Configure User Access and Authentication

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.

- Manage Users using vManage, on page 1
- Configure User Using CLI, on page 3
- Manage a User Group, on page 4
- Creating Groups Using CLI, on page 5
- Configuring RADIUS Authentication Using CLI, on page 5
- Configure SSH Authentication, on page 6
- Configure the Authentication Order, on page 7
- Role-Based Access with AAA, on page 9
- Configuring AAA using vManage Template, on page 11
- Configuring IEEE 802.1X and IEEE 802.11i Authentication, on page 17
- Configure IEEE 802.1X Authentication for WANs, on page 19

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 to 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$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAldMOFQfD.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 example, 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:

```
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
```

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**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Shell Authentication Using RSA Keys</td>
<td>Cisco IOS XE SD-WAN Release 16.12.1b</td>
<td>This feature helps configure RSA keys by securing communication between a client and a Cisco SD-WAN server.</td>
</tr>
</tbody>
</table>

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 1024 and 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 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 directory 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.

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.

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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
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 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>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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, gnat, 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.</td>
</tr>
<tr>
<td>Password</td>
<td>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, <em>The YANG 1.1 Data Modeling Language</em>. 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.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the user.</td>
</tr>
</tbody>
</table>
### Table 5:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Groups</td>
<td>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.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Feature</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retransmit Count</td>
<td>Specify how many times to search through the list of RADIUS servers while attempting to locate a server.</td>
</tr>
</tbody>
</table>
|                       | *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:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Enter the IP address of the RADIUS server host.</td>
</tr>
<tr>
<td>Tag</td>
<td>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.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>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. <em>Default</em>: Port 1812</td>
</tr>
</tbody>
</table>
| 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
Device(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:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 TACACS Server, and configure the following parameters:

**Table 9:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Enter the IP address of the TACACS+ server host.</td>
</tr>
</tbody>
</table>
| 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:**

---

## Configuring IEEE 802.1X and IEEE 802.11i Authentication

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

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

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

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

### Configure RADIUS Authentication Servers

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

```
Device(config)# radius server 10.99.144.201
Device(config-radius-server)#
```

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

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

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

### Enable RADIUS Accounting

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

### Configure Authentication with Wake on LAN

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

When a client that uses wake on LAN and that attaches through an 802.1X port powers off, the 802.1X port becomes unauthorized. The port can only receive and send EAPOL packets, and wake-on-LAN magic packets cannot reach the client. When the device is powered off, it is not authorized, and the switch port is not opened.
Without wake on LAN, when an 802.1X port is unauthorized, the router's 802.1X interface block traffic other than EAPOL packets coming from unauthorized clients.

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

**Configure 802.1X Host Mode**

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

- **Single-host mode**—The 802.1X interface grants access only to the first authenticated client. All other clients attempting access are denied and dropped.

- **Multiple-host mode**—A single 802.1X interface grants access to multiple clients. In this mode, only one of the attached clients must be authorized for the interface to grant access to all clients. If the interface becomes unauthorized, the Cisco IOS XE SD-WAN device denies network access to all the attached clients.

- **Multiple-authentication mode**—A single 802.1X interface grants access to multiple authenticated clients on data VLANs.

**Set the Timeout for Inactive Clients**

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

```
Device(config-if)# dot1x timeout auth-period 1
```

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

**Enable Periodic Client Reauthentication**

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

```
Device(config-if)#dot1x reauthentication
```

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

**Configure Dynamic Authorization Service for RADIUS Change of Authorization**

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

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

To enable DAS for an 802.1X interface, you configure information about the RADIUS server from which the interface can accept CoA requests. In the context of configuring DAS, the Cisco IOS XE SD-WAN device is the server and the RADIUS server (or other authentication server) is the client.
The port number can be a value from 1 through 65535. If you configure DAS on multiple 802.1X interfaces on a Cisco IOS XE SD-WAN device, you must configure each interface to use a different UDP port.

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

**Enabling IEEE 802.1X and AAA on a Port**

To enable IEEE 802.1X and AAA on a port, use the following commands:

```
Device> enable
Device# config-transaction
Device(config)# dot1x system-auth-control
Device(config)# aaa authentication dot1x default group radius
Device(config)# interface GigabitEthernet0/0/0
Device(config)# authentication port-control auto
Device(config)# dot1x pae authenticator
Device(config)# end
```

**Enabling IEEE 802.1X RADIUS Accounting**

To enable IEEE 802.1X RADIUS accounting, use the following commands:

```
Device(config)# radius-server host 172.20.39.46 auth-port 1812 acct-port 1813 key rad123
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# aaa accounting system default start-stop group radius
Device(config)# end
```

**Enable MAC Authentication Bypass**

```
Device(config)# int GigabitEthernet0/0/0
Device(config)# dot1x mac-auth-bypass
```

---

**Configure IEEE 802.1X Authentication for WANs**

**Table 10: Feature History**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Support for SD-WAN</td>
<td>Cisco IOS XE Release Amsterdam 17.2.1r</td>
<td>This feature lets you enable the 802.1X authentication on Cisco IOS XE SD-WAN devices. Starting from Cisco IOS XE Release Amsterdam 17.2.1r, 802.1X is supported based on Identity-Based Networking Services (IBNS) 1.0 IOS-XE CLIs. This feature is supported on Cisco IOS XE SD-WAN devices only.</td>
</tr>
</tbody>
</table>

This feature lets you enable 802.1X authentication on Cisco IOS XE SD-WAN devices. Starting from Cisco IOS XE Release Amsterdam 17.2.1r, 802.1X is supported based on Identity-Based Networking Services (IBNS) 1.0 IOS-XE CLIs. This feature is supported on Cisco IOS XE SD-WAN devices only.

**Prerequisites**

The following are required for Cisco vManage to push 802.1X related configurations:

- Enable authentication services for 802.1X by RADIUS authentication servers.
• Allow configuring 802.1X port security on switch-port interface.

• Allow configuring following VLANs for Authenticated and Unauthenticated clients:
  • Restricted VLAN (or authentication rejected VLAN)
  • Guest VLAN
  • Critical VLAN (or authentication failed VLAN)
  • Critical Voice VLAN

• Allow one of the following host-mode authentication:
  • Single-host mode
  • Multiple-host mode
  • Multiple-authentication mode
  • Multi-domain mode

• RADIUS Accounting Attributes.

Restrictions
• Multiple groups cannot be supported in AAA authentication 802.1X and AAA accounting 802.1X.

• Authentication order 802.1X MAB CLI cannot be disabled through Cisco vManage. This results in a 60 second delay in MAB authentication when MAB client is online.

• 802.1X Authentication event using VLAN ID has to be enabled in the Add-on template, if required.

Configure IEEE 802.1X Authentication for WANs using vManage

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

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

To configure IEEE 802.1X authentication for WANs on the interface, first create a feature template:

1. Navigate to Configuration > Templates
2. Select the Feature tab and click on Add Template.
3. Select your device from the list on the left panel.
4. Select the Cisco AAA template.
5. Enter the Template Name and Description.
6. Select the RADIUS tab and under RADIUS SERVER click on New RADIUS Server.
7. Configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Server</td>
<td>Enter the tag of the RADIUS server to use for 802.1X authentication. It can be from 4 through 16 characters long. Use the AAA feature template to configure.</td>
</tr>
</tbody>
</table>
Configure User Access and Authentication

Configure IEEE 802.1X Authentication for WANs using vManage

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Set IP Address of the RADIUS server.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Click Authentication, then click Add New Authentication Entry to configure RADIUS authentication attribute–value (AV) pairs to send to the RADIUS server during an 802.1X session. To save the entry, click Add.</td>
</tr>
<tr>
<td>Accounting Port</td>
<td>Click Accounting, then click Add New Accounting Entry to configure RADIUS accounting attribute–value (AV) pairs to send to the RADIUS server during an 802.1X session. To save the entry, click Add.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Configure how long to wait for replies from the RADIUS server.</td>
</tr>
<tr>
<td>Retransmit Count</td>
<td>Configure how many times this RADIUS server is contacted.</td>
</tr>
<tr>
<td>Key</td>
<td>Set the RADIUS server shared key.</td>
</tr>
<tr>
<td>RADIUS Group</td>
<td>Define the AAA server group with a group name.</td>
</tr>
<tr>
<td>VPN-ID</td>
<td>Set the VPN through which the RADIUS or other authentication server is reachable.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Set the interface that will be used to reach the RADIUS server.</td>
</tr>
</tbody>
</table>

8. Select RADIUS GROUP and click on New RADIUS Group to configure these parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Group</td>
<td>Define the AAA server group with a group name.</td>
</tr>
<tr>
<td>VPN-ID</td>
<td>Set the VPN through which the RADIUS or other authentication server is reachable.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Set the interface that will be used to reach the RADIUS server.</td>
</tr>
</tbody>
</table>

9. Select the 802.1X tab and set these parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>Configure this to enable IEEE 802.1X on the interface.</td>
</tr>
<tr>
<td>Authentication Parameters</td>
<td>Set the Authentication configurations parameters to &quot;On&quot;.</td>
</tr>
<tr>
<td>Accounting Parameters</td>
<td>Set the Accounting configurations parameters to &quot;On&quot;.</td>
</tr>
</tbody>
</table>

10. To save this feature template, click Save.

11. To create a Switch Port template, repeat steps 2 and 3.

12. Scroll down and select the Switch Port template.

13. Enter the Template Name and Description.
14. Select the Interface tab click on New Interface.

15. Configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>Set the interface name.</td>
</tr>
<tr>
<td>Speed</td>
<td>Set the interface speed.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Set the VLAN name.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Set the VLAN identifier associated with the bridging domain.</td>
</tr>
<tr>
<td>802.1X</td>
<td>Enable IEEE 802.1X authentication on this interface. Select “On”.</td>
</tr>
<tr>
<td>Interface PAE Type</td>
<td>Set the 802.1x Interface PAE type.</td>
</tr>
<tr>
<td>Control Direction</td>
<td>Set unidirectional or bidirectional authorization mode.</td>
</tr>
</tbody>
</table>
| Host Mode               | Select whether an 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. |
| Periodic Reauthentication | Enter how often to reauthenticate 802.1X clients. By default, no reauthentication attempts are made after the initial LAN access request. Range: 0 through 1440 minutes |

16. Click on Advanced Options and set the following:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Order</td>
<td>Set the order of authentication methods to use when authenticating devices for connection to the 802.1X WAN. The default authentication order is RADIUS, then MAC authentication bypass (MAB).</td>
</tr>
<tr>
<td>MAC Authentication Bypass</td>
<td>Select to enable MAC authentication bypass (MAB) on the RADIUS server and to authenticate non-802.1X–compliant clients using a RADIUS server.</td>
</tr>
<tr>
<td>Port Control Mode</td>
<td>Set the port control mode to enable 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.</td>
</tr>
<tr>
<td>Voice VLAN ID</td>
<td>Configure the Voice VLAN ID.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Critical VLAN</td>
<td>Set the critical VLAN (or authentication failed VLAN) for 802.1x-compliant clients. Configure network access when RADIUS authentication or the RADIUS server fails.</td>
</tr>
<tr>
<td>Critical Voice VLAN</td>
<td>Enable the critical voice VLAN.</td>
</tr>
<tr>
<td>Guest VLAN</td>
<td>Configure guest VLAN to drop non-802.1X enabled clients, if the client is not in the MAB list.</td>
</tr>
<tr>
<td>Restricted VLAN</td>
<td>Set the restricted VLAN (or authentication failed VLAN) for 802.1x-compliant clients. Configure limited services to 802.1X–compliant clients that failed RADIUS authentication.</td>
</tr>
</tbody>
</table>

17. Click on Add.

18. To save this feature template, click Save.

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

**Configure IEEE 802.1X Authentication for WANs using CLIs**

**Configuration**

For this feature, two sets of configurations are required-

1. **Configure the Global AAA commands:**
   a. Enable or disable 802.1X globally
      ```
      Device(config)# aaa authentication dot1x default group radius-0
      Device(config)# aaa authorization network default group radius-0
      Device(config)# dot1x system-auth-control
      Device(config)# radius-server dead-criteria time 10 tries 3
      Device(config)# radius-server deadtime 15
      ```
   b. Enable accounting
      ```
      Device(config)# aaa accounting dot1x default start-stop group radius-0
      ```

2. **Configure the Interface Level commands:**
   a. Enable or disable 802.1X on port-basis
      ```
      Device(config-if)# dot1x pae authenticator
      Device(config-if)# authentication port-control auto
      ```
   b. Enable or disable MAB on port-basis
      ```
      Device(config-if)# mab
      ```
   c. Select host-mode
      ```
      Device(config-if)# authentication host-mode <multi-auth | multi-domain | multi-host | single-host>
      ```
   d. Configure voice vlan
      ```
      Device(config-if)# switchport voice vlan <vlan-id>
      ```
Configure IEEE 802.1X Authentication for WANs using CLIs

- **e. Select 802.1X control direction**
  
  `Device(config-if)# authentication control-direction <both | in>`

- **f. Enable periodic re-authentication and corresponding re-authentication interval and inactivity timeout time**
  
  - `Device(config-if)# authentication periodic`
  - `Device(config-if)# authentication timer reauthenticate <internal-in-sec>`
  - `Device(config-if)# authentication timer inactivity <timeout-in-sec>`

- **g. Configurable authentication orders on per-port basis**
  
  `Device(config-if)# authentication order dot1x mab`

- **h. Specify the restricted VLAN**
  
  `Device(config-if)# authentication event fail action authorize vlan <vlan-id>`

- **i. Specify the guest VLAN**
  
  `Device(config-if)# authentication event no-response action authorize vlan <vlan-id>`

- **j. Specify the critical VLAN**
  
  `Device(config-if)# authentication event server dead action authorize vlan <vlan-id>`

- **k. Enable the critical voice VLAN feature**
  
  `Device(config-if)# authentication event server dead action authorize voice`