Wireless Guest Access

Wireless Guest Access

The Wireless Guest Access feature addresses the need to provide internet access to guests in a secure and accountable manner. The implementation of a wireless guest network uses the enterprise's existing wireless and wired infrastructure to the maximum extent. This reduces the cost and complexity of building a physical overlay network. Wireless Guest Access solution comprises of two controllers - a Guest Foreign and a Guest Anchor. An administrator can limit bandwidth and shape the guest traffic to avoid impacting the performance of the internal network.

Note

- When a client joins through a capwap tunnel from an AP, the RADIUS NAS-Port-Type is set as "wireless 802.11". Here, Point of Attachment (PoA) and Point of Presence (PoP) is the same.
- When a client joins through a mobility tunnel, the RADIUS NAS-Port-Type is set as "virtual". Here, PoA is the Foreign controller and PoP is the Anchor controller as the client is anchored. For information on the standard types, see the following link:

  https://www.iana.org/assignments/radius-types/radius-types.xhtml#radius-types-13

Wireless Guest Access feature comprises the following functions:

- Guest Anchor controller is the point of presence for a client.

- Guest Anchor Controller provides internal security by forwarding the traffic from a guest client to a Cisco Wireless Controller in the demilitarized zone (DMZ) network through the anchor controller.
- Guest Foreign controller is the point of attachment of the client.
- Guest Foreign Controller is a dedicated guest WLAN or SSID and is implemented throughout the campus wireless network wherever guest access is required. A WLAN with mobility anchor (guest controller) configured on it identifies the guest WLAN.
- Guest traffic segregation implements Layer 2 or Layer 3 techniques across the campus network to restrict the locations where guests are allowed.
- Guest user-level QoS is used for rate limiting and shaping, although it is widely implemented to restrict the bandwidth usage for a guest user.
- Access control involves using embedded access control functionality within the campus network, or implementing an external platform to control guest access to the Internet from the enterprise network.
- Authentication and authorization of guests that are based on variables, including date, duration, and bandwidth.
- An audit mechanism to track who is currently using, or has used, the network.
- A wider coverage is provided by including areas such as lobbies and other common areas that are otherwise not wired for network connectivity.
- The need for designated guest access areas or rooms is removed.

Note To use IRCM with AireOS in your network, contact Cisco TAC for assistance.

Table 1: Supported Controllers

Controller Name	Supported as Guest Anchor	Supported as Guest Foreign
Cisco Catalyst 9800-40 Wireless Controller	Yes	Yes
Cisco Catalyst 9800-80 Wireless Controller	Yes	Yes
Cisco Catalyst 9800-CL Wireless Controller	Yes	Yes
Cisco Catalyst 9800-L Wireless Controller	Yes	Yes
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	No	No
Cisco Catalyst 9800 Embedded Wireless Controller on Cisco Catalyst 9100 Series APs	No	No

Following is a list of features supported by Cisco Guest Access:

Supported Features

- Sleeping Clients
- FQDN
- AVC (AP upstream and downstream)
- Native Profiling
- Open Authentication
- OpenDNS
- Supported Security Methods:
  - MAB Central Web Authentication (CWA)
  - Local Web Authentication (LWA)
  - LWA on MAB Failure
  - 802.1x + CWA
  - 802.1x
  - PSK
  - 802.1x + LWA
  - PSK + CWA
  - PSK + LWA
  - iPSK + CWA
- SSID QoS Upstream and Downstream (Foreign)
- AP/ Client SSO
- Static IP Roaming
- Client IPv6
- Roaming across controllers
- RADIUS Accounting

Note In a guest access scenario, accounting is always performed at the foreign controller for all authentication methods.

- QoS: Client-Level Rate Limiting
- Guest Anchor Load Balancing
- Workgroup Bridges (WGB)

Note To enable the controller to support multiple VLANs from a WGB, use **wgb vlan** command.

