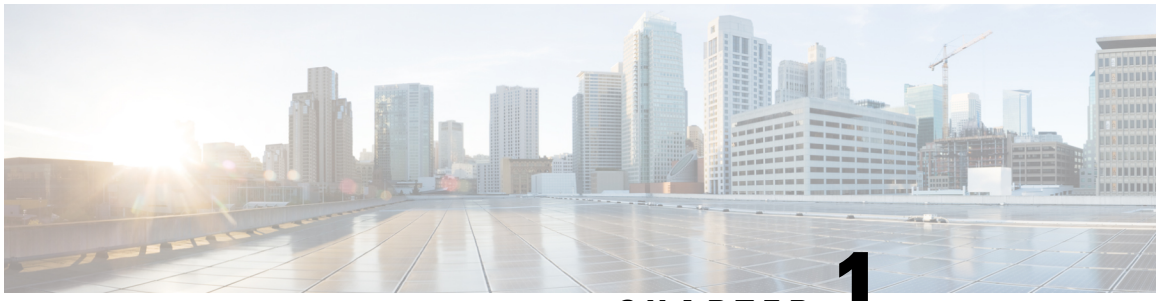
Cisco Catalyst SD-WAN User Management Guide, Releases 26.x and Later

First Published: 2026-03-02

Last Modified: 2026-04-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Read Me First

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17
- User Documentation for Cisco SD-WAN Release 20

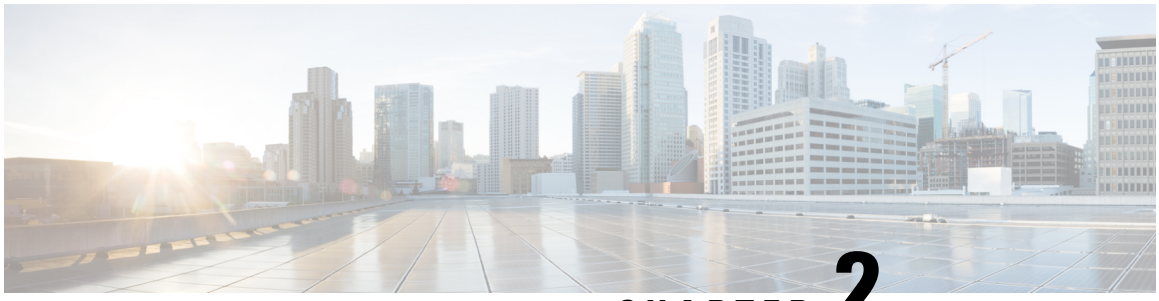
Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.

- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.



CHAPTER 2

Users and Access

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

Table 1: Feature history

Feature name	Release Information	Description
Inactivity lockout	Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature lets you configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days.
Unsuccessful login attempts lockout	Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature lets you configure Cisco SD-WAN Manager to lock out users who have made a designated number of consecutive unsuccessful login attempts within a designated period.
Configure Sessions in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco vManage Release 20.3.1	This feature lets you see all the HTTP sessions that are open within Cisco SD-WAN Manager. It gives you details about the username, source IP address, domain of the user, and other information. A user with User Management Write access, or a netadmin user can trigger a log out of any suspicious user's session.

Reference the Chapter Map here

Users and access

Users and access

Users and access is a feature in SD-WAN Manager that

- controls and manages the authorization permissions for users on Cisco IOS XE Catalyst SD-WAN devices
- involves defining users who are allowed to log in
- enables grouping these users into user groups, and
- associating privileges with each group to specify the commands users are authorized to execute.

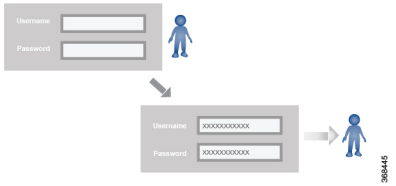
Users and user groups

Users are entities that represent individuals or processes authorized to access and operate Cisco IOS XE Catalyst SD-WAN devices.

User groups are collections of users based on common roles or privileges to control authorization permissions on Cisco IOS XE Catalyst SD-WAN.

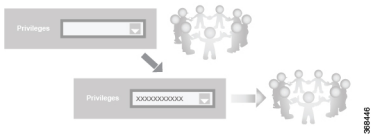
Users and user groups

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

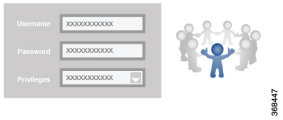


The Cisco Catalyst SD-WAN software provides one standard username, admin, which is a user who has full administrative privileges, similar to a UNIX superuser. By default, the admin username password is admin. You cannot delete or modify this username, but you can and should change the default password.

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



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



Standard user groups

Cisco Catalyst SD-WAN software provides standard user groups and allows creation of custom user groups as needed.

- **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.
- **network_operations**: From Cisco vManage Release 20.9.1, network_operations user group is supported. 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.
- **security_operations**: From Cisco vManage Release 20.9.1, security_operations user group is supported. 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 All user groups, regardless of the read or write permissions selected, can view the information displayed on the Cisco SD-WAN Manager Dashboard screen.

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.

User group permissions

You can add, edit, view, or delete users and user groups based on the permissions listed here.

- Only an admin or a user who has Manage Users write permission can add, edit, or delete users and user groups from SD-WAN Manager.
- Each user group can have read or write permission. Write permission includes read permission.
- All user groups, regardless of the read or write permissions selected, can view the information displayed in the SD-WAN Manager dashboard.

Table 2: User group permissions for different device types

Permissions	Sections
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 commands

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 you create for a user through the CLI can be different from SD-WAN Manager credentials. You can create different credentials for a user on each device. All Cisco IOS XE Catalyst SD-WAN device users with the netadmin privilege can create a new user.

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

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

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

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

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

Table 3: username, password, and group name requirements

username	The username can be 1 to 128 characters long, and 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 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.
password	Each username must have a password, and users are allowed to change their own password. The CLI immediately encrypts the string and does not display a readable version of the password. When a user logs in to a Cisco IOS XE Catalyst SD-WAN device, they have five chances to enter the correct password. After the fifth incorrect attempt, the user is locked out of the device, and must wait for 15 minutes before attempting to log in again.
group name	Group name is the name of a standard 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.

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”.

Configure password for admin users using CLI commands

The factory-default password for the admin username is admin and we recommend to modify this password the first time you configure a Cisco IOS XE Catalyst SD-WAN device.

Procedure

Step 1 Modify the factory-default password for admin the first time you configure a Cisco IOS XE Catalyst SD-WAN device:

Example:

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

Step 2 Configure the password as an ASCII string. The CLI immediately encrypts the string and does not display a readable version of the password.

Example:

```
Device# show run | sec username
username admin privilege 15 secret 9 $9$3F2M2l2G2/UM3U$TGe2kqoIibdIRDEj4cOVKbVFP/o4vnlFAwWnmzx1rRE
username appnav privilege 15 secret 9 $9$3l2L2V.F2VIM1k$p3MBAyBtGxKf/yBGnUSHQ1g/ae1QhfIbieg28buJJGI
```

```
username eft secret 9 $9$3FMJ3/UD2VEL2E$d.kE4.an41v7wEhrQc6k5wIfE9M9WkNAJxUvbbempS.
username lab privilege 15 secret 9 $9$3l.J3FUD2F.E2.$/AiVn9PmLCpgr6ExVrE7dH979Wu8nbdtAfbzUtfysg.
username test secret 9 $9$1l2J3l6D3/QL3k$7PZOXJAJOI1os5UI763G3XcpVhXlqcwJ.qEmgmx4X9g
username vbonagir privilege 15 secret 9 $9$3/2K2UwF2lQF3U$VbdQ5bq18590rRthF/NnNnOsw.dw1/EViMTFZ5.ctus
Device#
```

Step 3 If you are using RADIUS to perform AAA authentication, you can configure a specific RADIUS server to verify the password:

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

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

Create user groups

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
Step 2 Click **User Groups**.
Step 3 Click **Add User Group**.
Step 4 Enter **User Group Name**.
Step 5 Select the **Read** or **Write** check box against feature that you want to assign to a user group.
Step 6 Click **Add**.
Step 7 You can view the new user group in the left navigation path. Click **Edit** to edit the existing read or write rules.
Step 8 Click **Save**.

Create user groups using CLI commands

Create additional custom groups and configure privilege roles that the group members have.

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** user group.

Procedure

Step 1 To create a custom group with specific authorization, configure the group name and privileges:

Example:

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

Group name can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. Some group names are reserved, so you cannot configure them. For a list of them, see the aaa configuration command.

If a remote RADIUS or TACACS+ server validates authentication but does not specify a user group, the user is placed into the basic user group. 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).

Step 2 Under task, list the roles that the group members have.

The role can be one or more of the following: interface, policy, routing, security, and system.

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.

Procedure

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

Step 2 Click **User Groups**.

Step 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.

Step 4 Click **Trash** icon.

Step 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.

Procedure

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

Step 2 Click **User Groups**.

Step 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.

Step 4 Click **Edit**, and edit privileges as needed.

Step 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.

Account lockout

Account Lockout

Account Lockout is a configuration category within Cisco SD-WAN Manager that

- defines security features to control and manage user access to Cisco SD-WAN Manager, and
- includes mechanisms such as inactivity lockout and unsuccessful login attempts lockout.

Account Lockout options

From Cisco Catalyst SD-WAN Manager Release 20.12.1, a netadmin user can enable the following account lockout options:

- Inactivity lockout: You can configure 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 SD-WAN Manager until an administrator unlocks their accounts. See Configure Account Lockout.
- Unsuccessful login lockout: You can configure 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 SD-WAN Manager until a configured amount of time passes or an administrator unlocks their user accounts.

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

  See Configure unsuccessful login attempts lockout.

Configure Account Lockout

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

Use this procedure to lock out users.

Before you begin

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

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

Procedure

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

Step 2 Click **Account Lockout** and enable the **Inactive days before locked out** option.

In Cisco Catalyst SD-WAN Manager Release 20.12.x, locate **Account Lockout**, click **Edit**, and enable **Inactive days before locked out**.)

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

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

Step 4 Click **Save**.

Configure unsuccessful login attempts lockout

Use this procedure to configure Cisco SD-WAN Manager to lock out users after a specified number of consecutive unsuccessful login attempts within a defined timeframe

Before you begin

From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can configure Cisco SD-WAN Manager to lock out users who have made a designated number of consecutive unsuccessful login attempts within a period of time.

Note From Cisco Catalyst SD-WAN Manager Release 20.13.1 or later, use the procedure described in Configure Account Lockout, on page 10.

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

Procedure

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

Step 2 Click **Account Lockout**.

Step 3 In the **Lockout on failed login attempts** row, click **Edit**.

Step 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

User sessions

User sessions

A user session is a period of interaction between a user and a system that

- begins when the user successfully authenticates or logs in
- maintains state and context for the user's activities, and
- ends when the user logs out or the session expires due to inactivity or timeout.

Restrictions for configuring user sessions

Client Session Timeout

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

Session Lifetime

You can edit **Session Lifetime** in a multitenant environment only if you have provider access.

Server Session Timeout

You cannot access **Server Session Timeout** in a multitenant environment, even if you have provider access or tenant access.

Configure a client session timeout in SD-WAN Manager

Use this procedure to 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.

Before you begin

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

Procedure

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

Step 2 Click **User Sessions**.

Step 3 Under **Client Session Timeout**, click **Session Timeout**.

Step 4 Specify the timeout value, in minutes.

Step 5 Click **Save**.

Configure a session lifetime in SD-WAN Manager

Use this procedure to 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.

Before you begin

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

Procedure

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

Step 2 Click **User Sessions**.

Step 3 In the **SessionLifeTime Timeout (minutes) field**, specify the session timeout value, in minutes, from the drop-down list.

Step 4 Click **Save**.

Configure the Server Session Timeout in SD-WAN Manager

Use this procedure to 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.

Procedure

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

Step 2 Click **User Sessions**.

Step 3 In **Server Session Timeout Timeout(minutes)** field, specify the timeout value, in minutes.

Step 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.

If the **Max Sessions Per User** 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 Sessions Per User**: 1 to 255.

Default: If undefined, there is no limit on the number of concurrent sessions for that role.

The value also applies to CLI sessions.

Procedure

Step 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.

Step 2 Click the role name, edit the **Max user sessions** value, and click **Update**.

Note
From Cisco Catalyst SD-WAN Manager 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.

Ciscotac user access

Ciscotac user access

Cisco Edge software provides two special user accounts, ciscotacro and ciscotacrw, for use by the Cisco Support team. These user accounts

- operate using a consent-token challenge and token response authentication, requiring a new token for each login session, and
- can access SD-WAN Manager web server, SSH Terminal on SD-WAN Manager using a token, including SD-WAN Validator, SD-WAN Controllers, and Cisco vEdge devices.

