Multiple Authentications for a Client

- Multiple authentications for a client, on page 1
- Configure multiple authentications for a client, on page 2
- Configuring 802.1x and CWA on controller (CLIs), on page 9
- Configuring ISE for Central Web Authentication with Dot1x (GUI), on page 16
- Verify multiple authentication configurations, on page 19

Multiple authentications for a client

Multiple authentications for a client is a network security feature that

- enables both Layer 2 (L2) and Layer 3 (L3) authentication for wireless client devices
- enhances security by requiring clients to complete multiple types of authentication before connecting, and
- applies only to regular client devices joining a wireless network.

Additional information

- You can enable both L2 and L3 authentication for a given SSID.
- Multiple authentications feature is not supported for guest or specialized client types.

Supported combination of authentications for a client

The Multiple Authentications for a Client feature supports multiple combination of authentications for a given client configured in the WLAN profile.

The Multiple Authentications for a Client feature supports multiple combinations of authentications for clients configured in the WLAN profile.

The table outlines the supported combinations of authentications for clients.

Layer 2	Layer 3	Supported
MAB	CWA	Yes
MAB Failure	LWA	Yes

802.1X	CWA	Yes
PSK	CWA	Yes
iPSK + MAB	CWA	Yes
iPSK	LWA	No
MAB Failure + PSK	LWA	No Yes
MAB Failure + PSK	CWA	No

Unsupported combinations

The table outlines the combination of authentications on MAC failure that are not supported on a given client:

Authentication Types	Foreign	Anchor	Supported
WPA3-OWE+LWA	Cisco AireOS	Cisco Catalyst 9800 Controller	No
WPA3-SAE+LWA	Cisco AireOS	Cisco Catalyst 9800 Controller	No

Jumbo frame support for RADIUS packets

RADIUS packets are fragmented according to the MTU of the egress interface when you meet all of these conditions.

- The command **ip radius source-interface** is configured under the relevant AAA group server radius group to point to the egress interface.
- The **ip mtu NNN** command is configured on the egress interface.

Note If you set the MTU of the source interface to less than 1500 bytes, additional fragmentation can occur. This may cause packet drops by upstream devices, such as firewalls and load balancers. Authentication failures may result. Verify these configurations during upgrades to prevent these issues.

\

Configure multiple authentications for a client

Configure a WLAN for 802.1X and LWA

Set up a WLAN to enforce strong user authentication with 802.1X and provide local web authentication using the controller interface.

Perform this task when you want to secure WLAN user access with 802.1X credentials and enable local web authentication for guest or additional user workflows.

Before you begin

Confirm that WLAN profiles and the necessary authentication lists are already created or available.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Select the required WLAN from the list of WLANs displayed.

Step 3 Choose **Security** > **Layer2** tab.

Step 4 Select the security method from the **Layer 2 Security Mode** drop-down list.

Step 5 In the **Auth Key Mgmt**, check the **802.1x** check box.

Step 6 Check the **MAC Filtering** check box to enable the feature.

Step 7 After MAC Filtering is enabled, from the **Authorization List** drop-down list, choose an option.

Step 8 Choose **Security** > **Layer3** tab.

Step 9 Check the **Web Policy** check box to enable the web authentication policy.

Step 10 From the **Web Auth Parameter Map** and the **Authentication List** drop-down lists, choose an option.

Step 11 Click **Update & Apply to Device**.

The WLAN is now configured to use both 802.1X authentication and local web authentication policies.

Configure a WLAN for 802.1X and LWA (CLI)

Set up a WLAN to enforce strong user authentication with 802.1X and provide local web authentication using the controller interface.

Perform this task when you want to secure WLAN user access with 802.1X credentials and enable local web authentication for guest or additional user workflows.

Before you begin

Confirm that WLAN profiles and the necessary authentication lists are already created or available.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN.

Example:

```
Device(config)# wlan wlan-name wland-id SSID-name
```

- **wlan-name** is the name of the configured WLAN.
- **wlan-id** is the WLAN identifier. The range is one to 512.
- **SSID-name** is the SSID name which can have up to 32 alphanumeric characters.

If you have already created and configured the WLAN, use the **wlan** *wlan-name* command.

Step 3 Enable security authentication list for dot1x security.

