



Wireless Guest Access

- [Wireless guest access, on page 1](#)
- [Load balancing among multiple guest controllers, on page 5](#)
- [Guidelines for wireless guest access, on page 5](#)
- [Configure mobility tunnel for guest access \(GUI\), on page 6](#)
- [Configure mobility tunnel for guest access \(CLI\), on page 6](#)
- [Configure guest access policy \(GUI\), on page 7](#)
- [Configure guest access policy \(CLI\), on page 8](#)
- [View guest access debug information \(CLI\), on page 10](#)
- [Verify wireless guest access enablement, on page 10](#)
- [Configure guest access using different security methods, on page 11](#)

Wireless guest access

Wireless guest access is a network security feature that

- provides internet access to guests in a secure and accountable manner
- uses the enterprise's existing wireless and wired infrastructure to the maximum extent, and
- reduces the cost and complexity of building a physical overlay network.

Wireless guest access architecture and components

The 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 these 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.

This table shows controller support for guest access functions.

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

Controller Name	Supported as Guest Anchor	Supported as Guest Foreign
Cisco Catalyst 9800 Embedded Wireless Controller on Cisco Catalyst 9100 Series APs	No	No

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

- 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

A foreign map is a guest access feature that

- supports guest access using Policy Profile and WLAN Profile configuration models in the controller
- is achieved with policy profile and WLAN profile config model, and
- configures two different WLAN profiles on two Guest Foreigns where seamless roaming is not allowed between them.

Foreign map configuration

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

Foreign map commands

- 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

Load balancing among multiple guest controllers is a network configuration feature that

- distributes large guest client volumes across up to 72 controllers for a single export foreign guest WLAN configuration
- supports priority-based anchor configuration with primary anchors (priority 1,3) and backup anchors for failure scenarios, and
- automatically handles failover by disconnecting clients from failed primary anchors and redirecting them to secondary anchors.

Configuration and failover behavior

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.

When the highest priority anchor goes down before the keep-alive timeout completes, the export anchor request for new clients fails, and Foreign selects the next highest priority Anchor in the list to export the clients.

Guidelines 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.

Recommendation: 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 these 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: Configure unicast RA depending on your platform.
- 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.

For 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
```

Configure mobility tunnel for guest access (GUI)

Enable secure guest network access by establishing a mobility tunnel that allows traffic to traverse between network segments while maintaining security policies.

Use this procedure when setting up guest network access that requires mobility tunneling to route guest traffic through designated mobility anchors in your wireless infrastructure.

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**.
-

The mobility tunnel for guest access is configured and the selected switch is designated as the mobility anchor for the wireless network.

Configure mobility tunnel for guest access (CLI)

Configure a mobility tunnel to enable guest access across mobility groups.

Follow the procedure given below to configure a mobility tunnel. This allows guest clients to roam between access points in different mobility groups while maintaining their network session.

Procedure

-
- Step 1** Configure a mobility group.

Example:

```
Device(config)# wireless mobility group name group-name
```

Example:

```
Device(config)# wireless mobility group name mtunnelgrp
```

Step 2 Configure a mobility MAC address.

Example:

```
Device(config)# wireless mobility mac-address mac-address
```

Example:

```
Device(config)# wireless mobility mac-address 0d:4c:da:3a:f2:21
```

Step 3 Configure a mobility peer.

Example:

```
Device(config)# wireless mobility group member mac-address 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
```

The mobility tunnel is now configured, allowing guest clients to seamlessly roam between controllers in the mobility group.

Configure guest access policy (GUI)

Configure guest access policies to manage how guest users connect to and use your wireless network.

Guest access policies define the network access parameters and security settings for temporary users who need network connectivity without full user credentials.

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**.

The guest access policy is configured and applied to the device, allowing guest users to access the network according to the defined parameters.

Configure guest access policy (CLI)

Create and configure a guest access profile policy to enable guest networking on wireless clients.

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

Step 1

Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2

Configure the policy profile and enter wireless profile configuration mode.

Example:

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

Example:

```
Device(config)# wireless profile policy guest-test-policy
```

Note

- You can use the **default-policy-profile** to configure the profile policy.

Step 3

Shut down the policy if it exists before configuring the anchor.

Example:

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

Step 4

(Optional) Enable central switching.

Example:

```
Device(config-wireless-policy)# central switching
```

Step 5

Configure Guest Foreign or Guest Anchor.

- Configure Guest Foreign with anchor IP address

- Configure Guest Anchor

Example:

For Guest Foreign:

```
Device(config-wireless-policy)# mobility anchor anchor-ip-address
```

For Guest Anchor:

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

Step 6 (Optional) Configure duration of idle timeout, in seconds.

Example:

```
Device (config-wireless-policy)# idle-timeout timeout
```

Example:

```
Device (config-wireless-policy)# idle-timeout 1000
```

Step 7 Configure VLAN name or VLAN ID.

Example:

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

Example:

```
Device(config-wireless-policy)# vlan 2
```

Note

VLAN is optional for a Guest Foreign controller.

Step 8 Enable policy profile.

Example:

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

Step 9 Exit the configuration mode and return to privileged EXEC mode.

Example:

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

Step 10 (Optional) Display the configured profiles.

Example:

```
Device# show wireless profile policy summary
```

Step 11 (Optional) Display detailed information of a policy profile.

Example:

```
Device# show wireless profile policy detailed policy-profile-name
```

Example:

```
Device# show wireless profile policy detailed guest-test-policy
```

The guest access policy is configured and enabled, allowing guest clients to connect using the specified mobility anchor and VLAN settings.

View guest access debug information (CLI)

View guest access debug information using commands.

- To display client level detailed information about mobility state and the anchor IP address, use this command:
show wireless client mac-add *mac-address* detail
- To display the client mobility statistics, use this command:
show wireless client mac-address *mac-address* mobility statistics
- To display client level roam history for an active client in sub-domain, use this command:
show wireless client mac-address *mac-address* mobility history
- To display detailed parameters of a given profile policy, use this command:
show wireless profile policy detailed *policy-name*
- To display the global level summary for all mobility messages, use this command:
show wireless mobility summary
- To display the statistics for the Mobility manager, use this command:
show wireless stats mobility

Verify wireless guest access enablement

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

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

-----
Vlan : 666
Learning Enabled : true
DHCPDN 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

These sections provide information about:

Open authentication

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

1. Configuring the WLAN Profile
2. [#unique_1731](#)



Note No tag is required unless AVC is enabled.

Configure a WLAN profile for guest access with open authentication (GUI)

Create a WLAN profile that allows guest users to connect to the wireless network without requiring authentication credentials, providing open access for temporary or visitor use.

Guest access with open authentication is commonly used in public areas, visitor networks, or temporary access scenarios where security requirements are minimal and ease of access is prioritized.

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**.
-

The WLAN profile is created and configured for guest access with open authentication. Guest users can now connect to the wireless network without providing authentication credentials.

Configure a WLAN profile for guest access with open authentication (CLI)

Establish a guest access WLAN that allows users to connect without authentication credentials.

Open authentication WLANs are commonly used for guest networks where ease of access is prioritized over security. This configuration removes all security barriers, making it suitable for public or temporary access scenarios.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN and SSID.

Example:

```
Device(config)# wlan profile-name wlan-id ssid-name
```

Example:

```
Device(config)# wlan mywlan 34 mywlan-ssid
```

Step 3 Disable WPA security.

Example:

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

Step 4 Disable security AKM for dot1x.

Example:

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

Step 5 Disable WPA2 security.

Example:

```
Device(config-wlan)# no security wpa wpa2
```

Step 6 Disable WPA2 ciphers for AES.

Example:

```
Device(config-wlan)# no security wpa wpa2 ciphers aes
```

Step 7 Save the configuration.

Example:

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

The WLAN profile is now configured with open authentication, allowing guest users to connect without any security credentials.

Configure a policy profile (CLI)

Create a policy profile that establishes WLAN connectivity rules and mobility configurations for wireless network access.

Policy profiles define how wireless clients connect to and interact with the network, including VLAN assignments, mobility settings, and switching behavior. Configure these profiles to control client access and network segmentation.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure WLAN policy profile and enter the wireless policy configuration mode.

Example:

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

Example:

```
Device(config)# wireless profile policy open_it
```

Step 3 Configure Guest Foreign or Guest Anchor. 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 anchor-ip-address
```

For Guest Anchor:

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

Step 4 Enable Central switching.

