Lobby Ambassador Account

Information About Lobby Ambassador Account

A global administrator can create a lobby ambassador (lobby admin) user for creating guest users.

While creating a guest user, a lobby ambassador can create and delete a guest user, besides setting the following parameters for a guest user:

- Password
- Lifetime of the guest user
- Guest role profiles (Quality-of-Service profiles that should be applied on a guest using the AAA attribute list.

You must ensure that the RADIUS server must be configured with Cisco-AV-pair privilege level with a value greater than zero.

Note You can create a lobby admin from a RADIUS or TACACS server, instead of creating one locally.

Only the admin can create WLAN and web authentication policies. The admin can also create an AAA attribute list, which the lobby admin can use to map to the corresponding guest user.

After an upgrade to Cisco Catalyst 9800 Controller Software release 17.2.x , you must clear the browser cache data to view the lobby admin GUI correctly.

Creating a Lobby Ambassador User Account (GUI)

You can configure administrator or lobby ambassador usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information.

Creating a User Account

Procedure

Step 1 From the home page, choose **Administration** > **User Administration**.

Step 2 Click **Add**.

Step 3 In the **User Name** field, enter a user name for the new account.

Step 4 From the **Policy** drop-down list, choose the policy that you want to associate with the user.

Step 5 From the **Privilege** drop-down list, choose the privilege level that you want to associate with the user by clicking the user privilege icon. The following are the options:

- **Go to Basic Mode**
- **Go to Advanced Mode**

Go to Basic Mode: This privilege level defines the commands that users can enter using the CLI after they have logged into the device. Privilege 1 allows access in user EXEC mode and privilege 15 allows access in Privileged EXEC mode.

Go to Advanced Mode:

Admin: Users with Privilege 15 can execute all the **show**, **config**, and **exec** commands on the device. These users will have access to all the sections of the GUI.

Read Only: Users with Privileges 1 to 14 are considered read-only users. The default privilege is 1 if a user is created using the GUI. These users will have access only to the Dashboard and the Monitoring sections.

No Access: Users with Privilege 0 can log in to the device through Telnet or SSH and access the CLI. However, they cannot access the GUI.

Lobby Admin: Users who can create only guest user accounts. While creating a guest user, a lobby ambassador can create and delete a guest user, besides setting the following parameters for a guest user:

- Password
- Lifetime of the guest user
- Guest role profiles (quality-of-service) profiles that should be applied on a guest using the AAA attribute list.

Step 6 In the **Password** field, enter a password for the new account.

Step 7 In the **Confirm Password** field, enter the same password again to reconfirm.

Step 8 Click **Apply to Device**.

Logging In Using the Lobby Account

Note Execute the following commands before logging in using the lobby credentials:

aaa new-model

aaa authorization exec default local

ip http authentication aaa

Logout from the Administrator account and login using the lobby credentials.

You get to view the **Guest User** page.

Creating a Lobby Ambassador Account (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**user-name** *user-name* **Example:** `Device(config)# user-name example-user`	Creates a user account.
Step 3	**type lobby-admin** **Example:** `Device(config-user-name)# type lobby-admin`	Specifies the account type as lobby admin.
Step 4	**password 0** *password* **Example:** `Device(config-user-name)# password 0 example-password`	Creates a password for the lobby administrator account.
Step 5	**aaa attribute list** *user-name* **Example:** `Device(config-user-name)# aaa attribute list example-user`	Creates attribute list for lobby admin access.
Step 6	**attribute type** *wlan-profile-name* **Example:** `Device(config-user-name)# attribute type wlan_wl_mab`	Creates attribute type for lobby admin access.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Device(config-user-name)# exit`	Returns to global configuration mode.

Configuring WLAN (GUI)

Before you begin

You need to enable MAC filtering for Layer 2 authentication to download the redirect URL and ACL.

Procedure

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

Step 2 In the **WLANs** window, click the name of the **WLAN** or click **Add** to create a new one.

Step 3 In the **Add/Edit WLAN** window that is displayed, click the **General** tab to configure the following parameters.

- In the **Profile Name** field, enter or edit the name of the profile.
- In the **SSID** field, enter or edit the SSID name.

  The SSID name can be alphanumeric, and up to 32 characters in length.
- In the **WLAN ID** field, enter or edit the ID number. The valid range is between 1 and 512.
- From the **Radio Policy** drop-down list, choose the **802.11** radio band.
- Using the **Broadcast SSID** toggle button, change the status to either **Enabled** or **Disabled** .
- Using the **Status** toggle button, change the status to either **Enabled** or **Disabled** .

