



Managing User Accounts

- [Configuring Guest User Accounts, page 1](#)
- [Configuring Administrator Usernames and Passwords, page 4](#)
- [Changing the Default Values for SNMP v3 Users, page 6](#)

Configuring Guest User Accounts

Information About Creating Guest Accounts

The controller can provide guest user access on WLANs. The first step in creating guest user accounts is to create a lobby administrator user, also known as a lobby ambassador account. Once this account has been created, a lobby ambassador can create and manage guest user accounts on the controller. The lobby ambassador has limited configuration privileges and access only to the web pages used to manage the guest accounts.

The lobby ambassador can specify the amount of time that the guest user accounts remain active. After the specified time elapses, the guest user accounts expire automatically.

Guidelines and Limitations

The local user database is limited to a maximum of 2048 entries, which is also the default value. This database is shared by local management users (including lobby ambassadors), local network users (including guest users), MAC filter entries, exclusion list entries, and access point authorization list entries. Together they cannot exceed the configured maximum value.

Creating a Lobby Ambassador Account

Creating a Lobby Ambassador Account (GUI)

Step 1 Choose **Management > Local Management Users** to open the Local Management Users page.

This page lists the names and access privileges of the local management users.

Note If you want to delete any of the user accounts from the controller, hover your cursor over the blue drop-down arrow and choose **Remove**. However, deleting the default administrative user prohibits both GUI and CLI access to the controller. Therefore, you must create a user with administrative privileges (ReadWrite) before you remove the default user.

Step 2 Click **New** to create a lobby ambassador account. The Local Management Users > New page appears.

Step 3 In the User Name text box, enter a username for the lobby ambassador account.

Note Management usernames must be unique because they are stored in a single database.

Step 4 In the **Password** and **Confirm Password** text boxes, enter a password for the lobby ambassador account.

Note Passwords are case sensitive. The settings for the management User Details parameters depends on the settings that you make in the Password Policy page. The following requirements are enforced on the password

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain a management username or the reverse letters of a username.
- The password should not contain words like Cisco, oscic, admin, nimda, or any variant obtained by changing the capitalization of letters by substituting l, |, or ! or substituting 0 for o or substituting \$ for s.

Step 5 Choose **LobbyAdmin** from the User Access Mode drop-down list. This option enables the lobby ambassador to create guest user accounts.

Note The ReadOnly option creates an account with read-only privileges, and the ReadWrite option creates an administrative account with both read and write privileges.

Step 6 Click **Apply** to commit your changes. The new lobby ambassador account appears in the list of local management users.

Step 7 Click **Save Configuration** to save your changes.

Creating a Lobby Ambassador Account (CLI)

To create a lobby ambassador account use the following command:

```
config mgmtuser add lobbyadmin_username lobbyadmin_pwd lobby-admin
```



Note Replacing **lobby-admin** with **read-only** creates an account with read-only privileges. Replacing **lobby-admin** with **read-write** creates an administrative account with both read and write privileges.

Creating Guest User Accounts as a Lobby Ambassador (GUI)

-
- Step 1** Log into the controller as the lobby ambassador, using the username and password. The Lobby Ambassador Guest Management > Guest Users List page appears.
- Step 2** Click **New** to create a guest user account. The Lobby Ambassador Guest Management > Guest Users List > New page appears.
- Step 3** In the User Name text box, enter a name for the guest user. You can enter up to 24 characters.
- Step 4** Perform one of the following:
- If you want to generate an automatic password for this guest user, select the **Generate Password** check box. The generated password is entered automatically in the Password and Confirm Password text boxes.
 - If you want to create a password for this guest user, leave the **Generate Password** check box unselected and enter a password in both the **Password** and **Confirm Password** text boxes.
- Note** Passwords can contain up to 24 characters and are case sensitive.
- Step 5** From the Lifetime drop-down lists, choose the amount of time (in days, hours, minutes, and seconds) that this guest user account is to remain active. A value of zero (0) for all four text boxes creates a permanent account.
Default: 1 day
Range: 5 minutes to 30 days
- Note** The smaller of this value or the session timeout for the guest WLAN, which is the WLAN on which the guest account is created, takes precedence. For example, if a WLAN session timeout is due to expire in 30 minutes but the guest account lifetime has 10 minutes remaining, the account is deleted in 10 minutes upon guest account expiry. Similarly, if the WLAN session timeout expires before the guest account lifetime, the client experiences a recurring session timeout that requires reauthentication.
- Note** You can change a guest user account with a nonzero lifetime to another lifetime value at any time while the account is active. However, to make a guest user account permanent using the controller GUI, you must delete the account and create it again. If desired, you can use the **config netuser lifetime user_name 0** command to make a guest user account permanent without deleting and recreating it.
- Step 6** From the WLAN SSID drop-down list, choose the SSID that will be used by the guest user. The only WLANs that are listed are those WLANs for which Layer 3 web authentication has been configured.
- Note** We recommend that you create a specific guest WLAN to prevent any potential conflicts. If a guest account expires and it has a name conflict with an account on the RADIUS server and both are on the same WLAN, the users associated with both accounts are disassociated before the guest account is deleted.
- Step 7** In the Description text box, enter a description of the guest user account. You can enter up to 32 characters.
- Step 8** Click **Apply** to commit your changes. The new guest user account appears in the list of guest users on the Guest Users List page.
From this page, you can see all of the guest user accounts, their WLAN SSID, and their lifetime. You can also edit or remove a guest user account. When you remove a guest user account, all of the clients that are using the guest WLAN and are logged in using that account's username are deleted.
- Step 9** Repeat this procedure to create any additional guest user accounts.
-

Viewing Guest User Accounts

Viewing the Guest Accounts (GUI)

To view guest user accounts using the controller GUI, choose **Security > AAA > Local Net Users**. The Local Net Users page appears.

