



MAC Filtering for Lobby Ambassadors

- [Introduction](#) 2
- [Pre-requisite](#) 2
- [Components Used](#) 2
- [Conventions](#) 2
- [Feature Introduction](#) 2
- [Implementation](#) 2
- [Work Flow for Administrative Privileges and Lobby Admin Role](#) 2
- [Configuring Global Admin and Lobby Admin User using GUI](#) 3
- [Configuring Global Admin and Lobby Admin User using CLI](#) 6

Introduction

This document introduces MAC Filtering for Lobby Ambassadors feature and provides general guidelines for its deployment. The purpose of this document is to:

- Provide an overview of MAC Filtering for Lobby Ambassadors feature
- Highlight supported Key Features
- Provide details on deploying and managing MAC Filtering for Lobby Ambassadors on WLC

Pre-requisite

Beta customers must have AireOS 8.0 or higher release on a Wireless LAN Controller in order to upgrade to the 8.4 code.

Components Used

The information in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Feature Introduction

The MAC Filtering feature for Lobby Ambassadors is designed for guest user management for having clients in the allowed list on the Wireless LAN Controller.

Implementation

This feature allows for clients to be put in an allowed list on a particular WLAN/SSID. The end goal is to have control on which of the clients can access a particular WLAN. This feature uses the currently existing features - MAC filtering option on WLAN, adding lobby admin user and re-using AAA database to store the list of allowed clients on a WLAN.

Work Flow for Administrative Privileges and Lobby Admin Role

Sequence of using this feature is as under:

1. Global Admin adds a lobby admin user account on the WLC
2. Global Admin enables lobby-admin-access on required WLANs on the WLC
3. Lobby admin logs into the guest management page on the WLC
4. Lobby admin selects the WLAN (for which lobby admin access is enabled) on which client whitelisting needs to be enabled

5. Lobby admin disables mac filtering on the WLAN
6. Lobby-admin will be shown a list of current connected clients as well as those already added clients (in the allowed list) for the selected WLAN
7. Lobby-admin selects all or selected clients from the associated client list based of available filtering options
8. Lobby-admin adds the required or all clients to the client allowed-list bucket
9. Lobby admin will enable mac filtering on the WLAN

The roles of read-write admin and lobby admin are broken down in the following order:

User with Administrative Privileges

- Administrator user with read-write access will create a local admin (lobby-admin) on the WLC
- The read-write administrator will also need to set admin lobby access on selected WLAN’s that will allow client whitelisting

User Lobby Admin Role

- Login to the Guest user web page of the WLC
- View a list of WLAN/SSIDs that have lobby-admin access enabled along with a list of all clients connected to the WLAN/SSID
- Privilege access to enable mac-filtering option on a selected WLAN
- Privilege access to add/Delete client mac addresses to the allowed list

Configuring Global Admin and Lobby Admin User using GUI

Configuring Global Admin User using GUI

To configure global admin user using GUI, perform the following steps:

Procedure

Step 1 Add local lobby-admin to WLC under **Management > Local Management Users**.



Local Management Users

Services Entries 1 - 12 of 12

| User Name | User Access Mode | Telnet Capable |
|-----------|------------------|-------------------------------------|
| admin | ReadWrite | <input checked="" type="checkbox"/> |
| cisco1 | ReadWrite | <input checked="" type="checkbox"/> |
| cisco10 | ReadWrite | <input checked="" type="checkbox"/> |
| cisco2 | ReadWrite | <input checked="" type="checkbox"/> |
| cisco3 | ReadWrite | <input checked="" type="checkbox"/> |
| cisco4 | ReadWrite | <input checked="" type="checkbox"/> |
| cisco5 | ReadWrite | <input checked="" type="checkbox"/> |
| cisco6 | ReadWrite | <input checked="" type="checkbox"/> |
| cisco7 | ReadWrite | <input checked="" type="checkbox"/> |
| cisco8 | ReadWrite | <input checked="" type="checkbox"/> |
| cisco9 | ReadWrite | <input checked="" type="checkbox"/> |
| lobby | LobbyAdmin | <input checked="" type="checkbox"/> |

Step 2 Enable lobby-admin access on WLAN by going to **WLANS > WLAN > Advanced**.

WLANS > Edit 'pod2'

General **Security** **QoS** **Policy-Mapping** **Advanced**

PMF

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption AES TKIP

OSEN Policy

Authentication Key Management [19](#)

802.1X Enable

CCKM Enable

PSK Enable

FT 802.1X Enable

FT PSK Enable

WPA gtk-randomize State [14](#)

Lobby Admin Configuration

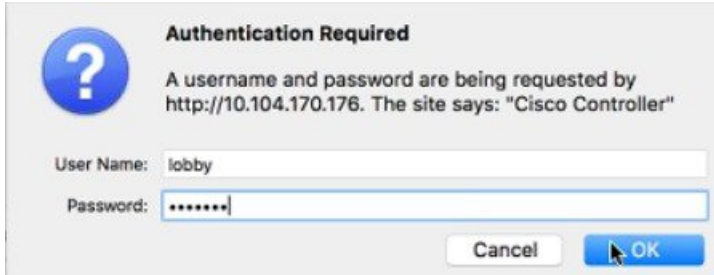
Lobby Admin Access

Configuring Lobby Admin User using GUI

To configure lobby admin user, perform the following steps:

Procedure

Step 1 Login to guest management page of WLC using Lobby admin username, password.



