



Configuring Password Encryption

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

This chapter includes the following sections:

- [Finding Feature Information, on page 1](#)
- [Information About Password Encryption, on page 1](#)
- [Licensing Requirements for Password Encryption, on page 2](#)
- [Guidelines and Limitations for Password Encryption, on page 2](#)
- [Default Settings for Password Encryption, on page 3](#)
- [Configuring Password Encryption, on page 3](#)
- [Verifying the Password Encryption Configuration, on page 5](#)
- [Configuration Examples for Password Encryption, on page 6](#)
- [Additional References for Password Encryption, on page 6](#)
- [Feature History for Password Encryption, on page 7](#)

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at <https://tools.cisco.com/bugsearch/> and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information" chapter or the Feature History table in this chapter.

Information About Password Encryption

This section includes information about password encryption on Cisco NX-OS devices.

AES Password Encryption and Master 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 master encryption key, which is used to encrypt and decrypt passwords.

After you enable AES password encryption and configure a master 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 Master Key and Enabling the AES Password Encryption Feature](#)
- [Configuring Global RADIUS Keys](#)
- [Configuring a Key for a Specific RADIUS Server](#)
- [Configuring Global TACACS+ Keys](#)
- [Configuring a Key for a Specific TACACS+ Server](#)

Virtualization Support for Password Encryption

The master key used with the AES password encryption feature is unique for each VDC.



Note For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Licensing Requirements for Password Encryption

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	<p>Password encryption 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.</p> <p>For an explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i>.</p>

Guidelines and Limitations for Password Encryption

Password encryption has the following configuration guidelines and limitations:

- Only users with administrator privilege (network-admin or vdc-admin) can configure the AES password encryption feature, associated encryption and decryption commands, and master 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 master key is present in the system.
- Deleting the master key stops type-6 encryption and causes all existing type-6 encrypted passwords to become unusable, unless the same master key is reconfigured.
- Before you downgrade from Cisco NX-OS Release 5.2 to an earlier release, decrypt all type-6 passwords, disable the AES password encryption feature, and delete the master key.

- To move the device configuration to another device, either decrypt the configuration before porting it to the other device or configure the same master 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
Master key	Not configured

Configuring Password Encryption

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



Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Configuring a Master Key and Enabling the AES Password Encryption Feature

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

SUMMARY STEPS

1. `[no] key config-key ascii`
2. `configure terminal`
3. `[no] feature password encryption aes`
4. (Optional) `show encryption service stat`
5. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>[no] key config-key ascii</code> Example: <pre>switch# key config-key ascii New Master Key: Retype Master Key:</pre>	<p>Configures a master key to be used with the AES password encryption feature. The master key can contain between 16 and 32 alphanumeric characters. You can use the no form of this command to delete the master key at any time.</p> <p>If you enable the AES password encryption feature before configuring a master key, a message appears stating that</p>

	Command or Action	Purpose
		password encryption will not take place unless a master key is configured. If a master key is already configured, you are prompted to enter the current master key before entering a new master key.
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	(Optional) show encryption service stat Example: switch(config)# show encryption service stat	Displays the configuration status of the AES password encryption feature and the master 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 master key in the running configuration and the startup configuration.

Related Topics[Configuring Text for a Key](#)[Configuring Accept and Send Lifetimes for a Key](#)[AES Password Encryption and Master Encryption Keys](#)

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 master key.

SUMMARY STEPS

1. encryption re-encrypt obfuscated

DETAILED STEPS

	Command or Action	Purpose
Step 1	encryption re-encrypt obfuscated Example:	Converts existing plain or weakly encrypted passwords to type-6 encrypted passwords.

	Command or Action	Purpose
	switch# encryption re-encrypt obfuscated	

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 master key.

SUMMARY STEPS

1. encryption decrypt type6

DETAILED STEPS

	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.

SUMMARY STEPS

1. encryption delete type6

DETAILED STEPS

	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
<code>show encryption service stat</code>	Displays the configuration status of the AES password encryption feature and the master key.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Examples for Password Encryption

The following example shows how to create a master 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=="
```

Additional References for Password Encryption

This section includes additional information related to implementing password encryption.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	<i>Cisco NX-OS Licensing Guide</i>
Command reference	<i>Cisco Nexus 7000 Series NX-OS Security Command Reference</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.	—

Feature History for Password Encryption

This table lists the release history for this feature.

Table 2: Feature History for Password Encryption

Feature Name	Releases	Feature Information
Password encryption	5.2(1)	This feature was introduced.

