



## SAF Commands: A through bandwidth-percent

---

- [accept-lifetime](#), on page 2
- [allow-list](#), on page 5
- [authentication key-chain \(EIGRP\)](#), on page 6
- [authentication mode \(EIGRP\)](#), on page 8
- [bandwidth-percent](#), on page 11

## 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 {infiniteend-time | duration seconds}
no accept-lifetime [start-time {infiniteend-time | duration seconds}]
```

### Syntax Description

<i>start-time</i>	Beginning time that the key specified by the <b>key</b> command is valid to be received. The syntax can be either of the following:  <i>hh</i> : <i>mm</i> : <i>ss</i> <i>Month</i> <i>date</i> <i>year</i> <i>hh</i> : <i>mm</i> : <i>ss</i> <i>date</i> <i>Month</i> <i>year</i> <ul style="list-style-type: none"> <li>• <i>hh</i> --hours</li> <li>• <i>mm</i> --minutes</li> <li>• <i>ss</i>-- s econds</li> <li>• <i>Month</i>-- first three letters of the month</li> <li>• <i>date</i>-- date (1-31)</li> <li>• <i>year</i>-- y ear (four digits)</li> </ul> <p>The default start time and the earliest acceptable date is January 1, 1993.</p>
<b>infinite</b>	Key is valid to be received from the <i>start-time</i> value on.
<i>end-time</i>	Key is valid to be received from the <i>start-time</i> value until the <i>end-time</i> value. The syntax is the same as that for the <i>start-time</i> value. The <i>end-time</i> value must be after the <i>start-time</i> value. The default end time is an infinite time period.
<b>duration</b> <i>seconds</i>	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.

Release	Modification
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

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), 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)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
!
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

```

**Related Commands**

Command	Description
<b>key</b>	Identifies an authentication key on a key chain.
<b>key chain</b>	Defines an authentication key-chain needed to enable authentication for routing protocols.
<b>key-string (authentication)</b>	Specifies the authentication string for a key.
<b>send-lifetime</b>	Sets the time period during which an authentication key on a key chain is valid to be sent.
<b>show key chain</b>	Displays authentication key information.

# allow-list

To restrict the IP addresses that are permitted to connect as an XMCP (Extensible Messaging Client Protocol) client, use the **allow-list** command in XMCP configuration mode. To remove this restriction, use the **no** form of this command.

```
allow-list {ipv4 | ipv6} {acl-name}
no allow-list {ipv4 | ipv6}
```

Syntax Description	Parameter	Description
	<b>ipv4</b>	Restricts IPv4 client IP addresses. Only one allow list may be configured at a time.
	<b>ipv6</b>	Restricts IPv6 client IP addresses. Only one allow list may be configured at a time.
	<i>acl-name</i>	Access control list to use to restrict client IP addresses.

**Command Default** No ACL is configured, which allows all source IP addresses to connect as XMCP clients.

**Command Modes** XMCP configuration (config-xmcp)

Command History	Release	Modification
	15.2(1)S	This command was introduced.
	Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
	15.2(2)T	This command was integrated into Cisco IOS 15.2(2)T.

**Usage Guidelines** The **allow-list** command is used to restrict the IP addresses that are permitted to connect as clients. After an allow list is configured, a client attempting to register will be permitted only if its IP address is permitted by the access list specified.

After an allow list is added or modified, any currently connected clients that would no longer be permitted by the new allow list will have their sessions terminated.

Only one IPv4 and one IPv6 allow list may be configured at a time.

## Examples

The following example show how to restrict access for IPv4 clients to connect only from source IP addresses permitted by the access list `client_acl` and restricts access for IPv6 clients to connect only from source IP addresses permitted by the access list `acl_ipv6`:

```
Router(config)# service-routing xmcp listen
Router(config-xmcp)# allow-list ipv4 client_acl
Router(config-xmcp)# allow-list ipv6 acl_ipv6
Router(config-xmcp)# end
```

Related Commands	Command	Description
	<b>service-routing xmcp listen</b>	Defines a port on which XMCP clients can connect.

## 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

<i>name-of-chain</i>	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)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.

### 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**

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

<b>hmac-sha-256</b>	Specifies the Hashed Message Authentication Code (HMAC)-Secure Hash Algorithm (SHA)-256 authentication.
<b>0</b>	Indicates that there is no password encryption. 0 is the default.
<b>7</b>	Indicates that there is an explicit password encryption.
<i>password</i>	Password string to be used with SHA authentication. The string can contain 1 to 32 characters including white spaces; however, the first character cannot be a number.
<b>md5</b>	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)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.
15.1(2)S	This command was modified. The <b>hmac-sha-256</b> keyword and the <i>encryption-type</i> and <i>password</i> arguments were added.
Cisco IOS XE Release 3.3S	This command was modified. The <b>hmac-sha-256</b> keyword and the <i>encryption-type</i> and <i>password</i> arguments were added.
15.2(1)T	This command was modified. The <b>hmac-sha-256</b> keyword and the <i>encryption-type</i> and <i>password</i> arguments were added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.



**Usage Guidelines**

You can 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 shows how to configure 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 HMAC 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 HMAC 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
<b>address-family (EIGRP)</b>	Enters address family configuration mode to configure an EIGRP routing instance.
<b>af-interface</b>	Enters address family interface configuration mode to configure interface-specific EIGRP commands.
<b>authentication key-chain</b>	Specifies the type of authentication used in EIGRP address-family or service-family packets for the EIGRP instance.

Command	Description
<b>key chain</b>	Defines an authentication key chain needed to enable authentication for routing protocols.
<b>router eigrp</b>	Configures an EIGRP routing 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**

<b>Syntax Description</b>	<i>maximum-bandwidth-percentage</i>	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)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.

**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**

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