Configura dominio &FMC e ruolo utente

Problema

In questo documento viene descritto come configurare autorizzazioni utente diverse per più utenti in FMC in domini globali e secondari.

Ambiente

- Cisco Secure Firewall Management Center (FMC) - 7.6.4 (applicabile a tutti i FMC)
- Distribuzione multidominio con dominio globale e sottodomini
- Più dispositivi FTD assegnati a sottodomini diversi
- Più utenti che richiedono livelli di autorizzazione diversi

Risoluzione

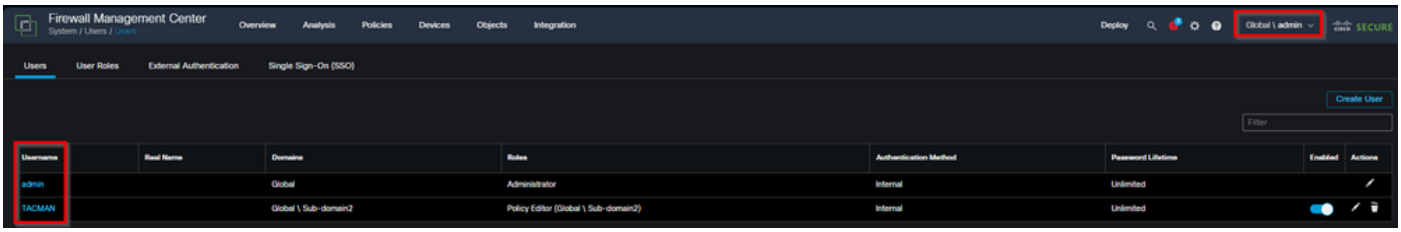
In questo documento viene descritto come configurare autorizzazioni utente diverse per più utenti in FMC in domini globali e sottodomini, con la possibilità di limitare l'accesso tra domini e l'accesso al dominio globale per utenti specifici. Cisco FMC supporta l'assegnazione granulare dei ruoli utente in più domini, con la possibilità di limitare l'accesso tra domini. La configurazione prevede la creazione di utenti in domini specifici e l'assegnazione di ruoli appropriati per il controllo dei livelli di accesso.

Creazione del comportamento di accesso utente e dominio

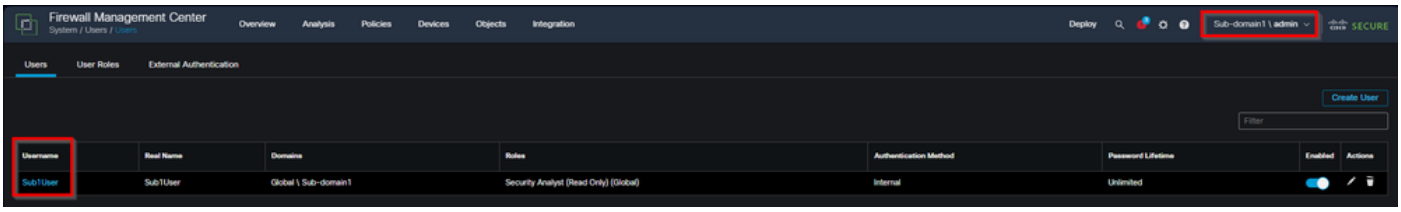
Il sistema di gestione degli utenti di FMC funziona in modo diverso in base al luogo di creazione degli utenti:

Utenti creati nei sottodomini

- Gli utenti creati direttamente in un sottodominio sono visibili solo all'interno del dominio specifico:

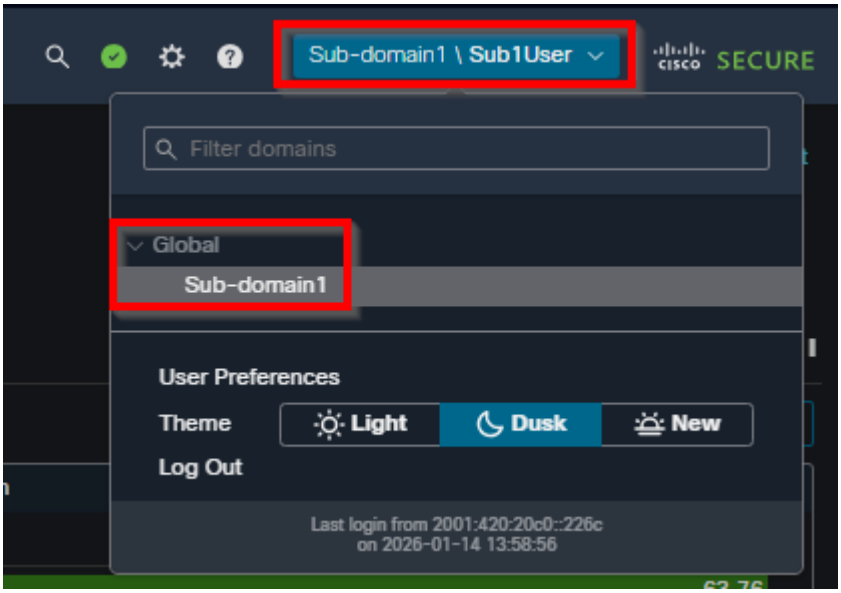


inline_image_0.png



inline_image_1.png

- Questi utenti devono eseguire l'accesso utilizzando il formato di specifica del dominio: sottodominio omeutente.
- L'accesso viene limitato automaticamente al dominio in cui è stato creato l'utente:



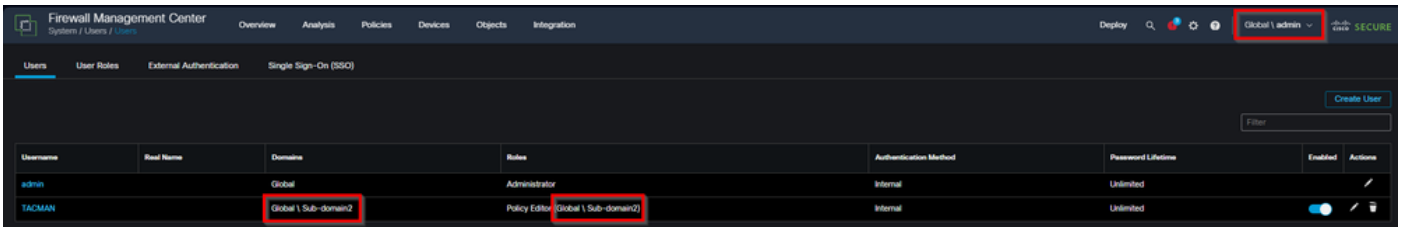
inline_image_2.png

- I ruoli personalizzati creati nel sottodominio si applicano solo a tale dominio.

Utenti creati nel dominio globale:

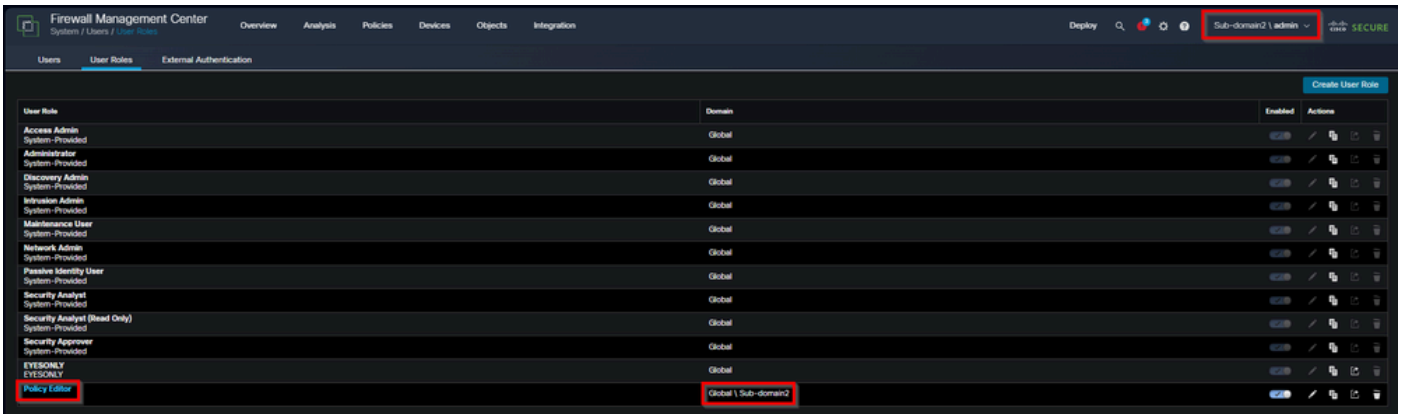
- Gli utenti creati dal dominio globale possono eseguire l'accesso solo con il proprio nome utente, anche se i loro ruoli si trovano solo nei sottodomini.