You can use these user accounts in both cloud and on-premises installations.

Ciscotac user accounts and privileges

The default CLI templates include configuration for the ciscotacro and ciscotacrw users. These users are enabled by default but you can disable them if needed.

- ciscotacro user: This account belongs to the operator user group and has read-only privileges. This account allows monitoring configurations but does not permit operations that modify network configurations.
- ciscotacrw user: This account belongs to the netadmin user group and has read-write privileges. This account allows modification of network configurations. Only this user can access the root shell using a consent token.

To allow the network administrator can access system shell, use the **tools consent-token** command. Starting Cisco Catalyst SD-WAN Control Components Release 20.12.x, the **request support ciscotac** command is deprecated.

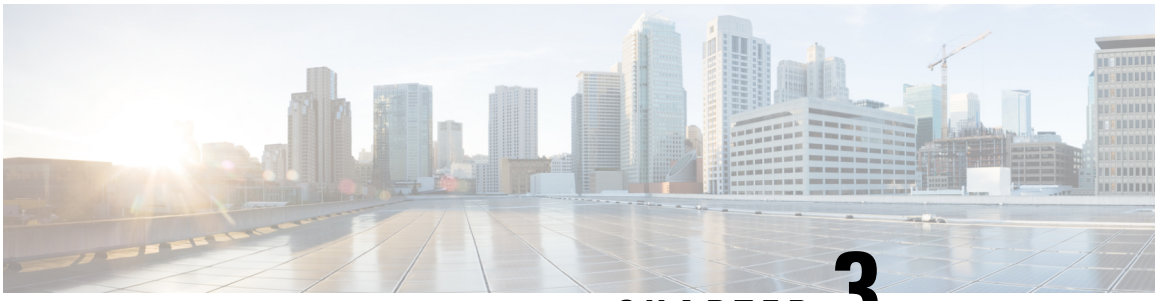
Limitations for Ciscotac user access

Ciscotac user sessions

- 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.

Removing Ciscotac users

You can remove the ciscotacro and ciscotacrw users. If removed, you can open a case and share temporary login credentials or share the screen with the Cisco Support team for troubleshooting an issue.



CHAPTER 3

Password Management

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

Table 4: Feature History

Feature Name	Release Information	Description
Hardened passwords	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature enables password policy rules in Cisco SD-WAN Manager. After password policy rules are enabled, Cisco SD-WAN Manager enforces the use of strong passwords.
	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature lets you configure Cisco SD-WAN Manager to enforce predefined-medium security or high-security password criteria.
Type 6 Passwords on Cisco IOS XE SD-WAN Routers	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature allows you to use type 6 passwords that use secure reversible encryption. This encryption provides enhanced security by using more secure algorithms to encrypt your passwords. These passwords are supported for the templates detailed in Supported platforms and templates, on page 23.

Hardened passwords

Restrictions for passwords

Password attempts and password change

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

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

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

Password change policy

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

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

Password requirements

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

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

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

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

Table 5: Password criteria and requirements

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

Enable Password Policy

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

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

Procedure

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

Step 2 Click **Password Policy**.

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

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

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

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

Step 4 Click **Save**.

Reset a locked user using SD-WAN Manager

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

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

Use these steps to reset a locked user.

Procedure

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

Step 2 Choose the user account you want to unlock.

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

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

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

Reset a locked user using CLI commands

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

Procedure

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

Step 2 Run the following command:

Example:

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

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

Type 6 passwords

Type 6 passwords

Type 6 password is an encryption method that

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

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

Type 6 passwords in SD-WAN Manager

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

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

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

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

Supported platforms and templates

Type 6 passwords are supported for these platforms and templates.

Supported platforms:

- Cisco IOS XE Catalyst SD-WAN devices

Supported templates:

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

Restrictions for Type 6 passwords

SNMP templates

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

Password length

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

Upgrade existing templates to Type 6 passwords

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

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

Procedure

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

Step 2 Click **Feature Templates**.

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

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

Step 4 Click **Edit**.

Step 5 Click **Save**.

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

Type 6 encryption for CLI commands

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

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

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

Methods for verifying Type 6 passwords

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

Verifying using SD-WAN Manager

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

For example:

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

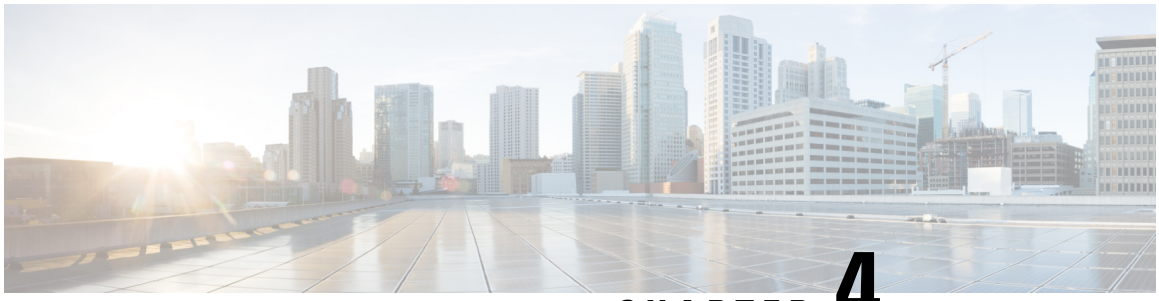
Although the command displays the type as `0`, the `$CRYPT_CLUSTER$ptqX7nQr6QvC8YZuoMGOkw==$6cVCeSpOfoVFe5iqhJqvQQ==` string represents your encrypted password. If your password is encrypted, it will begin with `$CRYPT_CLUSTER$`.

Verifying on a device

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

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

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



CHAPTER 4

Authentication

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

Table 6: Feature History

Feature Name	Release Information	Description
Duo Multifactor Authentication Support	Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature lets you configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to Cisco SD-WAN ManagerCisco SD-WAN Manager.
Secure Shell Authentication Using RSA Keys	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature helps configure RSA keys by securing communication between a client and a Cisco Catalyst SD-WAN server.
Authorization and Accounting	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature allows you to configure authorization, which verifies and permits the commands a user enters on a device before execution, and accounting, which generates a record of the commands a user executes on the device
Posture Assessment Support	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature enables you to utilize Posture Assessment capabilites to validate the compliance of endpoints according to security policies of your enterprise. Identity Services Engine (ISE) Posture functions are integrated into Cisco 1100 Integrated Services Routers. This feature can only be configured using the Add-On feature template in Cisco SD-WAN Manager.

Authentication

Authentication in Cisco SD-WAN Manager is a security mechanism that

- ensures only authorized devices and users can access the network, and
- integrates with AAA, RADIUS, and TACACS+ to authenticate users and control device access and operations.

Authentication order

The authentication order is a configuration setting that

- 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, and
- provides a way to proceed with authentication if the current authentication method is unavailable.

Default authentication order

The default authentication order is local, followed by radius, and then tacacs. The default authentication order works as follows:

- local: The authentication process checks for a username and passwords in the running configuration of the device.
- radius: The authentication process uses a RADIUS server to validate credentials.
- tacacs: The authentication process uses a TACACS+ server to validate credentials. 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, you are authenticated or denied access based on that server's TACACS+ database. If you have configured multiple TACACS+ servers, then the authentication process contacts one server, and if that server is not available, the process continues in sequence to the other servers. You are then authenticated or denied access based on one of the reachable TACACS+ servers.

  If none of the authentication processes succeed, access to the device is denied.

Modifying the default authentication order

You can use the **auth-order** command to modify the default authentication order. 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 modify the authentication order for admin users, include the keyword **admin** in the preceding command, for e.g., **admin-auth-order** and then specify the authentication method(s).

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

Authentication fallback mechanism

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

If the authentication order is configured as

- radius local: With radius as 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.
- local radius: With local as the default authentication, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device.
- radius tacacs local: With radius as 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.

User group assignment after authentication

After the remote server authenticates a user, it assigns the user to a user group:

- If a remote server validates the authentication but does not specify a user group, it places the user in the *basic* user group.
- If a remote server validates the authentication and specifies a user group (say, X), it assigns the user to that group only. However, if that user is also configured locally and belongs to a user group (for example, group Y), the user is assigned to both groups (X and Y).
- If a remote server validates the authentication and the user is not configured locally, the system logs the user into the vshell as the *basic* user, with a home directory of /home/basic.
- If a remote server validates the authentication and the user is configured locally, the system logs the user into the vshell under their local username (for example, "eve") with a home directory of /home/*username* (for example, /home/eve).

Configure authentication order

The authentication order determines the order in which the system authenticates users, and helps users proceed with authentication if the current authentication method is unavailable.

Configure the authentication order for devices using these steps.

Procedure

Step 1 To configure AAA authentication order on a Cisco IOS XE Catalyst SD-WAN device, select the **Authentication** tab and configure the **Server Group Order** parameter.

Using AAA server groups allows you to group existing server hosts. By grouping these hosts, you can select a specific subset of configured servers to use for a particular service.

Step 2 Change the default order of authentication methods that the software uses to verify user's access to a Cisco IOS XE Catalyst SD-WAN device:

a) Click the **ServerGroups priority order** field to display the drop-down list of server groups.

The list displays groups from local, RADIUS, and TACACS authentication methods.

b) Select the groups in the order the software should use to verify users accessing the device.

Note
Select at least one group from the list.

Duo Multi-factor authentication

Duo Multi-factor authentication

Duo multi-factor authentication is a security feature that

- integrates with Cisco SD-WAN Manager and controllers to enhance user login security
- requires users to verify their identity using a second factor after entering their username and password, and
- helps prevent unauthorized access by adding a second authentication factor aligned with zero-trust principles.

Configure Duo multifactor authentication

From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to SD-WAN Manager and other controllers.

Before you begin

Create local users in your Duo account before proceeding.

By default, Duo MFA does not apply to the admin user. To enable Duo MFA for the admin user, enable the **DUO MFA Configuration** option, and enter the admin-auth-order command in the CLI.

Once Duo authentication is set up, users are prompted to authenticate with their Duo credentials on their mobile devices and thereafter log in to SD-WAN Manager.

SD-WAN Manager does not display any message that an MFA request has been sent to the user's mobile device.

Follow these steps to set up Duo authentication.

Procedure

Step 1 Log in to the Duo Admin Panel.

Step 2 Create an Auth API application.

This step gives you the Duo integration key, secret key, and API hostname information required to complete Duo MFA configuration. See Duo Auth API for more information.

Step 3 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 4 Click **DUO MFA Configuration**.

If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.

Step 5 Click **Enabled**.

Step 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) Displays the server proxy used to access the Duo server if SD-WAN Manager is behind a firewall. Set this server proxy with the **system http proxy** or the **system https proxy** command. **Note** If SD-WAN Manager is deployed on a cloud that can be reached by an external network, a server proxy should not be set.

Step 7 Click **Save**.

