FMCドメインの設定(&N)：ユーザアクセスおよびロール

お問い合わせ内容

このドキュメントでは、グローバルドメインとサブドメインにまたがるFMCの複数のユーザに対して異なるユーザ権限を設定する方法について説明します。

環境

- Cisco Secure Firewall Management Center(FMC):7.6.4（すべてのFMCに適用）
- グローバルドメインとサブドメインを使用したマルチドメイン展開
- 異なるサブドメインに割り当てられた複数のFTDデバイス
- 異なるアクセス許可レベルを必要とする複数のユーザー

解決策

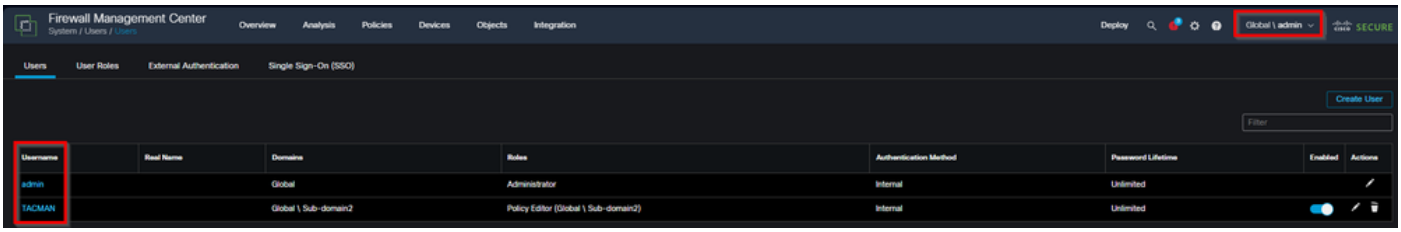
このドキュメントでは、ドメイン間のアクセスを制限し、特定のユーザのグローバルドメインアクセスを制限する機能を使用して、グローバルドメインとサブドメインにまたがるFMCの複数のユーザに対して異なるユーザ権限を設定する方法について説明します。 Cisco FMCは、複数のドメイン間でアクセスを制限する機能を使用して、複数のドメインに対するきめ細かなユーザロールの割り当てをサポートします。 この設定には、特定のドメインでのユーザの作成と、アクセスレベルを制御するための適切なロールの割り当てが含まれます。

