Configurer le domaine FMC Accès utilisateur et rôle

Problème

Ce document décrit comment configurer différentes autorisations d'utilisateur pour plusieurs utilisateurs dans FMC à travers Global et sous-domaines.

Environnement

- Cisco Secure Firewall Management Center (FMC) - 7.6.4 (applicable à tous les FMC)
- Déploiement multidomaine avec domaine global et sous-domaines
- Plusieurs périphériques FTD attribués à différents sous-domaines
- Plusieurs utilisateurs nécessitant différents niveaux d'autorisation

Résolution

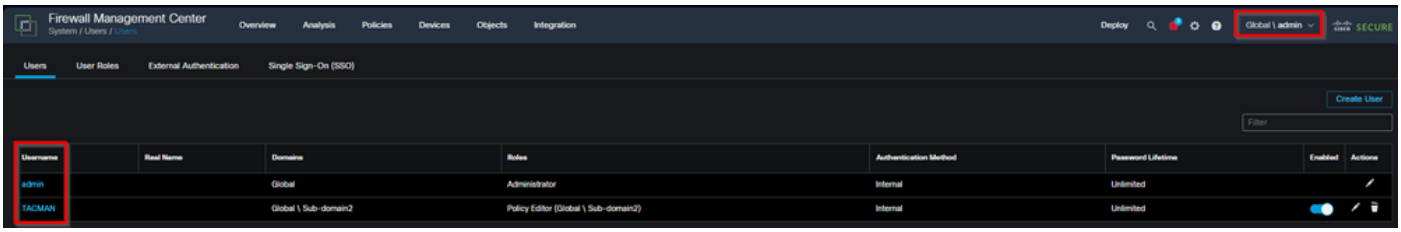
Ce document explique comment configurer différentes autorisations d'utilisateur pour plusieurs utilisateurs dans FMC à travers Global et sous-domaines, avec la possibilité de restreindre l'accès entre les domaines et de limiter l'accès au domaine Global pour des utilisateurs spécifiques. Cisco FMC prend en charge l'attribution granulaire de rôles d'utilisateur à travers plusieurs domaines avec la possibilité de restreindre l'accès entre les domaines. La configuration implique la création d'utilisateurs dans des domaines spécifiques et l'attribution de rôles appropriés pour contrôler les niveaux d'accès.

Créer un comportement d'accès utilisateur et domaine

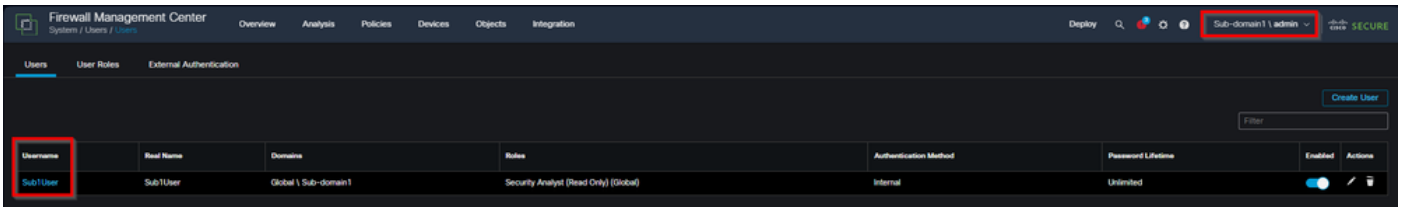
Le système de gestion des utilisateurs FMC fonctionne différemment en fonction de l’endroit où les utilisateurs sont créés :

Utilisateurs créés dans des sous-domaines

- Les utilisateurs créés directement dans un sous-domaine ne sont visibles que dans le domaine spécifique :

