Keychain Management Commands

This module describes the commands used to configure keychain management.

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

- accept-lifetime, on page 2
- ao, on page 4
- accept-tolerance, on page 5
- key (key chain), on page 6
- key (tcp ao keychain), on page 7
- keychain, on page 8
- key chain (key chain), on page 9
- key-string (keychain), on page 11
- send-lifetime, on page 13
- show key chain, on page 15
- tcp ao, on page 17

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*}]

Syntax Description

start-time	Start time, in *hh:mm:ss day month year* 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 *duration value*	(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.
end-time	(Optional) Time, in *hh:mm:ss day month year* format, after which the key expires. The range is from 0:0:0 to 23:59:59.

Command Default

None

Command Modes

Key configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	The range values were added for the *start-time* argument.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# accept-lifetime 1:00:00 June 29 2006 infinite
```

Related Commands

Command	Description
key (key chain), on page 6	Creates or modifies a keychain key.
key chain (key chain), on page 9	Creates or modifies a keychain.
key-string (keychain), on page 11	Specifies the text for the key string.
send-lifetime, on page 13	Sends the valid key.
show key chain, on page 15	Displays the keychain.

ao

To specify the name the key chain used in the authentication option **ao** command in BGP neighbor configuration mode.

ao *key-chain-name* { **inheritance-disable** | **include-tcp-options** { **disable** | **enable** } **accept-ao-mismatch-connection** }

Syntax Description

key-chain-name	Specifies the name of the key chain. String of maximum length of 32 characters.
inheritance-disable	Prevents the key chain from being inherited from the parent.
include-tcp-options	Includes or excludes other TCP options in the header for MAC calculation.
disable	Excludes other TCP options in the header.
enable	Includes other TCP options in the header.
accept-ao-mismatch-connection	Accepts connection even if there is a mismatch of AO options between peers.

Command Default

The key chain has no specified name.

Command Modes

BGP neighbor

Command History

Release	Modification
Release 6.5.1	This command was introduced.

This example shows how to specify the name the key chain used in the authentication option :

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#router bgp 100
RP/0/RP0/CPU0:router(config-bgp)#neighbor 10.51.51.1
RP/0/RP0/CPU0:router(config-bgp-nbr)#address-family vpnv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr)#ao tcpao1 include-tcp-options disable
accept-ao-mismatch-connection
```

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**}]

Syntax Description

value	(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.

Command Default

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.

Usage Guidelines

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# accept-tolerance infinite
```

Related Commands

Command	Description
accept-lifetime, on page 2	Accepts the valid key.
key chain (key chain), on page 9	Creates or modifies a keychain.
show key chain, on page 15	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*

Syntax Description

key-id	48-bit integer key identifier of from 0 to 281474976710655.

Command Default

No default behavior or values

Command Modes

Keychain-key configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)#
```

Related Commands

Command	Description
accept-lifetime, on page 2	Accepts the valid key.
key chain (key chain), on page 9	Creates or modifies a keychain.
key-string (keychain), on page 11	Specifies the text for the key string.
send-lifetime, on page 13	Sends the valid key.
show key chain, on page 15	Displays the keychain.

key (tcp ao keychain)

To configure in send and receive identifiers for the key, use the **key** command in TCP authentication option keychain configuration mode.

key *key-identifier* **sendID** *send-id-value* **ReceiveID** *receive-id-value*

Syntax Description

key-identifier	Identifier of the key. Acceptable values are 48-bit integers. Range is 0 to 281474976710655.
SendID *send-id-value*	Specifies the send identifier value. Range is 0 to 255.
ReceiveID *receive-id-value*	Specifies the receive identifier value to be used for the key. The range is 0 to 255.

Command Default

The key is not enabled.

Command Modes

TCP authentication option keychain

Command History

Release	Modification
Release 6.5.1	This command was introduced.