ユーザとドメインのアクセス動作の作成

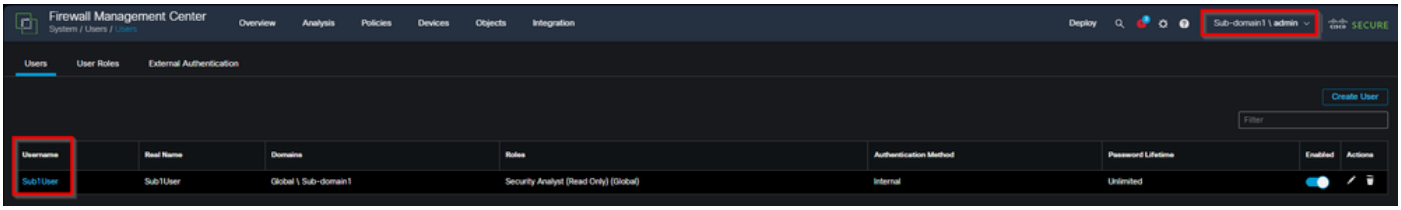
FMCのユーザ管理システムの動作は、ユーザが作成された場所によって異なります。

サブドメインで作成されたユーザ

- サブドメインで直接作成されたユーザは、特定のドメイン内でのみ表示されます。

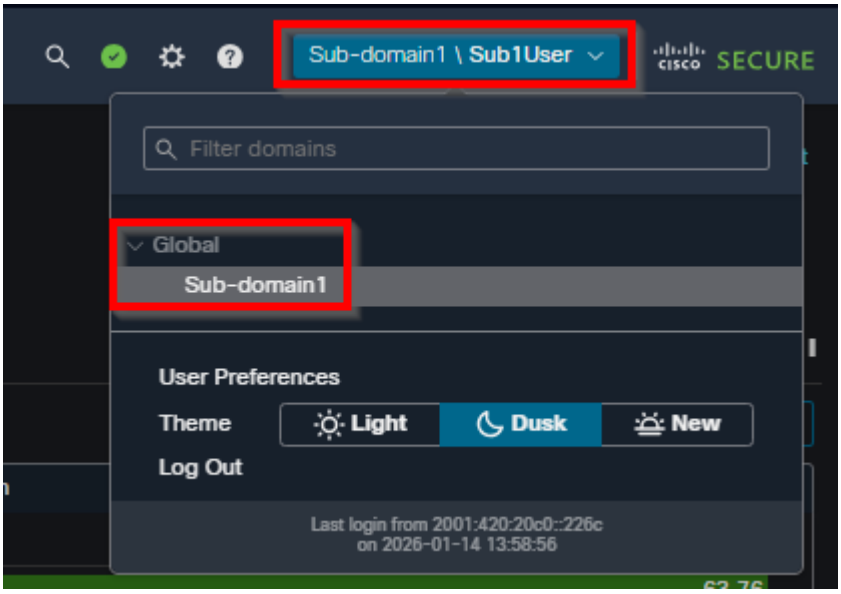


inline_image_0.png (インラインイメージ_0.png)



inline_image_1.pngファイル

- これらのユーザは、subdomain\usernameのドメイン指定形式でログインする必要があります。
- アクセスは、ユーザが作成されたドメインに自動的に制限されます。



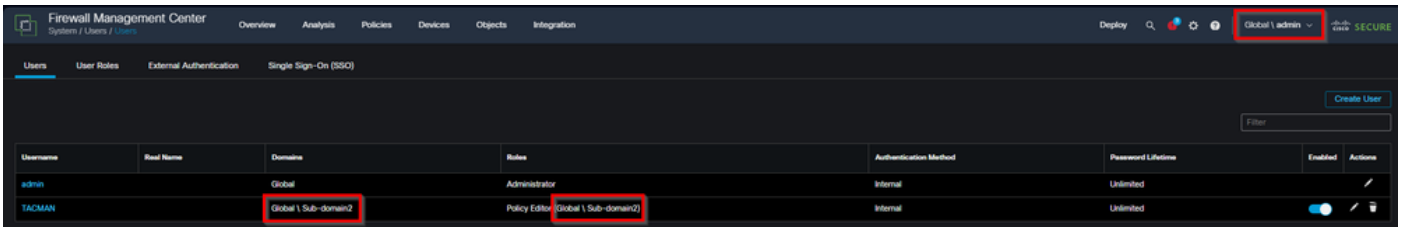
inline_image_2.pngファイル

- サブドメインで作成されたカスタムロールは、そのドメインにのみ適用されます。

グローバルドメインで作成されたユーザー：

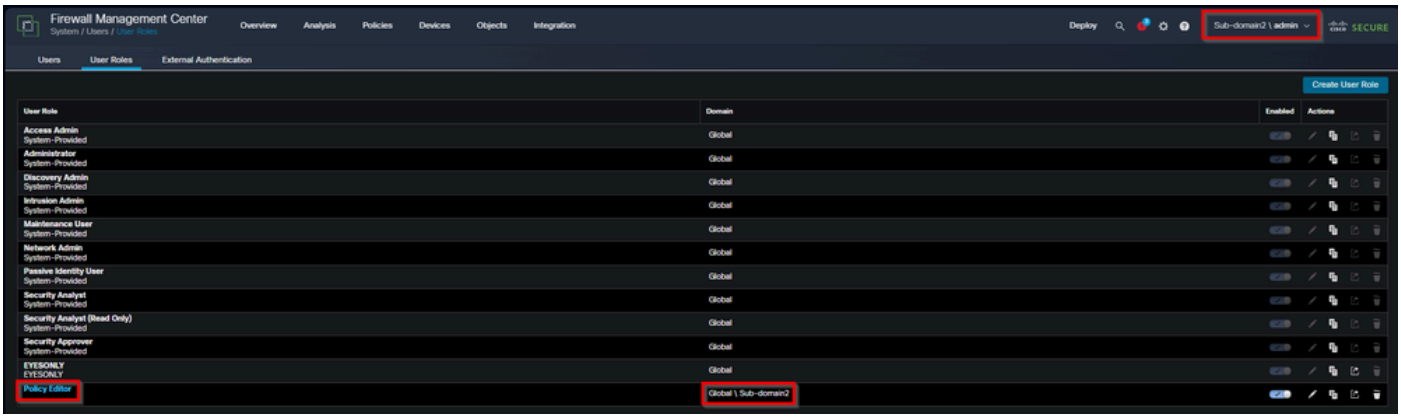
- グローバルドメインから作成されたユーザは、そのロールがサブドメイン内だけであっても、ユーザ名だけでログインできます。

