パスワード ポリシーの設定

パスワード ポリシーについて

パスワードポリシーを使用すると、コントローラおよびアクセスポイントの追加管理ユーザ用に新しく作成されたパスワードに対し、強力なパスワードチェックを適用できます。新規パスワードには次の要件が適用されます。

- コントローラが旧バージョンからアップグレードされた場合、古いパスワードはすべて現状のまま維持されます。ただし、パスワードの強度は低下します。システムのアップグレード後、強力なパスワード チェックが有効になると、それ以降は強力なパスワード チェックが適用され、以前に追加されたパスワードの強度のチェックまたは変更は行われません。
- [Password Policy] ページで設定された内容によっては、ローカル管理ユーザおよびアクセス ポイント ユーザの設定が影響を受けます。

パスワード ポリシーの設定（GUI）

ステップ 1 [Security] > [AAA] > [Password Policies] の順に選択して、[Password Policies] ページを開きます。

ステップ 2 小文字、大文字、数字、特殊文字の中から少なくとも 3 種類の文字をパスワードに含める場合は、[Password must contain characters from at least 3 different classes] チェックボックスをオンにします。

ステップ 3 新規パスワード内で同じ文字が 4 回以上連続して繰り返されないようにするには、[No character can be repeated more than 3 times consecutively] チェックボックスをオンにします。

ステップ 4 パスワードに Cisco、ocsic、admin、nimda や、大文字と小文字を変更したり、1、|、または ! を代用したり、o の代わりに 0 や、s の代わりに $ を使用したりするだけの変形文字列をパスワードに含めないようにするには、[Password cannot be the default words like cisco, admin] チェックボックスをオンにします。

ステップ 5 パスワードにユーザ名またはユーザ名を逆にした文字を含めないようにするには、[Password cannot contain username or reverse of username] チェックボックスをオンにします。

ステップ 6 [Apply] をクリックして、変更を確定します。

ステップ 7 [Save Configuration] をクリックして、変更を保存します。

パスワード ポリシーの設定（CLI）

- 次のコマンドを入力して、AP および WLC に対して強力なパスワード チェックを有効または無効にします。
  config switchconfig strong-pwd {case-check | consecutive-check | default-check | username-check | all-checks| position-check | case-digit-check} {enable | disable}

  値は次のとおりです。

  - **case-check**：同じ文字が 3 回連続して使用されているかを確認します。
  - **consecutive-check**：デフォルト値またはそのバリアントが使用されているかを確認します。
  - **default-check**：ユーザ名またはそれを逆にした文字が使用されているかを確認します。
  - **all-checks**：強力なパスワード チェックをすべて有効または無効にします。
  - **position-check**：古いパスワードからの 4 文字の流用を確認します。
  - **case-digit-check**：小文字、大文字、数字、特殊文字の 4 つすべての組み合わせが含まれているかを確認します。

- 次のコマンドを入力して、パスワード内の小文字、大文字、数字、特殊文字の最小数を設定します。

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

- 次のコマンドを入力して、パスワードの最小長を設定します。
  config switchconfig strong-pwd min-length *pwd-length*
- 次のコマンドを入力して、管理または SNMPv3 ユーザのロックアウトを設定します。
  config switchconfig strong-pwd lockout {**mgmtuser** | **snmpv3user**} {**enable** | **disable**}
- 次のコマンドを入力して、管理または SNMPv3 ユーザのロックアウト時間を設定します。
  config switchconfig strong-pwd lockout time {**mgmtuser** | **snmpv3user**} *timeout-in-mins*
- 次のコマンドを入力して、管理または SNMPv3 ユーザの試行連続失敗回数を設定します。
  config switchconfig strong-pwd lockout attempts {**mgmtuser** | **snmpv3user**} *num-of-failure-attempts*
- 次のコマンドを入力して、管理または SNMPv3 ユーザのライフタイムを設定します。
  config switchconfig strong-pwd lifetime {**mgmtuser** | **snmpv3user**} *lifetime-in-days*
- 次のコマンドを入力して、強力なパスワード チェックに設定されたオプションを表示します。
  show switchconfig

  以下に類似した情報が表示されます。

```
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
```