Lobby Ambassador Account

Lobby ambassador account

A lobby ambassador account is a user account that

- allows designated personnel (lobby ambassadors) to create and delete guest users on the network
- allows lobby ambassadors to assign guest user parameters such as password, life span, and role profile, and
- restricts lobby ambassadors from creating WLAN or web authentication policies.

Feature history

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature history for lobby ambassador account

Feature Name	Release Information	Feature Description
Lobby ambassador account	Cisco IOS XE Dublin 17.2.x	From Cisco IOS XE Cupertino 17.2.x onwards, lobby administrators can add or delete a client from the allowed list to manage the association with a WLAN or SSID.

As a global administrator, you create a lobby ambassador user to manage guest accounts.

Configure the RADIUS server with the Cisco-AV-pair privilege level set greater than zero to enable lobby ambassador functionality.

Note An administrator can create lobby ambassador accounts remotely using a RADIUS or TACACS server, or locally.

Only the administrator can create WLAN policies, web authentication policies, and AAA attribute lists. Lobby ambassadors use these attribute lists to map guest users to role profiles, including Quality-of-Service profiles.

After upgrading to Cisco Catalyst 9800 Controller software release 17.2.x, clear the browser cache to correctly view the lobby admin GUI.

Create a lobby ambassador user account

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

Create a user account (GUI)

Add a new user account to the system.

Procedure

Step 1 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 Select the policy that you want to associate with the user from the **Policy** drop-down list.

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

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

Go to Basic Mode: This privilege level defines the commands that users enter using the CLI after they have logged into the device. Privilege one 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 GUI sections.

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

No Access: Users with Privilege zero can log in to the device through Telnet or SSH to access the CLI, but cannot access the GUI.

Lobby Admin: Users who can create only guest user accounts. Lobby ambassadors can create and delete guest users and set parameters such as:

- 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 confirm again.

Step 8 Click **Apply to Device**.

Log in using the lobby account (CLI)

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

Procedure

Step 1 Enable NEW access control commands and functions.

Example:

```
aaa new-model
```

Step 2 Enter the local database.

Example:

```
aaa authorization exec default local
```

Step 3 Set HTTP server authentication method and use AAA access control methods.

Example:

```
ip http authentication aaa
```

Log out from the administrator account. Then, log in using the lobby credentials. After logging in, the **Guest User** page appears.

Create a lobby ambassador account (CLI)

Add a new lobby ambassador (guest network administrator) to the system using CLI commands.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a user account.

Example:

```
Device(config)# user-name user-name example-user
```

Step 3 Specify the account type as lobby admin.

Example:

```
Device(config-user-name)# type lobby-admin
```

Step 4 Create a password for the lobby administrator account.

Example:

```
Device(config-user-name)# password 0 password example-password
```

Step 5 Create an attribute list for lobby admin access.

Example:

```
Device(config-user-name)# aaa attribute list user-name example-user
```

Step 6 Create an attribute type for lobby admin access.

Example:

```
Device(config-user-name)# attribute type wlan-profile-name wlan_wl_mab
```

Step 7 Return to the global configuration mode.

Example:

```
Device(config-user-name)# exit
```

Configure WLAN (GUI)

Set up a new WLAN on your wireless controller using the GUI.

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. The **Add/Edit WLAN** window is displayed.

Step 3 In the **Add/Edit WLAN** window, click the **General** tab to configure these 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 is alphanumeric and can be up to 32 characters in length.
- In the **WLAN ID** field, enter or edit the ID number. The valid range is between one and 512.
- Select the **802.11** radio band from the **Radio Policy** drop-down list.
- 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 select the **Layer 2** tab to configure these parameters:

- Select **None** from the **Layer 2 Security Mode** drop-down list. This setting disables Layer 2 security.
- Enter the **Reassociation Timeout** value, in seconds. This value specifies the duration before 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 ensures backwards compatibility.
- Choose Fast Transition (802.11r), the IEEE standard for fast roaming. This standard allows the initial handshake with a new AP to occur before the client roams to the target AP. This method is known as 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

A client allowed list is a WLAN security feature that

- enables creation of an allowed list for clients on a particular WLAN or SSID-based MAC address, and
- is supported only with MAC addresses that do not include delimiters.

If you create a new client MAC address as an allowed list user with an invalid WLAN profile name, map the client MAC address to the WLAN profile carefully.

If you are a client in a university or hotel, you may need network access for a limited time. Many guests bring multiple devices. Protect networks from misuse or unauthorized access and allow legitimate clients to connect.

There are two types of administrator roles:

- Global Administrator: Creates a lobby admin user on the controller and enables each lobby administrator to access the WLAN.

- Lobby Administrator: Adds or deletes clients from the allowed list using the GUI to manage association to a WLAN or SSID. Existing lobby administrators can also configure the allowed list.

Restrictions for client allowed list

A lobby admin can add clients to the allowed list only through the GUI, not through the CLI.

Creating a client allowed list (GUI)

As a lobby administrator, you can use several methods to create an allowed list for valid WLAN users.

Adding single MAC address to allowed list

Import a specific MAC address into your WLAN whitelist efficiently using the admin portal.

Procedure

Step 1 Log in to the Lobby Admin portal.
Step 2 Click **Whitelist Users**.
Step 3 Select **WLAN** from the drop-down list.
Step 4 Click **Add New Whitelist User**.
Step 5 Click **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

Import multiple MAC addresses into your WLAN whitelist efficiently using the admin portal.

Procedure

Step 1 Log in to the Lobby Admin portal.
Step 2 Click **Whitelist Users**.
Step 3 Select the WLAN from the drop-down list.
Step 4 Click **Add New Whitelist User**.
Step 5 Click **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**.

Manage guest users (GUI)

Add and manage guest user access through the controller GUI.

Procedure

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

Step 2 Click **Whitelist Users**.

Step 3 Select the corresponding **WLAN** from the **WLAN** drop-down list.

Step 4 Select **Onboarding** from the **WLAN Mode** to enable clients to access the network.

Step 5 Click **Apply**.

Step 6 Select a MAC address from the **Connected/Not Whitelisted** in the Whitelist window. 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, 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**.

View a client allowed list

See which clients are connected or whitelisted on a WLAN.

Procedure

Step 1 Log in to the Lobby Admin portal.

Step 2 Click **Whitelist Users**.

Step 3 Select the corresponding **WLAN** from the **WLAN** drop-down list.

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**: Lists the clients that are not connected, but added to the allowed list.