Example:

```
Device(config-wlan)# security dot1x authentication-list auth-list-name
```

The configuration is similar for all dot1x security WLANs.

Step 4 Enable web authentication.

Example:

```
Device(config-wlan)# security web-auth
```

Step 5 Enable authentication list for dot1x security.

Example:

```
Device(config-wlan)# security web-auth authentication-list default authenticate-list-name
```

Step 6 Map the parameter map name.

Example:

```
Device(config-wlan)# security web-auth parameter-map parameter-map-name
```

If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

Step 7 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

The WLAN is now configured to use both 802.1X authentication and local web authentication policies.

Configure WLAN for Preshared Key (PSK) and LWA (GUI)

Set up a WLAN to use both Preshared Key (PSK) and local web authentication via the graphical user interface.

Use this procedure when you want to enforce both PSK and local web authentication for user access to your wireless network.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Select the required WLAN.

Step 3 Choose **Security** > **Layer2** tab.

Step 4 Select the security method from the **Layer 2 Security Mode** drop-down list.

Step 5 In the Auth Key Mgmt, uncheck the **802.1x** check box.

Step 6 Check the **PSK** check box.

Step 7 Enter the **Pre-Shared Key**. Next, choose the PSK Format from the **PSK Format** drop-down list. Then, choose the PSK Type from the **PSK Type** drop-down list.

Step 8 Choose **Security** > **Layer3** tab.

Step 9 Check the **Web Policy** checkbox to enable web authentication policy.

Step 10 Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list. Then, choose the authentication list from the **Authentication List** drop-down list.

Step 11 Click **Update & Apply to Device**.

The selected WLAN now enforces both PSK and local web authentication settings

Configure WLAN for Preshared Key (PSK) and LWA (CLI)

Set up a WLAN to use both Preshared Key (PSK) and local web authentication.

Use this procedure when you want to enforce both PSK and local web authentication for user access to your wireless network.

Procedure

	Command or Action	Purpose
Step 1	Enter global configuration mode. **Example:** `Device# configure terminal`	
Step 2	Configure the WLAN. **Example:** `Device(config)# wlan wlan-name wland-id SSID-name`	• **wlan-name** is the name of the configured WLAN. • **wlan-id** is the WLAN identifier. The range is one to 512. • **SSID-name** is the SSID name which can have up to 32 alphanumeric characters. If you have already created and configured the WLAN, use the **wlan** *wlan-name* command.
Step 3	Configure the PSK shared key using the **security wpa psk set-key** *ascii/hex key password* command. **Example:**	

	Command or Action	Purpose
	`Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	
Step 4	Disable security AKM for dot1x. **Example:** `Device(config-wlan)# no security wpa akm dot1x`	
Step 5	Configure the PSK support. **Example:** `Device(config-wlan)# security wpa akm psk`	
Step 6	Enable web authentication for WLAN. **Example:** `Device(config-wlan)# security web-auth`	
Step 7	Enable authentication list for dot1x security. **Example:** `Device(config-wlan)# security web-auth authentication-list authenticate-list-name`	
Step 8	Configure the parameter map. **Example:** `(config-wlan)# security web-auth parameter-map parameter-map-name`	If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

The selected WLAN now enforces both PSK and local web authentication settings.

Configure WLAN for PSK or iPSK and CWA

Configure WLAN for PSK or iPSK and CWA (GUI)

Configure a WLAN to use either a Pre-Shared Key (PSK) or Identity Pre-Shared Key (iPSK) for authentication, and enable central web authentication for enhanced wireless security.

Use this task to set up secure WLAN access for users and devices, combining key-based authentication with web-based login, using your wireless controller's GUI.

Before you begin

Gather required PSK or iPSK values and authentication lists, as needed.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Select the required WLAN.

Step 3 Choose **Security** > **Layer2** tab.

Step 4 Select the security method from the **Layer 2 Security Mode** drop-down list.

Step 5 In the **Auth Key Mgmt**, uncheck the **802.1x** check box.

Step 6 Check the **PSK** check box.

Step 7 Enter the **Pre-Shared Key**. Then, choose the PSK Format from the **PSK Format** drop-down list and the PSK Type from the **PSK Type** drop-down list.

Step 8 Check the **MAC Filtering** check box to enable the feature.

