

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	You can 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	You can 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	You can set client session timeouts, session lifetimes, server session timeouts, and enable the maximum number of user sessions in Cisco SD-WAN Manager.

- Users and access, on page 1
- Account lockout, on page 8
- User sessions, on page 11
- Ciscotac user access, on page 14

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.

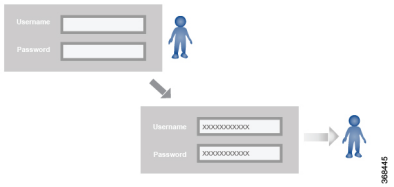
Users and user groups

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.

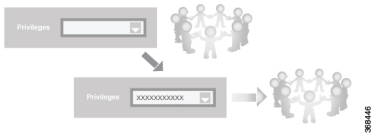
Users and user groups

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.



Note Previously, users with roles other than netadmin, such as basic, network_operations, security_operations, and operator, could execute arbitrary commands on the host system, which posed a significant security risk. To resolve this issue, only specific users (root, vmanage-admin, ciscotacro, ciscotacrw) were given permission to execute the commands. Now, only ciscotacro and ciscotacrw users have access to the **request execute** function, while netadmin group members are permitted access only when Cisco SD-WAN Manager is enabled. This change blocks unauthorized users from alternative shell or command execution methods, enforces proper restrictions, and mitigates the security risk.

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 for Cisco IOS XE Catalyst SD-WAN devices
User group permissions related to Cisco Catalyst Wireless Gateway device configuration.	User group permissions for 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
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 8.

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

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

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.