Task ID

Task ID	Operations
bgp	read

Examples

This example shows how to configure the send and receive identifier for the key.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# tcp ao
RP/0/RP0/CPU0:router(conf-tcp-ao)# keychain tcpao1
RP/0/RP0/CPU0:router(config-tcp-ao-tpcao1)# key 10 sendID 5 receiveID 5
```

keychain

To configure the keychain to be used in TCP authentication option, use the **tcp ao** command in TCP authentication option configuration mode.

keychain *keychain-name*

Syntax Description

This command has no arguments or keywords.

Command Default

The keychain is not enabled.

Command Modes

TCP authentication option

Command History

Release	Modification
Release 6.5.1	This command was introduced.

Task ID

Task ID	Operations
bgp	read

Examples

This example shows how to configure the **keychain** for TCP Authentication option:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# tcp ao
RP/0/RP0/CPU0:router(conf-tcp-ao)keychain tcpao1
```

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*

Syntax Description

key-chain-name	Specifies the name of the keychain. The maximum number of characters is 48.

Command Default

No default behavior or values

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.4.1	The maximum number of characters allowed in the keychain name was changed from 32 to 48.

Usage Guidelines

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)#
```

Related Commands

Command	Description
accept-lifetime, on page 2	Accepts the valid key.
accept-tolerance, on page 5	Configures a tolerance value to accept keys for the keychain.
key (key chain), on page 6	Creates or modifies a keychain key.
key-string (keychain), on page 11	Specifies the text for the key string.
send-lifetime, on page 13	Sends the valid key.

Command	Description
show key chain, on page 15	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*

Syntax Description

clear	Specifies the key string in clear-text form.
password	Specifies the key in encrypted form.
key-string-text	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: • Plain-text key strings—Minimum of 1 character and a maximum of 32. • Encrypted key strings—Minimum of 4 characters and no maximum.

Command Default

The default value is clear.

Command Modes

Keychain-key configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

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 hexadecimals.
- 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

From Cisco IOS XR Software Release 6.7.2, , and later, if you are using any **HMAC-SHA** algorithm for a session, then you must ensure that the configured *key-string* has a minimum length of 14 characters. Otherwise, the session goes down. This guideline is applicable only for FIPS mode.

Task ID

Task ID	Operations
system	read, write

Examples

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

```
RP/0/RP0/CPU0:router:# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# key-string password 850aefd
```

Related Commands

Command	Description
accept-lifetime, on page 2	Accepts the valid key.
key (key chain), on page 6	Creates or modifies a keychain key.
key chain (key chain), on page 9	Creates or modifies a keychain.
send-lifetime, on page 13	Sends the valid key.
show key chain, on page 15	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*}]

Syntax Description

start-time	Start time, in *hh:mm:ss day month year* 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 *duration value*	(Optional) Determines the lifetime of the key in seconds.
infinite	(Optional) Specifies that the key never expires once it becomes valid.
end-time	(Optional) Time, in *hh:mm:ss day month year* format, after which the key expires. The range is from 0:0:0 to 23:59:59

Command Default

No default behavior or values

Command Modes

Keychain-key configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	The range values were added for the *start-time* argument.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# send-lifetime 1:00:00 June 29 2006 infinite
```

Related Commands

Command	Description
accept-lifetime, on page 2	Accepts the valid key.
key (key chain), on page 6	Creates or modifies a keychain key.
key chain (key chain), on page 9	Creates or modifies a keychain.
key-string (keychain), on page 11	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

key-chain-name	Names of the keys in the specified keychain. The maximum number of characters is 32.

Command Default

If the command is used without any parameters, then it lists out all the key chains.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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 primary 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/RP0/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, on page 2	Accepts the valid key.
accept-tolerance, on page 5	Configures a tolerance value to accept keys for the keychain.
key (key chain), on page 6	Creates or modifies a keychain key.
key chain (key chain), on page 9	Creates or modifies a keychain.
key-string (keychain), on page 11	Specifies the text for the key string.

Command	Description
send-lifetime, on page 13	Sends the valid key.

tcp ao

To enable the TCP authentication option, use the **tcp ao** command in global configuration mode.

tcp ao
no tcp ao

Syntax Description

This command has no arguments or keywords.

Command Default

The TCP authentication option is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 6.5.1	This command was introduced.

Task ID

Task ID	Operations
bgp	read

Examples

This example shows how to configure the **tcp ao** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# tcp ao
```