Step 9 With MAC Filtering enabled, choose the Authorization List from the **Authorization List** drop-down list.

Step 10 Choose **Security** > **Layer3** tab.

Step 11 Check the **Web Policy** checkbox to enable web authentication policy.

Step 12 Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list and the authentication list from the **Authentication List** drop-down list.

Step 13 Click **Update &Apply to Device**.

The WLAN is now updated to use PSK or iPSK authentication and central web authentication, combining key-based access with web-based login for network users.

Configure WLAN for PSK or iPSK and CWA (CLI)

Configure a WLAN to use either a Pre-Shared Key (PSK) or Identity Pre-Shared Key (iPSK) for authentication, and enable central web authentication for enhanced wireless security.

Use this task to set up secure WLAN access for users and devices, combining key-based authentication with web-based login, using your wireless controller's CLI.

Before you begin

Gather required PSK or iPSK values and authentication lists, as needed.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN.

Example:

```
Device(config)# wlan wlan-name wland-id SSID-name
```

- **wlan-name** is the name of the configured WLAN.
- **wlan-id** is the WLAN identifier. The range is one to 512.
- **SSID-name** is the SSID name which can have up to 32 alphanumeric characters.

If you have already created and configured the WLAN, use the **wlan** *wlan-name* command.

Step 3 Disable security AKM for dot1x.

Example:

```
Device(config-wlan)# no security wpa akm dot1x
```

Step 4 Configure the PSK AKM shared key using the **security wpa psk set-key** *ascii/hex key password* command.

Example:

```
Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD
```

Step 5 Set the MAC filtering parameters.

Example:

```
Device(config-wlan)# mac-filtering auth-list-name
```

The WLAN is now updated to use PSK or iPSK authentication and central web authentication, combining key-based access with web-based login for network users.

Apply a policy profile to a WLAN

Configure and activate a policy profile for a WLAN using CLI.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the default policy profile.

Example:

```
Device(config)# wireless profile policy policy-iot policy-profile-name
```

Step 3 Configure AAA override to apply policies coming from the AAA or ISE servers.

Example:

```
Device(config-wireless-policy)# aaa-override
```

Step 4 Configure NAC in the policy profile.

Example:

```
Device(config-wireless-policy)# nac
```

Step 5 Shutdown the WLAN.

Example:

```
Device(config-wireless-policy)# no shutdown
```

Step 6 Return to privileged EXEC mode.

Example:

```
Device(config-wireless-policy)# end
```

The policy profile is applied to the WLAN and operational.

Configuring 802.1x and CWA on controller (CLIs)

Configure AAA authentication

Set up authentication, authorization, and accounting (AAA) on your device.

Decide which authentication methods and servers you want to use if you plan to configure additional settings.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create an AAA authentication model.

Example:

```
Device(config)# aaa new-model
```

AAA authentication is now enabled on the controller. Configure specific authentication methods as needed.

Configure AAA server for external authentication

Configure an AAA server to enable external authentication using a RADIUS server.

Use this process to allow external authentication for network devices through a specified RADIUS server.

Before you begin

- Obtain the RADIUS server IP address, key, and server name.
- Confirm network connectivity between the device and the RADIUS server.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a call station identifier sent in the RADIUS authentication messages.

Example:

```
Device(config)# radius-server attribute wireless authentication call-station-id ap-name-ssid
```

Step 3 Set the RADIUS server.

Example:

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

Step 4 Specify the RADIUS server address.

Example:

```
Device(config-radius-server)# address ipv4 radius-server-ip-address
```

Step 5 Specify the time-out value in seconds.

Example:

```
Device(config-radius-server)# timeout time-in-seconds
```

The range is between 10 and 1000 seconds.

Step 6 Specify the number of retries to the server.

Example:

```
Device(config-radius-server)# retransmit number-of-retries
```

The range is between zero and 100.

Step 7 Specify the authentication and encryption key used between the device and the key string RADIUS daemon running on the RADIUS server.

Example:

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

key-name can assume these values:

- 0—Specifies unencrypted key.
- 6—Specifies encrypted key.
- 7—Specifies HIDDEN key.
- Word—Unencrypted (cleartext) server key.

Step 8 Return to the configuration mode.

Example:

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

Step 9 Create a RADIUS server group identification.