- これらのユーザは、グローバルドメインユーザリストに表示されたままです。



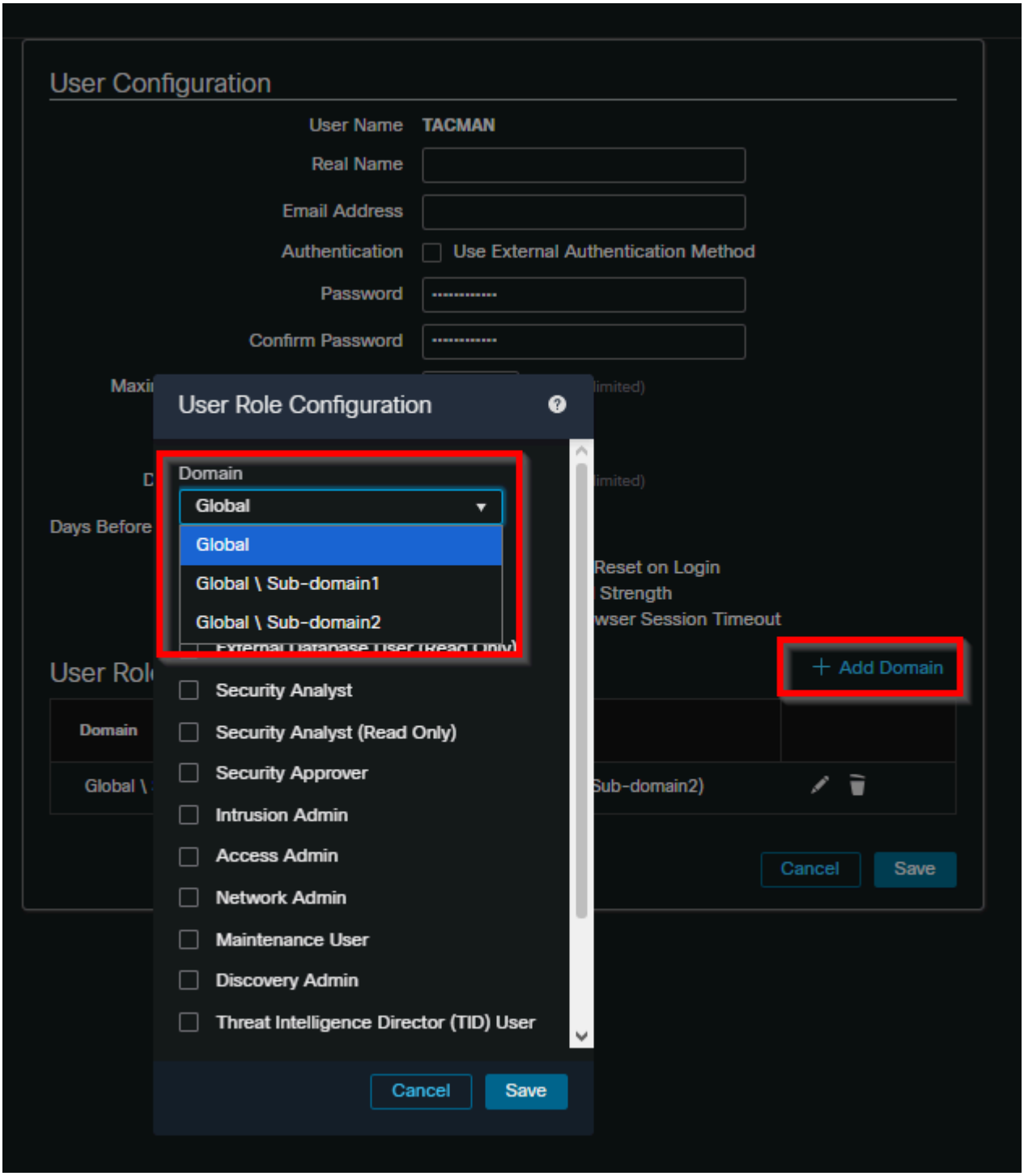
inline_image_3.png (インラインイメージ_3.png)