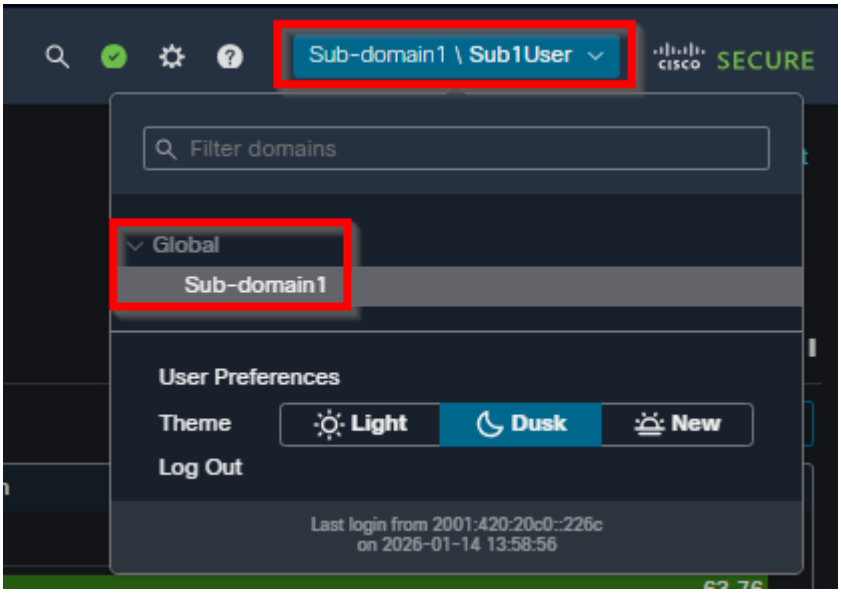


image_en_ligne_0.png



image_inline_1.png

- Ces utilisateurs doivent se connecter en utilisant le format de spécification de domaine : subdomain\username.
- L'accès est automatiquement limité au domaine dans lequel l'utilisateur a été créé :

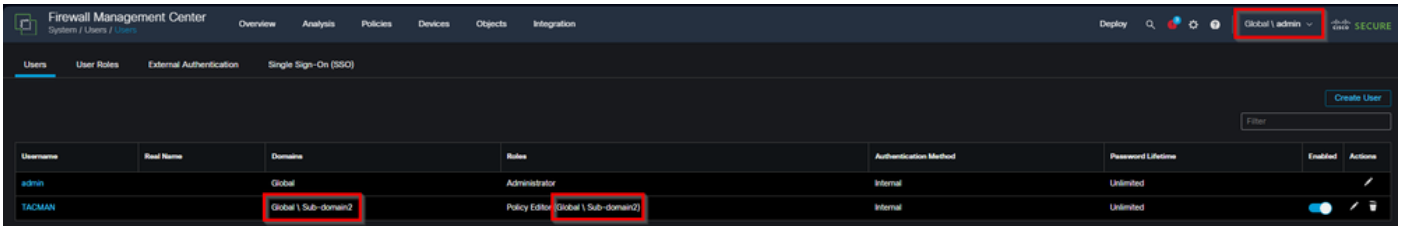


image_en_ligne_2.png

- Les rôles personnalisés créés dans le sous-domaine s'appliquent uniquement à ce domaine.

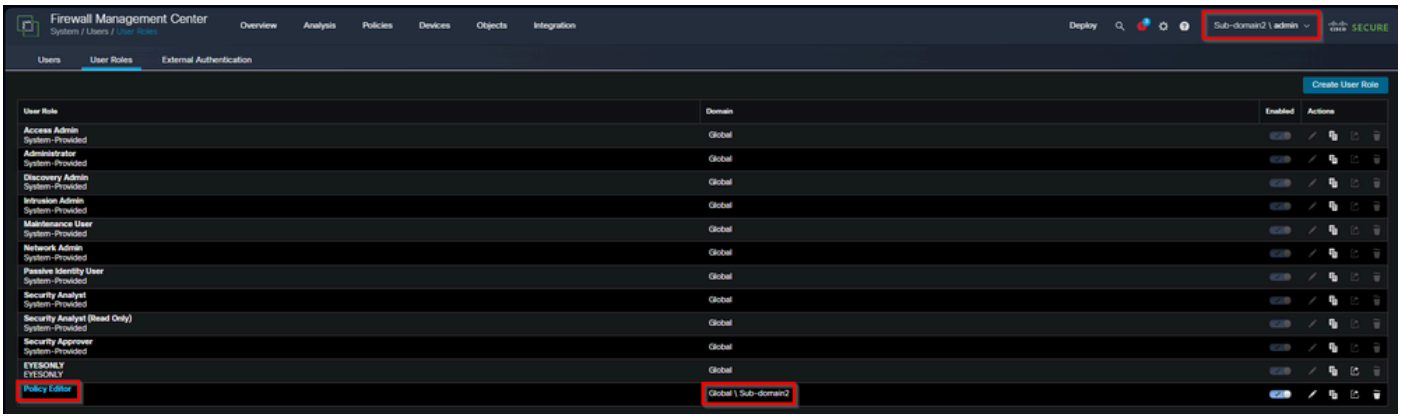
Utilisateurs créés dans le domaine global :

- Les utilisateurs créés à partir du domaine global peuvent se connecter uniquement avec leur nom d'utilisateur, même si leurs rôles se trouvent uniquement dans des sous-domaines.
- Ces utilisateurs restent visibles dans la liste globale des utilisateurs du domaine :



