Password Management

This table describes the developments of this feature, by release.

Table 1: Feature History

Feature Name	Release Information	Description
Hardened passwords	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature enables password policy rules in Cisco SD-WAN Manager. After password policy rules are enabled, Cisco SD-WAN Manager enforces the use of strong passwords.
	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature lets you configure Cisco SD-WAN Manager to enforce predefined-medium security or high-security password criteria.
Type 6 Passwords on Cisco IOS XE SD-WAN Routers	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature allows you to use type 6 passwords that use secure reversible encryption. This encryption provides enhanced security by using more secure algorithms to encrypt your passwords. These passwords are supported for the templates detailed in Supported platforms and templates, on page 5.

Hardened passwords

Restrictions for passwords

Password attempts and password change

You are allowed five consecutive password attempts before your account is locked. After six failed password attempts, you are locked out for 15 minutes. If you enter an incorrect password on the seventh attempt, you are not allowed to log in, and the 15-minute lock timer starts again.

If your account is locked, wait for 15 minutes for the account to automatically be unlocked. Alternatively, reach out to an administrator to reset the password, or have an administrator unlock your account.

Note Your account gets locked even if password is not entered multiple times. When you do not enter anything in the password field, it is considered as invalid or wrong password.

Password change policy

When resetting your password, you must set a new password. You cannot reset a password using an old password.

In Cisco vManage Release 20.6.4, Cisco vManage Release 20.9.1 and later releases, a user that is logged out, or a user whose password has been changed locally or on the remote TACACS server cannot log in using their old password. The user can log in only using their new password.

Password requirements

SD-WAN Manager enforces these password requirements after you have enabled the password policy rules.

The following password requirements are applicable to releases before Cisco vManage Release 20.9.1:

- Must contain a minimum of eight characters and a maximum of 32 characters.
- Must contain at least one uppercase character.
- Must contain at least one lowercase character.
- Must contain at least one numeric character.
- Must contain at least one of the following special characters: # ? ! @ $ % ^ & * -.
- Must not contain the full name or username of the user.
- Must not reuse a previously used password.
- Change at least four characters so their positions differ from those in your old password.

From Cisco IOS XE Catalyst SD-WAN Release 17.9.1a:

Table 2: Password criteria and requirements

Password criteria	Requirements
Medium security	• Must contain a minimum of eight characters • Must contain no more than 32 characters • Must contain at least one lowercase character • Must contain at least one uppercase character • Must contain at least one numeric character • Must contain at least one of the following special characters: # ? ! @ $ % ^ & * - • Must not be identical to any of the last five passwords used • Must not contain the full name or username of the user
High security	• Must contain a minimum of 15 characters • Must contain no more than 32 characters • Must contain at least one lowercase character • Must contain at least one uppercase character • Must contain at least one numeric character • Must contain at least one of the following special characters: # ? ! @ $ % ^ & * - • Must not be identical to any of the last five passwords used • Must not contain the full name or username of the user • Change at least eight characters so their positions differ from those in your old password

Enable Password Policy

Enable password policy rules in Cisco SD-WAN Manager to enforce use of strong passwords.

After you enable a password policy rule, the passwords that are created for new users must meet the requirements defined by the rule. From Cisco vManage Release 20.9.1, you are prompted to change your password the next time you log in if your existing password does not meet the requirements defined by the rule.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Click **Password Policy**.

Step 3 Perform one of these actions, based on your SD-WAN Manager release:

a) For releases before Cisco vManage Release 20.9.1, click **Enabled**.

b) From Cisco vManage Release 20.9.1, click **Medium Security** or **High Security** to choose the password criteria.

By default, **Password Policy** is set to **Disabled**.

Step 4 Click **Save**.

Reset a locked user using SD-WAN Manager

If a user is locked out after multiple incorrect password attempts, an administrator with the necessary rights can update the user's password. You can unlock the user account by either changing the password or by getting the user account unlocked.

Note Only a netadmin user or a user with the User Management Write role can perform this operation.

Use these steps to reset a locked user.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**).

Step 2 Choose the user account you want to unlock.

Step 3 Click **. . .** and choose **Reset Locked User**.

Step 4 Click **OK** to confirm that you want to reset the password of the locked user. This operation cannot be undone.

Alternatively, click **Cancel** to cancel the operation.

Reset a locked user using CLI commands

Use this procedure to reset a locked user by changing the password using CLI commands.

Procedure

Step 1 Log in to the device as an admin user.

Step 2 Run the following command:

Example:

```
Device# request aaa unlock-user username
```

Step 3 When prompted, enter a new password for the user.