Example:

```
Device(config-wireless-policy)# central switching
```

Step 5 Configure a VLAN name or VLAN ID.

Example:

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

Example:

```
Device(config-wireless-policy)# vlan 16
```

Note

VLAN is optional for a Guest Foreign controller.

Step 6 Enable the policy profile.

Example:

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

The policy profile is now configured and enabled, ready to be applied to WLAN configurations for wireless client connectivity.

Local web authentication

To configure LWA, follow these steps:

1. [Configure the Parameter Map.](#)
2. [Configure the WLAN Profile.](#)
3. [Applying Policy Profile on a WLAN](#)
4. [Configure the AAA Server.](#)

Configure a parameter map (GUI)

Configure a parameter map to define web authentication settings including connection limits and timeout values.

Parameter maps are used to configure web authentication parameters that control how users authenticate through the web interface. This configuration is performed through the device's graphical user interface.

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**.
-

The parameter map is configured and applied to the device with the specified web authentication settings.

Configure a parameter map (CLI)

Define web authentication parameters and timeout settings to control client authentication behavior.

Parameter maps are used to configure global web authentication settings that control how clients authenticate and how long they remain in various authentication states.

Procedure

- Step 1** Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a parameter map and enter parameter-map WEBAUTH configuration mode.

Example:

```
Device(config)# parameter-map type webauth global
```

Step 3 Configure the WEBAUTH type parameter.

Example:

```
Device(config-params-parameter-map)# type webauth
```

Step 4 Configure the WEBAUTH timeout in seconds.

Example:

```
Device(config-params-parameter-map)# timeout init-state sec timeout-seconds
```

Example:

```
Device(config-params-parameter-map)# timeout init-state sec 3600
```

Valid range for time is from 60 to 3932100 seconds.

Step 5 Configure a virtual IP address.

Example:

```
Device(config-params-parameter-map)# virtual-ip ipv4 virtual-IP-address
```

Example:

```
Device(config-params-parameter-map)# virtual-ip ipv4 209.165.201.1
```

The parameter map is configured with web authentication settings, timeout values, and virtual IP address for client authentication.

Configure a WLAN profile for guest access with local web authentication (GUI)

Configure a WLAN profile to enable guest access with local web authentication, allowing temporary network access for visitors while maintaining security controls.

Use this procedure when you need to provide internet access to guests through a web-based authentication portal. This configuration enables controlled access for users who do not have permanent network credentials.

Follow these steps to configure a WLAN profile for guest access with local web authentication:

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**.

The WLAN profile is configured with local web authentication for guest access. Guest users connecting to this WLAN will be redirected to a web authentication portal where they can obtain network access.

Configure a WLAN profile for guest access with local web AUTHENTICATION (CLI)

This task configures a WLAN profile with local web AUTHENTICATION to provide secure guest access to the wireless network.

Local web AUTHENTICATION allows guest users to access the network through a web-based AUTHENTICATION portal. This configuration is typically used in guest access scenarios where users need to authenticate via a web interface before gaining network access.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN and SSID.

Example:

```
Device# Device(config)# wlan mywlan 38 mywlan-ssid1
```

Step 3 Enable web authentication for a WLAN.

Example:

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

Step 4 Configure the default parameter map.

Example:

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

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 Configure the global parameter map.

Example:

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

Step 6 Set the authentication list for IEEE 802.1x.

Example:

```
Device(config-wlan)# security web-auth authentication-list lwa-authentication
```

The WLAN profile is configured with local web AUTHENTICATION for guest access. Guest users will now be prompted to authenticate through a web interface when connecting to the wireless network.

Configure an AAA server for local web authentication (GUI)

This task allows you to set up AAA server configuration for local web authentication using the graphical user interface.