- ロールの割り当ては、どの子孫ドメインに対しても実行できます。



inline_image_4.pngファイル

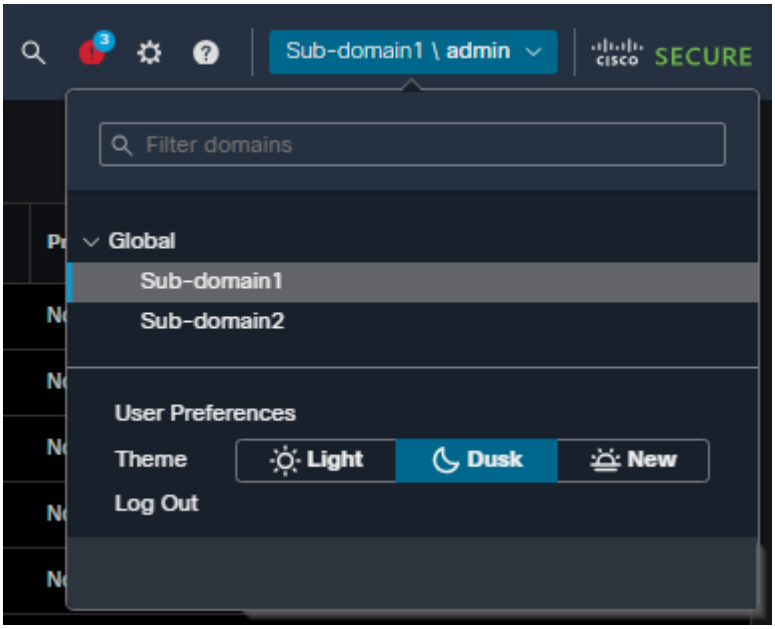
- ロールの割り当てにより、アクセスを特定のサブドメインに制限できます。



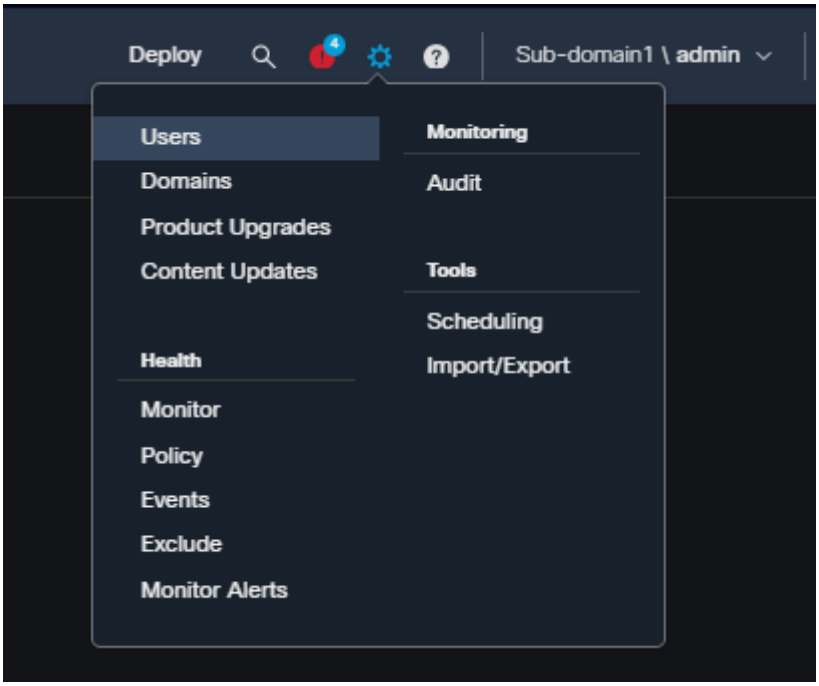
inline_image_5.png (インラインイメージ_5.png)