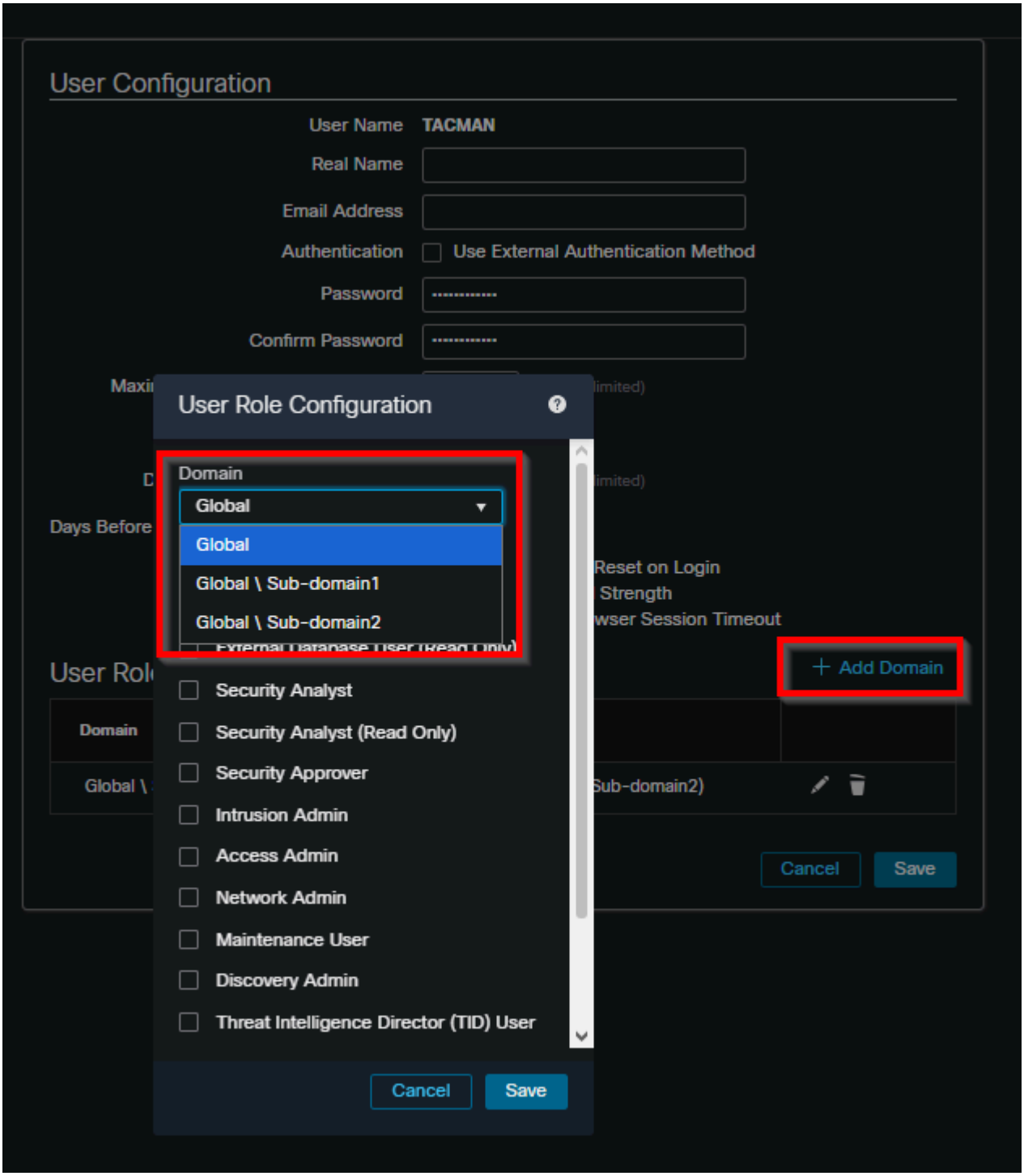
image_en_ligne_3.png

- Les attributions de rôles peuvent être effectuées pour n'importe quel domaine descendant :



image_en_ligne_4.png

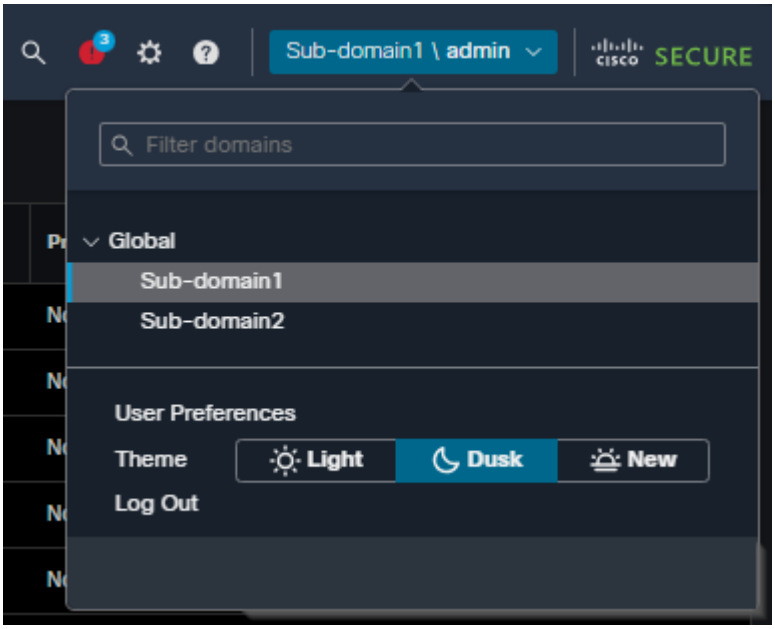
- L'accès peut être limité à des sous-domaines spécifiques par l'attribution de rôles :



