Configurar dominio FMC Acceso de usuario y función

Problema

Este documento describe cómo configurar diferentes permisos de usuario para varios usuarios en FMC en dominios globales y subdominios.

Entorno

- Cisco Secure Firewall Management Center (FMC) - 7.6.4 (aplicable a todos los FMC)
- Implementación multidominio con dominio global y subdominios
- Varios dispositivos FTD asignados a diferentes subdominios
- Varios usuarios que requieren diferentes niveles de permisos

Resolución

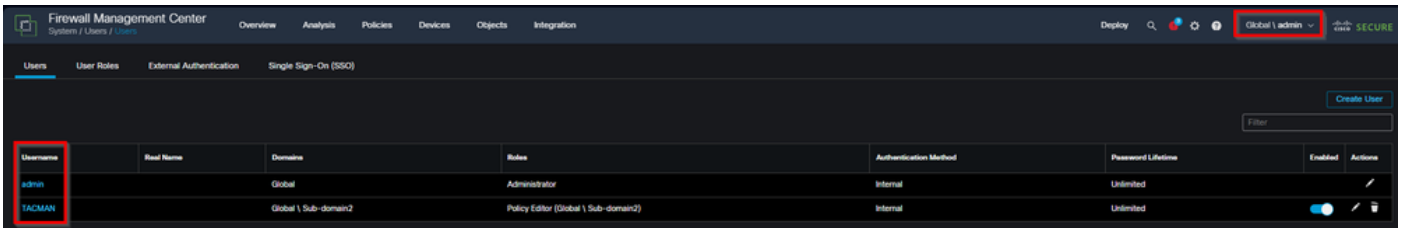
Este documento resuelve cómo configurar diferentes permisos de usuario para varios usuarios en FMC a través de dominios globales y subdominios, con la capacidad de restringir el acceso entre dominios y limitar el acceso a dominios globales para usuarios específicos. Cisco FMC admite la asignación granular de roles de usuario en varios dominios con la capacidad de restringir el acceso entre dominios. La configuración implica la creación de usuarios en dominios específicos y la asignación de roles apropiados para controlar los niveles de acceso.

Crear comportamiento de acceso de usuario y dominio

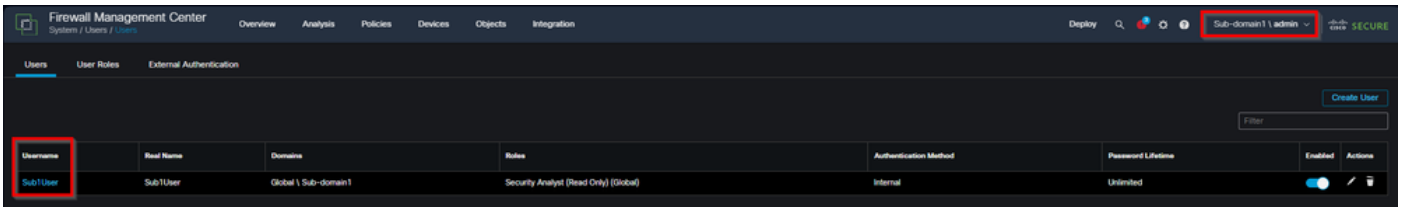
El sistema de gestión de usuarios del CSP funciona de forma diferente en función de dónde se crean los usuarios:

Usuarios creados en subdominios

- Los usuarios creados directamente en un subdominio solo son visibles dentro del dominio específico:

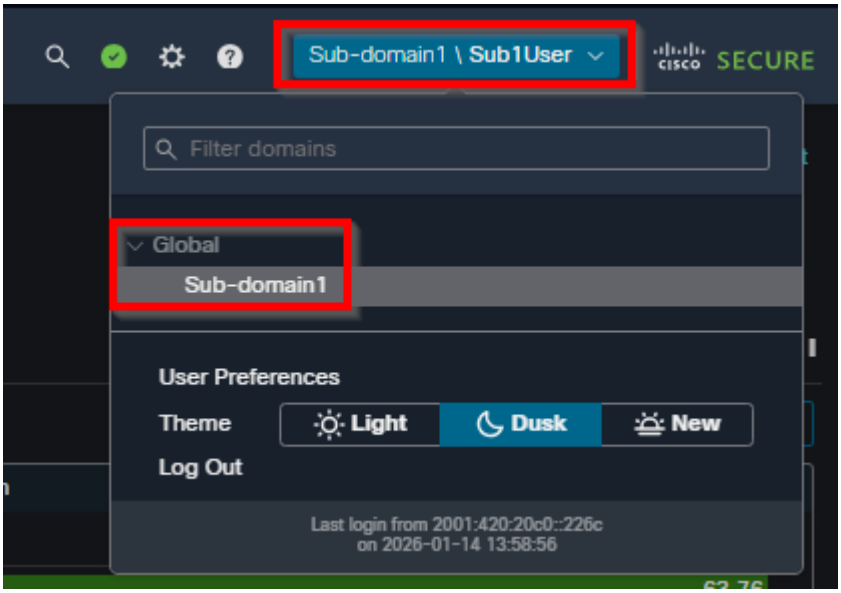


inline_image_0.png



inline_image_1.png

- Estos usuarios deben iniciar sesión con el formato de especificación de dominio: subdominio\nombre de usuario.
- El acceso se restringe automáticamente al dominio en el que se creó el usuario:



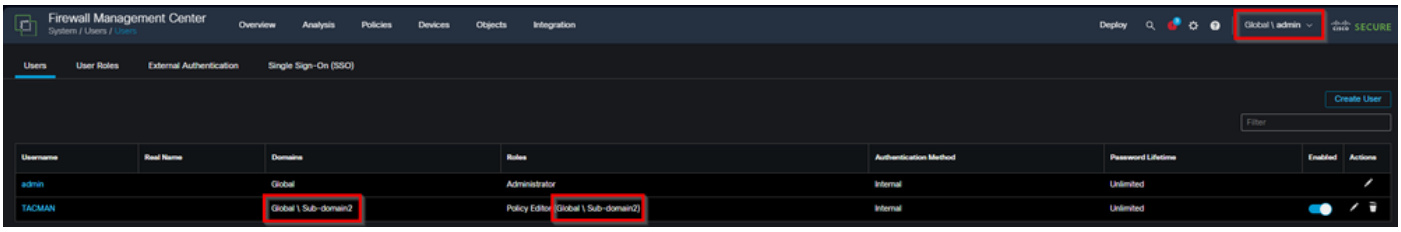
inline_image_2.png

- Los roles personalizados creados en el subdominio se aplican únicamente a ese dominio.

Usuarios creados en dominio global:

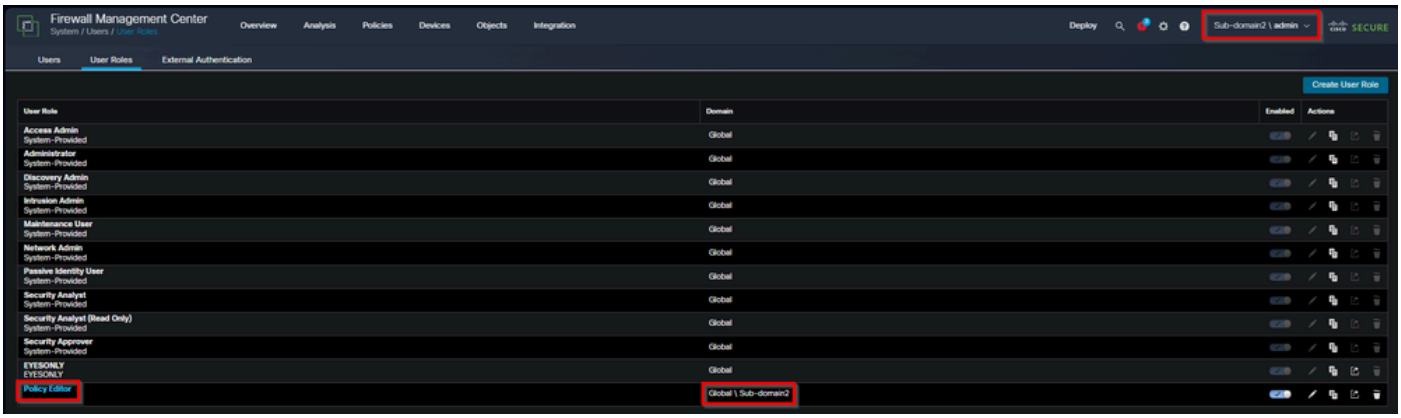
- Los usuarios creados a partir del dominio global pueden iniciar sesión solo con su nombre de usuario, incluso si sus funciones están solo en subdominios.

