Authentication

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

Table 1: Feature History

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

Authentication

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

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

Authentication order

The authentication order is a configuration setting that

- dictates the order in which authentication methods are tried when verifying user access to a Cisco IOS XE Catalyst SD-WAN device through an SSH session or a console port, and
- provides a way to proceed with authentication if the current authentication method is unavailable.

Default authentication order

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

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

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

Modifying the default authentication order

You can use the **auth-order** command to modify the default authentication order. Specify one, two, or three authentication methods in the preferred order, starting with the one to be tried first. If you configure only one authentication method, it must be local.

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

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

Authentication fallback mechanism

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

If the authentication order is configured as

- radius local: With radius as the default authentication, local authentication is used only when all RADIUS servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for local authentication.
- local radius: With local as the default authentication, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device.
- radius tacacs local: With radius as the default authentication, TACACS+ is tried only when all RADIUS servers are unreachable, and local authentication is tried only when all TACACS+ servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for the TACACS+ server. Similarly, if a TACACS+ server denies access, the user cannot log via local authentication.

User group assignment after authentication

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

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

Configure authentication order

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

Configure the authentication order for devices using these steps.

Procedure

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

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

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

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

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

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

Note
Select at least one group from the list.

Duo Multi-factor authentication

Duo Multi-factor authentication

Duo multi-factor authentication is a security feature that

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

Configure Duo multifactor authentication

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

Before you begin

Create local users in your Duo account before proceeding.

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

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

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

Follow these steps to set up Duo authentication.

Procedure

Step 1 Log in to the Duo Admin Panel.

Step 2 Create an Auth API application.

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

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

Step 4 Click **DUO MFA Configuration**.

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

Step 5 Click **Enabled**.

Step 6 Configure the following options:

Field	Description
Integration Key	Enter the integration key (Ikey) for your Duo account.
Secret Key	Enter the secret key (Skey) for your Duo account.
API Hostname	Enter the API hostname (api-hostname) for your Duo account.
Server proxy	(Read only) Displays the server proxy used to access the Duo server if SD-WAN Manager is behind a firewall. Set this server proxy with the **system http proxy** or the **system https proxy** command. **Note** If SD-WAN Manager is deployed on a cloud that can be reached by an external network, a server proxy should not be set.

Step 7 Click **Save**.

Step 8 If a Cisco SD-WAN Validator or a Cisco SD-WAN Controller does not have internet access, enter the following commands in the CLI or the device template to provide access to the Duo MFA feature.

These commands configure the device with proxy information about the device on which Duo MFA is enabled.

```
vm# config
vm(config)# system aaa
vm(config-aaa)# multi-factor-auth
vm(config-multi-factor-auth)# duo
vm(config-duo)# api-hostname name
vm(config-duo)# secret-key key
vm(config-duo)# integration-key key
vm(config-duo)# proxy proxy_url
vm(config-duo)# commit
```

RADIUS authentication

Radius authentication

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

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

Configure RADIUS authentication using CLI commands

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

Procedure

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

Example:

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

Specify the key as a clear text string up to 31 characters, or provide it as an AES 128-bit encrypted key. The local device passes the key to the RADIUS server. The password must match the one used on the server.

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

Step 3 Optionally, configure these RADIUS parameters:

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

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

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

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

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

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

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

Note

Tags are used for grouping, describing, or finding devices. You can tag RADIUS and TACAC servers for authentication and accounting. You can add more than one tag to a device. Starting from Cisco vManage Release 20.9.1, following new tags are used in authentication:

- Viptela-User-Group: for user group definitions instead of Viptela-Group-Name.
- Viptela-Resource-Group: for resource group definitions.

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

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

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

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

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

SSH authentication

SSH authentication

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

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

Enabling SSH authentication

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

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

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

Restrictions for SSH authentication

SSH RSA key size

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

Supported methods for configuring SSH authentication using CLI commands

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

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

Traditional IOS CLI, allow support for:

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

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

Configure SSH Authentication using templates

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

Procedure

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

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

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

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

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

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

Step 6 Enter **SSH RSA Key**.

Note

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

IEEE 802.1X authentication

IEEE 802.1X authentication

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

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

IEEE 802.1X open authentication and host modes

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

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

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

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

Restrictions for configuring IEEE 802.1X authentication

Authentication, Authorization, and Accounting

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

Authentication order

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

Open authentication

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

Prerequisites for configuring IEEE 802.1X authentication

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

RADIUS

Enable RADIUS authentication servers to authenticate IEEE 802.1x services.

Configure RADIUS Accounting attributes.

Switch port

Enable IEEE 802.1X configuration on the switch port interface.

