Configure User Access and Authentication

Use the **Manage Users** screen to add, edit, or delete users and user groups from Cisco SD-WAN Manager.

Only a user logged in as the **admin** user or a user who has Manage Users write permission can add, edit, or delete users and user groups from Cisco SD-WAN Manager.

Configure Hardened Passwords

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.

Enforce Strong Passwords

We recommend the use of strong passwords. You must 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 that the rule defines. In addition, for releases 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 that the rule defines.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. IClick **Password Policy**.
3. Perform one of these actions, based on your Cisco SD-WAN Manager release:
   - For releases before Cisco vManage Release 20.9.1, click **Enabled**.
   - For releases 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**.
4. Click **Save**.

Password Requirements

Cisco SD-WAN Manager enforces the following password requirements after you have enabled the password policy rules:

- The following password requirements apply 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.
- Must contain different characters in at least four positions in the password.

- Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1:

Password Criteria	Requirements
Medium Security	• Must contain a minimum of 8 characters • Must contain no more than 32 characters • Must contain at least 1 lowercase character • Must contain at least 1 uppercase character • Must contain at least 1 numeric character • Must contain at least 1 of the following special characters: # ? ! @ $ % ^ & * - • Must not be identical to any of the last 5 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 1 lowercase character • Must contain at least 1 uppercase character • Must contain at least 1 numeric character • Must contain at least 1 of the following special characters: # ? ! @ $ % ^ & * - • Must not be identical to any of the last 5 passwords used • Must not contain the full name or username of the user • Must have at least eight characters that are not in the same position they were in the old password

Password Attempts Allowed

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 no password is entered multiple times. When you do not enter anything in the password field, it is considered as invalid or wrong password.

Password Change Policy

Note You must have enabled password policy rules first for strong passwords to take effect. For more information, see Enforce Strong Passwords, on page 2.

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

Note 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.

Reset a Locked User

If a user is locked out after multiple password attempts, an administrator with the required rights can update passwords for this user.

There are two ways to unlock a user account, by 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.

To reset the password of a user who has been locked out:

1. In **Users** (**Administration** > **Manage Users**), choose the user in the list whose account you want to unlock.
2. Click **. . .** and choose **Reset Locked User**.
3. Click **OK** to confirm that you want to reset the password of the locked user. Note that this operation cannot be undone.

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

Reset a Locked User Using the CLI

You can reset a locked user using the CLI as follows:

1. Log in to the device as an `admin` user.
2. Run the following command:

   ```
   Device# request aaa unlock-user username
   ```
3. When prompted, enter a new password for the user.

Configure User Login Options

Table 2: Feature History

Feature Name	Release Information	Description
Inactivity Lockout	Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature lets you configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days.
Unsuccessful Login Attempts Lockout	Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature lets you configure Cisco SD-WAN Manager to lock out users who have made a designated number of consecutive unsuccessful login attempts within a designated period.
Duo Multifactor Authentication Support	Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature lets you configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to Cisco SD-WAN Manager.

Beginning with Cisco Catalyst SD-WAN Manager Release 20.12.1, a netadmin user can enable the following Cisco SD-WAN Manager user login features:

Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, you can access Cisco SD-WAN Manager with basic privileges even if TACACS user is not mapped to a group. Prior to Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the access to Cisco SD-WAN Manager was denied.

- Inactivity lockout: You can configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days. Locked out users cannot log in to Cisco SD-WAN Manager until an administrator unlocks their accounts.

  See Configure Account Lockout , on page 6.

- Unsuccessful login lockout: You can configure Cisco SD-WAN Manager to prevent users who make a designated number of consecutive unsuccessful login attempts within a designated time period from

logging in to Cisco SD-WAN Manager until a configured amount of time passes or an administrator unlocks their user accounts.

By default, Cisco SD-WAN Manager locks out users for 15 minutes after five consecutive unsuccessful login attempts within 15 minutes. After a lockout period expires, a user can log in with the correct user name and password.

See Configure Unsuccessful Login Attempts Lockout, on page 7.

- Duo multifactor authentication: You can configure Cisco SD-WAN Manager to require the use of Duo multifactor authentication to verify identity before users can log in. Users must confirm a login attempt by using Duo multifactor authentication on their mobile devices.

  See Configure Duo Multifactor Authentication, on page 9.

Configure Account Lockout

Before You Begin

Beginning with Cisco Catalyst SD-WAN Manager Release 20.12.1, you can configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days.

Cisco SD-WAN Manager marks locked out users as inactive, and they cannot log in again until an administrator unlocks their accounts in Cisco SD-WAN Manager.

Note To unlock a user account, see Reset a Locked User.

Configure Account Lockout

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Account Lockout** and enable the **Inactive days before locked out** option.

   (In Cisco Catalyst SD-WAN Manager Release 20.12.x, locate the **Account Lockout**, click **Edit**, and enable **Inactive days before locked out**.)
3. Configure the following options:

Field	Description
Inactive days before account locked out	Enable this option and enter the number of consecutive inactive days after which Cisco SD-WAN Manager locks out a user. An inactive day is defined as a day on which a user does not log in to Cisco SD-WAN Manager. Valid values are 2 through 90.

Field	Description
Number of failed login attempts before lockout	Enter the number of failed login attempts after which Cisco SD-WAN Manager locks out a user. Possible values: 1 through 3600 Default: 3600
Duration within which the failed attempts are counted (minutes)	Enter the period, in minutes, during which the system counts consecutive unsuccessful login attempts. For example, if you set this period to 10 minutes, and set the number of failed login attempts before lockout to 5, Cisco SD-WAN Manager locks out a user if the user makes 5 consecutive unsuccessful login attempts within 10 minutes. Possibe values: 1 through 60 Default: 60
Cooldown or Lockout period	This option controls whether Cisco SD-WAN Manager automatically resets a user who is locked because of unsuccessful login attempts. This option is enabled by default. If you disable it, an administrator must manually unlocks the account of a locked-out user. **a.** Click **Enabled** adjacent to **Cooldown or Lockout period**. **b.** In the **Lockout Interval (minutes)** field, enter the number of minutes after which Cisco SD-WAN Manager automatically resets a locked out user. Possible values: 1 through 60 Default: 15

4. Click **Save**.

Configure Unsuccessful Login Attempts Lockout

Before You Begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1

Note From Cisco Catalyst SD-WAN Manager Release 20.13.1 or later, use the procedure described in Configure Account Lockout , on page 6.

You can configure Cisco SD-WAN Manager to lock out users who have made a designated number of consecutive unsuccessful login attempts within a period of time.

Cisco SD-WAN Manager prevents locked out users from logging in again until a configured amount of time has passed or an administrator unlocks their accounts in Cisco SD-WAN Manager.

Note To unlock a user account, see Reset a Locked User.

Configure Unsuccessful Login Attempts Lockout

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Account Lockout**
3. In the **Lockout on failed login attempts** row, click **Edit**.
4. Configure the following options:

Field	Description
Number of failed login attempts before lockout	Enter the number of failed login attempts after which Cisco SD-WAN Manager locks out a user. Possible values: 1 through 3600 Default: 3600
Duration within which the failed attempts are counted (minutes)	Enter the period, in minutes, during which the system counts consecutive unsuccessful login attempts. For example, if you set this period to 10 minutes, and set the number of failed login attempts before lockout to 5, Cisco SD-WAN Manager locks out a user if the user makes 5 consecutive unsuccessful login attempts within 10 minutes. Possibe values: 1 through 60 Default: 60

Field	Description
Cooldown or Lockout period	This option controls whether Cisco SD-WAN Manager automatically resets a user who is locked because of unsuccessful login attempts. This option is enabled by default. If you disable it, an administrator must manually unlocks the account of a locked-out user. **a.** Click **Enabled** adjacent to **Cooldown or Lockout period**. **b.** In the **Lockout Interval (minutes)** field, enter the number of minutes after which Cisco SD-WAN Manager automatically resets a locked out user. Possible values: 1 through 60 Default: 15

5. Click **Save**.

Configure Duo Multifactor Authentication

Beginning with Cisco Catalyst SD-WAN Manager Release 20.12.1, you can configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to Cisco SD-WAN Manager and other controllers. When you configure this feature, users are prompted on their mobile devices to authenticate with Duo after they enter a username and password and click **Log In** on the Cisco SD-WAN Manager **Login** screen.

This feature requires that you have a Duo account with local users created on that account.