サブドメインユーザ制限の設定手順

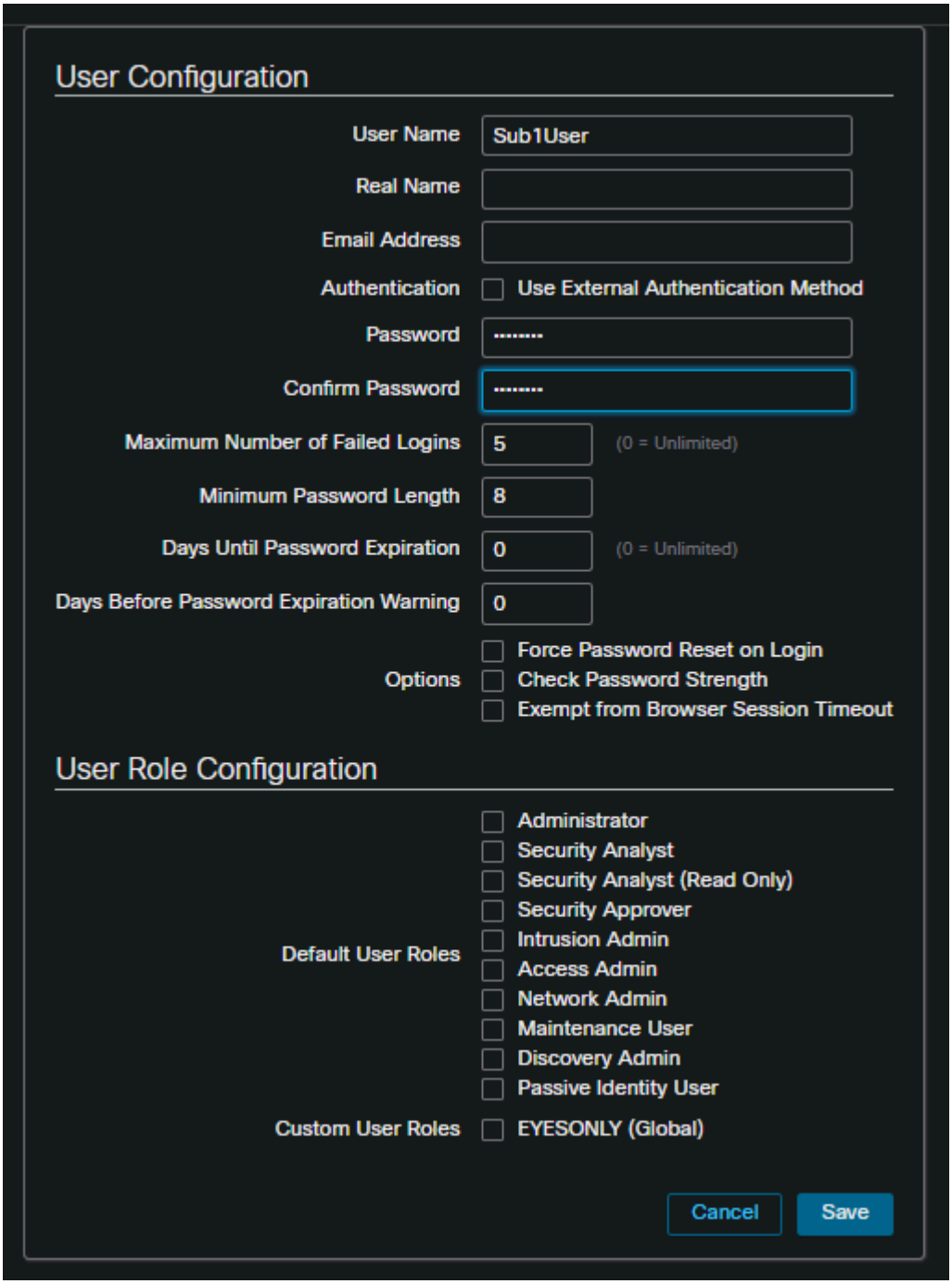
- アクセスを制限する必要がある特定のサブドメインに移動し、System / Usersの下にユーザアカウントを作成します。



inline_image_6.png (インラインイメージ_6.png)

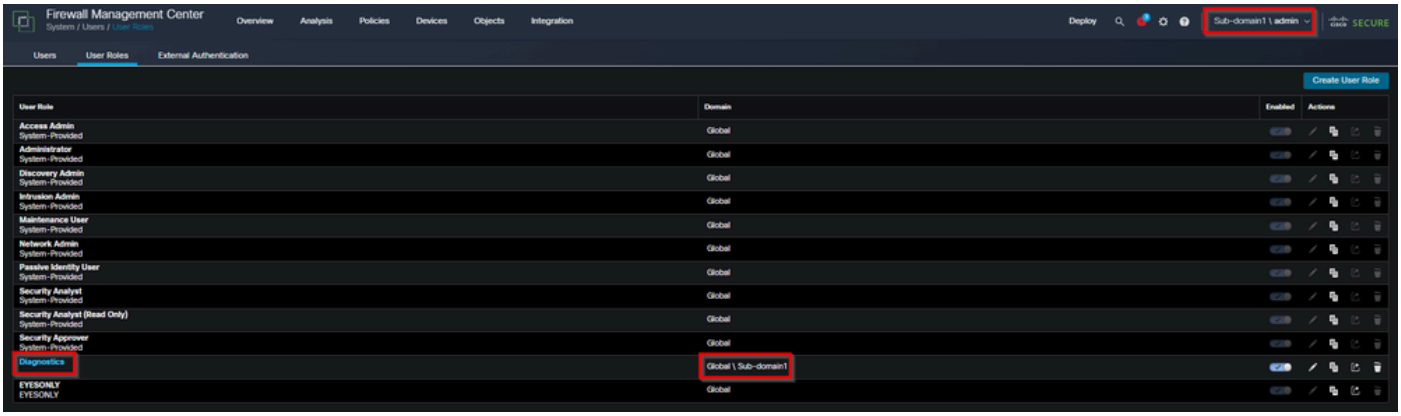


inline_image_7.png (インラインイメージ_7.png)