- Estos usuarios permanecen visibles en la lista de usuarios de dominio global:



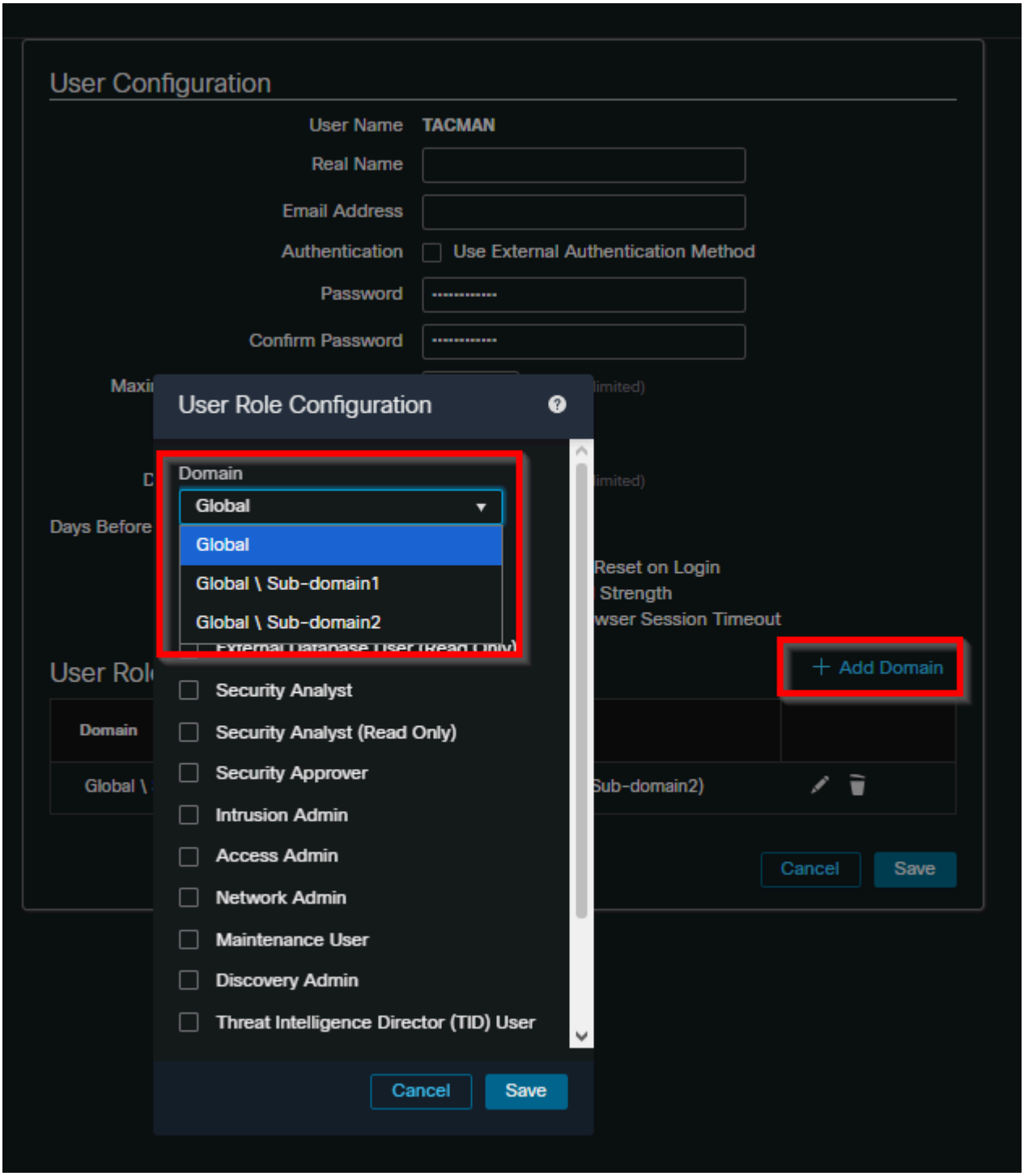
inline_image_3.png

- Las asignaciones de funciones se pueden realizar para cualquier dominio descendiente:



inline_image_4.png

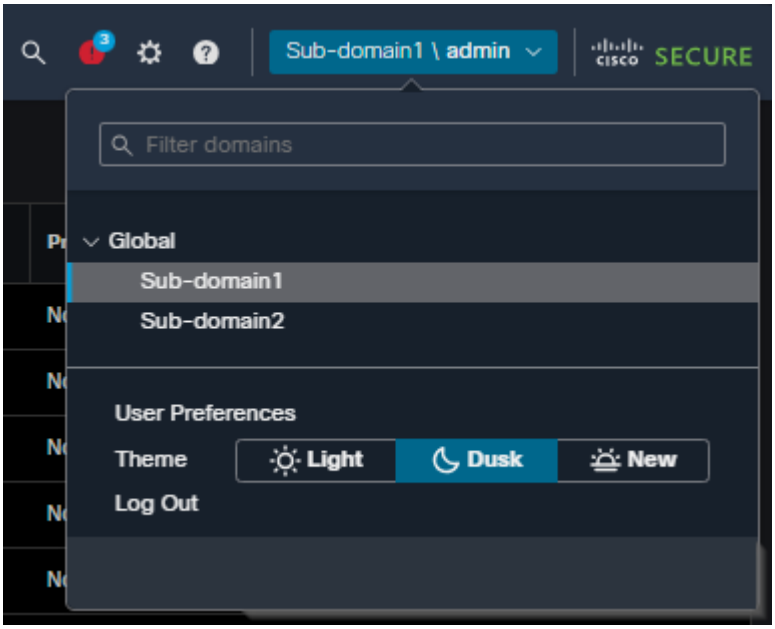
- El acceso se puede restringir a subdominios específicos mediante la asignación de funciones:



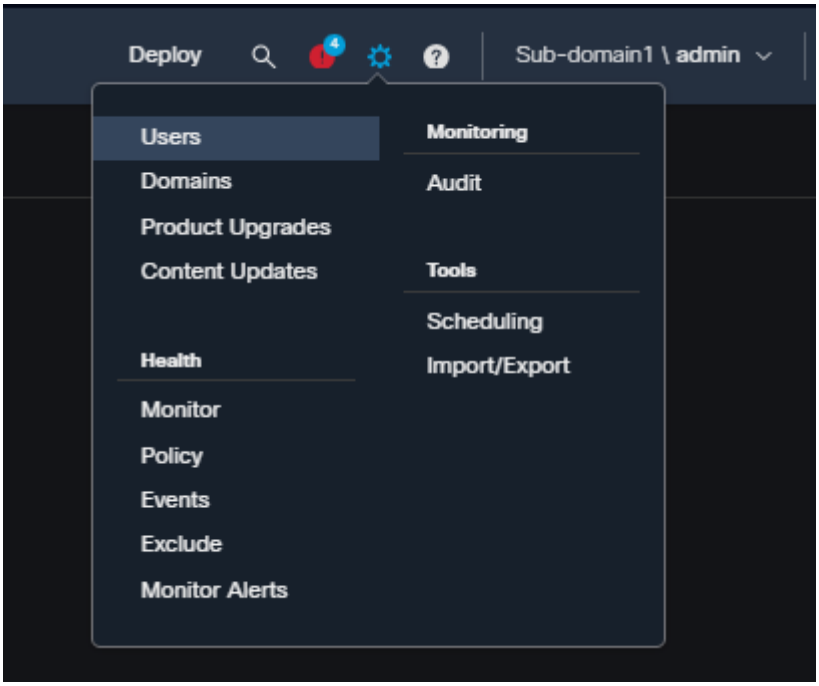
inline_image_5.png

Pasos de configuración para la restricción de usuarios de subdominio

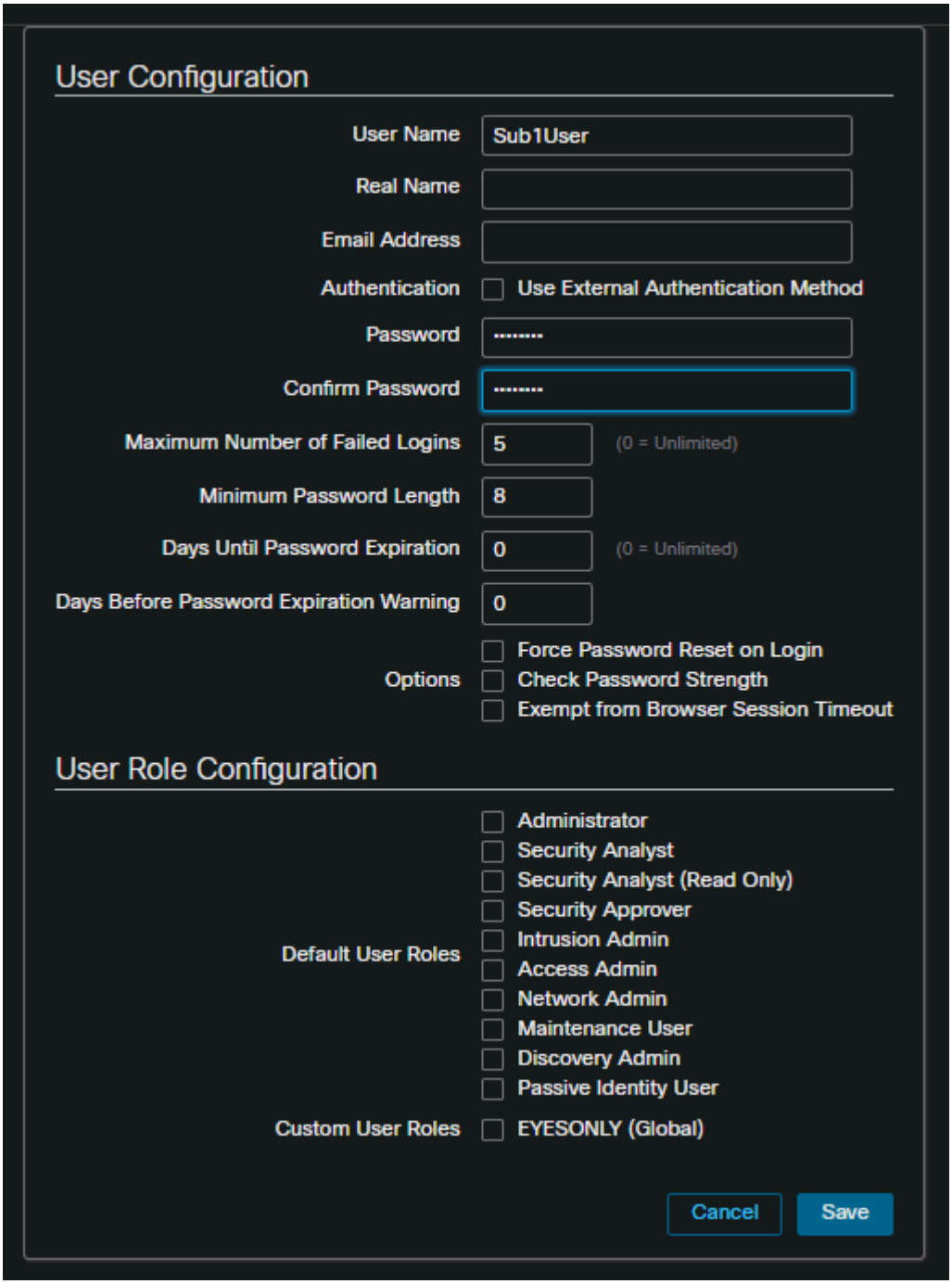
- Navegue hasta el subdominio específico donde debe restringirse el acceso y cree la cuenta de usuario en Sistema / Usuarios.