Note

- Duo MFA does not apply to the admin user by default. To enable Duo MFA for the admin user, enable the**DUO MFA Configuration** option, and then enter the admin-auth-order command from the CLI.
- Users do not see a message in Cisco SD-WAN Manager that an MFA request has been sent to a mobile device.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **DUO MFA Configuration**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.
3. Click **Enabled**.
4. Configure the following options:

Field	Description
Integration Key	Enter the integration key (Ikey) for your Duo account.
Secret Key	Enter the secret key (Skey) for your Duo account.
API Hostname	Enter the API hostname (api-hostname) for your Duo account.
Server proxy	(Read only) Shows the server proxy that is used to access the Duo server if Cisco SD-WAN Manager is behind a firewall. Set this server proxy with the **system http proxy** or the **system https proxy** command. **Note** If Cisco SD-WAN Manager is deployed on a cloud that can be reached by an external network, a server proxy should not be set.

5. Click **Save**.
6. If a Cisco SD-WAN Validator or a Cisco SD-WAN Controller does not have internet access, use the following commands in the CLI or the device template of the device to provide access to the Duo MFA feature.

   These commands configure the device with proxy information about the device on which Duo MFA is enabled.

```
vm# config
vm(config)# system aaa
vm(config-aaa)# multi-factor-auth
vm(config-multi-factor-auth)# duo
vm(config-duo)# api-hostname name
vm(config-duo)# secret-key key
vm(config-duo)# integration-key key
vm(config-duo)# proxy proxy_url
vm(config-duo)# commit
```

Manage Users

From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** to add, edit, view, or delete users and user groups.

Please note the following:

- Only a user logged in as the **admin** user or a user who has Manage Users write permission can add, edit, or delete users and user groups from Cisco SD-WAN Manager.
- Each user group can have read or write permission for the features listed in this section. Write permission includes Read permission.
- All user groups, regardless of the read or write permissions selected, can view the information displayed in the Cisco SD-WAN Manager Dashboard.

Table 3: User Group Permissions for Different Device Types

Permissions	See This Section
User group permissions related to Cisco IOS XE Catalyst SD-WAN device configuration.	User Group Permissions: Cisco IOS XE Catalyst SD-WAN Devices
User group permissions related to Cisco Catalyst Wireless Gateway device configuration.	User Group Permissions: Cisco Catalyst Wireless Gateway Devices

Configure Users Using CLI

You can use the CLI to configure user credentials on each device. This way, you can create additional users and give them access to specific devices. The credentials that you create for a user by using the CLI can be different from the Cisco SD-WAN Manager credentials for the user. In addition, you can create different credentials for a user on each device. All Cisco IOS XE Catalyst SD-WAN device users with the **netadmin** privilege can create a new user.

To create a user account, configure the username and password, and place the user in a group:

This example, shows the addition of user, Bob, to an existing group:

```
Device(config)# system aaa user bob group basic
```

This example, shows the addition of user, Alice, to a new group `test-group`:

```
Device(config)# system aaa user test-group
Device(config)# system aaa user alice group test-group
```

The Username can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. Because some usernames are reserved, you cannot configure them. For a list of reserved usernames, see the **aaa** configuration command in the Cisco Catalyst SD-WAN Command Reference Guide.

The Password is the password for a user. Each username must have a password, and users are allowed to change their own password. The CLI immediately encrypts the string and does not display a readable version of the password. When a user logs in to a Cisco IOS XE Catalyst SD-WAN device, they have five chances to enter the correct password. After the fifth incorrect attempt, the user is locked out of the device, and must wait for 15 minutes before attempting to log in again.

Note Enclose any user passwords that contain the special character ! in double quotation marks (“ “). If a double quotation is not included for the entire password, the config database (?) treats the special character as a space and ignores the rest of the password.

For example, if the password is C!sc0, use “C!sc0”.

Group name is the name of a standard Cisco Catalyst SD-WAN group (**basic**, **netadmin**, or **operator**) or of a group configured with the **usergroup** command (discussed below). If an admin user changes the permission of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

The factory-default password for the admin username is admin. We strongly recommend that you modify this password the first time you configure a Cisco IOS XE Catalyst SD-WAN device:

```
Device(config)# username admin password
$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c
```

Configure the password as an ASCII string. The CLI immediately encrypts the string and does not display a readable version of the password, for example:

```
Device# show run | sec username
username admin privilege 15 secret 9
$9$3F2M2l2G2/UM3U$TGe2kqoIibdIRDEj4cOVKbVFP/o4vnlFAwWnmzx1rRE
username appnav privilege 15 secret 9
$9$3l2L2V.F2VIM1k$p3MBAyBtGxKf/yBGnUSHQ1g/ae1QhfIbieg28buJJGI
username eft secret 9 $9$3FMJ3/UD2VEL2E$d.kE4.an41v7wEhrQc6k5wIfE9M9WkNAJxUvbbempS.
username lab privilege 15 secret 9
$9$3l.J3FUD2F.E2.$/AiVn9PmLCpgr6ExVrE7dH979Wu8nbdtAfbzUtfysg.
username test secret 9 $9$1l2J3l6D3/QL3k$7PZOXJAJOI1os5UI763G3XcpVhXlqcwJ.qEmgmx4X9g
username vbonagir privilege 15 secret 9
$9$3/2K2UwF2lQF3U$VbdQ5bq18590rRthF/NnNnOsw.dw1/EViMTFZ5.ctus
Device#
```

If you are using RADIUS to perform AAA authentication, you can configure a specific RADIUS server to verify the password:

```
Device(config)#  radius server tag
```

The tag is a string that you defined with the **radius server tag** command, as described in the Cisco Catalyst SD-WAN Command Reference Guide.

Manage a User Group

Users are placed in groups, which define the specific configuration and operational commands that the users are authorized to view and modify. A single user can be in one or more groups. Cisco Catalyst SD-WAN software provides standard user groups, and you can create custom user groups, as needed:

- **basic**: Includes users who have permission to view interface and system information.
- **netadmin**: Includes the admin user, by default, who can perform all operations on the Cisco SD-WAN Manager. You can add other users to this group.
- **operator**: Includes users who have permission only to view information.
- Minimum supported release: Cisco vManage Release 20.9.1

  network_operations: Includes users who can perform non-security operations on Cisco SD-WAN Manager, such as viewing and modifying non-security policies, attaching and detaching device templates, and monitoring non-security data.
- Minimum supported release: Cisco vManage Release 20.9.1

  security_operations: Includes users who can perform security operations on Cisco SD-WAN Manager, such as viewing and modifying security policies, and monitoring security data.

Note: All user groups, regardless of the read or write permissions selected, can view the information displayed on the Cisco SD-WAN Manager Dashboard screen.

Delete a User Group

You can delete a user group when it is no longer needed. For example, you might delete a user group that you created for a specific project when that project ends.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **User Groups**.
3. Click the name of the user group you wish to delete.

Note You cannot delete any of the default user groups—basic, netadmin, operator, network_operations, and security_operations.

4. Click **Trash** icon.
5. To confirm the deletion of the user group, click **OK**.

Edit User Group Privileges

You can edit group privileges for an existing user group. This procedure lets you change configured feature read and write permissions for the user group needed.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **User Groups**.
3. Select the name of the user group whose privileges you wish to edit.

Note You cannot edit privileges for the any of the default user groups—basic, netadmin, operator, network_operations, and security_operations.

4. Click **Edit**, and edit privileges as needed.
5. Click **Save**.

If an **admin** user changes the privileges of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

Creating Groups Using CLI

The Cisco Catalyst SD-WAN software provides default user groups: **basic**, **netadmin**, **operator**, **network_operations**, and **security_operations**. The username **admin** is automatically placed in the **netadmin** usergroup.

If needed, you can create additional custom groups and configure privilege roles that the group members have. To create a custom group with specific authorization, configure the group name and privileges:

```
Device(config)# aaa authentication login user1 group radius enable
Device(config)# aaa authentication login user2 group radius enable
Device(config)# aaa authentication login user3 group radius enable
Device(config)#
```

group-name can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any

uppercase letters Some group names are reserved, so you cannot configure them. For a list of them, see the aaa configuration command.

If a remote RADIUS or TACACS+ server validates authentication but does not specify a user group, the user is placed into the user group **basic**. If a remote server validates authentication and specifies a user group (say, X) using VSA Cisco SD-WAN-Group-Name, the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).

