Configuring User Access and Authentication

This article describes how to use AAA in combination with RADIUS and TACACS+ to configure authentication, authorization, and accounting for users wishing to access Cisco vEdge devices.

Configuring AAA

AAA allows you to configure local users on the Cisco vEdge device. AAA configuration is done in two steps:

- Configure users—First, you configure usernames and passwords for individuals who are allowed to access the Cisco vEdge device. The Cisco SD-WAN software provides one standard username, **admin**, and you can also create custom usernames, as needed.
- Configure groups—Second, you place users in groups, which define the specific configuration and operational commands that the users are authorized to view and modify. A single user can be in one or more groups. See Role-Based Access for AAA for more information about user and group privileges and the authorization that they provide.

Creating Users

The Cisco SD-WAN software provides one standard username, **admin**. Only a user who is logged is as the admin user is permitted to create additional users.

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

```
Viptela(config)# system aaaVipteal(config)# user
username
password
passwordViptela(config-aaa)# group
group-name
```

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

password is the password for the user. Each username must have a password, and each user is allowed to change their own password. The CLI immediately encrypts the string and never displays a readable version of the password. When a user is logging in to the Cisco vEdge device, they have five chances to enter the correct password. After the fifth incorrect attempt, the user is locked out of the device, and they must wait 15 minutes before attempting to log in again.

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

The factory-default password for the **admin** username is **admin**. It is strongly recommended that you modify this password the first time you configure a Cisco vEdge device.

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

Configure the password as an ASCII string. The CLI immediately encrypts the string and never displays a readable version of the password. For example:

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

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

```
Viptela(config)# system aaa radius-servers
tag
```

tag is a string that you defined with the **radius server tag** command, as described below.

Creating Groups

The Cisco SD-WAN software provides three fixed group names: **basic**, **netadmin**, and **operator**. The username **admin** is automatically placed in the **netadmin** usergroup.

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

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

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

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

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

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

```
vEdge# show running-config system aaa
system
 aaa
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password $1$tokPB7tf$vchR2JI9Sw1/dqgkqup9S.
  !
 !
!
```

Configuring RADIUS Authentication

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

```
Viptela(config)#  system radiusViptela(config-radius)# server
ip-addressViptela(config-server)# secret-key
passwordViptela(config-server)# priority
numberViptela(config-server)# auth-port
port-numberViptela(config-server#) acct-port
port-numberViptela(config-server)# source-interface
interface-nameViptela(config-server)# tag
tagViptela(config-server)# vpn
vpn-id
```

For each RADIUS server, you must configure, at a minimum, its IP address and a password, or key. You can specify the key as a clear text string up to 32 characters long or as an AES 128-bit encrypted key. The local device passes the key to the RADIUS server. The password must match the one used on the server. To configure more than one RADIUS server, include the **server** and **secret-key** commands for each server.

The remaining RADIUS configuration parameters are optional.

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

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

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

You can tag RADIUS servers so that a specific server or servers can be used for AAA, IEEE 802.1X, and IEEE 802.11i authentication and accounting. Define the tag here, with a string from 4 to 16 characters long.

Then associate the tag with the **radius-servers** command when you configure AAA, and when you configure interfaces for 802.1X and 802.11i.

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

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

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

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

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

Configuring TACACS+ Authentication

To have a Cisco vEdge device use TACACS+ servers for user authentication, configure one or up to 8 servers:

```
Viptela(config)#  system tacacs Viptela(config)# server
ip-addressViptela(config-server)# secret-key
passwordViptela(config-server)# priority
numberViptela(config-server)# auth-port
port-numberViptela(config-server)# source-interface
interface-nameViptela(config-server)# vpn
vpn-id
```

For each TACACS+ server, you must configure, at a minimum, its IP address and and a password, or key. You can specify the key as a clear-text string up to 32 characters long or as an AES 128-bit encrypted key. The local device passes the key to the TACACS+ server. The password must match the one used on the server. To configure more than one TACACS+ server, include the **server** and **secret-key** commands for each server.

The remaining TACACS+ configuration parameters are optional.

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

By default, the Cisco vEdge device uses port 49 to connect to the TACACS+ server. To change this, use the **auth-port** command.

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

If the TACACS+ server is located in a different VPN from the Cisco vEdge device, configure the server's VPN number so that the Cisco vEdge device can locate it. If you configure multiple TACACS+ servers, they must all be in the same VPN.

