

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 , on page 2
- Configure User Login Options, on page 5
- Manage Users, on page 10
- Configure Users Using CLI, on page 10
- Manage a User Group, on page 12
- Creating Groups Using CLI, on page 13
- Ciscotac User Access, on page 14
- Configure Sessions in Cisco SD-WAN Manager, on page 15
- Configuring RADIUS Authentication Using CLI, on page 17
- Configure SSH Authentication, on page 18
- Configure the Authentication Order, on page 19
- Configure NAS Attributes using CLI, on page 21
- Role-Based Access with AAA, on page 23
- Configure AAA Using a Configuration Group, on page 32
- Configuring AAA using Cisco SD-WAN Manager Template, on page 36
- Configuring Password Policy for AAA on Devices, on page 46
- Configuring IEEE 802.1X and IEEE 802.11i Authentication, on page 48

Configure Hardened Passwords

Table 1: Feature History

Feature Name	Release Information	Description
Hardened Passwords	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 SD-WAN Release 20.9.1 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. Click **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 SD-WAN Release 20.9.1, 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		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		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		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 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

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.
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

Field	Description
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

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

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
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

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. Log into the Duo Admin Panel.
2. Create an Auth API application.

   This provides the Duo integration key, secret key, and API hostname information required to complete Duo MFA configuration. Read more about Duo Auth API.
3. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
4. Click **DUO MFA Configuration**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.
5. Click **Enabled**.
6. 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.

7. Click **Save**.
8. 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 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:

```
vEdge(config)# system aaa
vEdge(config)# user username password  password
vEdge(config-aaa)# group group-name
```

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 vEdge 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 vEdge device :

```
vEdge(config)# system aaa admin password  password
```

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:

```
vEdge(config-user-admin)# show config
system
 aaa
  user admin
   password $1$xULc8yYH$k71cTjvKESmeIGgImNDaC.
  !
  user eve
   password $1$8z3q4qoU$F6DMBr9vPBF0s/sl45ax5.
   group    basic
  !
 !
!
```

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

```
vEdge(config)# system aaa radius-servers 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:

```
vEdge(config)# system  aaa usergroup group-name task privilege
```

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**.

In the following example, the **basic** user group has full access to the **system** and **interface** portions of the configuration and operational commands, and the **operator** user group can use all operational commands but can make no modifications to the configuration:

```
vEdge# show running-config system aaa
system
 aaa
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
```

```
  user admin
   password $1$tokPB7tf$vchR2JI9Sw1/dqgkqup9S.
  !
 !
!
```

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 SD-WAN Release 20.3.1 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**.

Set the maximum sessions per user role

You can configure the maximum number of concurrent login sessions for each configured user role. This maximum value applies to all users assigned to that role.

For example, if the “Max user sessions” value for the netadmin role is set to 3, then each user assigned to the netadmin role can have up to 3 concurrent login sessions across the platform. If a fourth session is initiated by one of those users, an error message appears.

Range for “Max user sessions”: 1 to 255. Default: If undefined, there is no limit on the number of concurrent sessions for that role. For government installations, recommended values are 3 sessions for administrative roles and 2 sessions for conventional roles.

The value also applies to CLI sessions.

Change maximum sessions value for a user role

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access** > **Roles**.

   The “Max user sessions value” is displayed for each defined role, including both default and custom roles.
2. Click the role name, edit the **Max user sessions** value, and click **Update**.

Note As of Release 20.18.1, the previous method for changing this value in **Settings** > **Trust and Privacy** is no longer supported. If a "Max user sessions" value has been defined on your system by that method, that value serves as the maximum value for all user roles until changed.

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 vEdge device use RADIUS servers for user authentication, configure one or up to 8 servers:

```
vEdge(config)#  system radius
vEdge(config-radius)# server  ip-address
vEdge(config-server)# secret-key  password
vEdge(config-server)# priority number
vEdge(config-server)# auth-port  port-number
vEdge(config-server#) acct-port port-number
vEdge(config-server)# source-interface interface-name
vEdge(config-server)# tag tag
vEdge(config-server)# vpn vpn-id
```

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 vEdge 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 vEdge device , configure the server's VPN number so that the Cisco vEdge device can locate it. If you configure multiple RADIUS servers, they must all be in the same VPN.

When a Cisco vEdge device is trying to locate a RADIUS server, it goes through the list of servers three times. To change this behavior, use the **retransmit** command, setting the number to a value from 1 to 1000:

```
vEdge(config-radius)# retransmit  number
```

When waiting for a reply from the RADIUS server, a Cisco vEdge 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:

```
vEdge(config-radius)# timeout  seconds
```

Configure SSH Authentication

Table 5: Feature History

Feature Name	Release Information	Description
Secure Shell Authentication Using RSA Keys	Cisco Catalyst SD-WAN Release 19.2.1	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.

Note By default, the SSH service on Cisco vEdge devices is always listening on both ports 22 and 830 on LAN. Cisco vManage uses these ports and the SSH service to perform device management. Due to this, any client machine that uses the Cisco vEdge device for internet access can attempt to SSH to the device. For each of the listening ports, we recommend that you create an ACL to block and/or allow access to Cisco vEdge devices and SSH connections for the listening ports.

Restrictions for SSH Authentication on Cisco Catalyst SD-WAN

- The range of SSH RSA key size supported by Cisco vEdge devices is from 2048 to 4096. SSH RSA key size of 1024and 8192 are not supported.
- A maximum of 10 keys are required on Cisco vEdge devices.

SSH Authentication using vManage on Cisco vEdge Devices

1. In vManage NMS, select the **Configuration ► Templates** screen.
2. In the **Feature Templates** tab, click **Create Template**.

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

3. From the **Device Model** check box, select the type of device for which you are creating the template.

4. From the **Basic Information** tab, choose **AAA** template.
5. From the **Local** section, **New User** section, enter the **SSH RSA Key**. You must enter the complete public key from the id_rsa.pub file in the SSH RSA Key text box.

Configure SSH Authentication using CLI on Cisco vEdge Devices

When a user is created in the **/home/<user>** directory, SSH authentication configures the following parameters:

- Create the .ssh directory with permissions 700
- Create the authorized_keys files in the directory with permission 600

When the public-key is copied and pasted in the key-string, the public key is validated using the **ssh-keygen** utility. The **key-string** and **key-type** fields can be added, updated, or deleted based on your requirement. Similarly, the key-type can be changed.

When a user associated with an SSH directory gets deleted, the **.ssh** directory gets deleted.

Types of Public Keys Supported on Cisco vEdge devices:

- SSH-RSA
- SSH-DSS
- ecdsa-sha2-nistp256
- ecdsa-sha2- nistp384
- ecdsa-sha2-nistp521
- ssh-ed25519

SSH Autentication using CLI

