# Configuring Password Policies


- Password Policies, on page 1
- Configuring Password Policies (GUI), on page 2
- Configuring Password Policies (CLI), on page 2


# 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.

### Restrictions on 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 3 characters and maximum of 32 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)

**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
```