- Questi utenti rimangono visibili nell'elenco degli utenti del dominio globale:



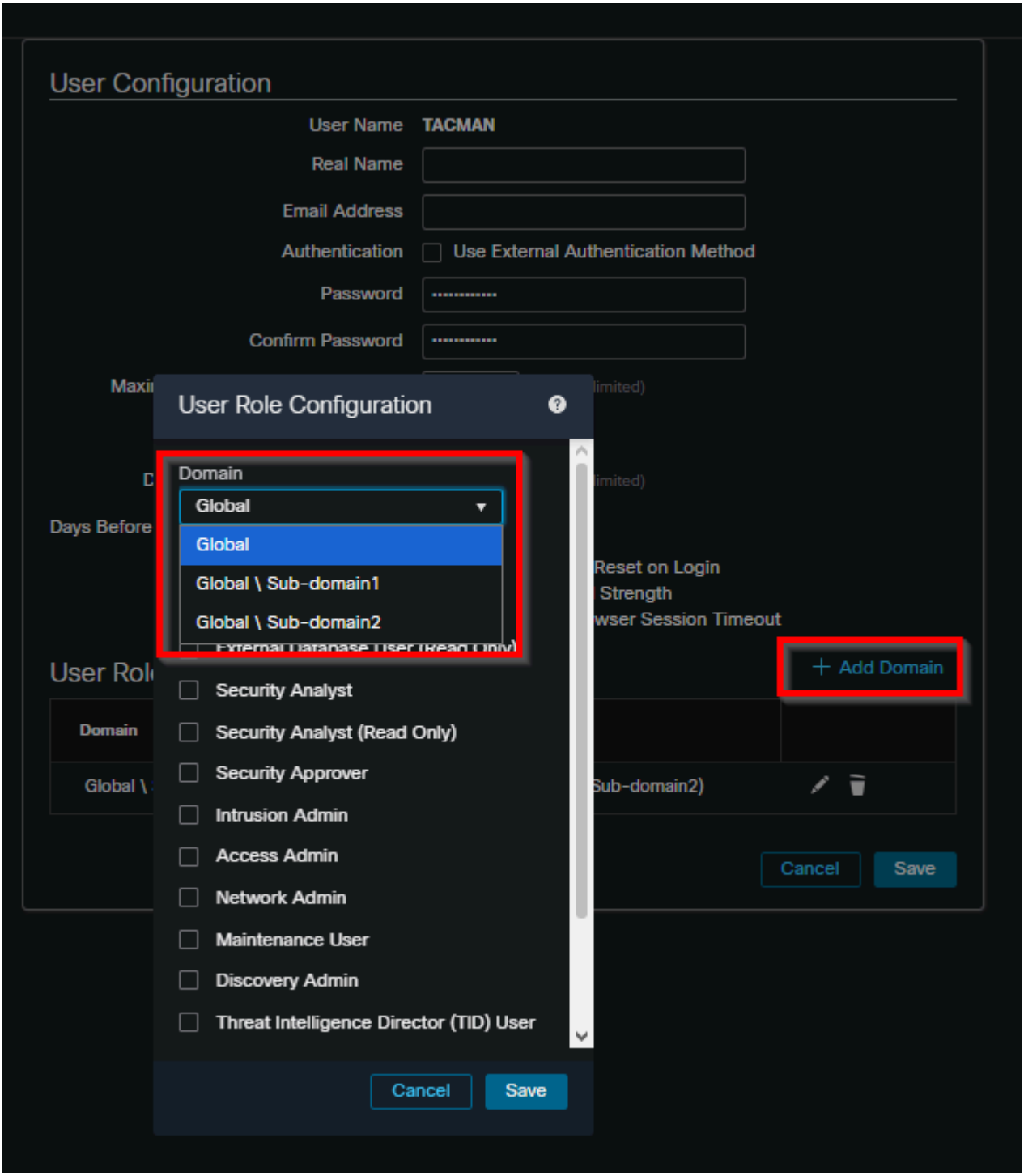
inline_image_3.png

- Le assegnazioni di ruolo possono essere effettuate per qualsiasi dominio discendente:



inline_image_4.png

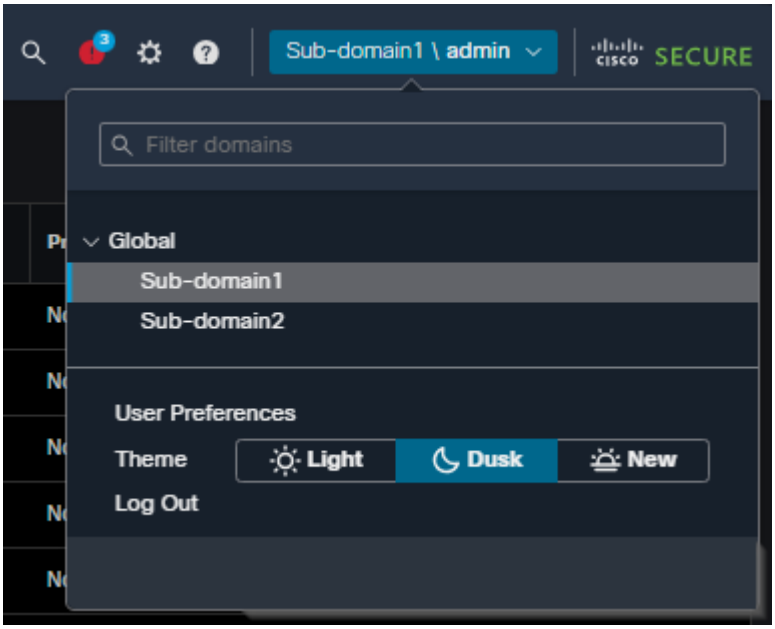
- L'accesso può essere limitato a sottodomini specifici tramite l'assegnazione dei ruoli:



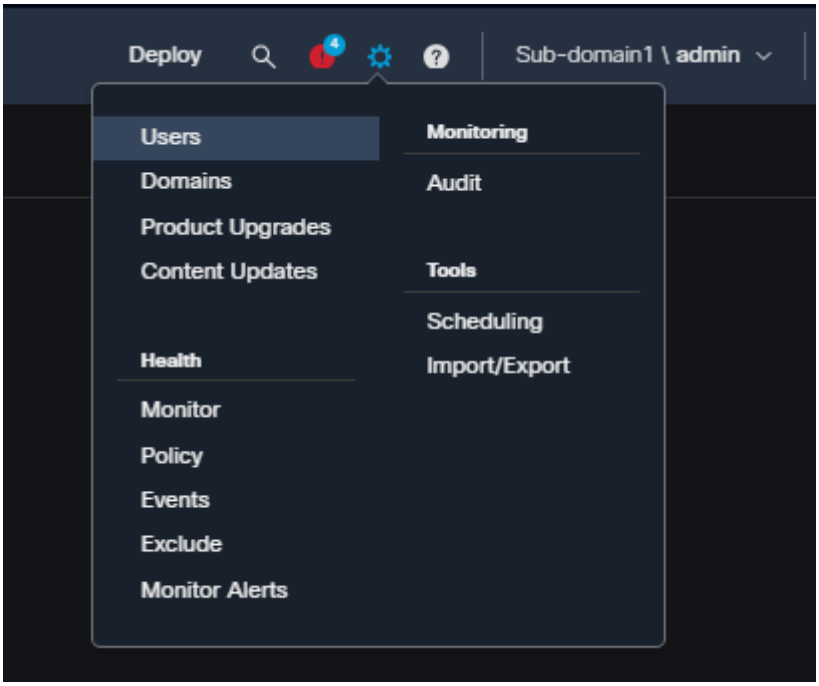
inline_image_5.png

Procedura di configurazione per la limitazione degli utenti del sottodominio

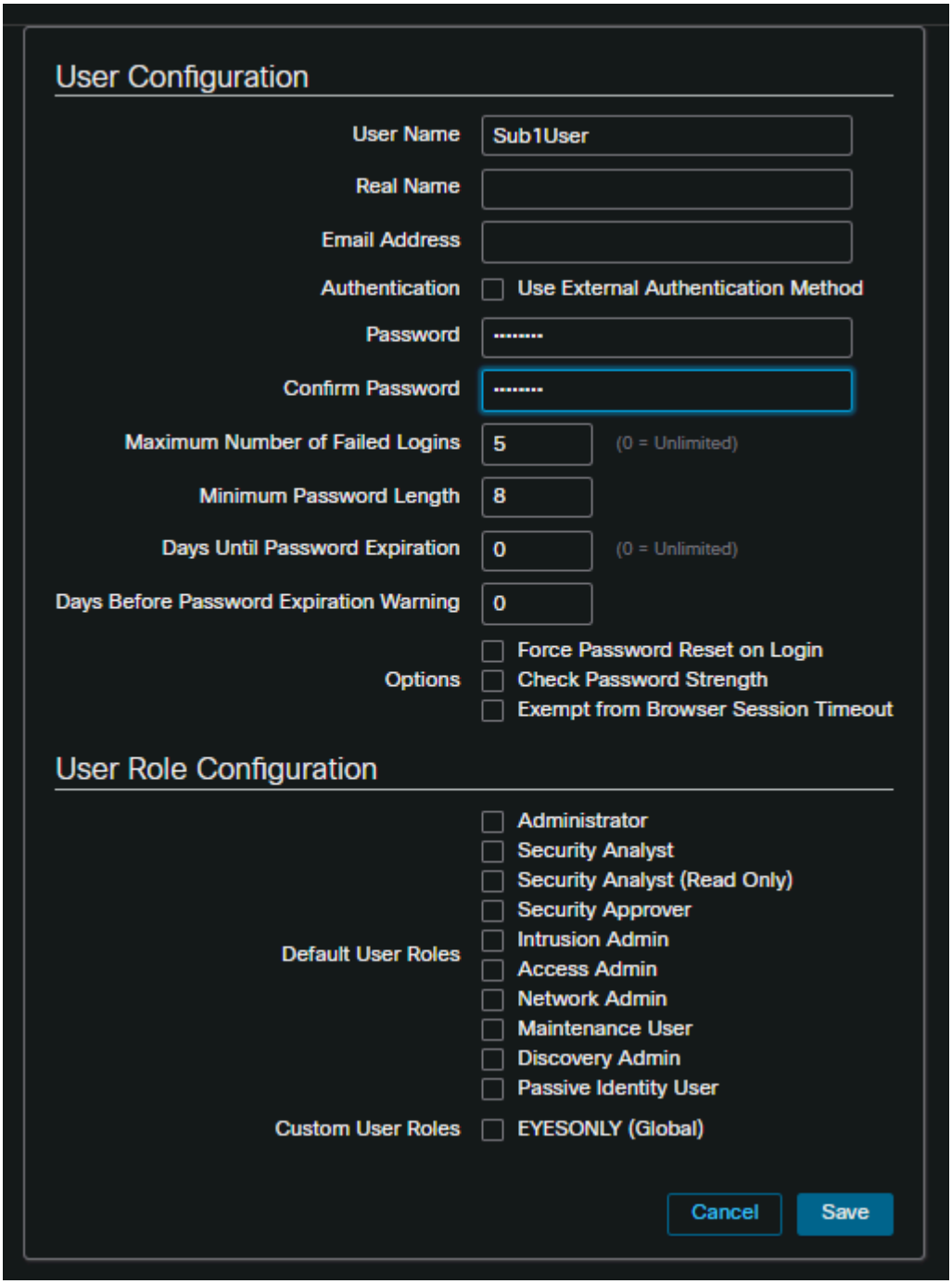
- Passare al sottodominio specifico in cui l'accesso deve essere limitato e creare l'account utente in Sistema/Utenti.



inline_image_6.png

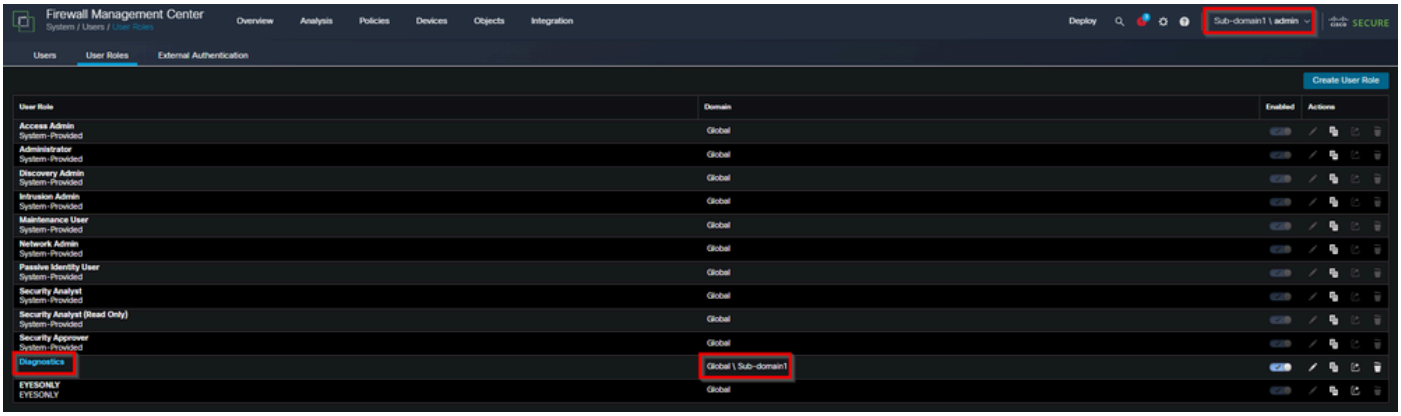


inline_image_7.png



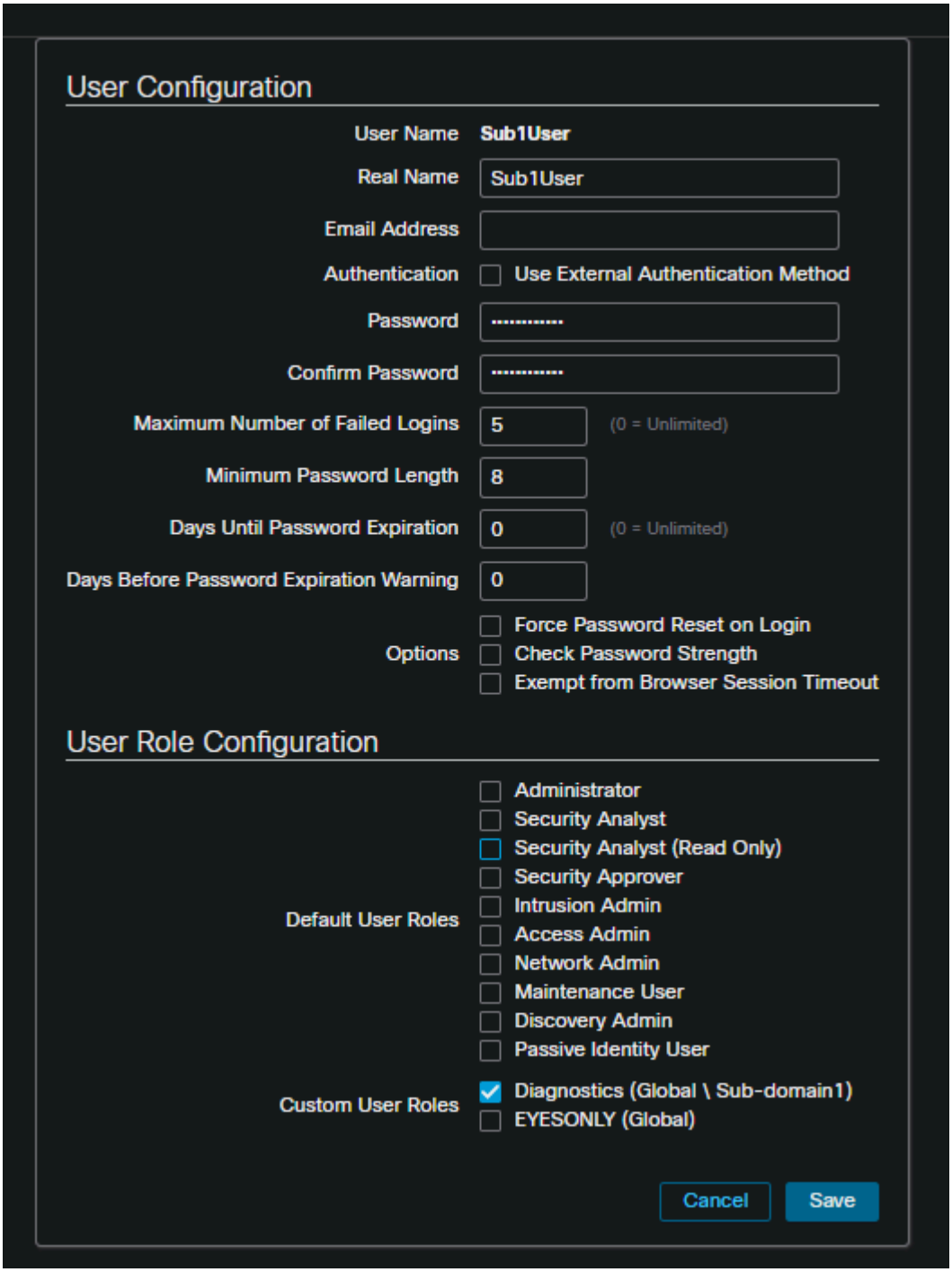
inline_image_8.png

- Creare ruoli personalizzati all'interno del sottodominio in Ruoli utente/di sistema. I ruoli utente personalizzati creati in un sottodominio sono disponibili solo all'interno di tale dominio e non sono accessibili da altri domini.



inline_image_9.png

- Assegnare il ruolo personalizzato all'utente. L'utente eredita le autorizzazioni solo per il dominio in cui sono stati creati sia l'utente che il ruolo.



inline_image_10.png

- Formato di accesso utente per gli utenti del sottodominio. Gli utenti creati nei sottodomini devono utilizzare il seguente formato di accesso:

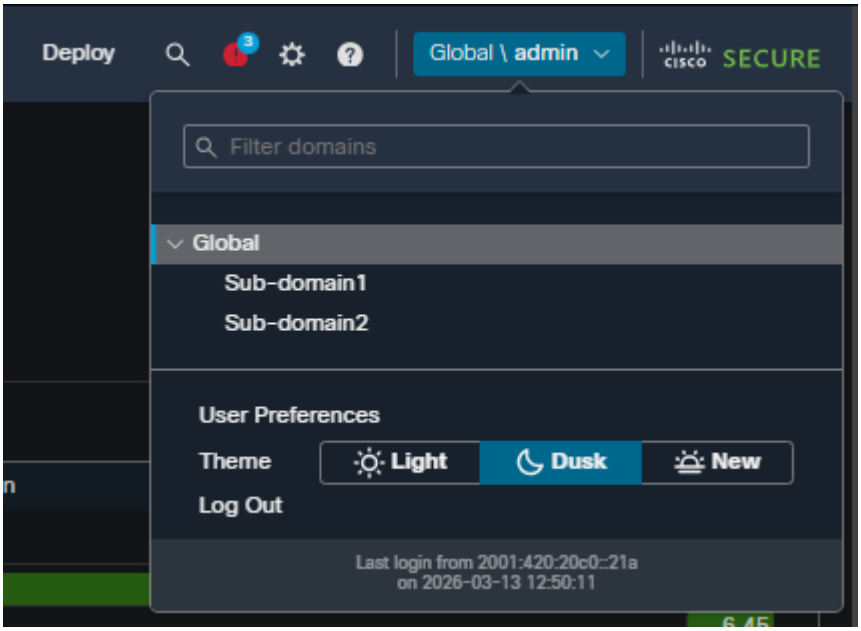
```
Nome utente: Sottodominio\nomeutente
```

```
Password: [password utente]
```

inline_image_11.png

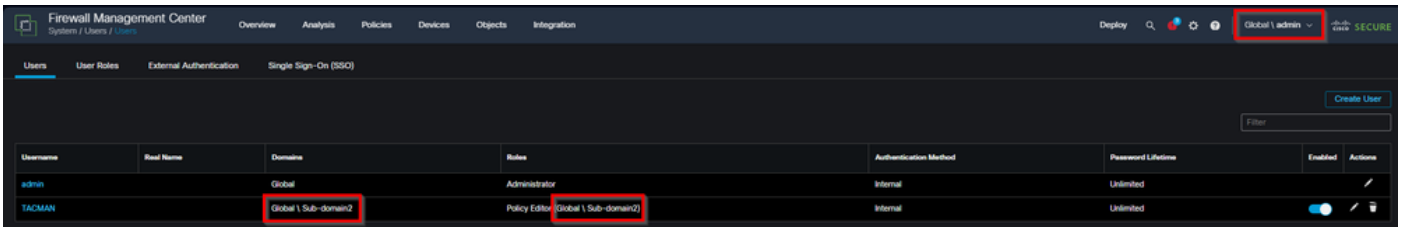
Procedura di configurazione per gli utenti del dominio globale con restrizioni per i sottodomini

- Creare l'utente nel dominio globale in Sistema/Utenti. Utilizzare un account amministrativo con accesso al dominio globale per creare l'utente.

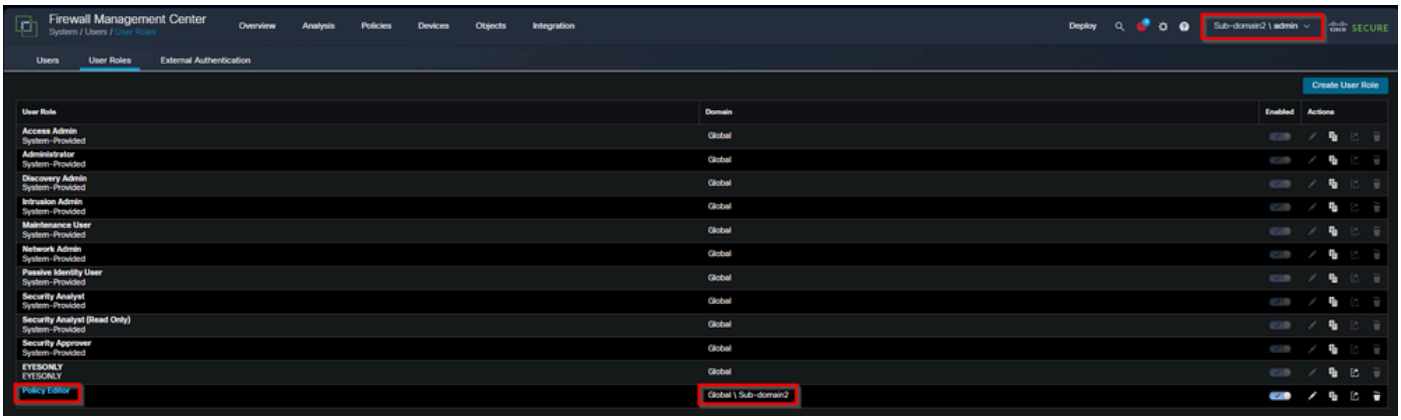


inline_image_12.png

- Assegnare i ruoli solo per sottodomini specifici in Sistema/Utenti. Nella configurazione utente, assegnare i ruoli esclusivamente per i sottodomini di destinazione senza fornire alcuna autorizzazione di dominio globale.



inline_image_3.png



inline_image_14.png

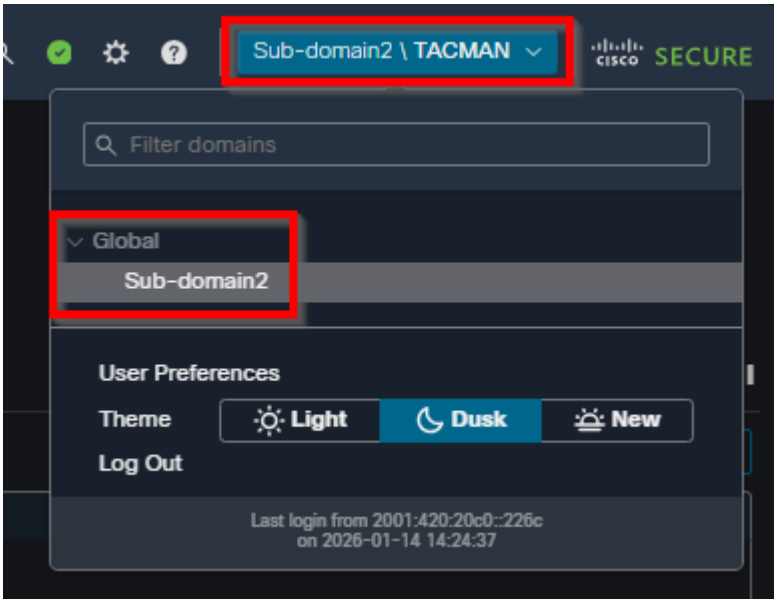
- Questi utenti possono eseguire l'accesso solo con il proprio nome utente, senza specificare il dominio:

```
Nome utente: username
```

```
Password: [password utente]
```

inline_image_15.png

- L'utente ha accesso solo ai sottodomini a cui sono stati assegnati ruoli, senza accesso al dominio globale o ad altri sottodomini.



inline_image_16.png

Flessibilità di assegnazione dei ruoli

Gli utenti possono disporre di privilegi diversi in ogni dominio:

- Privilegi di sola lettura nel dominio globale con privilegi di amministratore in un dominio discendente
- Nessun accesso al dominio globale con autorizzazioni di amministratore complete in sottodomini specifici
- Autorizzazioni Editor criteri in un sottodominio senza accesso ad altri sottodomini

Considerazioni sugli utenti esterni

Per gli utenti esterni (autenticazione LDAP o RADIUS):

- Se i ruoli utente vengono assegnati tramite l'appartenenza ai gruppi o gli attributi utente, non è possibile rimuovere i diritti di accesso minimi.
- È possibile assegnare diritti aggiuntivi a un ambito più ampio del ruolo utente predefinito.
- Gli oggetti di autenticazione esterna sono disponibili solo nel dominio in cui sono stati creati.
- Per impostare le restrizioni appropriate, è necessario configurare le autorizzazioni dei singoli utenti in un ambito superiore a quello del ruolo Utente predefinito.

Limitazioni e considerazioni

- I ruoli utente personalizzati creati nei domini predecessori non possono essere modificati dai domini discendenti.
- L'autenticazione della shell è disponibile solo nel dominio globale e non nei sottodomini.
- Le preferenze utente e le impostazioni del dashboard si applicano a tutti i domini a cui l'account ha accesso.
- Le modifiche delle autorizzazioni per gli utenti vengono configurate singolarmente e non in gruppi o in modalità bulk.

Causa

Il requisito deriva dalla necessità di implementare il controllo granulare dell'accesso in installazioni FMC multidominio in cui gli utenti richiedono diversi livelli di accesso ai domini globali e secondari, con restrizioni specifiche tra i domini per mantenere i limiti di sicurezza.

Contenuto correlato

- Cisco Secure Firewall Management Center Administration Guide, 7.6: Utenti
- Cisco Secure Firewall Management Center Administration Guide, 7.6: Crea ruoli utente personalizzati
- Cisco Secure Firewall Management Center Administration Guide, 7.6: Aggiungere o modificare un utente interno
- Cisco Secure Firewall Management Center Administration Guide, 7.6: Utenti e domini
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).