By default, PAP is used as the authentication type for the password for all TACACS+ servers. You can change the authentication type to ASCII:

```
Viptela(config-tacacs)# authentication ascii
```

When waiting for a reply from the TACACS+ server, a Cisco vEdge device waits 5 seconds before retransmitting its request. To change this time interval, use the **timeout** command, setting a value from 1 to 1000 seconds:

```
Viptela(config-tacacs)# timeout
seconds
```

Configuring the Authentication Order

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

- The authentication process first checks whether a username and matching password are present in the running configuration on the local device.
- If local authentication fails, and if you have not configured authentication fallback (with the **auth-fallback** command), the authentication process stops. However, if you have configured authentication fallback, the authentication process next checks the RADIUS server. For this method to work, you must configure one or more RADIUS servers with the **system radius server** command. If a RADIUS server is reachable, the user is authenticated or denied access based on that server's RADIUS database. If a RADIUS server is unreachable and if you have configured multiple RADIUS servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's RADIUS database.
- If the RADIUS server is unreachable (or all the servers are unreachable), the authentication process checks the TACACS+ server. For this method to work, you must configure one or more TACACS+ servers with the **system tacacs server** command. If a TACACS+ server is reachable, the user is authenticated or denied access based on that server's TACACS+ database. If a TACACS+ server is unreachable and if you have configured multiple TACACS+ servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's TACACS+ database.
- If the TACACS+ server is unreachable (or all TACACS+ servers are unreachable), user access to the local Cisco vEdge device is denied.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configuring NAS Attributes

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

The VSA file must be named dictionary.Cisco SD-WAN, and it must contain text in the following format:

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

```
#
#
# Version:      $Id$
#

VENDOR          Viptela                         41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name              1    string
```

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

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

To create new user groups, use this command:

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

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

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

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

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

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

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

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


- Manage Users using vManage, on page 8
- Configure User Using CLI, on page 10
- Manage a User Group, on page 11
- Creating Groups Using CLI, on page 12

Manage Users using vManage

Use the Manage Users screen to add, edit, or delete users and user groups from the vManage NMS.

Only a user logged in as the **admin** user or a user who has Manage Users write permission can add, edit, or delete users and user groups from the vManage NMS.

Add a User

To perform operations on a device, you configure usernames and passwords for users who are allowed to access the device. The Cisco SD-WAN software provides one standard username, **admin**, and you can create custom usernames, as needed. We recommend that you configure strong passwords for users.

To add a user:

1. In the Users tab, click Add User.
2. In the Add User popup window, enter the full name, username, and password for the user. Note that uppercase characters are not allowed in usernames.
3. From the User Groups drop-down list, select the groups that the user will be a member of.
4. Click Add. The user is then listed in the user table.

Delete a User

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

To delete a user:

1. In the Users tab, select the user you wish to delete.
2. Click the More Actions icon to the right of the column and click Delete.
3. Click OK to confirm deletion of the user.

Edit User Details

Editing user details lets you update login information for a user, and add or remove a user from a user group. If you edit details for a user who is logged in, the changes take effect after the user logs out.

To edit user details:

1. In the Users tab, select the user whose details you wish to edit.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit login details, and add or remove the user from user groups.
4. Click Update.

Change User Password

You can update passwords for users as needed. We recommend that you use strong passwords.

To change a password for a user:

1. In the Users tab, select the user whose password you wish to change.
2. Click the More Actions icon to the right of the column and click Change Password.
3. Enter, and then confirm, the new password. Note that the user, if logged in, is logged out.
4. Click Done.

Configure User Using CLI

You can use the CLI to configure user credentials on each edge device. In this way, you can create additional users to give them access specific devices. The credentials that you create for a user by using the CLI can be different than the vManage credentials for the user, and you can create different credentials for a user on each device. Any Cisco IOS XE SD-WAN device user with the netadmin privilege can create a new user.

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

```
Device(config)# aaa authentication login user1 group basic
Device(config)# aaa authentication login user2 group operator
Device(config)# aaa authentication login user3 group netadmin
```

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

password is the password for the user. Each username must have a password, and each user is allowed to change their own password. The CLI immediately encrypts the string and never displays a readable version of the password. When a user is logging in to the Cisco IOS XE 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 they must wait 15 minutes before attempting to log in again.

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

The factory-default password for the **admin** username is **admin**. It is strongly recommended that you modify this password the first time you configure a Cisco IOS XE SD-WAN device.