inline_image_6.png

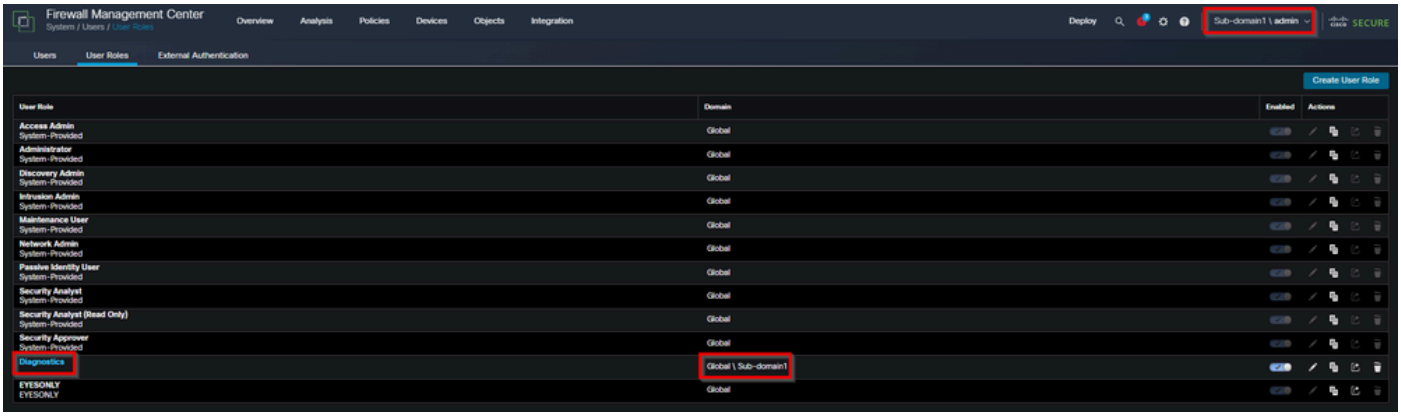


inline_image_7.png



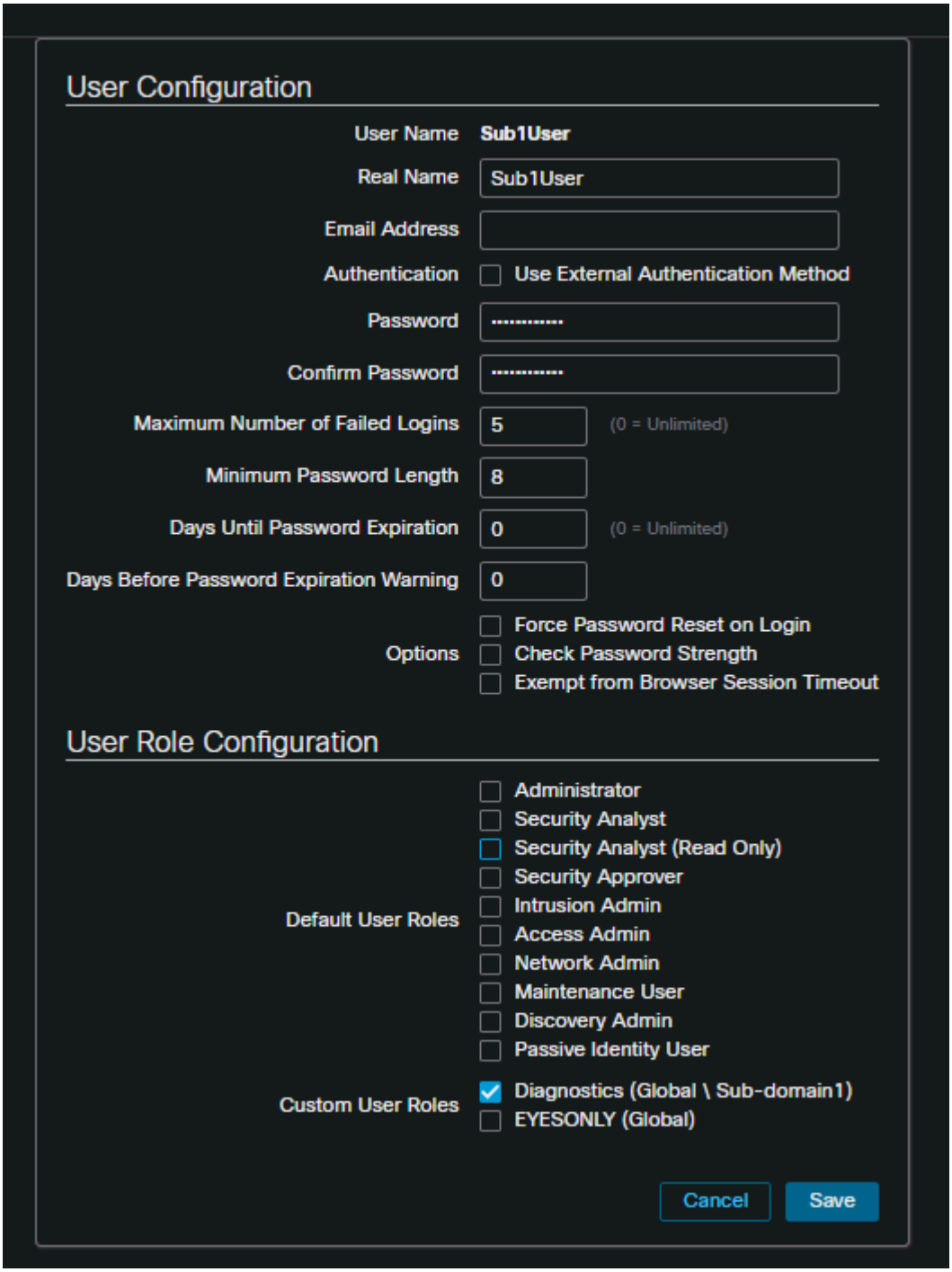
inline_image_8.png

- Cree roles personalizados dentro del subdominio en Roles del Sistema/Usuario. Los roles de usuario personalizados creados en un subdominio sólo están disponibles dentro de ese dominio y no se puede acceder a ellos desde otros dominios.



inline_image_9.png

- Asigne la función personalizada al usuario. El usuario hereda permisos sólo para el dominio en el que se crearon el usuario y la función.



inline_image_10.png

- Formato de inicio de sesión de usuario para usuarios de subdominios. Los usuarios creados en subdominios deben utilizar este formato de inicio de sesión:

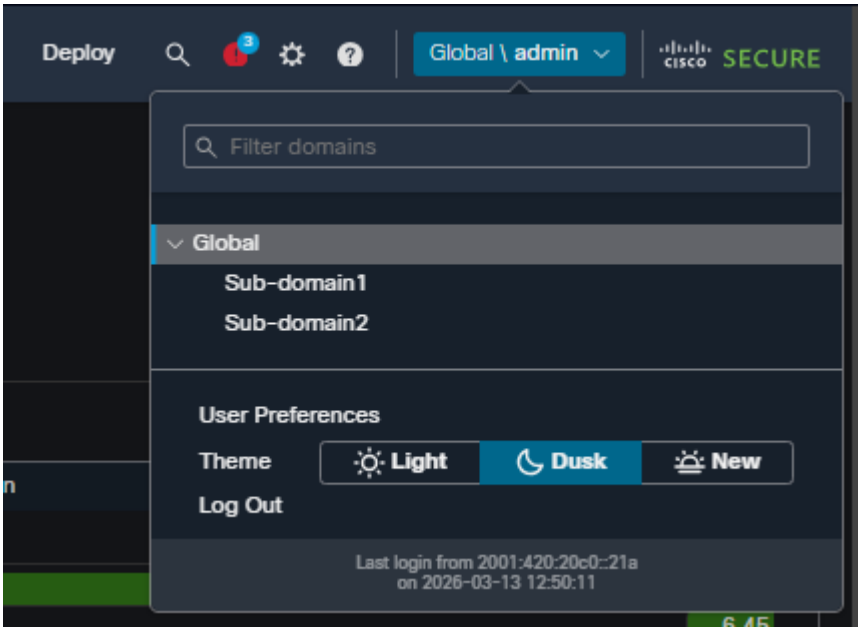
```
Nombre de usuario: Sub-domain\username
```

```
Contraseña: [user password]
```

inline_image_11.png

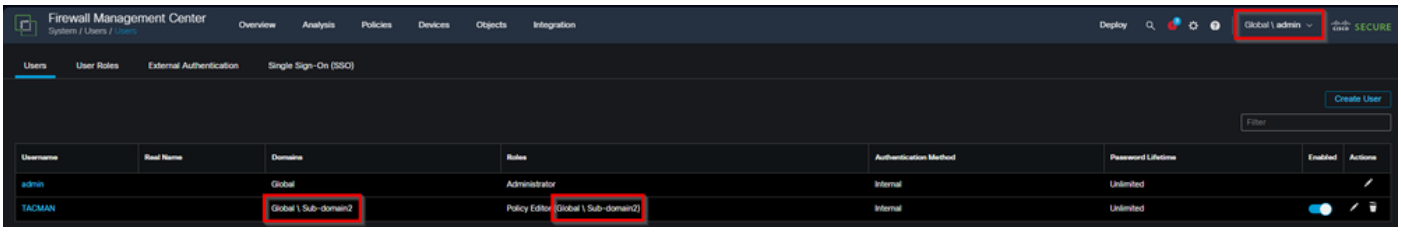
Pasos de configuración para usuarios de dominio global con restricciones de subdominio

- Cree el usuario en el dominio global en Sistema/Usuarios. Utilice una cuenta administrativa con acceso a dominio global para crear el usuario.

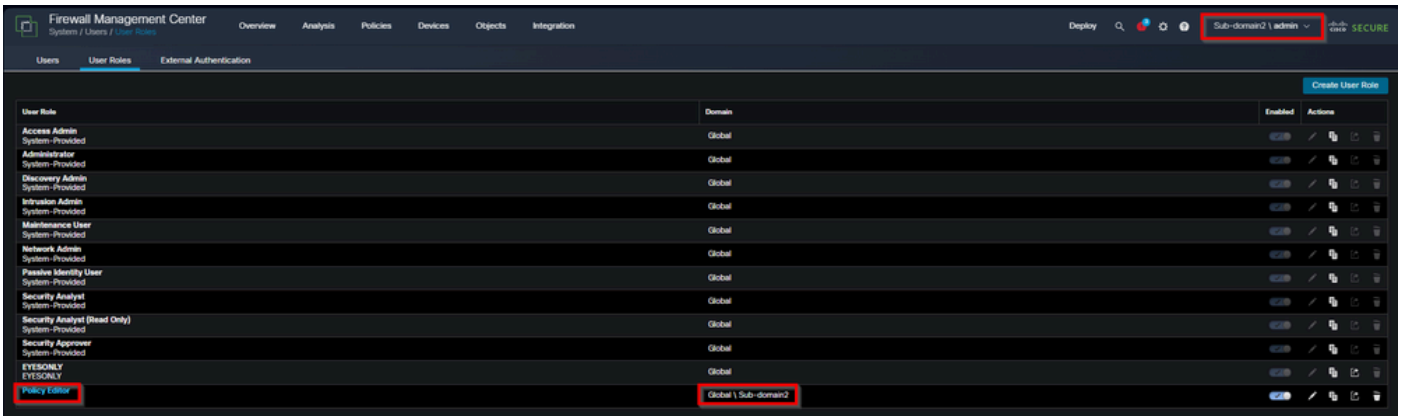


inline_image_12.png

- Asigne roles sólo para subdominios específicos en Sistema/Usuarios. En la configuración de usuario, asigne roles exclusivamente para los subdominios de destino sin proporcionar ningún permiso de dominio global.



