



Keychain Management Commands on Cisco IOS XR Software

This module describes the commands used to configure keychain Cisco IOS XR Software.

For detailed information about keychain management concepts, configuration tasks, and examples, see the *Implementing Keychain Management on Cisco IOS XR Software* configuration module of *Cisco IOS XR System Security Configuration Guide*.

accept-lifetime

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

accept-lifetime *start-time* [**duration** *duration value* | **infinite** | *end-time*]

no accept-lifetime *start-time* [**duration** *duration value* | **infinite** | *end-time*]

Syntax Description

<i>start-time</i>	Start time, in <i>hh:mm:ss day month year</i> format, in which the key becomes valid. The range is from 0:0:0 to 23:59:59. The range for the number of days of the month is from 1 to 31. The range for the years is from 1993 to 2035.
duration <i>duration value</i>	(Optional) Determines the lifetime of the key in seconds. The range is from 1-2147483646.
infinite	(Optional) Specifies that the key never expires after it becomes valid.
<i>end-time</i>	(Optional) Time, in <i>hh:mm:ss day month year</i> format, after which the key expires. The range is from 0:0:0 to 23:59:59.

Defaults

No default behavior or values

Command Modes

Key configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	The range values were added for the <i>start-time</i> argument.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **accept-lifetime** command:

```
RR/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# key chain isis-keys
RP/0/0/CPU0:router(config-isis-keys)# key 8
RP/0/0/CPU0:router(config-isis-keys-0x8)# accept-lifetime 1:00:00 June 29 2006 infinite
```

Related Commands

Command	Description
key (key chain)	Creates or modifies a keychain key.
key chain (key chain)	Creates or modifies a keychain.
key-string (keychain)	Specifies the text for the key string.
send-lifetime	Sends the valid key.
show key chain	Displays the keychain.

accept-tolerance

To specify the tolerance or acceptance limit, in seconds, for an accept key that is used by a peer, use the **accept-tolerance** command in keychain configuration mode. To disable this feature, use the **no** form of this command.

accept-tolerance [*value* | **infinite**]

no accept-tolerance [*value* | **infinite**]

Syntax Description

<i>value</i>	(Optional) Tolerance range, in seconds. The range is from 1 to 8640000.
infinite	(Optional) Specifies that the tolerance specification is infinite. The accept key never expires. The tolerance limit of infinite indicates that an accept key is always acceptable and validated when used by a peer.

Defaults

The default value is 0, which is no tolerance.

Command Modes

Keychain configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator.

If you do not configure the **accept-tolerance** command, the tolerance value is set to zero.

Even though the key is outside the active lifetime, the key is deemed acceptable as long as it is within the tolerance limit (for example, either prior to the start of the lifetime, or after the end of the lifetime).

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **accept-tolerance** command:

```
RP/0/0/CPU0:router# configure  
RP/0/0/CPU0:router(config)# key chain isis-keys  
RP/0/0/CPU0:router(config-isis-keys)# accept-tolerance infinite
```

Related Commands

Command	Description
accept-lifetime	Accepts the valid key.
key chain (key chain)	Creates or modifies a keychain.
show key chain	Displays the keychain.

cryptographic-algorithm

To specify the choice of the cryptographic algorithm to be applied to the packets using the key string configured for the key ID, use the **cryptographic-algorithm** command in keychain-key configuration mode. To disable this feature, use the **no** form of this command.

cryptographic-algorithm [HMAC-MD5 | HMAC-SHA1-12 | HMAC-SHA1-20 | MD5 | SHA-1]

no cryptographic-algorithm [HMAC-MD5 | HMAC-SHA1-12 | HMAC-SHA1-20 | MD5 | SHA-1]

Syntax Description	Command	Description
	HMAC-MD5	Configures HMAC-MD5 as a cryptographic algorithm with a digest size of 16 bytes.
	HMAC-SHA1-12	Configures HMAC-SHA1-12 as a cryptographic algorithm with a digest size of 12 bytes.
	HMAC-SHA1-20	Configures HMAC-SHA1-20 as a cryptographic algorithm with a digest size of 20 bytes.
	MD5	Configures MD5 as a cryptographic algorithm with a digest size of 16 bytes.
	SHA-1	Configures SHA-1-20 as a cryptographic algorithm with a digest size of 20 bytes.

Defaults No default behavior or values

Command Modes Keychain-key configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced.
	Release 3.5.0	No modification.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.
	Release 3.8.0	No modification.
	Release 3.9.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator.

If you do not specify the cryptographic algorithm, MAC computation and API verification would be invalid.

These protocols support the following cryptographic algorithms:

- Border Gateway Protocol (BGP) supports only HMAC-MD5 and HMAC-SHA1-12.

- Intermediate System-to-Intermediate System (IS-IS) supports only HMAC-MD5.
- Open Shortest Path First (OSPF) supports only MD5.

Task ID	Task ID	Operations
	system	read, write

Examples

The following example shows how to use the **cryptographic-algorithm** command:

```
RP/0/RSP00/CPU0:router# configure
RP/0/RSP00/CPU0:router(config)# key chain isis-keys
RP/0/RSP00/CPU0:router(config-isis-keys)# key 8
RP/0/RSP00/CPU0:router(config-isis-keys-0x8)# cryptographic-algorithm HMAC-MD5
```

Related Commands

Command	Description
accept-lifetime	Accepts the valid key.
key chain (key chain)	Creates or modifies a keychain.
show key chain	Displays the keychain.

key (key chain)

To create or modify a keychain key, use the **key** command in keychain-key configuration mode. To disable this feature, use the **no** form of this command.

key *key-id*

no key *key-id*

Syntax Description	<i>key-id</i>	48-bit integer key identifier of from 0 to 281474976710655.
---------------------------	---------------	---

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	Keychain-key configuration
----------------------	----------------------------

Command History	Release	Modification
	Release 3.3.0	This command was introduced.
Release 3.4.0	No modification.	
Release 3.5.0	No modification.	
Release 3.6.0	No modification.	
Release 3.7.0	No modification.	
Release 3.8.0	No modification.	
Release 3.9.0	No modification.	

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator.
-------------------------	---

For a Border Gateway Protocol (BGP) keychain configuration, the range for the *key-id* argument must be from 0 to 63. If the range is above the value of 63, the BGP keychain operation is rejected.

Task ID	Task ID	Operations
	system	read, write

Examples

The following example shows how to use the **key** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# key chain isis-keys
RP/0/0/CPU0:router(config-isis-keys)# key 8
RP/0/0/CPU0:router(config-isis-keys-0x8)#
```

Related Commands

Command	Description
accept-lifetime	Accepts the valid key.
key chain (key chain)	Creates or modifies a keychain.
key-string (keychain)	Specifies the text for the key string.
send-lifetime	Sends the valid key.
show key chain	Displays the keychain.

key chain (key chain)

To create or modify a keychain, use the **key chain** command in global configuration mode. To disable this feature, use the **no** form of this command.

key chain *key-chain-name*

no key chain *key-chain-name*

Syntax Description	<i>key-chain-name</i>	Specifies the name of the keychain. The maximum number of characters is 48.
--------------------	-----------------------	---

Defaults	No default behavior or values
----------	-------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	Release 3.3.0	This command was introduced.
	Release 3.4.0	No modification.
	Release 3.4.1	The maximum number of characters allowed in the keychain name was changed from 32 to 48.
	Release 3.5.0	No modification.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.
	Release 3.8.0	No modification.
	Release 3.9.0	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator.

You can configure a keychain for Border Gateway Protocol (BGP) as a neighbor, session group, or neighbor group. BGP can use the keychain to implement a hitless key rollover for authentication.

Task ID	Task ID	Operations
	system	read, write

Examples The following example shows that the name of the keychain isis-keys is for the **key chain** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# key chain isis-keys
```

```
RP/0/0/CPU0:router(config-isis-keys)#
```

Related Commands

Command	Description
accept-lifetime	Accepts the valid key.
accept-tolerance	Configures a tolerance value to accept keys for the keychain.
key (key chain)	Creates or modifies a keychain key.
key-string (keychain)	Specifies the text for the key string.
send-lifetime	Sends the valid key.
show key chain	Displays the keychain.

key-string (keychain)

To specify the text string for the key, use the **key-string** command in keychain-key configuration mode. To disable this feature, use the **no** form of this command.

key-string [**clear** | **password**] *key-string-text*

no key-string [**clear** | **password**] *key-string-text*

Syntax Description

clear	Specifies the key string in clear-text form.
password	Specifies the key in encrypted form.
<i>key-string-text</i>	Text string for the key, which is encrypted by the parser process before being saved to the configuration. The text string has the following character limitations: <ul style="list-style-type: none"> • Plain-text key strings—Minimum of 1 character and a maximum of 32. • Encrypted key strings—Minimum of 4 characters and no maximum.