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

Configure the password as an ASCII string. The CLI immediately encrypts the string and never displays a readable version of the password. For example:

```
Device(config)# show run
...
aaa authentication login default local
aaa authentication login user1 group basic
aaa authentication login user2 group operator
aaa authentication login user3 group netadmin
aaa authorization exec default local
```

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

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

tag is a string that you defined with the **radius server tag** command, as described below.

Manage a User Group

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

- basic—Includes users who have permission to view interface and system information.
- netadmin—Includes the admin user, by default, who can perform all operations on the vManage NMS. You can add other users to this group.
- operator—Includes users who have permission only to view information.

To add a user group:

1. In the User Groups tab, click Add User Group.
2. In the Add User Group popup window, enter the user group name and select the desired read and write permissions for each feature. Note that uppercase characters are not allowed in user group names.
3. Click OK. The user group is then listed in the left pane.

Each user group can have read or write permission for the features listed below. Write permission includes read permission.

Note: All user groups, regardless of the read or write permissions selected, can view the information displayed in the vManage Dashboard screen.

Delete a User Group

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

1. In the User Groups tab, click the name of the user group you wish to delete. Note that you cannot delete any of the three standard user groups—basic, netadmin, and operator.
2. Click the Trash icon.
3. Click OK to confirm deletion of the user group.

Edit User Group Privileges

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

1. In the User Groups tab, select the name of the user group whose privileges you wish to edit. Note that you cannot edit privileges for the three standard user groups—basic, netadmin, and operator.
2. Click the Edit button located directly above the privilege level table, and edit privileges as needed.
3. Click Save.

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

Creating Groups Using CLI

The Cisco SD-WAN software provides three fixed group names: **basic**, **netadmin**, and **operator**. The username **admin** is automatically placed in the **netadmin** usergroup.

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

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

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

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

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

Configuring RADIUS Authentication Using CLI

The Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco devices and send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

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

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

For each RADIUS server, you must configure, at a minimum, its IP address and a password, or key. You can specify the key as a clear text string up to 32 characters long or as an AES 128-bit encrypted key. The local device passes the key to the RADIUS server. The password must match the one used on the server. To configure more than one RADIUS server, include the **server** and **secret-key** commands for each server.

The remaining RADIUS configuration parameters are optional.

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

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

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

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

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

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

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

Configure SSH Authentication

Table 1: Feature History

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

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

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

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

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

Restrictions for SSH Authentication on Cisco SD-WAN

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

SSH Authentication using vManage on Cisco IOS XE SD-WAN Devices

1. In vManage NMS, select the **Configuration ► Templates** screen.
2. In the **Feature** tab, click **Create Template**.
3. From the **Device Model** check box, select the type of device for which you are creating the template.
4. From the **Basic Information** tab, choose **AAA-CISCO** template.
5. From the Local tab, New User section, enter the SSH RSA Key. You must enter the complete public key from the id_rsa.pub file in the SSH RSA Key text box.

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

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

Traditional IOS CLI, allow support for:

• Key-string

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

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

Public Keys supported on Cisco IOS XE SD-WAN Devices

- SSH-RSA

Configure the Authentication Order

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

- The authentication process first checks whether a username and matching password are present in the running configuration on the local device.
- If local authentication fails, and if you have not configured authentication fallback (with the **auth-fallback** command), the authentication process stops. However, if you have configured authentication fallback, the authentication process next checks the RADIUS server. For this method to work, you must configure one or more RADIUS servers with the **system radius server** command. If a RADIUS server is reachable, the user is authenticated or denied access based on that server's RADIUS database. If a RADIUS server is unreachable and if you have configured multiple RADIUS servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's RADIUS database.
- If the RADIUS server is unreachable (or all the servers are unreachable), the authentication process checks the TACACS+ server. For this method to work, you must configure one or more TACACS+ servers with the **system tacacs server** command. If a TACACS+ server is reachable, the user is

authenticated or denied access based on that server's TACACS+ database. If a TACACS+ server is unreachable and if you have configured multiple TACACS+ servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's TACACS+ database.

- If the TACACS+ server is unreachable (or all TACACS+ servers are unreachable), user access to the local Cisco IOS XE SD-WAN device device is denied.

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**.