VLAN configurations

Enable these VLAN configurations to manage authenticated and unauthenticated clients:

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

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

Host-mode authentication

Enable one of these host-mode authentications:

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

Configure IEEE 802.1X Authentication using templates

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

Procedure

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

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

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

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

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

Step 5 Select the **RADIUS** tab.

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

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

b) Click **Add**.

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

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

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

b) Click **Add**.

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

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

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

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

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

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

What to do next

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

Create a Switch Port template using templates

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

Procedure

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

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

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

Step 3 Select your device from the list.

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

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

a) Configure these parameters:

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

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

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

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

c) Click **Add**.

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

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

IEEE 802.1X Open Authentication using CLI commands

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

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

Configure IEEE 802.1X Authentication using CLI commands

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

- Global AAA commands
- Interface level commands

Procedure

Step 1 Configure the Global AAA commands.

a) Enable or disable IEEE 802.1X globally:

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

b) Enable accounting:

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

Step 2 Configure the interface level commands.

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

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

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

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

c) Configure voice VLAN:

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

d) Select IEEE 802.1X control direction:

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

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

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

f) Configure authentication orders on per-port basis:

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

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

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

h) Specify the critical VLAN:

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

i) Enable the critical voice VLAN feature:

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

Configure Switch Port using a configuration group

Configure Switch Port settings using these steps.

Before you begin

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

Procedure

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

Step 2 Create and configure a Switch Port feature in a Service profile.

Table 2: Switch Port

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

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

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

What to do next

Also see Deploy a configuration group.

Authentication, Authorization, and Accounting

Restrictions to configure authorization and accounting

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

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

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

Configure AAA using a configuration group

Before you begin

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

Procedure

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

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

a) Configure users.

Table 3: Local

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

Field	Description
Password	Enter a password for the user. The password is an MD5 digest string, and it can contain any characters, including tabs, carriage returns, and linefeeds. For more information, see Section 9.4 in RFC 7950, The YANG 1.1 Data Modeling Language. Each username must have a password. Users are allowed to change their own passwords. The default password for the admin user is admin. We strongly recommended that you change this password.
Confirm Password	Re-enter the password for the user.
Privilege	Select between privilege level 1 or 15. • Level 1: User EXEC mode. Read-only, and access to limited commands, such as the ping command. • Level 15: Privileged EXEC mode. Full access to all commands, such as the reload command, and the ability to make configuration changes. By default, the EXEC commands at privilege level 15 are a superset of those available at privilege level 1.
Add Public Key Chain	
Key String*	Enter the authentication string for a key.
Key Type	Choose **ssh-rsa**.

b) Configure RADIUS servers.

Table 4: RADIUS

Field	Description
Address*	Enter the IP address of the RADIUS server host.
Acct Port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 1 - 65534. Default: 1813
Auth Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. Default: 1812 Range: 1 - 65534
Retransmit	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 3 Range: 0 - 100

Field	Description
Timeout	Enter the number of seconds a device waits for a reply to a RADIUS request before retransmitting the request. Default: 5 seconds Range: 1 through 1000
Key*	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption.
Key Type	Choose Protected Access Credential (PAC) key.

c) Configure TACACS servers.

Table 5: TACACS Server

Field	Description
Address*	Enter the IP address of the TACACS+ server host.
Port	Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0. Default: 49
Timeout	Enter the number of seconds a device waits for a reply to a TACACS+ request before retransmitting the request. Default: 5 seconds Range: 1 through 1000
Key*	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the TACACS+ server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS+ server.

d) Configure accounting rules.

Table 6: Accounting

Field	Description
Rule Id*	Enter the accounting rule ID.

Field	Description
Method*	Specifies the accounting method list. Choose one of the following: • **commands**: Provides accounting information about specific, individual EXEC commands associated with a specific privilege level. • **exec**: Provides accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times. • **network**: Runs accounting for all network-related service requests. • **system**: Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
Level	Choose the privilege level (1 or 15). Accounting records are generated only for commands entered by users with this privilege level.
Start Stop	Enable this option to if you want the system to send a start accounting notice at the beginning of an event and a stop record notice at the end of the event.
Use Server-group*	Choose a previously configured TACACS group. The parameters that this accounting rule defines are used by the TACACS servers that are associated with this group.

e) Configure authorization parameters.

Table 7: Authorization

Field	Description
Server Auth Order*	Choose the authentication order. It dictates the order in which authentication methods are tried when verifying user access to a Cisco IOS XE Catalyst SD-WAN device through an SSH session or a console port.
Authorization Console	Enable this option to perform authorization for console access commands.
Authorization Config Commands	Enable this option to perform authorization for configuration commands.
Add Authorization Rule	
Rule Id*	Enter the authorization rule ID.
Method*	Choose **Commands**, which causes commands that a user enters to be authorized.
Level	Choose the privilege level (1 or 15) for commands to be authorized. Authorization is provided for commands entered by users with this privilege level.
If Authenticated	Enable this option to apply the authorization rule parameters only to the authenticated users. If you do not enable this option, the rule is applied to all users.