Step 8 If a Cisco SD-WAN Validator or a Cisco SD-WAN Controller does not have internet access, enter the following commands in the CLI or the device template 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
```

RADIUS authentication

Radius authentication

The Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that

- secures networks against unauthorized access
- enables RADIUS clients on Cisco devices to send authentication requests to a central RADIUS server, and
- stores all user authentication and network service access information on the central server.

Configure RADIUS authentication using CLI commands

Authenticate a Cisco IOS XE Catalyst SD-WAN device with up to 8 RADIUS servers by configuring each server's parameters as explained here.

Procedure

Step 1 For each RADIUS server, configure the IP address and a password, or key at a minimum.

Example:

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

Specify the key as a clear text string up to 31 characters, or provide it 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.

Step 2 To add additional RADIUS servers, include the **server** and **secret-key** commands for each server.

Step 3 Optionally, configure these RADIUS parameters:

a) Set the priority of a RADIUS server that you want to use.

Priority is a means of choosing or load balancing among multiple RADIUS servers. The priority value can range from 0 to 7. The server with the lower priority number will be prioritized over those with higher numbers.

b) To change the default port numbers, use the **auth-port** and **acct-port** commands.

By default, the Cisco IOS XE Catalyst SD-WAN device uses port 1812 for authentication connections to the RADIUS server and port 1813 for accounting connections.

c) If the RADIUS server is reachable through specific interface, set that interface with the **source-interface** command.

d) Define a tag for the RADIUS server and then associate the tag with the **radius-servers** command.

A tag can be a string with 4 to 16 characters. 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.

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.

e) Configure a VPN number for the server so that the device can locate it.

This is required if the RADIUS server is located in a different VPN from the Cisco IOS XE Catalyst SD-WAN device. If you configure multiple RADIUS servers, they must all be in the same VPN.

f) Change the time interval using the **timeout** command, and set a value from 1 to 1000 seconds.

When waiting for a reply from the RADIUS server, a Cisco IOS XE Catalyst SD-WAN device by default waits three seconds before retransmitting its request.

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

SSH authentication

SSH authentication

The Secure Shell (SSH) protocol is a network protocol that

- provides secure remote access connection to network devices
- supports user authentication using public and private keys, and
- enables encrypted communication between clients and network devices.

Enabling SSH authentication

To enable SSH authentication, store your public key in your home directory of in the following location:

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

A new key is generated on the client machine which owns the private key. The client decrypts any message encrypted with the SSH server's public key using the client's private key.

Restrictions for SSH authentication

SSH RSA key size

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

Supported methods for configuring SSH authentication using CLI commands

Use these supported SSH RSA key-based authentication methods when configuring SSH authetnciation using the CLI.

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

Traditional IOS CLI, allow support for:

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

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

Configure SSH Authentication using templates

Configure SSH authentication on Cisco IOS XE Catalyst SD-WAN devices using these steps.

Procedure

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

Step 2 Click **Feature Templates**, and click **Add Template**.

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

Step 3 From **Select Devices**, select the type of device for which you are creating the template.

Step 4 From **Basic Information**, choose **CISCO AAA** template.

Step 5 From **Local**, click **New User** and enter the details.

Step 6 Enter **SSH RSA Key**.

Note

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

IEEE 802.1X authentication

IEEE 802.1X authentication

IEEE 802.1X is a port-based network access control (PNAC) protocol that

- prevents unauthorized network devices from gaining access to wired networks, and
- provides authentication for devices that want to connect to a wired network.

IEEE 802.1X open authentication and host modes

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

You can enable open authentication by entering the **authentication open** command after host mode configuration. This acts as an extension to the configured host mode. For example, if open authentication is enabled with single-host mode, then the port will allow only one MAC address. When preauthentication open access is enabled, initial traffic on the port is restricted and independent of 802.1X is configured on the port. If you don't configure any access restriction other than 802.1X on the port, then a client device will have a full access on the configured VLAN.

Note You can configure open authentication using CLI template only. You cannot configure open authentication using dot1x feature template on SD-WAN Manager.

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

Restrictions for configuring IEEE 802.1X authentication

Authentication, Authorization, and Accounting

IEEE 802.1X Authentication, Authorization, and Accounting (AAA) is not supported on multiple groups.

Authentication order

Authentication order IEEE 802.1X MAB CLI cannot be disabled through SD-WAN Manager. The presence of this authentication order CLI results in a 60 second delay in MAB authentication when MAB client is online.

Open authentication

Authentication open is not supported in feature templates but can be deployed with a CLI add on template.

Prerequisites for configuring IEEE 802.1X authentication

Enable or configure these prerequisites before you configure IEEE 802.1X authentication with templates, CLI commands or configuration groups.

RADIUS

Enable RADIUS authentication servers to authenticate IEEE 802.1x services.

Configure RADIUS Accounting attributes.

Switch port

Enable IEEE 802.1X configuration on the switch port interface.

VLAN configurations

Enable these VLAN configurations to manage authenticated and unauthenticated clients:

- Restricted VLAN (or authentication rejected VLAN)
- Guest VLAN
- Critical VLAN (or authentication failed VLAN)
- Critical Voice VLAN

Enable IEEE 802.1X authentication event by VLAN ID in the Add-on template, if required.

Host-mode authentication

Enable one of these host-mode authentications:

- Single-host mode
- Multiple-host mode
- Multiple-authentication mode
- Multi-domain mode

Configure IEEE 802.1X Authentication using templates

IEEE 802.1X is a port-based network access control (PNAC) protocol that prevents unauthorized devices from accessing wired networks by authenticating devices that want to connect. Before any client can use network services, a RADIUS authentication server must authenticate each connected client. Use a Cisco AAA feature template to configure IEEE 802.1X authentication on the interface.

Procedure

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

Step 2 Click **Feature Templates**. Then, click **Add Template**.

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

Step 3 Select your device from the list on the left panel.

Step 4 Select the **Cisco AAA** template and enter the **Template Name** and **Description**.

Step 5 Select the **RADIUS** tab.

a) Under **RADIUS SERVER** click **New RADIUS Server** and configure these parameters:

Parameter Name	Description
Mark as Optional Row	Check the **Mark as Optional Row** check box to mark your configuration as device-specific.
Address	Enter IP Address of the RADIUS server.
Authentication Port	Click **Authentication**, then click **Add New Authentication Entry** to configure RADIUS authentication attribute–value (AV) pairs to send to the RADIUS server during an IEEE 802.1X session. To save the entry, click **Add**.
Accounting Port	Click **Accounting**, then click **Add New Accounting Entry** to configure RADIUS accounting attribute–value (AV) pairs to send to the RADIUS server during an IEEE 802.1X session. To save the entry, click **Add**.
Timeout	Configure how long to wait for replies from the RADIUS server.
Retransmit Count	Configure how many times the system contacts this RADIUS server.
Key	Enter the RADIUS server shared key.

b) Click **Add**.

Step 6 Select the **RADIUS GROUP** tab.

a) Under **New RADIUS Group** configure these parameters:

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

b) Click **Add**.

Step 7 Select the **802.1X** tab and enter these parameters:

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

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

Step 8 To save this feature template, click **Save**.

Step 9 To enable this feature on your device, ensure to add these feature templates to your device template.

Note
You need to recreate the AAA feature templates as the templates created prior to Cisco vManage Release 20.5.1 fails when attached to the device.

What to do next

Create a **Switch Port** template that can be used for the Switch Port device.

Create a Switch Port template using templates

Create a **Switch Port** template for the Switch Port device.

Procedure

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

Step 2 Click **Feature Templates**, and then click **Add Template**.

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

Step 3 Select your device from the list.

Step 4 Select the **Switch Port** template and enter the **Template Name** and **Description**.

Step 5 Select the **Interface** tab and click **New Interface**.

a) Configure these parameters:

Parameter Name	Description
Interface name	Enter the interface name.
Speed	Enter the interface speed.
VLAN Name	Enter the VLAN name.
VLAN ID	Enter the VLAN identifier associated with the bridging domain.
802.1X	Enable IEEE 802.1X authentication on this interface. Select "On". This will provide a further set of parameters listed below.
Interface PAE Type	Enter the IEEE 802.1x Interface PAE type.
Control Direction	Enter unidirectional or bidirectional authorization mode.

Parameter Name	Description
Host Mode	Select whether an IEEE 802.1X interface grants access to a single host (client) or to multiple hosts (clients): • Multi Auth—Grant access to one host on a voice VLAN and multiple hosts on data VLANs. • Multi Host—Grant access to multiple hosts • Single Host—Grant access only to the first authenticated host. This is the default. • Multi-Domain—Grant access to both a host and a voice device, such as an IP phone on the same switch port. **Note** These options are available only in the 'Global' Host Mode settings.
Periodic Reauthentication	Enter how often to reauthenticate IEEE 802.1X clients. By default, no reauthentication attempts are made after the initial LAN access request. Range: 0 to 1440 minutes

b) Click **Advanced Options** and configure these parameters:

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

c) Click **Add**.

Step 6 To save this feature template, click **Save**.

Step 7 To enable this feature on your device, ensure to add these feature templates to your device template.

IEEE 802.1X Open Authentication using CLI commands

You can configure IEEE 802.1X Open Authentication using the CLI add-on template:

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

Configure IEEE 802.1X Authentication using CLI commands

For configuring IEEE 802.1x using CLI commands, two sets of configuration are required:

- Global AAA commands
- Interface level commands

Procedure

Step 1 Configure the Global AAA commands.

a) Enable or disable IEEE 802.1X globally:

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

b) Enable accounting:

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

Step 2 Configure the interface level commands.

a) Enable or disable IEEE 802.1X on port-basis:

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

b) Enable or disable MAB on port-basis and then select host-mode:

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

c) Configure voice VLAN:

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

d) Select IEEE 802.1X control direction:

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

e) Enable periodic re-authentication and corresponding re-authentication interval and inactivity timeout time:

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

f) Configure authentication orders on per-port basis:

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

g) Specify the restricted VLAN and then specify the guest VLAN:

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

h) Specify the critical VLAN:

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

i) Enable the critical voice VLAN feature:

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

Configure Switch Port using a configuration group

Configure Switch Port settings using these steps.

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 Switch Port feature in a Service profile.

Table 7: Switch Port

Field	Description
Age Out Time	Enter how long an entry is in the MAC table before it ages out. Set the value to 0 to prevent entries from timing out. Range: 0, 10 through 1000000 seconds Default: 300 seconds
Configure Interface	
Interface Name	Enter the name of the interface to associate with the bridging domain, in the format **`geslot/port`**.

Field	Description
Mode	Choose the switch port mode. • **access**: Configure the interface as an access port. You can configure only one VLAN on an access port, and the port can carry traffic only for one VLAN. When you choose **access**, the following field appears: **Switchport Access Vlan**: Enter the VLAN number, which can be a value from 1 through 4094. • **trunk**: Configure the interface as a trunk port. You can configure one or more VLANs on a trunk port, and the port can carry traffic for multiple VLANs. When you choose **trunk**, the following fields appear: • **Allowed Vlans**: Enter the number of the VLANs for which the trunk can carry traffic and a description for the VLAN. • **Switchport Trunk Native Vlan**: Enter the number of the VLAN allowed to carry untagged traffic.
Shutdown	Enable the interface. By default, an interface is disabled.
Speed	Enter the speed of the interface.
Duplex	Choose **full** or **half** to specify whether the interface runs in full-duplex or half-duplex mode.
Port Control	Choose the port control mode to enable IEEE 802.1X port-based authentication on the interface. • **auto**: Enables IEEE 802.1X authentication and starts the port in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The device requests the identity of the supplicant and starts relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the device by using the supplicant MAC address. • **force-unauthorized**: Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The device cannot provide authentication services to the supplicant through the port. • **force-authorized**: Disables IEEE 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client.
Voice VLAN	Enter the Voice VLAN ID.
Pae Enable	The Cisco Catalyst SD-WAN device acts as a port access entity (PAE), allowing authorized network traffic and preventing unauthorized network traffic ingressing to and egressing from the controlled port.

Field	Description