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

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

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

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

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

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

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

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

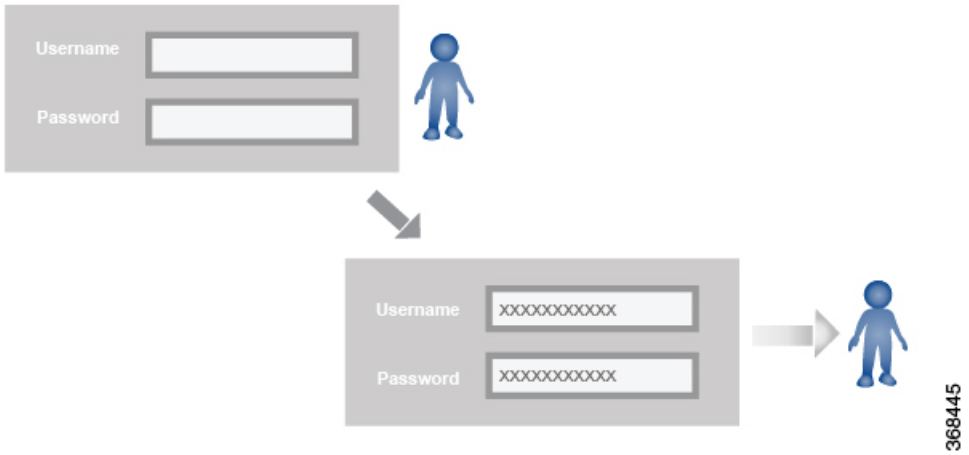
Role-Based Access with AAA

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

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

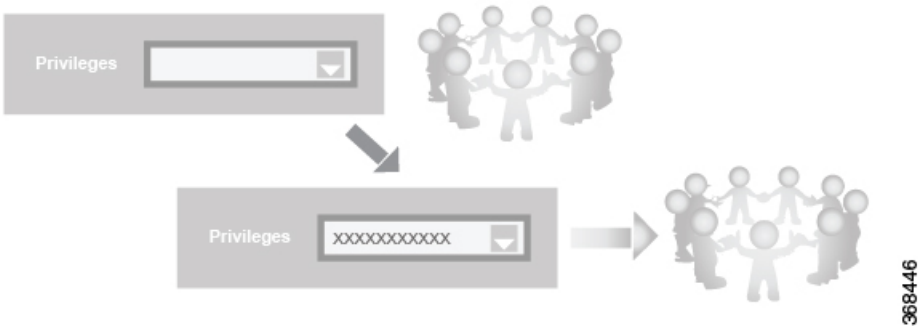
Users and User Groups

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

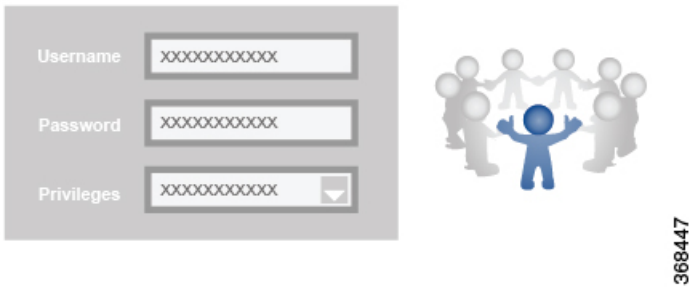


The Cisco SD-WAN software provides one standard username, **admin**, which is a user who has full administrative privileges, similar to a UNIX superuser. By default, the **admin** username password is **admin**. You cannot delete or modify this username, but you can and should change the default password.

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



The Cisco SD-WAN software provides three standard user groups. The two groups **basic** and **operator** are configurable. While you can use these two groups for any users and privilege levels, the **basic** group is designed to include users who have permission to both view and modify information on the device, while the **operator** group is designed to include users who have permission only to view information. The third group is **net admin**, which is non-configurable. By default, it 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.

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

Privileges for Role-Based Access

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

- Interface—Privileges for controlling the interfaces on the Cisco IOS XE SD-WAN device.
- Policy—Privileges for controlling control plane policy, OMP, and data plane policy.
- Routing—Privileges for controlling the routing protocols, including BFD, BGP, OMP, and OSPF.

- Security—Privileges for controlling the security of the device, including installing software and certificates. Only users belonging to the **netadmin** group can install software on the system.
- System—General systemwide privileges.

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

User Authorization Rules for Operational Commands

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

Note that any user can issue the **config** command to enter configuration mode, and once in configuration mode, they are allowed to issue any general configuration command. Also, any user is allowed to configure their password by issuing the **system aaa user** *self* **password** *password* command and then committing that configuration change. For the actual commands that configure device operation, authorization is defined according to user group membership. See User Group Authorization Rules for Configuration Commands.

