Multiple Authentications for a Client

Information About Multiple Authentications for a Client

Multiple Authentication feature is an extension of Layer 2 and Layer 3 security types supported for client join.

Note You can enable both L2 and L3 authentication for a given SSID.

Note The Multiple Authentication feature is applicable for regular clients only.

Information About 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 following table outlines the supported combination of authentications:

Layer 2	Layer 3	Supported
MAB	CWA	Yes

MAB	LWA	Yes
MAB + PSK	-	Yes
MAB + 802.1X	-	Yes
MAB Failure	LWA	Yes
802.1X	CWA	Yes
802.1X	LWA	Yes
PSK	-	Yes
PSK	LWA	Yes
PSK	CWA	Yes
iPSK	-	Yes
iPSK	CWA	Yes
iPSK + MAB	CWA	Yes
iPSK	LWA	No
MAB Failure + PSK	LWA	Yes
MAB Failure + PSK	CWA	No
MAB Failure + OWE	LWA	Yes
MAB Failure + SAE	LWA	Yes

From 16.10.1 onwards, 802.1X configurations on WLAN support web authentication configurations with WPA or WPA2 configuration.

The feature also supports the following AP modes:

- Local
- FlexConnect
- Fabric

Jumbo Frame Support for RADIUS Packets

This document describes how to configure IP Maximum Transmission Unit (MTU) size for RADIUS server. RADIUS packets will get fragmented based on IP MTU, if source interface is attached to RADIUS group. With the new design, the RADIUS packets get fragmented at interface IP MTU configured value.

Note Fragmentation size is fixed.

Combination of Authentications on MAC Failure Not Supported on a Client

The following 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

Configuring Multiple Authentications for a Client

Configuring WLAN for 802.1X and Local Web Authentication (GUI)

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 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**.

Configuring WLAN for 802.1X and Local Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name*	Enters WLAN configuration sub-mode.

	Command or Action	Purpose
	Example: `Device(config)# wlan wlan-test 3 ssid-test`	• *profile-name*: Profile name of the configured WLAN. • *wlan-id*: Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name*: SSID that can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter the **wlan** *profile-name* command.
Step 3	**security dot1x authentication-list** *auth-list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
Step 4	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication.
Step 5	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for dot1x security.
Step 6	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Maps the parameter map. **Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Example

```
wlan wlan-test 3 ssid-test
 security dot1x authentication-list default
 security web-auth
 security web-auth authentication-list default
 security web-auth parameter-map WLAN1_MAP
 no shutdown
```

Configuring WLAN for Preshared Key (PSK) and Local Web Authentication (GUI)

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** and choose the PSK Format from the **PSK Format** drop-down list and 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 and the authentication list from the **Authentication List** drop-down list.
Step 11	Click **Update & Apply to Device**.

Configuring WLAN for Preshared Key (PSK) and Local Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration sub-mode. • *profile-name*- Is the profile name of the configured WLAN. • *wlan-id* - Is the wireless LAN identifier. Range is from 1 to 512. • *SSID_Name* - Is the SSID which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *profile-name* command.

	Command or Action	Purpose
Step 3	**security wpa psk set-key** *ascii/hex key password* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	Configures the PSK shared key.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures the PSK support.
Step 6	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication for WLAN.
Step 7	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list webauth`	Enables authentication list for dot1x security.
Step 8	**security web-auth parameter-map** *parameter-map-name* **Example:** `(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Configures the parameter map. **Note** If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

Example

```
wlan wlan-test 3 ssid-test
 security wpa psk set-key ascii 0 PASSWORD
 no security wpa akm dot1x
 security wpa akm psk
 security web-auth
 security web-auth authentication-list webauth
 security web-auth parameter-map WLAN1_MAP
```

Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication (GUI)

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** and 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**.

Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication

Configuring WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration sub-mode. • *profile-name* - Is the profile name of the configured WLAN. • *wlan-id* - Is the wireless LAN identifier. Range is from 1 to 512.

	Command or Action	Purpose
		• *SSID_Name* - Is the SSID which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *profile-name* command.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**security wpa psk set-key** *ascii/hex key password* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	Configures the PSK AKM shared key.
Step 5	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.

Example

```
wlan wlan-test 3 ssid-test
 no security wpa akm dot1x
 security wpa psk set-key ascii 0 PASSWORD
 mac-filtering test-auth-list
```

Applying Policy Profile to a WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-iot`	Configures the default policy profile.

	Command or Action	Purpose
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply policies coming from the AAA or ISE servers.
Step 4	**nac** **Example:** `Device(config-wireless-policy)# nac`	Configures NAC in the policy profile.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Shutdown the WLAN.
Step 6	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Example

```
wireless profile policy policy-iot
 aaa-override
 nac
 no shutdown
```

Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Pre-Shared Key (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name*: Profile name of the configured WLAN. • *wlan-id*: Wireless LAN identifier. Range is from 1 to 512.

