FMC-Domäne und -Rolle für Benutzerzugriff konfigurieren

Problem

In diesem Dokument wird beschrieben, wie Sie in FMC unterschiedliche Benutzerberechtigungen für mehrere Benutzer in globalen und untergeordneten Domänen konfigurieren.

Umwelt

- Cisco Secure Firewall Management Center (FMC) - 7.6.4 (für alle FMCs)
- Bereitstellung mehrerer Domänen mit globaler Domäne und untergeordneten Domänen
- Mehrere FTD-Geräte, die verschiedenen Subdomänen zugewiesen sind
- Mehrere Benutzer mit unterschiedlichen Berechtigungsstufen

Auflösung

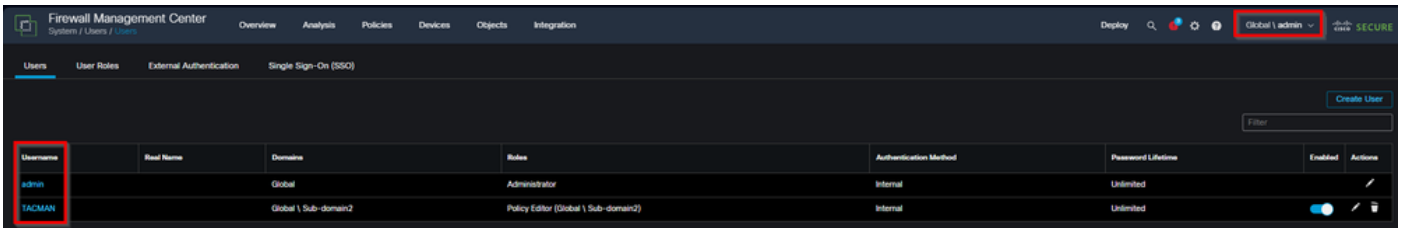
In diesem Dokument wird die Konfiguration unterschiedlicher Benutzerberechtigungen für mehrere Benutzer in FMC über globale und untergeordnete Domänen hinweg erläutert. Dabei wird die Möglichkeit geboten, den Zugriff zwischen Domänen einzuschränken und den globalen Domänenzugriff für bestimmte Benutzer einzuschränken. Cisco FMC unterstützt die präzise Zuweisung von Benutzerrollen über mehrere Domänen hinweg, wobei der Zugriff zwischen Domänen eingeschränkt werden kann. Die Konfiguration umfasst das Erstellen von Benutzern in bestimmten Domänen und das Zuweisen entsprechender Rollen zur Steuerung der Zugriffsebenen.

Benutzer- und Domänenzugriffsverhalten entwickeln

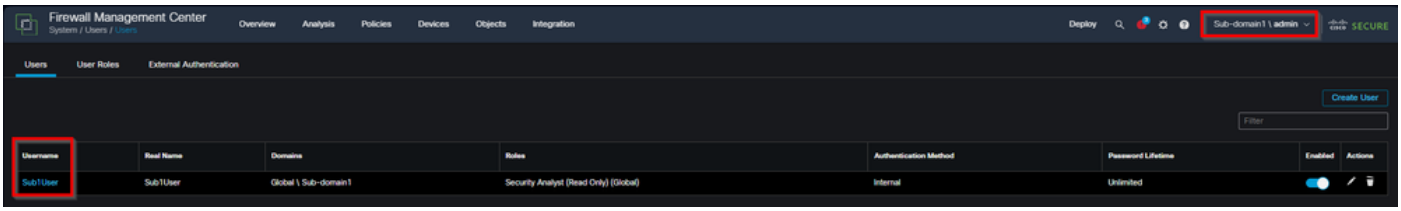
Das FMC-Benutzermanagementsystem funktioniert unterschiedlich, je nachdem, wo Benutzer erstellt werden:

In Unterdomänen erstellte Benutzer

- Direkt in einer Subdomäne erstellte Benutzer sind nur innerhalb der jeweiligen Domäne sichtbar:

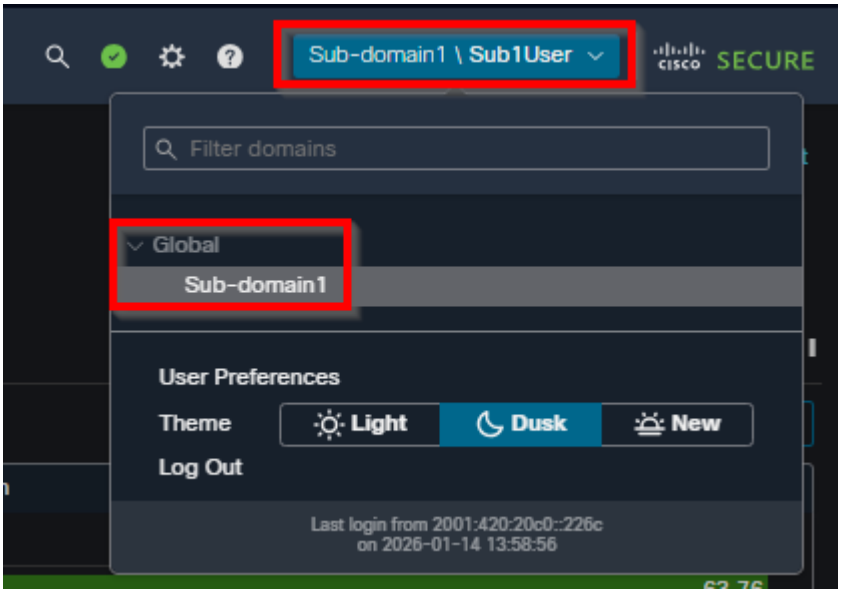


inline_image_0,png



inline_image_1.png

- Diese Benutzer müssen sich mit dem Domänenspezifikationsformat anmelden: subdomain\username.
- Der Zugriff wird automatisch auf die Domäne beschränkt, in der der Benutzer erstellt wurde:

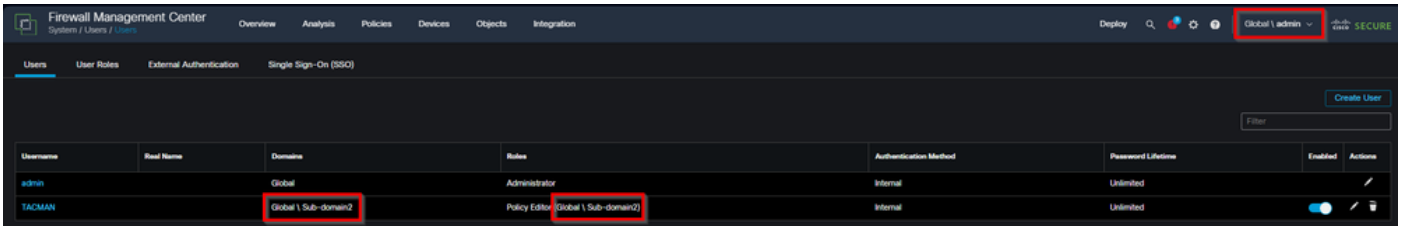


inline_image_2.png

- Benutzerdefinierte Rollen, die in der Unterdomäne erstellt wurden, gelten nur für diese Domäne.

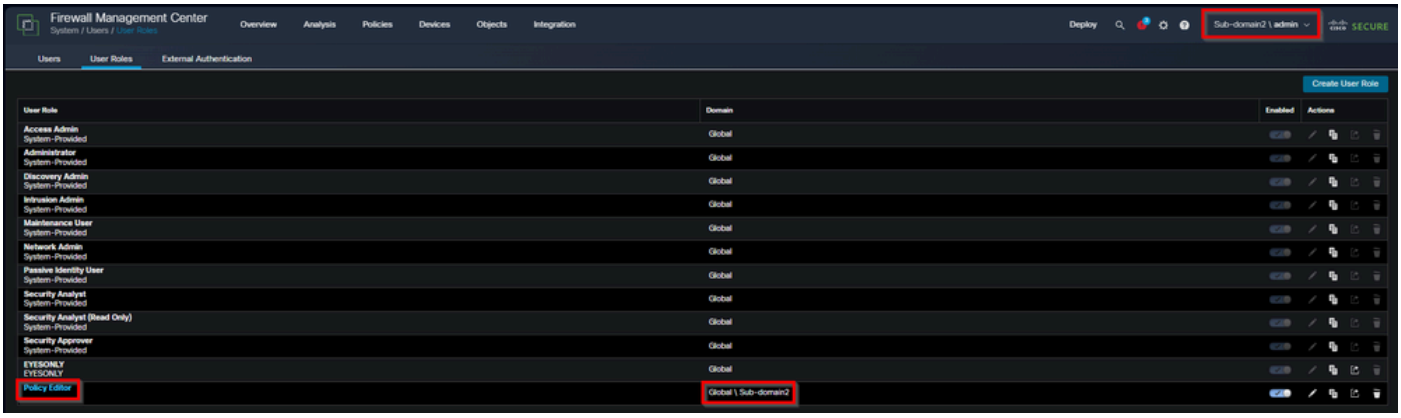
In globaler Domäne erstellte Benutzer:

- Benutzer, die von der globalen Domäne erstellt wurden, können sich nur mit ihrem Benutzernamen anmelden, auch wenn sich ihre Rollen nur in Subdomänen befinden.
- Diese Benutzer bleiben in der Liste der globalen Domänenbenutzer weiterhin sichtbar:



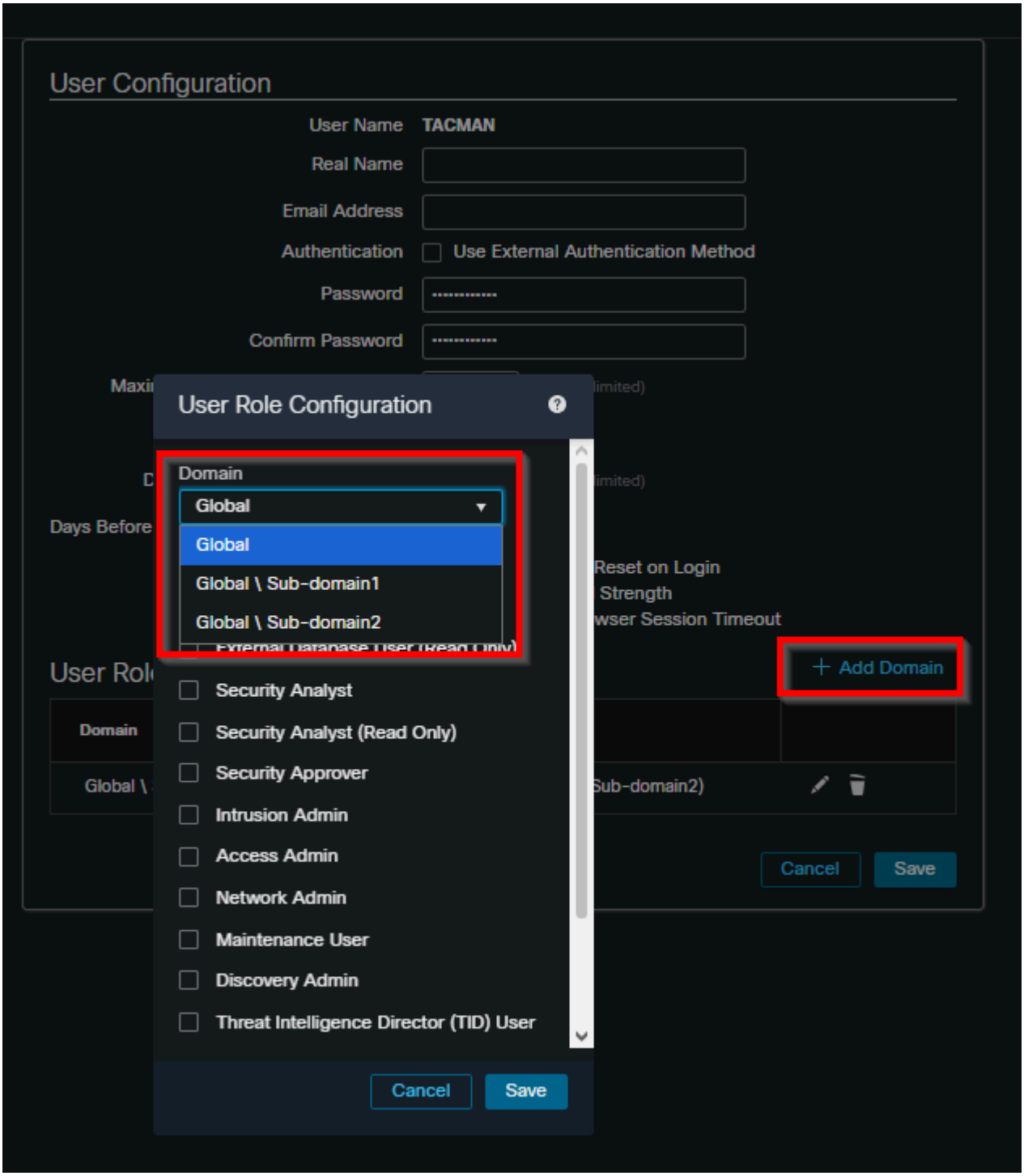
inline_image_3.png

- Rollenzuweisungen können für jede abhängige Domäne vorgenommen werden:



inline_image_4.png

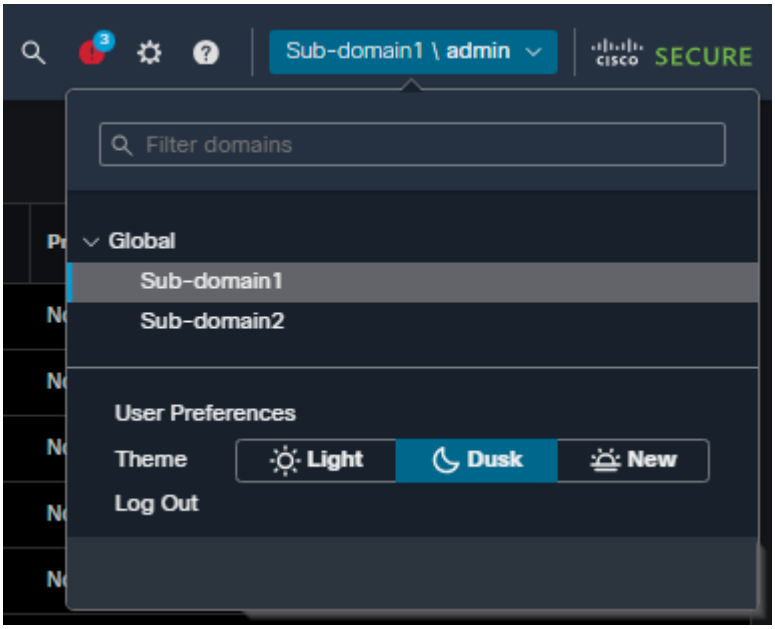
- Der Zugriff kann durch Rollenzuweisung auf bestimmte Sub-Domänen beschränkt werden:



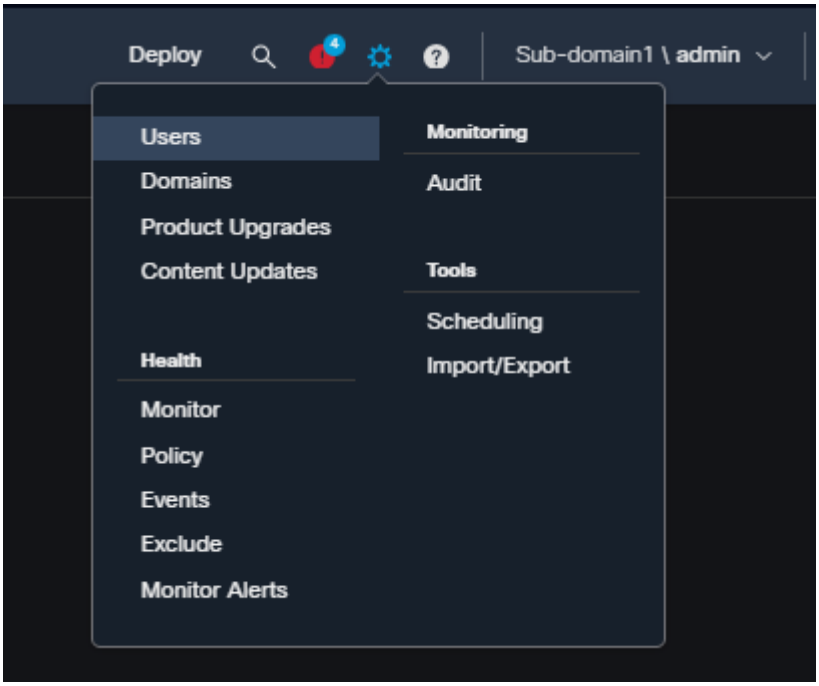
inline_image_5,png

Konfigurationsschritte für Unterdomänenbenutzerbeschränkung

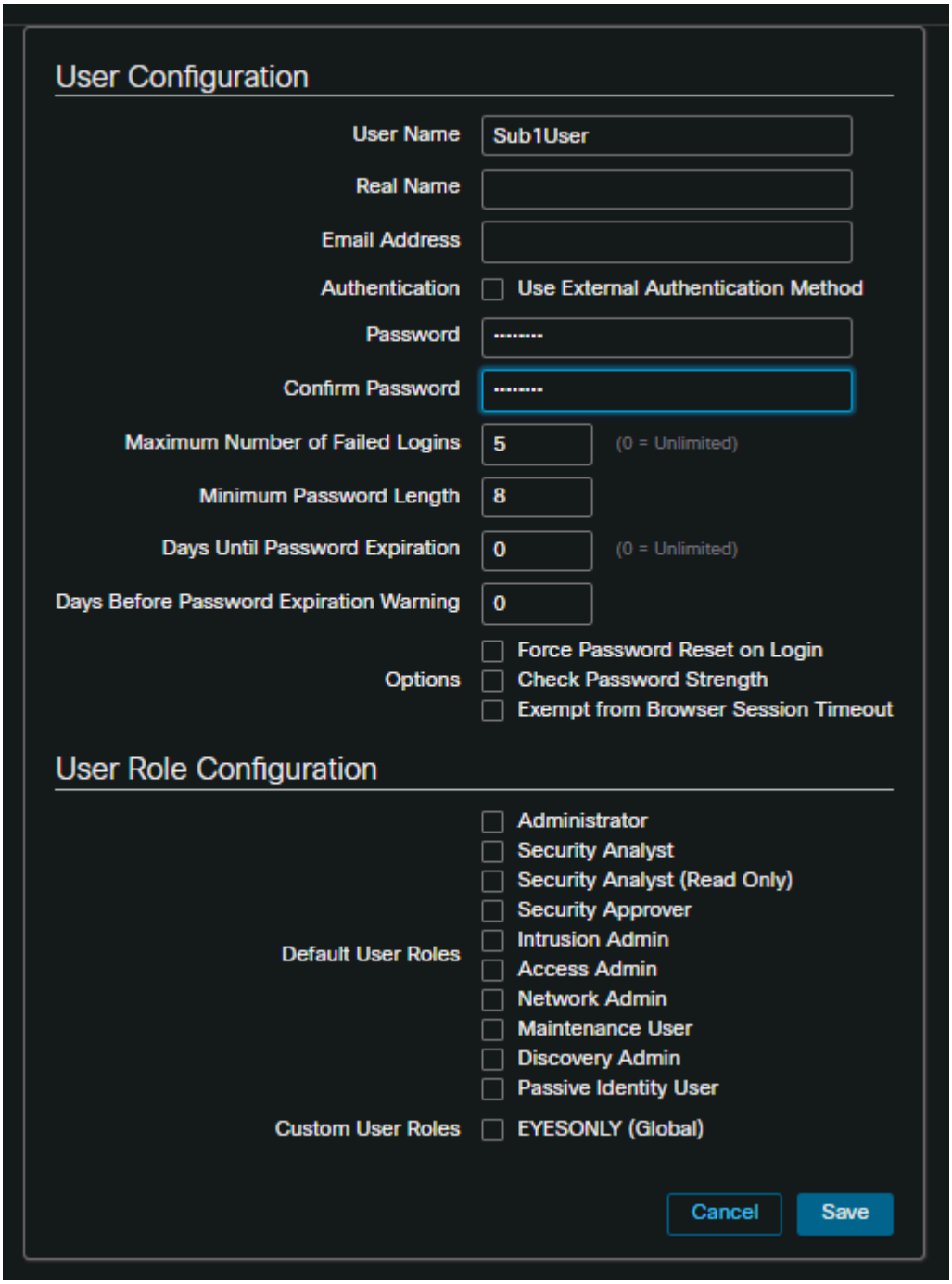
- Navigieren Sie zur jeweiligen Unterdomäne, in der der Zugriff eingeschränkt werden muss, und erstellen Sie das Benutzerkonto unter System / Users.



inline_image_6,png

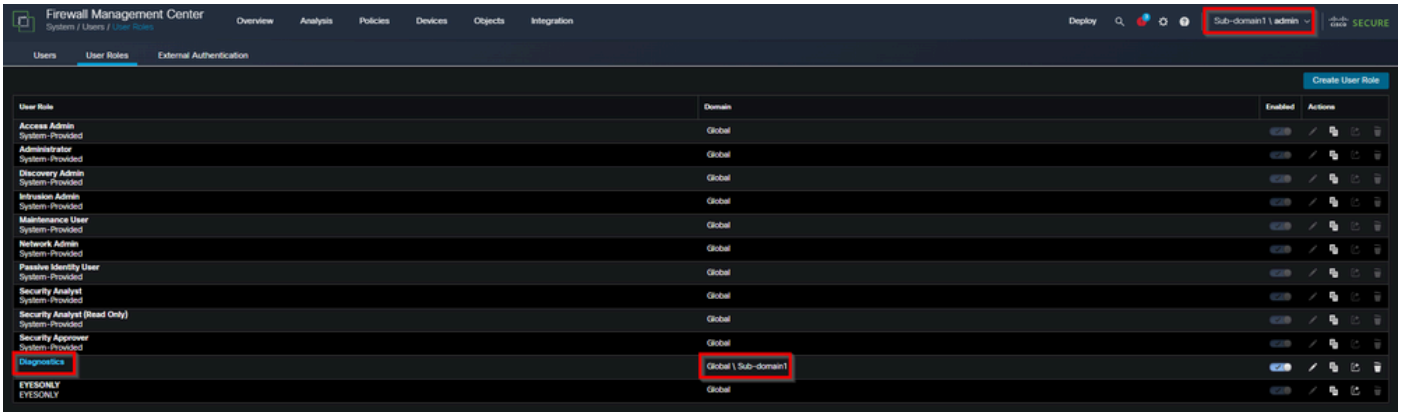


inline_image_7,png



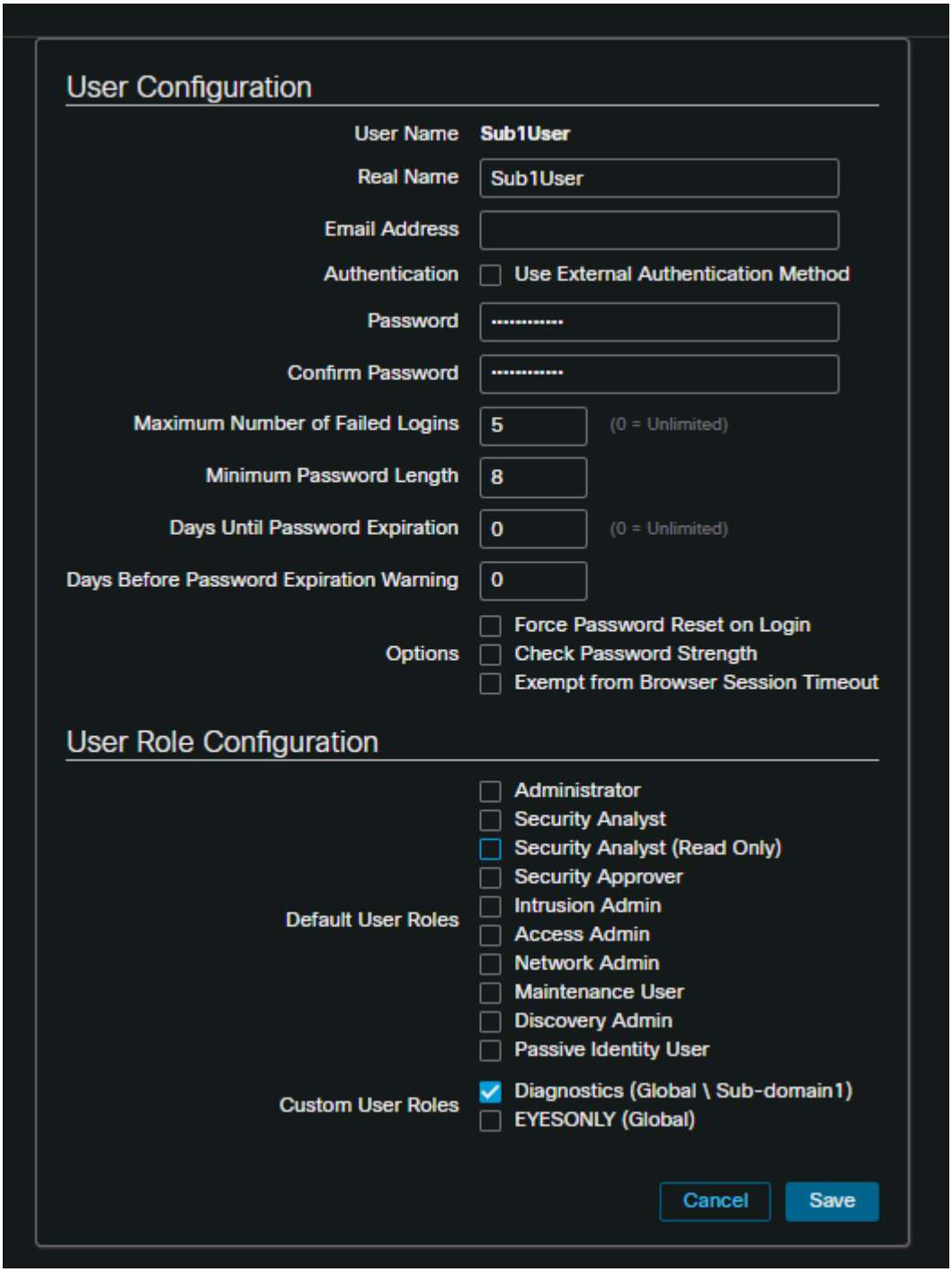
inline_image_8,png

- Erstellen Sie benutzerdefinierte Rollen in der Unterdomäne unter System/Benutzerrollen. Benutzerdefinierte Benutzerrollen, die in einer Unterdomäne erstellt wurden, sind nur innerhalb dieser Domäne verfügbar und können nicht von anderen Domänen aus aufgerufen werden.



inline_image_9.png

- Weisen Sie dem Benutzer die benutzerdefinierte Rolle zu. Der Benutzer erbt die Berechtigungen nur für die Domäne, in der sowohl der Benutzer als auch die Rolle erstellt wurden.



inline_image_10,png

- Benutzeranmeldeformat für Benutzer mit untergeordneten Domänen. Benutzer, die in untergeordneten Domänen erstellt wurden, müssen das folgende Anmeldeformat verwenden:

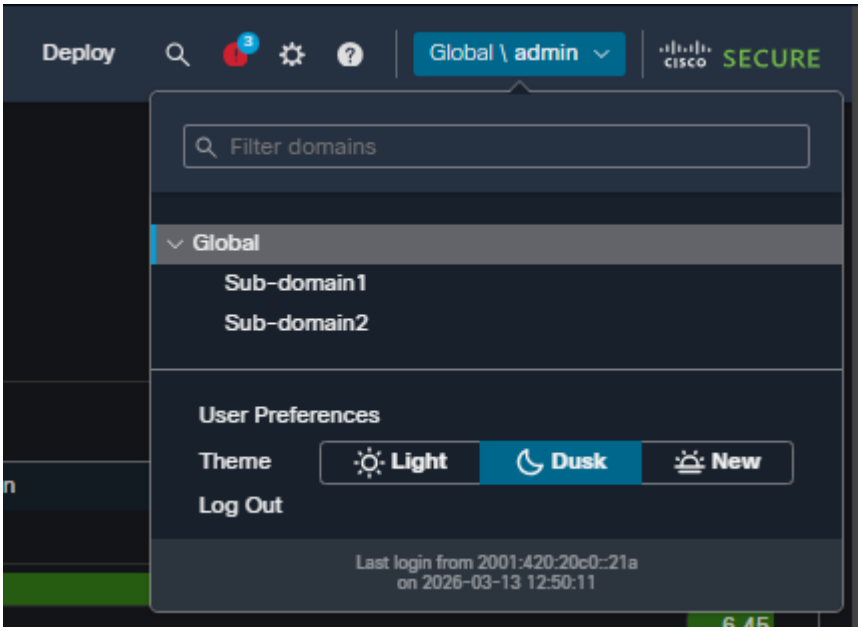
```
Benutzername: Sub-Domäne\Benutzername
```

```
Kennwort: [Benutzerkennwort]
```

inline_image_11,png

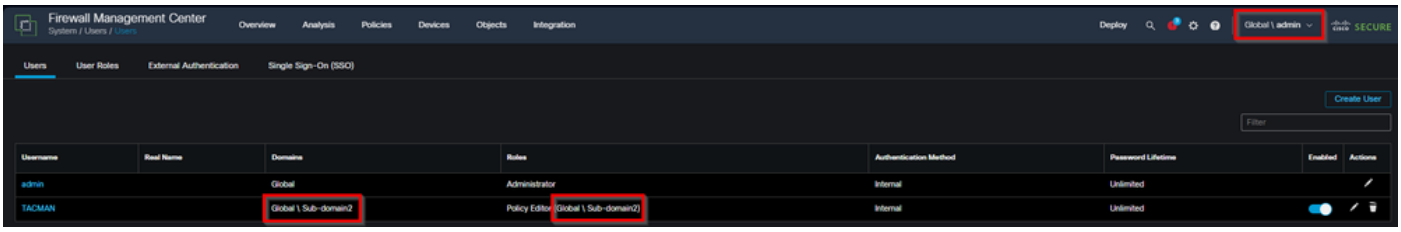
Konfigurationsschritte für globale Domänenbenutzer mit Unterdomäneneinschränkungen

- Erstellen Sie den Benutzer in der globalen Domäne unter System/Benutzer. Verwenden Sie ein Administratorkonto mit globalem Domänenzugriff, um den Benutzer zu erstellen.

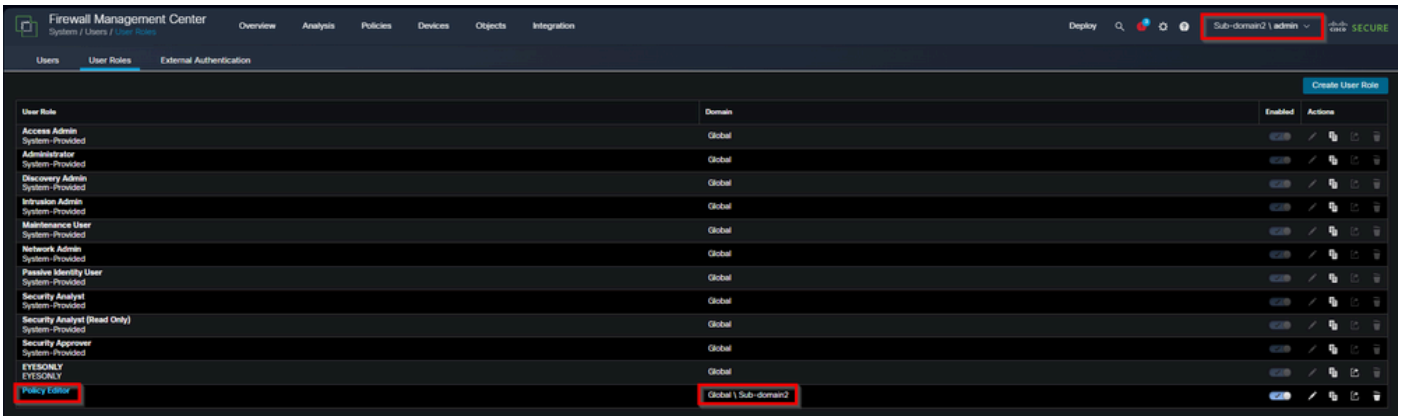


inline_image_12,png

- Weisen Sie unter "System/Benutzer" Rollen nur für bestimmte Unterdomänen zu. Weisen Sie in der Benutzerkonfiguration Rollen ausschließlich für die Ziel-Unterdomäne(n) zu, ohne globale Domänenberechtigungen bereitzustellen.