In the **task** option, list the privilege roles that the group members have. The role can be one or more of the following: **interface**, **policy**, **routing**, **security**, and **system**.

Ciscotac User Access

The Cisco Edge software provides two users—**ciscotacro** and **ciscotacrw**—that are for use only by the Cisco Support team. These users are available for both cloud and on-premises installations. They operate on a consent-token challenge and token response authentication in which a new token is required for every new login session. The ciscotacro and ciscotacrw users can use this token to log in to Cisco SD-WAN Manager web server as well as the SSH Terminal on Cisco SD-WAN Manager. These users can also access Cisco SD-WAN Validator, Cisco SD-WAN Controllers, and Cisco vEdge devices using the SSH Terminal on Cisco SD-WAN Manager.

The default CLI templates include the ciscotacro and ciscotacrw user configuration. These users are enabled by default. However, a customer can disable these users, if needed.

- **ciscotacro User:** This user is part of the operator user group with only read-only privileges. This user can only monitor a configuration but cannot perform any operation that will modify the configuration of the network.
- **ciscotacrw User:** This user is part of the netadmin user group with read-write privileges. This user can modify a network configuration. In addition, only this user can access the root shell using a consent token.

Use the **tools consent-token** command to authenticate the network administrator of an organization to access system shell. Starting Cisco Catalyst SD-WAN Control Components Release 20.12.x, the **request support ciscotac** command is deprecated.

Limitations

- Only 16 concurrent sessions are supported for the ciscotacro and ciscotacrw users.
- The session duration is restricted to four hours. It is not configurable.
- The inactivity timer functionality closes user sessions that have been idle for a specified period of time. This feature is enabled by default and the timeout value is 30 minutes. However, the user configuration includes the option of extending the inactivity timer.
- A customer can remove these two users. If removed, the customer can open a case and share temporary login credentials or share the screen with the Cisco Support team for troubleshooting an issue.

Configure Sessions in Cisco SD-WAN Manager

Table 4: Feature History

Feature History	Release Information	Description
Configure Sessions in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature lets you see all the HTTP sessions that are open within Cisco SD-WAN Manager. It gives you details about the username, source IP address, domain of the user, and other information. A user with User Management Write access, or a netadmin user can trigger a log out of any suspicious user's session.

Set a Client Session Timeout in Cisco SD-WAN Manager

You can set a client session timeout in Cisco SD-WAN Manager. When a timeout is set, such as no keyboard or keystroke activity, the client is automatically logged out of the system.

Note You can edit Client Session Timeout in a multitenant environment only if you have a Provider access.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **User Sessions**.
3. Under **Client Session Timeout**, click **Session Timeout**.
4. Specify the timeout value, in minutes.
5. Click **Save**.

Set a Session Lifetime in Cisco SD-WAN Manager

You can specify how long to keep your session active by setting the session lifetime, in minutes. A session lifetime indicates the amount of time for which a session can be active. If you keep a session active without letting the session expire, you will be logged out of the session in 24 hours, which is the default session timeout value.

The default session lifetime is 1440 minutes or 24 hours.

Note You can edit Session Lifetime in a multitenant environment only if you have a Provider access.

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

2. Click **User Sessions**.
3. In the **SessionLifeTime Timeout (minutes) field**, specify the session timeout value, in minutes, from the drop-down list.
4. Click **Save**.

Set the Server Session Timeout in Cisco SD-WAN Manager

You can configure the server session timeout in Cisco SD-WAN Manager. The server session timeout indicates how long the server should keep a session running before it expires due to inactivity. The default server session timeout is 30 minutes.

Note Server Session Timeout is not available in a multitenant environment even if you have a Provider access or a Tenant access.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **User Sessions**.
3. In **Server Session Timeout Timeout(minutes)** field, specify the timeout value, in minutes.
4. Click **Save**.

Enable Maximum Sessions Per User

You can enable the maximum number of concurrent HTTP sessions allowed per username. If you enter 2 as the value, you can only open two concurrent HTTP sessions. If you try to open a third HTTP session with the same username, the third session is granted access, and the oldest session is logged out.

Note Maximum Session Per User is not available in a multitenant environment even if you have a Provider access or a Tenant access.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In Max Session Per User, click **Session**.
3. In the **Max Sessions Per User** field, specify a value for the maximum number of user sessions.
4. Click **Save**.

Configuring RADIUS Authentication Using CLI

The Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco devices and send authentication

requests to a central RADIUS server, which contains all user authentication and network service access information.

To have a Cisco IOS XE Catalyst SD-WAN device use RADIUS servers for user authentication, configure one or up to 8 servers:

```
Deviceconfig-transaction
Device(config)# radius server test address ipv4 10.1.1.55 acct-port 110
Device(config-radius-server)# key 33
Device(config-radius-server)# exit
Device(config)# radius server test address ipv4 10.1.1.55 auth-port 330
Device(config-radius-server)# key 55
Device(config-radius-server)#
```

For each RADIUS server, you must configure, at a minimum, its IP address and a password, or key. You can specify the key as a clear text string up to 31 characters long or as an AES 128-bit encrypted key. The local device passes the key to the RADIUS server. The password must match the one used on the server. To configure more than one RADIUS server, include the **server** and **secret-key** commands for each server.

The remaining RADIUS configuration parameters are optional.

To set the priority of a RADIUS server, as a means of choosing or load balancing among multiple RADIUS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.

By default, the Cisco IOS XE Catalyst SD-WAN device uses port 1812 for authentication connections to the RADIUS server and port 1813 for accounting connections. To change these port numbers, use the **auth-port** and **acct-port** commands.

If the RADIUS server is reachable via a specific interface, configure that interface with the **source-interface** command.

You can tag RADIUS servers so that a specific server or servers can be used for AAA, IEEE 802.1X, and IEEE 802.11i authentication and accounting. Define the tag here, with a string from 4 to 16 characters long. Then associate the tag with the **radius-servers** command when you configure AAA, and when you configure interfaces for 802.1X and 802.11i.

If the RADIUS server is located in a different VPN from the Cisco IOS XE Catalyst SD-WAN device, configure the server's VPN number so that the Cisco IOS XE Catalyst SD-WAN device can locate it. If you configure multiple RADIUS servers, they must all be in the same VPN.

When waiting for a reply from the RADIUS server, a Cisco IOS XE Catalyst SD-WAN device waits 3 seconds before retransmitting its request. To change this time interval, use the **timeout** command, setting a value from 1 to 1000 seconds:

```
Device# config-transaction
 Device(config)# aaa group server radius server-10.99.144.201
 Device(config-sg-radius)# server-private 10.99.144.201 auth-port 1812 timeout 5 retransmit
 3
```

Configure SSH Authentication

Table 5: Feature History

Feature Name	Release Information	Description
Secure Shell Authentication Using RSA Keys	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature helps configure RSA keys by securing communication between a client and a Cisco Catalyst SD-WAN server.

The Secure Shell (SSH) protocol provides secure remote access connection to network devices.

SSH supports user authentication using public and private keys. To enable SSH authentication, public keys of the users are stored in the home directory of authenticating user in the following location:

```
~<user>/.ssh/authorized_keys
```

A new key is generated on the client machine which owns the private-key. Any message encrypted using the public key of the SSH server is decrypted using the private key of the client.

Restrictions for SSH Authentication on Cisco Catalyst SD-WAN

- The range of SSH RSA key size supported by Cisco IOS XE Catalyst SD-WAN devices is from 2048 to 4096. SSH RSA key size of 1024and 8192 are not supported.
- A maximum of two keys per user are allowed on Cisco IOS XE Catalyst SD-WAN devices.

SSH Authentication using Cisco SD-WAN Manager on Cisco IOS XE Catalyst SD-WAN Devices

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

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

3. From **Select Devices**, select the type of device for which you are creating the template.
4. From **Basic Information**, choose **CISCO AAA** template.
5. From **Local**, click **New User** and enter the details.
6. Enter **SSH RSA Key**.

Note You must enter the complete public key from the id_rsa.pub file in **SSH RSA Key**.

Configure SSH Authentication using CLI on Cisco IOS XE Catalyst SD-WAN Devices

SSH key based login is supported on IOS. Per user a maximum of 2 keys can be supported. Also, IOS only supports RSA based keys.

Traditional IOS CLI, allow support for:

• Key-string

• Key-hash – The key-string is base64 decoded and MD5 hash is run on it.

However, the transaction yang model has provision to only copy the key-hash (instead of the entire key-string). Cisco SD-WAN Manager does this conversion and pushes the configuration to the device.