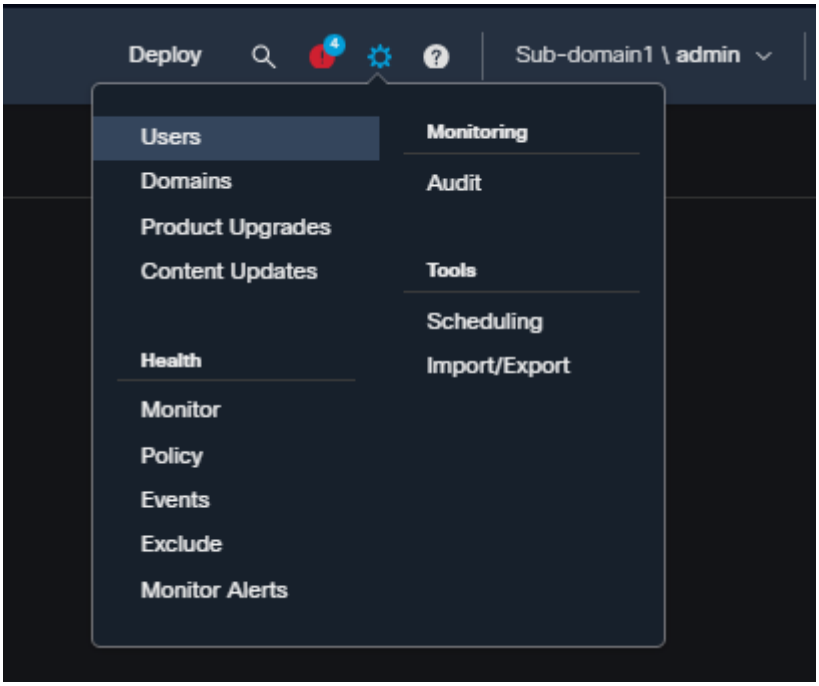
image_inline_5.png

Étapes de configuration de la restriction utilisateur de sous-domaine

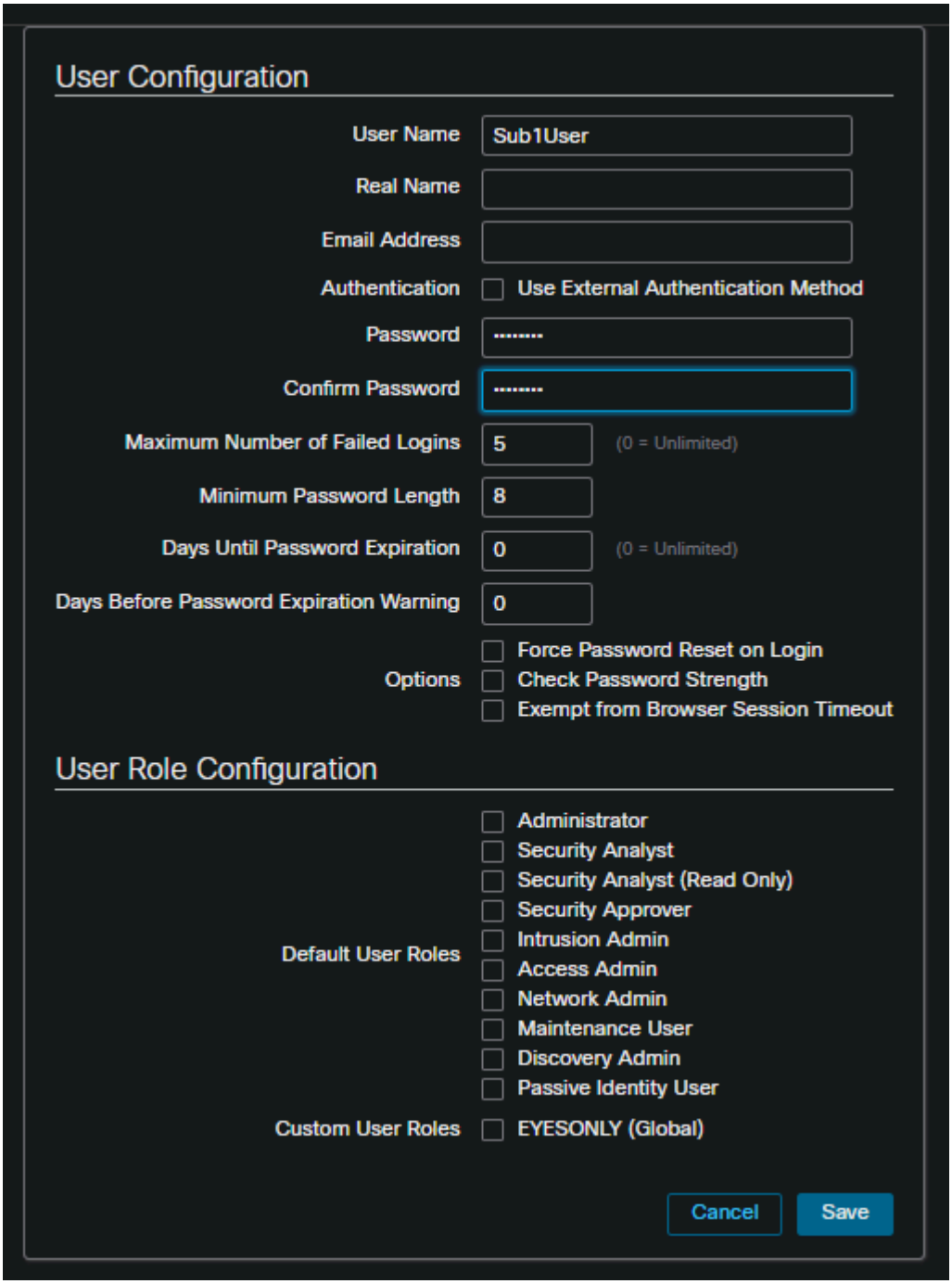
- Accédez au sous-domaine spécifique où l'accès doit être restreint et créez le compte d'utilisateur sous Système / Utilisateurs.



