

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
- Guidelines and limitations for password encryption, on page 2
- Password encryption default settings, on page 4
- Configuring password encryption, on page 4
- Password encryption configuration verification, on page 8
- Configuration examples for password encryption, on page 9

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.

Related Topics

Configure a primary key and enable the AES password encryption feature, on page 4
Configure global RADIUS keys
Configure a key for a specific RADIUS server
Configure global TACACS+ keys
Configure a key for a specific TACACS+ server
Configure a primary key and enable the AES password encryption feature, on page 4

Guidelines and limitations for password encryption

Use this reference to review the guidelines and limitations for password encryption.

Password encryption has the following configuration guidelines and limitations:

Configuration and application support guidelines

- Only users with administrator privilege (network-admin) can configure the AES password encryption feature, associated encryption and decryption commands, and primary keys.
- Beginning with Cisco NX-OS Release 10.3(3)F, RPM keychain infra supports AES password encryption for RPM legacy keychains on Cisco Nexus 9000 Series platform switches.
- 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.
- For TACACS+ and RPM legacy keychain, 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 keychain limitations

- Type-6 encryption is supported only for MACsec and RPM legacy keychain. It is not supported for 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.
- Starting from Cisco NX-OS Release 10.3(3)F, converting Type-6 encrypted passwords back to original state is not supported for RPM legacy 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 configuration under the keychain infra is automatically encrypted with 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.
- For RPM legacy keychains, Type-6 key-strings can be configured without AES password encryption feature enabled and primary key configured, but these Type-6 key-strings are unusable until AES password encryption feature is enabled and the primary key with which the Type-6 key-strings were generated is configured.

Upgrade, downgrade, and primary key limitations

- 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.
- After ISSU upgrade from an older image which includes the Type-7 encrypted keys to a new image that supports Type-6 encryption, if configuration replace is done using the configuration file saved in older image or configuration file saved after upgrade without re-encrypting the password to Type-6 by using the **encryption re-encrypt obfuscated** command, the configuration replace will fail.
- 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.
- Starting from Cisco NX-OS Release 10.3(2)F, you can configure primary key using DME payload and non-interactive mode.
- 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.

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 enable 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.

Beginning with Cisco NX-OS Release 10.3(3)F, Type-6 encryption is supported for RPM legacy keychain.

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:

{"actionLSubj": {"attributes": {"dn": "sys/action/lsubj-[sys/passwdenc]"}
"children": [{"smartcardPasswdEncryptMasterKeyConfigLTask": {"attributes": {"adminSt":
"start",
"dn": "sys/action/lsubj-[sys/passwdenc]/smartcardPasswdEncryptMasterKeyConfigLTask",
"key": "ciscociscociscocisco",
"oldKey": "test1test1test1test1",
"delete": "no",
"freq": "one-shot"}}}]}}
```

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#show encryption service stat
```

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

Example:

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

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

Related Topics

AES password encryption and primary encryption keys, on page 1
AES password encryption and primary encryption keys, on page 1
Configure text for a key
Configure accept and send lifetimes for a key

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. This functionality is not supported for macsec keychain.

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.

Enable 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

Step 1 [**no**] **key config-key ascii**

Example:

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

Configures the primary key (`Master Key`).

Step 2 **configure terminal**

Example:

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

Enters global configuration mode.

Step 3 [**no**] **feature password encryption aes tam**

Example:

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

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

Delete 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.
show encryption mkey info [**all** | **hash-prefix** | **last-updated** | **length** | **protection-type**]	Displays the details of a primary key. • **all** : Displays all details of Type-6 primary key. • **hash-prefix** : Displays the first 16 characters of the stored Type-6 primary key's hash. • **last-updated** :Displays the time when the Type-6 primary key was last modified in YYYY-MM-DD HH:MM:SS.SSS format (for example, 2023-07-06 17:30:21.123). • **length** : Displays the length of user provided Type-6 primary key. • **protection-type** : Displays the protection type of stored Type-6 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 tam
show encryption service status
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=="
```

Configuration examples for "show encryption mkey info" command

This example shows the output of various options of the **show encryption mkey info [all | hash-prefix | last-updated | length | protection-type]** command:

- **all**

