CHAPTER 17

Configuring Keychain Management

This chapter describes how to configure keychain management on an NX-OS device.

This chapter includes the following sections:

Information About Keychain Management

This section includes the following topics:

Keychains and Keychain Management

Keychain management allows you to create and maintain keychains, which are sequences of keys (sometimes called shared secrets). You can use keychains with features that secure communications with other devices by using key-based authentication. The device allows you to configure multiple keychains.

Some routing protocols that support key-based authentication can use a keychain to implement a hitless key rollover for authentication. For more information, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0*.

Lifetime of a Key

To maintain stable communications, each device that uses a protocol that is secured by key-based authentication must be able to store and use more than one key for a feature at the same time. Based on the send and accept lifetimes of a key, keychain management provides a secure mechanism to handle key rollover. The device uses the lifetimes of keys to determine which keys in a keychain are active.

Each key in a keychain has two lifetimes, as follows:

- Accept lifetime—The time interval within which the device accepts the key during key exchange with another device.
- Send lifetime—The time interval within which the device sends the key during key exchange with another device.

You define the send and accept lifetimes of a key using the following parameters:

- Start-time—The absolute time that the lifetime begins.
- End-time—The end time can be defined in one of the following ways:
  - The absolute time that the lifetime ends
  - The number of seconds after the start time that the lifetime ends
  - Infinite lifetime (no end-time)

During a key send lifetime, the device sends routing update packets with the key. The device does not accept communication from other devices when the key sent is not within the accept lifetime of the key on the device.

We recommend that you configure key lifetimes that overlap within every keychain. This practice avoids failure of neighbor authentication due to the absence of active keys.

Virtualization Support

The following information applies to keychains used in Virtual Device Contexts (VDCs):

- Keychains are unique per VDC. You cannot use a keychain that you created in one VDC in a different VDC.
- Because keychains are not shared by VDCs, you can reuse keychain names in different VDCs.
- The device does not limit keychains on a per-VDC basis.

Licensing Requirements for Keychain Management

The following table shows the licensing requirements for this feature:

Product	License Requirement
NX-OS	Keychain management requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0*.

Prerequisites for Keychain Management

Keychain management has no prerequisites.

Guidelines and Limitations

Keychain management has the following configuration guideline and limitation:

- Changing the system clock impacts the when keys are active.

Configuring Keychain Management

This section includes the following topics:

Creating a Keychain

You can create a keychain on the device.

BEFORE YOU BEGIN

A new keychain contains no keys. For information about adding a key, see the "Configuring a Key" section on page 17-5.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **key chain** *name*
3. **show key chain** *name*
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**key chain** *name* **Example:** switch(config)# key chain glbp-keys switch(config-keychain)#	Creates the keychain and enters keychain configuration mode.
Step 3	**show key chain** *name* **Example:** switch(config-keychain)# show key chain glbp-keys	(Optional) Displays the keychain configuration.
Step 4	**copy running-config startup-config** **Example:** switch(config-keychain)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Removing a Keychain

You can remove a keychain on the device.

Note Removing a keychain removes any keys within the keychain.

BEFORE YOU BEGIN

If you are removing a keychain, ensure that no feature uses it. If a feature is configured to use a keychain that you remove, that feature is likely to fail to communicate with other devices.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **no key chain** *name*
3. **show key chain** *name*
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**no key chain** *name* **Example:** switch(config)# no key chain glbp-keys	Removes the keychain and any keys that the keychain contains.
Step 3	**show key chain** *name* **Example:** switch(config-keychain)# show key chain glbp-keys	(Optional) Confirms that the keychain no longer exists in running configuration.
Step 4	**copy running-config startup-config** **Example:** switch(config-keychain)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring a Key

You can configure a key for a keychain.

A new key contains no text (shared secret). For information about adding text to a key, see the "Configuring Text for a Key" section on page 17-6.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

The default accept and send lifetimes for a new key are infinite. For more information, see the "Configuring Accept and Send Lifetimes for a Key" section on page 17-7.