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

CLI Command	Any User	Admin User
clear history	X	X
commit confirm	X	X
complete-on-space	X	X
config	X	X
exit	X	X
file	X	X
help	X	X
[no] history	X	X
idle-timeout	X	X
job	X	X
logout	—	X (users in netadmin group only)
monitor	X	X
nslookup	X	X
paginate	X	X
ping	X	X

CLI Command	Any User	Admin User
poweroff	—	X(users in netadmin group only)
prompt1	X	X
prompt2	X	X
quit	X	X
reboot	—	X (users in netadmin group only)
request aaa request admin-tech request firmware request interface-reset request nms request reset request software	—	X (users in netadmin group only)
request execute request download request upload	X	X
request (everything else)	—	X
rollback (configuration mode command)	—	X (users in netadmin group only)
screen-length	X	X
screen-width	X	X
show cli	X	X
show configuration commit list	X	X
show history	X	X
show jobs	X	X
show parser dump	X	X
show running-config	X	X
show users	X	X
system aaa user *self* password *password* (configuration mode command) (Note: A user cannot delete themselves)		
tcpdump	X	X
timestamp	X	X
tools ip-route	X	X
tools netstat	X	X

CLI Command	Any User	Admin User
tools nping	X	X
traceroute	X	X
vshell	X	X (users in netadmin group only)

User Group Authorization Rules for Operational Commands

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

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

Operational Command	Interface	Policy	Routing	Security	System
clear pppoe	X				
clear system					X
clear tunnel				X	
clear wlan	X				
clear ztp				X	X
clock					X
debug bgp			X		
debug cellular	X				
debug cflowd		X			
debug chmgr					X
debug config-mgr					X
debug dhcp-client					X
debug dhcp-helper					X
debug dhcp-server					X
debug fpm		X			
debug ftm					X
debug igmp			X		
debug netconf					X
debug omp			X		
debug ospf			X		
debug pim			X		
debug resolver			X		
debug snmp					X
debug sysmgr					X
debug transport					X
debug ttm					X
debug vdaemon				X	X
debug vrrp				X	

Operational Command	Interface	Policy	Routing	Security	System
debug wlan	X				
request certificate				X	
request control-tunnel				X	
request controller				X	
request controller-upload				X	
request csr				X	
request device				X	
request device-upload				X	
request on-vbond-controller				X	
request port-hop				X	
request root-cert-chain				X	
request security				X	
request vedge				X	
request vedge-upload				X	
request vsmart-upload				X	
show aaa					X
show app		X			
show app-route		X			
show arp	X				
show bfd			X		X
show bgp			X		
show boot-partition					X
show bridge	X				
show cellular	X				
show certificate				X	
show clock					X
show control				X	X

Operational Command	Interface	Policy	Routing	Security	System
show crash					X
show debugs—same as debug commands					
show dhcp					X
show external-nat				X	X
show hardware					X
show igmp			X		
show interface	X				
show ip			X		X
show ipsec				X	
show licenses					X
show logging					X
show multicast			X		
show nms-server					X
show notification					X
show ntp					X
show omp		X	X		X
show orchestrator				X	
show ospf			X		
show pim			X		
show policer		X			
show policy		X			
show ppp	X				
show pppoe	X				
show reboot					X
show security-info				X	
show software					X
show system					X

Operational Command	Interface	Policy	Routing	Security	System
show transport					X
show tunnel				X	
show uptime					X
show users					X
show version					X
show vrrp	X				
show wlan	X				
show ztp				X	

User Group Authorization Rules for Configuration Commands

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

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

Configuring AAA using vManage Template

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

Use the AAA template for Cisco vBond Orchestrators, vManage NMSs, Cisco vSmart Controllers, and Cisco IOS XE SD-WAN devices.

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

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

Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the **Configuration ► Templates** screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the **Device Model** drop-down, select the type of device for which you are creating the template.
5. Select the **Basic Information** tab.
6. To create a custom template for AAA, select the Factory_Default_AAA_Template and click Create Template. The AAA template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining AAA parameters.
7. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

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

Table 2:

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 SD-WAN device to a device template . When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Cisco IOS XE 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 Authentication Order and Fallback

You can configure the authentication order and authentication fallback for device. The authentication order specifies the order in which the system attempts to authenticate user, and provides a way to proceed with authentication if the current authentication method is unavailable. Fallback provides a mechanism for authentication is the user cannot be authenticated or if a RADUS or TACACS+ server is unreachable

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

Table 3:

Parameter Name	Description
Authentication Order	The default order is local, then radius, and then tacacs. To change the default order of authentication methods that the software tries when verifying user access to a Cisco IOS XE SD-WAN device: **1.** Click the dropdown arrow to display the list of authentication methods. **2.** In the list, click the up arrows to change the order of the authentication methods and click the boxes to select or deselect a method. If you select only one authentication method, it must be **local**.