Type 6 passwords

Type 6 passwords

Type 6 password is an encryption method that

- enables secure reversible encryption for authentication, authorization, and accounting (AAA) and Simple Network Management Protocol (SNMP) configurations using the advanced encryption scheme (AES) algorithm
- uses a symmetric key to encrypt and decrypt stored passwords, and
- is the default password format in SD-WAN Manager templates released Cisco vManage Release 20.4.1 onwards.

Reversible encryption is the process by which a password is encrypted with a reversible, symmetric encryption algorithm. To check if the password entered by the user is valid, the password is decrypted and compared to the user-input password. To perform this encryption, the symmetric encryption algorithm requires a key that you can provide. The encryption algorithm used is advanced encryption standard (AES) algorithm in Cipher Block Chaining (CBC) mode with a PKCS#5 padding. This algorithm is used for AAA features such as RADIUS, TACACS+, SNMP, and TrustSec.

Type 6 passwords in SD-WAN Manager

SD-WAN Manager encrypts the passwords and sends the passwords to the router over a secure tunnel. The router encrypts the passwords in type 6 format and stores them on the device. You cannot use type 6 passwords on Viptela software.

Use type 6 passwords to reduce the risks of attacks on password integrity. When you upgrade your devices to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, all AAA, RADIUS key, and TACACS+ keys are encrypted to type 6.

Note SD-WAN Manager encrypted passwords show up as either 6 or 8 whereas, Cisco IOS XE devices use encryption streams defined as type 0, type 5, type 6, type 8, and similar types. On the other hand, SD-WAN Manager runs on Viptela OS which is based on Linux. Linux uses hashing and encryption schemes. Encrypted passwords on SD-WAN Manager starting with 6 refer to sha512-crypt. Passwords beginning with 8 represent aes-cfb 128 encryption.

Note On Cisco IOS XE Catalyst SD-WAN devices, an admin user with privilege 15 is created by default during day-0 bringup of the device. We recommend that users do not delete this admin user.

Supported platforms and templates

Type 6 passwords are supported for these platforms and templates.

Supported platforms:

- Cisco IOS XE Catalyst SD-WAN devices

Supported templates:

- RADIUS and TACACS authentication using the Cisco AAA template
- SNMP template
- CLI add-on template

Restrictions for Type 6 passwords

SNMP templates

In SNMP templates, the community name is encrypted by default. To upgrade your SNMP templates to use type 6 passwords, delete and re-create the community and trap target.

Password length

When you use type 6 passwords with the keychain key-string command, you can enter up to 38 characters in clear text.

Upgrade existing templates to Type 6 passwords

Use this procedure to upgrade passwords in your existing templates on Cisco SD-WAN Manager to type 6 passwords.

When you upgrade your routers to Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, all supported passwords are automatically upgraded to type 6 passwords.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 For the template that you want to upgrade to type 6 passwords, click **…**.

Step 4 Click **Edit**.

Step 5 Click **Save**.

To update the passwords, you do not need to make any other changes to the template. When you click **Save**, SD-WAN Manager automatically upgrades the passwords to type 6 passwords.

Type 6 encryption for CLI commands

This section explains how you can encrypt your passwords to Type 6 using a CLI add-on template.

In the CLI add-on template, you can encrypt supported CLIs including passwords, keys, secret text, community name, and other strings. See Commands supported for Type 6 encryption for more information.

Simply select the plaintext password, key, or similar in the CLI and click the **Encrypt Type 6** button and save the configuration.

Methods for verifying Type 6 passwords

You can use one or more of these verification commands to verify that your passwords are upgraded to type 6 passwords.

Verifying using SD-WAN Manager

In Cisco SD-WAN Manager, when you attach a configuration that supports type 6 passwords to your device, the configuration preview displays the encrypted password.

For example:

```
snmp-server community 0 $CRYPT_CLUSTER$ptqX7nQr6QvC8YZuoMGOkw==$6cVCeSpOfoVFe5iqhJqvQQ==
ro
```

Although the command displays the type as `0`, the `$CRYPT_CLUSTER$ptqX7nQr6QvC8YZuoMGOkw==$6cVCeSpOfoVFe5iqhJqvQQ==` string represents your encrypted password. If your password is encrypted, it will begin with `$CRYPT_CLUSTER$`.

Verifying on a device

You can run the following command on your device to display your encrypted passwords:

```
Device#show run | sec aaa
aaa new-model
aaa group server tacacs+ tacacs-0
server-private 10.0.0.1 key 6 BibgKcVeWF]^aK[XfEIICXMCbdScBYAAB
aaa group server radius radius-0
server-private 10.0.0.2 timeout 5 retransmit 3 key 6 CHd_VK[]NHEdcVCWGCaENGINQHLBEhDBe
```

The output indicates that your password is type 6 and includes your encrypted password.