Cisco SAF Commands

accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the **accept-lifetime** command in key chain key configuration mode. To revert to the default value, use the **no** form of this command.

accept-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no accept-lifetime [*start-time* {**infinite** | *end-time* | **duration** *seconds*}]

Syntax Description

start-time	Beginning time that the key specified by the **key** command is valid to be received. The syntax can be either of the following: *hh*:*mm*:*ss Month date year* *hh*:*mm*:*ss date Month year* • *hh*—hours • *mm*—minutes • *ss*—seconds • *Month*—first three letters of the month • *date*—date (1–31) • *year*—year (four digits) The default start time and the earliest acceptable date is January 1, 1993.
infinite	Key is valid to be received from the *start-time* value on.
end-time	Key is valid to be received from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.
duration *seconds*	Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

Command Default

The authentication key on a key chain is received as valid forever (the starting time is January 1, 1993, and the ending time is infinite).

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
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 Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), Service Advertisement Framework (SAF), and Routing Information Protocol (RIP) Version 2 use key chains.

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration** *seconds.*

We recommend running Network Time Protocol (NTP) or some other time synchronization method if you assign a lifetime to a key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and will be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and will be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain)# key-string key2
Router(config-keychain)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
```

```
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following named configuration example configures a key chain named chain1 for EIGRP service-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# network 10.0.0.0
Router(config-router-sf)# sf-interface ethernet0/0
Router(config-router-sf-interface)# authentication key-chain trees
Router(config-router-sf-interface)# authentication mode md5
Router(config-router-sf-interface)# exit
Router(config-router-sf)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
authentication key-chain	Specifies an authentication key chain EIGRP.
authentication mode (EIGRP)	Specifies the type of authentication used in EIGRP packets for the EIGRP instance.
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
network	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP process.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
service-family	Configures VRF metrics for a Cisco SAF service-family.
sf-interface	Configure interface-specific commands for a Cisco SAF service family.
show key chain	Displays authentication key information.

authentication key-chain (EIGRP)

To specify an authentication key chain for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **authentication key-chain** (EIGRP) command in address-family interface configuration mode or service-family interface configuration mode. To remove the authentication key-chain, use the **no** form of this command.

authentication key-chain *name-of-chain*

no authentication key-chain *name-of-chain*

Syntax Description

name-of-chain	Group of keys that are valid.

Command Default

No key chains are specified for EIGRP.

Command Modes

Address-family interface configuration (router-config-af-interface)
Service-family interface configuration (router-config-sf-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

The **key-chain** command has no effect until the **authentication mode md5** command is configured.

Only one authentication key chain is applied to EIGRP at one time. That is, if you configure a second **authentication key-chain** command, the first is overridden.

Examples

The following example configures EIGRP to apply authentication to address-family autonomous system 1 and identifies a key chain named SITE1:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain SITE1
Router(config-router-af-interface)# authentication mode md5
```

The following example configures EIGRP to apply authentication to service-family autonomous system 1 and identifies a key chain named SITE1:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 1
Router(config-router-sf)# sf-interface ethernet0/0
Router(config-router-sf-interface)# authentication key-chain SITE1
Router(config-router-sf-interface)# authentication mode md5
```

Related Commands

Command	Description
authentication mode (EIGRP)	Specifies the type of authentication used in EIGRP address-family packets for the EIGRP instance.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
router eigrp	Configures the EIGRP address-family process.

authentication mode (EIGRP)

To specify the type of authentication used in Enhanced Interior Gateway Routing Protocol (EIGRP) address-family or service-family packets for an EIGRP instance, use the **authentication mode** command in address family interface configuration mode or service family interface configuration mode. To disable a configured authentication type, use the **no** form of this command.

authentication mode {**hmac-sha-256** {**0** | **7**} *password* | **md5**}

no authentication mode

Syntax Description

hmac-sha-256	Specifies the Hash-based Message Authentication Code (HMAC)-Secure Hash Algorithms (SHA)-256 authentication.
0	Indicates no password encryption. The default is 0.
7	Indicates explicit password encryption.
password	Password string to be used with SHA authentication. The string can contain 1 to 32 characters including whitespaces, except that the first character cannot be a number.
md5	Specifies message digest algorithm 5 (MD5) authentication.

