K through L

keepalive (isakmp profile)

To allow the gateway to send dead peer detection (DPD) messages to the peer, use the **keepalive** command in Internet Security Association Key Management Protocol (ISAKMP) profile configuration mode. To return to the default, use the **no** form of this command.

keepalive *seconds* **retry** *retry-seconds*
no keepalive *seconds* **retry** *retry-seconds*

Syntax Description

seconds	Number of seconds between DPD messages. The range is from 10 to 3600 seconds.
retry *retry-seconds*	Number of seconds between retries if DPD message fails. The range is from 2 to 60 seconds.

Command Default

If this command is not configured, a DPD message is not sent to the client.

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use this command to enable the gateway (instead of the client) to send DPD messages to the client. Internet Key Exchange (IKE) DPD is a new keepalive scheme that sends messages to let the router know that the client is still connected.

Examples

The following example shows that DPD messages have been configured to be sent every 60 seconds and every 5 seconds between retries if the peer does not respond:

```
crypto isakmp profile vpnprofile
 keepalive 60 retry 5
```

kerberos clients mandatory

To cause the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server, use the **kerberos clients mandatory** command in global configuration mode. To make Kerberos optional, use the **no** form of this command.

kerberos clients mandatory
no kerberos clients mandatory

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is not configured and the user has Kerberos credentials stored locally, the **rsh**, **rcp**, **rlogin**, and **telnet** commands attempt to negotiate the Kerberos protocol with the remote server and will use the non-Kerberized protocols if unsuccessful.

If this command is not configured and the user has no Kerberos credentials, the standard protocols for **rcp** and **rsh** are used to negotiate.

Examples

The following example causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server:

```
kerberos clients mandatory
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
kerberos credentials forward	Forces all network application clients on the router to forward the Kerberos credentials of users upon successful Kerberos authentication.
rlogin	Logs in to a UNIX host using rlogin.
rsh	Executes a command remotely on a remote rsh host.
telnet	Logs in to a host that supports Telnet.

kerberos credentials forward

To force all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication, use the **kerberos credentials forward** command inglobal configuration mode. To turn off forwarding of Kerberos credentials, use the **no** form of this command.

kerberos credentials forward
no kerberos credentials forward

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Enable credentials forwarding to have users' ticket granting tickets (TGTs) forwarded to the host on which they authenticate. In this way, users can connect to multiple hosts in the Kerberos realm without running the KINIT program each time they need to get a TGT.

Examples

The following example forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication:

```
kerberos credentials forward
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
rlogin	Logs in to a UNIX host using rlogin.
rsh	Executes a command remotely on a remote rsh host.
telnet	Logs in to a host that supports Telnet.

kerberos instance map

To map Kerberos instances to Cisco IOS privilege levels, use the **kerberos instance map** command in global configuration mode. To remove a Kerberos instance map, use the **no** form of this command.

kerberos instance map *instance privilege-level*
no kerberos instance map *instance*

Syntax Description

instance	Name of a Kerberos instance.
privilege-level	The privilege level at which a user is set if the user's Kerberos principal contains the matching Kerberos instance. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges.

Command Default

Privilege level 1

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to create user instances with access to administrative commands.

Examples

The following example sets the privilege level to 15 for authenticated Kerberos users with the *admin* instance in Kerberos realm:

```
kerberos instance map admin 15
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

kerberos local-realm

To specify the Kerberos realm in which the router is located, use the **kerberos local-realm** command in global configuration mode. To remove the specified Kerberos realm from this router, use the **no** form of this command.

kerberos local-realm *kerberos-realm*
no kerberos local-realm

Syntax Description

kerberos-realm	The name of the default Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters .

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The router can be located in more than one realm at a time. However, there can only be one instance of Kerberos local-realm. The realm specified with this command is the default realm.

Examples

The following example specify the Kerberos realm in which the router is located as EXAMPLE.COM:

```
kerberos local-realm EXAMPLE.COM
```

Related Commands

Command	Description
kerberos preauth	Specifies a preauthentication method to use to communicate with the KDC.
kerberos realm	Maps a host name or DNS domain to a Kerberos realm.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.

kerberos password

To set the password shared with the key distribution center, use the **kerberos password**command in global configuration mode. To disable the configured password, use the **no** form of this command.

kerberos password [*text-string*]
no kerberos password [*text-string*]

Syntax Description

text-string	(Optional) The password string.

Command Default

The password is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Kerberos is a network authentication protocol that allows a secured way of node communication in a nonsecure network.

Examples

The following example shows how to set the password:

```
Router# configure terminal
Router(config)# kerberos password treas123
```

Related Commands

Command	Description
kerberos clients mandatory	Specifies the default direction of filters from RADIUS.
kerberos credentials forward	Forces all network application clients on the router to forward the Kerberos credentials of users upon successful Kerberos authentication.

kerberos preauth

To specify a preauthentication method to use to communicate with the key distribution center (KDC), use the **kerberos preauth**command in global configuration mode. To disable Kerberos preauthentication, use the **no** form of this command.

kerberos preauth [{**encrypted-unix-timestamp** | **encrypted-kerberos-timestamp** | **none**}]
no kerberos preauth

Syntax Description

encrypted-unix-timestamp	(Optional) Use an encrypted UNIX timestamp as a quick authentication method when communicating with the KDC.
encrypted-kerberos-timestamp	(Optional) Use the RFC1510 kerberos timestamp as a quick authentication method when communicating with the KDC.
none	(Optional) Do not use Kerberos preauthentication.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

It is more secure to use a preauthentication for communications with the KDC. However, communication with the KDC will fail if the KDC does not support this particular version of **kerberos preauth.** If that happens, turn off the preauthentication with the **none** option.

The **no** form of this command is equivalent to using the **none** keyword.

Examples

The following example enables Kerberos preauthentication:

```
kerberos preauth encrypted-unix-timestamp
```

The following example disables Kerberos preauthentication:

```
kerberos preauth none
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.

Command	Description
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.

kerberos processes

To set the number of kerberos processes to service requests, use the **kerberos processes** command in global configuration mode. To disable the configuration, use the **no** form of this command.

kerberos processes *number*
no kerberos processes

Syntax Description

number	Number of processes. The range is from 1 to 10. The default is 1.

Command Default

The default process is 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to set the number of kerberos processes to 10:

```
Router# configure terminal
Router(config)# kerberos processes
 10
```

Related Commands

Command	Description
debug kerberos	Displays information associated with the Kerberos Authentication Subsystem.

kerberos realm

To map a host name or Domain Name System (DNS) domain to a Kerberos realm, use the **k erberos realm**command in global configuration mode. To remove a Kerberos realm map, use the **no** form of this command.

kerberos realm {*dns-domainhost*} *kerberos-realm*
no kerberos realm {*dns-domainhost*} *kerberos-realm*

Syntax Description

dns-domain	Name of a DNS domain or host.
host	Name of a DNS host.
kerberos-realm	Name of the Kerberos realm to which the specified domain or host belongs.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

DNS domains are specified with a leading dot (.) character; host names cannot begin with a dot (.) character. There can be multiple entries of this line.

A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters. The router can be located in more than one realm at a time. Kerberos realm names must be in all uppercase characters.

Examples

The following example maps the domain name “example.com” to the Kerberos realm, EXAMPLE.COM:

```
kerberos realm .example.com EXAMPLE.COM
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.

Command	Description
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

kerberos retry

To configure the number of retry attempts for the key distribution center (KDC) sessions, use the **kerberos retry** command in global configuration mode. To return to the default setting (4 retries), use the **no** form of this command.

kerberos retry *number*
no kerberos retry

Syntax Description

number	Number of retry attempts. The range is from 1 to 5. The default value is 4.

Command Default

The default value is four retry attempts.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

When multiple KDCs are configured, there is no way to control the timeout so that failover occurs. This causes common client applications to fail before the next KDC is contacted. Therefore, the kerberos retry command enables you to establish stable communication with the KDCs.

Examples

The following example shows how to configure the retry value for the KDC session:

```
Router> enable
Router# configure terminal
Router(config)# kerberos retry 3
```

Related Commands

Command	Description
kerberos clients mandatory	Causes the **rsh**, **rcp**, **rlogin**, and **telnet**commands to fail if they cannot negotiate the Kerberos protocol with the remote server.
kerberos credentials forward	Forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication.

kerberos server

To specify the location of the Kerberos server for a given Kerberos realm, use the **kerberos server**command in global configuration mode. To remove a Kerberos server for a specified Kerberos realm, use the **no** form of this command.

kerberos server *kerberos-realm* {*host-nameip-address*} [*port-number*]
no kerberos server *kerberos-realm* {*host-nameip-address*}

Syntax Description

kerberos-realm	Name of the Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase letters.
host-name	Name of the host functioning as a Kerberos server for the specified Kerberos realm (translated into an IP address at the time of entry).
ip-address	IP address of the host functioning as the Kerberos server for the specified Kerberos realm.
port-number	(Optional) Port that the key distribution center (KDC) monitors (defaults to 88).

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **kerberos server** command to specify the location of the Kerberos server for a given realm.

Examples

The following example specifies 192.168.47.66 as the Kerberos server for the Kerberos realm EXAMPLE.COM:

```
kerberos server EXAMPLE.COM 192.168.47.66
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos realm	Maps a host name or DNS domain to a Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.

Command	Description
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

kerberos srvtab entry

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the kerberos srvtab entry command in global configuration mode. To remove a SRVTAB entry from the router's configuration, use the **no** form of this command.

kerberos srvtab entry *kerberos-principal principal-type timestamp key-version number key-type key-length encrypted-keytab*
no kerberos srvtab entry *kerberos-principal principal-type*

Syntax Description

kerberos-principal	A service on the router.
principal-type	Version of the Kerberos SRVTAB.
timestamp	Number representing the date and time the SRVTAB entry was created.
key-version number	Version of the encryption key format.
key-type	Type of encryption used.
key-length	Length, in bytes, of the encryption key.
encrypted-keytab	Secret key the router shares with the key distribution center (KDC). It is encrypted with the private Data Encryption Standard (DES) key (if available) when you write out your configuration.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from a remote host (generally the KDC), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry**format. The key for each SRVTAB entry is encrypted with a private DES key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** router configuration command to write the router's running configuration to NVRAM.