	Command or Action	Purpose
		• *SSID_Name*: SSID that can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter the **wlan** *profile-name* command.
Step 3	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.
Step 4	**security wpa psk set-key** *ascii/hex key password* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	Configures the PSK AKM shared key.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures PSK support.
Step 7	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for dot1x security.
Step 8	**security web-auth authorization-list** *authorize-list-name* **Example:** `Device(config-wlan)# security web-auth authorization-list default`	Enables authorization list for dot1x security.
Step 9	**security web-auth on-macfilter-failure** **Example:** `Device(config-wlan)# security web-auth on-macfilter-failure`	Enables web authentication on MAC filter failure.
Step 10	**security web-auth parameter-map** *parameter-map-name*	Configures the parameter map.

	Command or Action	Purpose
	Example: `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	**Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with OWE (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name*: Profile name of the configured WLAN. • *wlan-id*: Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name*: SSID that can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter the **wlan** *profile-name* command.
Step 3	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.

	Command or Action	Purpose
Step 5	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 6	**security wpa akm owe** **Example:** `Device(config-wlan)# security wpa akm owe`	Enables WPA3 OWE support.
Step 7	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for dot1x security.
Step 8	**security web-auth authorization-list** *authorize-list-name* **Example:** `Device(config-wlan)# security web-auth authorization-list default`	Enables authorization list for dot1x security.
Step 9	**security web-auth on-macfilter-failure** **Example:** `Device(config-wlan)# security web-auth on-macfilter-failure`	Enables web authentication on MAC filter failure.
Step 10	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Configures the parameter map. **Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Secure Agile Exchange (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name*: Profile name of the configured WLAN. • *wlan-id*: Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name*: SSID that can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter the **wlan** *profile-name* command.
Step 3	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 6	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables AKM SAE support.
Step 7	**security web-auth authentication-list** *authenticate-list-name*	Enables authentication list for dot1x security.

	Command or Action	Purpose
	Example: `Device(config-wlan)# security web-auth authentication-list default`	
Step 8	**security web-auth authorization-list** *authorize-list-name* **Example:** `Device(config-wlan)# security web-auth authorization-list default`	Enables authorization list for dot1x security.
Step 9	**security web-auth on-macfilter-failure** **Example:** `Device(config-wlan)# security web-auth on-macfilter-failure`	Enables web authentication on MAC filter failure.
Step 10	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Configures the parameter map. **Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring 802.1x and Central Web Authentication on Controller (CLIs)

Creating AAA Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.

Configuring AAA Server for External Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**radius-server attribute wireless authentication call-station-id ap-name-ssid** **Example:** `Device(config)# radius-server attribute wireless authentication call-station-id ap-name-ssid`	Configures a call station identifier sent in the RADIUS authentication messages.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server ISE2`	Sets the RADIUS server.
Step 4	**address ipv4** *radius-server-ip-address* **Example:** `Device(config-radius-server)# address ipv4 111.111.111.111`	Specifies the RADIUS server address.
Step 5	**timeout** *seconds* **Example:** `Device(config-radius-server)# timeout 10`	Specify the time-out value in seconds. The range is between 10 and 1000 seconds.
Step 6	**retransmit** *number-of-retries* **Example:** `Device(config-radius-server)# retransmit 10`	Specify the number of retries to the server. The range is between 0 and 100.
Step 7	**key** *key* **Example:** `Device(config-radius-server)# key cisco`	Specifies the authentication and encryption key used between the device and the key string RADIUS daemon running on the RADIUS server. *key* covers the following: • 0—Specifies unencrypted key. • 6—Specifies encrypted key. • 7—Specifies HIDDEN key. • Word—Unencrypted (cleartext) server key.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to the configuration mode.
Step 9	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius ISE2`	Creates a RADIUS server-group identification.
Step 10	**server name** *server-name* **Example:** `Device(config)# server name ISE2`	Configures the server name.
Step 11	**radius-server deadtime** *time-in-minutes* **Example:** `Device(config)# radius-server deadtime 5`	Defines the time in minutes when a server marked as DEAD is held in that state. 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 1 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.

Configuring AAA for Authentication

Before you begin

Configure the RADIUS server and AAA group server.

Procedure

	Command or Action	Purpose
Step 1	**aaa authentication login** **Example:** `Device# aaa authentication login ISE_GROUP group ISE2 local`	Defines the authentication method at login.
Step 2	**aaa authentication dot1x** **Example:** `Device(config)# aaa authentication network ISE_GROUP group ISE2 local`	Defines the authentication method at dot1x.

Configuring Accounting Identity List

Before you begin

Configure the RADIUS server and AAA group server.