MAC Authentication Bypass	Enable this option to allow MAC authentication bypass (MAB) on the RADIUS server and to authenticate non-IEEE 802.1X–compliant clients using a RADIUS server.
Host Mode	Choose whether an IEEE 802.1X interface grants access to a single host (client) or to multiple hosts (clients). • **single-host**: Grant access only to the first authenticated host. This is the default. • **multi-auth**: Grant access to one host on a voice VLAN and multiple hosts on data VLANs. • **multi-host**: Grant access to multiple hosts. • **multi-domain**: Grant access to both a host and a voice device, such as an IP phone on the same switch port.
Enable Periodic Reauth	Enable periodic re-authentication. By default, this option is enabled.
Inactivity	Enter the inactivity timeout time in seconds. Default: 60 seconds
Reauthentication	Enter the re-authentication interval in seconds.
Control Direction	Choose **both** (bidirectional) or **in** (unidirectional) authorization mode.
Restricted VLAN	Enter the restricted VLAN (or authentication-failed VLAN) for IEEE 802.1x-compliant clients. Configure limited services to IEEE 802.1X-compliant clients that failed RADIUS authentication.
Guest VLAN	Enter the guest VLAN to drop non-IEEE 802.1X enabled clients, if the client is not in the MAB list.
Critical VLAN	Enter the critical VLAN (or authentication-failed VLAN) for IEEE 802.1x-compliant clients. Configure network access when RADIUS authentication or the RADIUS server fails.
Enable Voice	Enable the critical voice VLAN.
Configure Static Mac Address	
MAC Address	Enter the static MAC address to map to the switch port interface.
Interface Name	Enter the name of the switch port interface.
VLAN ID	Enter the number of the VLAN for the switch port.

What to do next

Also see Deploy a configuration group.

Authentication, Authorization, and Accounting

Restrictions to configure authorization and accounting

If you enter a configuration and press enter before you choose a value from an enumeration, the CLI shows a choice sub-menu. In this scenario, the system does not send the final value for authorization.

You cannot use the **load merge** and **load override** commands when authorization is configured.

Commands that you configure using load or rollback are not authorized or accounted.

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 8: 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.

Field	Description
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.
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 9: 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

Field	Description
Timeout	Enter the number of seconds a device waits for a reply to a RADIUS request before retransmitting the request. Default: 5 seconds Range: 1 through 1000
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 10: 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 11: Accounting

Field	Description
Rule Id*	Enter the accounting rule ID.

Field	Description
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.
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 12: 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.

Field	Description
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.

Methods of configuring AAA using templates

You can configure authentication, authorization, and accounting (AAA) using Cisco SD-WAN Manager template and push these settings to selected devices of the same type. This helps you to conveniently configure several devices of the same type at once.

You can use the AAA template for Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager instances, Cisco Catalyst SD-WAN Controllers, Cisco IOS XE Catalyst SD-WAN devices.

Cisco IOS XE Catalyst SD-WAN devices support configuration of AAA in combination with RADIUS and TACACS+ servers.

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

Create a template

Procedure

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

Step 2 Click **Device Templates**, and click **Create Template**.

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

Step 3 From the **Create Template** drop-down list, select **From Feature Template**.

Step 4 From the **Device Model** drop-down list, select the type of device for which you are creating the template.

Step 5 Select **Basic Information**.

Step 6 To create a custom template for AAA, select **Factory_Default_AAA_CISCO_Template** and click **Create Template**.

The AAA template form appears. The top of the form has fields where you name the template, and the bottom has fields where you define AAA parameters.

Step 7 In the **Template Name** field, enter a name for the template.

The name can include up to 128 alphanumeric characters.

Step 8 In the **Template Description** field, enter a description of the template.

The description can include up to 2048 alphanumeric characters.

Step 9 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 these:

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

Configure 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.

Procedure

Step 1 To configure local access for individual users, select **Local**.

Step 2 To add a new user, click **+ New User**, and configure the following parameters:

Parameter Name	Description
Name	Enter a name for the user. The name must start with a letter and be between 1 and 128 characters. Use only lowercase letters, numbers 0 through 9, hyphens (-), underscores (_), or periods (.). The name should not contain any uppercase letters. These 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. In addition to these, names starting 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 changing this password. **Note** When configuring local users using a Cisco SD-WAN Manager AAA template, SD-WAN Manager uses a Cisco type 9 password type that uses the scrypt algorithm for hashing the passwords of local users. If you configure local users using a device CLI template or a CLI add-on template, you can choose other Cisco password types for hashing of local user passwords. For more information, see Using Type 6 encryption in a CLI add-on template.
Privilege Level 1 OR 15	Select between privilege level 1 or 15. • **Level 1**: User EXEC mode. Read-only, and access to limited commands, such as the **ping** command. • **Level 15**: Privileged EXEC mode. Full access to all commands, such as the **reload** command, and the ability to make configuration changes. By default, the EXEC commands at privilege level 15 are a superset of those available at privilege level 1.
SSH RSA Key(s)	Click **+ Add** to add SSH RSA keys. Paste your SSH RSA key in the field. To remove a key, click -. Devices support a maximum of 2 SSH RSA keys.

Step 3 Click **Add** to add the new user. Click **+ New User** again to add additional users.

To configure local access for user groups, 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.

Step 4 From **Local**, select **User Group**.

Step 5 Click **+ New User Group**, and configure the following parameters:

Parameter Name	Description
Name	Name of an authentication group. The name must start with a letter and be between 1 and 128 characters. Use only lowercase letters, numbers 0 through 9, hyphens (-), underscores (_), or periods (.). The name should not contain any uppercase letters. SD-WAN Manager 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 basic group. Users in the basic group have the same permissions to perform tasks, as in the operator group. You cannot configure these groups as they are reserved: 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 starting with the string viptela-reserved are reserved.
Feature Type	Click **Preset** to display a list of preset roles for the user group. Click **Custom** to display a list of authorization tasks that have been configured.
Feature	The feature table lists the roles for the user group. These roles are Interface, Policy, Routing, Security, and System. Each role allows the user group to read or write specific portions of the device's configuration and to execute specific types of operational commands. Click the appropriate boxes for **Read**, **Write**, or **None** to assign privileges to the group for each role.

Step 6 Click **Add** to add the new user group.

Step 7 To add another user group, click **+ New User Group** again.

Step 8 To delete a user group, click the trash icon. You cannot delete the three standard user groups, basic, netadmin, and operator.

Configure RADIUS authentication

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

Procedure

Step 1 To configure a connection to a RADIUS server, from **RADIUS**, click **+ New Radius Server**, and configure the following parameters:

Table 13:

Parameter Name	Description
Address	Enter the IP address of the RADIUS server host.

Parameter Name	Description
Authentication Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If you do not use the server for authentication, set the port number to 0. Default: Port 1812
Accounting Port	Enter the UDP port to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 0 to 65535. Default: 1813.
Timeout	Enter the number of seconds a device should wait for a reply to a RADIUS request before retransmitting the request. Default: 5 seconds. Range: 1 to 1000
Retransmit Count	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 5 seconds.
Key (Deprecated)	Enter the Cisco IOS XE Catalyst SD-WAN devicekey the passes to the RADIUS server for authentication and encryption. Type the key as a text string from 1 to 31 characters. The system encrypts it immediately. Alternatively, type an AES 128-bit encrypted key. Use the same AES encryption key as on the RADIUS server.

Step 2 Click **Add** to add a new RADIUS server.

Step 3 To add another RADIUS server, click **+ New RADIUS Server** again.

Step 4 To remove a server, click the trash icon.

CLI equivalent:

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

Configure TACACS+ authentication

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

Procedure

Step 1 To configure a connection to a TACACS+ server, from **TACACS**, click **+ New TACACS Server**.

Step 2 Configure these parameters:

Parameter Name	Description
Address	Enter the IP address of the TACACS+ server host.
Port	Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0. Default: Port 49
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.

Configure authentication order

The authentication order determines the order in which the system authenticates users, and helps users proceed with authentication if the current authentication method is unavailable.

Configure the authentication order for devices using these steps.

Procedure

Step 1 To configure AAA authentication order on a Cisco IOS XE Catalyst SD-WAN device, select the **Authentication** tab and configure the **Server Group Order** parameter.

Using AAA server groups allows you to group existing server hosts. By grouping these hosts, you can select a specific subset of configured servers to use for a particular service.

Step 2 Change the default order of authentication methods that the software uses to verify user's access to a Cisco IOS XE Catalyst SD-WAN device:

a) Click the **ServerGroups priority order** field to display the drop-down list of server groups.

The list displays groups from local, RADIUS, and TACACS authentication methods.

b) Select the groups in the order the software should use to verify users accessing the device.

Note
Select at least one group from the list.

Configure authorization

You can configure authorization, that causes a TACACS+ server to authorize commands that the user enters on a device before the commands can be executed. Authorization is based on the policies that are configured in the TACACS+ server and on the parameters that you configure on the **Authorization** tab.

Before you begin

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

Procedure

Step 1 To configure authorization, choose the **Authorization** tab, click **+ New Authorization Rule**.

Step 2 Configure the following parameters:

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

Step 3 Click **Add** to add the new authorization rule.

Step 4 To add another authorization rule, click **+ New Accounting Rule** again.

Step 5 To remove an authorization rule, click the trash icon on the right side of the line.

CLI commands for configuring authorization:

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

Configure accounting

Configure accounting so that the TACACS+ server generates a record of commands executed by the user on a device.

Before you begin

Ensure to configure the TACACS+ server as the first option and local server as the second option in the authentication order on the **Authentication** tab. See Configure authentication order for details.

Procedure

Step 1 To configure accounting, choose the **Accounting** tab and click **+ New Accounting Rule**.

Step 2 Configure these parameters:

Table 14: Accounting

Parameter Name	Description
Method	Choose **Command** to log commands executed by a user.
Privilege Level 1 OR 15	Choose the privilege level (1 or 15). Accounting records are generated only for commands entered by users with this privilege level.
Enable Start-Stop	Click **On** to have the system send a start accounting notice at the beginning of an event and a stop record notice at the end of the event.
Groups	Choose a previously configured TACACS group. TACACS servers associated with this group use the parameters defined by this accounting rule.

Step 3 Click **Add** to add the new accounting rule.

Step 4 To add another accounting rule, click **+ New Accounting Rule** again.

Step 5 To remove an accounting rule, click the trash icon on the right side of the line.

CLI commands for configuring authorization:

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

Posture assessment support

Posture assessment support

Cisco AnyConnect Posture Assessment is a posture assessment solution that

- installs on endpoints to enforce security policies downloaded from an ISE server,
- checks endpoint conditions such as anti-malware, anti-spyware, anti-virus, application, and USB compliance, and
- reports compliance status to the ISE server to control network access based on posture evaluation.

Network endpoint validation and posture assessment workflow

Endpoint validation plays a critical role in network security by ensuring that devices connecting to a company's network comply with established security policies. The posture module enforces these policies on endpoints that are connected to the network. When Cisco 1100 Integrated Services Routers communicate with Cisco Identity Services Engine (ISE), they require authentication interaction. Use IEEE 802.1X as the recommended standard for posture assessment authentication. If required, MAC Authentication Bypass (MAB) can also be used.

After successful authentication and authorization using redirect Access Control Lists (ACLs), the posture assessment process begins. Once the system completes posture assessment and authentication, the ISE policy set triggers the RADIUS Change of Authorization (CoA) process to re-authenticate or re-authorize endpoints and enforce new or updated policies.

Following successful posture assessment and CoA re-authentication, endpoints and the Cisco ISR 1100 router receive full access to the network, ensuring that only compliant devices interact with network resources.

Restrictions for Posture Assessment

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

Configure posture assessment using CLI commands

Use the CLI Add-on template to configure AAA, IEEE 802.1x, posture assessment and redirect ACL and device-tracking.

Before you begin

Ensure these requirements are met before proceeding to configure posture assessment support:

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

Refer instructions to create a CLI Add-on template and then add the configuration explained next.

Procedure

Step 1 Configure AAA.

Example:

```
aaa new-model
radius server ISE1

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

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

interface vlan 15
 ip address 198.51.100.1 198.51.100.254

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

ip radius source-interface vlan 15
```

Note
`aaa new-model` is enabled by default on Cisco Catalyst SD-WAN and you cannot configure it. However, you can configure it on a non SD-WAN image.

Step 2 Configure IEEE 802.1x authentication and authorization.

Example:

```
policy-map type control subscriber simple_dot1x
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
!
interface GigabitEthernet0/1/7
 switchport access vlan 22
 switchport mode access
 access-session closed
 access-session port-control auto
 dot1x pae authenticaton
 service-policy type control subscriber simple_dot1x
!
interface Vlan22
 ip address 198.51.100.1 198.51.100.254
```

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

Step 3 Configure posture assessment and redirect ACL.

Example:

```
ip http server
ip http secure-server
```

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

Step 4 Configure device tracking.

Example:

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

Note
The IP address mentioned belongs to ISE.

Step 5 Configure CoA reauthentication and dACL on ISE.

a) Create a downloadable ACL and define the ACEs in it.

ACL name: TEST_IP_PERMIT_ALL

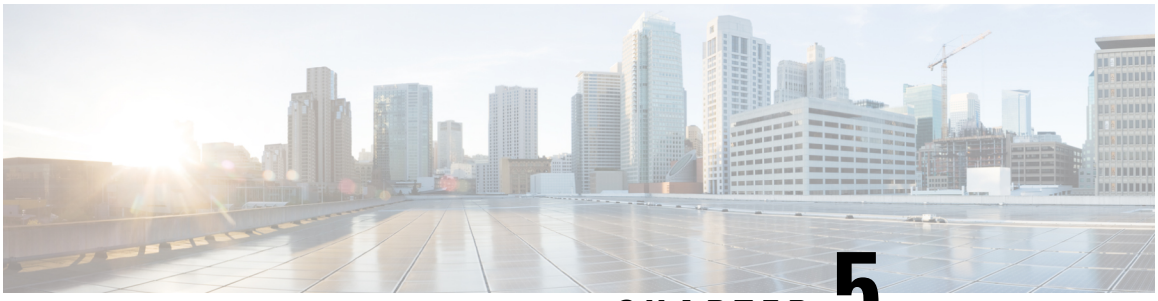
ACEs: permit ip any any

b) Create an authorization result and choose the downloadable ACL as dACL.

c) Navigate to **Administration** > **System** > **Settings** > **Policy Settings**, and in **Policy Sets** configuration, select the authorization result as authorization policy.

Step 6 After creating the CLI Add-On template, attach it to a device template.

SD-WAN Manager pushes all the configuration in the device template onto your device.



CHAPTER 5

Role-Based Access Control

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

Table 15:

Feature Name	Release Information	Feature Description
Co-Management: Granular Role-Based Access Control	Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature introduces Role-Based Access Control (RBAC) based on sites, scope, or roles. It is a method of authorizing system access for users based on a combination of role and scope of a user. You can create scopes, users, and roles with required read and write permissions for Cisco SD-WAN Manager policies. RBAC prevents unauthorized access and reduces the risk of data breaches and other security incidents.
Canadian French language support on Cisco Catalyst SD-WAN Manager	Cisco Catalyst SD-WAN Manager Release 20.13.1	Added support for using Canadian French for Cisco SD-WAN Manager user interface.
RBAC by resource group	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature introduces Role-Based Access Control (RBAC) based on sites or resource groups. It is a method of authorizing system access for users based on a combination of user groups and resource groups. For large Cisco Catalyst SD-WAN deployments across multiple geographical locations, this feature helps you to split the network administration among different regional administrators.

Feature Name	Release Information	Feature Description
RBAC for policies	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature allows you to create users and user groups with required read and write permissions for Cisco SD-WAN Manager policies. RBAC for policies provides users with the access to all the details of policies to help maximize the operational efficiency. It makes it easier to meet configuration requirements and ensures that authorized users on the system are only given access to what they need.
Co-Management: Granular RBAC for feature templates	Cisco vManage Release 20.7.1	This feature introduces greater granularity in assigning RBAC permissions for template use. This enables you to give a tenant self-management of network configuration tasks. Network administrators and managed service providers can use this feature to assign permissions to their end customers.
Co-Management: Improved granular configuration task permissions	Cisco vManage Release 20.9.1	To enable a user to self-manage specific configuration tasks, you can assign the user permissions to perform specific configuration tasks while excluding other tasks. This feature introduces numerous new permission options, enabling fine granularity in determining which configuration task permissions to provide to a user.

Feature Name	Release Information	Feature Description
RBAC for security operations and network operations default user groups	Cisco vManage Release 20.9.1	This feature provides the following default user groups: • network_operations user group for non-security policies • security_operations user group for security policies RBAC for policies allows you to create users and user groups with the required read and write permissions for security and non-security policies. Users can perform configuration and monitoring actions only for the authorized policy type.
Co-Management: Improved granular configuration for resource group features	Cisco vManage Release 20.11.1	To enable a user to self-manage specific configuration tasks, you can assign the user permissions to perform specific configuration tasks while excluding other tasks. This feature introduces new permission options for the following configuration groups and feature profiles. • AppQoE under other feature profile • GPS under transport feature profile • Cisco VPN Interface GRE under WAN/LAN profile. • Cisco VPN Interface IPsec under WAN profile. • Cisco Multicast under LAN profile. • UCSE under other feature profile. • IPv4 Tracker and Tracker Group under transport and service feature profiles. • IPv6 DIA Tracker and Tracker Group, under transport feature profile.

Feature Name	Release Information	Feature Description
Assigning roles locally for SSO-authenticated users	Cisco vManage Release 20.11.1	If you are using an identity provider, such as Okta, for security assertion markup language (SAML)-based single sign-on (SSO), then in most use cases, you define user roles through the identity provider. This feature enables you to assign user groups locally in Cisco SD-WAN Manager, in case no roles are defined for the user by the identity provider.

Role-Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and scope.

A role is a set of permissions the user receives that

- defines the privileges a user has in the system
- specifies the allowed actions (read, write, or deny) for different APIs or functionalities, and
- determines access based on the organizations or domains (locales) assigned to the user.

Scope defines the set of objects (sites, devices or templates) a user can act on.

Users

A user is an entity that performs different actions in Cisco SD-WAN Manager and belongs to a role.

Users are not directly assigned privileges. To manage individual user privileges, you can assign the appropriate roles and scopes. A user is granted write access to system resources only when both the assigned role provides access privileges and the assigned locale permits access.

Permissions for users

- Users with read or write access can view and make changes to the selected features.
- Users with read access can only view information.
- Users with deny access cannot view information or make changes to Cisco IOS XE Catalyst SD-WAN.

System default roles

You cannot change system default roles. Cisco IOS XE Catalyst SD-WAN software provides these system default roles:

- basic: The basic role is a system default role and is pre-built in Cisco SD-WAN Manager. You cannot modify or delete it. To modify the role, create a copy and modify the copy as a new customer role.
- operator: The operator role is configurable and can be assigned to users at any privilege level. This role is intended for users who have permission to only view information.
- netadmin: The netadmin role is a non-configurable role. By default, this role includes the admin user. You can add other users to this role. Users with this role are permitted to perform all operations on the device.
- network_operations: The network_operations role is a non-configurable role. Users in this role 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 an application aware routing policy or Cflowd policy. Users with this role are authorized to apply policies to a device, revoke applied policies, and edit device templates.
- security_operations: The security_operations role is a non-configurable role. Users in this role 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 with this role require network_operations users to intervene on day-0 to deploy a 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 netadmin users can view the running and local configuration. Users associated with a predefined operator role do not have access to the running and local configurations. The predefined operator role provides read access for the template configuration. To assign a subset of admin privileges, create a new role with the selected features from the features list, grant both read and write access, and associate the role with the custom user.

Privileges for Role-Based Access Control

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

- Interface: Privileges for controlling the interfaces on the Cisco IOS XE Catalyst SD-WAN device.
- Policy: Privileges for controlling the 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 who belong to the netadmin group can install software on the system.
- System: General system-wide privileges.

Restrictions for configuring RBAC

Role and scope per user

From Cisco Catalyst SD-WAN Manager Release 20.13.1, you can only configure one role and one scope per user.

Enabling or disabling Cloud SaaS feeds

To enable or disable Cloud SaaS feeds, a user role requires write permission for the **Application Priority Write** option.

In Cisco Catalyst SD-WAN Manager Release 20.13.x and Cisco Catalyst SD-WAN Manager Release 20.14.x, a user with the security_operations role can enable or disable Cloud SaaS feeds. From Cisco Catalyst SD-WAN Manager Release 20.15.1, the security_operations role does not include write permission for the **Application Priority Write** option, and does not support enabling or disabling Cloud SaaS feeds.

Granular RBAC for feature templates

To use any of the template restriction options that are provided for RBAC for co-management, provide permissions for the **Template Configuration** option. If a specific user role does not have any permissions assigned in the **Template Configuration** option, the **Templates** menu will not be visible to the user in SD-WAN Manager. See User group permissions.

To enable an RBAC user to apply templates to devices, provide write permission to the **Template Deploy** option.

RBAC by VPN

RBAC by VPN is a network access control method that enables administrators to

- define VPN groups with one or more network segments
- assign users to specific VPN groups to manage and control their access, and
- restrict user permissions so that access and monitoring are limited to devices and features within designated VPN groups in Cisco SD-WAN Manager.

Restricted access capabilities for users assigned to a VPN group

RBAC by VPN provides these restricted access to users configured with a VPN group:

- Access to the VPN dashboard
- Monitor devices, network, and application status via VPN dashboard
- VPN dashboard information restricted to devices with segments in the VPN group
- Monitor option restricted to devices with segments in the VPN group
- Interface monitoring on each device restricted to interfaces of segments in the VPN group

VPN dashboard

Users configured with VPN group can access only the VPN dashboard in read-only mode. Users with admin access can create the VPN groups and access both the Admin Dashboard and VPN Dashboard(s). An admin user can access these dashboards by choosing **Dashboard** from the Cisco SD-WAN Manager menu.

RBAC with AAA

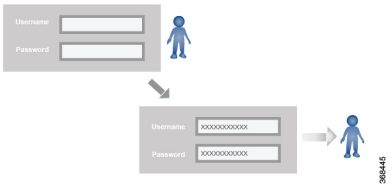
The Cisco Catalyst SD-WAN AAA software implements role-based access to control the authorization permissions for users on Cisco IOS XE Catalyst SD-WAN devices.

RBAC consists of three components:

- Users: They are allowed to log in to a Cisco IOS XE Catalyst SD-WAN device.
- User groups: They are collections of users.
- Privileges: These are associated with each group. Privileges define the commands that the users are authorized to issue.

Users and user groups

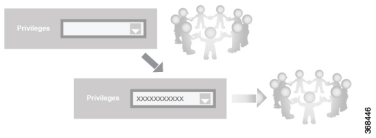
All users who are permitted to perform operations on a Cisco IOS XE Catalyst SD-WAN device device must have a login account. For the login account, you configure a username and a password on the device itself. These allow the user to log in to that device. A username and password must be configured on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



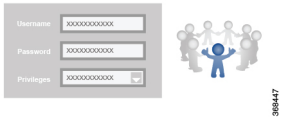
The Cisco Catalyst SD-WAN software provides one standard username, admin, which is a user who has full administrative privileges, similar to a UNIX superuser. By default, the admin username password is admin. You cannot delete or modify this username, but you can and should change the default password.

User groups pool together users who have common roles, or privileges, on the Cisco IOS XE Catalyst SD-WAN device. As part of configuring the login account information, you specify which user group or groups that

user is a member of. You do not need to specify a group for the admin user, because this user is automatically in the user group netadmin and is permitted to perform all operations on the SD-WAN device.



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



Standard user groups

Cisco Catalyst SD-WAN software provides standard user groups and allows creation of custom user groups as needed.

- **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.
- **network_operations**: From Cisco vManage Release 20.9.1, network_operations user group is supported. 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.
- **security_operations**: From Cisco vManage Release 20.9.1, security_operations user group is supported. 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 All user groups, regardless of the read or write permissions selected, can view the information displayed on the Cisco SD-WAN Manager Dashboard screen.

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.

User authorization rules for operational and configuration commands

The user authorization rules for operational commands are based simply on the username. Any user who is allowed to log in to the Cisco IOS XE Catalyst SD-WAN device can execute most of the 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.

Any user can issue the **config** command to enter configuration mode. In configuration mode, users are allowed to issue any general configuration command. Also, users can configure their passwords using the **system aaa user** *self* **password** *password* command and then commit the 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.

This table 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)

CLI Command	Any User	Admin User
monitor	X	X
nslookup	X	X
paginate	X	X
ping	X (users in netadmin group only)	X (users in netadmin group only)
poweroff	—	X(users in netadmin group only)
prompt1	X	X
prompt2	X	X
quit	X	X
reboot	—	X (users in netadmin group only)
request aaa request admin-tech request firmware request interface-reset request nms request reset request software	—	X (users in netadmin group only)
request execute request download request upload	X	X
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)		

CLI Command	Any User	Admin User
tcpdump	X	X
timestamp	X	X
tools ip-route	X	X
tools netstat	X	X
tools nping	X	X
traceroute	X	X
vshell	X (The availability of vshell command is unavailable to all users that are not in netadmin group in Cisco vManage Release 20.9.5.)	X (The vshell AAA authorized access is limited only to users that are in netadmin group.)

User group authorization rules for operational commands

This table lists the user group authorization rules for operational commands.

Table 16: User group authorization rules 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	

Operational Command	Interface	Policy	Routing	Security	System
clear interface	X				
clear ip			X		
clear notification					X
clear omp			X		
clear orchestrator				X	
clear ospf			X		
clear pim			X		
clear policy		X			
clear pppoe	X				
clear system					X
clear tunnel				X	
clear wlan	X				
clear ztp				X	X
clock					X
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		

Operational Command	Interface	Policy	Routing	Security	System
debug pim			X		
debug resolver			X		
debug snmp					X
debug sysmgr					X
debug transport					X
debug ttm					X
debug vdaemon				X	X
debug vrrp				X	
debug wlan	X				
request certificate				X	
request control-tunnel				X	
request controller				X	
request controller-upload				X	
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

Operational Command	Interface	Policy	Routing	Security	System
show app		X			
show app-route		X			
show arp	X				
show bfd			X		X
show bgp			X		
show boot-partition					X
show bridge	X				
show cellular	X				
show certificate				X	
show clock					X
show control				X	X
show crash					X
show debugs—same as debug commands					
show dhcp					X
show external-nat				X	X
show hardware					X
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

Operational Command	Interface	Policy	Routing	Security	System
show orchestrator				X	
show ospf			X		
show pim			X		
show policer		X			
show policy		X			
show ppp	X				
show pppoe	X				
show reboot					X
show security-info				X	
show software					X
show system					X
show transport					X
show tunnel				X	
show uptime					X
show users					X
show version					X
show vrrp	X				
show wlan	X				
show ztp				X	