Public Keys supported on Cisco IOS XE Catalyst SD-WAN Devices

- SSH-RSA

Configure the Authentication Order

The authentication order dictates the order in which authentication methods are tried when verifying user access to a Cisco IOS XE Catalyst SD-WAN device through an SSH session or a console port. The default authentication order is **local**, then **radius**, and then **tacacs**. With the default authentication order, the authentication process occurs in the following sequence:

- The authentication process first checks whether a username and matching password are present in the running configuration on the local device.
- If the RADIUS server is unreachable (or all the servers are unreachable), the authentication process checks the TACACS+ server. For this method to work, you must configure one or more TACACS+ servers with the **system tacacs server** command. If a TACACS+ server is reachable, the user is authenticated or denied access based on that server's TACACS+ database. If a TACACS+ server is unreachable and if you have configured multiple TACACS+ servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's TACACS+ database.
- If the TACACS+ server is unreachable (or all TACACS+ servers are unreachable), user access to the local Cisco IOS XE Catalyst SD-WAN device device is denied.

To modify the default order, use the **auth-order** command:

Specify one, two, or three authentication methods in the preferred order, starting with the one to be tried first. If you configure only one authentication method, it must be **local**.

To have the "admin" user use the authentication order configured in the **auth-order** command, use the following command:

```
Device(config-system-aaa)# admin-auth-order
```

If you do not include this command, the "admin" user is always authenticated locally.

You can configure authentication to fall back to a secondary or tertiary authentication mechanism when the higher-priority authentication method fails to authenticate a user, either because the user has entered invalid credentials or because the authentication server is unreachable (or all the servers are unreachable):

- If the authentication order is configured as **radius local**:
  - With the default authentication, local authentication is used only when all RADIUS servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for local authentication.
- If the authentication order is configured as **local radius**:
  - With the default authentication, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device.
- If the authentication order is configured as **radius tacacs local**:
  - With the default authentication, TACACS+ is tried only when all RADIUS servers are unreachable, and local authentication is tried only when all TACACS+ servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for the TACACS+ server. Similarly, if a TACACS+ server denies access, the user cannot log via local authentication.

If a remote server validates authentication but does not specify a user group, the user is placed into the user group **basic**.

If a remote server validates authentication and specifies a user group (say, X), the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).

If a remote server validates authentication and that user is not configured locally, the user is logged in to the vshell as the user **basic**, with a home directory of /home/basic.

If a remote server validates authentication and that user is configured locally, the user is logged in to the vshell under their local username (say, eve) with a home direction of /home/*username* (so, /home/eve).

Note Tags are used for grouping, describing, or finding devices. You can tag RADIUS and TACAC servers for authentication and accounting. You can add more than one tag to a device. Starting from Cisco vManage Release 20.9.1, following new tags are used in authentication:

- Viptela-User-Group: for user group definitions instead of Viptela-Group-Name.
- Viptela-Resource-Group: for resource group definitions.

The authentication fails if there is any space between keys and the values. For example, **key=value**.

Role-Based Access with AAA

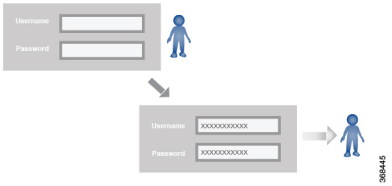
The Cisco Catalyst SD-WAN AAA software implements role-based access to control the authorization permissions for users on Cisco IOS XE Catalyst SD-WAN devices. Role-based access consists of three components:

- Users are those who are allowed to log in to a Cisco IOS XE Catalyst SD-WAN device.
- User groups are collections of users.

- Privileges are associated with each group. They define the commands that the group's users are authorized to issue.

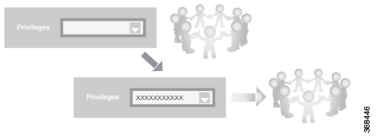
Users and User Groups

All users who are permitted to perform operations on a Cisco IOS XE Catalyst SD-WAN device must have a login account. For the login account, you configure a username and a password on the device itself. These allow the user to log in to that device. A username and password must be configured on each device that a user is allowed to access.



The Cisco Catalyst SD-WAN software provides one standard username, **admin**, which is a user who has full administrative privileges, similar to a UNIX superuser. By default, the **admin** username password is **admin**. You cannot delete or modify this username, but you can and should change the default password.

User groups pool together users who have common roles, or privileges, on the Cisco IOS XE Catalyst SD-WAN device. As part of configuring the login account information, you specify which user group or groups that user is a member of. You do not need to specify a group for the **admin** user, because this user is automatically in the user group **netadmin** and is permitted to perform all operations on the Cisco IOS XE Catalyst SD-WAN device.



The user group itself is where you configure the privileges associated with that group. These privileges correspond to the specific commands that the user is permitted to execute, effectively defining the role-based access to the Cisco Catalyst SD-WAN software elements.

The Cisco Catalyst SD-WAN software provides the following standard user groups:

- **basic**: The basic group is a configurable group and can be used for any users and privilege levels. This group is designed to include users who have permission to both view and modify information on the device.
- **operator**: The operator group is also a configurable group and can be used for any users and privilege levels. This group is designed to include users who have permission only to view information.
- **netadmin**: The netadmin group is a non-configurable group. By default, this group includes the **admin** user. You can add other users to this group. Users in this group are permitted to perform all operations on the device.
- Minimum supported release: Cisco vManage Release 20.9.1

network_operations: The **network_operations** group is a non-configurable group. Users in this group can perform all non-security-policy operations on the device and only view security policy information. For example, users can create or modify template configurations, manage disaster recovery, and create non-security policies such as application aware routing policy or CFlowD policy.

- Minimum supported release: Cisco vManage Release 20.9.1

security_operations: The **security_operations** group is a non-configurable group. Users in this group can perform all security operations on the device and only view non-security-policy information. For example, users can manage umbrella keys, licensing, IPS signatures auto update, TLS/SSL proxy settings, and so on.

Users of the **network_operations** group are authorized to apply policies to a device, revoke applied policies, and edit device templates. Users of the **security_operations** group require **network_operations** users to intervene on day-0 to deploy security policy on a device and on day-N to remove a deployed security policy. However, after a security policy is deployed on a device, **security_operations** users can modify the security policy without needing the **network_operations** users to intervene.

Note Only admin users can view running and local configuration. Users associated with predefined operator user group do not have access to the running and local configurations. The predefined user group operator has only read access for the template configuration. If you need only a subset of admin user privileges, then you need to create a new user group with the selected features from the features list with both read and write access and associate the group with the custom user.

Privileges for Role-Based Access

Role-based access privileges are arranged into five categories, which are called *tasks:*

- Interface—Privileges for controlling the interfaces on the Cisco IOS XE Catalyst SD-WAN device.
- Policy—Privileges for controlling control plane policy, OMP, and data plane policy.
- Routing—Privileges for controlling the routing protocols, including BFD, BGP, OMP, and OSPF.
- Security—Privileges for controlling the security of the device, including installing software and certificates. Only users belonging to the **netadmin** group can install software on the system.
- System—General systemwide privileges.

The tables in the following sections detail the AAA authorization rules for users and user groups. These authorization rules apply to commands issued from the CLI and to those issued from Netconf.

User Authorization Rules for Operational Commands

The user authorization rules for operational commands are based simply on the username. Any user who is allowed to log in to the Cisco IOS XE Catalyst SD-WAN device can execute most operational commands. However, only the **admin** user can issue commands that affect the fundamental operation of the device, such as installing and upgrading the software and shutting down the device.

Note that any user can issue the **config** command to enter configuration mode, and once in configuration mode, they are allowed to issue any general configuration command. Also, any user is allowed to configure their password by issuing the **system aaa user** *self* **password** *password* command and then committing that

configuration change. For the actual commands that configure device operation, authorization is defined according to user group membership. See User Group Authorization Rules for Configuration Commands.

The following tables lists the AAA authorization rules for general CLI commands. All the commands are operational commands except as noted. Also, some commands available to the "admin" user are available only if that user is in the "netadmin" user group.

