source MAC address rate limiting using the per-source-rate from the associated cpu-protection policy.

ip-src-monitoring — Enables per SAP + IP source address rate limiting for certain protocol packets using the per-source-rate and include-protocols from the associated cpu-protection policy. The ip-src-monitoring is useful in subscriber management architectures that have routers between the subscriber and the BNG (router). In layer-3 aggregation scenarios all packets from all subscribers behind the same aggregation router will arrive with the same source MAC address and as such the mac-monitoring functionality can not differentiate traffic from different subscribers.

eth-cfm-monitoring — Enables the Ethernet Connectivity Fault Management cpu-protection extensions on the associated SAP/SDP/template.

aggregate — applies the rate limit to the sum of the per-peer packet rates.

car — (Committed Access Rate) Ignores Eth-CFM packets when enforcing overall-rate.

cpu-protection

Syntax
cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]
no cpu-protection

Context
config>service>epipe>sap
config>service>epipe>spoke-sdp
config>service>ipipe>sap
config>service>template>vpls-sap-template
config>service>vpls>mesh-sdp
config>service>vpls>sap
config>service>vpls>spoke-sdp

Description
Use this command to apply a specific CPU protection policy to the associated SAP, SDP or template. If the mac-monitoring keyword is given then per MAC rate limiting should be performed, using the per-source-rate from the associated cpu-protection policy.

If no CPU-protection policy is assigned to a SAP, then a default policy is used to limit the overall-rate according to the default policy. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

The **no** form of the command reverts to the default values.

Default
cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

The configuration of **no cpu-protection** returns the SAP/SDP/template to the default policies as shown above.

Parameters
mac-monitoring — Enables per SAP + source MAC address rate limiting using the per-source-rate from the associated cpu-protection policy.

eth-cfm-monitoring — Enables the Ethernet Connectivity Fault Management cpu-protection extensions on the associated SAP/SDP/template.

aggregate — applies the rate limit to the sum of the per-peer packet rates.

car — (Committed Access Rate) Ignores Eth-CFM packets when enforcing overall-rate.

Distributed CPU Protection Commands

dist-cpu-protection

Syntax **dist-cpu-protection**

Context config>system>security

Description This command enters the CLI context for configuration of the Distributed CPU Protection (DCP) feature.

policy

Syntax **[no] policy** *policy-name*

Context config>system>security>dist-cpu-protection

Description This command configures one of the maximum 16 Distributed CPU Protection policies. These policies can be applied to objects such as SAPs and network interfaces.

Parameters *policy-name* — Name of the policy to be configured.

description

Syntax **[no] description** *string*

Context config>system>security>dist-cpu-protection>policy

rate

Syntax **rate kbps** *kilobits-per-second*|*max* **[mbs** *size*] **[bytes|kilobytes]**
rate packets {*ppi***|max} within** *seconds* **[initial-delay** *packets***]**
no rate

Context config>system>security>dist-cpu-protection>policy>static-policer
config>system>security>dist-cpu-protection>policy>local-monitoring-policer
config>system>security>dist-cpu-protection>policy>protocol>dynamic-parameters

Description This command configures the rate and burst tolerance for the policer in either a packet rate or a bit rate.

The actual hardware may not be able to perfectly rate limit to the exact configured parameters. In this case, the configured parameters will be adapted to the closest supported rate. The actual (operational) parameters can be seen in CLI, for example, “show service id 33 sap 1/1/3:33 dist-cpu-protection detail”.

Default rate packets max within 1

Parameters **packets|kbps —** specifies that the rate is either in units of packets per interval or in units of kilobits-per-second.   The packets option would typically be used for lower rates (for example, for per subscriber DHCP rate limiting) while the kbps option would typically be used for higher rates (for example, per interface BGP rate limiting).

ppi — Specifies packets per interval. 0..255 or max (0 = all packets are non-conformant)

- rate of max=effectively disable the policier (always conformant)
- rate of packets 0 = all packets considered non-conformant.

within *seconds* **—** Specifies the length of the ppi rate measurement interval.