Example:

```
Device(config)# aaa group server radius server-group
```

Step 10 Configure the server name.

Example:

```
Device(config)# server name server-name
```

Step 11 Define the time in minutes when a server marked as DEAD is held in that state

Example:

```
Device(config)# radius-server deadtime time-in-mins
```

Once the deadtime expires, the controller marks the server as UP (ALIVE) and notifies the registered clients about the state change. If the server is still unreachable after the state is marked as UP and if the DEAD criteria is met, then server is marked as DEAD again for the deadtime interval.

time-in-mins—Valid values range from one to 1440 minutes. Default value is zero. To return to the default value, use the **no radius-server deadtime** command.

The **radius-server deadtime** command can be configured globally or per aaa group server level.

You can use the **show aaa dead-criteria** or **show aaa servers** command to check for dead-server detection. If the default value is zero, deadtime is not configured.

The AAA server is configured for external authentication using the specified RADIUS server settings.

Configure AAA for authentication

Specify authentication methods for user logins and network access.

Use this task to define how the device authenticates users when accessing the CLI or network services. This process ensures that only authorized individuals can log in.

Before you begin

Ensure you have defined the necessary AAA server groups (for example, ISE2).

Procedure

	Command or Action	Purpose
Step 1	Define the authentication method at login. **Example:** `Device# aaa authentication login ISE_GROUP group ISE2 local`	Defines the authentication method at login.
Step 2	Define the authentication method at 802.1X. **Example:** `Device(config)# aaa authentication network ISE_GROUP group ISE2 local`	

The device now uses the authentication methods you specified for login and network access. This enforces AAA policies and improves security

Configure an accounting identity list

Enable accounting for user sessions on your device. This allows you to track when users are authorized and when their sessions end.

Use this configuration to send accounting records to a RADIUS server for identity management. This process also supports auditing and compliance.

Before you begin

Ensure the RADIUS server and AAA group server are configured.

Procedure

Enable accounting so that a start record accounting notice is sent when a client is authorized, and a stop record notice is sent when the session ends.

Example:

```
Device# aaa accounting identity ISE-named-list start-stop group ISE-server-group-name
```

Note
You can use the default list instead of specifying a named list.

The device sends accounting records to the specified RADIUS server when a user's session is authorized and when the session ends.

Configure AAA for CWA

Enable Change of Authorization (CoA) for RADIUS authentication on the controller for Central Web Authentication (CWA).

Before you begin

Ensure the RADIUS server and AAA group server are configured.

Procedure

Step 1 Configures the CoA on the controller.

Example:

```
Device# aaa server radius dynamic-author
```

Step 2 Configure a server key for a RADIUS client.

Example:

```
Device(config-locsvr-da-radius)# client client-ip-addr server-key key
```

After completing these steps, the controller uses dynamic CoA for Central Web Authentication. RADIUS clients can trigger authorization changes.

Define an ACL for RADIUS server

Create an access control list (ACL) to restrict and control traffic flow to and from the RADIUS server. Only authorized access is allowed, and authentication redirection is enforced.

Configure an extended access control list to work with Cisco Identity Services Engine (ISE) to redirect unauthenticated web traffic. Explicitly deny or permit specific protocols and sources.

Before you begin

Identify the IP addresses of your Cisco ISE, DHCP, and DNS servers.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the redirect ACL.

Example:

```
Device(config)# ip access-list extended redirect
```

HTTP and HTTPS browsing does not work without authentication per the other ACL. ISE is configured to use a redirect ACL named **redirect**.

Step 3 Specify packets to reject according to the sequence number

Example:

```
Device(config-ext-nacl)# sequence-number deny icmp any
```

.

Note
You must have the DHCP, DNS, and ISE servers in the reject sequences. See Configuration Example to Define an Access Control List for Radius Server, wherein the *111.111.111.111* refers to the IP address of the ISE server.

Step 4 Redirect all HTTP or HTTPS access to the Cisco ISE login page.

Example:

```
Device(config-ext-nacl)# permit TCP any any eq web-address
```

The ACL restricts access as specified by your deny rules and directs unauthenticated HTTP or HTTPS traffic to the Cisco ISE login page.