User group authorization rules for configuration commands

This table lists the user group authorization rules for configuration commands.

Table 17: User group authorization rules for configuration commands

Configuration Command	Interface	Policy	Routing	Security	System
apply-policy		X			
banner					X
bfd			X		X
bridge	X				

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

RBAC by resource group

RBAC by resource group

RBAC by resource groups is a method of restricting or authorizing system access for users based on user groups and resource groups.

A user group defines the privileges of a user in the system and the resource group defines the organizations (domains) to which a user is allowed access.

Assigning user and resource groups

Users are not directly assigned privileges, but you can manage individual user privileges by assigning the appropriate user and resource groups.

For large Cisco Catalyst SD-WAN deployments across multiple geographical locations, you can split the network administration among different regional administrators.

Network administrators can be classified as global administrators or regional administrators, based on the user groups and resource groups assigned to them:

- Global administrators have access to all resources in every resource group and have complete read-write privileges for all features.
- Regional administrators also have full read-write privileges for all the features. However, the resources they can access are limited by the resource groups assigned to them.

Global admin

A global admin is responsible for overseeing the entire network, but is not involved in the operations of the individual devices on a daily basis. User accounts in the global resource group have access to all resources.

Any user in a single tenant setup with netadmin privileges who is also part of global resource group is considered a global admin. The default admin user on SD-WAN Manager is also a global-admin. The global resource group contains all WAN edges and controllers in a single view.

A global admin can:

- assign devices to their corresponding regions
- assign regional admin accounts
- manage controllers
- maintain sharable and centralized configurations
- operate on the individual devices when necessary
- switch to view only a specific resource group and can create templates
- assign more global admins

Local resource group admins, also called regional admins can clone global templates and reuse them within their resource groups.

Regional admin

A regional admin is responsible for day-to-day operations (configuration, monitoring, onboarding, and so on) for devices in the corresponding regions. Regional admins do not have access to or visibility into devices outside of their region. A regional admin can create these user groups:

- Resource group admin – full read/write access to devices in the corresponding resource group, can troubleshoot, monitor, attach, or detach templates for the WAN edges in their group
- Resource group operator – read-only access to WAN edges within their resource group
- Resource group basic – basic access within their resource group

Resource group admins can create new templates and attach or detach them from WAN edges in their group. They can also copy and reuse global templates.

The resource group determines the resources accessible to a user; however, the level of access is controlled by the existing user group.

- If a user is in resource group resource_group_a and user group resource_group_admin, they have full read/write access to all resources in resource_group_a.
- If a user is in resource group resource_group_a and user group resource_group_operator, they have read-only access to all resources in resource_group_a.
- If a user is in resource group resource_group_a and user group resource_group_basic, they have read-only access to interface and system resources in resource_group_a.

Global resource group

The global group is a special, system-predefined resource group with these different access control rules:

- Users within this group are considered as global-admins, who can have full access to all resources (devices, templates and policies) in the system and they can manage the resource groups and assign resources and users to groups.
- All other users have read-only access to resources within this group.
- The system default admin account (or tenantadmin account in a multitenant setup) is always in this group. This privilege cannot be changed. However, the admin account may add/remove other user accounts to or from this group.

IdP (SSO)-managed group

An identity provider (IdP) is a service that stores and verifies user identity. IdPs typically work with single sign-on (SSO) providers to authenticate users. If a user is authenticated with a SSO service of an IdP, the group information is also provided and managed by the IdP. An IdP passes the information about the user, including the user name and all the group names, where the user belongs to. SD-WAN Manager matches the group names with the group names stored in the database to further distinguish if a particular group name passed from IdP is for user group or resource group or VPN group.

Configure resource groups

From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco vManage Release 20.5.1 you can configure resource groups to restrict or authorize user access to specific sets of resources.

Procedure

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

The table displays a list of resource groups configured in SD-WAN Manager.

Step 2 To edit or delete a resource group, click **...**, and click **Edit** or **Delete**.

Step 3 To add s new resource group, click **Add Resource Group**.

Step 4 Enter **Resource Group Name** and the **Description**.

Step 5 Under **Site ID**, enter **Range** or **Select ID(S)** from the drop-down list to include in the resource group.

Step 6 To add the resource group to a device, click **Add**.

Multitenancy support

With Cisco Catalyst SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco SD-WAN Manager. The tenants share Cisco SD-WAN Manager instances, Cisco SD-WAN Validator, and Cisco SD-WAN Controller. The domain name of the service provider has subdomains for each tenant. Cisco SD-WAN Manager is deployed and configured by the service provider. The provider enables multitenancy and creates a Cisco SD-WAN Manager cluster to serve tenants. Only the provider can access a Cisco SD-WAN Manager instance through the SSH terminal.

Provider has these features:

- Resource group is not applicable as the provider manages only the controllers.

- When provider provisions a new tenant, the default user account for the tenant is tenantadmin.
- Other user accounts created by the provider are included in the default global resource group.
- When a provider creates a template for a tenant, the template is included in the global resource group.

Granular RBAC

Granular RBAC for templates

When setting user group permissions, use the template permissions defined in this section. This approach allows you to provide an RBAC user with specific access to various types of templates and control which device configurations they can apply.

From Cisco vManage Release 20.7.1, you can use these template permissions:

Permission	Description
CLI Add-On Template	Provides access to the CLI add-on feature template.
Device CLI Template	Provides access to the device CLI template.
SIG Template	Provides access to the SIG feature template and SIG credential template.
Other Feature Templates	Provides access to all feature templates except the SIG feature template, SIG credential template, and CLI add-on feature template.
Feature Profile	Provides access to all feature profiles.
Config Group	Provides access to all configuration groups.

Expand each feature profile to specify granular RBAC. After you set the permissions for the user group, verify that you can access the required feature profiles under **Templates** > **Configuration Groups**.

Single-tenant and multi-tenant scenarios

You can use granular RBAC for feature templates in single-tenant and multi-tenant Cisco SD-WAN Manager scenarios.

You can create user groups to assign specific permissions to a tenant's various teams, enabling teams to manage only specific network services without granting permission to use device CLI templates.

Avoid granting tenants the permission to apply device CLI templates because they can override any other template or device configuration. For example, create a user group for a tenant's security operations group. Grant them read/write access only to the SIG Template option to enable them to manage security configurations.

Benefits of granular RBAC

From Cisco vManage Release 20.7.1, the permissions configured for co-management in Cisco Catalyst SD-WAN allow for very detailed and specific control over who can access and modify network configurations. They are useful when using Cisco Catalyst SD-WAN with tenants, enabling you to provide a tenant access

to specific types of templates. This setup lets tenants manage their own network configuration tasks within their own VPN.

For information about the permissions added for co-management, see Granular RBAC for templates, on page 77.

RBAC for policies

RBAC for policies

RBAC for policies allows a user or user group to have selective read and write (RW) access to Cisco SD-WAN Manager policies.

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, a user can perform these actions with read and write access:

- For Cflowd policy: Configure Cflowd policy, but cannot configure application-aware routing policy.
- For application aware routing (AAR) policy: Configure application-aware routing policy, but cannot configure other policies.

Note This feature is only supported for centralized and localized policies, but not supported for security policies.

Configure RBAC for policies

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, you can configure required access for policies.

Procedure

Step 1 Create user groups with required read or write access to selected control or data policies.

For details on creating user groups, refer Create User Groups.

Step 2 Create users and assign them to required user groups. .

Refer Add Users.

Step 3 Create or modify or view policy configurations as required.

For information about configuring policies, see Configure Centralized Policies Using Cisco SD-WAN Manager.

Modify policy configurations

FromCisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, you can modify or update policy configurations as per your requirement.

Simply log in to Cisco SD-WAN Manager to view the user group components that are assigned to you and you can modify the policy configurations. For more details on configuring policies, see Cisco Catalyst SD-WAN Policies Configuration Guide

Configure RBAC for CFlowd policy

Create a CFlowd user group

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, you can create a CFlowd user group and assign users to modify a CFlowd data policy.

Procedure

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

Step 2 Click **User Groups** and **Add User Group**.

Step 3 Enter **User Group Name**.

For example, cflowd-policy-only.

Step 4 Check the Read or Write check box against the CFlowD Policy feature that you want to assign to a user group.

Step 5 Click **Add**.

You can view the new user group in the left navigation path.

Step 6 Click **Edit** to edit the existing read or write rules.

Step 7 Click **Save**.

Create a CFlowd policy user

To modify a CFlowd policy, create a CFlowd policy user and assign it to the Cflowd policy user group.

Procedure

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

Step 2 Click **Users**.

Step 3 Click **Add User**.

Step 4 In the Add New User page, enter **Full Name**, **Username**, **Password**, and **Confirm Password** details.

Step 5 Choose **cflowd-policy-only** from the **User Groups** drop-down list.

Allow the **Resource Group** to select the default resource group.

Step 6 Click **Add**.

You can view the new user in the **Users** window.

Step 7 To edit the existing read or write rules for a user, click **Edit**.

Modify a CFlowd policy

You can modify CFlowd policies associated with the related CFlowd user group.

Procedure

Step 1 Log in to Cisco SD-WAN Manager with the CFlowd user credentials.

You can access only CFlowd policies as your login is associated to cflowd-policy-only user group.

Step 2 You can create, modify, or update the configurations based on your requirement.

Assigning roles to users defined by identity providers

From Cisco vManage Release 20.11.1 you can manage user roles and permissions through the identity provider (IdP) when users authenticate via Okta to log into Cisco SD-WAN Manager.

When a user logs in, SD-WAN Manager retrieves the user's role(s) from the IdP and maps them to user group permissions in SD-WAN Manager. The permissions granted to the user correspond to these mapped user groups.

If a user does not have a role defined in the IdP, a network administrator—who has access to SD-WAN Manager but does not have access to the IdP—can assign the user to a specific local user group within SD-WAN Manager to provide the necessary permissions.

However, if both a role is defined for a user in the IdP and a user group is assigned locally in SD-WAN Manager, the role defined in the IdP will take precedence over the local assignment.

This table summarizes the methods available for assigning specific permissions to a user:

IdP for SAML SSO	Roles defined in the IdP	How user permissions are defined
Not using an IdP	Not applicable	In SD-WAN Manager, assign a user to one or more user groups locally. This provides the user with the corresponding user group permissions.

IdP for SAML SSO	Roles defined in the IdP	How user permissions are defined
Using an IdP	IdP has one or more roles defined for the user.	Define roles for the user through the IdP. SD-WAN Manager provides the user with the user group permissions corresponding to the roles.
	IdP does not have a role defined for the user.	Use the **Remote User** option for adding a user (**Administration** > **Manage Users** > **Add User**). See Add a User. In SD-WAN Manager, assign a user to one or more user groups locally. This provides the user with the corresponding user group permissions.

Configure RBAC

Configure scope

Procedure

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

By default **Scope** menu is selected. The table displays the list of scopes configured in the device.

Step 2 Click **Add Scope**.

Step 3 Enter **Scope Name** and **Description**.

Step 4 Click **Add Nodes**.

Step 5 Choose the required nodes and click **Save**.

You can click **Edit Nodes** to update the existing nodes in the list.

Step 6 (Optional) In the **Associations** pane, click **Add Users** to associate users.

a) In the **Add Users** pop-up window, choose the users that you want to add.

b) Click **Save**.

The selected users are associated to a scope.

Step 7 (Optional) In the **Configurations** tab, click **Add Configurations** to add configurations. Choose the available configurations from the following tabs:

a) **Configuration Group**

b) **Device Template**

c) **Feature Template**

d) **Feature Profile**
e) **Security Policy**
f) **Localized Policy**

Step 8 Click **Save**.

A new scope with nodes, users and required configurations is created.

Configure roles

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access**.
Step 2 Click **Roles**.
The table displays the list of roles configured in the device.
Step 3 Click **Add Role**.
Step 4 Enter **Custom Role Name** in the **Add Custom Role** page.
Step 5 Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to assign a role.
Step 6 Click **Add**.

You can view the new role in the table in the **Roles** page.

Copy custom role

To create a copy of a custom role, use these steps.

Procedure

Step 1 In the list of roles, for the role you wish to copy, click **...**, and click **Copy**.
The **Copy Custom Role** page is displayed.
Step 2 Enter **Custom Role Name**.
Step 3 Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to update for a role.
Step 4 Click **Copy**.

You can view the new role in the table in the **Roles** page.

Edit custom role

Procedure

Step 1 In the list of roles, for the role you wish to copy, click **...**, and click **Edit**.

The **Edit Custom Role** page is displayed.

Step 2 Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to update for a role.

Note
Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, the permissions for a role and its descendents may differ in the Deny/Read/Write table. Therefore, do not assume the parent role as the entire role for the sub-tree under it.

If you have a role with write permissions for Configuration Groups but deny or read permission for deploy, a **Change device variables** button appears instead of **Deploy** button. This button allows you to modify device-specific values during the deploy process, without initiating the deployment.

Step 3 Click **Update**.

You can view the updated role in the table in the **Roles** page.

Delete a role

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

Procedure

Step 1 Choose the role you wish to delete, click **...**, and click **delete**.

The **Warning** page is displayed.

Step 2 To confirm the deletion of the role, click **Delete**.

This deletes the role.

Prerequisites for Application Catalog features

You can grant certain permissions to a custom role for viewing and creating applications through the **Discovered Applications** page. **Discovered Applications** appear on the **Configuration** > **Application Catalog** > **Discovered Applications** page.

To enable a custom role to view discovered applications, grant these permissions:

- read permission for **Cloud OnRamp**

- read permission for
  - **Policy Configuration**
  - **Policy Group**
  - **Security Policy Configuration**