image_inline_6.png

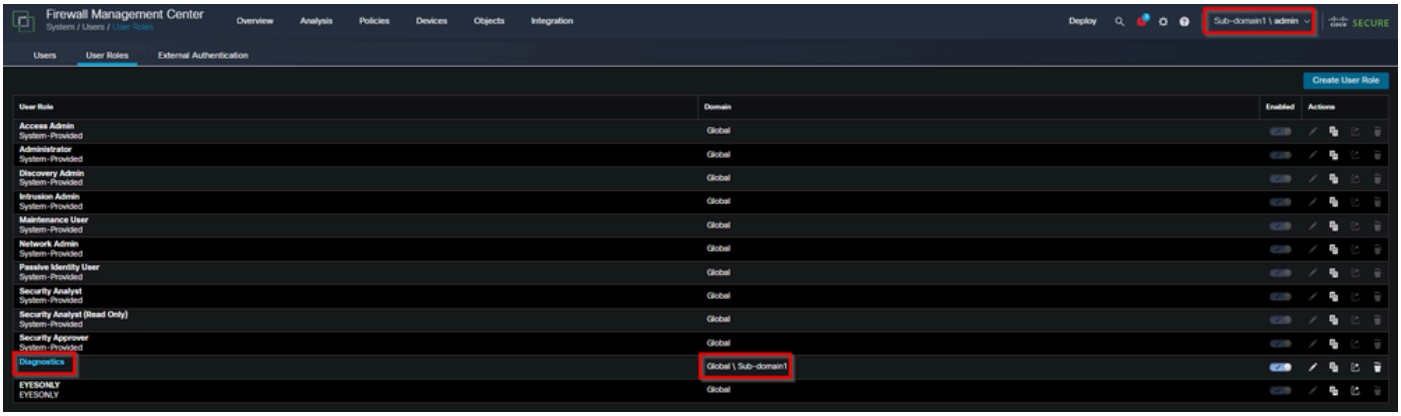


image_en_ligne_7.png



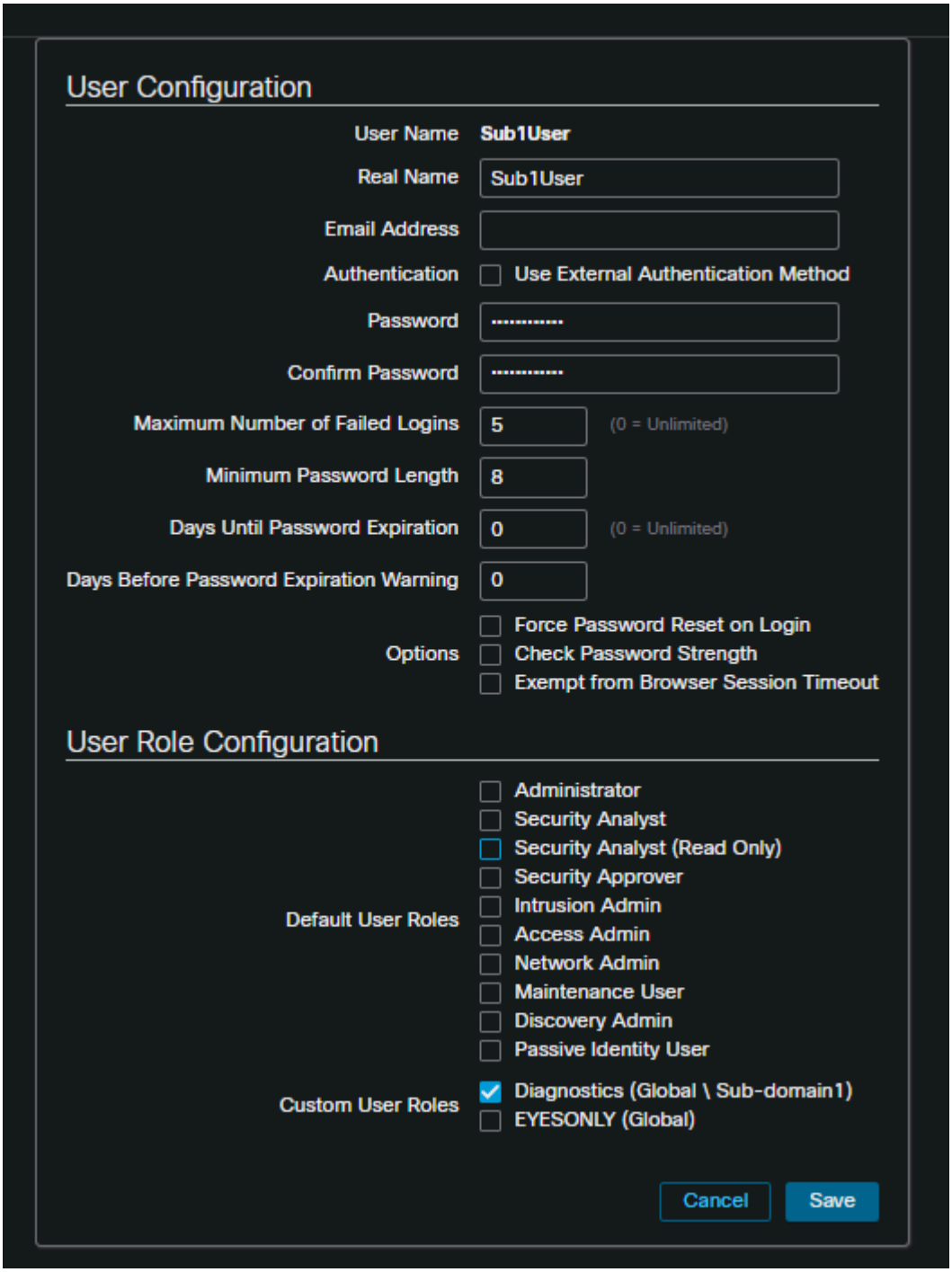
image_en_ligne_8.png

- Créez des rôles personnalisés dans le sous-domaine sous Rôles système / utilisateur. Les rôles d'utilisateur personnalisés créés dans un sous-domaine sont uniquement disponibles dans ce domaine et ne sont pas accessibles à partir d'autres domaines.



image_en_ligne_9.png

- Attribuez le rôle personnalisé à l'utilisateur. L'utilisateur hérite des autorisations uniquement pour le domaine dans lequel l'utilisateur et le rôle ont été créés.



image_inline_10.png

- Format de connexion utilisateur pour les utilisateurs de sous-domaines. Les utilisateurs créés dans des sous-domaines doivent utiliser le format de connexion suivant :