Example: Define an ACL for RADIUS server

This example shows how to define an access control list for RADIUS server:

```
Device# configure terminal
Device(config-ext-nacl) # 10 deny icmp any
Device(config-ext-nacl) # 20 deny udp any any eq bootps
Device(config-ext-nacl) # 30 deny udp any any eq bootpc
Device(config-ext-nacl) # 40 deny udp any any eq domain
Device(config-ext-nacl) # 50 deny tcp any host 111.111.111.111 eq 8443
Device(config-ext-nacl) # 55 deny tcp host 111.111.111.111 eq 8443 any
Device(config-ext-nacl) # 40 deny udp any any eq domain
Device(config-ext-nacl) # end
```

Configure WLAN with 802.1X authentication

Set up a WLAN with 802.1X authentication using CLI commands.

Perform this task to enable secure wireless access via a controller supporting 802.1X authentication.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter WLAN configuration mode.

Example:

```
Device(config)# wlan wlan-name
```

Step 3 Configure 802.1X for a WLAN.

Example:

```
Device(config-wlan)# security dot1x authentication-list ISE_GROUP
```

Step 4 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

You have configured and enabled your WLAN with 802.1X authentication.

Configure policy profile

Configure a wireless policy profile supporting AAA, DHCP, NAC, and VLAN, then enable it for use on your network.

Use this task to define policy settings applied to wireless clients, including authentication, DHCP handling, network access control, and VLAN assignment. These settings help enforce security and operational requirements for WLAN deployments.

Before you begin

Know the desired profile name, accounting list name, and VLAN ID.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the policy profile.

Example:

```
Device(config)# wireless profile policy profile-name
```

Step 3 Configure AAA override to apply policies coming from the AAA or Cisco Identify Services Engine (ISE) server.

Example:

```
Device(config-wireless-policy)# aaa-override
```

Step 4 Set the accounting list for IEEE 802.1x.

Example:

```
Device(config-wireless-policy)# accounting-list list-name
```

Step 5 Configure DHCP parameters for WLAN.

Example:

```
Device(config-wireless-policy)# ipv4 dhcp required
```

Step 6 Configure Network Access Control (NAC) in the policy profile. NAC is used to trigger the Central Web Authentication (CWA).

Example:

```
Device(config-wireless-policy)# nac
```

Step 7 Configure guest VLAN profile.

Example:

```
Device(config-wireless-policy)# vlan 25
```

Step 8 Enable policy profile.

Example:

```
Device(config-wireless-policy)# no shutdown
```

The wireless policy profile is configured with specified authentication, access control, DHCP, and VLAN parameters, and is enabled for use

Map a WLAN and policy profile to a policy tag

Assign a policy profile to a WLAN and link both to a policy tag, enabling dynamic assignment of policies to wireless networks.

Use this task when you need to organize WLAN and policy profiles under a single policy tag on your wireless controller using CLI commands.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure policy tag and enters policy tag configuration mode.

Example:

```
Device(config-policy-tag)# wireless tag policy policy-tag-name
```

Step 3 Map a policy profile to a WLAN profile.

Example:

```
Device(config-policy-tag)# wlan wlan-name policy profile-policy-name
```

Step 4 Save the configuration and exits the configuration mode and returns to privileged EXEC mode.

Example:

```
Device(config-policy-tag)# end
```

The WLAN and policy profile are now associated with the selected policy tag, and the configuration is applied to the device.

Configuring ISE for Central Web Authentication with Dot1x (GUI)

Define guest portal

Configure or select a guest portal for visitor access in Cisco Identity Services Engine (ISE).

Before you begin

Decide whether to create a new guest portal or use the default guest portal.

Procedure

Step 1 Login to the Cisco Identity Services Engine (ISE).

Step 2 Choose **Work Centers** > **Guest Access** > **Portals & Components**.

Step 3 Click **Guest Portal**.

The Guest Portal page opens, allowing you to configure the portal settings or use the default configuration for guest access.

Define authorization profile for a client

Configure an authorization profile in Cisco Identity Services Engine (ISE) to manage client redirection, guest portal access, and network authorization parameters.

Authorization profiles in Cisco ISE control how clients are redirected, such as directing guests to authentication portals. They also set parameters that manage client access to the network. You can create a custom profile or modify the default Cisco_Webauth result to suit your configuration needs.

Before you begin

Identify the requirements for client access, including portal settings and access control lists (ACLs).