inline_image_3.png



inline_image_14.png

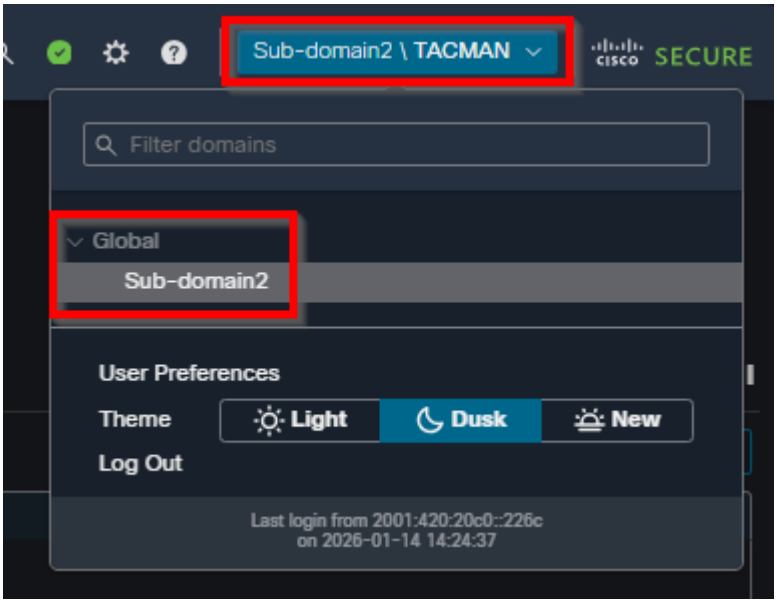
- Estos usuarios pueden iniciar sesión sólo con su nombre de usuario, sin especificación de dominio:

```
Nombre de usuario: username
```

Contraseña: [user password]

inline_image_15.png

- El usuario solo tiene acceso a los subdominios a los que se asignaron roles de forma específica, sin acceso a dominios globales ni a otros subdominios.



inline_image_16.png

Flexibilidad de asignación de roles

Los usuarios pueden tener diferentes privilegios en cada dominio:

- Privilegios de sólo lectura en el dominio global con privilegios de administrador en un dominio descendiente
- Sin acceso a dominio global con permisos de administrador completos en subdominios específicos
- Permisos del Editor de directivas en un subdominio sin acceso a otros subdominios

Consideraciones del usuario externo

Para usuarios externos (autenticación LDAP o RADIUS):

- Si las funciones de usuario se asignan mediante la pertenencia a grupos o atributos de usuario, no se pueden quitar los derechos de acceso mínimos.
- A los derechos adicionales se les puede asignar un ámbito mayor que la función de usuario predeterminada.
- Los objetos de autenticación externa sólo están disponibles en el dominio en el que se han creado.
- Los permisos de usuario individuales deben configurarse en un ámbito mayor que la función Usuario predeterminado para que la restricción sea correcta.

Limitaciones y consideraciones

- Las funciones de usuario personalizadas creadas en dominios antecesores no se pueden editar desde dominios descendientes.
- La autenticación de shell sólo está disponible en el dominio global, no en los subdominios.
- Las preferencias de usuario y la configuración del panel se aplican a todos los dominios a los que tiene acceso la cuenta.
- Las modificaciones de permisos para los usuarios se configuran de forma individual y no en grupos ni en métodos masivos.

Causa

El requisito se deriva de la necesidad de implementar un control de acceso granular en implementaciones de FMC en varios dominios en las que los usuarios requieren diversos niveles de acceso a dominios globales y subdominios, con restricciones específicas entre dominios para mantener los límites de seguridad.

Contenido relacionado

- Guía de administración de Cisco Secure Firewall Management Center, 7.6: Usuarios
- Guía de administración de Cisco Secure Firewall Management Center, 7.6: Crear funciones de usuario personalizadas
- Guía de administración de Cisco Secure Firewall Management Center, 7.6: Agregar o editar un usuario interno
- Guía de administración de Cisco Secure Firewall Management Center, 7.6: Usuarios y dominios
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).