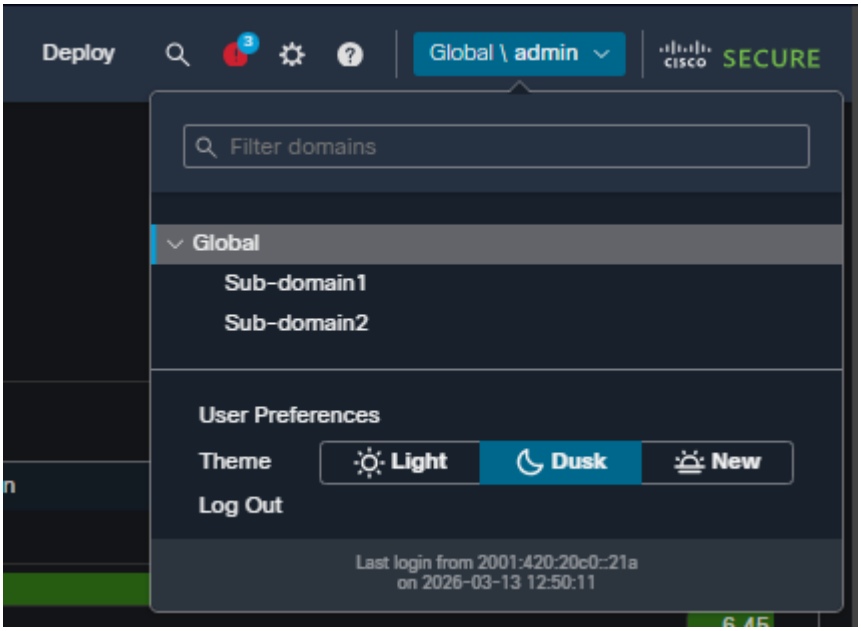
```
Nom d'utilisateur : Sous-domaine\nom d'utilisateur
```

```
Mot de passe : [user password]
```

image_inline_11.png

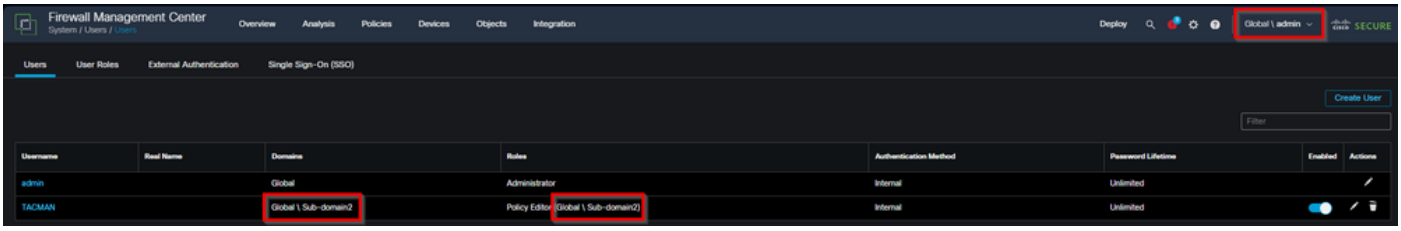
Étapes de configuration pour les utilisateurs du domaine global avec restrictions de sous-domaine

- Créez l'utilisateur dans le domaine global sous Système / Utilisateurs. Utilisez un compte d'administrateur avec un accès au domaine global pour créer l'utilisateur.

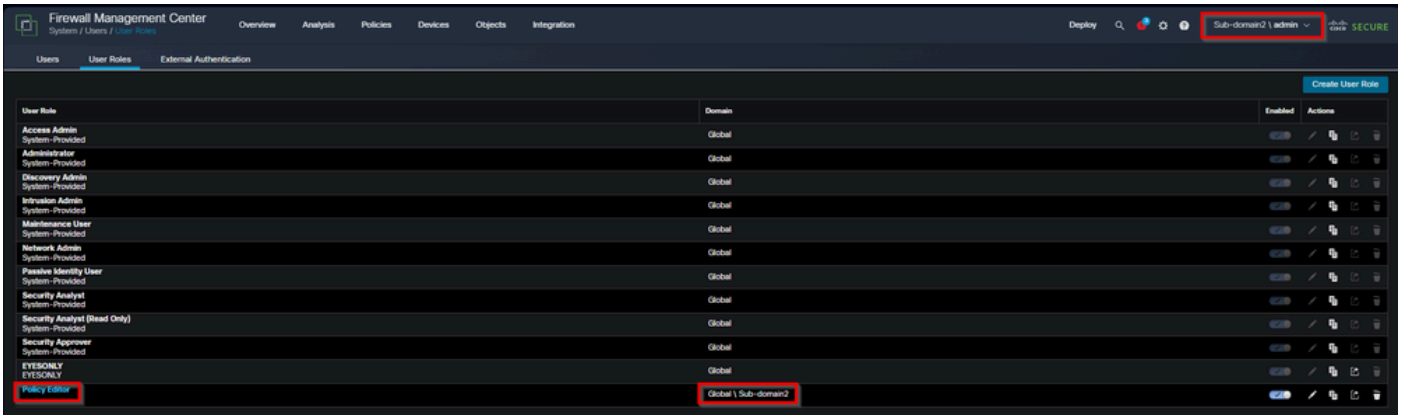


image_inline_12.png

- Affectez des rôles uniquement à des sous-domaines spécifiques sous Système / Utilisateurs. Dans la configuration utilisateur, affectez des rôles exclusivement aux sous-domaines cibles sans fournir d'autorisations de domaine globales.