CLI Command	Any User	Admin User
clear history	X	X
commit confirm	X	X
complete-on-space	X	X
config	X	X
exit	X	X
file	X	X
help	X	X
[no] history	X	X
idle-timeout	X	X
job	X	X
logout	—	X (users in netadmin group only)
monitor	X	X
nslookup	X	X
paginate	X	X
ping	X (users in netadmin group only)	X (users in netadmin group only)
poweroff	—	X(users in netadmin group only)
prompt1	X	X
prompt2	X	X
quit	X	X
reboot	—	X (users in netadmin group only)
request aaa request admin-tech request firmware request interface-reset request nms request reset request software	—	X (users in netadmin group only)
request execute request download request upload	X	X

CLI Command	Any User	Admin User
request (everything else)	—	X
rollback (configuration mode command)	—	X (users in netadmin group only)
screen-length	X	X
screen-width	X	X
show cli	X	X
show configuration commit list	X	X
show history	X	X
show jobs	X	X
show parser dump	X	X
show running-config	X	X
show users	X	X
system aaa user *self* password *password* (configuration mode command) (Note: A user cannot delete themselves)		
tcpdump	X	X
timestamp	X	X
tools ip-route	X	X
tools netstat	X	X
tools nping	X	X
traceroute	X	X
vshell	X (The availability of vshell command is unavailable to all users that are not in netadmin group in Cisco vManage Release 20.9.5.)	X (The vshell AAA authorized access is limited only to users that are in netadmin group.)

User Group Authorization Rules for Operational Commands

The following table lists the user group authorization roles for operational commands.

Operational Command	Interface	Policy	Routing	Security	System
clear app		X			
clear app-route		X			
clear arp	X				
clear bfd			X		X
clear bgp			X		X
clear bridge	X				
clear cellular	X				
clear control				X	
clear crash					X
clear dhcp					X
clear dns					X
clear igmp			X		
clear installed-certificates				X	
clear interface	X				
clear ip			X		
clear notification					X
clear omp			X		
clear orchestrator				X	
clear ospf			X		
clear pim			X		
clear policy		X			
clear pppoe	X				
clear system					X
clear tunnel				X	
clear wlan	X				
clear ztp				X	X
clock					X

Operational Command	Interface	Policy	Routing	Security	System
debug bgp			X		
debug cellular	X				
debug cflowd		X			
debug chmgr					X
debug config-mgr					X
debug dhcp-client					X
debug dhcp-helper					X
debug dhcp-server					X
debug fpm		X			
debug ftm					X
debug igmp			X		
debug netconf					X
debug omp			X		
debug ospf			X		
debug pim			X		
debug resolver			X		
debug snmp					X
debug sysmgr					X
debug transport					X
debug ttm					X
debug vdaemon				X	X
debug vrrp				X	
debug wlan	X				
request certificate				X	
request control-tunnel				X	
request controller				X	
request controller-upload				X	

Operational Command	Interface	Policy	Routing	Security	System
request csr				X	
request device				X	
request device-upload				X	
request on-vbond-controller				X	
request port-hop				X	
request root-cert-chain				X	
request security				X	
request vedge				X	
request vedge-upload				X	
request vsmart-upload				X	
show aaa					X
show app		X			
show app-route		X			
show arp	X				
show bfd			X		X
show bgp			X		
show boot-partition					X
show bridge	X				
show cellular	X				
show certificate				X	
show clock					X
show control				X	X
show crash					X
show debugs—same as debug commands					
show dhcp					X
show external-nat				X	X
show hardware					X

Operational Command	Interface	Policy	Routing	Security	System
show igmp			X		
show interface	X				
show ip			X		X
show ipsec				X	
show licenses					X
show logging					X
show multicast			X		
show nms-server					X
show notification					X
show ntp					X
show omp		X	X		X
show orchestrator				X	
show ospf			X		
show pim			X		
show policer		X			
show policy		X			
show ppp	X				
show pppoe	X				
show reboot					X
show security-info				X	
show software					X
show system					X
show transport					X
show tunnel				X	
show uptime					X
show users					X
show version					X
show vrrp	X				

Operational Command	Interface	Policy	Routing	Security	System
show wlan	X				
show ztp				X	

User Group Authorization Rules for Configuration Commands

The following table lists the user group authorization rules for configuration commands.

Configuration Command	Interface	Policy	Routing	Security	System
apply-policy		X			
banner					X
bfd			X		X
bridge	X				
omp		X	X		X
policy		X			
security				X	X
snmp					X
system					X
vpn interface	X				
vpn ip			X		
vpn router			X		
vpn service			X		
vpn (everything else, including creating, deleting, and naming)					X
wlan	X				

Configuring AAA using Cisco SD-WAN Manager Template

Table 6: Feature History

Feature Name	Release Information	Description
Authorization and Accounting	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature provides for the configuration of authorization, which authorizes commands that a user enters on a device before the commands can be executed, and accounting, which generates a record of commands that a user executes on a device.

Configuring AAA by using the Cisco SD-WAN Manager template lets you make configuration setting inCisco SD-WAN Manager and then push the configuration to selected devices of the same type. This procedure is a convenient way to configure several of the same type of devices at one time.

Use the AAA template for Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager instances, Cisco Catalyst SD-WAN Controllers, and Cisco IOS XE Catalyst SD-WAN devices.

Cisco IOS XE Catalyst SD-WAN devices support configuration of authentication, authorization, and accounting (AAA) in combination with RADIUS and TACACS+.

Note You must configure a local user with a secret key via the template if you are using PPP or using MLPPP with CHAP.

Navigating to the Template Screen and Naming the Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and click **Create Template**.

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

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Select **Basic Information**.
6. To create a custom template for AAA, select Factory_Default_AAA_CISCO_Template and click **Create Template**. The AAA template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining AAA parameters.
7. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

8. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the **Scope** drop-down list to the left of the parameter field and select one of the following:

Table 7:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco IOS XE Catalyst SD-WAN device to a device template . When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Cisco IOS XE Catalyst SD-WAN device to a device template. For more information, see Create a Template Variables Spreadsheet . To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configuring Local Access for Users and User Groups

You can configure local access to a device for users and user groups. Local access provides access to a device if RADIUS or TACACS+ authentication fails.

To configure local access for individual users, select **Local**.

To add a new user, from **Local** click **+ New User**, and configure the following parameters:

Table 8:

Parameter Name	Description
Name	Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. The following usernames are reserved, so you cannot configure them: backup, basic, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, quagga, root, sshd, sync, sys, uucp, and www-data. Also, names that start with viptela-reserved are reserved.

Parameter Name	Description
Password	Enter a password for the user. Each username must have a password. Users are allowed to change their own passwords. The default password for the admin user is admin. We strongly recommended that you change this password. **Note** When configuring local users using a Cisco SD-WAN Manager AAA template, Cisco SD-WAN Manager uses a Cisco type 9 password type. The Cisco type 9 password type uses the scrypt algorithm for hashing the passwords of local users. The Cisco SD-WAN Manager AAA template uses only the Cisco type 9 password type for hashing of local user passwords. If you configure local users using a device CLI template or a CLI add-on template, you can choose other Cisco password types for hashing of local user passwords. For more information, see Configure Type 6 Passwords Using CLI Add-On Template.
Privilege Level 1 OR 15	Select between privilege level 1 or 15. • **Level 1**: User EXEC mode. Read-only, and access to limited commands, such as the `ping` command. • **Level 15**: Privileged EXEC mode. Full Access to all commands, such as the `reload` command, and the ability to make configuration changes. By default, the EXEC commands at privilege level 15 are a superset of those available at privilege level 1
SSH RSA Key(s)	Add SSH RSA Keys by clicking the **+ Add** button. A new field is displayed in which you can paste your SSH RSA key. To remove a key, click the - button. Devices support a maximum of 2 SSH RSA keys.

Click **Add** to add the new user. Click **+ New User** again to add additional users.

To configure local access for user groups, you first place the user into either the basic or operator group. The admin is automatically placed in the netadmin group. Then you configure user groups. To make this configuration, from **Local** select **User Group**.