If you reload a configuration, with a SRVTAB encrypted with a private DES key, on to a router that does not have a private DES key defined, the router displays a message informing you that the SRVTAB entry has been corrupted, and discards the entry.

If you change the private DES key and reload an old version of the router's configuration that contains SRVTAB entries encrypted with the old private DES keys, the router will restore your Kerberos SRVTAB entries, but the SRVTAB keys will be corrupted. In this case, you must delete your old Kerberos SRVTAB entries and reload your Kerberos SRVTABs on to the router using the **kerberos srvtab remote** command.

Although you can configure **kerberos srvtab entry** on the router manually, generally you would not do this because the keytab is encrypted automatically by the router when you copy the SRVTAB using the **kerberos srvtab remote** command.

Examples

In the following example, host/new-router.example.com@EXAMPLE.COM is the host, 0 is the type, 817680774 is the timestamp, 1 is the version of the key, 1 indicates the DES is the encryption type, 8 is the number of bytes, and .cCN.YoU.okK is the encrypted key:

```
kerberos srvtab entry host/new-router.example.com@EXAMPLE.COM 0 817680774 1 1 8 .cCN.YoU.okK
```

Related Commands

Command	Description
kerberos srvtab remote	Retrieves a krb5 SRVTAB file from the specified host.
key config-key	Defines a private DES key for the router.

kerberos srvtab remote

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the kerberos srvtab remote command in global configuration mode.

kerberos srvtab remote *boot_device:URL*

Syntax Description

URL	Machine that has the Kerberos SRVTAB file.
ip-address	IP address of the machine that has the Kerberos SRVTAB file .
filename	Name of the SRVTAB file.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from the remote host (generally the key distribution center [KDC]), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry** format. The key for each SRVTAB entry is encrypted with the private Data Encryption Standard (DES) key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** configuration command to write the router's running configuration to NVRAM.

Examples

The following example copies the SRVTAB file residing on b1.example.com to a router named s1.example.com:

```
kerberos srvtab remote tftp://b1.example.com/s1.example.com-new-srvtab
```

Related Commands

Command	Description
kerberos srvtab entry	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.
key config-key	Defines a private DES key for the router.

kerberos timeout

To configure the timeout for key distribution center (KDC) requests, use the **kerberos timeout** command in global configuration mode. To return to the default setting (5 seconds), use the **no** form of this command.

kerberos timeout *seconds*
no kerberos timeout

Syntax Description

seconds	Timeout, in seconds, for KDC requests. The value range is from 1 to 10. The default value is 5 seconds.

Command Default

The timeout for KDC requests is 5 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

When multiple KDCs are configured, there is no way to control the timeout so that failover occurs. This causes common client applications to fail before the next KDC is contacted. Therefore, the kerberos retry command enables you to establish stable communication with the KDCs.

Examples

The following example shows how to configure the timeout value for KDC requests:

```
Router> enable
Router# configure terminal
Router(config)# kerberos timeout 3
```

Related Commands

Command	Description
kerberos clients mandatory	Causes the **rsh**, **rcp**, **rlogin**, and **telnet**commands to fail if they cannot negotiate the Kerberos protocol with the remote server.
kerberos credentials forward	Forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication.

key (config-radius-server)

To specify the authentication and encryption key for all RADIUS communications between the device and the RADIUS server, use the **key** command in RADIUS server configuration mode. To remove the configured key, use the **no** form of this command.

key {**0** *string* | **6** *string* | **7** *string*} *string*
no key

Syntax Description

0 *string*	Specifies that an unencrypted key follows. • *string*—The unencrypted (clear text) shared key.
6 *string*	Specifies that an advanced encryption scheme (AES) encrypted key follows. • *string*—The advanced encryption scheme [AES] encrypted key.
7 *string*	Specifies that a hidden key follows. • *string*—The hidden shared key.
string	The unencrypted (cleartext) shared key.

Command Default

The authentication and encryption key is disabled.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.4(1)T	This command was modified. The **6** keyword was added.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) authentication with the **aaa new-model** command, you must set the authentication and encryption key using the **radius server key** command.

Note Specify a RADIUS key after you issue the **aaa new-model** command.

The key entered must match the key used on the RADIUS server. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

The following example shows how to specify the host with IP address 192.0.2.2 as the RADIUS server and set rad123 as the encryption key:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# key rad123
```

The following example shows how to set the authentication and encryption key to anykey. The keyword 7 specifies that a hidden key follows.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# key 7 anykey
```

After you save your configuration and use the **show running-config** command, an encrypted key is displayed as follows:

```
Device> enable
Device# show running-config

radius server myserver
  address ipv4 192.0.2.2
  key 7 19283103834782sda
! The leading 7 indicates that the following text is encrypted.
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
address ipv4	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.
password encryption aes	Enables a type 6 encrypted preshared key.
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.
show running-config	Displays the current configuration of your routing device.

key (isakmp-group)

To specify the Internet Key Exchange (IKE) preshared key for group policy attribute definition, use the **key** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove a preshared key, use the **no** form of this command.

key *name*
no key *name*

Syntax Description

name	IKE preshared key that matches the password entered on the client. **Note** This value must match the "password" field that is defined in the Cisco VPN Client 3.x configuration GUI.

Command Default

No default behavior or values.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Use the key command to specify the IKE preshared key when defining group policy information for Mode Configuration push. (It follows the crypto isakmp client configuration group command.) You must configure this command if the client identifies itself to the router with a preshared key. (You do not have to enable this command if the client uses a certificate for identification.)

Examples

The following example shows how to specify the preshared key "cisco":

```
crypto isakmp client configuration group default
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

key (TACACS+)

To configure the per-server encryption key on the TACACS+ server, use the **key** command in TACACS+ server configuration mode. To remove the per-server encryption key, use the **no** form of this command.

key [{**0** | **6** | **7**}] *key-string*
no key [{**0** | **6** | **7**}] *key-string*

Syntax Description

0	(Optional) Specifies that an unencrypted key follows.
6	(Optional) Specifies that an advanced encryption scheme (AES) encrypted key follows.
7	(Optional) Specifies that a hidden key follows.
key-string	The unencrypted shared key.

Command Default

No TACACS+ encryption key is configured.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T. The **6** keyword was added.

Usage Guidelines

The **key** command allows you to configure a per-server encryption key.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

The following example shows how to specify an unencrypted shared key named “key1”:

```
Device> enable
Device# configure terminal
Device(config)# tacacs server server1
Device(config-server-tacacs)# key 0 key1
```

Related Commands

Command	Description
password encryption aes	Enables a type 6 encrypted preshared key.
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

key config-key

To define a private DES key for the router, use the **key config-key**command in global configuration mode. To delete a private Data Encryption Standard (DES) key from the router, use the **no** form of this command.

key config-key 1 *string*
no key config-key 1 *string*

Syntax Description

1	Key number. This number is always 1.
string	Private DES key (can be up to eight alphanumeric characters).

Command Default

No DES-key defined.

Command Modes

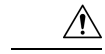
Global configuration

Command History

Release	Modification
11.2	This command was released.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command defines a private DES key for the router that will not show up in the router configuration. This private DES key can be used to DES-encrypt certain parts of the router's configuration.



Caution The private DES key is unrecoverable. If you encrypt part of your configuration with the private DES key and lose or forget the key, you will not be able to recover the encrypted data.

Examples

The following example sets *keyxx* as the private DES key on the router:

```
key config-key 1 keyxx
```

Related Commands

Command	Description
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

key config-key password-encryption

To store a type 6 encryption key in private NVRAM, use the **key config-key password-encryption**command in global configuration mode. To disable the encryption, use the **no** form of this command.

key config-key password-encryption [*text*]
no key config-key password-encryption [*text*]

Syntax Description

text	(Optional) **Password or master key**. **Note** It is recommended that you do not use the *text* argument but instead use interactive mode (using the enter key after you enter the **key config-key password-encryption**command) so that the preshared key will not be printed anywhere and, therefore, cannot be seen.

Command Default

No type 6 password encryption

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

You can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encryption**command with the **password encryption aes**command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) configured using the **key config-key password-encryption** command is the primary encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes**command without configuring the **key config-key password-encryption**command, the following message is printed at startup or during any nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands have been configured:

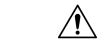
```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

Changing a Password

If the password (primary key) is changed, or reencrypted, using the **key config-key password-encryption**command), the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

Deleting a Password

If the primary key that was configured using the **key config-key password-encryption**command is deleted from the system, a warning is printed (and a confirm prompt is issued) that states that all type 6 passwords will become useless. As a security measure, after the passwords have been encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be reencrypted as explained in the previous paragraph.



Caution If the password configured using the **key config-key password-encryption**command is lost, it cannot be recovered. The password should be stored in a safe location.

Unconfiguring Password Encryption

If you later unconfigure password encryption using the **no password encryption aes** command, all existing type 6 passwords are left unchanged, and as long as the password (primary key) that was configured using the **key config-key password-encryption**command exists, the type 6 passwords will be decrypted as and when required by the application.

Storing Passwords

Because no one can "read" the password (configured using the **key config-key password-encryption**command), there is no way that the password can be retrieved from the router. Existing management stations cannot "know" what it is unless the stations are enhanced to include this key somewhere, in which case the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the **key config-key password-encryption**command). The password can be manually added to the stored configuration but is not recommended because adding the password manually allows anyone to decrypt all passwords in that configuration.

Configuring New or Unknown Passwords

If you enter or cut and paste cipher text that does not match the primary key, or if there is no primary key, the cipher text is accepted or saved, but an alert message is printed. The alert message is as follows:

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

If a new primary key is configured, all the plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old primary key is lost or unknown, you have the option of deleting the primary key using the **no key config-key password-encryption**command. Deleting the primary key using the **no key config-key password-encryption** command causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

Examples

The following example shows that a type 6 encryption key is to be stored in NVRAM:

```
Router (config)# key config-key password-encryption
```

Related Commands

Command	Description
password encryption aes	Enables a type 6 encrypted preshared key.
password logging	Provides a log of debugging output for a type 6 password operation.

key-hash

To specify the Secure Shell (SSH) Rivest, Shamir, and Adleman (RSA) key type and name, use the **key-hash**command in SSH public key configuration mode. To remove the SSH RSA Rivest, Shamir, and Adleman (RSA) public key, use the **no** form of this command.

key-hash *key-type key-name*
no key-hash [*key-type key-name*]

Syntax Description

key-type key-name	The SSH RSA public key type and name.

Command Default

SSH key type and name are not specified.

Command Modes

SSH public key configuration (conf-ssh-pubkey-user)

Command History

Release	Modification
12.2(33)SRA	This command was introduced in release earlier than Cisco IOS Release 12.(33)SRA.

Usage Guidelines

The key type must be **ssh-rsa** for configuration of private-public key pairs. You can use a hashing software to compute the hash of the public key string or you can copy the hash value from another Cisco IOS router. Using the **key-string** command is the preferred method for entering the public key data for the first time.

Examples

The following example shows how to specify the SSH key type and name:

```
Router(config)# ip ssh pubkey-chain
Router(conf-ssh-pubkey)# username test
Router(conf-ssh-pubkey-user)# key-hash ssh-rsa key1
Router(conf-ssh-pubkey-user))# exit
Router(config-pubkey)# exit
Router(config)# exit
```

Related Commands

Command	Description
key-string	Specifies the SSH RSA public key of the remote peer.

keyring

To configure a keyring with an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **keyring**command in ISAKMP profile configuration mode. To remove the keyring from the ISAKMP profile, use the **no** form of this command.

keyring *keyring-name*
no keyring *keyring-name*

Syntax Description

keyring-name	The keyring name, which must match the keyring name that was defined in the global configuration.

Command Default

If this command is not used, the ISAKMP profile uses the keys defined in the global configuration.

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The ISAKMP profile successfully completes authentication of peers if the peer keys are defined in the keyring that is attached to this profile. If no keyring is defined in the profile, the global keys that were defined in the global configuration are used.

Examples

The following example shows that “vpnkeyring” is configured as the keyring name:

```
crypto isakmp profile vpnprofile
 keyring vpnkeyring
```

keyring (IKEv2 profile)

To specify a locally defined or accounting, authentication and authorization (AAA)-based keyring, use the **keyring** command in IKEv2 profile configuration mode. To delete the keyring, use the **no** form of this command.

keyring {**local** *keyring-name* | **aaa** *list-name* [{**name-mangler** *mangler-name* | **password** *password*}]}
no keyring

Syntax Description

local	Specifies the local keyring.
keyring-name	The keyring name for a locally defined keyring.
aaa	Specifies the AAA-based preshared keys list name.
list-name	The AAA method list name.
name-mangler	Derives the username from the peer identity in the preshared key lookup on the AAA list.
mangler-name	(Optional) Globally defined name mangler.
password *password*	Specifies a password for the password. This argument defines the following values: • **0**—Specifies that the password is unencrypted. • **6**—Specifies that the password is encrypted. • *password*—Specifies an unencrypted user password.

Command Default

A keyring is not specified.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(2)T	This command was modified. The keyword **local** and the keyword argument pair **name-mangler** *mangler-name* was added.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.3(3)M	This command was modified. The **password** *password* was added.

Usage Guidelines

Use this command to specify a keyring for use with the local and remote preshared key authentication methods. Only one keyring can be configured either local or AAA based with or without the name mangler. If you configure an AAA based keyring with the name mangler, the name mangler cannot be deleted.

When using AAA, the default password for a Radius access request is "cisco". You can use the **password** keyword within the **keyring** command to change the password.

Note Local AAA is not supported for AAA-based preshared keys.

If the **name-mangler** keyword is not specified, the entire peer identity is used for key lookup.

Examples

The following example shows how to configure an AAA-based keyring and assign the keyring to a profile:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login aaa-psk-list default group radius
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# keyring aaa aaa-psk-list name-mangler mangler1
```

The following example shows how to configure a locally defined keyring:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# keyring keyring1
```

Related Commands

Command	Description
crypto ikev2 keyring	Defines an IKEv2 keyring.

key-set

To associate a key set with a TIDP group, use the **key-set** command in TIDP group configuration mode. To remove the key set from the TIDP group configuration, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **key-set** command is not available in Cisco IOS software.

key-set *name*
no key-set

Syntax Description

name	Name of the key set.

Command Default

None.

Command Modes

TIDP group configuration (config-tidp-grp)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The **key-set** command is entered in TIDP group configuration mode to associate a global key set with a TIDP group. A key set must be configured before a TIDP group can be activated. The key set is first configured with the **tidp key-set** command in global configuration mode. This key set defines the authentication key for TIDP peer communication. This key set can be optionally configured with an encryption key to protect the contents of TIDP messages.

Examples

The following example configures TIDP group 10 to use the key set name KEY_1:

```
Router(config)# tidp key-set KEY_1

Router(config-tidp-ks)# authentication-key send key-string 0 Aa1Bb2Cc3

Router(config-tidp-ks)# authentication-key receive key-string 0 Dd4Ee5Ff6

Router(config-tidp-ks)# exit

Router(config)# tidp group 10

Router(config-tidp-grp)# key-set KEY_1

Router(config-tidp-grp)# registration retry-interval min 30 max 600
Router(config-tidp-grp)# peer 10.1.1.1

Router(config-tidp-grp)# peer 10.1.1.2
```

```
Router(config-tidp-grp)# peer 10.1.1.3

Router(config-tidp-grp)# active
```

Related Commands

Command	Description
active	Activates a TIDP group.
peer	Configures a consumer as a member of a TIDP group.
registration retry-interval (TIDP)	Configures the length of time and number of attempts for TIDP group registration.
tidp group	Configures a TIDP group.
tidp key-set	Configures a key-set for TIDP peer authentication and/or message encryption.

key-string (IKE)

To specify the Rivest, Shamir, and Adelman (RSA) public key of the remote peer, use the **key-string**command in public key configuration mode. To remove the RSA public key, use the **no** form of this command.

key-string *key-string*
no key-string *key-string*

Syntax Description

key-string	Enter the key in hexadecimal format. While entering the key data, you can press Return to continue entering data.

Command Default

No default behavior or values

Command Modes

Public key configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before using this command, you must enter the **rsa-pubkey** command in the crypto keyring mode.

If possible, to avoid mistakes, you should cut and paste the key data (instead of attempting to type in the data).

To complete the command, you must return to the global configuration mode by typing **quit** at the config-pubkey prompt.

Examples

The following example manually specifies the RSA public keys of an IP Security (IPSec) peer:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring.
rsa-pubkey	Defines the RSA public key to be used for encryption or signatures during IKE authentication.
show crypto keyring	Displays keyrings on your router.

key-string (SSH)

To specify the Secure Shell (SSH) Rivest, Shamir, and Adleman (RSA) public key of the remote peer, use the **key-string**command in SSH public key configuration mode. To remove the SSH RSA public key, use the **no** form of this command.

key-string
no key-string

Syntax Description

This command has no arguments or keywords.

Command Default

SSH RSA public key of the remote peer is not specified.

Command Modes

SSH public key configuration (conf-ssh-pubkey-user)

Command History

Release	Modification
12.2(33)SRA	This command was introduced in release earlier than Cisco IOS Release 12.(33)SRA.

Usage Guidelines

The **key-string**command specifies the SSH RSA public key of the remote peer and enters public-key data configuration mode. You can obtain the public key value from an open SSH client (.ssh/id_rsa.pub file).

You can return to global configuration mode by entering the **quit** command in public-key data configuration mode and then by entering the **exit** command in public key configuration mode.

Examples

The following example shows how to specify the SSH RSA public keys of the remote peer:

```
Router(config)# ip ssh pubkey-chain
Router(conf-ssh-pubkey)# username test
Router(conf-ssh-pubkey-user)# key-string
Router(conf-ssh-pubkey-data))# quit
Router(config-pubkey)# exit
Router(conf)# exit
```

Related Commands

Command	Description
key-hash	Specifies the SSH key type and name.

language

To specify the language to be used in a webvpn context, use the **language** command in webvpn context configuration mode. To remove the language, use the **no** form of this command.

language {**Japanese** | **customize** *language-name device* **:** *file*}
no language {**Japanese** | **customize** *language-name device* **:** *file*}

Syntax Description

Japanese	Specifies that the language to be used is Japanese.
customize *language-name device* **:** *file*	Specifies that a language other than English or Japanese is to be used. • *language-name* --This language will be displayed in the selection box on the login and portal pages. • *device* **:** *file* --Storage device on the system and the file name. The file name should include the directory location.

Command Default

English is the language.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Examples

The following example shows that the language to be used is Japanese:

```
Router (config)# webvpn context
 Router (config-webvpn-context)# language Japanese
```

The following example shows that the language (mylang) is to be customized from the file "lang.js," which is in flash:

```
Router (config)# webvpn context
 Router (config-webvpn-context)# language customize mylang flash:lang.js
```

Related Commands

Command	Description
webvpn create template	Creates templates for multilanguage support for messages in an SSL VPN.

ldap attribute-map

To configure a dynamic Lightweight Directory Access Protocol (LDAP) attribute map, use the **ldap attribute-map**command in global configuration mode. To remove the attribute maps, use the **no** form of this command.

ldap attribute-map *map-name*
no ldap attribute-map *map-name*

Syntax Description

map-name	Name of the attribute map.

Command Default

Default mapping is applied.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

You can create LDAP attribute maps to map your existing user-defined LDAP attribute names and values to Cisco attribute names and values that are compatible. You can then bind these attribute maps to LDAP server configuration or remove them as required. The default map is displayed using the **show ldap attributes** command.

Examples

The following command shows how to create an unpopulated LDAP attribute map table named att_map_1:

```
Router(config)# ldap attribute-map att_map_1
```

Related Commands

Command	Description
attribute-map	Attaches an attribute map to a particular LDAP server.
map-type	Defines the mapping of a attribute in the LDAP server.
show ldap attribute	Displays information about default LDAP attribute mapping.

ldap search

To search a Lightweight Directory Access Protocol (LDAP) server, use the **ldap search** command in privileged EXEC mode.

ldap search *server-address port-number search-base scope-number search-filter* **ssl**

Syntax Description

server-address	The IP address of the server.
port-number	The remote TCP port. The range is from 0 to 65535.
search-base	The search base.
scope-number	The scope of the search. The range is from 0 to 2, which denotes to search from BASE, ONELEVEL, and SUBTREE.
search-filter	The filter for the search.
ssl	Specifies LDAP over Secure Socket Layer (SSL).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRB	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows how to search an LDAP server:

```
Router# ldap search 10.0.0.1 265 c 2 sea ssl
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

ldap server

To define a Lightweight Directory Access Protocol (LDAP) server and enter LDAP server configuration mode, use the **ldap server** command in global configuration mode. To remove an LDAP server configuration, use the **no** form of this command.

ldap server *name*
no ldap server *name*

Syntax Description

name	Name of the LDAP server configuration.

Command Default

No LDAP server is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.3(2)T	This command was modified. IPv6 transport support for LDAP server was added.

Usage Guidelines

You can define the following parameters in LDAP server configuration mode:

- IP address of the LDAP server
- Transport protocol to connect to the server
- Security protocol for peer-to-peer communication
- LDAP timers

Examples

The following example shows how to define an LDAP server named server1:

```
Device(config)# ldap server server1
```

Related Commands

Command	Description
ipv4 (ldap)	Creates an IPv4 address within an LDAP server address pool.
transport port (ldap)	Configures the transport protocol for establishing a connection with the LDAP server.

length (RITE)

To specify the length the captured portion of the packets being captured in IP traffic export capture mode, use the **length** command in RITE configuration mode. To return to the default condition of capturing entire packets, use the **no** form of this command.

length *bytes*
no length

Syntax Description

bytes	The length in bytes of the packet captured in IP traffic export capture mode. Acceptable values are 128, 256, and 512.

Command Default

When you do not use this command, the entire packet is captured.

Command Modes

RITE configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to limit the length of the portion of the packets being captured in IP traffic export capture mode. The captured portion of the packets are limited to 128, 256, or 512 bytes. If you do not use the **length** command, entire packets are captured.

Examples

The following example shows the use of the **length** command in the configuration of IP traffic export capture mode profile "corp2":

```
Router(config)# ip traffic-export profile corp2 mode_capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported or captured across a monitored interface.
incoming	Configures filtering for incoming IP traffic export or IP traffic capture traffic.
ip traffic-export apply profile	Applies an IP traffic export or IP traffic capture profile to a specific interface.

Command	Description
ip traffic-export profile	Creates an IP traffic export or IP traffic capture profile on an ingress interface.
outgoing	Configures filtering for outgoing IP traffic export or IP traffic capture traffic.
traffic-export interface	Controls the operation of IP traffic capture mode.

license (parameter-map)

To configure a license that is sent to Cloud Web Security for authentication, use the **license** command in parameter-map type inspect configuration mode. To remove the license, use the **no** form of this command.

license {**0** *key* | **7** *key*}
no license {**0** *key* | **7** *key*}

Syntax Description

0 *key*	Specifies an unencrypted 32-character hexadecimal license key.
7 *key*	Specifies an encrypted 66-character hexadecimal license key.

Command Default

The license is not configured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type cws global** command before you configure the **license** command.

When the server license or the private key is not configured, content scan drops the traffic. When the server license or private key is wrong, content scan forwards the traffic to Cloud Web Security and Cloud Web Security sends a blocked warning page to the end user.

Examples

The following example shows how to configure an unencrypted license key:

```
Device(config)# parameter-map type cws global
Device(config-profile)# license 0 D7BF98AFEB0B4AFA5954CB0F81FFB620
```

Related Commands

Command	Description
parameter-map type cws global	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.

lifetime (cs-server)

To specify the lifetime of the certification authority (CA) or a certificate, use the **lifetime** command in certificate server configuration mode. To return to the default lifetime values, use the **no** form of this command.

lifetime {**ca-certificate** | **certificate**} *days* [*hours* [*minutes*]]
no lifetime {**ca-certificate** | **certificate**}

Syntax Description

ca-certificate	Specifies that the lifetime applies to the CA certificate of the certificate server.
certificate	Specifies that the lifetime applies to the certificate of the certificate server. The maximum certificate lifetime is 1 month less than the expiration date of the CA certificate's lifetime.
days	An integer specifying the certificate lifetime in days. Valid values range from 0 to 7305.
hours	(Optional) An integer specifying the certificate lifetime in hours. Valid values range from 0 to 24.
minutes	(Optional) An integer specifying the certificate lifetime in minutes. Valid values range from 0 to 59. It is recommended that if you set the certificate lifetime in minutes, that the value be set to 3 minutes or greater. Setting the certificate lifetime to a value of less than 3 minutes will not allow certificate rollover to function.

Command Default

The default CA certificate lifetime is 1095 days, or 3 years.

The default certificate lifetime is 365 days, or 1 year.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

Use the **lifetime** command if you want to specify lifetime values other than the default values for the CA certificate and the certificate of the certificate server.

After the certificate generates its signed certificate, the lifetime cannot be changed. All certificates are valid when they are issued.

Examples

The following example shows how to set the lifetime value for the CA to 30 days:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# lifetime ca certificate 30
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant none	Specifies all certificate requests to be rejected.

Command	Description
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
mode ra	Enters the PKI server into RA certificate server mode.
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.
show (cs-server)	Displays the PKI CS configuration.
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

lifetime (IKE policy)

To specify the lifetime of an Internet Key Exchange (IKE) security association (SA), use the **lifetime**command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode . To reset the SA lifetime to the default value, use the **no** form of this command.

lifetime *seconds*
no lifetime

Syntax Description

seconds	Number of many seconds for each each SA should exist before expiring. Use an integer from 60 to 86,400 seconds, which is the default value.

Command Default

The default is 86,400 seconds (one day).

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use this command to specify how long an IKE SA exists before expiring.

When IKE begins negotiations, the first thing it does is agree upon the security parameters for its own session. The agreed-upon parameters are then referenced by an SA at each peer. The SA is retained by each peer until the SA's lifetime expires. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec SAs. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec SAs. New IPSec SAs are negotiated before current IPSec SAs expire.

So, to save setup time for IPSec, configure a longer IKE SA lifetime. However, shorter lifetimes limit the exposure to attackers of this SA. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

Note that when your local peer initiates an IKE negotiation between itself and a remote peer, an IKE policy can be selected only if the lifetime of the remote peer's policy is shorter than or equal to the lifetime of the local peer's policy. Then, if the lifetimes are not equal, the shorter lifetime will be selected. To restate this behavior: If the two peer's policies' lifetimes are not the same, the initiating peer's lifetime must be longer and the responding peer's lifetime must be shorter, and the shorter lifetime will be used.

Examples

The following example configures an IKE policy with a security association lifetime of 600 seconds (10 minutes), and all other parameters are set to the defaults:

```
crypto isakmp policy 15
 lifetime 600
 exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
show crypto isakmp policy	Displays the parameters for each IKE policy.

lifetime (IKEv2 profile)

To specify the lifetime for an Internet Key Exchange Version 2 (IKEv2) security association (SA), use the **lifetime**command in IKEv2 profile configuration mode . To reset the SA lifetime to the default value, use the **no** form of this command.

lifetime *seconds*
no lifetime

Syntax Description

seconds	The time that each IKE SA should exist before expiring. Use an integer from 60 to 86,400 seconds.

Command Default

The default is 86,400 seconds (one day).

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to specify the lifetime of an IKE SA. When IKE begins negotiations, IKE agrees on the security parameters for its session that are referenced by an SA at each peer. The SA is retained by each peer until the SA expires, and before an SA expires, it can be reused by subsequent IKE negotiations, which saves time when setting up new IKE SA. Although, SA with a shorter lifetime limits the exposure to attacks, to save time configure an IKE SA that has a longer lifetime. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

Examples

The following example configures an IKEv2 profile with a security association lifetime of 600 seconds (10 minutes), and all other parameters are set to the defaults:

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# lifetime 600
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
show crypto ikev2 profile	Displays the IKEv2 profile.

lifetime crl

To define the lifetime of the certificate revocation list (CRL) that is used by the certificate server, use the **lifetime crl** command in certificate server configuration mode. To return to the default value of 1 week, use the **no** form of this command.

lifetime crl *time*
no lifetime crl *time*

Syntax Description

time	Lifetime value, in hours, of the CRL. Maximum lifetime value is 336 hours (2 weeks). The default value is 168 hours (1 week).

Command Default

168 hours (1 week)

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

After you create a certificate server via the **crypto pki server**command, use the **lifetime crl** command if you want to specify a value other than the default value for the CRL. The lifetime value is added to the CRL when the CRL is created.

The CRL is written to the specified database location as *ca-label*.crl.

