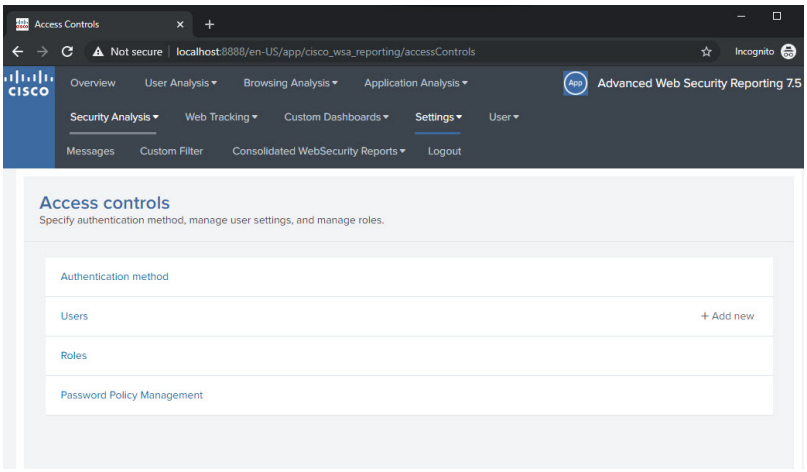
# パスワードポリシー管理

この章では、Cisco Advanced Web Security Reporting アプリケーションの Web GUI で実行できるパスワード関連の設定について説明します。これらの操作を実行するには、管理者権限が必要です。**[設定（Settings）] > [ユーザーと認証（USERS AND AUTHENTICATION）] > [アクセス制御（Access Controls）] > [パスワードポリシー管理（Password Policy Management）]** に移動して、[パスワードポリシー管理（Password Policy Management）] ページに移動します。





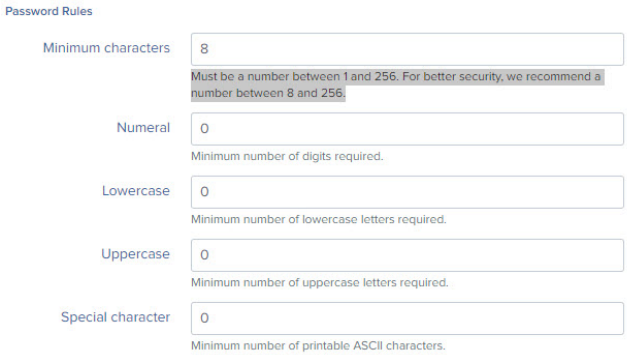

# パスワードの規則

パスワードは数字、小文字、大文字、英数字の組み合わせにする必要があります。パスワードを設定するには次のフィールドを指定できます。

- [最小文字数（Minimum Characters）]：パスワードで使用される最小文字数を設定します。

（注） 1 ～ 256 の範囲内の数を指定してください。8 を超える数を使用することをお勧めします。

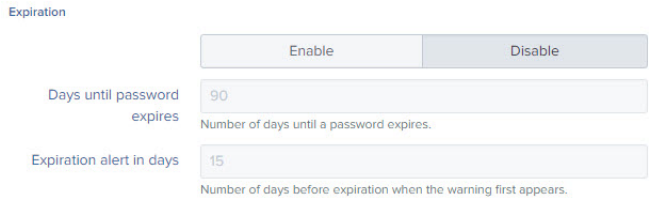
- [数字（Numerals）]：パスワードの数字の最小文字数を設定します。
- [小文字（Lowercase）]：パスワードの小文字の最小文字数を設定します。
- [大文字（Uppercase）]：大文字の最小文字数を設定します。
- [特殊文字（Special character）]：特殊文字または英数字の最小文字数を設定します。




# パスワードの期限

パスワードの期限の期間を有効または無効にできます。次のフィールドを設定できます。

- [パスワードの期限までの日数（Date until password expires）]：パスワードの期限が切れるまでの日数を設定します。
- [有効期限アラート（日数）（Expiration alert in days）]：ユーザにアラートが表示される有効期限までの日数を設定します。



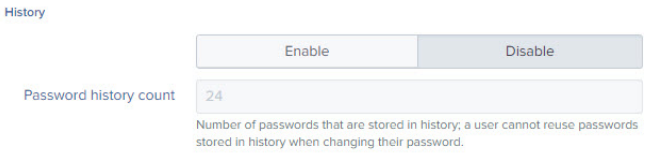

アラートの例を以下に示します。


# パスワード履歴

[パスワード履歴（Password History）] オプションを有効または無効にできます。

- [パスワード履歴カウント（Password History Count）]：履歴に保存されているパスワードの数。

（注） ユーザは、パスワードを変更するときに、履歴に保存されているパスワードを再利用できません。



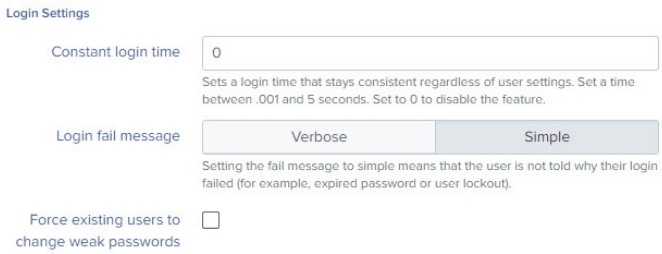

# ログイン設定

- [一定のログイン時間（Constant Login Time）]：ユーザ設定に関係なく一貫性を保つログイン時間を設定します。

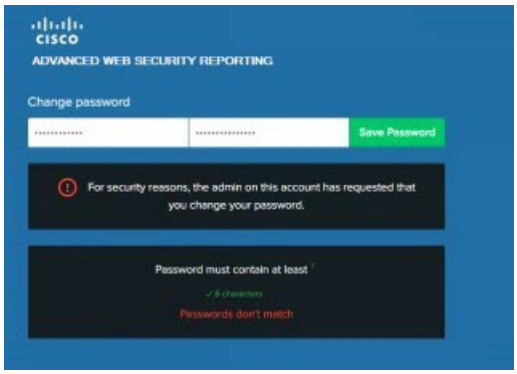
（注） この機能を無効にするには、0 に設定します。

- [ログイン失敗メッセージ（Login fail message）]：ユーザに示す失敗メッセージを設定します。[シンプル（Simple）] を選択した場合、ユーザには

ログインが失敗した理由（期限切れのパスワードやユーザのロックアウトなど）が通知されません。




パスワードの変更中にエラーが発生した場合は、エラーの理由が表示されます。次に例を示します。


# パスワード ロックアウト

この機能では、ブルートフォースログイン攻撃を防ぐために、単位時間あたりの各送信元のクレデンシャル試行回数を制限します。

次のフィールドを設定できます。

- [ログイン試行失敗回数（Failed login attempts:）]：ユーザがロックアウトされるまでに実行できるログイン試行回数。
- [ロックアウトしきい値（分単位）（Lockout threshold in minutes）]：最初のログイン失敗後、カウンタがリセットされるまでに必要な時間。
- [ロックアウト期間（分単位）（Lockout duration in minutes）]：ユーザが再度ログインを試行できるようになるまでのロックアウト期間。


ログインに失敗すると、管理者が指定したロックアウト期間中はユーザアカウントがロックされます。