Click **+ New User Group**, and configure the following parameters:

Table 9:

Parameter Name	Description
Name	Name of an authentication group. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. The Cisco Catalyst SD-WAN software provides three standard user groups, basic, netadmin, and operator. The user admin is automatically placed in the group netadmin and is the only user in this group. All users learned from a RADIUS or TACACS+ server are placed in the group basic. All users in the basic group have the same permissions to perform tasks, as do all users in the operator group. The following groups names are reserved, so you cannot configure them: adm, audio, backup, bin, cdrom, dialout, dip, disk, fax, floppy, games, gnats, input, irc, kmem, list, lp, mail, man, news, nogroup, plugdev, proxy, quagga, quaggavty, root, sasl, shadow, src, sshd, staff, sudo, sync, sys, tape, tty, uucp, users, utmp, video, voice, and www-data. Also, group names that start with the string viptela-reserved are reserved.
Feature Type	Click **Preset** to display a list of preset roles for the user group. Click **Custom** to display a list of authorization tasks that have been configured.
Feature	The feature table lists the roles for the user group. These roles are Interface, Policy, Routing, Security, and System. Each role allows the user group to read or write specific portions of the device's configuration and to execute specific types of operational commands. Click the appropriate boxes for Read, Write, and None to assign privileges to the group for each role.

Click **Add** to add the new user group.

To add another user group, click **+ New User Group** again.

To delete a user group, click the trash icon at the right side of the entry. You cannot delete the three standard user groups, basic, netadmin, and operator.

Configuring RADIUS Authentication

Configure RADIUS authentication if you are using RADIUS in your deployment.

To configure a connection to a RADIUS server, from **RADIUS**, click **+ New Radius Server**, and configure the following parameters:

Table 10:

Parameter Name	Description
Address	Enter the IP address of the RADIUS server host.
Authentication Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0. *Default:* Port 1812
Accounting Port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. *Range:* 0 through 65535. *Default:* 1813.

Parameter Name	Description
Timeout	Enter the number of seconds a device waits for a reply to a RADIUS request before retransmitting the request. *Default:* 5 seconds. *Range:* 1 through 1000
Retransmit Count	Enter the number of times the device transmits each RADIUS request to the server before giving up. *Default:* 5 seconds.
Key (Deprecated)	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.

Click **Add** to add the new RADIUS server.

To add another RADIUS server, click **+ New RADIUS Server** again.

To remove a server, click the trash icon.

CLI equivalent:

```
Device(config)# radius server 10.99.144.201
Device1(config-radius-server)# retransmit 5
Device(config-radius-server)# timeout 10
```

Configuring TACACS+ Authentication

Configure TACACS+ authentication if you are using TACACS+ in your deployment.

To configure a connection to a TACACS+ server, from **TACACS**, click **+ New TACACS Server**, and configure the following parameters:

Table 11:

Parameter Name	Description
Address	Enter the IP address of the TACACS+ server host.
Port	Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0. *Default:* Port 49
Timeout	Enter the number of seconds a device waits for a reply to a TACACS+ request before retransmitting the request. *Default:* 5 seconds. *Range:* 1 through 1000
Key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the TACACS+ server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS+ server.

Click **Add** to add the new TACACS server.

To add another TACACS server, click **+ New TACACS Server** again.

To remove a server, click the trash icon.

Configuring 8021X

For information on configuring 802.1X, see Configure IEEE 802.1X Authentication, on page 38.

Configuring Authentication Order

You can configure the authentication order for devices. The authentication order specifies the order in which the system attempts to authenticate user, and provides a way to proceed with authentication if the current authentication method is unavailable.

To configure AAA authentication order on a Cisco IOS XE Catalyst SD-WAN device, select the Authentication tab and configure the following parameters:

Table 12:

Parameter Name	Description
Server Group Order	Configuring a device to use AAA server groups provides a way to group existing server hosts. Grouping existing server hosts allows you to select a subset of the configured server hosts and use them for a particular service To change the default order of authentication methods that the software tries when verifying user access to a Cisco IOS XE Catalyst SD-WAN device: **1.** Click the ServerGroups priority order field to display the drop-down list of server groups. The list displays groups from local, RADIUS, and TACACS authentication methods. **2.** From the list, select the groups in the order that you want the software to verify a user trying to access a Cisco IOS XE Catalyst SD-WAN device. You must select at least one group from the list.

Configure Authorization and Accounting

Table 13: Feature History

Feature Name	Release Information	Description
Authorization and Accounting	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature provides for the configuration of authorization, which authorizes commands that a user enters on a device before the commands can be executed, and accounting, which generates a record of commands that a user executes on a device.

Configuring Authorization

You can configure authorization, which causes a TACACS+ server to authorize commands that users enter on a device before the commands can be executed. Authorization is based on the policies that are configured in the TACACS+ server an on the parameters that you configure on the Authorization tab.

Prerequisites

- The TACACS+ server and the local server must be configured as first in the authentication order on the **Authentication** tab.

To configure authorization, choose the **Authorization** tab, click **+ New Authorization Rule**, and configure the following parameters:

Parameter Name	Description
Console	Enable this option to perform authorization for console access commands.
Config Command	Enable this option to perform authorization for configuration commands.
Method	Choose **Command**, which causes commands that a user enters to be authorized.
Privilege Level 1 or 15	Choose the privilege level (1 or 15) for commands to be authorized. Authorization is provided for commands entered by users with this privilege level.
Groups	Choose a previously configured TACACS group. The parameters that this authorization rule defines are used by the TACACS servers that are associated with this group.
Authenticated	Enable this option to apply only to authenticated users the parameters that this authorization rule defines. If you do not enable this option, the rule is applied to all users.

Click Add to **add** the new authorization rule.

To add another authorization rule, click **+ New Accounting Rule** again.

To remove an authorization rule, click the trash icon on the right side of the line.

CLI equivalent:

```
system
   aaa
     aaa authorization console
     aaa authorization config-commands
     aaa authorization exec default list-name method
     aaa authorization commands level default list-name method
```

Configuring Accounting

You can configure accounting, which causes a TACACS+ server to generate a record of commands that a user executes on a device.

Prerequisite

- The TACACS+ server and the local server must be configured as first and second, respectively, in the authentication order on the **Authentication** tab. See Configuring Authentication Order.

To configure accounting, choose the **Accounting** tab, click **+ New Accounting Rule**, and configure the following parameters:

Table 14:

Parameter Name	Description
Method	Choose **Command**, which causes commands that a user executes to be logged.
Privilege Level 1 or 15	Choose the privilege level (1 or 15). Accounting records are generated only for commands entered by users with this privilege level.
Enable Start-Stop	Click **On** if you want the system to send a start accounting notice at the beginning of an event and a stop record notice at the end of the event.
Groups	Choose a previously configured TACACS group. The parameters that this accounting rule defines are used by the TACACS servers that are associated with this group.

Click **Add** to add the new accounting rule.

To add another accounting rule, click **+ New Accounting Rule** again.

To remove an accounting rule, click the trash icon on the right side of the line.

CLI equivalent:

```
system
  aaa
    aaa accounting exec default start-stop group group-name
    aaa accounting commands level default start-stop group group-name
    aaa accounting network default start-stop group group-name
    aaa accounting system default start-stop group group-name
```

Configure IEEE 802.1X Authentication

Table 15: Feature History

Feature Name	Release Information	Description
802.1X Support for SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature lets you enable the IEEE 802.1X authentication on Cisco IOS XE Catalyst SD-WAN devices. To be able to configure this feature using Cisco SD-WAN Manager, ensure that Cisco SD-WAN Manager is running Cisco SD-WAN Release 20.1.1.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, IEEE 802.1X is supported based on Identity-Based Networking Services (IBNS)1.0 IOS-XE CLIs. This feature is supported on both LAN and WAN interfaces.

IEEE 802.1X Open Authentication and Host Modes

Any of the four host modes (single-host mode, multiple-host mode, multi-domain authentication mode, and multiauthentication mode) may be configured to allow a device to gain network access before authentication.

Open authentication is enabled by entering the **authentication open** command after host mode configuration, and acts as an extension to the configured host mode. For example, if open authentication is enabled with single-host mode, then the port will allow only one MAC address. When preauthentication open access is enabled, initial traffic on the port is restricted and independent of 802.1X is configured on the port. If no access restriction other than 802.1X is configured on the port, then a client device will have a full access on the configured VLAN. You can configure open authentication using CLI template only. You cannot configure open authentication using dot1x feature template on Cisco SD-WAN Manager.

Prerequisites

- Enable RADIUS authentication servers to authenticate IEEE 802.1x services.
- Enable IEEE 802.1X configuration on switch-port interface.
- Enable the following VLAN configurations for authenticated and unauthenticated clients:
  - Restricted VLAN (or authentication rejected VLAN)
  - Guest VLAN
  - Critical VLAN (or authentication failed VLAN)
  - Critical Voice VLAN
- Enable one of the following host-mode authentication:
  - Single-host mode
  - Multiple-host mode
  - Multiple-authentication mode

- Multi-domain mode

- Configure RADIUS Accounting attributes.
- IEEE 802.1X Authentication event using VLAN ID has to be enabled in the Add-on template, if required.