Foreign Map Overview

Guest Access supports Foreign Map using Policy Profile and WLAN Profile configuration models in Cisco Catalyst 9800 Series Wireless Controller.

Foreign Map support in Cisco Catalyst 9800 Series Wireless Controller is achieved with the following policy profile and WLAN profile config model.

- Guest Foreign commands:
  - **Foreign1: wlanProf1 PolicyProf1**
  - **Foreign2: wlanProf2 PolicyProf2**
- Guest Anchor commands:
  - **wlanProf1, wlanProf2**
  - **PolicyProf1: Vlan100 - subnet1**
  - **PolicyProf2: Vlan200 - subnet2**

Foreign Map Roaming

Configure two different WLAN profiles on the two Guest Foreigns and seamless roaming is not allowed between them. This is expected configuration. However, seamless roaming is allowed if the same WLAN profile is configured on two Guest Foreigns, but it prevents Foreign Map feature from working.

Wireless Guest Access: Use Cases

The wireless guest access feature can be used to meet different requirements. Some of the possibilities are shared here.

Scenario One: Providing Secured Network Access During Company Merger

This feature can be configured to provide employees of **company A** who are visiting **company B** to access company A resources on company B network securely.

Scenario Two: Shared Services over Existing Setup

Using this feature, you can provide multiple services using multiple vendors piggy backing on the existing network. A company can provide services on an SSID which is anchored on the existing controller. This is while the existing service continues to serve over the same controller and network.

Load Balancing Among Multiple Guest Controllers

- You can configure export anchors to load balance large guest client volumes. For a single export foreign guest WLAN configuration, up to 72 controllers are allowed. To configure mobility guest controllers, use **mobility anchor** *ip address*.
- You can specify primary anchors with priority (1,3) and choose another anchor as backup in case of failure.
- In a multi-anchor scenario, when the primary anchor goes down, the clients get disconnected from the primary anchor and joins the secondary anchor.

Guidelines and Limitations for Wireless Guest Access

- Match the security profiles under WLAN on both Guest Foreign, and Guest Anchor.
- Match the policy profile attributes such as NAC and AAA Override on both Guest Foreign, and Guest Anchor controllers.
- On Export Anchor, the WLAN profile name and Policy profile name is chosen when a client joins at runtime and the same should match with the Guest Foreign controller.

Troubleshooting IPv6

When a guest export client cannot get a routable IPv6 address through SLAAC or cannot pass traffic when the IPv6 address is learned through DHCPv6, you can use the following workarounds:

- On IPv6 Routers: You can work around the RA multicast to unicast conversion by modifying behavior on the IPv6 gateway. Depending on the product, this may be the default behavior or may require configuration.
  - On Cisco IPv6 Routers
    - Cisco Nexus platform: Has solicited unicast RA enabled by default to help with wireless deployment.
    - Cisco IOS-XE platform: Use the following configuration command to turn on unicast RA to help with wireless deployment:

      ipv6 nd ra solicited unicast

  - On non-Cisco IPv6 Routers: If non-Cisco network devices do not support configuration command to enable solicited unicast RA then a work around does not exist.

Configure Mobility Tunnel for Guest Access (GUI)

Procedure

Step 1 Choose **Configure** > **Tags and Profiles** > **WLANs**.

Step 2 In the **Wireless Networks** area, click the relevant WLAN or RLAN and click **Mobility Anchor**.

Step 3 In the **Wireless Network Details** section, choose a device from the **Switch IP Address** drop-down list.

Step 4 Click **Apply**.

Configure Mobility Tunnel for Guest Access (CLI)

Follow the procedure given below to configure a mobility tunnel.

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility group name** *group name* **Example:** `Device(config)# wireless mobility group name mtunnelgrp`	Configures a mobility group.
Step 2	**wireless mobility mac-address** *mac address* **Example:** `Device(config)# wireless mobility mac-address 0d:4c:da:3a:f2:21`	Configures a mobility MAC address.
Step 3	**wireless mobility group member mac** *mac address* **ip** *ip address* **group** *group name* **Example:** `Device(config)# wireless mobility group member mac-address df:07:a1:a7:a8:55 ip 206.223.123.2 group mtgrp`	Configures a mobility peer.