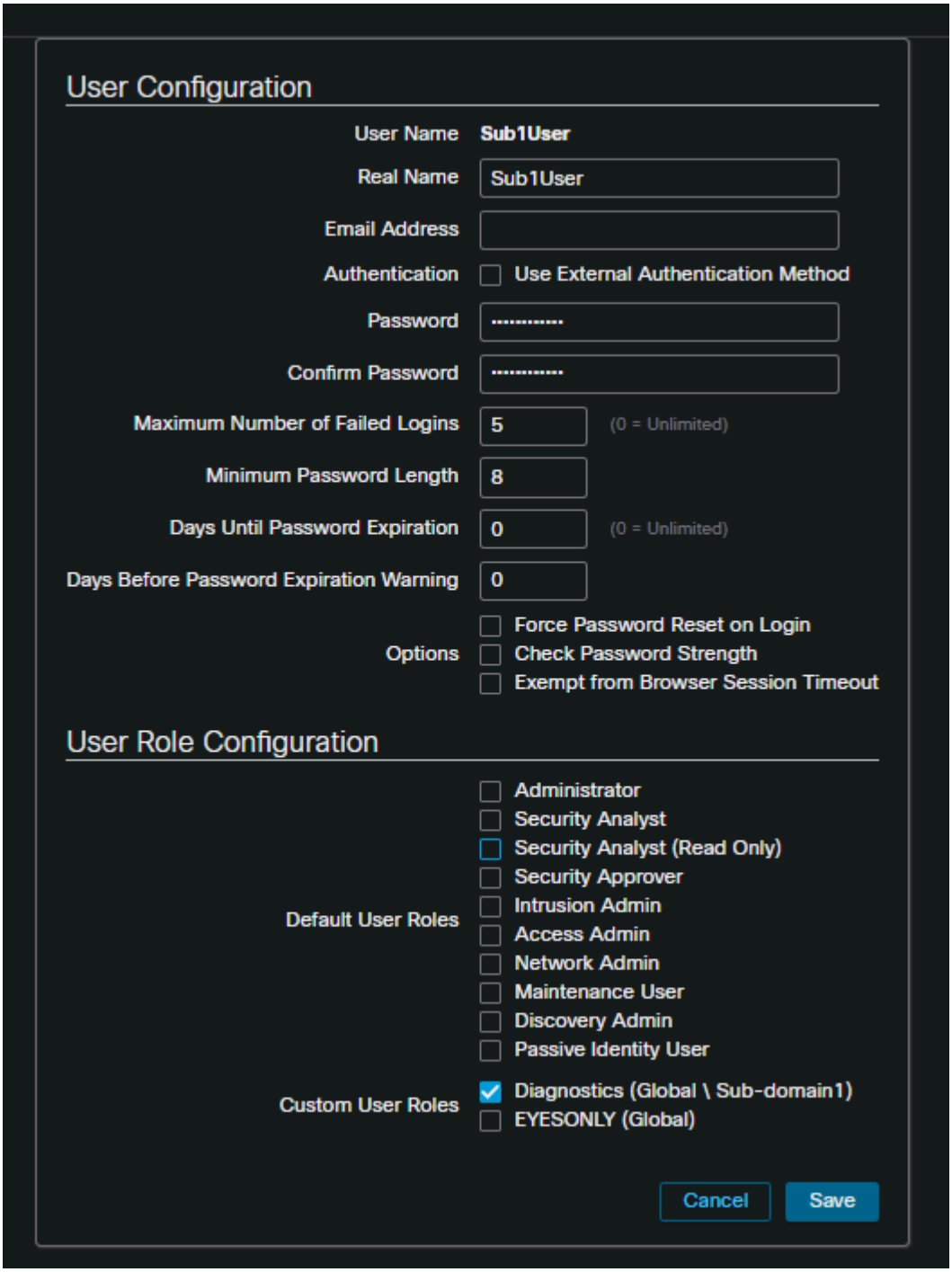
inline_image_8.png (インラインイメージ_8.png)

- System / User Rolesの下のサブドメイン内にカスタムロールを作成します。 サブドメインで作成されたカスタムユーザロールは、そのドメイン内でのみ使用でき、他のドメインからはアクセスできません。



inline_image_9.png (インラインイメージ_9.png)