```
vm5(config)# system aaa user ssh-user password vip group tenantadmin
vm5(config-user-ssh-user)# pubkey-chain ssh-usertag key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQDVe2mZGPLkveIgZHWm6cjqsFTyTJcgfPikgsBJDujFMhUlhnWZlh03sIvki29Og2NNSJYM3OCy0TA7pPWvpDDXQw/gD4/
Pb2TH09CRNEChdV0rA6K2fMowOZfmw2PvNRBlOzVlijjQaitd5Dqe7Ar5HGIafLWrVmku9HLQUDZSfeDt8cl/ftgn8sKQOxuTccIpwFhYZkth978Bqm029v8/O5R
BdQOVtT3VBr9NNeC4egutS0yENZeXWBPfrwecd4/aot38plF6jOolDvUjn60CUUOu9TQIaSFg/dFPUB0twtEOIUFMBeimRexT+cI3z8vMlD9tqFRDAI8EUegjU7BP
vm5(config-pubkey-chain-ssh-usertag)# commit
Commit complete.
```

Configure the Authentication Order

The authentication order dictates the order in which authentication methods are tried when verifying user access to a Cisco vEdge 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 local authentication fails, and if you have not configured authentication fallback (with the **auth-fallback** command), the authentication process stops. However, if you have configured authentication fallback,

the authentication process next checks the RADIUS server. For this method to work, you must configure one or more RADIUS servers with the **system radius server** command. If a RADIUS server is reachable, the user is authenticated or denied access based on that server's RADIUS database. If a RADIUS server is unreachable and if you have configured multiple RADIUS 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 RADIUS database.

- 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 vEdge device device is denied.

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

```
Device(config-system-aaa)#  auth-order  (local | radius | tacacs)
```

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):

```
vEdge(config-system-aaa)#  auth-fallback
```

Fallback to a secondary or tertiary authentication mechanism happens when the higher-priority authentication server fails to authenticate a user, either because the credentials provided by the user are invalid or because the server is unreachable.

The following examples illustrate the default authentication behavior and the behavior when authentication fallback is enabled:

- 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.
  - With authentication fallback enabled, local authentication is used when all RADIUS servers are unreachable or when a RADIUS server denies access to a user.
- 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.

- With authentication fallback enabled, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device. In this case, the behavior of two authentication methods is identical.

- 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.
  - With authentication fallback enabled, TACACS+ authentication is used when all RADIUS servers are unreachable or when a RADIUS server denies access a user. Local authentication is used next, when all TACACS+ servers are unreachable or when a TACACS+ server denies access to a user.

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**.

Configure NAS Attributes using CLI

For RADIUS and TACACS+, you can configure Network Access Server (NAS) attributes for user authentication and authorization. To do this, you create a vendor-specific attributes (VSA) file, also called a RADIUS dictionary or a TACACS+ dictionary, on the RADIUS or TACACS+ server that contains the desired permit and deny commands for each user. The Cisco vEdge device retrieves this information from the RADIUS or TACACS+ server.

The VSA file must be named dictionary.viptela, and it must contain text in the following format:

```
localhost$ more dictionary.viptela
 # -*- text -*-
#
```

```
#  dictionary.viptela
#
#
# Version:      $Id$
#

VENDOR          Viptela                         41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name              1    string
```

The Cisco SD-WAN software has three predefined user groups, as described above: **basic**, **netadmin**, and **operator**. These groups have the following permissions:

```
vEdge# show aaa usergroup
GROUP     USERS  TASK       PERMISSION
----------------------------------------
basic     -      system     read
                 interface  read
netadmin  admin  system     read write
                 interface  read write
                 policy     read write
                 routing    read write
                 security   read write
operator  -      system     read
                 interface  read
                 policy     read
                 routing    read
                 security   read
```

To create new user groups, use this command:

```
vEdge(config)# system aaa usergroup
group-name task privilege
```

Here is a sample user configuration on a RADIUS server, which for FreeRADIUS would be in the file "users":

```
user1   Cleartext-password := "user123"
        Service-Type = NAS-Prompt-User,
        Viptela-Group-Name = operator,
```

```
user1   Cleartext-password := "user123"        Service-Type = NAS-Prompt-User,
Viptela-Group-Name = operator,
```

Then in the dictionary on the RADIUS server, add a pointer to the VSA file:

```
$INCLUDE    /usr/share/freeradius/dictionary.viptela
```

For TACACS+, here is a sample configuration, which would be in the file tac_plus.conf:

```
group = test_group {
        default service = permit
        service = ppp protocol = ip {
              Viptela-Group-Name = operator
        }
}
user = user1 {
       pap = cleartext "user123"
       member = test_group
}
```

Note Starting from Cisco vManage Release 20.8.1, the unknown mandatory attributes from TACACS are not allowed. The authorization fails, when a client receives the configurations with the arguments that are not supported. For information about configuring ISE for Cisco SDWAN devices, see RADIUS and TACACS-Based User Authentication and Authorization.

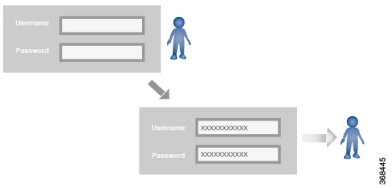
Role-Based Access with AAA

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

- Users are those who are allowed to log in to a Cisco vEdge 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.

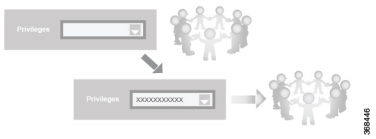
Users and User Groups

All users who are permitted to perform operations on a Cisco vEdge 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 vEdge 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 vEdge 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 vEdge 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 vEdge 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

CLI Command	Any User	Admin User
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
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

CLI Command	Any User	Admin User
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		

Operational Command	Interface	Policy	Routing	Security	System
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
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

Operational Command	Interface	Policy	Routing	Security	System
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	
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				

Operational Command	Interface	Policy	Routing	Security	System
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
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				

Operational Command	Interface	Policy	Routing	Security	System
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				
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		

Configuration Command	Interface	Policy	Routing	Security	System
vpn service			X		
vpn (everything else, including creating, deleting, and naming)					X
wlan	X				

Configure AAA Using a Configuration Group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

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

Step 2 Create and configure a AAA feature in a System profile.

a. Configure users.

Table 6: Local

Field	Description
Enable AAA Authentication	Enable authentication parameters.
Accounting Group	Enable accounting parameters.
Add AAA User	
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.
Password	Enter a password for the user. The password is an MD5 digest string, and it can contain any characters, including tabs, carriage returns, and linefeeds. For more information, see Section 9.4 in RFC 7950, The YANG 1.1 Data Modeling Language. 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.

Field	Description
Confirm Password	Re-enter the password for the user.
Privilege	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.
Add Public Key Chain	
Key String*	Enter the authentication string for a key.
Key Type	Choose **ssh-rsa**.

b. Configure RADIUS servers.

Table 7: RADIUS

Field	Description
Address*	Enter the IP address of the RADIUS server host.
Acct Port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 1 - 65534. Default: 1813
Auth Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. Default: 1812 Range: 1 - 65534
Retransmit	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 3 Range: 0 - 100
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
Key*	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption.
Key Type	Choose Protected Access Credential (PAC) key.

c. Configure TACACS servers.

Table 8: TACACS Server

Field	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: 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.

d. Configure accounting rules.

Table 9: Accounting

Field	Description
Rule Id*	Enter the accounting rule ID.
Method*	Specifies the accounting method list. Choose one of the following: • **commands**: Provides accounting information about specific, individual EXEC commands associated with a specific privilege level. • **exec**: Provides accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times. • **network**: Runs accounting for all network-related service requests. • **system**: Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
Level	Choose the privilege level (1 or 15). Accounting records are generated only for commands entered by users with this privilege level.
Start Stop	Enable this option to 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.

Field	Description
Use Server-group*	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.

e. Configure authorization parameters.

Table 10: Authorization

Field	Description
Server Auth Order*	Choose the authentication order. It 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.
Authorization Console	Enable this option to perform authorization for console access commands.
Authorization Config Commands	Enable this option to perform authorization for configuration commands.
Add Authorization Rule	
Rule Id*	Enter the authorization rule ID.
Method*	Choose **Commands**, which causes commands that a user enters to be authorized.
Level	Choose the privilege level (1 or 15) for commands to be authorized. Authorization is provided for commands entered by users with this privilege level.
If Authenticated	Enable this option to apply the authorization rule parameters only to the authenticated users. If you do not enable this option, the rule is applied to all users.
Use Server-group*	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.

f. Configure 802.1x parameters.

What to do next

Also see Deploy a configuration group .

Configuring AAA using Cisco SD-WAN Manager Template

Table 11: Feature History

Feature Name	Release Information	Description
Authorization and Accounting	Cisco SD-WAN Release 20.5.1 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 vEdge device s.

Cisco vEdge device s 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_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 12:

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 vEdge 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 vEdge 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 Authentication Order and Fallback

You can configure the authentication order and authentication fallback 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. Fallback provides a mechanism for authentication is the user cannot be authenticated or if a RADUS or TACACS+ server is unreachable.

To configure AAA authentication order and authentication fallback on a Cisco vEdge device, select the **Authentication** tab and configure the following parameters:

Table 13:

Parameter Name	Description
Authentication Order	The default order is local, then radius, and then tacacs. To change the default order of authentication methods that the software tries when verifying user access to a Cisco vEdge device: **1.** Click the drop-down arrow to display the list of authentication methods. **2.** In the list, click the up arrows to change the order of the authentication methods and click the boxes to select or deselect a method. If you select only one authentication method, it must be **local**.
Authentication Fallback	Click On to configure authentication to fall back from RADIUS or TACACS+ to the next priority authentication method if the user cannot be authenticated or if the RADIUS or TACACS+ servers are unreachable. With the default configuration (Off), authentication falls back only if the RADIUS or TACACS+ servers are unreachable.
Admin Authentication Order	Have the "admin" user use the authentication order configured in the Authentication Order parameter. If you do not configure the admin authentication order, the "admin" user is always authenticated locally.
Disable Netconf Logs	Click On to disable the logging of Netconf events. By default, these events are logged to the auth.info and messages log files.
Disable Audit Logs	Click On to disable the logging of AAA events. By default, these events are logged to the auth.info and messages log files.
RADIUS Server List	List the tags for one or two RADIUS servers. Separate the tags with commas. You set the tag under the RADIUS tab.

CLI equivalent:

```
system
   aaa
 admin-auth-order  auth-fallback  auth-order  (local | radius | tacacs)
    logs
     [no] audit-disable
     [no] netconf-disable
    radius-servers tag
```

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 14:

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. **Note** From Cisco Catalyst SD-WAN Manager Release 20.18.1, the character limit for local user accounts remains restricted to 32 characters. However, for TACACS users, usernames extend up to 128 characters.
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.
Description	Enter a description for the user.
User Groups	Select from the list of configured groups. You must assign the user to at least one group. The admin user is automatically placed in the netadmin group and is the only member of this group.
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 10 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 15:

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 Preset list in 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. The Custom list in the feature table lists the authorization tasks that you have created (see "Configure Authorization). To associate a task with this user group, choose **Read**, **Write**, or both options. The **Read** option grants to users in this user group read authorization to XPaths as defined in the task. The **Write** option allows users in this user group write access to XPaths as defined in the task.

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.

CLI equivalent:

```
system
  aaa
    user username
     group group-name
     password password usergroup group-name
     task (interface | policy | routing | security | system) (read | write)
```

Configuring RADIUS Authentication

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

To configure RADIUS authentication, select **RADIUS** and configure the following parameters:

Table 16:

Parameter Name	Description
Retransmit Count	Specify how many times to search through the list of RADIUS servers while attempting to locate a server. *Range:* 1 through 1000 *Default:* 3
Timeout	Specify how long to wait to receive a reply form the RADIUS server before retransmitting a request. *Range:* 1 through 1000 *Default:* 5 seconds

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

Table 17:

Parameter Name	Description
Address	Enter the IP address of the RADIUS server host.
Tag	Enter a text string to identify the RADIUS server. The tag can be 4 to 16 characters long. The tag allows you to configure authentication for AAA, IEEE 802.1X, and IEEE 802.11i to use a specific RADIUS server or servers. For Cisco vEdge devices running Cisco Catalyst SD-WAN software, this field is ignored.
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.
Key	This field is deprecated. Use the Secret Key field instead.
Secret Key	Enter the key the Cisco vEdge 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.
Source Interface	Enter the name of the interface on the local device to use to reach the RADIUS server.
VPN ID	Enter the number of the VPN in which the RADIUS server is located or through which the server can be reached. If you configure multiple RADIUS servers, they must all be in the same VPN.
Priority	Enter the priority of a RADIUS server. A server with a lower number is given priority. *Range:* 0 through 7. *Default:* 0

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:

```
system  radius
   retransmit number
   server ip-address
     acct-port port-number
     auth-port port-number
     priority number
     secret-key key
     source-interface interface-name
     tag tag
     vpn vpn-id
   timeout seconds
```

Configuring TACACS+ Authentication

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

To configure the device to use TACACS+ authentication, select **TACACS** and configure the following parameters:

Table 18:

Parameter Name	Description
Timeout	Enter how long to wait to receive a reply from the TACACS+ server before retransmitting a request. *Range:* 1 through 1000*Default:* 5 seconds
Authentication	Set the type of authentication to use for the server password. The default authentication type is PAP. You can change it to ASCII.

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

Table 19:

Parameter Name	Description
Address	Enter the IP address of the TACACS+ server host.
Authentication 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
Key (Deprecated)	This field is deprecated. Use the Secret Key field instead.

Parameter Name	Description
Secret Key	Enter the key the Cisco vEdge 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.
Source Interface	Enter the name of the interface on the local device to use to reach the TACACS+ server.
VPN ID	VPN in which the TACACS+ server is located or through which the server can be reached. If you configure multiple TACACS+ servers, they must all be in the same VPN.
Priority	Set the priority of a TACACS+ server. A server with lower priority number is given priority over one with a higher number.*Range:* 0 through 7*Default:* 0

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.

CLI equivalent:

```
system  tacacs
   authentication password-authentication
   server ip-address
     auth-port port-number
     priority number
     key key
     source-interface interface-name
     vpn vpn-id
   timeout seconds
```

Configure Authorization and Accounting

Table 20: Feature History

Feature Name	Release Information	Description
Authorization and Accounting	Cisco SD-WAN Release 20.5.1 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.

Restrictions to Configure Authorization and Accounting

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

- If you enter a configuration and press enter before selecting a value from an enumeration, the CLI presents a choice sub-menu. In this scenario, the final chosen value is not sent for authorization.
- The load merge and load override commands are not available when authorization is configued.

- The individual commands configured via load or rollback are not authorized or accounted.

Configuring Authorization

You can configure authorization, which causes the device to authorize commands that users enter on a device before the commands can be executed.

Configuring authorization involves creating one or more tasks. A task consists of a set of operational commands and a set of configuration commands. Operational commands are show commands and exec commands. Configuration commands are the XPath of configuration commands.

You define the default user authorization action for each command type. The default action can be accept or deny. You also can define user authorization accept or deny actions for individual commands or for XPath strings within a command type. In this way, you can override the default action for specific commands as needed.

A task is mapped to a user group, so all users in the user group are granted the authorizations that the command sets in the task define.

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

Table 21:

Parameter Name	Description
Name	Enter a unique name for the task
+ Add Oper	Click to add a set of operational commands. In the Add Oper window that pops up: **1.** From the **Default action** drop-down list, choose the default authorization action for operational commands. Choose **accept** to grant user authorization by default, or choose **deny** to prevent user authorization by default. **2.** To designate specific operational commands for which user authorization is granted or denied authorization, click **+ Add Oper** to expand the Add Oper area. In the **Oper** field that displays, click **accept** to grant user authorization for a command, or click **deny** to prevent user authorization for a command, and enter the command in the **CLI** field. Then click **Add** in the Add Oper area. Do not include quotes or a command prompt when entering a command. For example, **config terminal** is a valid entry, but **"config terminal"** is not valid. Repeat this Step 2 as needed to designate other commands. The actions that you specify here override the default action. In this way, you can designate specific commands that are not authorized when the default action is accept, and designate specific commands that are authorized when the default action is deny. To remove a specific command, click the trash icon on the right side of its line in the table at the bottom of the Add Oper window. **3.** Click **Add** at the bottom right of the Add Oper window.

Parameter Name	Description
+ Add Config	Click to add a set of XPath strings for configuration commands. In the Add Config window that pops up: **1.** From the **Default action** drop-down list, choose the default authorization action for configuration commands. Choose **accept** to grant user authorization by default, or choose **deny** to prevent user authorization by default. **2.** To designate specific configuration command XPath strings for which user is granted or denied authorization **Click + Add Config** to expand the Add Config area. In the **Config** field that displays, click **accept** to grant user authorization for an XPath, or click **deny** to prevent user authorization for an XPath, and enter the XPath string in the **CLI** field. Then click **Add** in the Add Config area. To display the XPath for a device, enter the **`show running-config | display xpath`** command on the device. Do not include quotes or a command prompt when entering an XPath string. Repeat this Step 2 as needed to designate other XPath strings. The actions that you specify here override the default action. In this way, you can designate specific XPath strings that are not authorized when the default action is accept, and designate specific XPath strings that are authorized when the default action is deny. To remove a specific command, click the trash icon on the right side of its line in the table at the bottom of the Add Config window. **3.** Click **Add** at the bottom right of the Add Config window.

To remove a task, click the trash icon on the right side of the task line.

After you create a tasks, perform these actions:

- Create or update a user group. Use the Custom feature type to associate one or more tasks with the user group by assigning read, write, or both privileges to each task. See Configure Local Access for Users and User Groups.

Note A user group can be associated with either a predefined task or with user-defined tasks. Associating a user group with a combination of both predefined and user-defined tasks is not supported.

- Add users to the user group. These users then receive the authorization for operational and configuration commands that the tasks that are associated with the user group define. See Configure Local Access for Users and User Groups.

  If a user is attached to multiple user groups, the user receives the authorization access that is configured for the last user group that was created.

CLI equivalent:

```
system aaa
   accounting
```

```
task name
  config
    default-action {accept | deny}
    accept "xpath"
    deny "xpath"
  oper-exec
    default-action {accept | deny}
    accept "command"
    deny ""command-id
usergroup group-name
  task authorization-task {read | write}
```

Configuring Accounting

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

Note Accounting does not generate a record of CLI commands for Cisco SD-WAN Manager template configuration.

Prerequisites

- The TACACS+ server must be configured with a secret key on the **TACACS** tab
- The TACACS+ server must be configured as first in the authentication order on the **Authentication** tab

To configure accounting, choose the **Accounting** tab and configure the following parameter:

Table 22:

Parameter Name	Description
Enable/disable user accounting	Click **On** to enable the accounting feature. Click **Off** to disable this feature.

CLI equivalent:

```
system  aaa
   accounting
```

Configuring Password Policy for AAA on Devices

In Cisco vManage Release 20.4.1, you can create password policies using Cisco AAA on Cisco vEdge devices. We recommend configuring a password policy to ensure that all users or users of a specific group are prompted to use strong passwords. You can customize the password policy to meet the requirements of your organization.

Note You can only configure password policies for Cisco AAA using device CLI templates.

You can configure the following parameters:

password-policy min-password-length *length*	The minimum allowed length of a password. You can specify between 8 to 32 characters.
password-policy num-lower-case-characters *number-of-lower-case-characters*	The minimum number of lower case characters. You can specify between 1 to 128 characters.
password-policy num-numeric-characters *number-of-numeric-characters*	The minimum number of numeric characters. You can specify between 1 to 128 characters.
password-policy num-special-characters *number-of-special-characters*	The minimum number of special characters. You can specify between 1 to 128 characters.
password-policy num-upper-case-characters *number-of-upper-case-characters*	The minimum number of upper case characters. You can specify between 1 to 128 characters.

Configure Password Policies Using Cisco vManage

Table 23: Feature History

Feature Name	Release Information	Description
Support for Password Policies using Cisco AAA	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	This feature allows you to create password policies for Cisco AAA. Password policies ensure that your users use strong passwords and can be customized based on your requirements. To configure password policies, push the `password-policy` commands to your device using Cisco SD-WAN Manager device CLI templates. For more information on the `password-policy` commands, see the `aaa` command reference page.

Configure password policies for Cisco AAA by doing the following:

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

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

3. Click **Create Template**.
4. Click **CLI Template**.
5. From the **Device Model** drop-down list, choose your Cisco vEdge device.
6. Enter a **Template Name**.

7. Enter a **Description**.
8. (Optional) From the **Load Running config from reachable device:** drop-down list, choose a device from which to load the running configuration.
9. Enter or append the password policy configuration.

   For more information on the `password-policy` commands, see the `aaa` command reference page.
10. Click **Add**.

    The device templates page appears.
11. Attach the templates to your devices as described in Attach a Device Template to Devices.

Configuring IEEE 802.1X and IEEE 802.11i Authentication

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

IEEE 802.11i prevents unauthorized network devices from gaining access to wireless networks (WLANs). 802.11i implements WiFi Protected Access II (WPA2) to provide authentication for devices that want to connect to a WLAN on a Cisco vEdge 100wm device.

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

This section describes how to configure RADIUS servers to use for 802.1X and 802.11i authentication. It describes how to enable 802.1X on Cisco vEdge device interfaces to have the router act as an 802.1X authenticator, responsible for authorizing or denying access to network devices on a WAN.

It also describes how to enable 802.11i on Cisco vEdge 100wm device routers to control access to WLANs.

It describes how to enable IEEE 802.1X and AAA on a port, and how to enable IEEE 802.1X RADIUS accounting.

Configure RADIUS Authentication Servers

Authentication services for IEEE 802.1X and IEEE 802.11i are provided by RADIUS authentication servers. You configure the RADIUS servers to use for 802.1X and 802.11i authentication on a system-wide basis:

```
vEdge(config)#  system radius
 vEdge(config-radius)# server ip-address
```

Specify the IP address of the RADIUS server. You can configure one or two RADIUS servers to perform 802.1X and 802.11i authentication. (Note that for AAA authentication, you can configure up to eight RADIUS servers.)

For each RADIUS server, you can configure a number of optional parameters.

You can configure the VPN through which the RADIUS server is reachable and the router interface to use to reach the server:

```
vEdge(config-server)# vpn vpn-id
vEdge(config-server)# source-interface interface-name
```

If you configure two RADIUS servers, they must both be in the same VPN, and they must both be reachable using the same source interface.

You must configure a tag to identify the RADIUS server:

```
vEdge(config-server)# tag tag
```

The tag can be from 4 through 16 characters. You use this tag when configuring the RADIUS servers to use with IEEE 802.1X authentication and with IEEE 802.11i WPA enterprise authentication.

For authentication between the router and the RADIUS server, you can authenticate and encrypt packets sent between the Cisco vEdge device and the RADIUS server, and you can configure a destination port for authentication requests. To authenticate and encrypt packets, configure a key:

```
vEdge(config-server)# secret-key password
```

Enter the password as clear text, which is immediately encrypted, or as an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.

By default, UDP port 1812 is used as the destination port on the RADIUS server to use for authentication requests. You can change the port number to a number from 1 through 65535. To disable authentication, set the port number to 0.

```
vEdge(config-server)# auth-port number
```

You can set the priority of a RADIUS server, to choose which one to use first when performing 802.1X authentication:

```
vEdge(config-server)# priority number
```

The priority can be a value from 0 through 7. The server with the lower priority number is given priority. If you do not include this command in the RADIUS server configuration, the priority is determined by the order in which you enter the IP addresses in the **system radius server** command.

By default, accounting in enabled for 802.1X and 802.11i interfaces. Accounting information is sent to UDP port 1813 on the RADIUS server. To change this port:

```
vEdge(config-server)# acct-port number
```

The port number can be from 1 through 65535.

Configure IEEE 802.1X Port Security

To enable basic 802.1X port security on an interface, configure it and at least one RADIUS server to use for 802.1X authentication. The 802.1X interface must be in VPN 0.

```
vEdge(config)# vpn 0
interface interface-name
vEdge(config-interface)#  dot1x
vEdge(config-dot1x)#  radius-servers tag
```

For 802.1X authentication to work, you must also configure the same interface under an untagged bridge:

```
vEdge(config)#  bridge number
vEdge(config)# interface interface-name
```

The interface name in the **vpn 0 interface** and **bridge interface** commands must be the same. Do not configure a VLAN ID for this bridge so that it remains untagged.

You can enable 802.1X on a maximum of four wired physical interfaces. The interface cannot also be configured as a tunnel interface.

Configure the tags associated with one or two RADIUS servers to use for 802.1X client authentication and accounting. (You configure the tags with the **system radius server tag** command.) If you specify tags for two RADIUS servers, they must both be reachable in the same VPN. If you do not configure a priority value when you configure the RADIUS server with the **system radius server priority** command, the order in which you list the IP addresses is the order in which the RADIUS servers are tried.

Enable RADIUS Accounting

By default, the Cisco vEdge device never sends interim accounting updates to the 802.1X RADIUS accounting server. Accounting updates are sent only when the 802.1X session ends.

To enable the sending of interim accounting updates, configure the interval at which to send the updates:

```
vEdge(config-dot1x)#  accounting-interval seconds
```

The time can be from 0 through 7200 seconds.

Enable MAC Authentication Bypass

IEEE 802.1X authentication is accomplished through an exchange of Extensible Authentication Procotol (EAP) packets. After 802.1X-compliant clients respond to the EAP packets, they can be authenticated and granted access to the network. Enabling MAC authentication bypass (MAB) provides a mechanism to allow non-802.1X–compliant clients to be authenticated and granted access to the network.

The Cisco vEdge device determines that a device is non-802.1X–compliant clients when the 802.1X authentication process times out while waiting for an EAPOL response from the client.

To enable MAC authentication bypass for an 802.1X interface on the Cisco vEdge device :