Configuring Guest Access Policy (GUI)

Procedure

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

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** and enable the **Central Switching** toggle button.

Step 4 In the **Access Policies** tab, under the **VLAN** settings, choose the vlans from the **VLAN/VLAN Group** drop-down list.

Step 5 In the **Mobility** tab, under the **Mobility Anchors** settings, check the **Export Anchor** check box.

Step 6 In the **Advanced** tab, under the **WLAN Timeout** settings, enter the **Idle Timeout (sec)**.

Step 7 Click **Apply to Device**.

Configuring Guest Access Policy (CLI)

Follow the procedure given below to create and configure the guest access profile policy. Alternately, you may use the existing default policy profile after configuring the mobility anchor to that policy.

You can only configure anchors which are peers. Ensure that the IP address that is used is a mobility peer and is included in the mobility group. The system shows an invalid anchor IP address error message when any other IP address is used.

To delete the mobility group, ensure that the mobility peer which is also a mobility anchor is removed from the policy profile.

Note

- No payload is sent to Guest Foreign to display the VLAN.
- To avoid a client exclusion from occurring due to VLAN, Cisco Catalyst 9800 Series Controllers need to define VLAN along with the associated name being pushed from ISE.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan_policy_profile* **Example:** `Device(config)# wireless profile policy guest-test-policy`	Configures the policy profile and enters wireless profile configuration mode. **Note** • You can use the **default-policy-profile** to configure the profile policy.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Shuts down the policy if it exists before configuring the anchor.
Step 4	**central switching** **Example:**	(Optional) Enables central switching.

	Command or Action	Purpose
	`Device(config-wireless-policy)# central switching`	

Step 5	Choose the first option to configure the Guest Foreign or second option to configure the Guest Anchor:
	• **mobility anchor** *anchor-ip-address*
	• **mobility anchor**
	Example:
	For Guest Foreign:
	`Device(config-wireless-policy)# mobility anchor 19.0.2.1`
	For Guest Anchor:
	`Device(config-wireless-policy)# mobility anchor`
		Configures Guest Foreign or Guest Anchor.

Step 6	**idle-timeout** *timeout* **Example:** `Device (config-wireless-policy)# idle-timeout 1000`	(Optional) Configures duration of idle timeout, in seconds.
Step 7	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan 2`	Configures VLAN name or VLAN Id. **Note** VLAN is optional for a Guest Foreign controller.
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables policy profile.
Step 9	**end** **Example:** `Device(config-wireless-policy)# end`	Exits the configuration mode and returns to privileged EXEC mode.
Step 10	**show wireless profile policy summary** **Example:** `Device# show wireless profile policy summary`	(Optional) Displays the configured profiles.
Step 11	**show wireless profile policy detailed** *policy-profile-name* **Example:** `Device# show wireless profile policy detailed guest-test-policy`	(Optional) Displays detailed information of a policy profile.

Viewing Guest Access Debug Information (CLI)

- To display client level detailed information about mobility state and the anchor IP address, use the following command:.

  show wireless client mac-add *mac-address* **detail**

- To display the client mobility statistics, use the following command:

  show wireless client mac-address *mac-address* **mobility statistics**

- To display client level roam history for an active client in sub-domain, use the following command:

  show wireless client mac-address *mac-address* **mobility history**

- To display detailed parameters of a given profile policy, use the following command:

  show wireless profile policy detailed *policy-name*

- To display the global level summary for all mobility messages, use the following command:

  show wireless mobility summary

- To display the statistics for the Mobility manager, use the following command:

  show wireless stats mobility

Verifying Wireless Guest Access Enablement

To check if wireless guest access is enabled, run the following command.

```
Device# show platform hardware chassis  active  qfp feature sw client vlan all

------------------------------------------------------------
Vlan : 666
Learning Enabled : true
DHCPSN Enabled : true
Non IP Multicast Enabled : false
Broadcast Enabled : false
Wireless Passive Client Enabled : false
Guest-Lan Enabled : true
MTU : 65535
Input UIDB : 65503
Output UIDB : 65497
Flood List : 0XB8658A0
```

Configure Guest Access Using Different Security Methods

The following sections provide information about the following:

Open Authentication

To configure the guest access with open authentication, follow the steps:

1. Configuring the WLAN Profile
2. #unique_1612

Note No tag is required unless AVC is enabled.

Configure a WLAN Profile for Guest Access with Open Authentication (GUI)

Procedure

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

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**. Choose the radio policy from the **Radio Policy** drop-down list. Enable or disable the **Status** and **Broadcast SSID** toggle buttons.

Step 4 Choose **Security** > **Layer2** tab. Uncheck the **WPA Policy**, **WPA2 Policy**, **AES** and **802.1x** check boxes.

Step 5 Click **Apply to Device**.

Configure a WLAN Profile For Guest Access with Open 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*. **Example:** `Device(config)# wlan mywlan 34 mywlan-ssid`	Configures the WLAN and SSID.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**no security wpa wpa2** **Example:**	Disables WPA2 security.

	Command or Action	Purpose
	`Device(config-wlan)# no security wpa wpa2`	
Step 6	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Saves the configuration.

Configuring a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile* **Example:** `Device(config)# wireless profile policy open_it`	Configures WLAN policy profile and enters the wireless policy configuration mode.

Step 3	Choose the first option to configure a Guest Foreign or second option to configure a Guest Anchor:
	• **mobility anchor** *anchor-ip-address*
	• **mobility anchor**
	Example:
	For Guest Foreign:
	`Device (config-wireless-policy)# mobility anchor 19.0.2.1`
	For Guest Anchor:
	`Device (config-wireless-policy)# mobility anchor`
		Configures Guest Foreign or Guest Anchor.

Step 4	**central switching**. **Example:** `Device(config-wireless-policy)# central switching`	Enables Central switching
Step 5	**vlan** *id*	Configures a VLAN name or VLAN ID.

	Command or Action	Purpose
	Example: `Device(config-wireless-policy)# vlan 16`	**Note** VLAN is optional for a Guest Foreign controller.
Step 6	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.

Local Web Authentication

To configure LWA, follow these steps:

1. Configure a Parameter Map (CLI)
2. Configure a WLAN Profile for Guest Access with Local Web Authentication (CLI)
3. Applying Policy Profile on a WLAN
4. Configure an AAA Server for Local Web Authentication (CLI)

Configure a Parameter Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Web Auth**.

Step 2 Click **Add**.

Step 3 Enter the **Parameter-map name**, **Maximum HTTP connections**,**Init-State Timeout(secs)** and choose **webauth** in the **Type** drop-down list.

Step 4 Click **Apply to Device**.

Configure a Parameter Map (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth global** **Example:** `Device(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode.

	Command or Action	Purpose
Step 3	**type webauth** **Example:** `Device(config-params-parameter-map)#type webauth`	Configures the webauth type parameter.
Step 4	**timeout init-state sec** *timeout-seconds* **Example:** `Device(config-params-parameter-map)# timeout inti-state sec 3600`	Configures the WEBAUTH timeout in seconds. Valid range for the time in sec parameter is 60 to 3932100 seconds.
Step 5	**virtual-ip ipv4** *virtual_IP_address* **Example:** `Device(config-params-parameter-map)#virtual-ip ipv4 209.165.201.1`	Configures a VLAN name or VLAN ID.

Configure a WLAN Profile for Guest Access with Local Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2 Click on the **WLAN** name.
Step 3 Choose **Security** > **Layer3**.
Step 4 Check the **Web Policy** check box.
Step 5 Choose a parameter map from the **Web Auth Parameter Map** drop-down list.
Step 6 Choose an authentication list from the **Authentication List** drop-down list.
Step 7 Click **Update & Apply to Device**.

Configure a WLAN Profile for Guest Access with Local Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-id ssid-name* **Example:** `Device# Device(config)# wlan mywlan 38 mywlan-ssid1`	Configures the WLAN and SSID.

	Command or Action	Purpose
Step 3	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication for a WLAN.
Step 4	**security web-auth parameter-map** *default* **Example:** `Device(config-wlan)# security web-auth parameter-map default`	Configure the default parameter map. **Note** When **security web-auth** is enabled, you get to map the **default authentication-list** and global **parameter-map**. This is applicable for authentication-list and parameter-map that are not explicitly mentioned.
Step 5	**security web-auth parameter-map** *global* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Configure the global parameter map.
Step 6	**security web-auth authentication-list** *LWA-AUTHENTICATION* **Example:** `Device(config-wlan)# security web-auth authentication-list LWA-AUTHENTICATION`	Sets the authentication list for IEEE 802.1x.

Configure an AAA Server for Local Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **AAA Advanced** > **Global Config**.

Step 2 Choose the options from the **Local Authentication**, **Authentication Method List**, **Local Authorization** and **Authorization Method List** drop-down lists.

Step 3 Enable or Disable the **Radius Server Load Balance** using toggle button.

Step 4 Check the **Interim Update** check box.

Step 5 Click **Apply**.

Configure an AAA Server for Local Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**aaa authentication login** *LWA-AUTHENTICATION* **local** **Example:** `Device(config)#aaa authentication login lwa-authentication local`	Defines the authentication method at login.
Step 3	**aaa authorization network default local if-authenticated** **Example:** `Device(config)#aaa authorization network default local if-authenticated`	Sets the authorization method to local if the user has authenticated.

Global Configuration

Follow the procedure given below for global configuration:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**username** *name* **password 0** *clear-text-password* **Example:** `Device(config)# #username base password 0 pass1`	Sets the clear text password for the user.
Step 3	**ip http server** **Example:** `Device(config)#ip http server`	Enables the HTTP server.
Step 4	**ip http authentication local** **Example:** `Device(config)#ip http authentication local`	Sets the HTTP server authentication method to local. **Note** You will get the admin access rights regardless of the user privilege, if the **ip http authentication local** is disabled and username is the same as enable password.

Central Web Authentication

To configure CWA, follow these steps:

1. Configure a WLAN Profile for Guest Access with Central Web Authentication (CLI)
2. #unique_1626
3. AAA Server Configuration (CLI)
4. #unique_1628

Configure a WLAN Profile for Guest Access with Central Web Authentication (GUI)

Procedure

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

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.

Step 4 To enable the WLAN, set **Status** as **Enabled**.

Step 5 From the **Radio Policy** drop-down list, select the radio policy.

Step 6 To enable the **Broadcast SSID**, set the status as **Enabled**.

Step 7 Choose **Security** > **Layer2** tab. Uncheck the **WPA Policy**, **WPA2 Policy**, **AES** and **802.1x** check boxes.

Step 8 Check the **MAC Filtering** check box to enable the feature. With MAC Filtering enabled, choose the Authorization list from the **Authorization List** drop-down list.

Step 9 Click **Apply to Device**.

Configure a WLAN Profile for Guest Access with Central Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-id ssid-name* **Example:** `Device# Device(config)# wlan mywlan 38 mywlan-ssid1`	Configures the WLAN and SSID.
Step 3	**mac-filtering** *remote_authorization_list_name* **Example:** `Device(config-wlan)# mac-filtering auth-list`	Enables MAB authentication for the remote RADIUS server.
Step 4	**no security wpa** **Example:**	Disables WPA security.

	Command or Action	Purpose
	`Device(config-wlan)# no security wpa`	
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 7	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Saves the configuration.