Parameter Name	Description
Authentication Fallback	Click On to configure authentication to fall back from RADIUS or TACACS+ to the next priority authentication method if the user cannot be authenticated or if the RADIUS or TACACS+ servers are unreachable. With the default configuration (Off), authentication falls back only if the RADIUS or TACACS+ servers are unreachable.
Admin Authentication Order	Have the "admin" user use the authentication order configured in the Authentication Order parameter. If you do not configure the admin authentication order, the "admin" user is always authenticated locally.
Disable Netconf Logs	Click On to disable the logging of Netconf events. By default, these events are logged to the auth.info and messages log files.
Disable Audit Logs	Click On to disable the logging of AAA events. By default, these events are logged to the auth.info and messages log files.
RADIUS Server List	List the tags for one or two RADIUS servers. Separate the tags with commas. You set the tag under the RADIUS tab.

CLI equivalent:

Configure Local Access for Users and User Groups

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

To configure local access for individual users, select the Local tab. To add a new user, select the User tab, click Add New User, and configure the following parameters:

Table 4:

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

Parameter Name	Description
User Groups	Select from the list of configured groups. You must assign the user to at least one group. The admin user is automatically placed in the netadmin group and is the only member of this group.

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

To configure local access for user groups, you first place the user into either the basic or operator group. The admin is automatically placed in the netadmin group. Then you configure user groups. To make this configuration, select the Local tab, select the User Group tab, click Add New User Group, and configure the following parameters:

Table 5:

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

Click Add to add the new user group.

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

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

CLI equivalent:

Configure RADIUS Authentication

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

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

Table 6:

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

To configure a connection to a RADIUS server, select the RADIUS tab, click Add New Radius Server, and configure the following parameters:

Table 7:

Parameter Name	Description
Address	Enter the IP address of the RADIUS server host.
Tag	Enter a text string to identify the RADIUS server. The tag can be 4 to 16 characters long. The tag allows you to configure authentication for AAA, IEEE 802.1X, and IEEE 802.11i to use a specific RADIUS server or servers. For Cisco IOS XE SD-WAN devices running Cisco SD-WAN software, this field is ignored.
Authentication Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0.*Default:* Port 1812
Accounting Port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server.*Range:* 0 through 65535*Default:* 1813
Key (Deprecated)	This field is deprecated. Use the Secret Key field instead.
Secret Key	Enter the key the Cisco IOS XE SD-WAN device passes to the RADIUS server for authentication and encryption. You can type the key as a text string from 1 to 32 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.
Source Interface	Enter the name of the interface on the local device to use to reach the RADIUS server.
VPN ID	Enter the number of the VPN in which the RADIUS server is located or through which the server can be reached. If you configure multiple RADIUS servers, they must all be in the same VPN.
Priority	Enter the priority of a RADIUS server. A server with a lower number is given priority.*Range:* 0 through 7*Default:* 0

Click Add to add the new RADIUS server.

To add another RADIUS server, click Add New RADIUS Server again.

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

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.

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

Table 8:

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

To configure a connection to a TACACS+ server, select the TACACS tab, click Add New TACSCS Server, and configure the following parameters:

Table 9:

Parameter Name	Description
Address	Enter the IP address of the TACACS+ server host.
Authentication Port	Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0. *Default:* Port 49
Key (Deprecated)	This field is deprecated. Use the Secret Key field instead.
Secret Key	Enter the key the Cisco IOS XE SD-WAN device passes to the TACACS+ server for authentication and encryption. You can type the key as a text string from 1 to 32 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS+ server.
Source Interface	Enter the name of the interface on the local device to use to reach the TACACS+ server.
VPN ID	VPN in which the TACACS+ server is located or through which the server can be reached. If you configure multiple TACACS+ servers, they must all be in the same VPN.
Priority	Set the priority of a TACACS+ server. A server with lower priority number is given priority over one with a higher number.*Range:* 0 through 7*Default:* 0

Click Add to add the new TACACS server.

To add another TACACS server, click Add New TACACS Server again.

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

CLI equivalent: