Configurar acesso e função do usuário do FMC

Problema

Este documento descreve como configurar permissões de usuário diferentes para vários usuários no FMC em subdomínios e domínios globais.

Ambiente

- Cisco Secure Firewall Management Center (FMC) - 7.6.4 (aplicável a todos os FMCs)
- Implantação em vários domínios com domínio e subdomínios globais
- Vários dispositivos FTD atribuídos a diferentes subdomínios
- Vários usuários que exigem diferentes níveis de permissão

Resolução

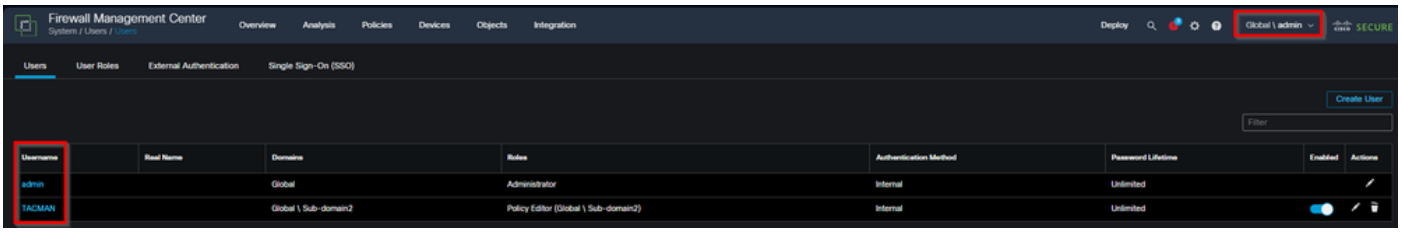
Este documento resolve como configurar permissões de usuário diferentes para vários usuários no FMC em domínios globais e subdomínios, com a capacidade de restringir o acesso entre domínios e limitar o acesso global ao domínio para usuários específicos. O Cisco FMC suporta atribuição de função de usuário granular em vários domínios com a capacidade de restringir o acesso entre domínios. A configuração envolve a criação de usuários em domínios específicos e a atribuição de funções apropriadas para controlar níveis de acesso.

Criar comportamento de acesso de usuário e domínio

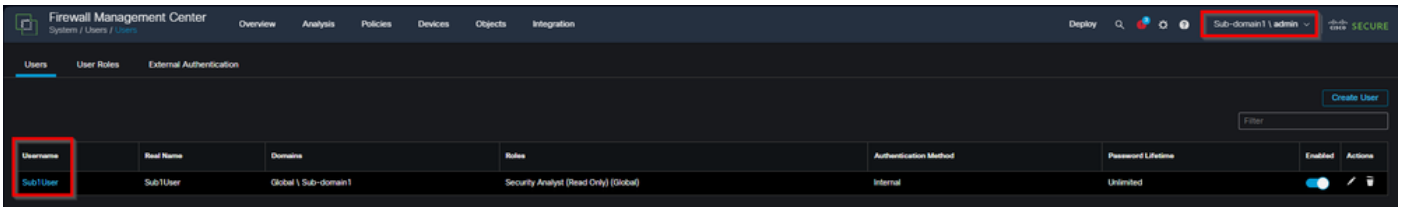
O sistema de gestão de utilizadores do CVP funciona de forma diferente consoante o local onde os utilizadores são criados:

Usuários criados em subdomínios

- Os usuários criados diretamente em um subdomínio só são visíveis dentro do domínio específico:

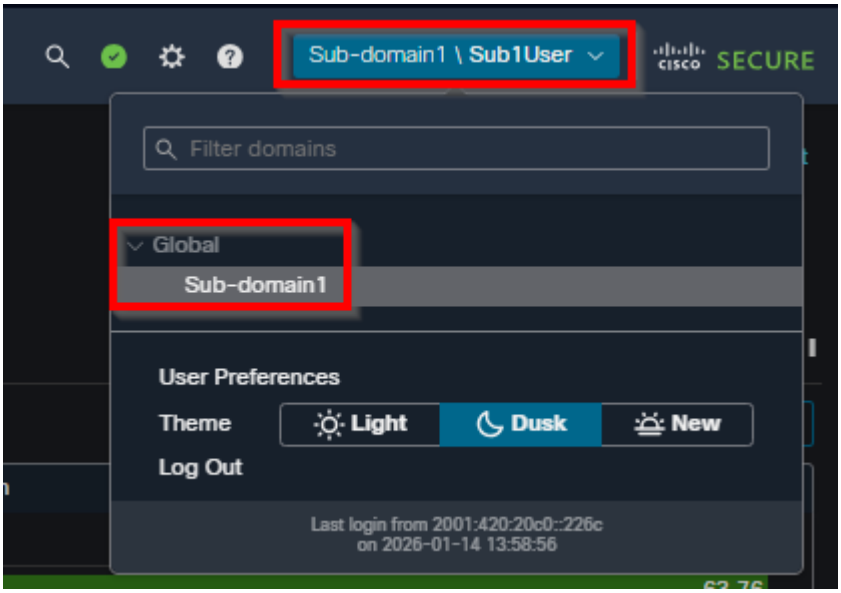


inline_image_0.png



inline_image_1.png

- Esses usuários devem fazer logon usando o formato de especificação de domínio: subdomínio\nome de usuário.
- O acesso é automaticamente restrito ao domínio em que o usuário foi criado:



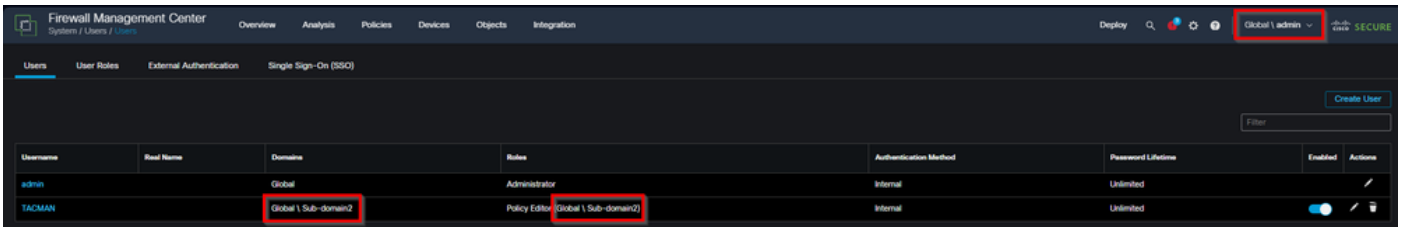
inline_image_2.png

- As funções personalizadas criadas no subdomínio aplicam-se somente a esse domínio.

Usuários criados no domínio global:

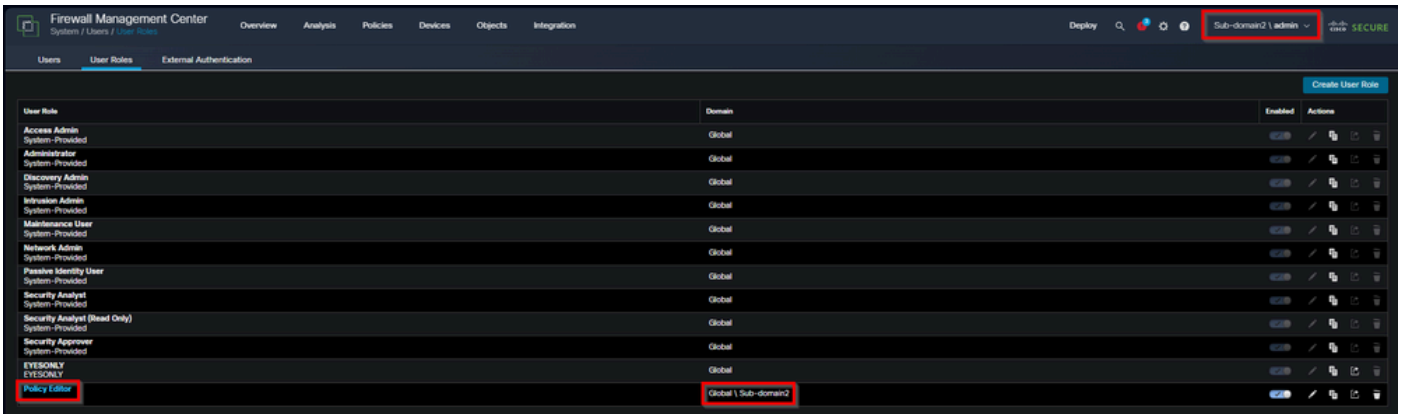
- Os usuários criados a partir do domínio global podem fazer login apenas com seu nome de usuário, mesmo que suas funções estejam apenas em subdomínios.

- Esses usuários permanecem visíveis na lista de usuários do domínio global:



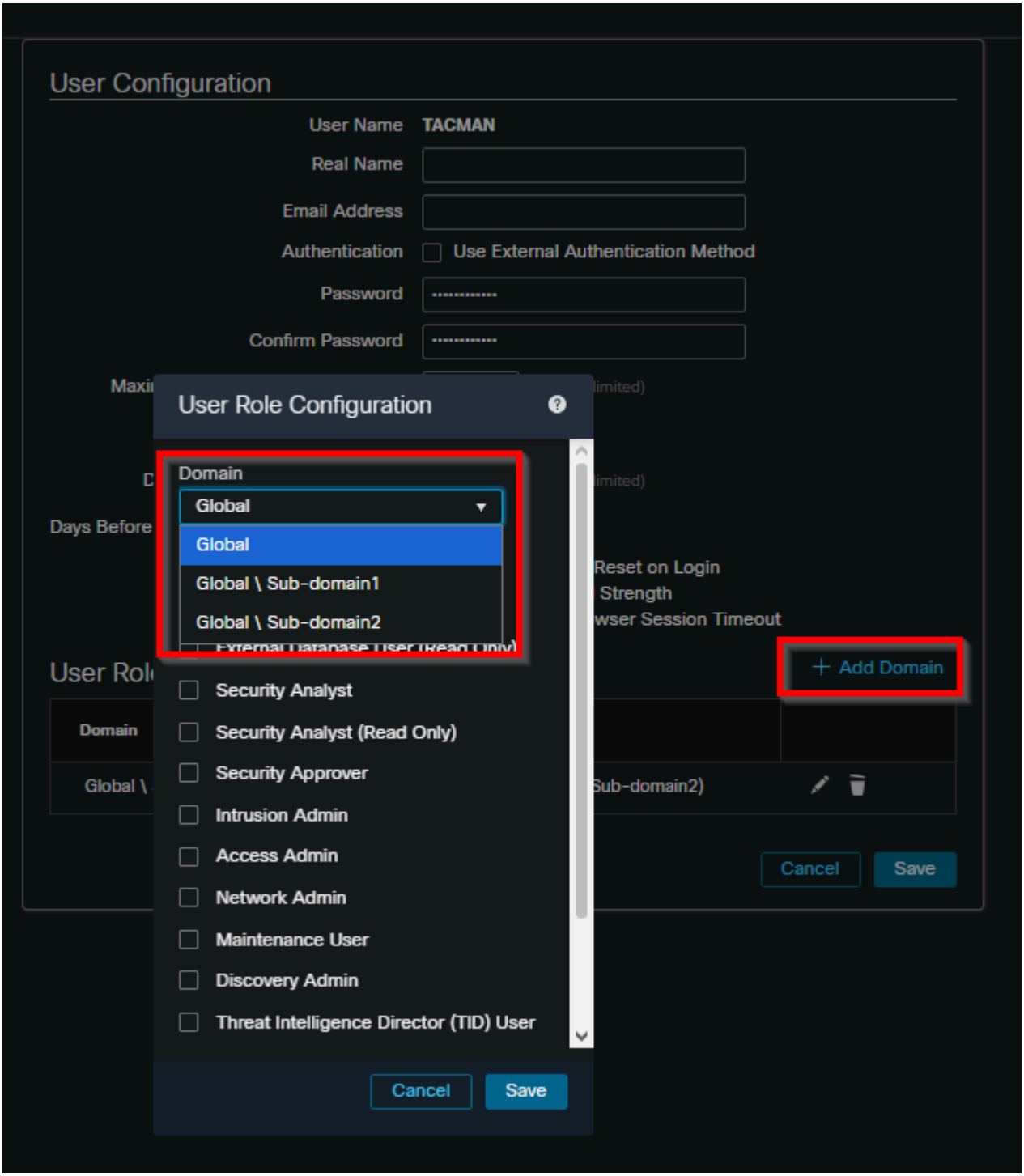
inline_image_3.png

- As atribuições de função podem ser feitas para qualquer domínio descendente:



inline_image_4.png

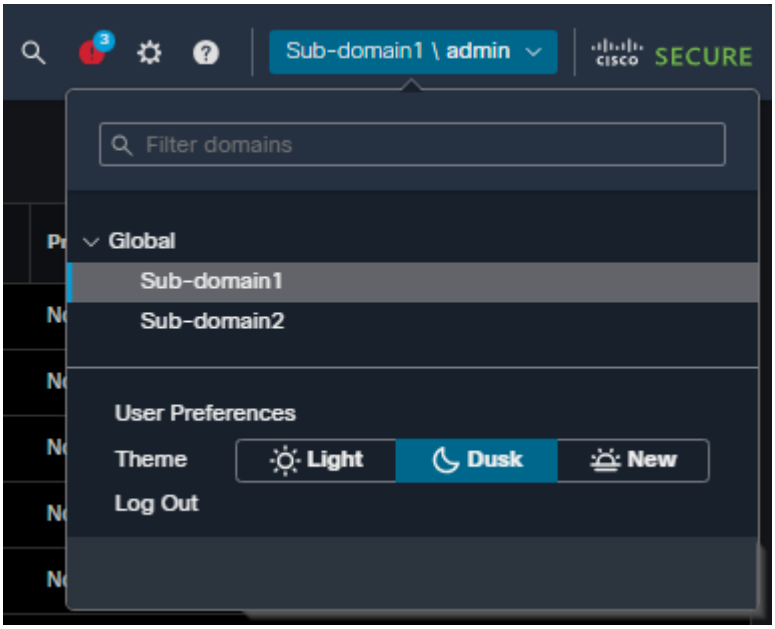
- O acesso pode ser restrito a subdomínios específicos por meio da atribuição de funções:



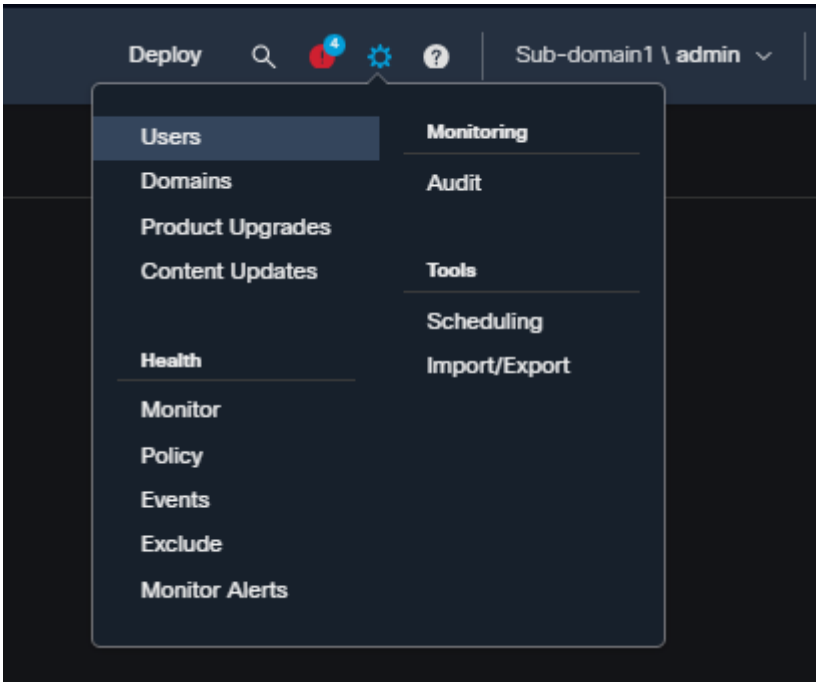
inline_image_5.png

Etapas de Configuração para Restrição de Usuário do Subdomínio

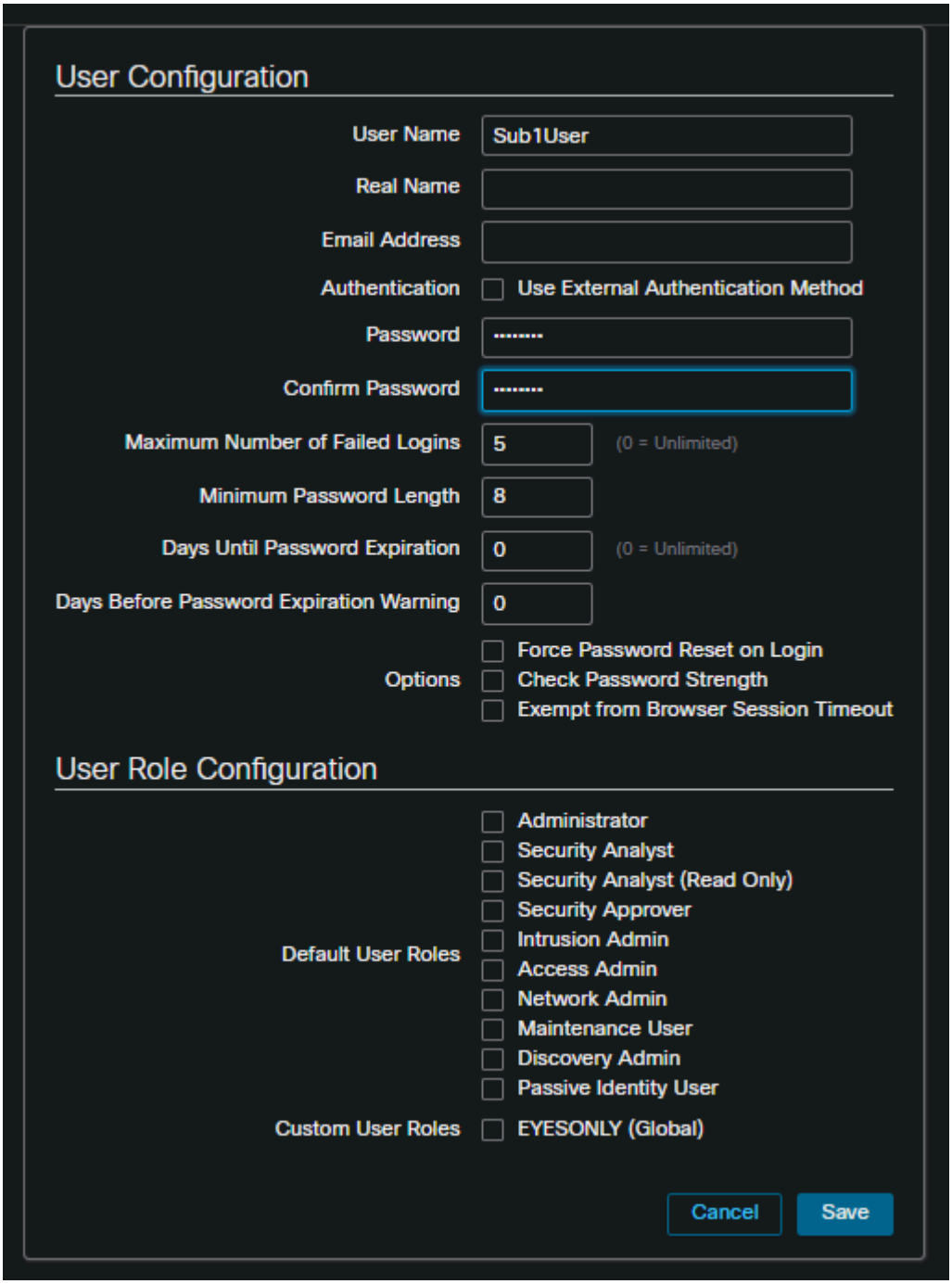
- Navegue até o subdomínio específico onde o acesso deve ser restrito e crie a conta de usuário em Sistema/Usuários.



inline_image_6.png

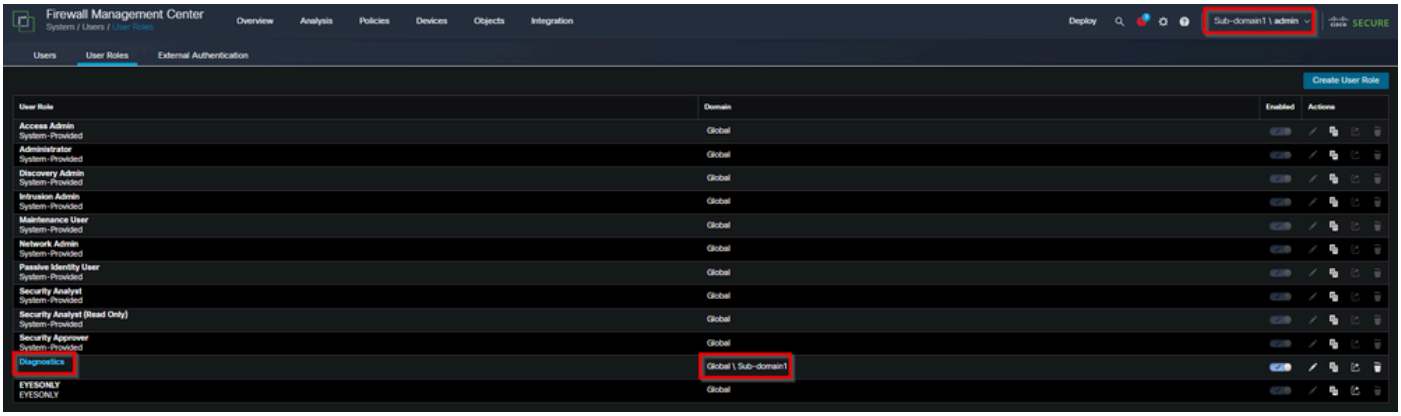


inline_image_7.png



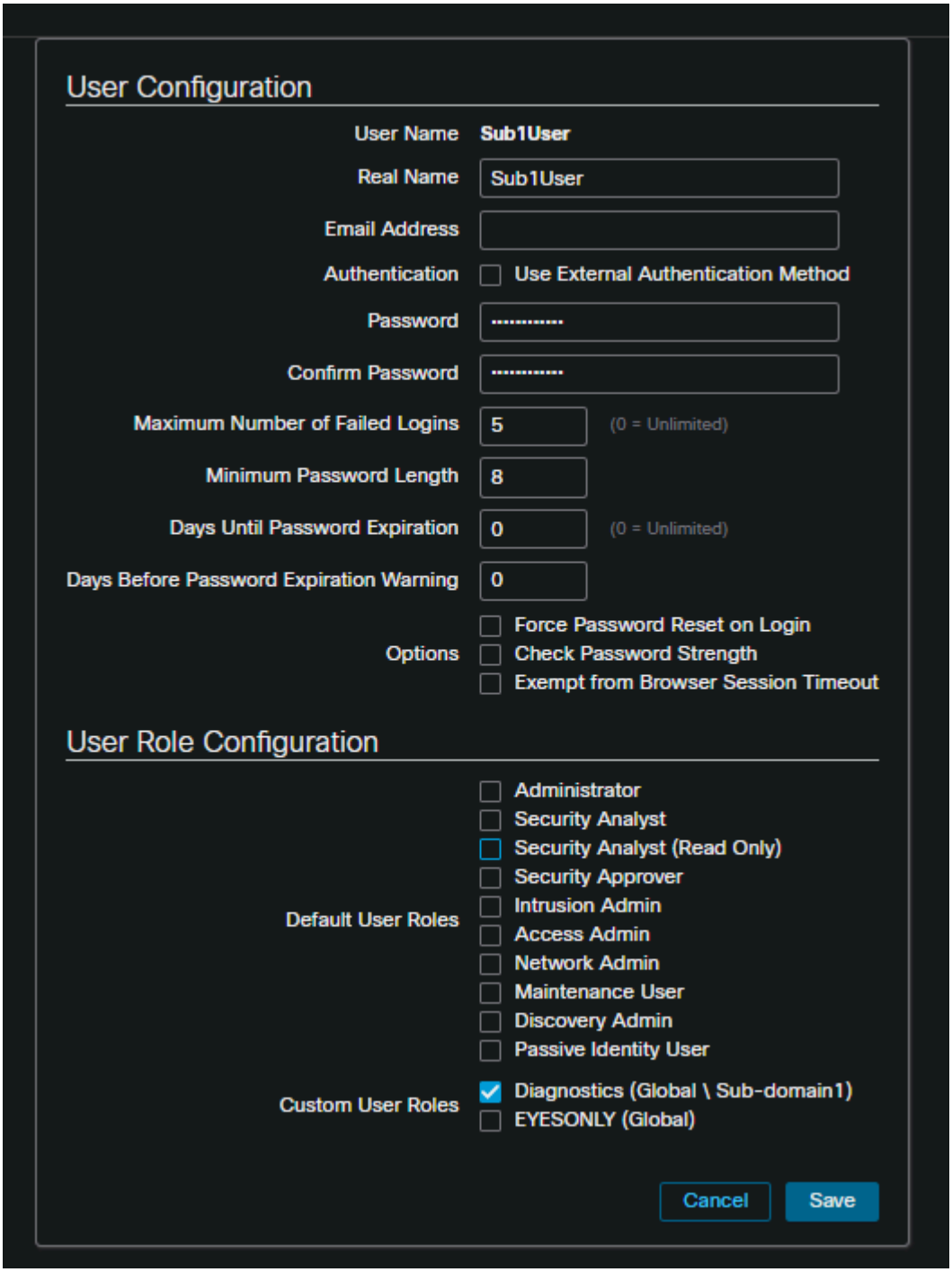
inline_image_8.png

- Crie funções personalizadas no subdomínio em Sistema / Funções de Usuário. As funções de usuário personalizadas criadas em um subdomínio estão disponíveis apenas nesse domínio e não podem ser acessadas de outros domínios.



inline_image_9.png

- Atribua a função personalizada ao usuário. O usuário herda permissões somente para o domínio em que o usuário e a função foram criados.



inline_image_10.png

- Formato de logon do usuário para usuários de subdomínio. Os usuários criados em subdomínios devem usar este formato de logon:

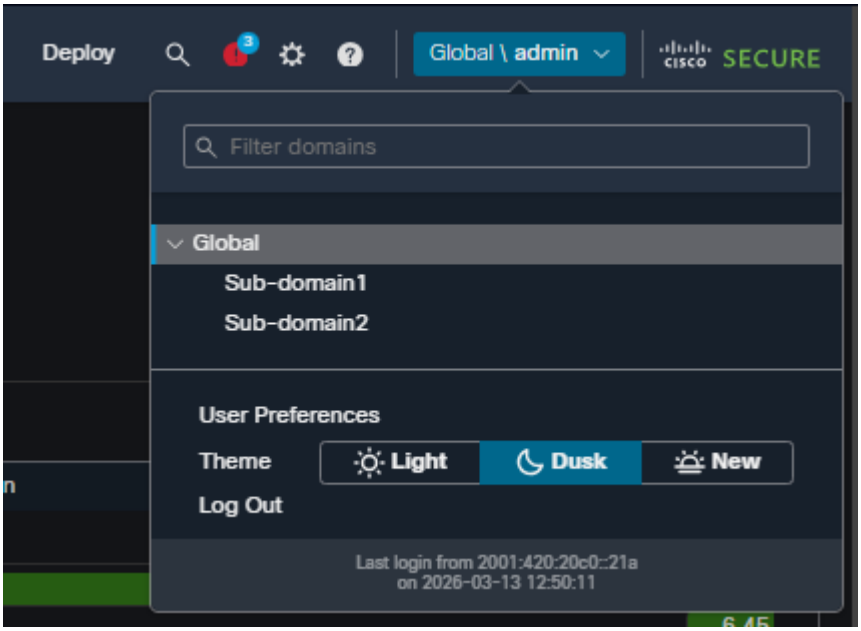
```
Nome de usuário: Subdomínio\nome de usuário
```

```
Senha: [senha do usuário]
```

inline_image_11.png

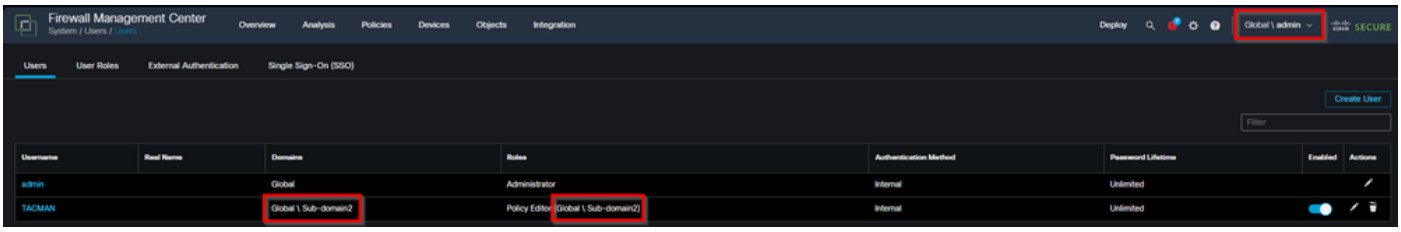
Etapas de Configuração para Usuários de Domínio Global com Restrições de Subdomínio

- Crie o usuário no domínio Global em Sistema / Usuários. Use uma conta administrativa com acesso de domínio Global para criar o usuário.

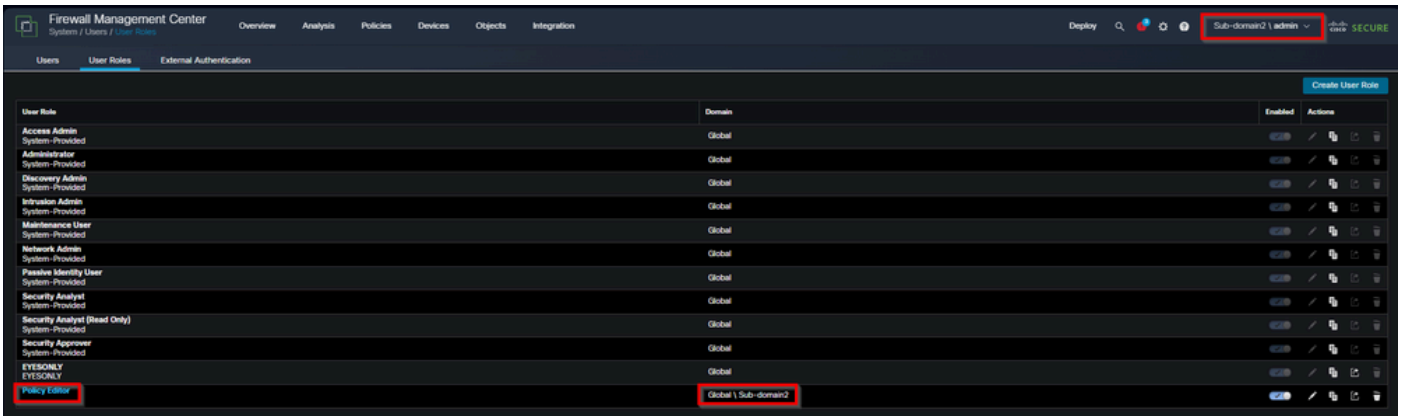


inline_image_12.png

- Atribua funções somente para subdomínios específicos em Sistema/Usuários. Na configuração do usuário, atribua funções exclusivamente para o(s) subdomínio(s) de destino sem fornecer nenhuma permissão de domínio Global.



