Configuring Password Encryption

This chapter describes how to configure password encryption on Cisco NX-OS devices.

This chapter includes the following sections:

About AES Password Encryption and Primary Encryption Keys

You can enable strong, reversible 128-bit Advanced Encryption Standard (AES) password encryption, also known as Type-6 encryption. To start using Type-6 encryption, you must enable the AES password encryption feature and configure a primary encryption key, which is used to encrypt and decrypt passwords.

After you enable AES password encryption and configure a primary key, all existing and newly created clear-text passwords for supported applications (currently RADIUS and TACACS+) are stored in Type-6 encrypted format, unless you disable Type-6 password encryption. You can also configure Cisco NX-OS to convert all existing weakly encrypted passwords to Type-6 encrypted passwords.

Related Topics

Configuring a Primary Key and Enabling the AES Password Encryption Feature, on page 3
Configuring Global RADIUS Keys
Configuring a Key for a Specific RADIUS Server
Configuring Global TACACS+ Keys
Configuring a Key for a Specific TACACS+ Server
Configuring a Primary Key and Enabling the AES Password Encryption Feature, on page 3

Guidelines and Limitations for Password Encryption

Password encryption has the following configuration guidelines and limitations:

- Only users with administrator privilege (network-admin) can configure the AES password encryption feature, associated encryption and decryption commands, and primary keys.

- RADIUS and TACACS+ are the only applications that can use the AES password encryption feature.
- Configurations containing Type-6 encrypted passwords are not rollback-compliant.
- You can enable the AES password encryption feature without a primary key, however the encryption starts only when a primary key is present in the system.
- For TACACS+, after you enable the AES password encryption feature and configure a primary key, you must run the **encryption re-encrypt obfuscated** command to convert the passwords to Type-6 encrypted passwords.
- Deleting the primary key stops Type-6 encryption and causes all existing Type-6 encrypted passwords to become unusable, unless the same primary key is reconfigured.
- To move the device configuration to another device, either decrypt the configuration before porting it to the other device or configure the same primary key on the device to which the configuration will be applied.
- Type-6 encryption is supported only for MACsec keychain. It is not supported for legacy RPM or cloudsec keys.
- Starting from Cisco NX-OS Release 9.3(6), converting Type-6 encrypted passwords back to original state is not supported on MACsec keychain.
- Type-6 encryption can be configured only when the AES password encryption feature is enabled and the primary key is configured.
- When the primary key is configured and the AES password encryption feature is enabled on a switch, each MACsec key string configurations under the keychain infra are automatically encrypted with the Type-6 encryption.
- Primary key configuration is local to the switch. If you take the Type-6 configured running data from one switch and apply it on another switch where a different primary key is configured, then decryption on the new switch fails.
- If you erase the startup configuration and use the configuration replace feature after a Type-6 encryption, the configuration replace fails because the primary key is not stored in PSS. Therefore, there is configuration loss for MACsec Type-6 encrypted key string.
- When you configure the Type-6 keys, you cannot modify the existing Type-6 encrypted key strings to Type-7 encrypted key string without applying the decrypt command provided by SKSD.
- If you downgrade the system by cold reboot with an old image where the Type-6 encryption is not supported, you must take out the configuration before you proceed with the cold reboot. Failing to do so leads to loss in configuration.
- After you downgrade the system, the Type-6 configuration is lost.
- If you downgrade the system by ISSD, capability conf check is invoked and it notifies you to remove the configuration before proceeding with the downgrade. You can use the **encryption decrypt** command to convert the Type-6 encrypted keys to Type-7 encryption keys, and then proceed with the downgrade.
- During an ISSU upgrade, if you migrate from an older image which includes the Type-7 encrypted keys to a new image that supports Type-6 encryption, the rpm does not convert the existing keys to Type-6 encrypted keys until re-encryption is enforced. To enforce a re-encryption, use the **encryption re-encrypt obfuscated** command.

- If you change the primary key after a Type-6 encryption, the decrypt command fails on the existing Type-6 encrypted key-string. You must delete the existing Type-6 key string and configure a new key string.
- During upgrade, while performing device reload, if ASCII replay is triggered without binary restore, primary key gets lost. The primary key must be reconfigured after device reload. Use the **key config-key ascii** command to reconfigure the primary key and avoid encryption issues. However, upgrade with binary restore retains the primary key after the reboot.
- During downgrade, where both source and target images support Type-6 encryption, while performing device reload, if ASCII replay is triggered without binary restore, primary key gets lost. The primary key must be reconfigured after device reload. Use the **key config-key ascii** command to reconfigure the primary key and avoid encryption issues. However, downgrade with binary restore retains the primary key after the reboot, provided both source and target images support Type-6 encryption.

  If you downgrade the system from an image that supports Type-6 encryption to an image that does not support Type-6 encryption, compatibility check fails.

Default Settings for Password Encryption

This table lists the default settings for password encryption parameters.

Table 1: Default Password Encryption Parameter Settings

Parameters	Default
AES password encryption feature	Disabled
Primary key	Not configured

Configuring Password Encryption

This section describes the tasks for configuring password encryption on Cisco NX-OS devices.

Configuring a Primary Key and Enabling the AES Password Encryption Feature

You can configure a primary key for Type-6 encryption and enable the Advanced Encryption Standard (AES) password encryption feature.