image_en_ligne_3.png



inline_image_14.png

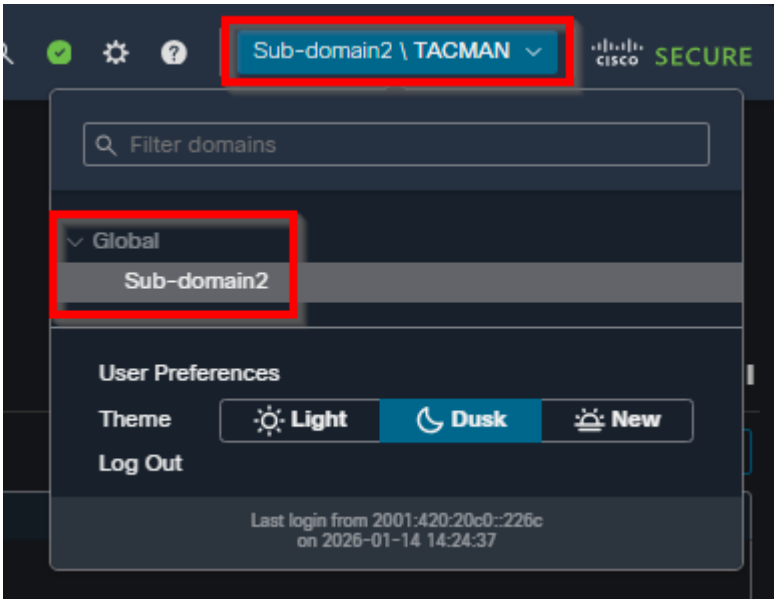
- Ces utilisateurs peuvent se connecter avec leur nom d'utilisateur uniquement, sans spécification de domaine :

```
Nom d'utilisateur
```

Mot de passe : [user password]

inline_image_15.png

- L'utilisateur n'a accès qu'aux sous-domaines où des rôles ont été spécifiquement attribués, sans accès au domaine global ou à d'autres sous-domaines.



image_inline_16.png

Flexibilité d'attribution des rôles

Les utilisateurs peuvent avoir des privilèges différents dans chaque domaine :

- Privilèges en lecture seule dans le domaine global avec des privilèges d'administrateur dans un domaine descendant
- Aucun accès au domaine global avec des autorisations d'administrateur complètes dans des sous-domaines spécifiques
- Autorisations de l'Éditeur de stratégie dans un sous-domaine sans accès aux autres sous-domaines

Considérations relatives aux utilisateurs externes

Pour les utilisateurs externes (authentification LDAP ou RADIUS) :

- Si des rôles d'utilisateur sont attribués via l'appartenance à un groupe ou des attributs d'utilisateur, les droits d'accès minimaux ne peuvent pas être supprimés.
- L'étendue des droits supplémentaires peut être supérieure au rôle d'utilisateur par défaut.
- Les objets d'authentification externes sont uniquement disponibles dans le domaine où ils sont créés.
- Les autorisations utilisateur individuelles doivent être configurées avec une étendue supérieure au rôle Utilisateur par défaut pour que la restriction soit correcte.

Limites et considérations

- Les rôles d'utilisateur personnalisés créés dans des domaines ancêtres ne peuvent pas être modifiés à partir de domaines descendants.
- L'authentification Shell n'est disponible que dans le domaine global et non dans les sous-domaines.
- Les préférences utilisateur et les paramètres du tableau de bord s'appliquent à tous les domaines auxquels le compte a accès.
- Les modifications d'autorisation pour les utilisateurs sont configurées individuellement et non par groupes ou par méthodes groupées.

Motif

Cette exigence découle de la nécessité de mettre en oeuvre un contrôle d'accès granulaire dans les déploiements FMC multidomaines où les utilisateurs ont besoin de différents niveaux d'accès aux sous-domaines et aux sous-domaines globaux, avec des restrictions spécifiques entre les domaines pour maintenir les limites de sécurité.

Autres informations utiles

- Guide d'administration de Cisco Secure Firewall Management Center, 7.6 : Utilisateurs
- Guide d'administration de Cisco Secure Firewall Management Center, 7.6 : Créer des rôles utilisateur personnalisés
- Guide d'administration de Cisco Secure Firewall Management Center, 7.6 : Ajouter ou modifier un utilisateur interne
- Guide d'administration de Cisco Secure Firewall Management Center, 7.6 : Utilisateurs et domaines
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.