From this page, you can see all of the local net user accounts (including guest user accounts) and can edit or remove them as desired. When you remove a guest user account, all of the clients that are using the guest WLAN and are logged in using that account's username are deleted.

Viewing the Guest Accounts (CLI)

To see all of the local net user accounts (including guest user accounts) using the controller CLI, enter this command:

```
show netuser summary
```

Configuring Administrator Usernames and Passwords

Information About Configuring Administrator Usernames and Passwords

You can configure administrator usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information. This section provides instructions for initial configuration and for password recovery.

Configuring Usernames and Passwords (GUI)

-
- Step 1** Choose **Management > Local Management Users**.
- Step 2** Click **New**.
- Step 3** Enter the username and password, and confirm the password.
Usernames and passwords are case-sensitive and can contain up to 24 ASCII characters. Usernames and passwords cannot contain spaces.
- Step 4** Choose the User Access Mode as one of the following:
- **ReadOnly**
 - **ReadWrite**
 - **LobbyAdmin**
- Step 5** Click **Apply**.
-

Configuring Usernames and Passwords (CLI)

Step 1 Configure a username and password by entering one of these commands:

- **config mgmtuser add *username password read-write***—Creates a username-password pair with read-write privileges.
- **config mgmtuser add *username password read-only***—Creates a username-password pair with read-only privileges.

Usernames and passwords are case-sensitive and can contain up to 24 ASCII characters. Usernames and passwords cannot contain spaces.

Note If you ever need to change the password for an existing username, enter the **config mgmtuser password *username new_password*** command.

Step 2 List the configured users by entering this command:

show mgmtuser

Restoring Passwords

Step 1 After the controller boots up, enter **Restore-Password** at the User prompt.

Note For security reasons, the text that you enter does not appear on the controller console.

Step 2 At the Enter User Name prompt, enter a new username.

Step 3 At the Enter Password prompt, enter a new password.

Step 4 At the Re-enter Password prompt, reenter the new password. The controller validates and stores your entries in the database.

Step 5 When the User prompt reappears, enter your new username.

Step 6 When the Password prompt appears, enter your new password. The controller logs you in with your new username and password.

Changing the Default Values for SNMP v3 Users

Information About Changing the Default Values for SNMP v3 Users

The controller uses a default value of “default” for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values.


Note

SNMP v3 is time sensitive. Ensure that you configure the correct time and time zone on your controller.

Changing the SNMP v3 User Default Values (GUI)

-
- Step 1** Choose **Management** > **SNMP** > **SNMP V3 Users** to open the SNMP V3 Users page.
- Step 2** If “default” appears in the User Name column, hover your cursor over the blue drop-down arrow for the desired user and choose **Remove** to delete this SNMP v3 user.
- Step 3** Click **New** to add a new SNMP v3 user. The SNMP V3 Users > New page appears.
- Step 4** In the User Profile Name text box, enter a unique name. Do not enter “default.”
- Step 5** Choose **Read Only** or **Read Write** from the Access Mode drop-down list to specify the access level for this user. The default value is Read Only.
- Step 6** From the Authentication Protocol drop-down list, choose the desired authentication method: **None**, **HMAC-MD5** (Hashed Message Authentication Coding-Message Digest 5), or **HMAC-SHA** (Hashed Message Authentication Coding-Secure Hashing Algorithm). The default value is HMAC-SHA.
- Step 7** In the Auth Password and Confirm Auth Password text boxes, enter the shared secret key to be used for authentication. You must enter at least 12 characters that include both letters and numbers.
- Step 8** From the Privacy Protocol drop-down list, choose the desired encryption method: **None**, **CBC-DES** (Cipher Block Chaining-Digital Encryption Standard), or **CFB-AES-128** (Cipher Feedback Mode-Advanced Encryption Standard-128). The default value is CFB-AES-128.
- Note** In order to configure CBC-DES or CFB-AES-128 encryption, you must have selected either HMAC-MD5 or HMAC-SHA as the authentication protocol in [Step 6](#).
- Step 9** In the Priv Password and Confirm Priv Password text boxes, enter the shared secret key to be used for encryption. You must enter at least 12 characters that include both letters and numbers.
- Step 10** Click **Apply**.
- Step 11** Click **Save Configuration**.
- Step 12** Reboot the controller so that the SNMP v3 user that you added takes effect.
-

Changing the SNMP v3 User Default Values (CLI)

- Step 1** See the current list of SNMP v3 users for this controller by entering this command:
show snmpv3user
- Step 2** If “default” appears in the SNMP v3 User Name column, enter this command to delete this user:
config snmp v3user delete *username*
The *username* parameter is the SNMP v3 username (in this case, “default”).
- Step 3** Create a new SNMP v3 user by entering this command:
config snmp v3user create *username* {ro** | **rw**} {**none** | **hmacmd5** | **hmacsha**} {**none** | **des** | **aescfb128**} *auth_key*
*encrypt_key***
where
- *username* is the SNMP v3 username.
 - **ro** is read-only mode and **rw** is read-write mode.
 - **none**, **hmacmd5**, and **hmacsha** are the authentication protocol options.
 - **none**, **des**, and **aescfb128** are the privacy protocol options.
 - *auth_key* is the authentication shared secret key.
 - *encrypt_key* is the encryption shared secret key.
- Do not enter “default” for the *username*, *auth_key*, and *encrypt_key* parameters.
- Step 4** Enter the **save config** command.
- Step 5** Reboot the controller so that the SNMP v3 user that you added takes effect by entering **reset system** command.
-