```
vEdge(config)# vpn 0 interface interface-name dot1x
vEdge(config-dot1x)# mac-authentication-bypass
```

With this configuration, the Cisco vEdge device authenticates non-802.1X–compliant clients using the configured RADIUS servers. The RADIUS server must be configured with the MAC addresses of non-802.1X–compliant clients that are allowed to access the network.

To enable MAB on the RADIUS server:

```
vEdge(config-dot1x)# mac-authentication-bypass server
```

To allow authentication to be performed for one or more non-802.1X–compliant clients before performing an authentication check with the RADIUS server, list their MAC addresses in the following command:

```
vEdge(config-dot1x)# mac-authentication-bypass allow mac-addresses
```

You can configure up to eight MAC addresses for MAC authentication bypass. For these devices, the Cisco vEdge device grants immediate network access based on their MAC addresses, and then sends a request to the RADIUS server to authenticate the devices.

Configure VLANs for Authenticated and Unauthenticated Clients

For clients that cannot be authenticated but that you want to provide limited network services to, you create VLANs to handle network access for these clients. You also create VLANs to handle authenticated clients.

You can create the following kinds of VLAN:

- Guest VLAN—Provide limited services to non-802.1X–compliant clients.
- Authentication Reject VLAN—Provide limited services to 802.1X-compliant clients that failed RADIUS authentication. An authentication-reject VLAN is similar to a restricted VLAN.

- Authentication Fail VLAN—Provide network access when RADIUS authentication or the RADIUS server fails. An authentication-fail VLAN is similar to a critical VLAN.
- Default VLAN—Provide network access to 802.1X–compliant clients that are successfully authenticated by the RADIUS server. If you do not configure a default VLAN on the Cisco vEdge device , successfully authenticated clients are placed into VLAN 0, which is the VLAN associated with an untagged bridge.

To configure the VLANs for authenticated and unauthenticated clients, first create the VLAN in a bridging domain, and then create the 802.1X VLANs for the unauthenticated clients by associating the bridging domain VLAN with an 802.1X VLAN.

To create the VLAN, configure a bridging domain to contain the VLAN:

```
vEdge(config)# bridge bridge-id
vEdge(config-bridge)# name text
vEdge(config-bridge)# vlan vlan-id
vEdge(config-bridge)# interface interface-name
vEdge(config-interface)# no shutdown
```

The bridging domain identifier is a number from 1 through 63. A best practice is to have the bridge domain ID be the same as the VLAN number.

The name is optional, but it is recommended that you configure a name that identifies the 802.1X VLAN type, such as Guest-VLAN and Default-VLAN.

The VLAN number can be from 1 through 4095. This is the number that you associate with an 802.1X VLAN.

The interface name is the interface that is running 802.1X.

Then configure the 802.1X VLANs to handle unauthenticated clients.

A guest VLAN provides limited services to non-802.1X–compliant clients, and it can be used to allow clients to download 802.1X client software. An interface running 802.1X assigns clients to a guest VLAN when the interface does not receive a response to EAP request/identity packets that it has sent to the client, or when the client does not send EAPOL packets and MAC authentication bypass is not enabled. To configure a guest VLAN:

```
vEdge(config)# vpn 0 interface interface-name interface dot1x
vEdge(config-dot1x)# guest-vlan vlan-id
```

The VLAN number must match one of the VLANs you configured in a bridging domain. A best practice is to have the VLAN number be the same as the bridge domain ID.

An authentication-reject VLAN provides limited services to 802.1X-compliant clients that have failed RADIUS authentication. To configure an authentication-reject VLAN:

```
vEdge(config-dot1x)# auth-reject-vlan vlan-id
```

The VLAN number must match one of the VLANs you configure in a bridging domain. A best practice is to have the VLAN number be the same as the bridge domain ID.

When the RADIUS authentication server is not available, 802.1X-compliant clients attempting to authenticate are placed in an authentication-fail VLAN if it is configured. If this VLAN is not configured, the authentication request is eventually dropped. To configure the authentication-fail VLAN:

```
vEdge(config-dot1x)#  auth-fail-vlan vlan-id
```

The VLAN number must match one of the VLANs you configure in a bridging domain. A best practice is to have the VLAN number be the same as the bridge domain ID.

The following configuration snippet illustrates the interrelationship between the 802.1X configuration and the bridging domain configuration. This snippet shows that the bridging domain numbers match the VLAN

numbers, which is a recommended best practice. Also, the bridging domain name identifies the type of 802.1X VLAN.

```
system
 ...
 radius
  server 10.1.15.150
   tag              freerad1
   source-interface ge0/0
   secret-key       $4$L3rwZmsIic8zj4BgLEFXKw==
   priority         1
  exit
  server 10.20.24.150
   auth-port        2000
   acct-port        2001
   tag              freerad2
   source-interface ge0/4
   secret-key       $4$L3rwZmsIic8zj4BgLEFXKw==
   priority         2
  exit
 !
!
bridge 1
 name Untagged_bridge
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
bridge 10
 name Authorize_VLAN
 vlan 10
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
bridge 20
 name Guest_VLAN
 vlan 20
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
bridge 30
 name Critical_VLAN
 vlan 30
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
bridge 40
 name Restricted_VLAN
 vlan 40
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
vpn 0
 interface ge0/0
  ip address 10.1.15.15/24
```

```
  tunnel-interface
   encapsulation ipsec
   ...
  !
  no shutdown
 !
 interface ge0/1
  ip address 60.0.1.16/24
  no shutdown
 !
 interface ge0/2
  ip address 10.1.19.15/24
  no shutdown
 !
 interface ge0/4
  ip address 10.20.24.15/24
  no shutdown
 !
 interface ge0/5
  dot1x
   auth-reject-vlan 40
   auth-fail-vlan   30
   guest-vlan       20
   default-vlan     10
   radius-servers   freerad1
  !
  no shutdown
 !
 interface ge0/7
  ip address 10.0.100.15/24
  no shutdown
 !
!
vpn 1
 interface ge0/2.1
  ip address 10.2.19.15/24
  mtu      1496
  no shutdown
 !
 interface irb1
  ip address 56.0.1.15/24
  mac-address 00:00:00:00:aa:01
  no shutdown
  dhcp-server
   address-pool 56.0.1.0/25
   offer-time   600
   lease-time   86400
   admin-state  up
   options
    default-gateway 56.0.1.15
   !
  !
 !
!
vpn 10
 interface ge0/2.10
  ip address 10.10.19.15/24
  mtu      1496
  no shutdown
 !
 interface irb10
  ip address 56.0.10.15/24
  mac-address 00:00:00:00:aa:10
  no shutdown
```

