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.

You can configure management user account password with the type-5 (MD5) or the existing type-0, type-6, or type-7 encryption. We recommend you to use the Type-5 encryption protocol because it provides enhanced security with a one-way hash.

Restrictions on Managing User Accounts

- The local user database is limited to a maximum of 12000 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 \.
- If you downgrade from Release 8.10.x to a release that does not support type-5 encryption, the management accounts that you created with the type-5 (MD5) encryption cannot be accessed. We recommend that you delete such management user accounts and create new ones without type-5 encryption.
- Type-5 encryption for management user accounts is not supported during day-0 setup. We recommend that you use the default type-7 password for management user accounts. After the accounts are created, you, as an administrator, can change the type-7 passwords to type-5 passwords, if required.

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. The passwords can contain up to 127 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

Client Whitelisting

Locations such as a university receive many guests with multiple devices. It becomes eminent to protect the network from misuse or unauthorized access and allow legitimate clients to connect to the network. Registering or deregistering of clients is a tedious and time consuming task to perform regularly. Hence the requirement for a simpler solution.

This feature addresses the need of allowing clients on a particular WLAN or SSID based on the MAC address. For this purpose, the currently existing features are reused - MAC filtering option on WLAN, adding lobby admin user and reuse AAA DB to store the list of allowed clients on a WLAN.

Two types of administrators manage the feature administration:

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

This section contains the following subsections:

Restrictions for Client Whitelisting

- For Cisco vWLC, the AAA database is restricted to 2048 entries.
- For Cisco 5520, 3504, and 8540 Wireless Controllers, the AAA database size is increased to 12000 entries.

- The MAC address cannot be registered under multiple WLANs or SSIDs.
- Lobby Administrator can only configure using GUI interface.

Note This AAA database is shared across:

- MAC filtering
- Local net users
- Management users
- Manual blocked list users
- AP authenticated list users
- Guest users

Configuring Lobby Administrator by Global Administrator (GUI)

This section provides instructions to create or delete the lobby administrator on the controller for the management of guest users and allowed users by the global administrator.

Procedure

Step 1 Choose **Management** > **Local Management Users**.

Step 2 In the Local Management Users section, add the lobby administrator:

a) Click **New**.
b) Enter the **User Name**.
c) Enter the **Password**.
d) Confirm **Password**.
e) Choose **lobby admin** under the **User Access Mode** drop-down list.
f) Click **Apply**.

What to do next

Configure Lobby Administrator Access on WLAN.

Configuring Lobby Administrator by Global Administrator (CLI)

Procedure

Step 1 Add a local lobby admin to controller by entering this command.

config mgmtuser add *username password* **lobby-admin**

Step 2 Enable or disable the lobby admin access on the WLAN by entering this command.

config wlan lobby-admin-access { **enable | disable**} *wlan-id*

Configuring Client Whitelist by Global Administrator (CLI)

The global administrator can configure clients that need to be allowed by using the following commands.

Procedure

Step 1 View the WLAN lobby access status by entering this command.

show wlan lobby-admin-access

Step 2 View the WLAN associated client list by entering this command.

show client wlan *wlan-id*

Step 3 Add selected or all clients of the allowed group by entering this command.

config mac-filter add *mac-address wlan-id interface description*

Note For this feature, the interface field value is set to 0.

Step 4 Delete selected or all selected clients of the allowed group by entering this command.

config mac-filter delete *mac-addr*

Step 5 View the summary of all the MAC filter entries on all WLANs by entering this command.

show macfilter summary

Step 6 View the list of all MAC filter entries on a given WLAN entering this command.

show macfilter wlan *wlan-id*

Step 7 Enable or disable MAC filtering on a WLAN by entering this command.

config wlan mac-filtering {**enable** | **disable**} *wlan-id*

Configuring Lobby Administrator Access on WLAN by Global Administrator (GUI)

This section provides instructions to enable the lobby admin for a WLAN.

Procedure

Step 1 Choose **WLANs** > **WLAN ID** > **Security** tab.
Step 2 Check the **Lobby Admin Access** check box.
Step 3 Click **Apply**.

Creating Client Whitelist by Lobby Administrator (GUI)

Adding MAC Addresses to a Whitelist by SSID

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

Before you begin

1. The lobby administrator must be in config mode under the required WLAN.
2. Inform the target users to connect their devices to a particular SSID.

Procedure

Step 1 Log in to the Controller as the lobby administrator.
Step 2 Choose **White List Users**.
Step 3 Choose the WLAN from the drop-down list for which the allowed list must be applied.
Step 4 Choose **Config Mode**.
Step 5 Click **Apply**.
Step 6 Click **Filter by**.

Select AP Name and enter the AP name.

Step 7 Click the **search icon**.

The result displays the connected clients to the select AP.

Step 8 Check the **Select All** check box.

All the clients displayed are selected.

Step 9 Enter the description in the **Description** field.

Enter an identity tag to this list for easy administration.

Step 10 Click **Add**.
Step 11 Select **Running Mode**.
Step 12 Click **Apply**.

The radio will restart for the new WLAN configuration to take effect.

Only clients in the allowed list continue to be associated, rest of the clients are disassociated from the AP.

Adding Single MAC Address to Whitelist

Procedure

Step 1 Log in to the Controller as the lobby ambassador.

Step 2 Choose **White List Users**.

Step 3 Choose the WLAN from the drop-down list for which the allowed list must be applied.

Step 4 Enter the **MAC address**.

Step 5 Enter the **Description**.

Step 6 Click **Add**.

Note Repeat steps 4 to 6 to add more single MAC address.

Importing MAC Address CSV List to Whitelist

Procedure

Step 1 Log in to the Controller as the lobby ambassador.

Step 2 Choose **White List Users**.

Step 3 Choose the WLAN from the drop-down list for which the allowed list must be applied.

Step 4 Click the **Config Mode** radio button.

Step 5 Click **Apply**.

Step 6 Check the **Upload CSV file** check box.

Step 7 Click **Browse File**.

Step 8 Choose the CSV file to import.

Click **OK** in the dialog box.

Step 9 Click **Add**

Deleting MAC Address from Whitelist (GUI)

You can delete a single MAC address or in bulk from the whitelist.

Procedure

Step 1 Log in to the Controller as the lobby administrator

Step 2 Choose **White List Users**

Step 3 Choose the WLAN from the drop-down list to retrieve the allowed list.

Step 4 Choose one of the following deletion methods:

a) Single client deletion—Either enter the **`client MAC address`** and click **delete** or click the **X** delete icon in front of the MAC address to delete.

b) Multiple client deletion—Filter the clients to be deleted based on either AP name or description, select all or selected multiple MAC addresses and click **delete**

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.
- Strings such as *nobody*, *rsyncuser*, and *root* are not allowed to be AP management username or password.
- We recommend that you follow the strong password policy guidelines when you configure SNMPv2 community and SNMPv3 passwords.

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 controller 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*

- Configure restore password option for management users by entering this command:

  config switchconfig restore-password {**enable** | **disable**}

  By default, this feature is in enabled state.

  Before Release 8.10, this feature was enabled by default and was nonconfigurable. In 8.10 and later releases, you are given the option to enable or disable it.

- 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
```