Restrictions

- IEEE 802.1X Authentication, Authorization, and Accounting (AAA) is not supported on multiple groups.
- Authentication order IEEE 802.1X MAB CLI cannot be disabled through Cisco SD-WAN Manager. The presence of this authentication order CLI results in a 60 second delay in MAB authentication when MAB client is online.
- Authentication open is not supported in feature templates but can be deployed with a CLI add on template.

Configure IEEE 802.1X Authentication using Cisco SD-WAN Manager

IEEE 802.1X is a port-based network access control (PNAC) protocol that prevents unauthorized network devices from gaining access to wired networks by providing authentication for devices that want to connect to a wired network.

A RADIUS authentication server must authenticate each client connected to a port before that client can access any services offered by network.

To configure IEEE 802.1X authentication on the interface, first create a **Cisco AAA** feature template:

1. In Cisco SD-WAN Manager, select **Configuration** > **Templates**
2. Click **Feature Templates**, and then click **Add Template.**

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

3. Select your device from the list on the left panel.
4. Select the **Cisco AAA** template.
5. Enter the **Template Name** and **Description.**
6. Select the **RADIUS** tab and under **RADIUS SERVER** click on **New RADIUS Server.**
7. Configure the following parameters:

Parameter Name	Description
Mark as Optional Row	Check the **Mark as Optional Row** check box to mark your configuration as device-specific.
Address	Enter IP Address of the RADIUS server.

Parameter Name	Description
Authentication Port	Click **Authentication**, then click Add New Authentication Entry to configure RADIUS authentication attribute–value (AV) pairs to send to the RADIUS server during an IEEE 802.1X session. To save the entry, click **Add**.
Accounting Port	Click **Accounting**, then click **Add New Accounting Entry** to configure RADIUS accounting attribute–value (AV) pairs to send to the RADIUS server during an IEEE 802.1X session. To save the entry, click **Add**.
Timeout	Configure how long to wait for replies from the RADIUS server.
Retransmit Count	Configure how many times this RADIUS server is contacted.
Key	Enter the RADIUS server shared key.

8. Click **Add.**
9. Select **RADIUS GROUP** and click on **New RADIUS Group** to configure these parameters:

Parameter Name	Description
VPN-ID	Enter the VPN through which the RADIUS or other authentication server is reachable.
Source Interface	Enter the interface that will be used to reach the RADIUS server.
Radius Server	Configure the Radius server.

10. Click **Add.**
11. Select the **802.1X** tab and enter these parameters:

Parameter Name	Description
Authentication Param	Click On to enable authentication parameters.
Accounting Param	Click On to enable accounting parameters.

12. To save this feature template, click **Save**.
13. To enable this feature on your device, ensure to add these feature templates to your device template.

Note You need to recreate the AAA feature templates as the templates created prior to Cisco vManage Release 20.5 fails when attached to the device.

Next create a **Switch Port** template that can be used for the Switch Port device:

1. To create a **Switch Port** template, repeat steps 1 to 3 from above.
2. Select the **Switch Port** template.

3. Enter the **Template Name** and **Description.**
4. Select the **Interface** tab click on **New Interface.**
5. Configure the following parameters:

Parameter Name	Description
Interface name	Enter the interface name.
Speed	Enter the interface speed.
VLAN Name	Enter the VLAN name.
VLAN ID	Enter the VLAN identifier associated with the bridging domain.
802.1X	Enable IEEE 802.1X authentication on this interface. Select "On". This will provide a further set of parameters listed below.
Interface PAE Type	Enter the IEEE 802.1x Interface PAE type.
Control Direction	Enter unidirectional or bidirectional authorization mode.
Host Mode	Select whether an IEEE 802.1X interface grants access to a single host (client) or to multiple hosts (clients): • Multi Auth—Grant access to one host on a voice VLAN and multiple hosts on data VLANs. • Multi Host—Grant access to multiple hosts • Single Host—Grant access only to the first authenticated host. This is the default. • Multi-Domain—Grant access to both a host and a voice device, such as an IP phone on the same switch port. **Note** These options are available only in the 'Global' Host Mode settings.
Periodic Reauthentication	Enter how often to reauthenticate IEEE 802.1X clients. By default, no reauthentication attempts are made after the initial LAN access request. Range: 0 to 1440 minutes

6. Click on **Advanced Options** and enter the following:

Parameter Name	Description
Authentication Order	Enter the order of authentication methods to use when authenticating devices for connection to the IEEE 802.1X interface. The default authentication order is RADIUS, then MAC authentication bypass (MAB).
MAC Authentication Bypass	Select to enable MAC authentication bypass (MAB) on the RADIUS server and to authenticate non-IEEE 802.1X–compliant clients using a RADIUS server.

Parameter Name	Description
Port Control Mode	Enter the port control mode to enable IEEE 802.1X port-based authentication on the interface. Auto- Configure this to enable IEEE 802.1X authentication and start the port in unauthorized state. This allows only EAPOL frames to be sent and received through the port.
Voice VLAN ID	Configure the Voice VLAN ID.
Critical VLAN	Enter the critical VLAN (or authentication failed VLAN) for IEEE 802.1x-compliant clients. Configure network access when RADIUS authentication or the RADIUS server fails.
Critical Voice VLAN	Enable the critical voice VLAN.
Guest VLAN	Configure guest VLAN to drop non-IEEE 802.1X enabled clients, if the client is not in the MAB list.
Restricted VLAN	Enter the restricted VLAN (or authentication failed VLAN) for IEEE 802.1x-compliant clients. Configure limited services to IEEE 802.1X–compliant clients that failed RADIUS authentication.

7. Click on **Add.**
8. To save this feature template, click **Save**.
9. To enable this feature on your device, ensure to add these feature templates to your device template.

Configure IEEE 802.1X Open Authentication

You can configure IEEE 802.1X open authentication using the CLI add-on template.

```
Device# config-transaction
Device(config)# interface GigabitEthernet2
Device(config-if)# authentication open
```

Configure IEEE 802.1X Authentication using CLIs

Configuration

For this feature, two sets of configurations are required-

1. **Configure the Global AAA commands:**
   a. Enable or disable IEEE 802.1X globally

```
Device(config)# aaa authentication dot1x default group radius-0
Device(config)# aaa authorization network default group radius-0
Device(config)# dot1x system-auth-control
Device(config)# radius-server dead-criteria time 10 tries 3
Device(config)# radius-server deadtime 15
```

   b. Enable accounting

```
Device(config)# aaa accounting dot1x default start-stop group radius-0
```

2. **Configure the Interface Level commands:**

   a. Enable or disable IEEE 802.1X on port-basis

   ```
   Device(config-if)# dot1x pae authenticator
   Device(config-if)# authentication port-control auto
   ```

   b. Enable or disable MAB on port-basis

   ```
   Device(config-if)# mab
   ```

   c. Select host-mode

   ```
   Device(config-if)# authentication host-mode  <multi-auth | multi-domain | multi-host
    | single-host>
   ```

   d. Configure voice vlan

   ```
   Device(config-if)# switchport voice vlan <vlan-id>
   ```

   e. Select IEEE 802.1X control direction

   ```
   Device(config-if)# authentication control-direction <both | in>
   ```

   f. Enable periodic re-authentication and corresponding re-authentication interval and inactivity timeout time

   ```
   Device(config-if)# authentication periodic
   Device(config-if)# authentication timer reauthenticate <internal-in-sec>
   Device(config-if)# authentication timer inactivity <timeout-in-sec>
   ```

   g. Configurable authentication orders on per-port basis

   ```
   Device(config-if)# authentication order dot1x mab
   ```

   h. Specify the restricted VLAN

   ```
   Device(config-if)#  authentication event fail action authorize vlan <vlan-id>
   ```

   i. Specify the guest VLAN

   ```
   Device(config-if)# authentication event no-response action authorize vlan <vlan-id>
   ```

   j. Specify the critical VLAN

   ```
   Device(config-if)# authentication event server dead action authorize vlan <vlan-id>
   ```

   k. Enable the critical voice VLAN feature

   ```
   Device(config-if)# authentication event server dead action authorize voice
   ```

Posture Assessment Support

Table 16: Feature History

Feature Name	Release Information	Description
Posture Assessment Support	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature enables you to utilize Posture Assessment capabilites to validate the compliance of endpoints according to security policies of your enterprise. Identity Services Engine (ISE) Posture functions are integrated into Cisco 1100 Integrated Services Routers. This feature can only be configured using the Add-On feature template in Cisco SD-WAN Manager.