Procedure

Step 1 Log in to the Cisco Identity Services Engine (ISE).

Step 2 Choose **Policy** > **Policy Elements** > **Authorization** > **Authorization Profiles**.

Step 3 Click **Add** to create your own custom or edit the Cisco_Webauth default result.

The authorization profile is configured in Cisco ISE, allowing targeted redirection and access control for clients according to your specified parameters.

Define an authentication rule

Create an authentication rule in Cisco Identity Services Engine (ISE) to specify user identification conditions within a policy set.

Use this task when you need to manage network access authentication criteria in your ISE deployment.

Procedure

Step 1 Login to the Cisco Identity Services Engine (ISE).

Step 2 Choose **Policy** > **Policy Sets** and click on the appropriate policy set.

Step 3 Expand **Authentication** policy.

Step 4 Expand **Options** and choose an appropriate **User ID**.

The authentication rule is configured for the selected policy set, allowing for defined user identification during authentication.

Define an authorization rule

Create an authorization rule to control access for users authenticating via 802.1x with a specific SSID in Cisco ISE.

Use this procedure to specify matching conditions and assign an authorization profile in Identity Services Engine (ISE).

Procedure

Step 1 Log in to the Cisco Identity Services Engine (ISE).

Step 2 Choose **Policy** > **Policy Sets** > **Authorization Policy**.

Step 3 Create a rule that matches the condition for 802.1x with a specific SSID (using Radius-Called-Station-ID).

Note
You get to view the CWA redirect attribute.

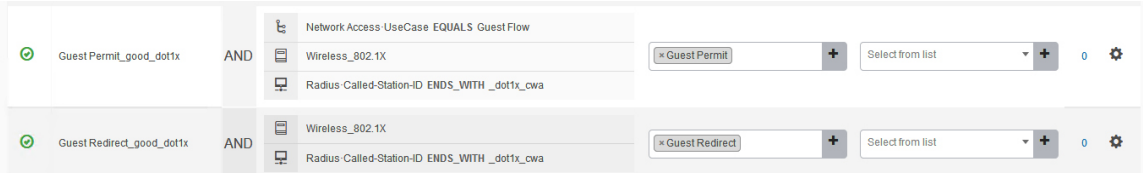
Step 4 Choose the already created authorization profile.

Step 5 From the **Result/Profile** column, choose the already created authorization profile.

Step 6 Click **Save**.

The image shows a sample working configuration.

Figure 1: Working Configuration Sample



The new authorization rule is now active and governs access based on the specified condition.

Create rules to match guest flow conditions

Before you begin

You must create a second rule that matches the guest flow condition and returns to network access details once the user completes authentication in the portal.

Configure Cisco ISE to grant network access to guest users after successful portal authentication.

Use this procedure to automatically apply the correct network access policies for guest users who connect to a specific SSID via 802.1X authentication.

Procedure

Step 1 Log in to the Cisco Identity Services Engine (ISE).

Step 2 Choose **Policy** > **Policy Sets** > **Authorization Policy**.

Step 3 Create a rule for 802.1X so Network Access-UseCase is Guest and a specific SSID is matched using RADIUS Called-Station-ID.

Note
You get to view the Permit Access.

Step 4 From the **Result/Profile** column, choose an existing authorization profile.

Step 5 Choose either the default or custom Permit Access profile.

Step 6 Click **Save**.

After successful authentication in the portal, guest users receive network access. The configured authorization profile is applied automatically.

Verify multiple authentication configurations

Layer 2 authentication

After L2 authentication (Dot1x) is complete, the client is moved to state.