Procedure

	Command or Action	Purpose
Step 1	[**no**] **key config-key ascii**[<new_key> old <old_master_key>] **Example:**	Configures a primary key (`Master Key`) to be used with the AES password encryption feature. The primary key can contain between 16 and 32 alphanumeric characters. You can use the

	Command or Action	Purpose

	`switch# key config-key ascii`
	`New Master Key:`
	`Retype Master Key:`
		no form of this command to delete the primary key at any time.
		If you enable the AES password encryption feature before configuring a primary key, a message appears stating that password encryption will not take place unless a primary key is configured. If a primary key is already configured, you are prompted to enter the current primary key before entering a new primary key.
		Note
		Starting with Cisco NX-OS Release 10.3(2)F, you can configure primary key using DME payload and non-interactive mode.

Step 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	[**no**] **feature password encryption aes** **Example:** `switch(config)# feature password encryption aes`	Enables or disables the AES password encryption feature.
Step 4	**encryption re-encrypt obfuscated** **Example:** `switch(config)# encryption re-encrypt obfuscated`	Converts existing plain or weakly encrypted passwords to Type-6 encrypted passwords.
Step 5	(Optional) **show encryption service stat** **Example:** `switch(config)# show encryption service stat`	Displays the configuration status of the AES password encryption feature and the primary key.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration. **Note** This command is necessary to synchronize the primary key in the running configuration and the startup configuration.

Related Topics

About AES Password Encryption and Primary Encryption Keys, on page 1
About AES Password Encryption and Primary Encryption Keys, on page 1
Configuring Text for a Key

Configuring Accept and Send Lifetimes for a Key

Converting Existing Passwords to Type-6 Encrypted Passwords

You can convert existing plain or weakly encrypted passwords to Type-6 encrypted passwords.

Before you begin

Ensure that you have enabled the AES password encryption feature and configured a primary key.

Procedure

	Command or Action	Purpose
Step 1	**encryption re-encrypt obfuscated** **Example:** `switch# encryption re-encrypt obfuscated`	Converts existing plain or weakly encrypted passwords to Type-6 encrypted passwords.

Converting Type-6 Encrypted Passwords Back to Their Original States

You can convert Type-6 encrypted passwords back to their original states. This functionality is not supported for macsec keychain.

Before you begin

Ensure that you have configured a primary key.

Procedure

	Command or Action	Purpose

Step 1	**encryption decrypt type6**
	Example:
	`switch# encryption decrypt type6`
	`Please enter current Master Key:`
		Converts Type-6 encrypted passwords back to their original states.

Enabling Type-6 Encryption on MACsec Keys

The type-6 encryption feature, also known as the Advanced Encryption Standard (AES) password encryption feature allows you to securely store MACsec keys in a type-6 encrypted format.

Beginning with Cisco NX-OS Release 9.3(5), you can store MACsec keys in a type-6 encrypted format on all Cisco Nexus 9000 Series switches which support the MACsec feature.

Procedure

	Command or Action	Purpose

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

Step 2	[**no**] **key config-key ascii**
	Example:
	`switch(config)# key config-key ascii`
	`switch(config)# New Master Key:`
	`Switch(config)# Retype Master Key:`
		Configures the primary key (`Master Key`).

Step 3	[**no**] **feature password encryption aes** **Example:** `switch(config)# feature password encryption aes`	Enables or disables the AES password encryption feature.

Step 4	**key chain** *name* **macsec**
	Example:
	`switch(config)# key chain 1 macsec`
	`switch(config-macseckeychain)#`
		Creates a MACsec keychain to hold a set of MACsec keys and enters MACsec keychain configuration mode.

Step 5	**key** *key-id*
	Example:
	`switch(config-macseckeychain)# key 1000`
	`switch(config-macseckeychain-macseckey)#`
		Creates a MACsec key and enters MACsec key configuration mode. The range is 1–32 octets, and the maximum size is 32 or 64 bits. AES_128 is used for 32 bit, while AES_256 is used for 64 bits.

Step 6	**key-octet-string** *octet-string* **cryptographic-algorithm** {**AES_128_CMAC** | **AES_256_CMAC**} **Example:** `switch(config-macseckeychain-macseckey)# key-octet-string abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789 cryptographic-algorithm AES_256_CMAC`	Configures the octet string for the key. The *octet-string* argument can contain up to 64 hexadecimal characters. The octet key is encoded internally, so the key in clear text does not appear in the output of the **show running-config macsec** command. The key octet string includes the following: • 0 Encryption Type - No encryption (default) • 6 Encryption Type - Proprietary (Type-6 encrypted) • 7 Encryption Type - Proprietary WORD key octet string with maximum 64 characters

Deleting Type-6 Encrypted Passwords

You can delete all Type-6 encrypted passwords from the Cisco NX-OS device.

Procedure

	Command or Action	Purpose
Step 1	**encryption delete type6** **Example:** `switch# encryption delete type6`	Deletes all Type-6 encrypted passwords.

Verifying the Password Encryption Configuration

To display password encryption configuration information, perform the following task:

Command	Purpose
show encryption service status	Displays the configuration status of the AES password encryption feature and the primary key.

Configuration Examples for Password Encryption

The following example shows how to create a primary key, enable the AES password encryption feature, and configure a Type-6 encrypted password for a TACACS+ application:

```
key config-key ascii
  New Master Key:
  Retype Master Key:
configure terminal
feature password encryption aes
show encryption service stat
  Encryption service is enabled.
  Master Encryption Key is configured.
  Type-6 encryption is being used.
feature tacacs+
tacacs-server key Cisco123
show running-config tacacs+
  feature tacacs+
  logging level tacacs 5
  tacacs-server key 6
"JDYkqyIFWeBvzpljSfWmRZrmRSRE8syxKlOSjP9RCCkFinZbJI3GD5c6rckJR/Qju2PKLmOewbheAA=="
```