- カスタムロールをユーザに割り当てます。 ユーザは、ユーザとロールの両方が作成されたドメインの権限のみを継承します。



インラインイメージ_10.png

- サブドメインユーザのユーザログイン形式。 サブドメインで作成されたユーザは、次のログイン形式を使用する必要があります。

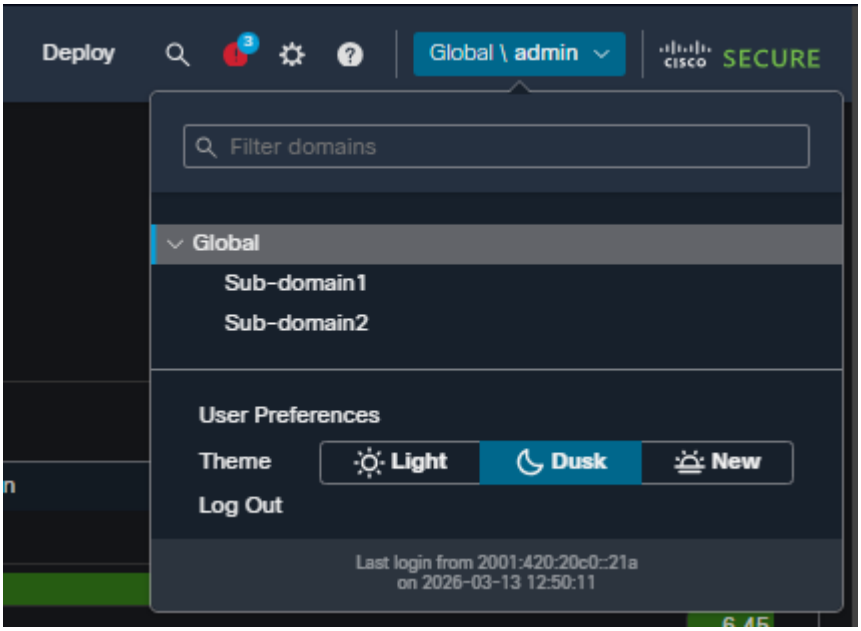
ユーザ名：Sub-domain\username

パスワード：［ユーザーパスワード］

インラインイメージ_11.png

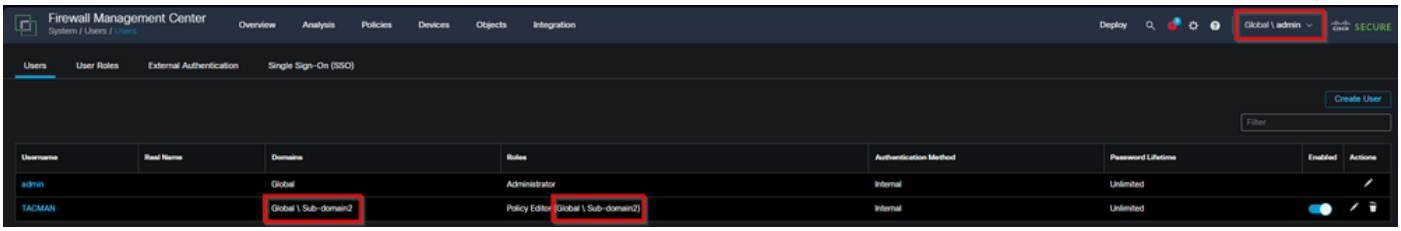
サブドメイン制限があるグローバルドメインユーザの設定手順

- System / Usersの下のグローバルドメインにユーザを作成します。 グローバルドメインアクセス権を持つ管理者アカウントを使用して、ユーザを作成します。

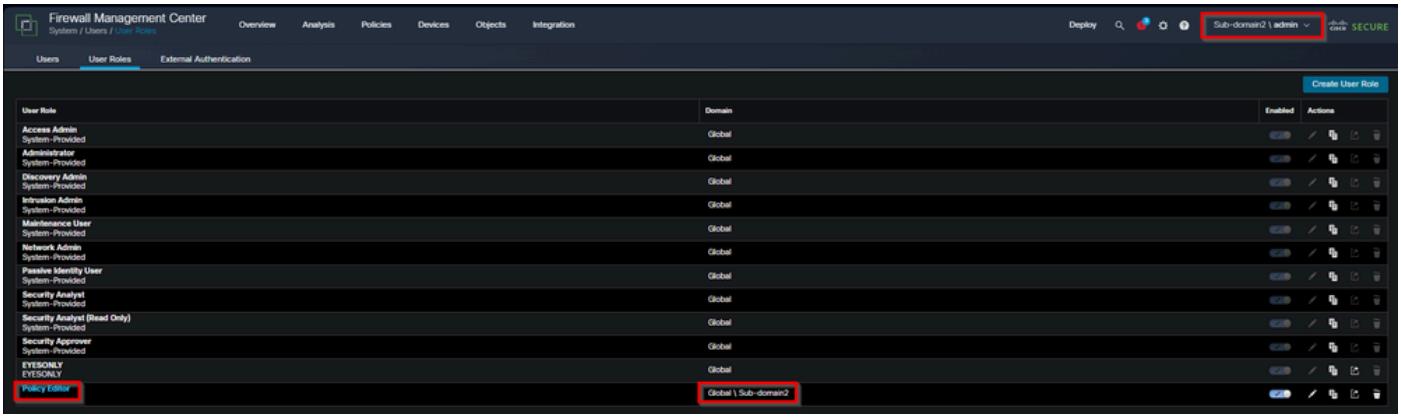


インラインイメージ_12.png

- System / Usersの下の特定のサブドメインにのみロールを割り当てます。 ユーザ設定では、グローバルドメイン権限を付与せずに、ターゲットサブドメインに排他的にロールを割り当てます。



inline_image_3.png (インラインイメージ_3.png)