To verify the client state after L2 authentication, use these commands:

```
Device# show wireless client summary
Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-----------------------------------------------------------------------------------------------------

58ef.68b6.aa60 ewlc1_ap_1   3  Webauth Pending    11n(5)        Dot1x  Local
Number of Excluded Clients: 0
```

```
Device# show wireless client mac-address <mac_address> detail

Auth Method Status List

Method: Dot1x
Webauth State: Init
Webauth Method: Webauth
Local Policies:
Service Template: IP-Adm-V6-Int-ACL-global (priority 100)
URL Redirect ACL: IP-Adm-V6-Int-ACL-global
Service Template: IP-Adm-V4-Int-ACL-global (priority 100)
URL Redirect ACL: IP-Adm-V4-Int-ACL-global
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50
```

```
Device# show platform software wireless-client chassis active R0

        ID  MAC Address      WLAN  Client     State
-------------------------------------------------------------------------------------
  0xa0000003      58ef.68b6.aa60    3             L3          Authentication
```

```
Device# show platform software wireless-client chassis active F0

    ID     MAC Address   WLAN  Client     State  AOM ID    Status
-----------------------------------------------------------------------------------------------------
```

```
0xa0000003    58ef.68b6.aa60    3           L3          Authentication.         730.
Done
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary

Client Type Abbreviations:
RG - REGULAR   BLE - BLE
HL - HALO    LI - LWFL INT

Auth State Abbrevations:
UK - UNKNOWN    IP - LEARN    IP IV - INVALID
L3 - L3 AUTH RN - RUN

Mobility State Abbreviations:
UK - UNKNOWN       IN - INIT
LC - LOCAL               AN - ANCHOR
FR - FOREIGN          MT - MTE
IV - INVALID


EoGRE Abbreviations:
N - NON EOGRE Y - EOGRE

CPP IF_H   DP IDX       MAC Address      VLAN   CT   MCVL AS MS E   WLAN      POA
------------------------------------------------------------------------------------
0X49     0XA0000003    58ef.68b6.aa60     50    RG     0  L3 LC N wlan-test 0x90000003
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath summary
Vlan   DP IDX         MAC Address      VLAN   CT   MCVL AS MS E   WLAN      POA
------------------------------------------------------------------------------------
0X49   0xa0000003    58ef.68b6.aa60     50    RG     0  L3 LC N wlan-test 0x90000003
```

Layer 3 Authentication

Once L3 authentication is successful, the client is moved to *Run* state.

To verify the client state after L3 authentication, use these commands:

```
Device# show wireless client summary

Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-------------------------------------------------------------------------------------------------------------------

58ef.68b6.aa60   ewlc1_ap_1  3     Run    11n(5)   Web Auth      Local
Number of Excluded Clients: 0
```

```
Device# show wireless client mac-address 58ef.68b6.aa60 detail

Auth Method Status List

Method: Web Auth
Webauth State: Authz
Webauth Method: Webauth
Local Policies:
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50

Server Policies:

Resultant Policies:
VLAN: 50
Absolute-Timer: 1800
```

```
Device# show platform software wireless-client chassis active R0

ID          MAC Address     WLAN    Client State
-------------------------------------------------
0xa0000001 58ef.68b6.aa60    3          Run

Device# show platform software wireless-client chassis active f0

ID         MAC Address       WLAN    Client State   AOM ID.  Status
-----------------------------------------------------------------------
0xa0000001 58ef.68b6.aa60.   3          Run         11633    Done

Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary

Client Type Abbreviations:
RG - REGULAR   BLE - BLE
HL - HALO      LI - LWFL INT

Auth State Abbrevations:
UK - UNKNOWN    IP - LEARN    IP IV - INVALID
L3 - L3 AUTH RN - RUN
Mobility State Abbreviations:
UK - UNKNOWN       IN - INIT
LC - LOCAL         AN - ANCHOR
FR - FOREIGN       MT - MTE
IV - INVALID
EoGRE Abbreviations:
N - NON EOGRE Y - EOGRE

CPP IF_H   DP IDX       MAC Address   VLAN  CT  MCVL AS MS E   WLAN     POA
-------------------------------------------------------------------------------
0X49     0XA0000003    58ef.68b6.aa60  50   RG   0   RN LC N wlan-test 0x90000003

Device# show platform hardware chassis active qfp feature wireless wlclient datapath summary

Vlan   pal_if_hd1        mac           Input Uidb     Output Uidb
-----------------------------------------------------------------
50     0xa0000003    58ef.68b6.aa60     95929            95927
```

Verifying PSK+Webauth Configuration

```
Device# show wlan summary

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 12:08:32.941 CEST Tue Oct 6 2020


Number of WLANs: 1

ID Profile Name SSID Status Security
-------------------------------------------------------------------------------------------------------------------

23 Gladius1-PSKWEBAUTH Gladius1-PSKWEBAUTH UP [WPA2][PSK][AES],[Web Auth]
```