Examples

The following example shows how to set the lifetime value for the CRL to 24 hours:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# lifetime crl 24
```

Related Commands

Command	Description
cdp-url	Specifies that CDP should be used in the certificates that are issued by the certificate server.
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.

lifetime enrollment-request

To specify how long an enrollment request should stay in the enrollment database, use the **lifetime enrollment-request**command in certificate server configuration mode. To return to the default value of 1 week, use the **no** form of this command.

lifetime enrollment-request *time*
no lifetime enrollment-request

Syntax Description

time	Lifetime value, in hours, of an enrollment request. The maximum lifetime value is 1000 hours. The default value is 168 hours (1 week).

Command Default

Lifetime value default is 168 hours.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

After the certificate server receives an enrollment request, it can leave the request in pending, reject it, or grant it. The request is left in the Enrollment Request Database for the lifetime of the enrollment request until the client polls the certificate server for the result of the request.

Examples

The following example shows how to set the lifetime value for the enrollment request to 24 hours:

```
Router (config)# crypto pki server mycs
Router (cs-server)# lifetime enrollment-request 24
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server.
crypto pki server grant	Grants all or certain SCEP requests.
crypto pki server remove	Removes enrollment requests that are in the certificate server Enrollment Request Database.

limit address-count

To limit the number of IPv6 addresses allowed to be used on the port, use the **limit address-count**command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode .

limit address-count *maximum*

Syntax Description

maximum	Sets the role of the device to host.

Command Default

The device role is host.

Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **limit address-count** command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size.

Use the **limit address-count**command after enabling NDP inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an NDP policy name as policy1, places the router in NDP inspection policy configuration mode, and limits the number of IPv6 addresses allowed on the port to 25:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# limit address-count 25
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy n ame and enters NDP inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

list (LSP Attributes)

To display the contents of a label switched path (LSP) attribute list, use the **list** command in LSP Attributes configuration mode.

list

Syntax Description

This command has no arguments or keywords.

Command Default

Contents of an LSP attribute list is not displayed.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command displays the contents of the LSP attribute list. You can display each of the following configurable LSP attributes using the **list** command: affinity, auto-bw, bandwidth, lockdown, priority, protection, and record-route.

Examples

The following example shows how to display the contents of an LSP attribute list identified with the string priority:

```
!
Router(config)# mpls traffic-eng lsp attributes priority
Router(config-lsp-attr)# priority 0 0
Router(config-lsp-attr)# list
 priority 0 0
Router(config-lsp-attr)#
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

list (WebVPN)

To list the currently configured access control list (ACL) entries sequentially, use the **list** command in webvpn acl configuration mode. This command has no **no** form.

list

Syntax Description

This command has no arguments or keywords.

Command Default

Currently configured ACL entries are not listed.

Command Modes

Webvpn acl configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Before using this command, you must have configured the web context and the **acl** command.

Examples

The following example shows that currently configured ACL entries are to be listed:

```
webvpn context context1
 acl acl1
  list
```

Related Commands

Command	Description
webvpn context	Configures the WebVPN context and enters SSL VPN configuration mode.
acl	Defines an ACL using a SSL VPN gateway at the Application Layer level.

li-view

To initialize a lawful intercept view, use the **li-view**command in global configuration mode.

li-view *li-password* **user** *username* **password** *password*

Syntax Description

li-password	Password for the lawful intercept view. This password is used by the system administrator or a level 15 privilege user who initialized the lawful intercept view to access and configure it. The password can contain any number of alphanumeric characters. **Note** The password is case sensitive.
user *username*	Specifies the user who can access the lawful intercept view.
password *password*	Provides the password for the specified **user**. The user must provide this password to access the lawful intercept view.

Command Default

A lawful intercept view cannot be accessed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Like a command-line interface (CLI) view, a lawful intercept view restricts access to specified commands and configuration information. Specifically, a lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of Network Management Protocol (SNMP) commands that stores information about calls and users.

Commands available in lawful intercept view belong to one of the following categories:

- Lawful intercept commands that should not be made available to any other view or privilege level.
- CLI commands that are useful for lawful intercept users but do not need to be excluded from other views or privilege levels.

Note Only a system administrator or a level 15 privilege user can initialize a lawful intercept view.

Examples

The following example shows how to configure a lawful intercept view, add users to the view, and verify the users that were added to the view:

```
!Initialize the LI-View.
Router(config)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config)# end
! Enter the LI-View; that is, check to see what commands are available within the view.
Router# enable view li-view
Password:
Router#
00:22:57:%PARSER-6-VIEW_SWITCH:successfully set to view 'li-view'.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view li-view

Router(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name      ===This option only resides in LI View.
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views
Router(config-view)#
! NOTE:LI View configurations are never shown as part of 'running-configuration'.
! Configure LI Users.
Router(config)# username lawful-intercept li-user1 password li-user1pass

Router(config)# username lawful-intercept li-user2 password li-user2pass
! Displaying LI User information.
Router# show users lawful-intercept
li_admin
li-user1
li-user2
Router#
```

Related Commands

Command	Description
show users	Displays information about the active lines on the router.
username	Establishes a username-based authentication system.

load-balance (server-group)

To enable RADIUS server load balancing for a named RADIUS server group, use the load-balance command in server group configuration mode. To disable named RADIUS server load balancing, use the **no** form of this command.

load-balance method least-outstanding [**batch-size** *number*] [**ignore-preferred-server**]
no load-balance

Syntax Description

method least-outstanding	Enables least outstanding mode for load balancing.
batch-size	(Optional) The number of transactions to be assigned per batch.
number	(Optional) The number of transactions in a batch. • The default is 25. • The range is 1-2147483647. **Note** Batch size may impact throughput and CPU load. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.
ignore-preferred-server	(Optional) Indicates if a transaction associated with a single authentication, authorization, and accounting (AAA) session should attempt to use the same server or not. • If set, preferred server setting will not be used. • Default is to use the preferred server.

Command Default

If this command is not configured, named RADIUS server load balancing will not occur.

Command Modes

Server group configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Examples

The following example shows load balancing enabled for a named RADIUS server group. It is shown in three parts: the current configuration of RADIUS command output, debug output, and AAA server status information.

Server Configuration and Enabling Load Balancing for Named RADIUS Server Group Example

The following shows the relevant RADIUS configuration:

```
Router# show running-config
.
.
.
aaa group server radius server-group1
 server 192.0.2.238 auth-port 2095 acct-port 2096
 server 192.0.2.238 auth-port 2015 acct-port 2016
 load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
.
.
```

The lines in the current configuration of RADIUS command output above are defined as follows:

- The **aaa group server radius** command shows the configuration of a server group with two member servers.
- The **load-balance** command enables load balancing for the global RADIUS server groups with the batch size specified.
- The **aaa authentication ppp**command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables the sending of all accounting requests to the AAA server after the client is authenticated and after the disconnect using the start-stop keyword.

Debug Output for Named RADIUS Server Group Example

The debug output below shows the selection of a preferred server and the processing of requests for the configuration above.

```
Router#
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
```

```
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.
```

Server Status Information for Named RADIUS Server Group Example

The output below shows the AAA server status for the named RADIUS server group configuration example.

```
Router# show aaa servers
RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
```

```
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
Router#
```

The output shows the status of two RADIUS servers. Both servers are alive, and no requests have been processed since the counters were cleared 0 minutes ago.

Related Commands

Command	Description
debug aaa sg-server selection	Shows why the RADIUS and TACACS+ server group system in a router is selecting a particular server.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS load balancing.
radius-server host	Enables RADIUS automated testing for load balancing.
radius-server load-balance	Enables RADIUS server load balancing for the global RADIUS server group.
test aaa group	Tests RADIUS load balancing server response manually.

load classification

Note Effective with Cisco IOS Release 15.2(4)M, the **load classification** command is not available in Cisco IOS software.

To load a traffic classification definition file (TCDF) for a Flexible Packet Matching (FPM) configuration, use the **load classification** command in global configuration mode. To unload all TCDFs from a specified location or a single TCDF, use the **no** form of this command.

load classification *location* **:** *filename*
no load classification *location* **:** *filename*

Syntax Description

location **:** *filename*	Location of the TCDF that is to be loaded onto the router. When used with the **no** form of this command, all TCDFs loaded from the specified filename will be unloaded. **Note** The location must be local to the routing device.

Command Default

No TCDF is loaded onto the router.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

A TCDF is an Extensible Markup Language (XML) file that you create in a text file or using an XML editor. FPM uses a TCDF to define classes of traffic and to specify actions to apply to the traffic classes for the purpose of blocking attacks on the network. Traffic classification behavior defined in a TCDF is identical to that configured using the command-line interface (CLI).

Use the **load classification** command to load the TCDF onto the routing device. The location to which you load the file must be local to the device. After the TCDF is loaded, you can use service policy CLI commands to attach the TCDF policies to a specific interface or interfaces. TCDP classes and policies, which are loaded, display as normal policies and classes when you issue a **show** command.

The TCDF requires that a relevant protocol header description file (PHDF) is already loaded onto the system through the use of the **load protocol** command. Standard PHDFs are provided with the FPM feature.

Examples

The following example shows how to create a TCDF for slammer packets (UDP 1434) for an FPM XML configuration. The match criteria defined within the **class** element is for slammer packets with an IP length not to exceed 404 (0x194) bytes, UDP port 1434 (0x59A), and pattern 0x4011010 at

224 bytes from start of the IP header. The policy “fpm-udp-policy” is defined with the action to drop slammer packets.