SUMMARY STEPS

1. **config t**
2. **key chain** *name*
3. **key** *key-ID*
4. **show key chain** *name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**key chain** *name* **Example:** switch(config)# key chain glbp-keys switch(config-keychain)#	Enters keychain configuration mode for the keychain that you specified.
Step 3	**key** *key-ID* **Example:** switch(config-keychain)# key 13 switch(config-keychain-key)#	Enters key configuration mode for the key that you specified. The *key-ID* argument must be a whole number between 0 and 65535.
Step 4	**show key chain** *name* **Example:** switch(config-keychain-key)# show key chain glbp-keys	(Optional) Shows the keychain configuration, including the key configuration.
Step 5	**copy running-config startup-config** **Example:** switch(config-keychain)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring Text for a Key

You can configure the text for a key. The text is the shared secret. The device stores the text in a secure format.

BEFORE YOU BEGIN

Determine the text for the key. You can enter the text as unencrypted text or in the encrypted form that NX-OS uses to display key text when you use the **show key chain** command. Using the encrypted form is particularly helpful if you are creating key text to match a key as shown in the **show key chain** command output from another device.

By default, accept and send lifetimes for a key are infinite, which means that the key is always valid. After you configure the text for a key, configure the accept and send lifetimes for the key. For more information, see the "Configuring Accept and Send Lifetimes for a Key" section on page 17-7.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **key chain** *name*
3. **key** *key-ID*
4. **key-string** [*encryption-type*] *text-string*

5. **show key chain** *name* [**mode decrypt**]
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**key chain** *name*
	
	Example:
	`switch(config)# key chain glbp-keys`
	`switch(config-keychain)#`
		Enters keychain configuration mode for the keychain that you specified.

Step 3	**key** *key-ID*
	
	Example:
	`switch(config-keychain)# key 13`
	`switch(config-keychain-key)#`
		Enters key configuration mode for the key that you specified. The *key-ID* argument must be a whole number between 0 and 65535.

Step 4	**key-string** [*encryption-type*] *text-string* **Example:** `switch(config-keychain-key)# key-string 0 AS3cureStr1ng`	Configures the text string for the key. The *text-string* argument is alphanumeric, case-sensitive, and supports special characters. The *encryption-type* argument can be one of the following values: • 0—The *text-string* argument that you enter is unencrypted text. This is the default. • 7—The *text-string* argument that you enter is encrypted. The encryption method is a Cisco proprietary method. This option is useful when you are entering a text string based on the encrypted output of a **show key chain** command that you ran on another NX-OS device.
Step 5	**show key chain** *name* [**mode decrypt**] **Example:** `switch(config-keychain-key)# show key chain glbp-keys`	(Optional) Shows the keychain configuration, including the key text configuration. The **mode decrypt** option, which can be used by a device administrator only, displays the keys in cleartext.
Step 6	**copy running-config startup-config** **Example:** `switch(config-keychain-key)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring Accept and Send Lifetimes for a Key

You can configure the accept lifetime and send lifetime for a key.

Note We recommend that you configure the keys in a keychain to have overlapping lifetimes. This practice prevents loss of key-secured communication due to moments where no key is active.

BEFORE YOU BEGIN

By default, accept and send lifetimes for a key are infinite, which means that the key is always valid.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **key chain** *name*
3. **key** *key-ID*
4. **accept-lifetime** [**local**] *start-time* [**duration** *duration-value* | **infinite** | *end-time*]
   send-lifetime [**local**] *start-time* [**duration** *duration-value* | **infinite** | *end-time*]
5. **show key chain** *name* [**mode decrypt**]
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**key chain** *name*
	
	Example:
	`switch(config)# key chain glbp-keys`
	`switch(config-keychain)#`
		Enters keychain configuration mode for the keychain that you specified.