Values 1..32767

initial-delay *packets* **—** The number of packets allowed (even at line rate) in an initial burst (or a burst after the policer bucket has drained to zero) in addition to the normal “ppi”. This would typically be set to a value that is equal to the number of received packets in several full handshakes/negotiations of the particular protocol.

Values 1..255

kbps *kilobits-per-second* **—** Specifies the kilobits per second.

Values 1..20000000|max max = This effectively disable the policer (always conformant).

mbs — The tolerance for the kbps rate

Values 0..4194304. A configured mbs of 0 will cause all packets to be considered non-conformant.

bytes|kilobytes — Specifies that the units of the mbs size parameter are either in bytes or kilobytes.

Default The default mbs sets the mbs to 10ms of the kbps.

detection-time

Syntax **detection-time** *seconds*

Context config>system>security>dist-cpu-protection>policy>static-policer

Description When a policer is declared as in an “exceed” state, it will remain as exceeding until a contiguous conformant period of **detection-time** passes. The **detection-time** only starts after the exceed-action hold-down is complete. If the policer detects another exceed during the detection count down then a hold-down is once again triggered before the policer re-enters the detection time (that is, the countdown timer starts again at the configured value). During the hold-down (and the detection-time), the policer is considered as in an “exceed” state.

Default 30

Parameters *seconds* — Specifies in seconds.

Values 1..128000

dynamic-enforcement-policer-pool

Syntax **[no] dynamic-enforcement-policer-pool** *number-of-policers*

Context config>dist-cpu-protection

Description This command reserves a set of policers for use as dynamic enforcement policers for the Distributed CPU Protection (DCP) feature. Policers are allocated from this pool and instantiated as per-object-per-protocol dynamic enforcement policers after a local monitor is triggered for an object (such as a SAP or Network Interface). Any change to this configured value automatically clears the high water mark, timestamp, and failed allocation counts as seen under "show card x fp y dist-cpu-protection" and in the tmnxFpDcpDynEnfrcPlcrStatTable in the TIMETRA-CHASSIS-MIB. Decreasing this value to below the currently used/allocated number causes all dynamic policers to be returned to the free pool (and traffic returns to the local monitors).

Default 0

Parameters *number-of-policers* — specifies the number of policers to be reserved.

Values 0, 1000..32k

exceed-action

Syntax **exceed-action {discard [hold-down** *seconds***] | low-priority [hold-down** *seconds***] | none}**

Context config>system>security>dist-cpu-protection>policy>static-policer
config>system>security>dist-cpu-protection>policy>protocol>dynamic-parameters

Description This command controls the action performed upon the extracted control packets when the configured policer rates are exceeded.

Default none

Parameters **discard —** Discards packets that are non-conformant.

low-priority — Marks packets that are non-conformant as low-priority. If there is congestion in the control plane of the SR OS router then unmarked control packets are given preferential treatment.

hold-down *seconds* **—** (optional) When the parameter is specified, it causes the following "hold-down" behavior.

When SR OS software detects that an enforcement policer has marked or discarded one or more packets (software may detect this some time after the packets are actually discarded), and an optional **hold-down** *seconds* value has been specified for the **exceed-action**, then the policer will be set into a "mark-all" or "drop-all" mode that cause the following:

- the policer state to be updated as normal

- all packets to be marked (if the action is "low-priority") or dropped (action = discard) regardless of the results of the policing decisions/actions/state.

The **hold-down** is cleared after approximately the configured time in seconds after it was set. The **hold-down** *seconds* option should be selected for protocols that receive more than one packet in a complete handshake/negotiation (for example, DHCP, PPP). **hold-down** is not applicable to a local monitoring policer. The "detection-time" will only start after any **hold-down** is complete. During the **hold-down** (and the detection-time), the policer is considered as in an "exceed" state. The policer may re-enter the hold-down state if an exceed packet is detected during the detection-time countdown. The allowed values are [none|1..10080|indefinite].