Procedure

	Command or Action	Purpose
Step 1	**aaa accounting identity** *named-list* **start-stop group** *server-group-name* **Example:** `Device# aaa accounting identity ISE start-stop group ISE2`	Enables accounting to send a start-record accounting notice when a client is authorized and a stop-record at the end. **Note** You can also use the default list instead of the named list.

Configuring AAA for Central Web Authentication

Before you begin

Configure the RADIUS server and AAA group server.

Procedure

	Command or Action	Purpose
Step 1	**aaa server radius dynamic-author** **Example:** `Device# aaa server radius dynamic-author`	Configures the Change of Authorization (CoA) on the controller.
Step 2	**client** *client-ip-addr* **server-key** *key* **Example:**	Configures a server key for a RADIUS client.

	Command or Action	Purpose
	`Device(config-locsvr-da-radius)# client 111.111.111.111 server-key ciscokey`	

Defining an Access Control List for Radius Server

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended redirect** **Example:** `Device(config)# ip access-list extended redirect`	The HTTP and HTTPS browsing does not work without authentication (per the other ACL) as ISE is configured to use a redirect ACL (named **redirect**).
Step 3	*sequence-number* **deny icmp any** **Example:** `Device(config-ext-nacl)# 10 deny icmp any`	Specifies packets to reject according to the sequence number. **Note** You must have the DHCP, DNS, and ISE servers in the reject sequences. Refer to 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	**permit TCP any any eq** *web-address* **Example:** `Device(config-ext-nacl)# permit TCP any any eq www`	Redirects all HTTP or HTTPS access to the Cisco ISE login page.

Configuration Example to Define an Access Control List 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
```

Configuring WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Device(config)# wlan wlan30`	Enters WLAN configuration mode.
Step 3	**security dot1x authentication-list ISE_GROUP** **Example:** `Device(config-wlan)# security dot1x authentication-list ISE_GROUP`	Configures 802.1X for a WLAN.
Step 4	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy wireless-profile1`	Configures policy profile.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply policies coming from the AAA or Cisco Identify Services Engine (ISE) server.
Step 4	**accounting-list** *list-name* **Example:**	Sets the accounting list for IEEE 802.1x.

	Command or Action	Purpose
	`Device(config-wireless-policy)# accounting-list ISE`	
Step 5	**ipv4 dhcp required** **Example:** `Device(config-wireless-policy)# ipv4 dhcp required`	Configures DHCP parameters for WLAN.
Step 6	**nac** **Example:** `Device(config-wireless-policy)# nac`	Configures Network Access Control (NAC) in the policy profile. NAC is used to trigger the Central Web Authentication (CWA).
Step 7	**vlan 25** **Example:** `Device(config-wireless-policy)# vlan 25`	Configures guest VLAN profile.
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables policy profile.

Mapping WLAN and Policy Profile to Policy Tag

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy xx-xre-policy-tag`	Configures policy tag and enters policy tag configuration mode.
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan wlan30 policy wireless-profile1`	Maps a policy profile to a WLAN profile.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.

Configuring ISE for Central Web Authentication with Dot1x (GUI)

Defining Guest Portal

Before you begin

Define the 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**.

Defining Authorization Profile for a Client

Before you begin

You can define the authorization profile to use guest portal and other additional parameters as per the requirement. Authorization profile redirects the client to the authentication portal. In the latest Cisco ISE version, Cisco_Webauth authorization results exist already, and you can edit the same to modify the redirection ACL name to match the configuration in the controller.

Procedure

Step 1 Login 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.

Defining Authentication Rule

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**.

Defining Authorization Rule

Procedure

Step 1 Login 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.

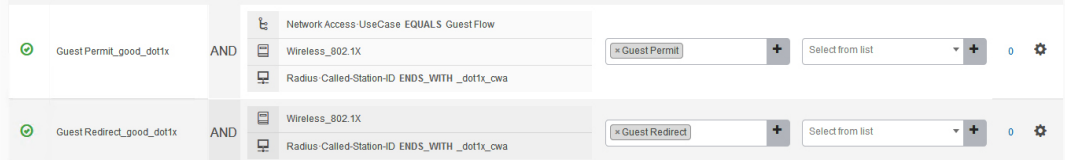
Step 4 Choose the already created authorization profile.

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

Step 6 Click **Save**.

Note The following image depicts the working configuration sample for your reference.

Figure 1: Working Configuration Sample



Creating Rules to Match Guest Flow Condition

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.

Procedure

Step 1 Login 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, Network Access-UseCase EQUALS Guest, and a specific SSID (using Radius-Called-Station-ID).

Note You get to view the Permit Access.

Step 4 From the **Result/Profile** column, choose the already created authorization profile.

Step 5 Choose the default or customized Permit Access.

Step 6 Click **Save**.

Verifying Multiple Authentication Configurations

Layer 2 Authentication

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

To verify the client state after L2 authentication, use the following 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 the following 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]
```