

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



## K Commands

---

This chapter describes the Cisco NX-OS security commands that begin with K.

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

## key

To create a key or to enter the configuration mode for an existing key, use the **key** command. To remove the key, use the **no key** form of this command.

**key** *key-ID*

**no key** *key-ID*

Syntax	Description
<i>key-ID</i>	ID of the key to configure. This ID must be a whole number between 0 and 65535.

Defaults	None
----------	------

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

Supported User Roles	network-admin vdc-admin
----------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	A new key contains no key strings. This command does not require a license.
------------------	--

Examples	This example shows how to enter key configuration mode for key 13 in the glbp-keys keychain:
----------	--

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)#
```

Related Commands	Command	Description
	<b>accept-lifetime</b>	Configures an accept lifetime for a key.
	<b>key chain</b>	Creates a keychain and enter keychain.
	<b>key-string</b>	Configures the shared secret (text) for a specific key.
	<b>send-lifetime</b>	Configures a send lifetime for a key.
	<b>show key chain</b>	Shows keychain configuration.

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

## key config-key

To configure the master key for type-6 encryption, use the **key config-key** command. To delete the master key and stop type-6 encryption, use the **no** form of this command.

**key config-key ascii** *new-master-key*

**no key config-key ascii**

Syntax Description	ascii	Specifies the ASCII format.
	<i>new-master-key</i>	The master key. The master key can be a minimum of 16 to a maximum of 32 alphanumeric characters.

Defaults	None
----------	------

Command Modes	Any command mode
---------------	------------------

SupportedUserRoles	network-admin vdc-admin
--------------------	----------------------------

Command History	Release	Modification
	5.2(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
------------------	--

Examples	This example shows how to configure the master key for type-6 encryption:
----------	---

```
switch# key config-key ascii
New Master Key:
Retype Master Key:
```

This example shows how to delete the master key and stop type-6 encryption:

```
switch# no key config-key ascii
Warning deletion of master-key will stop further type-6 encryption.
Do you want to proceed (y/n) [n]: [n] y

switch#
```

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

Related Commands	Command	Description
	<b>feature password encryption aes</b>	Enables the AES password encryption features.
	<b>show encryption service stat</b>	Displays the status of the encryption service.

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

## key-string

To configure the text for a key, use the **key-string** command. To remove the text, use the **no** form of this command.

**key-string** [*encryption-type*] *text-string*

**no key-string** *text-string*

Syntax Description	<i>encryption-type</i>	(Optional) Type of encryption to use. The <i>encryption-type</i> argument can be one of the following values:
		<ul style="list-style-type: none"> <li>0—The text-string argument that you enter is unencrypted text. This is the default.</li> <li>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 <b>show key chain</b> command that you ran on another Cisco NX-OS device.</li> </ul>
	<i>text-string</i>	Text of the key string, up to 63 case-sensitive, alphanumeric characters.

**Defaults** None

**Command Modes** Key configuration

**Supported User Roles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** The key-string text is a shared secret. The device stores key strings in a secure format. You can obtain encrypted key strings by using the **show key chain** command on another Cisco NX-OS device.

This command does not require a license.

**Examples** This example shows how to enter an encrypted shared secret for key 13:

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)# key-string 7 071a33595c1d0c1702170203163e3e21213c20361a021f11
switch(config-keychain-key)#
```

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

Related Commands	Command	Description
	<b>accept-lifetime</b>	Configures an accept lifetime for a key.
	<b>key</b>	Configures a key.
	<b>key chain</b>	Configures a keychain.
	<b>send-lifetime</b>	Configures a send lifetime for a key.
	<b>show key chain</b>	Shows keychain configuration.

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

## key chain

To create a keychain or to configure an existing keychain, use the **key chain** command. To remove the keychain, use the **no** form of this command.

**key chain** *keychain-name*

**no key chain** *keychain-name*

Syntax Description	<i>keychain-name</i>	Name of the keychain, up to 63 alphanumeric, case-sensitive characters in length.
--------------------	----------------------	---

Defaults	None
----------	------

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

SupportedUserRoles	network-admin vdc-admin
--------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	<p>This command creates the keychain if it does not already exist. A new keychain contains no keys. Removing a keychain also removes any keys that the keychain contains.</p> <p>Before you remove 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.</p> <p>This command does not require a license.</p>
------------------	--

Examples	This example shows how to configure a keychain named glbp-keys:
----------	---

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)#
```

Related Commands	Command	Description
	<b>accept-lifetime</b>	Configures an accept lifetime for a key.
	<b>key</b>	Configures a key.
	<b>key-string</b>	Configures a key string.

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

<b>Command</b>	<b>Description</b>
<b>send-lifetime</b>	Configures a send lifetime for a key.
<b>show key chain</b>	Configures a send lifetime for a key.