AAA Server Configuration (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **Servers/Groups** > **RADIUS** > **Server Groups**.

Step 2 Click the RADIUS server group.

Step 3 From the **MAC-Delimiter** drop-down list, choose an option.

Step 4 From the **MAC-Filtering** drop-down list, choose an option.

Step 5 Enter the **Dead-Time (mins)**.

Step 6 From the **Available Servers** on the left, move the servers you need to **Assigned Servers** on the right.

Step 7 Click **Update & Apply to Device**.

Step 8 Choose **Configuration** > **Security** > **AAA** > **Servers/Groups** > **RADIUS** > **Servers**.

Step 9 Click the RADIUS server.

Step 10 Enter the **IPv4/IPv6 Server Address**, **Auth Port**, **Acct Port**, **Server Timeout (seconds)** and **Retry Count**.

Step 11 Check or uncheck the **PAC Key** checkbox and choose the Key Type from the **Key Type** drop-down list. Enter the **Key** and **Confirm Key**.

Step 12 Enable or disable the **Support for CoA** toggle button.

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

AAA Server Configuration (CLI)

Note Configure AAA server for Guest Foreign only.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa authorization network** *authorization-list* **local group** *Server-group-name* **Example:** `Device(config)#aaa authorization network cwa local group ise`	Sets the authorization method to local.
Step 3	**aaa group server radius** *server-group-name* **Example:** `Device(config)#aaa group server radius ise`	Configures RADIUS server group definition. **Note** *server-group-name* refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.
Step 4	**server name** *radius-server-name* **Example:** `Device(config-sg-radius)#server name ise1`	Configures the RADIUS server name.
Step 5	**subscriber mac-filtering security-mode mac** **Example:** `Device(config-sg-radius)#$mac-filtering security-mode mac`	Sets the MAC address as the password.
Step 6	**mac-delimiter colon** **Example:** `Device(config-sg-radius)#mac-delimiter colon`	Sets the MAC address delimiter to colon.
Step 7	**end** **Example:** `Device(config-sg-radius)#end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.
Step 8	**radius server** *name* **Example:** `Device(config)#radius server ISE1`	Sets the RADIUS server name

	Command or Action	Purpose
Step 9	**address ipv4** *radius-server-ipaddress* **auth-port** *port-number* **acct-port** *port-number* **Example:** `Device(config-radius-server)#address ipv4 209.165.201.1 auth-port 1635 acct-port 33`	Configures the RADIUS server IP address authentication and accounting ports.

Configuring 802.1x with Local Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-profile wlan-id ssid* **Example:** `Device(config)# wlan testwprofile 22 ssid-3`	Configures the WLAN and SSID.
Step 3	**security dot1x authentication-list** *default* **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Configures 802.1X for an WLAN.
Step 4	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for 802.1x security on the WLAN.
Step 5	**security web-auth parameter-map** *global* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Configures the global parameter map.
Step 6	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring Local Web Authentication with PSK Protocol

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-profile wlan-id ssid* **Example:** `Device(config)# wlan psksec-profile 22 ssid-4`	Configures the WLAN and SSID.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 4	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
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 psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Enables the security type as PSK.
Step 7	**security wpa psk set-key** {*ascii* | *hex*} *key* **Example:** `Device(config-wlan)# security wpa akm psk set-key asci 0`	Configures the PSK shared key.
Step 8	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables the web authentication for the WLAN.
Step 9	**security web-auth authentication-list** *default* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for the WLAN.

	Command or Action	Purpose
Step 10	**security web-auth parameter-map** *global* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Configure the global parameter map.

Central Web Authentication with PSK Protocol

To configure the CWA with PSK security protocol, follow the steps:

1. Configure WLAN Profile for Central Web Authentication with PSK Protocol
2. Applying Policy Profile on a WLAN

Configure WLAN Profile for Central Web Authentication with PSK Protocol

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-profile wlan-id ssid* **Example:** `Device(config)# wlan cwasec-profile 27 ssid-5`	Configures the WLAN and SSID.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 4	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
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 psk** **Example:** `Device(config-wlan)# security wpa psk`	Enables the security type as PSK.