Values 1-10080 in seconds

none — no hold-down

indefinite — hold down is in place until the operator clears it manually using a tools command (tools perform security dist-cpu-protection release-hold-down) or removes the dist-cpu-protection policy from the object.

exceed-action

Syntax **exceed-action {discard | low-priority | none}**

Context config>system>security>dist-cpu-protection>policy>local-monitoring-policer

Description This command controls the action performed upon the extracted control packets when the configured policer rates are exceeded.

Default none

Parameters **discard —** Discards packets that are non-conformant.

low-priority — Marks packets that are non-conformant as low-priority. If there is congestion in the control plane of the SR OS router then unmarked control packets are given preferential treatment.

none — no hold-down

log-events

Syntax **[no] log-events [verbose]**

Context config>system>security>dist-cpu-protection>policy>static-policer

Description This command controls the creation of log events related to static-policer status and activity.

Default default = log-events

log-events: send the Exceed (Excd) and Conform events (e.g. sapDcpStaticExcd)

Parameters **verbose —** (optional) Sends the same events as just "log-events" plus Hold Down Start and Hold Down End events. The optional "verbose" includes some events that are more likely used during debug/tuning/investigations.

local-monitoring-policer

Syntax **[no] local-monitoring-policer** *policer-name* **[create]**

Context config>system>security>dist-cpu-protection>policy>local-monitoring-policer

Description This command configures a monitoring policier that is used to monitor the aggregate rate of several protocols arriving on an object (for example, SAP). When the **local-monitoring-policer** is determined to be in a non-conformant state (at the end of a minimum monitoring time of 60 seconds) then the system will attempt to allocate dynamic policers for the particular object for any protocols associated with the local monitor (for example, via the “protocol xyz enforcement” CLI command).

If the system cannot allocate all the dynamic policers within 150 seconds, it will stop attempting to allocate dynamic policers, raise a LocMonExcdAllDynAlloc log event, and go back to using the local monitor. The local monitor may then detect exceeded packets again and make another attempt at allocating dynamic policers.

Once this *policer-name* is referenced by a protocol then this policer will be instantiated for each “object” that is created and references this DDoS policy. If there is no policer free then the object will be blocked from being created.

Parameters *policy-name* — Specifies name of the policy.

Values [32 chars max]

log-events

Syntax **[no] log-events [verbose]**

Context config>system>security>dist-cpu-protection>policy>local-monitoring-policer

Description This command controls the creation of log events related to **local-monitoring-policer** status and activity.

Default log-events: send the DcpLocMonExcdOutOfDynRes events

Parameters **verbose —** This parameter sends the same events as just “log-events” plus DcpLocMonExcd, DcpLocMonExcdAllDynAlloc, and DcpLocMonExcdAllDynFreed. The optional “verbose” includes some events that are more likely used during debug/tuning/investigations

protocol

Syntax **[no] protocol** *name* **[create]**

Context config>system>security>dist-cpu-protection>policy

Description This command creates the protocol for control in the policy.

Control packets that are both forwarded (which means they could be subject to normal QoS policy policing) and also copied for extraction are not subject to distributed cpu protection (including in the all-unspecified bucket). This includes traffic snooping (for example, PIM in VPLS) as well as control traffic that is flooded in an R-VPLS instance and also extracted to the CPM such as ARP, ISIS and VRRP. Centralized per SAP/interface cpu-protection can be employed to rate limit or mark this traffic if desired.

Explanatory notes for some of the protocols:

- bfd-cpm: includes all bfd handled on the CPM including cpm-np type, single hop and multi-hop, and MPLS-TP CC and CV bfd
- dhcp: includes dhcp for IPv4 and IPv6
- eth-cfm: 802.1ag and includes Y.1731.   Eth-cfm packets on port and LAG based facility MEPs are not included (but packets on Tunnel MEPs are).
- icmp: includes IPv4 and IPv6 ICMP except Neighbor Discovery which is classified as a separate protocol 'ndis'
- isis: includes isis used for SPBM
- ldp: includes ldp and t-ldp
- mpls-ttl: MPLS packets that are extracted due to an expired mpls ttl field
- ndis: IPv6 Neighbor Discovery
- ospf: includes all OSPFv2 and OSPFv3 packets.
- pppoe-pppoa: includes PADx, LCP, PAP/CHAP and NCPs
- all-unspecified: a special 'protocol'. When configured, this treats all extracted control packets that are not explicitly created in the dist-cpu-protection policy as a single aggregate flow (or "virtual protocol"). It lumps together "all the rest of the control traffic" to allow it to be rate limited as one flow. It includes all control traffic of all protocols that are extracted and sent to the CPM (even protocols that cannot be explicitly configured with the distributed cpu protection feature). Control packets that are both forwarded and copied for extraction are not included. If an operator later explicitly configures a protocol, then that protocol is suddenly no longer part of the "all-unspecified" flow. The "all-unspecified" protocol must be explicitly configured in order to operate.

"no protocol x" means packets of protocol x are not monitored and not enforced (although they do count in the fp protocol queue) on the objects to which this dist-cpu-protection policy is assigned, although the packets will be treated as part of the all-unspecified protocol if the all-unspecified protocol is created in the policy.

Default none

Parameters *names* — Signifies protocol name.

Values arp|dhcp|http-redirect|icmp|igmp|mld|ndis|pppoe-pppoa|all-unspecified|mpls-ttl|bfd-cpm|bgp|eth-cfm|isis|ldp|ospf|pim|rsvp.

enforcement

Syntax **enforcement {static** *policer-name* **| dynamic {***mon-policer-name* **| local-mon-bypass}}**

Context config>system>security>dist-cpu-protection>policy>protocols

Description This command configures the enforcement method for the protocol.

Default dynamic local-mon-bypass

Parameters **static —** the protocol is always enforced using a static-policer. Multiple protocols can reference the same static-policer. Packets of protocols that are statically enforced bypass any local monitors.

policer name — Specifies the name is a static-policer.

dynamic — A specific enforcement policer for this protocol for this SAP/object is instantiated when the associated local-monitoring-policer is determined to be in a non-conformant state (at the end of a minimum monitoring time of 60 seconds to reduce thrashing).

mon-policer-name — Specifies which local-monitoring-policer to use

local-mon-bypass — This parameter is used to not include packets from this protocol in the local monitoring function, and when the local-monitor "trips", do not instantiate a dynamic enforcement policer for this protocol.

detection-time

Syntax **detection-time** *seconds*

Context config>system>security>dist-cpu-protection>policy>protocols>dynamic-parameters

Description When a dynamic enforcing policer is instantiated, it will remain allocated until at least a contiguous conformant period of detection-time passes.

dynamic-parameters

Syntax **dynamic-parameters**

Context config>system>security>dist-cpu-protection>policy>protocols

Description The dynamic-parameters are used to instantiate a dynamic enforcement policer for the protocol when the associated local-monitoring-policer is considered as exceeding its rate parameters (at the end of a minimum monitoring time of 60 seconds).

log-events

Syntax **[no] log-events [verbose]**

Context config>system>security>dist-cpu-protection>policy>protocols>dynamic-parameters

Description This command controls the creation of log events related to dynamic enforcement policer status & activity

Default log-events - send the Exceed (Excd) and Conform events

Parameters **verbose —** This parameter sends the send the same events as just "log-events" plus Hold Down Start, Hold Down End, DcpDynamicEnforceAlloc and DcpDynamicEnforceFreed events. The optional "verbose" includes the allocation/de-allocation events (typically used for debug/tuning only – could be very noisy even when there is nothing much of concern).

static-policer

Syntax **[no] static-policer policer-name [create]**

Context config>system>security>dist-cpu-protection>policy

Description Configures a static enforcement policer that can be referenced by one or more protocols in the policy. Once this policer-name is referenced by a protocol, then this policer will be instantiated for each object (e.g. SAP or network interface) that is created and references this policy. If there is no policer resource available on the associated card/fp then the object will be blocked from being created. Multiple protocols can use the same static-policer.

Parameters *policy-name* — Specifies the name of the policy.

Values [32 chars max]