Use this procedure when you need to configure authentication and authorization settings for local web authentication through the device's web interface.

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**.
-

The AAA server configuration for local web authentication is now configured with your selected settings.

Configure an AAA server for local web authentication (CLI)

Configure Authentication, Authorization, and Accounting (AAA) server settings to enable local web authentication on the device.

Use this procedure when you need to set up local authentication and authorization for web-based user access on your device.

Procedure

- Step 1** Enter global configuration mode.
Example:

```
Device# configure terminal
```
 - 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.
-

The AAA server is configured for local web authentication. Users can now authenticate locally when accessing the device through web interface.

Configure global settings (CLI)

Establish basic global configuration settings for system access and HTTP server functionality.

Global configuration sets system-wide parameters that affect device operation and user access methods.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Set the clear text password for the user.

Example:

```
Device(config)# username name password 0 clear-text-password
```

Example:

```
Device(config)# username base password 0 pass1
```

Step 3 Enable the HTTP server.

Example:

```
Device(config)# ip http server
```

Step 4 Set the HTTP server authentication method to local.

Example:

```
Device(config)# ip http authentication 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.

Global configuration settings are now applied, enabling HTTP server access with local authentication and user password configuration.

Central web authentication

Configure WLAN profile for guest access with central web authentication (GUI)

Configure a WLAN profile that enables guest access using central web authentication to provide secure network access for guest users.

Guest access with central web authentication allows visitors to access the network through a web-based authentication portal while maintaining security controls through MAC filtering and authorization lists.

Before you begin

Follow these steps to configure a WLAN profile for guest access with central web authentication:

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**.
-

The WLAN profile is configured for guest access with central web authentication. The profile is now available for guest users to connect through the web authentication portal.

Configure a WLAN profile for guest access with central web authentication (CLI)

Set up a WLAN profile that allows guest users to access the network through central web authentication, providing controlled access while maintaining security.

Guest access with central web authentication is used when you need to provide network access to temporary users while maintaining control and security through web-based authentication portals.

Procedure

-
- Step 1** Enter global configuration mode.
Example:

```
Device# configure terminal
```
 - Step 2** Configure the WLAN and SSID.
Example:

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


Example:

```
Device(config)# wlan mywlan 38 mywlan-ssid1
```
 - Step 3** Enable MAB authentication for the remote RADIUS server.
Example:

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


Example:

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

Step 4 Disable WPA security.

Example:

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

Step 5 Disable security AKM for dot1x.

Example:

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

Step 6 Disable WPA2 security.

Example:

```
Device(config-wlan)# no security wpa wpa2
```

Step 7 Disable WPA2 ciphers for AES.

Example:

```
Device(config-wlan)# no security wpa wpa2 ciphers aes
```

Step 8 Save the configuration and activate the WLAN.

Example:

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

The WLAN profile is configured for guest access with central web authentication, allowing guest users to connect and authenticate through the web portal.

Configure AAA server (GUI)

Configure RADIUS server groups and individual RADIUS servers to enable AAA authentication for network access control and user authentication.

AAA (Authentication, Authorization, and Accounting) servers provide centralized authentication services for network devices. RADIUS servers must be properly configured with server groups to ensure reliable authentication services.

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**.

The RADIUS server groups and servers are configured and applied to the device. AAA authentication is now available using the configured RADIUS servers.

Configure AAA server (CLI)

Set up AAA server configuration to enable authentication and authorization for network access control.

Configure AAA server for Guest Foreign only. This configuration establishes RADIUS server groups and authorization methods for network access control.

Procedure

- Step 1** Enter global configuration mode.

Example:

```
Device# configure terminal
```

- Step 2** Set the authorization method to local.

Example:

```
Device(config)# aaa authorization network authorization-list local group server-group-name
```

Example:

```
Device(config)# aaa authorization network cwa local group ise
```

- Step 3** Configure RADIUS server group definition.

Example:

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

Example:

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

Note

server-group-name refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.

- Step 4** Configure the RADIUS server name.

Example:

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

Example:

```
Device(config-sg-radius)# server name ise1
```

- Step 5** Set the MAC address as the password.

Example:

```
Device(config-sg-radius)# subscriber mac-filtering security-mode mac
```

Step 6 Set the MAC address delimiter to colon.

Example:

```
Device(config-sg-radius)# mac-delimiter colon
```

Step 7 Save the configuration, exit configuration mode, and return to privileged EXEC mode.

Example:

```
Device(config-sg-radius)# end
```

Step 8 Set the RADIUS server name.

Example:

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

Example:

```
Device(config)# radius server ISE1
```

Step 9 Configure the RADIUS server IP address authentication and accounting ports.

Example:

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

The AAA server configuration is now complete with RADIUS server group settings, authentication methods, and MAC filtering parameters established for Guest Foreign access control.

Configure 802.1x with local web authentication

Configure dual authentication mechanism using 802.1x and local web authentication for comprehensive WLAN security.

This configuration combines 802.1x network access control with local web authentication, providing layered security for wireless clients. This is typically used when both network-level and user-level authentication are required.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN and SSID.

Example:

```
Device(config)# wlan wlan-profile wlan-id ssid
```

Example:

```
Device(config)# wlan testwprofile 22 ssid-3
```

Step 3 Configure 802.1X for the WLAN.

Example:

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

Example:

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

Step 4 Enable authentication list for web authentication security on the WLAN.

Example:

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

Example:

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

Step 5 Configure the global parameter map for web authentication.

Example:

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

Step 6 Enable the WLAN.

Example:

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

The WLAN is configured with both 802.1x and local web authentication, providing dual-layer security for wireless clients.

Configure local web authentication with PSK protocol (CLI)

Enable secure wireless network access using both PSK encryption and web-based authentication for enhanced security.

Local web authentication with PSK protocol combines pre-shared key security with web-based user authentication, providing a dual-layer security approach for wireless networks where traditional enterprise authentication methods are not required.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN and SSID.

Example:

```
Device(config)# wlan wlan-profile wlan-id ssid
```

Example:

```
Device(config)# wlan psksec-profile 22 ssid-4
```

Step 3 Disable WPA security.

Example:

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

Step 4 Disable WPA2 security.

Example:

```
Device(config-wlan)# no security wpa wpa2
```

Step 5 Disable security AKM for dot1x.

Example:

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

Step 6 Enable the security type as PSK.

Example:

```
Device(config-wlan)# security wpa akm psk
```

Step 7 Configure the PSK shared key.

Example:

```
Device(config-wlan)# security wpa akm psk set-key {ascii | hex} key
```

Example:

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

Step 8 Enable the web authentication for the WLAN.

Example:

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

Step 9 Enable authentication list for the WLAN.

Example:

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

Step 10 Configure the global parameter map.

Example:

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

The WLAN is now configured with local web authentication using PSK protocol, requiring users to authenticate through a web portal while maintaining PSK encryption for wireless traffic.

Central web authentication with PSK protocol

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

1. [Configure the WLAN Profile.](#)
2. [Applying Policy Profile on a WLAN](#)

Configure WLAN profile for central web authentication with PSK protocol (CLI)

Set up central web authentication with PSK to provide secure wireless access with web-based client authentication.

Central web authentication with PSK allows wireless clients to connect using a shared key and then authenticate through a web portal. This configuration is useful in guest networks or environments requiring web-based user authentication while maintaining PSK connectivity.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN and SSID.

Example:

```
Device(config)# wlan wlan-profile wlan-id ssid
```

Example:

```
Device(config)# wlan cwasec-profile 27 ssid-5
```

Step 3 Disable WPA security.

Example:

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

Step 4 Disable WPA2 security.

Example:

```
Device(config-wlan)# no security wpa wpa2
```

Step 5 Disable security AKM for dot1x.

Example:

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

Step 6 Enable the security type as PSK.

Example:

```
Device(config-wlan)# security wpa psk
```

Step 7 Configure the PSK shared key.

Example:

```
Device(config-wlan)# security wpa psk set-key {ascii | hex} key
```

Example:

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

Step 8 Enable MAC filtering for PSK web authentication.

Example:

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

Example:

```
Device(config-wlan)# mac-filtering cwa-list
```

The WLAN profile is configured for central web authentication with PSK protocol, allowing clients to connect using the shared key and authenticate via web portal.

Central web authentication with iPSK protocol

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

1. [Configure the WLAN Profile.](#)

Configure WLAN profile for central web authentication with iPSK protocol

This task configures a WLAN profile that enables central web authentication with iPSK (Identity Pre-Shared Key) protocol, providing secure guest access while maintaining centralized authentication control.

Use this configuration when you need to provide guest wireless access with pre-shared key authentication combined with central web authentication. This approach allows for individualized keys per device while maintaining centralized authentication oversight.

Procedure

Step 1 Configure guest WLAN.

Example:

```
config# wlan guest-wlan-name wlan-id ssid
config# wlan ipsk-cwa-profile 28 ssid-6
```

Step 2 Disable security AKM for 802.1x.

Example:

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

Step 3 Configure the PSK AKM shared key.

Example:

```
Device(config-wlan)# security wpa akm psk set-key {ascii | hex} key
Device(config-wlan)# security wpa akm psk set-key ascii 0
```

Step 4 Enable MAC filtering for iPSK authentication.

Example:

```
Device(config-wlan)# mac-filtering authorization_list_name
Device(config-wlan)# mac-filtering cwa-list
```

The WLAN profile is configured for central web authentication with iPSK protocol. Guest devices can now connect using pre-shared keys while being subject to centralized web authentication control and MAC filtering.

Configure web authentication on MAC address bypass failure (GUI)

This task configures Web Authentication to handle situations where MAC address filtering fails, providing an alternative authentication method for network access.

When MAC filtering is enabled but a device's MAC address is not in the authorization list, you can configure the system to fall back to Web Authentication instead of denying access completely.

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:
- Choose **Security > Layer2** and check the **MAC Filtering** check box to enable MAC filtering.
 - From the **Authorization List** drop-down list, select a value.
 - Choose the **Layer3** tab.
 - Click **Show Advanced Settings** and check the **On MAC Filter Failure** checkbox.

Web Authentication is now configured to activate when MAC address filtering fails, allowing devices not on the authorization list to authenticate through the web interface.

Configure web authentication on MAC address bypass failure (CLI)

Enable web authentication fallback when MAC filter authentication fails to avoid client disassociations due to MAC filter authentication failures.

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.

Procedure

-
- Step 1** Enter global configuration mode.
- Example:**
- ```
Device# configure terminal
```
- Step 2** Configure WLAN policy profile and enter the wireless policy configuration mode.
- Example:**
- ```
Device(config)# wireless profile policy policy-name
```
- Example:**

```
Device(config)# wireless profile policy cwa
```

Step 3 Enable Central switching.

Example:

```
Device(config-wireless-policy)# central switching
```

Step 4 Configure Guest Foreign or Guest Anchor.

- mobility anchor *anchor-ip-address*
- mobility anchor

Example:

For Guests Foreign:

```
Device (config-wireless-policy)# mobility anchor anchor-ip-address
```

For Guest Anchor:

```
Device (config-wireless-policy)# mobility anchor
```

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 Configure a VLAN name or VLAN ID.

Example:

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

Example:

```
Device(config-wireless-policy)# vlan 16
```

Note

VLAN is optional for a Guest Foreign controller.

Step 6 Enable the policy profile.

Example:

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

Step 7 Configure guest WLAN.

Example:

```
config# wlan guest-wlan-name wlan-id ssid
```

Example:

```
config# wlan test-wlan-guest 10 wlan-ssid
```

Step 8 Configure MAC filtering support on WLAN.

Example:

```
config-wlan# mac-filtering mac-auth-listname authorization-override
```

Step 9 Enable web authentication.

Example:

```
config-wlan# security web-auth
```

Step 10

Enable web authentication if MAC filter authentication fails.

Example:

```
config-wlan# security web-auth on-macfilter-failure
```

Web authentication fallback is now configured for MAC filter authentication failures, preventing client disconnections when MAC authentication fails.