Defaults

The default value is clear.

Command Modes

Keychain-key configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator.

For an encrypted password to be valid, the following statements must be true:

- String must contain an even number of characters, with a minimum of four.
- The first two characters in the password string must be decimal numbers and the rest must be hexadecimal.
- The first two digits must not be a number greater than 53.

Either of the following examples would be valid encrypted passwords:

```
1234abcd
or
50aefd
```

Task ID	Task ID	Operations
	system	read, write

Examples

The following example shows how to use the **keystring** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# key chain isis-keys
RP/0/0/CPU0:myhost(config-isis-keys)# key 8
RP/0/0/CPU0:myhost(config-isis-keys-0x8)# key-string password 50aefd
```

Related Commands

Command	Description
accept-lifetime	Accepts the valid key.
key (key chain)	Creates or modifies a keychain key.
key chain (key chain)	Creates or modifies a keychain.
send-lifetime	Sends the valid key.
show key chain	Displays the keychain.

send-lifetime

To send the valid key and to authenticate information from the local host to the peer, use the **send-lifetime** command in keychain-key configuration mode. To disable this feature, use the **no** form of this command.

send-lifetime *start-time* [**duration** *duration value* | **infinite** | *end-time*]

no send-lifetime *start-time* [**duration** *duration value* | **infinite** | *end-time*]

Syntax Description

<i>start-time</i>	Start time, in <i>hh:mm:ss day month year</i> format, in which the key becomes valid. The range is from 0:0:0 to 23:59:59. The range for the number of days of the month to start is from 1 to 31. The range for the years is from 1993 to 2035.
duration <i>duration value</i>	(Optional) Determines the lifetime of the key in seconds.
infinite	(Optional) Specifies that the key never expires once it becomes valid.
<i>end-time</i>	(Optional) Time, in <i>hh:mm:ss day month year</i> format, after which the key expires. The range is from 0:0:0 to 23:59:59

Defaults

No default behavior or values

Command Modes

Keychain-key configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	The range values were added for the <i>start-time</i> argument.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **send-lifetime** command:

```
RR/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# key chain isis-keys
RP/0/0/CPU0:router(config-isis-keys)# key 8
RP/0/0/CPU0:router(config-isis-keys-0x8)# send-lifetime 1:00:00 June 29 2006 infinite
```

Related Commands

Command	Description
accept-lifetime	Accepts the valid key.
key (key chain)	Creates or modifies a keychain key.
key chain (key chain)	Creates or modifies a keychain.
key-string (keychain)	Specifies the text for the key string.

show key chain

To display the keychain, use the **show key chain** command in EXEC mode.

show key chain *key-chain-name*

Syntax Description	<i>key-chain-name</i>	Names of the keys in the specified keychain. The maximum number of characters is 32.
--------------------	-----------------------	--

Defaults	No default behavior or values
----------	-------------------------------

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	Release 3.3.0	This command was introduced.
	Release 3.4.0	No modification.
	Release 3.5.0	No modification.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.
	Release 3.8.0	No modification.
	Release 3.9.0	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator.
------------------	---

Task ID	Task ID	Operations
	system	read

Examples	When a secure key storage becomes available, it is desirable for keychain management to alternatively prompt you for a master password and display the key label after decryption. The following example displays only the encrypted key label for the show key chain command:
----------	---

```
RP/0/0/CPU0:router# show key chain isis-keys

Key-chain: isis-keys/ -

accept-tolerance -- infinite
Key 8 -- text "8"
  cryptographic-algorithm -- MD5
  Send lifetime: 01:00:00, 29 Jun 2006 - Always valid [Valid now]
```



```
Accept lifetime: 01:00:00, 29 Jun 2006 - Always valid [Valid now]
```

Related Commands

Command	Description
accept-lifetime	Accepts the valid key.
accept-tolerance	Configures a tolerance value to accept keys for the keychain.
cryptographic-algorithm	Specifies the choice of the cryptographic algorithm.
key (key chain)	Creates or modifies a keychain key.
key chain (key chain)	Creates or modifies a keychain.
key-string (keychain)	Specifies the text for the key string.
send-lifetime	Sends the valid key.

■ show key chain