```
<?xml version=”1.0” encoding=”UTF-8”?
>
<tcdf
>
    <class

name
=”ip-udp”
type
=”stack”>
       <match
>
          <eq

field
=”ip.protocol”
value
=”0x11”
next
=”udp”></eq
>
       </match
>
    </c
lass
>
    <class
 name=“slammer
” type
=”access-control” match
=”all”>
       <match
>
          <eq
 field
=”udp.dest-port” value
=”0x59A”></eq
>
          <eq
 field
=”ip.length” value
=”0x194”></eq
>
          <eq
 start
=“l3-start“ offset
=”224” size
=”4” value
=”0x00401010”></eq
>
       </match
>
    </class
>
    <policy
 type=”access-control”
name
=“fpm-udp-policy“>
       <class
```

```
name
="slammer"></class
>
       <action
>drop</action
>
    </policy
>
</tcdf
>
```

The following example shows how to load relevant PHDFs, load the TCDF file sql-slammer.tcdf, and attach the TCDF-defined policy to the interface Ethernet 0/1:

```
enable
configure terminal
load protocol localdisk1:ip.phdf
load protocol localdisk1:tcp.phdf
load protocol localdisk1:udp.phdf
load classification localdisk1:sql-slammer.tcdf
policy-map type access-control my-policy-1
class ip-udp
service-policy fpm-udp-policy
interface Ethernet 0/1
 service-policy type access control input my-policy-1
 end
```

The following CLI output is associated with the TCDF described in the example:

```
Router# show class-map type stack
.
.
.
class-map type stack match-all ip-udp
   match field IP protocol eq 0x11 next UDP
.
.
.
Router# show class-map type access-control
.
.
.
class-map type access-control match-all slammer
   match field UDP dest-port eq 0x59A
   match field IP length eq 0x194
   match start l3-start offset 224 size 4 eq 0x4011010
.
.
.
Router show policy-map my-policy-1
.
.
.
policy-map type access-control my-policy-1
  class slammer
    drop
.
.
.
```

Related Commands

Command	Description
load protocol	Loads a protocol header description file (PHDF) onto a router.

local-address

To limit the scope of an Internet Security Association and Key Management Protocol (ISAKMP) profile or an ISAKMP keyring configuration to a local termination address or interface, use the **local-address**command in ISAKMP profile configuration and keyring configuration modes. To remove the local address or interface, use the **no** form of this command.

local-address {*interface-name* | *ip-address* [*vrf-tag*]}
no local-address {*interface-name* | *ip-address* [*vrf-tag*]}

Syntax Description

interface-name	Name of the local interface.
ip-address	Local termination address.
vrf-tag	(Optional) Scope of the IP address will be limited to the VRF instance.

Command Default

If this command is not configured, the ISAKMP profile or ISAKMP keyring is available to all local addresses.

Command Modes

ISAKMP profile configuration
Keyring configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Examples

The following example shows that the scope of the ISAKMP profile is limited to interface serial2/0:

```
crypto isakmp profile profile1
  keyring keyring1
  match identity address 10.0.0.0 255.0.0.0
  local-address serial2/0
```

The following example shows that the scope of the ISAKMP keyring is limited only to interface serial2/0:

```
crypto keyring
  local-address serial2/0
  pre-shared-key address 10.0.0.1
```

The following example shows that the scope of the ISAKMP keyring is limited only to IP address 10.0.0.2:

```
crypto keyring keyring1
  local-address 10.0.0.2
  pre-shared-key address 10.0.0.2 key
```

The following example shows that the scope of an ISAKMP keyring is limited to IP address 10.34.35.36 and that the scope is limited to VRF examplevrf1:

```
ip vrf examplevrf1
  rd 12:3456
crypto keyring ring1
  local-address 10.34.35.36 examplevrf1
interface ethernet2/0
  ip vrf forwarding examplevrf1
  ip address 10.34.35.36 255.255.0.0
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.
crypto keyring	Defines a keyring and enters keyring configuration mode.

local-port (WebVPN)

To remap (forward) an application port number in a port forwarding list, use the **local-port** command in webvpn port-forward list configuration mode. To remove the application port mapping from the forwarding list, use the **no** form of this command.

local-port *number* **remote-server** *name* **remote-port** *number* **description** *text-string*
no local-port *number*

Syntax Description

number	Configures the port number to which the local application is mapped. Valid values are 1 to 65535.
remote-server *name*	Identifies the remote server. An IPv4 address or fully qualified domain name is entered.
remote-port *number*	Specifies the well-known port number of the application, for which port-forwarding is to be configured. Valid values are 1 to 65535.
description *text-string*	Configures a description for this entry in the port-forwarding list. The text string is displayed on the end-user applet window. A text string up to 64 characters in length is entered.

Command Default

An application port number is not remapped.

Command Modes

Webvpn port-forward list configuration (config-webvpn-port-fwd)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **local-port** command is configured to add an entry to the port-forwarding list. The forward list is created with the **port-forward** command in webvpn context configuration mode. The remote port number is the well-known port to which the application listens. The local port number is the entry configured in the port forwarding list. A local port number can be configured only once in a given port-forwarding list.

Examples

The following example configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# port-forward EMAIL

Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com remote-port
 110 description POP3

Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail.company.com remote-port
 25 description SMTP

Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail.company.com remote-port
```

```
143 description IMAP
```

Related Commands

Command	Description
port-forward	Enters webvpn port-forward list configuration mode to configure a port-forwarding list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

local priority

To set the local key server priority, use the **local priority**command in GDOI redundancy configuration mode. To remove the local key server priority that was set, use the **no** form of this command.

local priority *number*
no local priority *number*

Syntax Description

number	Priority number of the local server. Value = 1 through 255.

Command Default

If the local priority is not set by this command, the local priority defaults to 1.

Command Modes

GDOI redundancy configuration (gdoi-coop-ks-config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 Aggregation Services Series Routers.

Usage Guidelines

Configure the priority to determine the order of preference of the key servers (the higher priority device becomes the primary key server). If the priority of two devices is the same, the IP address is used to set the priority. The higher the IP address, the higher the priority.

Note If the **no local priority** option is configured, the default value of 1 is set for that key server.

Examples

The following example shows that the key server 10.1.1.1 has the highest priority and, therefore, becomes the primary key server:

```
address ipv4 10.1.1.1
redundancy
 local priority 10
 peer address ipv4 10.41.2.5
```

peer address ipv4 10.33.5.6

```
address ipv4 10.41.2.5
redundancy
 peer address ipv4 10.1.1.1
```

peer address ipv4 10.33.5.6

```
address ipv4 10.33.5.6
redundancy
 local priority 5
 peer address ipv4 10.41.2.5
```

peer address ipv4 10.1.1.1

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
peer address ipv4	Configures a GDOI redundant peer key server.
redundancy	Enters GDOI redundancy configuration mode and allows for peer key server redundancy.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

lockdown (LSP Attributes)

To disable reoptimization of the label switched path (LSP), use the **lockdown** command in LSP Attributes configuration mode. To reenable reoptimization, use the **no** form of this command.

lockdown
no lockdown

Syntax Description

This command has no arguments or keywords.

Command Default

Reoptimization of the LSP is enabled.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to set up in an LSP attribute list the disabling of reoptimization of an LSP triggered by a timer, or the issuance of the **mpls traffic-eng reoptimize** command, or a configuration change that requires the resignalling of an LSP.

To associate the LSP lockdown attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to configure disabling of reoptimization in an LSP attribute list:

```
Configure terminal
!
mpls traffic-eng lsp attributes 4
 bandwidth 1000
 priority 1 1
 lockdown
 end
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

log (policy-map)

To generate a log of messages, use the **log** command in policy-map configuration mode. To disable the log, use the **no** form of this command.

log
no log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Policy-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced in Cisco IOS Release 12.4(6)T.
12.4(20)T	This command was modified in Cisco IOS Release 12.4(20)T. This command can now be used after entering the **policy-map type inspect smtp**.

Usage Guidelines

You can use this command only after entering the following commands:

- **policy-map type inspect http**
- **policy-map type inspect imap**
- **policy-map type inspect smtp**

Examples

The following example generates a log of messages:

```
policy-map type inspect http mypolicy
 log
```

Related Commands

Command	Description
policy-map type inspect http	Creates a Layer 7 HTTP policy map.
policy-map type inspect imap	Creates a Layer 7 IMAP policy map.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map

log (parameter-map type)

To log the firewall activity for an inspect parameter map, use the **log** command in parameter-map type inspect configuration mode.

log {**dropped-packets** {**disable** | **enable**} | **summary** [**flows** *number*] [**time-interval** *seconds*]}

Syntax Description

dropped-packets	Logs the packets dropped by the firewall.
disable | enable	Disables or enables logging the dropped packets.
summary	Turns on the summary of the packets dropped during the firewall activity for interzone and intrazone traffic.
flows *number*	(Optional) Specifies the number of flows for which the summary logs must be printed. The default flow is 16.
time-interval *seconds*	(Optional) Specifies the time interval, in seconds. which the summary logs must be printed. The default is 60.

Command Default

The firewall activity is not captured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS-XE 2.4	This command was integrated into Cisco IOS-XE Release 2.4.

Usage Guidelines

Use this command to log the firewall activity as follows:

- Time interval for the summary logs
- Display the protocol information in the summary logs
- Enable summary logs for the specified flows

If the flow is specified as zero as **log summary flow 0**, the log activity is turned off and summary logs are not printed until the flow count is greater than zero.

To display the summary logs, use the **show policy-firewall summary-log** and **clear policy-firewall summary-log** to clear the summary logs.

Examples

The following examples show how to configure the summary logs in two scenarios.

In the following example, the summary logs are printed for 40 flows every 2 minutes:

```
Router(config)# parameter-map type inspect global
```

```
Router(config-profile)# log summary flows 40 time-interval 120
In the following example, the summary logs are printed for 30 flows at the default time
interval of 1 minute:
Router(config)# parameter-map type inspect global
Router(config-profile)# log summary flows 30
In the above example, the flow is not configured. Hence, the summary logs are printed by
default for 16 flows every 30 seconds:
Router(config)# parameter-map type inspect global
Router(config-profile)# log summary time-interval 30
```

Related Commands

Command	Description
clear policy-firewall	Clears the information collected by the firewall.
parameter-map type inspect	Defines an inspect type parameter map.
pass	Allows packets to be sent to the router without being inspected.
show policy-firewall summary-log	Displays the summary log of the firewall.

log (type access-control)

Note Effective with Cisco IOS Release 15.2(4)M, the **log** command is not available in Cisco IOS software.

To generate log messages for a predefined traffic class, use the **log** command in policy-map class configuration mode. To disable the log, use the **no** form of this command.

log [**all**]
no log [**all**]

Syntax Description

all	(Optional) Logs the entire stream of discarded packets belonging to the traffic class.