	Command or Action	Purpose
Step 7	**security wpa psk set-key** {*ascii* | *hex*} *key* **Example:** `Device(config-wlan)# security wpa psk set-key asci 0`	Configures the PSK shared key.
Step 8	**mac-filtering** *authorization_list_name* **Example:** `Device(config-wlan)# mac-filtering cwa-list`	Enables MAC filtering for PSK web authentication.

Central Web Authentication with iPSK Protocol

To configure the CWA with iPSK security protocol, follow the steps:

1. Configure WLAN Profile for Central Web Authentication with iPSK Protocol

Configure WLAN Profile for Central Web Authentication with iPSK Protocol

Procedure

	Command or Action	Purpose
Step 1	**wlan** *guest-wlan-name wlan-id ssid* **Example:** `config# wlan ipsk-cwa-profile 28 ssid-6`	Configures guest WLAN.
Step 2	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for 802.1x.
Step 3	**security wpa akm psk set-key** {*ascii* | *hex*} *key* **Example:** `Device(config-wlan)# security wpa akm psk set-key asci 0`	Configures the PSK AKM shared key.
Step 4	**mac-filtering** *authorization_list_name* **Example:** `Device(config-wlan)# mac-filtering cwa-list`	Enables MAC filtering for iPSK authentication.

Configure Web Authentication on MAC Address Bypass failure (GUI)

Procedure

Step 1 Click **Configuration** > **Tags and Profiles** > **WLANs**.

Step 2 Click **Add** to add a new WLAN Profile or click the one you want to edit.

Step 3 In the **Edit WLAN** window, complete the following steps:

a) Choose **Security** > **Layer2** and check the **MAC Filtering** check box to enable MAC filtering.

b) From the **Authorization List** drop-down list, select a value.

c) Choose the **Layer3** tab.

d) Click **Show Advanced Settings** and check the **On MAC Filter Failure** checkbox.

Configure Web Authentication on MAC Address Bypass Failure (CLI)

You can configure authentication to fall back to web authentication, if a client cannot authenticate using MAC filter (Local or RADIUS), while trying to connect to a WLAN. To enable this feature, configure both MAC filtering and Web Authentication on the device. This can also avoid disassociations that happen only because of MAC filter authentication failure. To configure this feature, follow the procedure:

Configure a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy cwa`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Enables Central switching.
Step 4	Choose the first option to configure a Guest Foreign or second option to configure a Guest Anchor: • **mobility anchor** *anchor-ip-address* • **mobility anchor**	Configures Guest Foreign or Guest Anchor.

	Command or Action	Purpose

	Example:
	For Guests Foreign:
	`Device (config-wireless-policy)# mobility anchor 19.0.2.1`
	For Guest Anchor:
	`Device (config-wireless-policy)# mobility anchor`	

Step 5	**vlan** *name* **Example:** `Device(config-wireless-policy)# vlan 16`	Configures a VLAN name or VLAN ID. **Note** VLAN is optional for a Guest Foreign controller.
Step 6	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.

Configure a WLAN Profile

Procedure

	Command or Action	Purpose
Step 1	**wlan** *guest-wlan-name wlan-id ssid* **Example:** `config# wlan test-wlan-guest 10 wlan-ssid`	Configures guest WLAN.
Step 2	**mac-filtering** *mac-auth-listname* **authorization-override** *override-auth-listname* **Example:** `config-wlan# mac-filtering mac-auth-listname authorization-override`	Configures MAC filtering support on WLAN.
Step 3	**security web-auth** **Example:** `config-wlan# security web-auth`	Enables web authentication.
Step 4	**security web-auth on-macfilter-failure** **Example:** `config-wlan# security web-auth on-macfilter-failure`	Enables web authentication if MAC filter authentication fails.