In a network, endpoint validation is necessary to ensure compliance with security policies of the company and posture assessment enables you to validate this. The posture module enforces security policies on endpoints that are connected to a network. For a connection between the endpoints of Cisco 1100 Integrated Services Router and ISE (Identity Services Engine), authentication interaction between them is required. IEEE 802.1X is the recommended standard authentication process for posture assessment, MAC Authentication Bypass (MAB) can be used as well.

The posture agent software used for this is Cisco AnyConnect Posture Assessment. The Cisco AnyConnect software is installed on the endpoint and has a module called posture. Cisco AnyConnect downloads security policies from ISE server and then checks the conditions (anti-malware condition, anti-spyware condition, anti-virus condition, application condition, USB condition) of the endpoints. If all conditions are met, Cisco AnyConnect gives a ‘Compliant’ result to the ISE server. If not, Cisco AnyConnect gives a ‘NonCompliant’ result. After authorization and authentication of the endpoints by authenticantion and redirect Access Control Lists (ACL), Cisco AnyConnect posture module on the client end initiates posture assessment with the posture-policy server.

After posture assessment is completed and authenticated, the RADIUS CoA (Change of Authorization) process is initiated by a policy set on ISE, from RADIUS servers to re-authenticate or re-authorize new policies. Once posture assessment is successful, access to the entire network is pushed down to the Cisco ISR 1100 router and to the client, through CoA re-authentication command.

Prerequisites for Posture Assessment

- Basic IEEE 802.1x authentication process should be functional.
- Change of Authorization (CoA) should be supported.
- Redirect ACL, downloadable ACL (dACL) and critical ACL should be available.
- Device tracking policy (for identity) should be supported.
- URL redirect should be supported.

Restrictions for Posture Assessment

- Only 8 port Cisco 1100 Integrated Services Routers support ACL functions such as dACL and redirect ACL.
- ACL and Access Control Entry (ACE) rules do not support compare operations, such as >, <, >=, <=
- Up to 120 dACL ACEs are supported, and 64 Redirect ACL ACEs are supported.
- Port ACL and IPv6 ACL are not supported.
- IP option and IP fragment ACL are not supported.
- Per-VLAN device-tracking is not supported.
- Only limited per-port device tracking policy options such as glean and address tracking are allowed.

Configuring Posture Assessment on Cisco Catalyst SD-WAN

1. Use the CLI Add-on template in Cisco SD-WAN Manager to configure AAA, IEEE 802.1x, posture assessment and redirect ACL and device-tracking.

   Example configurations are given below.

Note `aaa new-model` is enabled by default on Cisco Catalyst SD-WAN and is not configurable by the user. However, it must be configured on a non SD-WAN image.

a. Configure AAA

```
aaa new-model
radius server ISE1

address ipv4 198.51.100.255 auth-port 1812 acct-port 1813
key cisco

aaa group server radius ISE
 server name ISE1
!
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE

interface vlan 15
 ip address 198.51.100.1 198.51.100.254

interface GigabitEthernet0/1/0
 switchport mode access
 switchport access vlan 15

ip radius source-interface vlan 15
```

b. Configure IEEE 802.1x authentication and authorization

```
policy-map type control subscriber simple_dot1x
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
!
interface GigabitEthernet0/1/7
 switchport access vlan 22
 switchport mode access
```

```
 access-session closed
 access-session port-control auto
 dot1x pae authenticaton
 service-policy type control subscriber simple_dot1x
!
interface Vlan22
 ip address 198.51.100.1 198.51.100.254
```

Note The IEEE 802.1x endpoint is connected to GigabitEthernet0/1/7.

c. Configure posture assessment and redirect ACL

```
ip http server
ip http secure-server

ip access-list extended ACL-POSTAUTH-REDIRECT
10 deny tcp any host 192.0.2.255
20 deny tcp any any eq domain
30 deny udp any any eq domain
40 deny udp any any eq bootpc
50 deny udp any any eq bootps
60 permit tcp any any eq www
70 permit tcp any any eq 443
```

d. Configure device tracking

```
!
device-tracking policy tracking_test
 security-level glean
 no protocol ndp
 no protocol dhcp6
 tracking enable
!
interface GigabitEthernet0/1/7
 device-tracking attach-policy tracking_test
```

Note The IP address mentioned belongs to ISE.

The steps you have to perform to add this configuration into the CLI Add-On template on Cisco SD-WAN Manager are documented here.

2. To Configure CoA reauthentication and dACL on ISE:
   a. Create a downloadable ACL and define the ACEs in it.

      ACL name: TEST_IP_PERMIT_ALL

      ACEs: permit ip any any

   b. Create an authorization result and choose the downloadable ACL as dACL.
   c. Navigate to **Administration** > **System** > **Settings** > **Policy Settings**, and in **Policy Sets** configuration select the authorization result as authorization policy.

3. After creating the CLI Add-On template, attach it to a device template and then Cisco SD-WAN Manager pushes all the configuration in the device template onto your device.

Type 6 Passwords on Cisco IOS XE SD-WAN Routers

Table 17: Feature History

Feature Name	Release Information	Description
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 Templates, on page 48.

Overview of Type 6 Passwords

The Type 6 Passwords feature enables secure reversible encryption for authentication, authorization, and accounting (AAA) and Simple Network Management Protocol (SNMP) configurations based on the advanced encryption scheme (AES) algorithm.

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 which you can provide. The encryption algorithm used is advanced encryption scheme (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.

When you create a supported template in Cisco vManage Release 20.4.1 and later releases, by default type 6 passwords are used. Cisco SD-WAN Manager encrypts the passwords and sends the passwords to the router over a secure tunnel. The router then encrypts the passwords into the type 6 format and stores the password on the device. The Type 6 Passwords feature is not supported on Viptela software.

Note Cisco SD-WAN Manager encrypted passwords show up as either 6 or 8. Where as, Cisco IOS XE devices have encryption streams defined as type 0, type 5, type 6, type 8, and so on. On the other hand, Cisco SD-WAN Manager runs on Viptela OS which is based on Linux. Linux uses hashing and encryption schemes. Encrypted passwords on Cisco 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. It is recommended that users don't delete this admin user.

Note We recommend using type 6 passwords to reduce the vulnerability of a malicious attack against password integrity. On upgrading your device to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, all AAA, RADIUS key, and TACACS+ keys are encrypted to type 6.

Supported Platforms

Cisco IOS XE Catalyst SD-WAN devices.

Supported Templates

The following templates support Type 6 passwords:

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

Restrictions

- For SNMP templates, the community name is encrypted by default. Therefore, to upgrade existing SNMP templates to type 6 passwords, delete and re-create the community and trap target.
- When using type 6 passwords with the **keychain key-string** command, the maximum password length for a clear text is 38 characters.

Configure Type 6 Passwords Using Cisco SD-WAN Manager

Upgrade Existing Templates to Type 6 Passwords

To upgrade passwords in your existing templates on Cisco SD-WAN Manager to type 6 passwords, do the following:

Note When you upgrade your routers to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, all supported passwords are automatically upgraded to type 6 passwords.

1. Navigate to **Configuration** > **Templates**
2. Click **Feature Templates**.

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

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

4. Click **Edit**.
5. Click **Save**.

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

Configure Type 6 Passwords Using CLI Add-On Template

You can configure type 6 passwords when using CLI add-on feature templates by doing the following:

1. Navigate to **Configuration** > **Templates**.
2. Click **Feature Templates**.

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

3. Click **Add Template**.
4. Under the Select Devices pane, select the devices for which you are creating the template.
5. Under the Select Template pane, scroll down to the Other Templates section.
6. Click **CLI Add-On Template**. For information on CLI add-on feature templates, see CLI Add-On Feature Templates.
7. Enter a Template Name and Description.
8. Type or paste the CLI that you want to run on your device.
9. Select the plaintext password in the CLI and click the **Encrypt Type 6** button.
10. Click **Save**.

Verify Type 6 Passwords

To verify that your passwords are upgraded to type 6 passwords, you can do one of the following:

- On 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
  ```

  Despite the command displaying 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$`.

- On your device, you can run the following command 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 displays that the password is type 6 and also displays your encrypted password.