  - **Feature Profile** > **Embedded Security**, or
  - **Feature Profile** > **Embedded Security** > **NgFirewall**

To enable a custom role to create custom applications from **Discovered Applications**, grant write permissions for these:

- **Policy Configuration**
- **Policy Group**
- **Security Policy Configuration**
- **Feature Profile** > **Embedded Security**, or
- **Feature Profile** > **Embedded Security** > **NgFirewall**

Manage user group permissions

User group permissions for Cisco IOS XE Catalyst SD-WAN device

Table 18: User Group Permissions: Cisco IOS XE Catalyst SD-WAN devices

Feature	Read Permission	Write Permission
Alarms	Set alarm filters and view the alarms generated on the devices on the **Monitor** > **Logs** > **Alarms** page. Cisco vManage Release 20.6.x and earlier: Set alarm filters and view the alarms generated on the devices on the **Monitor** > **Alarms** page.	No additional permissions.

Feature	Read Permission	Write Permission
Audit Log	Set audit log filters and view a log of all the activities on the devices on the **Monitor** > **Logs** > **Alarms** page and the **Monitor** > **Logs** > **Audit Log** page. Cisco vManage Release 20.6.x and earlier: Set audit log filters and view a log of all the activities on the devices on the **Monitor** > **Alarms** page and the **Monitor** > **Audit Log** page.	No additional permissions.
Certificates	View a list of the devices in the overlay network under **Configuration** > **Certificates** > **WAN Edge List**. View a certificate signing request (CSR) and certificate on the **Configuration** > **Certificates** > **Controllers** window. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.	Validate and invalidate a device, stage a device, and send the serial number of valid controller devices to the Cisco Catalyst SD-WAN Validator on the **Configuration** > **Certificates** > **WAN Edge List** window. Generate a CSR, install a signed certificate, reset the RSA key pair, and invalidate a controller device on the **Configuration** > **Certificates** > **Controllers** window. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.
CLI Add-On Template (Minimum supported release: Cisco vManage Release 20.7.1)	View the CLI add-on feature template on the **Configuration** > **Templates** window. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, delete, and copy a CLI add-on feature template on the **Configuration** > **Templates** window. **Note** These operations require write permission for **Template Configuration**. **Note** For information about this option, see Information About Granular RBAC for Feature Templates

Feature	Read Permission	Write Permission
Cloud OnRamp	View the cloud applications on the**Configuration** > **Cloud OnRamp for SaaS** and **Configuration** > **Cloud OnRamp for IaaS** window.	No additional permissions.
Cluster	View information about the services running on SD-WAN Manager, a list of devices connected to a SD-WAN Manager server, and the services that are available and running on all the SD-WAN Manager servers in the cluster on the **Administration** > **Cluster Management** window.	Change the IP address of the current SD-WAN Manager, add a SD-WAN Manager server to the cluster, configure the statistics database, edit, and remove a SD-WAN Manager server from the cluster on the **Administration** > **Cluster Management** window.
Colocation	View the cloud applications on the **Configuration** > **Cloud OnRamp for Colocation** window.	No additional permissions.
Config Group > **Device** > **Deploy** (Minimum supported release: Cisco vManage Release 20.9.1)	This permission does not provide any functionality.	Deploy a configuration onto Cisco IOS XE Catalyst SD-WAN devices. **Note** To edit an existing feature configuration requires write permission for **Template Configuration**. For more details on deploying devices, see Deploy Devices.
Device CLI Template (Minimum supported release: Cisco vManage Release 20.7.1)	View the device CLI template on the **Configuration** > **Templates** window. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, delete, and copy a device CLI template on the **Configuration** > **Templates** window. **Note** These operations require write permission for **Template Configuration**. **Note** For information about this option, see Information About Granular RBAC for Feature Templates

Feature	Read Permission	Write Permission
Device Inventory	View the running and local configuration of devices, a log of template activities, and the status of attaching configuration templates to devices on the **Configuration** > **Devices** > **WAN Edge List** window. View the running and local configuration of the devices and the status of attaching configuration templates to controller devices on the **Configuration** > **Devices** > **Controllers** window. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.	Upload a device's authorized serial number file to SD-WAN Manager, toggle a device from SD-WAN Manager configuration mode to CLI mode, copy a device configuration, and delete the device from the network on the **Configuration** > **Devices** > **WAN Edge List** window. Add and delete controller devices from the overlay network, and edit the IP address and login credentials of a controller device on the **Configuration** > **Devices** > **Controllers** window. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

Feature	Read Permission	Write Permission
Device Monitoring	View the geographic location of the devices on the **Monitor** > **Geography** window. View events that have occurred on the devices on the **Monitor** > **Logs** > **Events** page. Cisco vManage Release 20.6.x and earlier: View events that have occurred on the devices on the **Monitor** > **Events** page. View a list of devices in the network, along with device status summary, SD-WAN Application Intelligence Engine (SAIE) and Cflowd flow information, transport location (TLOC) loss, latency, and jitter information, control and tunnel connections, system status, and events on the **Monitor** > **Devices** page (only when a device is selected). **Note** In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow. Cisco vManage Release 20.6.x and earlier: Device information is available in the **Monitor** > **Network** page.	Ping a device, run a traceroute, and analyze the traffic path for an IP packet on the **Monitor** > **Devices** page (only when a device is selected). **Note** These operations require read and write permissions for **Device Monitoring**.
Device Reboot	View the list of devices on which the reboot operation can be performed on the **Maintenance** > **Device Reboot** window.	Reboot one or more devices on the **Maintenance** > **Device Reboot** window.
Disaster Recovery	View information about active and standby clusters running on SD-WAN Manager on the **Administration** > **Disaster Recovery** window.	No additional permissions.

Feature	Read Permission	Write Permission
Events	View the geographic location of the devices on the **Monitor** > **Logs** > **Events** page. View the geographic location of the devices on the **Monitor** > **Events** page.	Ping a device, run a traceroute, and analyze the traffic path for an IP packet on the **Monitor** > **Logs** > **Events** page (only when a device is selected).
Feature Profile > **Other** > **Thousandeyes** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **ThousandEyes** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Other Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **ThousandEyes** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Other Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Dhcp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **DHCP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **DHCP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Lan/Vpn** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **LAN/VPN** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **LAN/VPN** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Lan/Vpn/Interface/Ethernet** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Ethernet Interface** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Ethernet Interface** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Service** > **Lan/Vpn/Interface/Svi** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **SVI Interface** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **SVI Interface** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Routing/Bgp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Routing/BGP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Routing/BGP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Routing/Ospf** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Routing/OSPF** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Routing/OSPF** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Switchport** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Switchport** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Switchport** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Service** > **Wirelesslan** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Wireless LAN** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Wireless LAN** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Interface/Ethernet** > **Aaa** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **AAA** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **AAA** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Interface/Ethernet** > **Banner** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Banner** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Banner** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Basic** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Basic** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Basic** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **System** > **Bfd** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **BFD** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **BFD** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Global** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Global** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Global** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Logging** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Logging** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Logging** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Ntp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **NTP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **NTP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **System** > **Omp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **OMP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **OMP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Snmp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **SNMP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **SNMP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Cellular Controller** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Cellular Controller** settings on the **Configuration** > **Templates** > **(View a configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Cellular Controller** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Cellular Profile** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Cellular Profile** settings on the **Configuration** > **Templates** > **(View a configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Cellular Profile** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Transport** > **Management/Vpn** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Management VPN** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Management VPN** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Management/Vpn/Interface/Ethernet** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Management Ethernet Interface** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Management VPN and Management Internet Interface** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Routing/Bgp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **BGP Routing** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **BGP Routing** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Tracker** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Tracker** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Tracker** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Transport** > **Wan/Vpn** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Wan/Vpn** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Wan/Vpn** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Wan/Vpn/Interface/Cellular** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Wan/Vpn/Interface/Cellular** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Wan/Vpn/Interface/Cellular** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Wan/Vpn/Interface/Ethernet** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Wan/Vpn/Interface/Ethernet** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Wan/Vpn/Interface/Ethernet** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Integration Management	View information about controllers running on SD-WAN Manager, on the **Administration** > **Integration Management** window.	No additional permissions.
License Management	View license information of devices running on SD-WAN Manager, on the **Administration** > **License Management** window.	On the **Administration** > **License Management** page, configure use of a Cisco Smart Account, choose licenses to manage, and synchronize license information between SD-WAN Manager and the license server.

Feature	Read Permission	Write Permission
Interface	View information about the interfaces on a device on the **Monitor** > **Devices** > **Interface** page. Cisco vManage Release 20.6.x and earlier: View information about the interfaces on a device on the **Monitor** > **Network** > **Interface** page	Edit **Chart Options** to select the type of data to display, and edit the time period for which to display data on the **Monitor** > **Devices** > **Interface** page.
Application Monitoring (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1)	View the application health of the devices on the **Monitor** > **Applications** window.	View the application health of the devices on the **Monitor** > **Applications** window.
Manage Users	View users and user groups on the **Administration** > **Manage Users** window.	Add, edit, and delete users and user groups from SD-WAN Manager, and edit user group privileges on the **Administration** > **Manage Users** window.
Other Feature Templates (Minimum supported release: Cisco vManage Release 20.7.1)	View all feature templates except the SIG feature template, SIG credential template, and CLI add-on feature template on the **Configuration** > **Templates** window. **Note** This operation requires read permission for **Template Configuration**. **Note** To check the mutual authentication option, you need read permission for certificates. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1)	Create, edit, delete, and copy all feature templates except the SIG feature template, SIG credential template, and CLI add-on feature template on the **Configuration** > **Templates** window. **Note** These operations require write permission for **Template Configuration**. **Note** For information about this option, see Information About Granular RBAC for Feature Templates **Note** To check the mutual authentication option, you need write permission for certificates. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1)

Feature	Read Permission	Write Permission
Policy	View the common policies for all Cisco Catalyst SD-WAN Controllers or devices in the network on the **Configuration** > **Policies** window.	Create, edit, and delete the common policies for all Cisco Catalyst SD-WAN Controllers or devices in the network on the **Configuration** > **Policies** window.
Policy Configuration	View the list of policies created and details about them on the **Configuration** > **Policies** window.	Create, edit, and delete the common policies for all the Cisco Catalyst SD-WAN Controllers and devices in the network on the **Configuration** > **Policies** window.
Policy Deploy	View the current status of the Cisco Catalyst SD-WAN Controllers to which a policy is being applied on the **Configuration** > **Policies** window.	Activate and deactivate the common policies for all SD-WAN Manager servers in the network on the **Configuration** > **Policies** window.
RBAC VPN	View the VPN groups and segments based on roles on the **Monitor** > **VPN** page. Cisco vManage Release 20.6.x and earlier: View the VPN groups and segments based on roles on the **Dashboard** > **VPN Dashboard** page.	Add, edit, and delete VPNs and VPN groups from SD-WAN Manager, and edit VPN group privileges on the **Administration** > **VPN Groups** window.
Routing	View real-time routing information for a device on the **Monitor** > **Devices** > **Real-Time** page. Cisco vManage Release 20.6.x and earlier: View real-time routing information for a device on the **Monitor** > **Network** > **Real-Time** page.	Add command filters to speed up the display of information on the **Monitor** > **Devices** > **Real-Time** page.
Security	View the current status of the Cisco Catalyst SD-WAN Controllers to which a security policy is being applied on the **Configuration** > **Security** window.	Activate and deactivate the security policies for all SD-WAN Manager servers in the network on the **Configuration** > **Security** window.
Security Policy Configuration	Activate and deactivate the common policies for all SD-WAN Manager servers in the network on the **Configuration** > **Security** > **Add Security Policy** window.	Activate and deactivate the security policies for all SD-WAN Manager servers in the network on the **Configuration** > **Security** > **Add Security Policy** window.

Feature	Read Permission	Write Permission