Field	Description
Use Server-group*	Choose a previously configured TACACS group. The parameters that this authorization rule defines are used by the TACACS servers that are associated with this group.

f) Configure 802.1x parameters.

What to do next

Also see Deploy a configuration group.

Methods of configuring AAA using templates

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

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

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

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

Create a template

Procedure

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

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

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

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

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

Step 5 Select **Basic Information**.

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

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

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

The name can include up to 128 alphanumeric characters.

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

The description can include up to 2048 alphanumeric characters.

Step 9 When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the **Scope** drop-down list to the left of the parameter field and select one of these:

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

Configure local access for users and user groups

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

Procedure

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

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

Parameter Name	Description
Name	Enter a name for the user. The name must start with a letter and be between 1 and 128 characters. Use only lowercase letters, numbers 0 through 9, hyphens (-), underscores (_), or periods (.). The name should not contain any uppercase letters. These usernames are reserved, so you cannot configure them: backup, basic, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, quagga, root, sshd, sync, sys, uucp, and www-data. In addition to these, names starting with viptela-reserved are reserved. **Note** From Cisco Catalyst SD-WAN Manager Release 20.18.1, the character limit for local user accounts remains restricted to 32 characters. However, for TACACS users, usernames extend up to 128 characters.
Password	Enter a password for the user. Each username must have a password. Users are allowed to change their own passwords. The default password for the admin user is admin. We strongly recommended changing this password. **Note** When configuring local users using a Cisco SD-WAN Manager AAA template, SD-WAN Manager uses a Cisco type 9 password type that uses the scrypt algorithm for hashing the passwords of local users. If you configure local users using a device CLI template or a CLI add-on template, you can choose other Cisco password types for hashing of local user passwords. For more information, see Using Type 6 encryption in a CLI add-on template.
Privilege Level 1 OR 15	Select between privilege level 1 or 15. • **Level 1**: User EXEC mode. Read-only, and access to limited commands, such as the **ping** command. • **Level 15**: Privileged EXEC mode. Full access to all commands, such as the **reload** command, and the ability to make configuration changes. By default, the EXEC commands at privilege level 15 are a superset of those available at privilege level 1.
SSH RSA Key(s)	Click **+ Add** to add SSH RSA keys. Paste your SSH RSA key in the field. To remove a key, click **-**. Devices support a maximum of 2 SSH RSA keys.

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

To configure local access for user groups, first place the user into either the basic or operator group. The admin is automatically placed in the netadmin group. Then you configure user groups.

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

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

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

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

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

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

Configure RADIUS authentication

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

Procedure

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

Table 8:

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

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

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

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

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

CLI equivalent:

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

Configure TACACS+ authentication

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

Procedure

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

Step 2 Configure these parameters:

Parameter Name	Description
Address	Enter the IP address of the TACACS+ server host.
Port	Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0. Default: Port 49
Key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the TACACS+ server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS+ server.

Configure authentication order

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

Configure the authentication order for devices using these steps.

Procedure

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

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

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

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

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

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

   Note
   Select at least one group from the list.

Configure authorization

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

Before you begin

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

Procedure

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

Step 2 Configure the following parameters:

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

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

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

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

CLI commands for configuring authorization:

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

Configure accounting

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

Before you begin

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

Procedure

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

Step 2 Configure these parameters:

Table 9: Accounting

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

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

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

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

CLI commands for configuring authorization:

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

Posture assessment support

Posture assessment support

Cisco AnyConnect Posture Assessment is a posture assessment solution that

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

Network endpoint validation and posture assessment workflow

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

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

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

Restrictions for Posture Assessment

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

Configure posture assessment using CLI commands

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

Before you begin

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

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

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

Procedure

Step 1 Configure AAA.

Example:

```
aaa new-model
radius server ISE1

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

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

interface vlan 15
 ip address 198.51.100.1 198.51.100.254

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

ip radius source-interface vlan 15
```

Note

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

Step 2 Configure IEEE 802.1x authentication and authorization.

Example:

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

Note

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

Step 3 Configure posture assessment and redirect ACL.

Example:

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

Step 4 Configure device tracking.

Example:

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

Note
The IP address mentioned belongs to ISE.

Step 5 Configure CoA reauthentication and dACL on ISE.

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

   ACL name: TEST_IP_PERMIT_ALL

   ACEs: permit ip any any

b) Create an authorization result and choose the downloadable ACL as dACL.
c) Navigate to **Administration** > **System** > **Settings** > **Policy Settings**, and in **Policy Sets** configuration, select the authorization result as authorization policy.

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

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