インラインイメージ_14.png

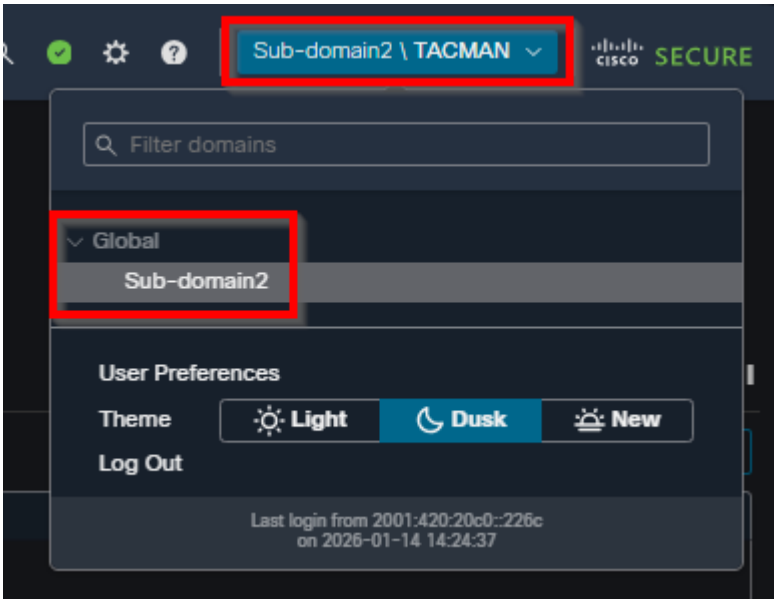
- 次のユーザは、ドメインを指定せずに、自分のユーザ名のみでログインできます。

ユーザ名：ユーザ名

パスワード：［ユーザーパスワード］

inline_image_15.pngファイル

- ユーザは、ロールが明示的に割り当てられたサブドメインにのみアクセスでき、グローバルドメインや他のサブドメインにはアクセスできません。



インラインイメージ_16.png

ロール割り当ての柔軟性

ユーザは、各ドメインで異なる権限を持つことができます。

- グローバルドメインの読み取り専用権限と子孫ドメインの管理者権限
- 特定のサブドメインで完全な管理者権限を持つグローバルドメインアクセスなし
- 1つのサブドメイン内のPolicy Editor権限で、他のサブドメインへのアクセス権がない

外部ユーザの考慮事項

外部ユーザ（LDAPまたはRADIUS認証）:

- ユーザロールがグループメンバーシップまたはユーザ属性を通じて割り当てられている場合、最小アクセス権は削除できません。
- 追加の権限には、デフォルトのユーザロールよりも大きなスコープを割り当てることができます。
- 外部認証オブジェクトは、作成されたドメインでのみ使用できます。
- 適切な制限を行うには、個々のユーザ権限をデフォルトユーザロールよりも広い範囲で設定する必要があります。

制限と考慮事項

- 祖先ドメインで作成されたカスタムユーザロールは、子孫ドメインから編集できません。
- シェル認証は、サブドメインではなく、グローバルドメインでのみ使用できます。
- ユーザー設定とダッシュボード設定は、アカウントがアクセス権を持つすべてのドメインに適用されます。
- ユーザの権限の変更は個別に設定され、グループまたはバルク方式では設定されません。

原因

この要件は、ユーザがグローバルドメインとサブドメインに対するさまざまなレベルのアクセスを必要とし、セキュリティ境界を維持するためにドメイン間で特定の制限を課すマルチドメイン

FMC展開において、きめ細かなアクセスコントロールを実装する必要性から生じています。

関連コンテンツ

- Cisco Secure Firewall Management Centerアドミニストレーションガイド7.6：ユーザ
- Cisco Secure Firewall Management Centerアドミニストレーションガイド7.6：カスタムユーザロールの作成
- Cisco Secure Firewall Management Centerアドミニストレーションガイド7.6：内部ユーザの追加または編集
- Cisco Secure Firewall Management Centerアドミニストレーションガイド7.6：ユーザとドメイン
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。