Command Default

Log messages are disabled.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
15.1(3)T	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

If the **log** command is specified with the **all** keyword, then this command can only be used with a predefined session-based Flexible Packet Matching (FPM) traffic class that was created with the **class-map type access-control** command.

The **log all** command is used when configuring a policy map that can be attached to one or more interfaces to specify a service policy that is created with the **policy-map type access-control** command.

Examples

The following example shows how to configure a class map and policy map to specify the protocol stack class, the match criteria and action to take, and a combination of classes using session-based (flow-based) and nonsession-based actions. The **log** command **all** keyword is associated with the action taken on the policy.

```
Router(config)# class-map type access-control match-all my-HTTP
Router(config-cm)# match field tcp destport eq 8080
Router(config-cm)# match start tcp payload-start offset 20 size 10 regex "GET"
Router(config)# class-map type access-control match-all my-FTP
Router(config-cmap)# match field tcp destport eq 21
Router(config)# class-map type access-control match all class1
Router(config-cmap)# match class my-HTTP session
Router(config-cmap)# match start tcp payload-start offset 40 size 20 regex "abc.*def"
Router(config)# policy-map type access-control my_http_policy
Router(config-pmap)# class class1
Router(config-pmap-c)# log all
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input my_http_policy
```

Related Commands

Command	Description
class	Specifies the name of a predefined traffic class, which was configured with the **class-map** command. This command also classifies traffic to the traffic policy and enters policy-map class configuration mode.
class-map type access-control	Creates a class map to be used for matching packets to a specified class and enters class map configuration mode for determining the exact pattern to look for in the protocol stack of interest.
drop	Configures a traffic class to discard packets belonging to a specific class.
match class session	Configures match criteria for a class map used to identify a session (flow) containing packets of interest, which is then applied to all packets transmitted during the session.
policy-map type access-control	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters policy-map configuration mode.
show class-map	Displays all class maps and their matching criteria.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

logging (parameter-map)

To enable the logging of Cloud Web Security content scan events, use the **logging** command in privileged EXEC mode. To disable logging, use the **no** form of this command.

logging
no logging

Syntax Description

This command has no arguments or keywords.

Command Default

Logging of events is disabled.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type cws global** before you configure the **logging** command.

All Cloud Web Security-related syslog displays the username, group name, IP address, and port number of the source and destination.

Examples

The following example shows how to enable logging of Cloud Web Security content scan events:

```
Device(config)# parameter-map type cws global
Device(config-profile)# logging
Device(config-profile)# end
```

Related Commands

Command	Description
parameter-map type cws global	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.

logging dmvpn

To display Dynamic Multipoint VPN (DMVPN)-specific system logging information, use the **logging dmvpn**command in global configuration mode. To turn off logging, use the **no** form of this command.

logging dmvpn [**rate-limit** *rate*]
no logging dmvpn [**rate-limit** *rate*]

Syntax Description

rate-limit *rate*	(Optional) Specifies the number of DMVPN syslog messages generated per minute. The range is from 1 to 10000. • The default rate is to generate 600 messages per minute.

Command Default

DMVPN system logging messages are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)M	This command was modified. The *rate*argument was modified to specify the number of DMVPN syslog messages per minute.

Usage Guidelines

Use the **logging dmvpn rate-limit** *rate*command to specify the rate at which the DMVPN-specific syslog messages are displayed. In Cisco IOS Release 12.4(24)T and earlier releases, the *rate* argument specifies the minimum interval, in seconds, between two DMVPN syslog messages, with a range of 0 to 3600, and a default value of 60.

In Cisco IOS Release 15.0(1)M and later releases, the *rate* argument specifies the number of DMVPN syslog messages per minute. If you have upgraded to Release Cisco IOS 15.0(1)M or later releases, you must reconfigure the DMVPN rate limit settings.

Examples

The following example shows how to configure the router to display five DMVPN-specific syslog messages per minute:

```
Router> enable
Router# configure terminal
Router(config)# logging dmvpn rate-limit 5
```

The following example shows a sample system log with DMVPN messages:

```
%DMVPN-7-CRYPTO_SS: Tunnel101-192.0.2.1 socket is UP
%DMVPN-5-NHRP_NHS: Tunnel101 192.0.2.251 is UP
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel1 Registered.
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel101 came UP.
%DMVPN-3-NHRP_ERROR: Registration Request failed for 192.0.2.251 on Tunnel101
```

Related Commands

Command	Description
debug dmvpn	Debugs DMVPN sessions.

logging enabled

To enable syslog messages, use the **logging enabled**command in parameter-map-type consent configuration mode.

logging enabled

Syntax Description

This command has no arguments or keywords.

Command Default

Logging messages are not enabled.

Command Modes

Parameter-map-type consent (config-profile)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

After the **logging enabled** command is entered, a log entry (a syslog), including the client's IP address and the time, is created everytime a response is received for the consent web page.

Examples

The following example shows how to define the consent-specific parameter map "consent_parameter_map" and a default consent parameter map. In both parameter maps, logging is enabled.

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
```

logging ip access-list cache (global configuration)

To configure the Optimized ACL Logging (OAL) parameters, use the **logging ip access-list cache** command in global configuration mode. To return to the default settings, use the **no** form of this command.

logging ip access-list cache {**entries** *entries* | **interval** *seconds* | **rate-limit** *pps* | **threshold** *packets*}
no logging ip access-list cache [{**entries** | **interval** | **rate-limit** | **threshold**}]

Syntax Description

entries *entries*	Specifies the maximum number of log entries that are cached in the software; valid values are from 0 to 1048576 entries.
interval *seconds*	Specifies the maximum time interval before an entry is sent to syslog; valid values are from 5 to 86400 seconds.
rate-limit *pps*	Specifies the number of packets that are logged per second in the software; valid values are from 10 to 1000000 pps.
threshold *packets*	Specifies the number of packet matches before an entry is sent to syslog; valid values are from 1 to 1000000 packets.

Command Default

The defaults are as follows:

- *entries* --**8000** entries.
- *seconds* --**300** seconds (5 minutes).
- **rate-limit** *pps* --**0** (rate limiting is off) and all packets are logged.
- **threshold** *packets* --**0** (rate limiting is off) and the system log is not triggered by the number of packet matches.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the **update-interval** *seconds* command, th e entry is removed from the cache.

If you enter the **no logging ip access-list cache** command without keywords, all the parameters are returned to the default values.

You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

When enabling the IP "too short" check using the mls verify ip length minimum command, valid IP packets with with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.

Caution Using optimized access-list logging (OAL) and the mls verify ip length minimum command together can cause routing protocol neighbor flapping as they are incompatible

Examples

This example shows how to specify the maximum number of log entries that are cached in the software:

```
Router(config)#
logging ip access-list cache entries 200
```

This example shows how to specify the maximum time interval before an entry is sent to the system log:

```
Router(config)#
logging ip access-list cache interval 350
```

This example shows how to specify the number of packets that are logged per second in the software:

```
Router(config)#
logging ip access-list cache rate-limit 100
```

This example shows how to specify the number of packet matches before an entry is sent to the system log:

```
Router(config)#
logging ip access-list cache threshold 125
```

Related Commands

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (interface configuration)	Enables an OAL-logging cache on an interface that is based on direction.
show logging ip access-list	Displays information about the logging IP access list.
update-interval *seconds*	Removes entries from the cache that are inactive for the duration that is specified in the command.

logging ip access-list cache (interface configuration)

To enable an Optimized ACL Logging (OAL)-logging cache on an interface that is based on direction, use the **logging ip access-list cache** command in interface configuration mode. To disable OAL, use the **no** form of this command.

logging ip access-list cache [{**in** | **out**}]
no logging ip access-list cache

Syntax Description

in	(Optional) Enables OAL on ingress packets.
out	(Optional) Enables OAL on egress packets.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

This command is supported on traffic that matches the **log** keyword in the applied ACL. You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

On systems that are configured with a PFC3A, support for the egress direction on tunnel interfaces is not supported.

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the **update-interval** *seconds* command, th e entry is removed from the cache.

If you enter the **no logging ip access-list cache** command without keywords, all the parameters are returned to the default values.

When enabling the IP "too short" check using the mls verify ip length minimum command, valid IP packets with with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.

Caution Using optimized access-list logging (OAL) and the mls verify ip length minimum command together can cause routing protocol neighbor flapping as they are incompatible

Examples

This example shows how to enable OAL on ingress packets:

```
Router(config-if)#
logging ip access-list cache in
```

This example shows how to enable OAL on egress packets:

```
Router(config-if)#
logging ip access-list cache out
```

Related Commands

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (global configuration)	Configures the OAL parameters.
show logging ip access-list	Displays information about the logging IP access list.
update-interval *seconds*	Removes entries from the cache that are inactive for the duration that is specified in the command.

login authentication

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the **login authentication**command inline configuration mode. To return to the default specified by the aaa authentication login command, use the **no** form of this command.

login authentication {**default***list-name*}
no login authentication {**default***list-name*}

Syntax Description

default	Uses the default list created with the **aaa authentication login** command.
list-name	Uses the indicated list created with the **aaa authentication login**command.

Command Default

Uses the default set with **aaa authentication login**.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is a per-line command used with AAA that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line).

Caution If you use a *list-name* value that was not configured with the **aaa authentication login**command, you will disable login on this line.

Entering the **no** version of **login authentication** has the same effect as entering the command with the **default** keyword.

Before issuing this command, create a list of authentication processes by using the global configuration **aaa authentication login**command.

Examples

The following example specifies that the default AAA authentication is to be used on line 4:

```
line 4
 login authentication default
```

The following example specifies that the AAA authentication list called *list1*is to be used on line 7:

```
line 7
 login authentication list1
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.

login-auth-bypass

To configure the domain name and FQDN ACL that are to be bypassed for a parameter map, use the **login-auth-bypass fqdn** command in parameter map configuration mode.

login-auth-bypass ip-access-list *acl-name* **domain-name-list** *domain-name*

Syntax Description

ip-access-list *acl-name*	Configures a FQDN standard, extended list to a named admission control rule. The value ranges from 1 through 199, or from 1300 through 2699 for expanded range.
domain-name-list *domain-name*	Configures a domain.

