



## CHAPTER 14

# 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, page 14-1](#)
- [Licensing Requirements for Keychain Management, page 14-2](#)
- [Prerequisites for Keychain Management, page 14-3](#)
- [Guidelines and Limitations, page 14-3](#)
- [Configuring Keychain Management, page 14-3](#)
- [Where to Go Next, page 14-7](#)
- [Field Descriptions for Keychain Management, page 14-7](#)
- [Additional References, page 14-8](#)

## Information About Keychain Management

This section includes the following topics:

- [Keychains and Keychain Management, page 14-1](#)
- [Lifetime of a Key, page 14-2](#)

## 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 DCNM Unicast Routing Configuration Guide, Release 4.0*.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## 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
DCNM	Keychain management requires a LAN Enterprise license. For a complete explanation of the DCNM licensing scheme and how to obtain and apply licenses, see the <i>Cisco DCNM Licensing Guide</i> .
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 <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i> .

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

## Prerequisites for Keychain Management

Keychain management has no prerequisites.

## Guidelines and Limitations

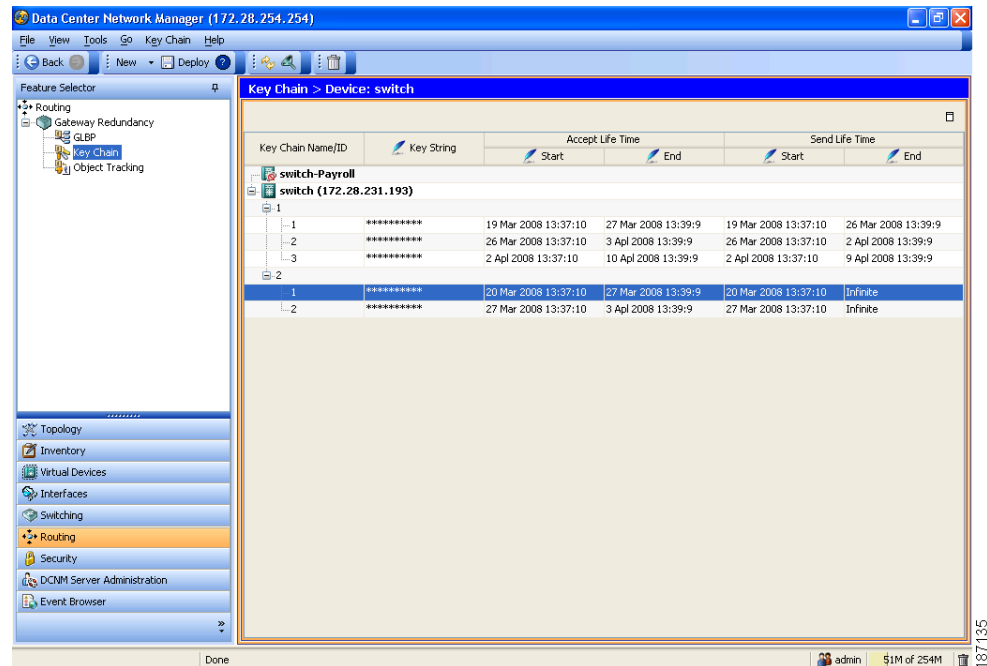
Keychain management has the following configuration guideline and limitation:

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

## Configuring Keychain Management

Figure 14-1 shows the Key Chain content pane.

**Figure 14-1** Key Chain Content Pane



This section includes the following topics:

- [Creating a Keychain, page 14-4](#)
- [Removing a Keychain, page 14-4](#)
- [Configuring a Key, page 14-5](#)
- [Configuring Text for a Key, page 14-5](#)
- [Configuring Accept and Send Lifetimes for a Key, page 14-6](#)

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## 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 14-5.

### DETAILED STEPS

To create a keychain, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Routing > Gateway Redundancy > Key Chain**.  
The available devices appear in the Summary pane.
  - Step 2** From the Summary pane, click the device that you want to configure with a keychain.
  - Step 3** From the menu bar, choose **Key Chain > Key Chain**.  
A new row appears in the Summary pane.
  - Step 4** Enter a name for the keychain. Valid keychain names are alphanumeric and can be up to 63 characters long.
  - Step 5** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## 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.

### DETAILED STEPS

To remove a keychain, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Routing > Gateway Redundancy > Key Chain**.  
The available devices appear in the Summary pane.
  - Step 2** From the Summary pane, double-click the device that has a keychain that you want to delete.  
Keychains on the device appear in the Summary table.
  - Step 3** Click the keychain you want to delete.
  - Step 4** From the menu bar, choose **Key Chain > Delete**.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

The keychain disappears from the Summary table.

**Step 5** From the menu bar, choose **File > Deploy** to apply your changes to the device.

---

## 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 14-5.

### BEFORE YOU BEGIN

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 14-6.