inline_image_3.png



inline_image_14.png

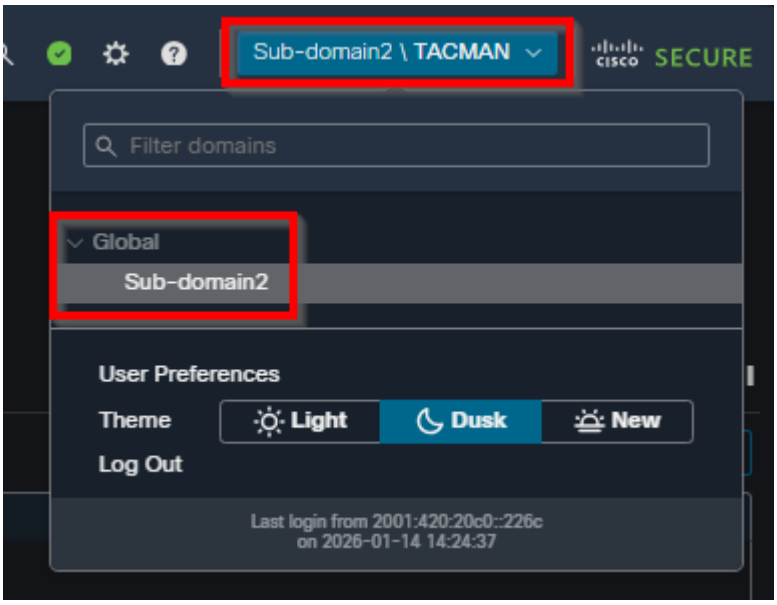
- Diese Benutzer können sich nur mit ihrem Benutzernamen ohne Domänenangabe anmelden:

```
Benutzername: Benutzername
```

```
Kennwort: [Benutzerkennwort]
```

inline_image_15,png

- Der Benutzer hat nur Zugriff auf die Subdomänen, denen spezifische Rollen zugewiesen wurden, ohne Zugriff auf die globale Domäne oder andere Subdomänen.



inline_image_16,png

Flexible Rollenzuweisung

Benutzer können über unterschiedliche Berechtigungen in jeder Domäne verfügen:

- Schreibgeschützte Berechtigungen in der globalen Domäne mit Administratorrechten in einer abhängigen Domäne
- Kein globaler Domänenzugriff mit vollständigen Administratorberechtigungen in bestimmten Unterdomänen
- Richtlinien-Editor-Berechtigungen in einer Unterdomäne ohne Zugriff auf andere Unterdomänen

Überlegungen externer Benutzer

Für externe Benutzer (LDAP- oder RADIUS-Authentifizierung):

- Wenn Benutzerrollen über Gruppenmitgliedschaften oder Benutzerattribute zugewiesen werden, können die Mindestzugriffsrechte nicht entfernt werden.
- Zusätzliche Rechte können in einem größeren Umfang zugewiesen werden als die Standardbenutzerrolle.
- Externe Authentifizierungsobjekte sind nur in der Domäne verfügbar, in der sie erstellt wurden.
- Einzelne Benutzerberechtigungen müssen in einem größeren Umfang konfiguriert werden als die Standardbenutzerrolle, um eine ordnungsgemäße Einschränkung zu erreichen.

Einschränkungen und Hinweise

- Benutzerdefinierte Benutzerrollen, die in Vorgängerdomänen erstellt wurden, können nicht in abhängigen Domänen bearbeitet werden.
- Die Shell-Authentifizierung ist nur in der globalen Domäne verfügbar, nicht in Subdomänen.
- Die Benutzereinstellungen und Dashboard-Einstellungen gelten für alle Domänen, auf die das Konto Zugriff hat.
- Berechtigungsänderungen für Benutzer werden einzeln konfiguriert und nicht in Gruppen oder in Sammelmethoden.

Ursache

Diese Anforderung ergibt sich aus der Notwendigkeit, eine präzise Zugriffskontrolle in FMC-Bereitstellungen mit mehreren Domänen zu implementieren, bei denen Benutzer unterschiedliche Zugriffsebenen für globale und untergeordnete Domänen benötigen, mit spezifischen Einschränkungen zwischen den Domänen, um Sicherheitsgrenzen zu wahren.

Verwandte Inhalte

- Cisco Secure Firewall Management Center Administration Guide, 7.6: Benutzer
- Cisco Secure Firewall Management Center Administration Guide, 7.6: Benutzerdefinierte Benutzerrollen erstellen
- Cisco Secure Firewall Management Center Administration Guide, 7.6: Hinzufügen oder Bearbeiten eines internen Benutzers
- Cisco Secure Firewall Management Center Administration Guide, 7.6: Benutzer und Domänen
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.