Command Default

No domain name and FQDN ACL is defined for bypass.

Command Modes

Parameter map configuration mode (config-params-parameter-map)

Command History

Release	Modification
Cisco IOS Release 15.2(2)S	This command was introduced.

Usage Guidelines

The FQDN ACL determines which IP addresses should redirect the BYOD to the ISE onboarding portal page. This ACL is same as the redirect ACL from ISE onboarding.

This example shows how to configure the domain name and FQDN ACL that are to be bypassed for a parameter map:

```
(config)# parameter-map type webauth Mymap
(config-params-parameter-map)# login auth-bypass ip-access-list byod domain-name-list abc
```

login block-for

To configure your Cisco IOS device for login parameters that help provide denial-of-service (DoS) detection, use the **login block-for**command in global configuration mode. To disable the specified login parameters and return to the default functionality, use the **no** form of this command.

login block-for *seconds* **attempts** *tries* **within** *seconds*
no login block-for

Syntax Description

seconds	Duration of time in which login attempts are denied (also known as a quiet period) by the Cisco IOS device. Valid values range from 1 to 65535 (18 hours) seconds.
attempts *tries*	Maximum number of failed login attempts that triggers the quiet period. Valid values range from 1 to 65535 tries.
within *seconds*	Duration of time in which the allowed number of failed login attempts must be made before the quiet period is triggered. Valid values range from 1 to 65535 (18 hours) seconds.

Command Default

No login parameters are defined.

A quiet period is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25).
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

If the specified number of connection attempts (via the **attempts** *tries* option) fail within a specified time (via the **within** *seconds* option), the Cisco IOS device will not accept any additional login attempts for a specified period of time (via the *seconds* argument).

All login parameters are disabled by default. You must issue the **login block-for** command, which enables default login functionality, before using any other login commands. After the **login block-for** command is enabled, the following defaults are enforced:

- A default login delay of 1 second
- All login attempts made via Telnet and secure shell (SSH) are denied during the quiet period; that is, no access control lists (ACLs) are exempt from the login period until the **login quiet-mode access-class** command is issued. If this command is not configured, then the default ACL **sl_def_acl** is created on

the router. This ACL is hidden in the running configuration. Use the **show access-list sl_def_acl** to view the parameters for the default ACL.

For example:

```
Router#show access-lists sl_def_acl
Extended IP access list sl_def_acl
    10 deny tcp any any eq telnet
    20 deny tcp any any eq www
    30 deny tcp any any eq 22
    40 permit ip any any
```

System Logging Messages

The following logging message is generated after the router switches to quiet mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for watching failures is 158 seconds,
[user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23
UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at
16:22:23 UTC Wed Feb 26 2003
```

Examples

The following example shows how to configure your router to block all login requests for 100 seconds if 15 failed login attempts are exceeded within 100 seconds. Thereafter, the **show login** command is issued to verify the login settings.

```
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# exit
Router# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5
```

The following example shows how to disable login parameters. Thereafter, the **show login** command is issued to verify that login parameters are no longer configured.

```
Router(config)# no login block-for
Router(config)# exit
Router# show login
No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps
Router NOT enabled to watch for login Attacks
```

Related Commands

Command	Description
login delay	Configures a uniform delay between successive login attempts.

Command	Description
login quiet-mode access-class	Specifies an ACL that is to be applied to the router when it switches to quiet mode.
show login	Displays login parameters.

login delay

To configure a uniform delay between successive login attempts, use the **login delay**command in global configuration mode. To return to the default functionality (which is a 1 second delay), use the **no** form of this command.

login delay *seconds*
no login delay

Syntax Description

seconds	Number of seconds between each login attempt. Valid values range from 1 to 10 seconds.

Command Default

If this command is not enabled, a login delay of 1 second is automatically enforced.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

A Cisco IOS device can accept connections (such as Telnet, secure shell (SSH), and HTTP) as fast as they can be processed. The **login delay** command introduces a uniform delay between successive login attempts. (The delay occurs for all login attempts--failed or successful attempts.) Thus, user users can better secure their Cisco IOS device from dictionary attacks, which are an attempt to gain username and password access to your device.

Although the **login delay** command allows users to configure a specific a delay, a uniform delay of 1 second is enabled if the **auto secure** command is issued. After the **auto secure** command is enabled, the autosecure dialog prompts users for login parameters; if login parameters have already been configured, the autosecure dialog will retain the specified values.

Examples

The following example shows how to configure your router to issue a delay of 10 seconds between each successive login attempt:

```
Router(config)# login delay 10
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.

Command	Description
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
show login	Displays login parameters.

login-message

To configure a login message for the text box on the user login page, use the **login-message** command in webvpn context configuration mode. To reconfigure the SSL VPN context configuration to display the default message, use the **no** form of this command.

login-message [*message-string*]
no login-message [*message-string*]

Syntax Description

message-string	*(Optional) Login message string up to 255 characters in length. The string value may contain 7-bit ASCII values, HTML tags, and escape sequences.*

Command Default

The following message is displayed if this command is not configured or if the **no** form is entered:

"Please enter your username and password"

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The optional form of this command is used to change or enter a login message. A text string up to 255 characters in length can be entered. The **no** *form of this command is entered to configure the default message to be displayed. When the* **login-message** *command is entered without the optional text string, no login message is displayed.*

Examples

The following example changes the default login message to "Please enter your login credentials":

```
Router(config)#
webvpn context context1

Router(config-webvpn-context)# login-message "Please enter your login credentials"
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

login quiet-mode access-class

To specify an access control list (ACL) that is to be applied to the router when the router switches to quiet mode, use the **login quiet-mode access-class**command in global configuration mode. To remove this ACL and allow the router to deny all login attempts, use the **no** form of this command.

login quiet-mode access-class {*acl-nameacl-number*}
no login quiet-mode access-class {*acl-nameacl-number*}

Syntax Description

acl-name	Named ACL that is to be enforced during quiet mode.
acl-number	Numbered (standard or extended) ACL that is to be enforced during quiet mode.

Command Default

All login attempts via Telnet, secure shell (SSH), and HTTP are denied.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Before using this command, you must issue the **login block-for** command, which allows you to specify the necessary parameters to enable a quiet period.

- Use the **login quiet-mode access-class** command to selectively allow hosts on the basis of a specified ACL. You may use this command to grant an active client or list of clients an infinite number of failed attempts that are not counted by the router; that is, the active clients are placed on a “safe list” that allows them access to the router despite a quiet period. If this command is not configured, then the default ACL **sl_def_acl** is created on the router. This ACL is hidden in the running configuration. Use the **show access-list sl_def_acl** to view the parameters for the default ACL.

For example:

```
Router#show access-lists sl_def_acl
Extended IP access list sl_def_acl
10 deny tcp any any eq telnet
20 deny tcp any any eq www
30 deny tcp any any eq 22
40 permit ip any any
```

System Logging Messages

The following logging message is generated after the router switches to quiet mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for watching failures is 158 seconds,
[user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23
UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at
16:22:23 UTC Wed Feb 26 2003
```

Examples

The following example shows how to configure your router to accept hosts only from the ACL "myacl" during the next quiet period:

```
Router(config)# login quiet-mode access-class myacl
```

Related Commands

Command	Description
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
show login	Displays login parameters.

login-photo

To set the photo parameters on a Secure Socket Layer Virtual Private Network (SSL VPN) login page, use the **login-photo** command in web vpn context configuration mode. To display the login page with no photo but with a message that spans the message and the photo columns, use the **no** form of this command.

login-photo [{**file** *file-name* | **none**}]
no login-photo

Syntax Description

file *file-name*	Points to a file to be displayed on the login page. The *file-name* argument can be **jpeg**, **bitmap**, or **gif**. However, gif files are recommended.
none	No photo appears on the login page.

Command Default

No photo appears, and the message spans the two columns (message and photo columns).

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

To display no photo, use the **login-photo none** option. To display no photo and have the message span both columns (message column and photo column), use the **no login-photo** option.

The best resolution for login photos is 179 x 152 pixels.

Examples

The following example shows that no photo is displayed:

```
Router (config)# webvpn context
Router (config-webvpn-context)# login-photo none
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

logo

To configure a custom logo to be displayed on the login and portal pages of an SSL VPN, use the **logo** command in SSLVPN configuration mode. To configure the Cisco logo to be displayed, use the **no** form of this command.

logo [{**file** *filename* | **none**}]
no logo [{**file** *filename* | **none**}]

Syntax Description

file *filename*	(Optional) Specifies the location of an image file. A gif, jpg, or png file can be specified. The file can be up to 100 KB in size. The name of the file can be up 255 characters in length.
none	(Optional) No logo is displayed.

Command Default

The Cisco logo is displayed if the **no** form of this command is not configured or if the **no** form is entered.

Command Modes

SSLVPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The source image file for the logo is a gif, jpg, or png file that is up to 255 characters in length (filename) and up to 100 kilobytes (KB) in size. The file is referenced from a local file system, such as flash memory. An error message will be displayed if the file is not referenced from a local file system. No logo will be displayed if the image file is removed from the local file system.

Examples

The following example references mylogo.gif (from flash memory) to use as the SSL VPN logo:

```
Router(config)#
webvpn context SSLVPN

Router(config-webvpn-context)#
logo file flash:/mylogo.gif

Router(config-webvpn-context)#
```

In the following example, no logo is to be displayed on the login or portal pages:

```
Router(config)#
webvpn context SSLVPN

Router(config-webvpn-context)#
logo none
Router(config-webvpn-context)#
```

The following example configures the SSL VPN to display the default logo (Cisco) on the login and portal pages:

```
Router(config)#
webvpn context SSLVPN

Router(config-webvpn-context)#
logo none
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.