# Managing Users



# 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.

## Restrictions on Managing User Accounts

- 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.
- For net user accounts or guest user accounts, the following special characters are allowed along with alphanumeric characters: ~, @, #, $, %, ^, &, (, ), !, _, -, `, ., [, ], =, +, *, :, ;, {, }, ,, /, and \.

### Related Topics

Maximum Local Database Entries

## Configuring Usernames and Passwords (GUI)

### Procedure

**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)

### Procedure

- Configure a username and password by entering one of these commands:
  - **config mgmtuser add** *username password* **read-write** *description*—Creates a username-password pair with read-write privileges.
  - **config mgmtuser add** *username password* **read-only** *description*—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.

  - **config mgmtuser add** *username password* **lobby-admin** *description*—Creates a username-password pair with Lobby Administrator privileges.
  - **config mgmtuser type5-add** *username md5-crypt_password* { **read-write** | **read-only** | **lobby-admin** } *description* —Creates a management username-password pair with type-5 encryption.
  - **config mgmtuser type5-password** *username md5-crypt_password* —Configures type-5 encrypted password for an existing management user account.
- List the configured users by entering this command:

  **show mgmtuser**
- View the type of password encryption used for the current user by entering this command:

  **debug aaa detail enable**

# Lobby Ambassador Account

This section contains the following subsections:

## Creating a Lobby Ambassador Account (GUI)

**Procedure**

**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 1, |, or ! or substituting 0 for o or substituting $ for s.
- If you want to downgrade from Release 8.6 to Release 8.5 or an earlier release, ensure that you have a management user account password that is less than or equal to 24 characters to be compatible with the earlier releases. Else, during the downgrade and before you can reboot the controller, you will be prompted with the following message:

  ```
  "Warning!!! Please Configure Mgmt user compatible with older release"
  ```

**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)

**Procedure**

- 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)

**Procedure**

**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 (Release 8.5 and earlier releases) and 127 characters (Release 8.6 and later releases) 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.

# Guest Accounts

The controller can provide guest user access on WLANs for which you must create guest user accounts. Guest user accounts can be created by network administrators, or, if you would like a non-administrator to be able to create guest user accounts on demand, you can do so through a lobby administrator account. The lobby ambassador has limited configuration privileges and has access only to the web pages used to manage the guest user 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.

This section contains the following subsections:

## Viewing the Guest Accounts (GUI)

**Procedure**

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)

### Procedure

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

  **show netuser summary**

# Password Policies

The password policies allows you to enforce strong password checks on newly created passwords for additional management users of controller and access point. The following are the requirements enforced on the new password:

- When the controller is upgraded from old version, all the old passwords are maintained as it is, even though the passwords are weak. After the system upgrade, if strong password checks are enabled, the same is enforced from that time and the strength of previously added passwords will not be checked or altered.
- Depending on the settings done in the Password Policy page, the local management and access point user configuration is affected.

### Guidelines and Restrictions for Password Policies

- Strong password requirement based on WLAN-CC requirement is applicable only to WLAN admin login passwords and is not applicable to AP Management user passwords.
- The valid length of AP Management user passwords is minimum of 8 characters and maximum of 127 characters. Also, it is not possible to change the AP Management user password. Therefore, the restrictions of local net users for strong password does not apply to AP Management user passwords.
- Strong password: lockout feature is not applied if you try to access the controller through a serial connection or a terminal server connection and it has unlimited attempts.

This section contains the following subsections:

## Configuring Password Policies (GUI)

### Procedure

**Step 1** Choose **Security** > **AAA** > **Password Policies** to open the Password Policies page.

**Step 2** Select the **Password must contain characters from at least 3 different classes** check box if you want your password to contain characters from at least three of the following classes: lower case letters, upper case letters, digits, and special characters.

**Step 3** Select the **No character can be repeated more than 3 times consecutively** check box if you do not want character in the new password to repeat more than three times consecutively.

**Step 4** Select the **Password cannot be the default words like cisco, admin** check box if you do not want the password to contain words such as Cisco, ocsic, admin, nimda, or any variant obtained by changing the capitalization of letters or by substituting 1, |, or! or substituting 0 for o or substituting $ for s.

**Step 5** Select the **Password cannot contain username or reverse of username** check box if you do not want the password to contain a username or the reverse letters of a username.

**Step 6** Click **Apply** to commit your changes.

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

# Configuring Password Policies (CLI)

### Procedure

- Enable or disable strong password check for AP and WLC by entering this command:

  **config switchconfig strong-pwd** {**case-check** | **consecutive-check** | **default-check** | **username-check** | **all-checks** | **position-check** | **case-digit-check**} {**enable** | **disable**}

  where

  - **case-check**—Checks the occurrence of same character thrice consecutively
  - **consecutive-check**—Checks the default values or its variants are being used.
  - **default-check**—Checks either username or its reverse is being used.
  - **all-checks**—Enables/disables all the strong password checks.
  - **position-check**—Checks four-character range from old password.
  - **case-digit-check**—Checks all four combinations to be present: lower, upper, digits, and special characters.

- Configure minimum number of upper, lower, digit, and special characters in a password by entering this command:

  **config switchconfig strong-pwd minimum** {**upper-case** | **lower-case** | **digits** | **special-chars**} *num-of-chars*

- Configure minimum length for a password by entering this command:

  **config switchconfig strong-pwd min-length** *pwd-length*

- Configure lockout for management or SNMPv3 users by entering this command:

  **config switchconfig strong-pwd lockout** {**mgmtuser** | **snmpv3user**} {**enable** | **disable**}

- Configure lockout time for management or SNMPv3 users by entering this command:

  **config switchconfig strong-pwd lockout time** {**mgmtuser** | **snmpv3user**} *timeout-in-mins*

- Configure the number of consecutive failure attempts for management or SNMPv3 users by entering this command:

**config switchconfig strong-pwd lockout attempts** {**mgmtuser** | **snmpv3user**} *num-of-failure-attempts*

- Configure lifetime for management or SNMPv3 users by entering this command:

  **config switchconfig strong-pwd lifetime** {**mgmtuser** | **snmpv3user**} *lifetime-in-days*

- See the configured options for strong password check by entering this command:

  **show switchconfig**

  Information similar to the following appears:

```
802.3x Flow Control Mode..... Disabled
FIPS prerequisite features..... Disabled
secret obfuscation..... Enabled
Strong Password Check Features:

         case-check ...........Enabled
         consecutive-check ....Enabled
         default-check .......Enabled
         username-check ......Enabled
```