Command Default

No authentication mode is provided for EIGRP packets.

Command Modes

Address family interface configuration (config-router-af-interface)
Service family interface configuration (config-router-sf-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.1(2)S	This command was modified. The **hmac-sha-256** keyword and the *encryption-type* and *password* arguments were added.

Usage Guidelines

Configure authentication to prevent unapproved sources from introducing unauthorized or false service messages.

When the **authentication mode** (EIGRP) command is used in conjunction with the **authentication key-chain** command, an MD5 keyed digest is added to each EIGRP packet.

To configure basic HMAC-SHA-256 authentication, use the **authentication mode hmac-sha-256** command on each interface of each router that should use authentication.

Examples

The following example shows how to configure the interface to use MD5 authentication in address-family packets:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain TEST1
Router(config-router-af-interface)# authentication mode md5
```

The following example configures the interface to use MD5 authentication in service-family packets:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 1
Router(config-router-sf)# sf-interface ethernet0/0
Router(config-router-sf-interface)# authentication key-chain TEST1
Router(config-router-sf-interface)# authentication mode md5
```

The following example shows how to configure the interface to use basic SHA authentication with password password1 in address-family packets:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv6 autonomous-system 4453
Router(config-router-af)# af-interface ethernet 0
Router(config-router-af-interface)# authentication mode hmac-sha-256 7 password1
```

The following example shows how to configure an interface to use basic SHA authentication with password password1 in service-family packets:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 6473
Router(config-router-sf)# sf-interface ethernet 0
Router(config-router-sf-interface)# authentication mode hmac-sha-256 7 password1
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
af-interface	Enters address family interface configuration mode to configure interface-specific EIGRP commands.
authentication key-chain	Specifies the type of authentication used in EIGRP address-family or service-family packets for the EIGRP instance.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
router eigrp	Configures the EIGRP address-family process.

bandwidth-percent

To configure the percentage of bandwidth that may be used by an Enhanced Interior Gateway Routing Protocol (EIGRP) address family or service family on an interface, use the **bandwidth-percent** command in address-family interface configuration mode or service-family interface configuration mode. To restore the default value, use the **no** form of this command.

bandwidth-percent *maximum-bandwidth-percentage*

no bandwidth-percent

Syntax Description

maximum-bandwidth-percentage	Percent of configured bandwidth that EIGRP may use to send packets. Valid range is 1 to 999999. The default is 50 percent.

Command Default

EIGRP limits bandwidth usage to 50 percent of the configured interface bandwidth.

Command Modes

Address-family interface configuration (config-router-af-interface)
Service-family interface configuration (config-router-sf-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **bandwidth-percent** command to configure a different percentage of bandwidth for use by EIGRP than specified for the link by using the **bandwidth interface** command. Values greater than 100 percent may be configured. This option might be useful if the link bandwidth is set artificially low for other reasons. The default bandwidth percent uses 50 percent of the configured bandwidth of the link.

Examples

The following example uses up to 75 percent (42 kbps) of a 56-kbps serial link for address-family autonomous system 4453:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# bandwidth-percent 75
```

The following example uses up to 75 percent (42 kbps) of a 56-kbps serial link for service-family autonomous system 4533:

```
Router(config)# router eigrp virtual-name
```

```
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# sf-interface serial 0
Router(config-router-sf-interface)# bandwidth-percent 75
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
af-interface	Enters address-family interface configuration mode to configure interface-specific EIGRP commands.
router eigrp	Configures the EIGRP address-family process.
service-family	Configures VRF metrics for an EIGRP service-family.
sf-interface	Configures interface-specific commands for an EIGRP service-family.