### DETAILED STEPS

To configure a key, follow these steps:

---

- Step 1** From the Feature Selector pane, choose **Routing > Gateway Redundancy > Key Chain**.  
The available devices appear in the Summary pane.
  - Step 2** From the Summary pane, double-click the device that you want to configure with a key.  
Keychains on the device appear in the Summary table.
  - Step 3** Double-click the keychain that you want to configure with a key.  
Keys in the keychain, if any, appear in the Summary table.
  - Step 4** (Optional) To create a new key, from the menu bar, choose **Key Chain > Key Chain Entry**.  
A new row appears below the keychain.
  - Step 5** Double-click the **Key Chain Name/ID** entry for the key that you want to configure. If you are creating a new key, the entry is blank.
  - Step 6** Enter an identifier for the key. The identifier must be a whole number between 0 and 65535.
  - Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## 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.

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).

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 14-6.

### DETAILED STEPS

To configure text for a key, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Routing > Gateway Redundancy > Key Chain**.  
The available devices appear in the Summary pane.
  - Step 2** From the Summary pane, double-click the device that has the key that you want to configure.  
Keychains on the device appear in the Summary table.
  - Step 3** Double-click the keychain that has the key that you want to configure.  
Keys in the keychain appear in the Summary table.
  - Step 4** Double-click the **Key String** entry for the key that you want to configure.  
The field becomes a drop-down list.
  - Step 5** Use the drop-down list to configure the text string, including whether the text string that you enter is unencrypted or encrypted. The text string can be up to 63 alphanumeric, case-sensitive characters. It also supports special characters.
  - Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## 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. For more information about accept and send lifetimes, see the [“Lifetime of a Key”](#) section on page 14-2.

### DETAILED STEPS

To configure text for a key, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Routing > Gateway Redundancy > Key Chain**.  
The available devices appear in the Summary pane.
  - Step 2** From the Summary pane, double-click the device that has the key that you want to configure.  
Keychains on the device appear in the Summary table.
  - Step 3** Double-click the keychain that has the key that you want to configure.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

Keys in the keychain appear in the Summary table.

- Step 4** Under Accept Life Time, double-click the **Start** entry for the key that you want to configure. The field becomes a drop-down list.
- Step 5** Use the drop-down list to configure the start date and time for the accept lifetime.
- Step 6** Under Accept Life Time, double-click the **End** entry. The field becomes a drop-down list.
- Step 7** Use the drop-down list to configure when the accept lifetime ends. You can specify the end of the accept lifetime as a specific date and time, as the duration in seconds of the lifetime, or as unending (infinite).
- Step 8** Under Send Life Time, double-click the **Start** entry for the key that you want to configure. The field becomes a drop-down list.
- Step 9** Use the drop-down list to configure the start date and time for the send lifetime.
- Step 10** Under Send Life Time, double-click the **End** entry. The field becomes a drop-down list.
- Step 11** Use the drop-down list to configure when the send lifetime ends. You can specify the end of the send lifetime as a specific date and time, as the duration in seconds of the lifetime, or as unending (infinite).
- Step 12** From the menu bar, choose **File > Deploy** to apply your changes to the device.

## Where to Go Next

For information about routing features that use keychains, see the *Cisco DCNM Unicast Routing Configuration Guide, Release 4.0*

## Field Descriptions for Keychain Management

This section includes the following topics:

- [Keychain Object, page 14-7](#)
- [Keychain Entry Object, page 14-8](#)
- [Related Fields, page 14-8](#)

### Keychain Object

**Table 14-1** Keychain Object

Field	Description
Key Chain Name/ID	Name assigned to the keychain. Valid names are 1 to 63 alphanumeric characters.

[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)

## Keychain Entry Object

Table 14-2 Keychain Entry Object

Field	Description
Key Chain Name/ID	Identification number assigned to the keychain. Valid identifier numbers are whole numbers from 0 to 65535.
Key String	Text string that is the shared secret of the key. Entries in this field are masked for security. Valid entries are alphanumeric, case-sensitive text strings, including special characters. The minimum length is one character; maximum length, 63 characters.
<b>Accept Life Time</b>	
Start	Date and time, in UTC, that the accept lifetime becomes active. If you specify no start date and time, the accept lifetime is always valid.
End	When the accept lifetime becomes inactive. You can specify the end of the accept lifetime in one of the following ways: <ul style="list-style-type: none"> <li>• Specific—The date and time when the accept lifetime becomes inactive.</li> <li>• Duration—The length in seconds of the accept lifetime. The maximum length is 2147483646 seconds (approximately 68 years).</li> <li>• Infinite—After the start time, the accept lifetime is always active.</li> </ul>
<b>Send Life Time</b>	
Start	Date and time, in UTC, that the send lifetime becomes active. If you specify no start date and time, the send lifetime is always active.
End	When the send lifetime becomes inactive. You can specify the end of the send lifetime in one of the following ways: <ul style="list-style-type: none"> <li>• Specific—The date and time when the send lifetime becomes inactive.</li> <li>• Duration—The length in seconds of the send lifetime. The maximum length is 2147483646 seconds (approximately 68 years).</li> <li>• Infinite—After the start time, the send lifetime is always active.</li> </ul>

## Related Fields

For information about fields that configure key chains, see the *Cisco DCNM Unicast Routing Configuration Guide, Release 4.0*.

## Additional References

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

- [Related Documents, page 14-9](#)
- [Standards, page 14-9](#)

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## Related Documents

Related Topic	Document Title
Gateway Load Balancing Protocol	<i>Cisco DCNM Unicast Routing Configuration Guide, Release 4.0</i>

## 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.	—

## ■ Additional References

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***