Authentication Required
A username and password are being requested by http://10.104.170.176. The site says: "Cisco Controller"

User Name: lobby
Password: [masked]

Cancel OK



Lobby Ambassador Guest Management

Guest Management

- Guest Users List
- White List Users

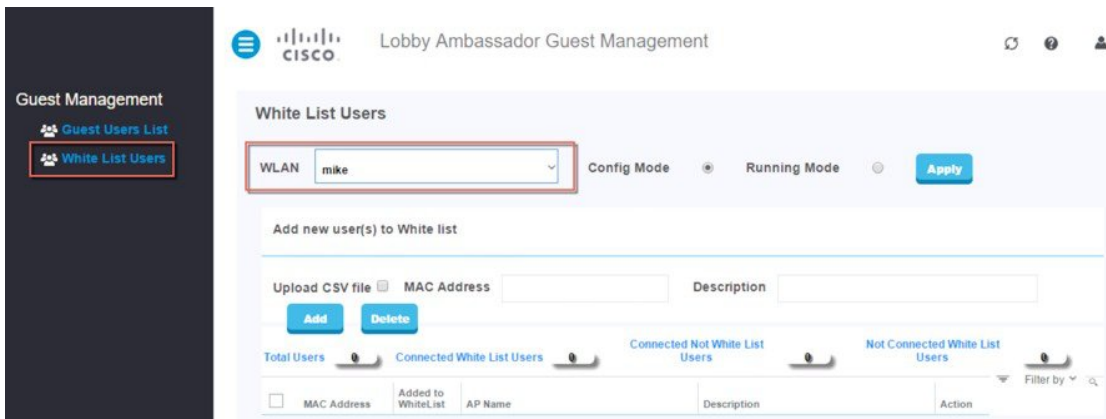
Guest Users List

New...

Items 0 to 0 of 0

| User Name | WLAN SSID | Account Remaining Time | Description |
|-----------|-----------|------------------------|-------------|
|-----------|-----------|------------------------|-------------|

Step 2 View WLAN list (that have lobby-admin access enabled) along with presently associated clients on a WLAN. Note the two modes next to WLAN.



Lobby Ambassador Guest Management

White List Users

WLAN: mike Config Mode Running Mode Apply

Add new user(s) to White list

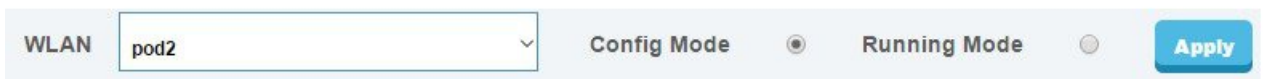
Upload CSV file MAC Address Description

Add Delete

Total Users Connected White List Users Connected Not White List Users Not Connected White List Users

| MAC Address | Added to WhiteList | AP Name | Description | Action |
|-------------|--------------------|---------|-------------|--------|
|-------------|--------------------|---------|-------------|--------|

Change the Mode to Config to disable Mac Filtering on WLAN.



WLAN: pod2 Config Mode Running Mode Apply

Allow selected users based on available Filter options.



Filter Options Clear Filter

MAC Address aa
 AP Name
 Description
 Not White List Users
 White List Users

Change to Running Mode to enable mac filtering on WLAN.

White List Users

WLAN Config Mode Running Mode

Add new user(s) to White list

MAC Address Description

Total Users **1** Connected White List Users **0** Connected Not White List Users **0** Not Connected White List Users **1** Filter by

| <input type="checkbox"/> | MAC Address | Added to WhiteList | AP Name | Description | Action |
|--------------------------|-------------------|--------------------|---------|-------------|--------|
| <input type="checkbox"/> | aa:bb:cc:aa:dd:01 | Yes | | batch_2016 | X |

Configuring Global Admin and Lobby Admin User using CLI

Configuring Global Admin User using CLI

To configure global admin user using CLI, perform the following steps:

1. Configuring Lobby Admin User using GUI

```
>config mgmtuser add <username> <password> lobby-admin <description>
```

2. Enable lobby-admin access on WLAN

```
>config wlan lobby-admin-access <enable/disable> <wlan-id>
```

Configuring Lobby Admin User using CLI

1. View WLAN list (that have lobby-admin access) with presently associated clients

```
>show wlan lobby-admin-access summary
```

```
>show client wlan <wlan id>
```

```
>show client whitelist <wlan-id>
```

2. Add/Delete all or selected clients to the allowed list group

```
>config mac-filter add <mac-address> <wlan-id> <interface><description>
```

```
>config mac-filter delete <mac-addr>
```

3. View mac-filter list per WLAN

```
>show mac-filter summary (for all wlans)
```

```
>show mac-filter wlan <wlan-id>
```

4. Enable mac-filtering on WLAN

```
>config wlan mac-filtering <enable/disable> <wlan-id>
```



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the
Cisco Website at www.cisco.com/go/offices.

© 2020 Cisco and/or its affiliates. All rights reserved.