inline_image_3.png



inline_image_14.png

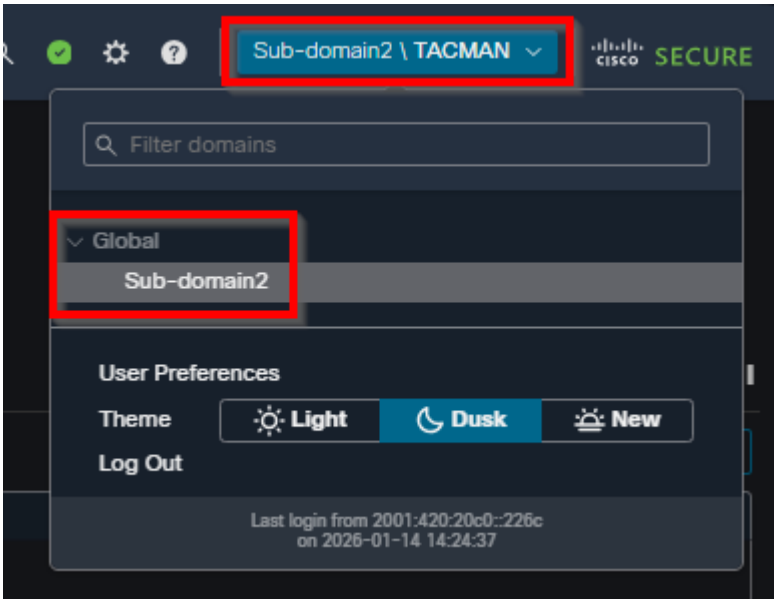
- Esses usuários podem fazer logon apenas com seus nomes de usuário, sem especificação de domínio:

```
Nome de usuário: nome de usuário
```

```
Senha: [senha do usuário]
```

inline_image_15.png

- O usuário só tem acesso aos subdomínios onde as funções foram especificamente atribuídas, sem acesso ao domínio global ou a outros subdomínios.



inline_image_16.png

Flexibilidade de atribuição de função

Os usuários podem ter privilégios diferentes em cada domínio:

- Privilégios somente leitura no domínio Global com privilégios de Administrador em um domínio descendente
- Sem acesso global ao domínio com permissões totais de administrador em subdomínios específicos
- Permissões do Policy Editor em um subdomínio sem acesso a outros subdomínios

Considerações do Usuário Externo

Para usuários externos (autenticação LDAP ou RADIUS):

- Se as funções de usuário forem atribuídas por meio de associação de grupo ou atributos de usuário, os direitos de acesso mínimos não poderão ser removidos.
- Direitos adicionais podem ser atribuídos a um escopo maior do que a função de usuário padrão.
- Os objetos de autenticação externa estão disponíveis apenas no domínio em que foram criados.
- Permissões de usuário individuais devem ser configuradas em um escopo maior do que a função de Usuário Padrão para a restrição apropriada.

Limitações e considerações

- As funções de usuário personalizadas criadas em domínios ancestrais não podem ser editadas a partir de domínios descendentes.
- A Autenticação Shell está disponível apenas no domínio Global, não em subdomínios.
- As preferências do usuário e as configurações do painel se aplicam a todos os domínios aos quais a conta tem acesso.
- As modificações de permissão para usuários são configuradas individualmente e não em grupos ou métodos em massa.

Causa

Este requisito decorre da necessidade de implementar um controlo de acesso granular em instalações de CVP com vários domínios em que os utilizadores necessitam de níveis variáveis de acesso a domínios globais e subdomínios, com restrições específicas entre domínios para manter os limites de segurança.

Conteúdo relacionado

- Guia de Administração do Cisco Secure Firewall Management Center, 7.6: Usuários
- Guia de Administração do Cisco Secure Firewall Management Center, 7.6: Criar funções de usuário personalizadas
- Guia de Administração do Cisco Secure Firewall Management Center, 7.6: Adicionar ou editar um usuário interno
- Guia de Administração do Cisco Secure Firewall Management Center, 7.6: Usuários e domínios
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.