Step 3	**key** *key-ID*
	
	Example:
	`switch(config-keychain)# key 13`
	`switch(config-keychain-key)#`
		Enters key configuration mode for the key that you specified.

	Command	Purpose
Step 4	**accept-lifetime** [**local**] *start-time* **duration** *duration-value* | **infinite** | *end-time*] **Example:** `switch(config-keychain-key)# accept-lifetime 00:00:00 Jun 13 2008 23:59:59 Sep 12 2008`	Configures an accept lifetime for the key. By default, the device treats the *start-time* and *end-time* arguments as UTC. If you specify the **local** keyword, the device treats these times as local times. The *start-time* argument is the time of day and date that the key becomes active. Specify the end of the lifetime with one of the following options: • **duration** *duration-value*—The length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years). • **infinite**—The accept lifetime of the key never expires. • *end-time*—The *end-time* argument is the time of day and date that the key becomes inactive.
	send-lifetime [**local**] *start-time* **duration** *duration-value* | **infinite** | *end-time*] **Example:** `switch(config-keychain-key)# send-lifetime 00:00:00 Jun 13 2008 23:59:59 Aug 12 2008`	Configures a send lifetime for the key. By default, the device treats the *start-time* and *end-time* arguments as UTC. If you specify the **local** keyword, the device treats these times as local times. The *start-time* argument is the time of day and date that the key becomes active. You can specify the end of the send lifetime with one of the following options: • **duration** *duration-value*—The length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years). • **infinite**—The send lifetime of the key never expires. • *end-time*—The *end-time* argument is the time of day and date that the key becomes inactive.
Step 5	**show key chain** *name* [**mode decrypt**] **Example:** `switch(config-keychain-key)# show key chain glbp-keys`	(Optional) Shows the keychain configuration, including the key text configuration. The **mode decrypt** option, which can be used by a device administrator only, displays the keys in cleartext.
Step 6	**copy running-config startup-config** **Example:** `switch(config-keychain-key)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Determining Active Key Lifetimes

To determine which keys within a keychain have active accept or send lifetimes, use the following command:

Command	Purpose
show key chain	Displays the keychains configured on the device.

For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

Verifying the Keychain Management Configuration

To display keychain management configuration information, perform one of the following tasks:

Command	Purpose
show key chain	Displays the keychains configured on the device.

For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

Example Configuration for Keychain Management

The following example shows how to configure a keychain named glbp keys. Each key text string is encrypted. Each key has longer accept lifetimes than send lifetimes, to help prevent lost communications by accidentally configuring a time in which there are no active keys.

```
key chain glbp-keys
  key 0
    key-string 7 zqdest
    accept-lifetime 00:00:00 Jun 01 2008 23:59:59 Sep 12 2008
    send-lifetime 00:00:00 Jun 01 2008 23:59:59 Aug 12 2008
  key 1
    key-string 7 uaeqdyito
    accept-lifetime 00:00:00 Aug 12 2008 23:59:59 Dec 12 2008
    send-lifetime 00:00:00 Sep 12 2008 23:59:59 Nov 12 2008
  key 2
    key-string 7 eekgsdyd
    accept-lifetime 00:00:00 Nov 12 2008 23:59:59 Mar 12 2009
    send-lifetime 00:00:00 Dec 12 2008 23:59:59 Feb 12 2009
```

Where to Go Next

For information about routing features that use keychains, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0*

Default Settings

Table 17-1 lists the default settings for keychain management parameters.

Table 17-1 Default Keychain Management Parameters

Parameters	Default
Key chains	No keychain exists by default.
Keys	No keys are created by default when you create a new keychain.
Accept lifetime	Always valid.
Send lifetime	Always valid.
Key-string entry encryption	Unencrypted.

Additional References

For additional information related to implementing keychain management, see the following sections:

- Related Documents, page 17-11
- Standards, page 17-11

Related Documents

Related Topic	Document Title
Gateway Load Balancing Protocol	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0*
Border Gateway Protocol	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0*
Keychain management commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—