Session Management	View user sessions on the **Administration** > **Manage Users** > **User Sessions** window.	Add, edit, and delete users and user groups from SD-WAN Manager, and edit user sessions on the **Administration** > **Manage Users** > **User Sessions** window.
Settings	View the organization name, Cisco Catalyst SD-WAN Validator DNS or IP address, certificate authorization settings, software version enforced on a device, custom banner on the SD-WAN Manager login page, and the current settings for collecting statistics on the **Administration** > **Settings** window.	Edit the organization name, Cisco Catalyst SD-WAN Validator DNS or IP address, certificate authorization settings, software version enforced on a device, custom banner on the SD-WAN Manager login page, current settings for collecting statistics, generate a certificate signing request (CSR) for a web server certificate, and install a certificate on the **Administration** > **Settings** window.
SIG Template (Minimum supported release: Cisco vManage Release 20.7.1)	View the SIG feature template and SIG credential template on the **Configuration** > **Templates** window. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, delete, and copy a SIG feature template and SIG credential template on the **Configuration** > **Templates** window. **Note** These operations require write permission for **Template Configuration**. **Note** For information about this option, see Information About Granular RBAC for Feature Templates
SIG Tunnels (Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.12.x	View information about the SIG tunnels on the **Monitor** > **Tunnels** > **SIG Tunnels** page.	View information about the SIG tunnels on the **Monitor** > **Tunnels** > **SIG Tunnels** page.
Software Upgrade	View a list of devices, the custom banner on SD-WAN Manager on which a software upgrade can be performed, and the current software version running on a device on the **Maintenance** > **Software Upgrade** window.	Upload new software images on devices, upgrade, activate, and delete a software image on a device, and set a software image to be the default image on devices on the **Maintenance** > **Software Upgrade** window.

Feature	Read Permission	Write Permission
System	View system-wide parameters configured using SD-WAN Manager templates on the **Configuration** > **Templates** > **Device Templates** window. **Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.	Configure system-wide parameters using SD-WAN Manager templates on the **Configuration** > **Templates** > **Device Templates** window. **Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.
Template Configuration	View feature and device templates on the **Configuration** > **Templates** window.	Create, edit, delete, and copy a feature or device template on the **Configuration** > **Templates** window. **Note** From Cisco vManage Release 20.7.1, to create, edit, or delete a template that is already attached to a device, the user requires write permission for the Template Deploy option.
Template Deploy	View the devices attached to a device template on the **Configuration** > **Templates** window.	Attach a device to a device template on the **Configuration** > **Templates** window.
Tools	Use the **admin tech** command to collect the system status information for a device on the **Tools** > **Operational Commands** window.	Use the **admin tech** command to collect the system status information for a device, and use the **interface reset** command to shut down and then restart an interface on a device in a single operation on the **Tools** > **Operational Commands** window. Rediscover the network to locate new devices and synchronize them with SD-WAN Manager on the **Tools** > **Operational Commands** window. Establish an SSH session to the devices and issue CLI commands on the **Tools** > **Operational Commands** window.
vAnalytics	Launch Cisco SD-WAN Analytics from > **vAnalytics** window.	No additional permissions.

Feature	Read Permission	Write Permission
Workflows	Launch workflow library from > **Workflows** window.	No additional permissions.
Config Group > **Device** > **Deploy** (Minimum supported release: Cisco vManage Release 20.11.1)	View the devices associated to a configuration group on the **Configuration** > **Templates** > **Edit Configuration Group** > **Associated Devices** window.	Deploy a configuration onto Cisco IOS XE Catalyst SD-WAN devices. **Note** To edit an existing feature configuration requires write permission for **Template Configuration**. For more details on deploying devices, see Deploy Devices.
Feature Profile > **Transport** > **IPv4 Tracker and Tracker Group** (Minimum supported release: Cisco vManage Release 20.11.1)	View the IPv4 Tracker and Tracker Group settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **IPv4 Tracker and Tracker Group** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **IPv6 Tracker and Tracker Group** (Minimum supported release: Cisco vManage Release 20.11.1)	View the IPv6 Tracker and Tracker Group settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **IPv6 Tracker and Tracker Group** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Transport** > **Gps** (Minimum supported release: Cisco vManage Release 20.11.1)	View the GPS settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Gps** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Other** > **APPQoE** (Minimum supported release: Cisco vManage Release 20.11.1)	View the APPQoE settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Other** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **APPQoE** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Other** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Other** > **UCSE** (Minimum supported release: Cisco vManage Release 20.11.1)	View the UCSE settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Other** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **UCSE** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Other** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Wan Profile** > **Cisco VPN Interface IPSec** (Minimum supported release: Cisco vManage Release 20.11.1)	View the Cisco VPN Interface IPSec settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Wan Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Cisco VPN Interface IPSec** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Wan Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Wan/Lan Profile** > **Cisco VPN Interface GRE** (Minimum supported release: Cisco vManage Release 20.11.1)	View the Cisco VPN Interface GRE settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Wan/Lan Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Cisco VPN Interface GRE** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Wan/Lan Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Lan Profile** > **Cisco Multicast** (Minimum supported release: Cisco vManage Release 20.11.1)	View the Cisco Multicast settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Lan Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Cisco Multicast** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Lan Profile** section. **Note** These operations require write permission for **Template Configuration**.

To create Service, System, and Transport feature profiles using configuration groups, provide read and write permissions for each of these features to access each configuration group.

Permission type	Features
Read and write permissions	**Feature Profile** > **System**
	Feature Profile > **System** > **AAA**
	Feature Profile > **System** > **BFD**
	Feature Profile > **System** > **Banner**
	Feature Profile > **System** > **Basic**
	Feature Profile > **System** > **Logging**
	Feature Profile > **System** > **NTP**
	Feature Profile > **System** > **OMP**
	Feature Profile > **System** > **SNMP**
	Feature Profile > **Service**
	Feature Profile > **Service** > **BFD**
	Feature Profile > **Service** > **LAN/VPN**
	Feature Profile > **Service** > **LAN/VPN/Interface/Ethernet**
	Feature Profile > **Service** > **Routing/BGP**
	Feature Profile > **Service** > **Routing/OSPF**
	Feature Profile > **Service** > **Routing/DHCP**
	Feature Profile > **Service** > **Routing/Multicast**
	Feature Profile > **Transport**
	Feature Profile > **Transport** > **Routing/BGP**
	Feature Profile > **Transport** > **WAN/VPN**
	Feature Profile > **Transport** > **WAN/VPN/Interface/Ethernet**

Note For more details on configuring features using Configuration Groups, see Feature Management.

User group permissions for Cisco Catalyst Wireless Gateway devices

This table lists the user group read or write permissions for Cisco Catalyst Wireless Gateway devices.

Table 19: User group permissions: Cisco Catalyst Wireless Gateway devices

Feature	Read Permission	Write Permission
Feature Profile > **Teleworker** > **Basic** (Minimum supported release: Cisco vManage Release 20.9.1)	View the basic settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure tthe basic settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.
Feature Profile > **Teleworker** > **Cellular** (Minimum supported release: Cisco vManage Release 20.9.1)	View the cellular network settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure the cellular network settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.
Feature Profile > **Teleworker** > **Ethernet** (Minimum supported release: Cisco vManage Release 20.9.1)	View the ethernet settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure the ethernet settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.
Feature Profile > **Teleworker** > **NetworkProtocol** (Minimum supported release: Cisco vManage Release 20.9.1)	View the network protocol settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure the network protocol settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Teleworker** > **SecurityPolicy** (Minimum supported release: Cisco vManage Release 20.9.1)	View the security policy settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure the security policy settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.
Feature Profile > **Teleworker** > **Vpn** (Minimum supported release: Cisco vManage Release 20.9.1)	View the VPN settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure the VPN settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.
Feature Profile > **Teleworker** > **Wifi** (Minimum supported release: Cisco vManage Release 20.9.1)	View the Wi-Fi settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure the Wi-Fi settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.

Configure Users

Add user

Use these steps to add users.

Procedure

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

Step 2 Click **Users**.

Step 3 Click **Add User**.

Step 4 Configure these fields:

Field	Description
Full Name	Enter the full name of the user.
User Name	Enter the user name.
Password	Enter a password.
Remote User	Enable the **Remote User** option for remote users. If you enable this option, enter an email for the user.
Roles	Choose roles for the user.
Scope	Choose the scope for the user.
Select Locale	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Choose a locale to set the language for SD-WAN Manager user interface.

Note
In Cisco Catalyst SD-WAN Manager Release 20.12.1 and earlier releases, SD-WAN Manager only supported the English language on the user interface. From Cisco Catalyst SD-WAN Manager Release 20.13.1, SD-WAN Manager user interface supports Canadian French.

Note
From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later releases, SD-WAN Manager user interface supports Japanese.

Step 5 Click **Add** to add the user.

What to do next

When creating a new user, you have an option for creating a remote user. You can create from SD-WAN Manager or using an API for external integrations like Security Cloud Control. You can also edit the remote user using SD-WAN Manager like any other user. However, if the user is created programmatically through API for external integrations, the user will have an impact when they login next time.

Edit user

To edit user details after adding users, use these steps.

Procedure

Step 1 In the **Users** page, for the user you wish to edit, click **...**, and click **Edit**.

The **Edit User** page is displayed.

Step 2 Enter **Full Name**, **Username**.

Step 3 Choose the role from the **Roles** drop-down list.

Step 4 Choose the scope from the **Scope** drop-down list.

Step 5 Choose the locale from the **Select Locale** drop-down list.

From Cisco Catalyst SD-WAN Manager Release 20.13.1 this option is available.

Step 6 Click **Update**.

Copy user

Create a copy of the user details with these steps:

Procedure

Step 1 To create a copy of the user, click **...**, and click **Copy**.

The **Copy User** page is displayed.

Step 2 Enter **Full Name**, **Username**.

Step 3 If the user is a remote user, then:

a) Enable the **Remote User** option.

b) Enter the email in the **Email** and **Confirm Email** field.

Step 4 If the user is not a remote user, then:

a) Enter the password in the **Password** and **Confirm Password**fields.

Step 5 Choose the role from the **Roles** drop-down list.

Step 6 Choose the scope from the **Scope** drop-down list.

Step 7 Choose the locale from the **Select Locale** drop-down list.

From Cisco Catalyst SD-WAN Manager Release 20.13.1 **Select Locale** option is available.

Step 8 Click **Copy**.

Delete user

If a user no longer needs access to devices, you can delete the user. Deleting a user does not log out the user if the user is logged in.

Procedure

Step 1 For the user you wish to delete, click **...**, and click **Delete**.

Step 2 To confirm the deletion of the user, click **OK**.

Change user password

Change user password with these steps.

Procedure

Step 1 To change the password for a user, click **...** and click **Change Password**.
Step 2 Enter the current user password in **Current logged in User Password** field.
Step 3 Enter the new password in the **New Password for User** field.
Step 4 Enter the new password again in the **Confirm New Password for User** field.
Step 5 Click **Update**.

Reset locked user

Procedure

Step 1 To reset the lock for a user, click **...** and click **Reset Locked User**.
Step 2 In the **Reset Locked User** pop-up menu, click **Yes**.

Apply administrative lock

Procedure

Step 1 To apply administrative lock for a user, click **...** and click **Administrative Lock**.
Step 2 In the **Lock User** pop-up menu, click **Yes**.

View users logged in to a device using SSH sessions

You can monitor users logged in to a device using SSH sessions using these steps.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

For Cisco vManage Release 20.6.x and earlier, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 Select the device you want to use under the **Hostname** column.

Step 3 Click **Real Time**.

Step 4 From **Device Options**, choose **AAA users** for Cisco IOS XE Catalyst SD-WAN devices.

You will see a list of users logged in to the device.

View users with active HTTP sessions

Procedure

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

Step 2 Click **User Sessions**.

A list of all the active HTTP sessions within Cisco SD-WAN Manager is displayed, including, username, domain, source IP address, and so on.

Configure user sessions

User Sessions page shows a list of all the active HTTP sessions within SD-WAN Manager, including username, domain, source IP address, and so on.

To remove a user session, choose the session from the list, and click **Remove Session**.

Configure VPN segments

Procedure

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

A web page displays the list of configured segments.

Step 2 To edit or delete an existing segment, click **…**, and click **Edit** or **Delete**.

Step 3 To add new segment, click **Add Segment**.

Step 4 Enter the name of the segment in the **Segment Name** field.

Step 5 Enter the number of VPNs you want to configure in **VPN Number** field.

Step 6 To add a new segment, click **Add**.

Configure VPN groups

Procedure

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

A web page displays the list of groups that are configured.

Step 2 To edit or delete a VPN group, click **…**, and click **Edit** or **Delete**.

Step 3 To view the existing VPN in the dashboard, click **…**, and click **View Dashboard**.

The **VPN Dashboard** displays the device details of the VPN device configured.

Step 4 To add a new VPN group, click **Add VPN Group** and enter these details:

a) Provide a VPN group name in the **VPN Group Name** field.
b) Enter a brief description of the VPN in the **Description** field.
c) Check **Enable User Group access** check box and enter the user group name.
d) From **Assign Segment**, click **Add Segment** drop-down list to add a new or existing segment to the VPN group.
e) Enter the **Segment Name** and **VPN Number** in the respective fields.

Step 5 Click **Save**.

Verify granular RBAC permissions

Use this procedure to verify the permissions that you have configured for a user group.

Before you begin

This verification method is supported for Cisco vManage Release 20.7.1 and later.

Procedure

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

Step 2 Click **User Groups**.

Step 3 In the pane that displays the user groups, select a user group to display the read and write permissions assigned to the user group.

Step 4 Scroll to the permissions that control template access to verify your configuration for the user group.

Monitor devices for VPN groups

To monitor devices for VPN groups, use these instructions.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 Click **WAN - Edge**.

Step 3 Select the **VPN Group** and **VPN Segment** for which you want to monitor the network.

A web page displays the list of VPN groups and segments that are configured to a device.