Step 4 Click the **Security** tab, and then **Layer 2** tab to configure the following parameters:

- From the **Layer 2 Security Mode** drop-down list, choose **None**. .This setting disables Layer 2 security.
- Enter the **Reassociation Timeout** value, in seconds. This is the time after which a fast transition reassociation times out.
- Check the **Over the DS** check box to enable Fast Transition over a distributed system.
- Choose OWE, Opportunistic Wireless Encryption (OWE) provides data confidentiality with encryption over the air between an AP radio and a wireless client. OWE Transition Mode is meant to provide a sort of backwards compatibility.
- Choose Fast Transition, 802.11r which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with a new AP is done even before the corresponding client roams to the target access point. This concept is called Fast Transition.
- Check the check box to enable MAC filtering in the WLAN.
- Check the **Lobby Admin Access** check box to enable Lobby Admin access.

Step 5 Click **Save & Apply to Device**.

Client Allowed List

Clients in universities and hotels need access to networks for a limited period of time. These locations also receive many guests with multiple devices. Therefore it becomes important to protect the networks from misuse or unauthorized access, and allow legitimate clients to connect to the corresponding network.

The client listing feature addresses the need of creating an allowed list for clients on a particular WLAN or SSID- based MAC address.

When you create a new client MAC address as an allowed list user with an invalid WLAN profile name, you must be careful while you map the client MAC to the WLAN profile.

Client allowed list is supported only with MAC addresses that are without a delimiter format.

Two types of administrator roles defined are:

- Global Administrator: Creates a lobby admin user on the controller and enables the lobby administrators access each to the WLAN.
- Lobby Administrator: Adds or deletes a client from the allowed list to manage the association to a WLAN or SSID through the GUI only. Existing lobby administrators can also be used to configure the allowed list.

Restrictions for Client Allowed List

A lobby admin can add clients to allowed list only through the graphical user interface (GUI) and not through the command-line interface (CLI).

Creating a Client Allowed List (GUI)

This section provides multiple methods that you can use as a lobby administrator to create an allowed list for valid users for a WLAN.

Adding Single MAC Address to Allowed List

Procedure

Step 1 Log into Lobby Admin portal.

Step 2 Click **Whitelist Users**.

Step 3 From the drop-down list, choose **WLAN**.

Step 4 Click **Add New Whitelist User**.

Step 5 Select **By MAC Address** radio button.

Step 6 Enter the **MAC address** and **Description**.

Step 7 Click **Apply to Device**.

Adding Bulk MAC Address to Allowed List

Procedure

Step 1 Log into Lobby Admin portal.

Step 2 Click **Whitelist Users**.

Step 3 From the drop-down list, choose the WLAN.

Step 4 Click **Add New Whitelist User**.

Step 5 Select **Bulk Import** radio button.

Step 6 Select the CSV file that lists the clients in MAC Address, Description format.

Step 7 Click **Apply to Device**.

Managing Guest Users

Procedure

Step 1 Log in to Lobby Admin portal using the lobby admin credentials.

Step 2 Click **Whitelist Users**.

Step 3 From the **WLAN**drop-down list, choose the corresponding**WLAN**.

Step 4 From the **WLAN Mode**, select **Onboarding** to enable clients to access the network.

Step 5 Click **Apply.**

Step 6 From the **Connected/Not Whitelisted** in the Whitelist window, select a MAC address . Once the clients join the controller, the MAC addresses are listed in the **Connected/Not Whitelisted**. In the Onboarding mode, MAC filtering in the selected WLAN is disabled. In such a scenario you can change the mode using **Secure** mode.

Step 7 Select **Secure** to automatically add the clients that are connected to the allowed list. In the secure mode, MAC filtering in the selected WLAN is enabled.

Step 8 Click **Apply to Device**.

The clients are listed in the **Connected/Whitelisted**.

Viewing a Client Allowed List

Procedure

Step 1 Log in to the Lobby Admin portal.

Step 2 Click **Whitelist Users**.

Step 3 From the **WLAN**drop-down list, choose the corresponding **WLAN** .

The window lists the following information:

- **Connected/Whitelisted**: Lists the clients that are connected and added to the allowed list by the Lobby admin.
- **Connected/Not Whitelisted**: Lists the clients that are connected, but not added to the allowed list by the Lobby admin.
- **Not Connected/Whitelisted**: Listed the clients that are not connected but added to the allowed list.