



Configuring Password Encryption

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

This chapter includes the following sections:

- [AES password encryption and primary encryption keys, on page 1](#)
- [Licensing Requirements for Password Encryption, on page 1](#)
- [Guidelines and Limitations for Password Encryption, on page 2](#)
- [Password encryption default settings, on page 2](#)
- [Configuring Password Encryption, on page 2](#)
- [Password encryption configuration verification, on page 5](#)
- [Configuration examples for password encryption, on page 5](#)

AES password encryption and primary encryption keys

AES password encryption also known as Type-6 encryption is a password security feature that

- uses 128-bit Advanced Encryption Standard to encrypt passwords,
- allows for reversible encryption via a primary encryption key, and
- supports storing passwords for applications (such as RADIUS and TACACS+) in encrypted format.

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.

Licensing Requirements for Password Encryption

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	Password encryption requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For an explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> .

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 master key, but 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.

Password encryption default settings

This table lists the default settings for password encryption parameters.

Table 1: Password encryption parameters default settings

Parameters	Default
Advanced Encryption Standard (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.

Configure a primary key and enabling the AES password encryption feature

Secure device authentication by using AES password encryption (Type-6).

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

Follow these steps to configure a primary key and enable the AES password encryption feature:

Procedure

- Step 1** Configures a primary key (`Master Key`) to be used with the AES password encryption feature using the [**no**] **key config-key ascii** [`<new_key>` `old` `<old_master_key>`] command.

Example:

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

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.

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** Enter the global configuration mode. **configure terminal**

Example:

```
switch# configure terminal
switch(config)#
```

- Step 3** Enable or disable the AES password encryption feature using the [**no**] **feature password encryption aes** command.

Example:

```
switch(config)# feature password encryption aes
.
```

- Step 4** Convert existing plain or weakly encrypted passwords to Type-6 encrypted passwords using the **encryption re-encrypt obfuscated** command.

Example:

```
switch(config)# encryption re-encrypt obfuscated
```

- Step 5** (Optional) Display the configuration status of the AES password encryption feature and the primary key using the **show encryption service stat** command.

Example:

```
switch(config)# show encryption service stat
```

Step 6 Copy the running configuration to the startup configuration using the **copy running-config startup-config** command.

Example:

```
switch(config)# copy running-config startup-config
```

Note

This command is necessary to synchronize the primary key in the running configuration and the startup configuration.

What to do next

-

Convert 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

Convert existing plain or weakly encrypted passwords to Type-6 encrypted passwords using the **encryption re-encrypt obfuscated** command.

Example:

```
switch# encryption re-encrypt obfuscated
```

Recover Original Passwords from Type-6 Encrypted Values

You can convert encrypted passwords to cleartext to carry out migration or troubleshooting.

You can convert Type-6 encrypted passwords back to their original states.

Before you begin

Ensure that you have configured a primary key.

Procedure

Use the **encryption decrypt type6** command to recover original passwords..

Example:

```
switch# encryption decrypt type6
Please enter current Master Key:
```

The console displays the original (cleartext) passwords after the system decrypts them.

What to do next

Verify that all required passwords have been decrypted. If you do not need cleartext outputs in your logs, remove them.

Deleting Type-6 Encrypted Passwords

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

Procedure

Delete all Type-6 encrypted passwords using the **encryption delete type6** command.

Example:

```
switch# encryption delete type6
```

Password encryption configuration verification

Use these commands to display password encryption configuration information.

Table 2: Password encryption configuration verification commands

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

Examples for password encryption

This example demonstrates how to create a primary key, enable the AES password encryption feature, and configure a Type-6 encrypted password for an application that uses TACACS+.

```
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=="
```