```
switch#show encryption mkey info all
Master-Key ID : 1
-------------------------------- ----------------------------------------------------
Type          :       Running (Active)
Key-Hash(first 16 chars)    :       SHA512: TNESx8lzL5C1fRpb
Protection-Type             :       Hardware
Length        :       20
Last updated  :       2024-11-03 16:35:26.074 IST
-------------------------------- ----------------------------------------------------
```

- **hash-prefix** : The key-Hash is the first 16 characters of the base64 encoding of the SHA-512 digest of the primary key.

```
switch#show encryption mkey info hash-prefix
Master-Key ID : 1
-------------------------------- ----------------------------------------------------
Key-Hash(first 16 chars)    :       SHA512: TNESx8lzL5C1fRpb
-------------------------------- ----------------------------------------------------
```

- **last-updated** : The Last updated attribute provides the timestamp of the last modification.

```
switch#show encryption mkey info last-updated
Master-Key ID : 1
-------------------------------- ----------------------------------------------------
Last updated  :       2024-11-03 16:35:26.074 IST
-------------------------------- ----------------------------------------------------
```

- **length** : The Length shows the length of the configured primary key.

```
switch#show encryption mkey info length
Master-Key ID : 1
```

```
-------------------------------- ------------------------------------------------
Length        :       23
-------------------------------- ------------------------------------------------
```

- **protection-type** : The protection-type indicates how the primary key is secured. The primary key is protected either by Hardware (which uses TAM encryption service) or Software (which uses internal hashing).

  Protection type - Hardware

```
switch(config)#feature password encryption aes tam
switch#show encryption mkey info all
Master-Key ID : 1
-------------------------------- ------------------------------------------------
Type          :       Running (Active)
Key-Hash(first 16 chars)    :       SHA512: TNESx8lzL5C1fRpb
Protection-Type             :       Hardware
Length        :       20
Last updated  :       2024-11-03 16:35:26.074 IST
-------------------------------- ------------------------------------------------
```

  Protection type - Software

```
switch#key config ascii <master-key> <retype master-key>
switch#show encryption mkey info all
Master-Key ID : 1
-------------------------------- ------------------------------------------------
Type          :       Running (Active)
Key-Hash(first 16 chars)    :       SHA512: TNESx8lzL5C1fRpb
Protection-Type             :       Software
Length        :       20
Last updated  :       2024-11-03 16:35:26.074 IST
-------------------------------- ------------------------------------------------
```

All attributes except Type and Protection-Type remain unchanged for a primary key. The use cases in this section describe how Type and Protection-Type fields change when you perform operations such as 'copy run start,' 'no key config ascii,' 'write erase,' or changing the primary key.

Case-1

When the primary key is configured for the first time, the primary key is currently “Active” and can be used for Type-6 encryption service.

```
switch#key config ascii <master-key> <retype master-key>
switch#show encryption mkey info all
Master-Key ID : 1
-------------------------------- ------------------------------------------------
Type          :       Running (Active)
Key-Hash(first 16 chars)    :       SHA512: TNESx8lzL5C1fRpb
Protection-Type             :       Software
Length        :       20
Last updated  :       2024-11-03 16:35:26.074 IST
-------------------------------- ------------------------------------------------
```

Note The configuration won’t be there post device-reload, as it is not saved to startup config (using copy run start).

Case-2

When the primary key is encrypted using the Type-6 encryption command, the Protection-type changes to Hardware, indicating that the stored-master-key has been encrypted using the Trust Anchor Module (TAM) provided encryption algorithm.

```
switch(config)#feature password encryption aes tam
switch#show encryption mkey info all
Master-Key ID : 1
-------------------------------- ----------------------------------------------------
Type          :       Running (Active)
Key-Hash(first 16 chars)    :       SHA512: TNESx8lzL5C1fRpb
Protection-Type             :       Hardware
Length        :       20
Last updated  :       2024-11-03 16:35:26.074 IST
-------------------------------- ----------------------------------------------------
```

Case-3

When the primary key is modified, the following two scenarios are observed:

1. If an active “Running” primary key exists, it will be replaced with a newly configured primary key of the same type.

   ```
   switch#key config ascii <current master-key> <new master-key> <retype new master-key>
   switch#show encryption mkey info all
   Master-Key ID : 1
   -------------------------------- ----------------------------------------------------
   Type          :       Running (Active)
   Key-Hash(first 16 chars)    :       SHA512: PWEQJonK0xzt21NJ
   Protection-Type             :       Hardware
   Length        :       26
   Last updated  :       2024-11-05 05:33:37.626IST
   -------------------------------- ----------------------------------------------------
   ```

2. When there is an active “Running & Startup” primary key, the existing primary key is replaced with a new configured primary key. The show command displays the following two separate primary keys:

   - One for the old primary key which is set to a new type as “Startup” and is marked as “Inactive” as this primary key can be used only after the next device-reload.
   - Other for newly configured primary key, which is of type “Running” and is currently active and can be used for new session (until device-reload).

   ```
   switch#show encryption mkey info all
   Master-key ID : 1
   -------------------------------- ----------------------------------------------------
         Type          :       Startup (Inactive)
   Key-Hash(first 16 chars)    :       SHA512: TNESx8lzL5C1fRpb
   Protection-Type             :       Hardware
   Length        :       20
   Last updated  :       2024-11-03 16:35:26.074 IST
   -------------------------------- ----------------------------------------------------

   Master-Key ID : 2
   -------------------------------- ----------------------------------------------------
   Type          :       Running (Active)
   Key-Hash(first 16 chars)    :       SHA512: PWEQJonK0xzt21NJ
   Protection-Type             :       Hardware
   Length        :       26
   Last updated  :       2024-11-05 05:33:37.626IST
   -------------------------------- ----------------------------------------------------
   ```

Case-4

When you copy the running configuration to startup configuration, the primary key configured in running-config is stored in startup-config. Its type changes to “Running & Startup,” indicating the key is active and can be used for Type-6 encryption service.

```
switch# copy r s
switch#show encryption mkey info all
Master-key ID : 1
------------------------------- ------------------------------------------------
Type          :Running & Startup (Active)
Key-Hash(first 16 chars)    :       SHA512: TNESx8lzL5C1fRpb
Protection-Type             :       Hardware
Length        :       20
Last updated  :       2024-11-03 16:35:26.074 IST
------------------------------- ------------------------------------------------
```



Note

- The configuration is there post device-reload, as it is saved to startup config (using copy run start).
- If copy run start is not performed before device-reload, there may be loss of primary key or if there was an existing primary key in startup-config, the last stored state of that primary key is retained post-reload.

Case-5

- When the primary key is removed from running-config, the following two scenarios are observed:

1. If only the “Running” primary key is present, removing the configured primary key from running-config deletes its entry, leaving the show command output empty.

   ```
   switch#no key config ascii
       switch#show encryption mkey info all
       switch#
   ```

2. When the “Running & Startup” primary key is there, the type after execution of the **no key config ascii** command will change to “Startup,” which means that the primary key is removed from running-config but it is still there in startup-config. This “Startup” primary key would not be active in this session though and it could be used only post device-reload. Also, a warning message is generated stating there is no active Type-6 primary key in the system now.

   ```
   switch#no key config ascii
   switch#show encryption mkey info all
   Master-key ID : 1
   ------------------------------- ------------------------------------------------
   Type          :Startup (Inactive)
   Key-Hash(first 16 chars)    :       SHA512: TNESx8lzL5C1fRpb
   Protection-Type             :       Hardware
   Length        :       20
   Last updated  :       2024-11-03 16:35:26.074 IST
   ------------------------------- ------------------------------------------------

   Warning: There is no “Running” master-key in the system as it may have been removed
    from running-config.
   ```