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.

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, but encryption starts only when a primary key is present in the system.
- 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.

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 pimary 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**
	Example:
	`switch# key config-key ascii`
	`New Master Key:`
	`Retype Master Key:`
		Configures a primary 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 **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.

Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 3	[**no**] **feature password encryption aes** **Example:** `switch(config)# feature password encryption aes`	Enables or disables the AES password encryption feature.
Step 4	(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 5	Required: **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.

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.

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.

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 stat	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=="
```