```
  dhcp-server
   address-pool 56.0.10.0/25
   offer-time   600
   lease-time   86400
   admin-state  up
   options
    default-gateway 56.0.10.15
   !
  !
 !
!
vpn 20
 interface ge0/2.20
  ip address 10.20.19.15/24
  mtu      1496
  no shutdown
 !
 interface irb20
  ip address 56.0.20.15/24
  mac-address 00:00:00:00:aa:20
  no shutdown
 !
!
vpn 30
 interface ge0/2.30
  ip address 10.30.19.15/24
  mtu      1496
  no shutdown
 !
 interface irb30
  ip address 56.0.30.15/24
  mac-address 00:00:00:00:aa:30
  no shutdown
 !
!
vpn 40
 interface ge0/2.40
  ip address 10.40.19.15/24
  mtu      1496
  no shutdown
 !
 interface irb40
  ip address 56.0.40.15/24
  mac-address 00:00:00:00:aa:40
  no shutdown
 !
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
!
```

Configure Control Direction

To configure how the 802.1X interface handles traffic when the client is unauthorized, set the control direction:

```
vEdge(config-dot1x)#  control-direction  (in-and-out | in-only)
```

The direction can be one of the following:

- **in-and-out**—The 802.1X interface can both send packets to and receive packets from the authorized client. Bidirectional control is the default behavior.

- **in-only**—The 802.1X interface can send packets to the unauthorized client, but cannot receive packets from that client.

Configure Authentication with Wake on LAN

IEEE 802.1X authentication wake on LAN (WoL) allows dormant clients to be powered up when the Cisco vEdge device receives a type of Ethernet frame called the magic packet. Administrators can use wake on LAN when to connect to systems that have been powered down.

When a client that uses wake on LAN and that attaches through an 802.1X port powers off, the 802.1X port becomes unauthorized. The port can only receive and send EAPOL packets, and wake-on-LAN magic packets cannot reach the client. When the device is powered off, it is not authorized, and the switch port is not opened.

Without wake on LAN, when an 802.1X port is unauthorized, the router's 802.1X interface block traffic other than EAPOL packets coming from unauthorized clients.

When you enable wake on LAN on an 802.1X port, the Cisco vEdge device is able to send magic packets even if the 802.1X port is unauthorized.

To enable wake on LAN on an 802.1X interface, use the following command:

```
vEdge(config)# vpn 0 interface interface-name dot1x
vEdge(config-dot1x)#  wake-on-lan
```

Configure 802.1X Host Mode

The host mode of an 802.1X interfaces determines whether the interface grants access to a single client or to multiple clients. Three host modes are available:

- Single-host mode—The 802.1X interface grants access only to the first authenticated client. All other clients attempting access are denied and dropped.
- Multiple-host mode—A single 802.1X interface grants access to multiple clients. In this mode, only one of the attached clients must be authorized for the interface to grant access to all clients. If the interface becomes unauthorized, the Cisco vEdge device denies network access to all the attached clients.
- Multiple-authentication mode—A single 802.1X interface grants access to multiple authenticated clients on data VLANs.

To configure the host mode of the 802.1X interface, use the following command:

```
vEdge(config)# vpn 0 interface interface-name dot1x
vEdge(config-dot1x)#  host-mode  (multi-auth | multi-host | single-host)
```

Set the Timeout for Inactive Clients

By default, when a client has been inactive on the network for 1 hour, its authentication is revoked, and the client is timed out. To change the timeout interval, use the following command:

```
vEdge(config)# vpn 0 interface interface-name dot1x
vEdge(config-dot1x)#  timeout inactivity minutes
```

The timeout interval can be from 0 through 1440 minutes (24 hours).

Enable Periodic Client Reauthentication

By default, once a client session is authenticated, that session remains functional indefinitely. To enable the periodic reauthentication of 802.1X clients, configure the number of minutes between reauthentication attempts:

```
vEdge(config)# vpn 0 interface interface-name dot1x
vEdge(config-dot1x)#  reauthentication minutes
```

The time can be from 0 through 1440 minutes (24 hours)

Configure Dynamic Authorization Service for RADIUS Change of Authorization

Dynamic authorization service (DAS) allows an 802.1X interface on a Cisco vEdge device to accept change of authorization (CoA) requests from a RADIUS or other authentication server and to act on the requests. The Cisco Catalyst SD-WAN implementation of DAS supports disconnect packets, which immediately terminate user sessions, and reauthentication CoA requests, which modify session authorization attributes.

DAS, defined in RFC 5176 , is an extension to RADIUS that allows the RADIUS server to dynamically change 802.1X session information without requiring the Cisco vEdge device to initiate the change request. When you enable DAS on the Cisco vEdge device , the router opens a socket to listen for CoA requests from the RADIUS server. If the network administrator of a RADIUS server modifies the authentication of an 802.1X client, the RADIUS server sends a CoA request to inform the router about the change of authorization. When the router receives the CoA request, it processes the requested change.

To enable DAS for an 802.1X interface, you configure information about the RADIUS server from which the interface can accept CoA requests. In the context of configuring DAS, the Cisco vEdge device is the server and the RADIUS server (or other authentication server) is the client.

To configure the RADIUS server from which to accept CoA requests, configure the server's IP address and the password that the RADIUS server uses to access the router's 802.1X interface:

```
vEdge(config)# vpn 0 interface interface-name dot1x
vEdge(config-dot1x)#  das
vEdge(config-das)# client ip-address
vEdge(config-das)# secret-key password
```

You can configure the VPN through which the RADIUS server is reachable:

```
vEdge(config-das)# vpn vpn-id
```

By default, the 802.1X interface uses UDP port 3799 to listen for CoA request from the RADIUS server. You can change the port number:

```
vEdge(config-das)# port port-number
```

The port number can be a value from 1 through 65535. If you configure DAS on multiple 802.1X interfaces on a Cisco vEdge device , you must configure each interface to use a different UDP port.

By default, the CoA requests that the Cisco vEdge device receives from the DAS client are all honored, regardless of when the router receives them. To have the router handle CoA within a specified time, you require that the DAS client timestamp all CoA requests:

```
vEdge(config-das)# require-timestamp
```

With this configuration, the Cisco vEdge device processes only CoA requests that include an event timestamp. Non-timestamped CoA requests are dropped immediately.

When timestamping is configured, both the Cisco vEdge device and the RADIUS server check that the timestamp in the CoA request is current and within a specific time window. The default time window is 300 seconds (5 minutes). This behavior means that if the DAS timestamps a CoA at 15:00 and the router receives it at 15:04, the router honors the request. However, if the router receives the request at 15:10, the router drops the CoA request. You can change the time window to a time from 0 through 1000 seconds:

```
vEdge(config-das)# time-window seconds
```

Configure RADIUS Authentication and Accounting Attributes

For IEEE 802.1X authentication and accounting, the Cisco vEdge device , acting as a network access server (NAS), sends RADIUS attribute–value (AV) pairs to the RADIUS server. These AV pairs are defined in RFC 2865 , RADIUS, RFC 2866 , RADIUS Accounting, and RFC 2869 , RADIUS Extensions. The AV pairs are placed in the Attributes field of the RADIUS packet.

By default, when you enable IEEE 802.1X port security, the following authentication attributes are included in messages sent to the RADIUS server:

Attribute Number	Attribute Name	Description
1	User-Name	Name of the user to be authenticated.
5	NAS-Port	Physical port number on the Cisco vEdge device that is authenticating the user.
12	Framed-MTU	Maximum MTU configured for the user.
30	Called-Station-Id	Phone number that the user called, using dialed number identification (DNIS) or similar technology used to access the RADIUS server.
31	Calling-Station-Id	Phone number that the call came in to the server, using automatic number identification (ANI) or similar technology.
44	Acct-Session-Id	Unique session identifier.
61	NAS-Port-Type	Type of physical port on the Cisco vEdge device that is authenticating the user.
77	Connect-Info	Nature of the user's connection.
79	EAP-Message	Encapsulate Extended Access Protocol (EAP) packets, to allow the Cisco vEdge device to authenticate dial-in users via EAP without having to run EAP.
80	Message-Authenticator	Sign RADIUS Access-Requests to prevent these requests from being spoofed by ARAP, CHAP, or EAP.

When you enable RADIUS accounting, the following accounting attributes are included, by default, in messages sent to the RADIUS server:

Attribute Number	Attribute Name	Description
1	User-Name	Name of the user to be authenticated.
5	NAS-Port	Physical port number on the Cisco vEdge device that is authenticating the user.
30	Called-Station-Id	Phone number that the user called, using dialed number identification (DNIS) or similar technology used to access the RADIUS server.

Attribute Number	Attribute Name	Description
31	Calling-Station-Id	Phone number that the call came in to the server, using automatic number identification (ANI) or similar technology.
40	Acct-Status-Type	Mark the beginning and end of an accounting request.
44	Acct-Session-Id	Unique accounting identifier used to match the start and stop records in a log file.
45	Acct-Authentic	How the user was authenticated.
61	NAS-Port-Type	Type of physical port on the Cisco vEdge device that is authenticating the user.
77	Connect-Info	Nature of the user's connection.

Several configuration commands allow you to add additional attribute information to RADIUS packets.

To include the NAS-IP-Address (attribute 4) in messages sent to the RADIUS server to indicate the IP address of the Cisco vEdge device that is acting as a NAS server:

```
vEdge(config-dot1x)  nas-ip-address ip-address
```

To include the NAS-Identifier (attribute 32) in messages sent to the RADIUS server, use the following command:

```
vEdge(config-dot1x)#  nas-identifier string
```

The NAS identifier is a unique string from 1 through 255 characters long that identifies the Cisco vEdge device that is acting as a NAS server.

To include a RADIUS authentication or accounting attribute of your choice in messages sent to the RADIUS server, use the following commands:

```
vEdge(config-dot1x)#  auth-req-attr attribute-number (integer integer | octet
octet | string string)
vEdge(config-dot1x)#  acct-req-attr attribute-number (integer integer | octet
octet | string
string)
```

Specify the desired value of the attribute as an integer, octet value, or string, depending on the attribute. For example, to set the Service-Type attribute to be authenticate-only:

```
vEdge(config-dot1x)# auth-req-attr 6 integer 8
```

Configure IEEE 802.11i Authentication

For Cisco vEdge device that support wireless LANs (WLANs), you can configure the router to support either a 2.4-GHz or 5-GHz radio frequency. Then, you segment the WLAN into multiple broadcast domains, which are called virtual access points, or VAPs. Users who connect to a VAP can be unauthenticated, or you can configure IEEE 802.11i authentication for each VAP.

For information about configuring the WLAN interface itself, see *Configuring WLAN Interfaces* .

To enable user authentication on the WLAN, you create a VAP on the desired radio frequency and then you configure Wi-Fi protected access (WPA) or WPA2 data protection and network access control for the VAP. WPA authenticates individual users on the WLAN using a username and password. WPA uses the Temporal

Key Integrity Protocol (TKIP), which is based on the RC4 cipher. WPA2 implements the NIST FIPS 140-2–compliant AES encryption algorithm along with IEEE 802.1X-based authentication, to enhance user access security over WPA. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is based on the AES cipher. Authentication is done either using preshared keys or through RADIUS authentication.

To enable personal authentication, which requires users to enter a password to connect to the WLAN, configure the authentication and password:

```
vEdge(config)#  wlan frequency
vEdge(config-wlan)# interface vap number
vEdge(config-vap)# no shutdown
vEdge(config-vap)#  data-security  (wpa-personal | wpa/wpa2-personal | wpa2-personal)
vEdge(config-vap)#  wpa-personal-key password
```

For the security, configure either WPA, WPA2, or both (WPA/WPA2). Enter the password either as clear text or an AES-encrypted key.

For each VAP, you can customize the security mode to control wireless client access.

To enable enterprise WPA security, configure the authentication and the RADIUS server to perform the authentication:

```
vEdge(config-vap)# data-security (wpa-enterprise | wpa/wpa2-enterprise | wpa2-enterprise)
vEdge(config-vap)#  radius-servers tag
```

For the security, configure either WPA, WPA2, or both (WPA/WPA2). Enter the password either as clear text or an AES-encrypted key.

In the **radius-servers** command, enter the tags associated with one or two RADIUS servers to use for 802.11i authentication. (You configure the tags with the **system radius server tag** command.) If you specify tags for two RADIUS servers, they must both be reachable in the same VPN. If you do not configure a priority value when you configure the RADIUS server with the **system radius server priority** command, the order in which you list the IP addresses is the order in which the RADIUS servers are tried.

By default, management frames sent on the WLAN are not encrypted. For each VAP, you can configure the encryption to be optional or required:

```
vEdge(config-vap)#  mgmt-security  (none | optional | required)
```