

FMC Domain configureren; gebruikerstoegang en rol

uitgeven

In dit document wordt beschreven hoe u verschillende gebruikersmachtigingen kunt configureren voor meerdere gebruikers in FMC in globale en subdomeinen.

milieu

- Cisco Secure Firewall Management Center (FMC) - 7.6.4 (van toepassing op alle FMC's)
- Implementatie van meerdere domeinen met wereldwijd domein en subdomeinen
- Meerdere FTD-apparaten toegewezen aan verschillende subdomeinen
- Meerdere gebruikers die verschillende machtigingsniveaus nodig hebben

resolutie

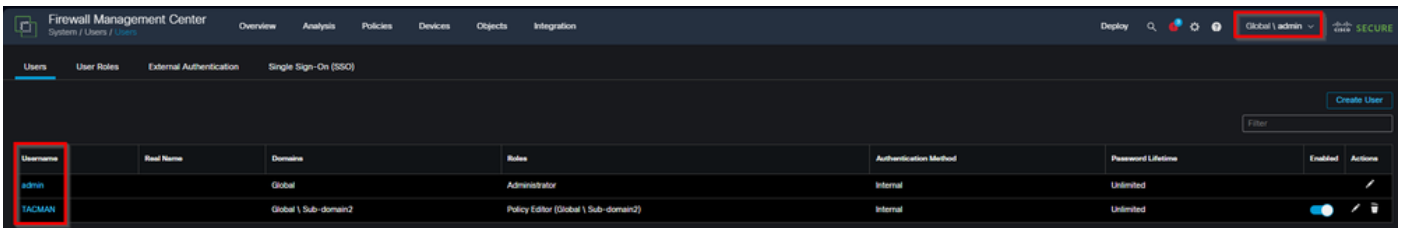
In dit document wordt beschreven hoe verschillende gebruikersmachtigingen voor meerdere gebruikers in FMC kunnen worden geconfigureerd voor wereldwijde en subdomeinen, met de mogelijkheid om de toegang tussen domeinen te beperken en de toegang tot het wereldwijde domein voor specifieke gebruikers te beperken. Cisco FMC ondersteunt granulaire toewijzing van gebruikersrollen over meerdere domeinen met de mogelijkheid om de toegang tussen domeinen te beperken. De configuratie omvat het maken van gebruikers in specifieke domeinen en het toewijzen van de juiste rollen om toegangsniveaus te beheren.

Gedrag voor gebruikers- en domeintoegang maken

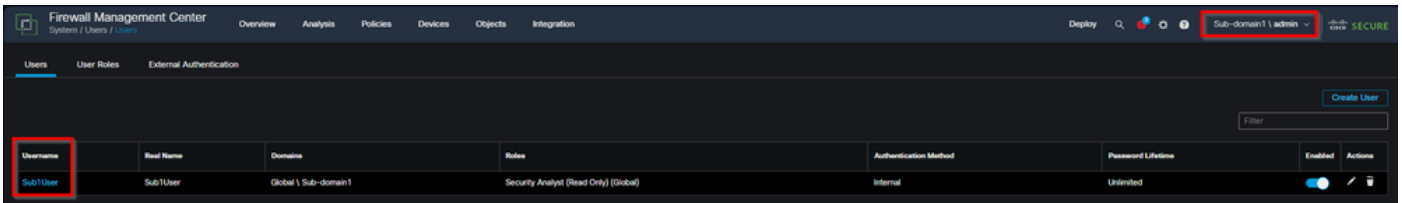
Het FMC-gebruikersbeheersysteem werkt anders op basis van waar gebruikers worden gemaakt:

Gebruikers gemaakt in subdomeinen

- Gebruikers die rechtstreeks in een subdomein zijn gemaakt, zijn alleen zichtbaar binnen het specifieke domein:

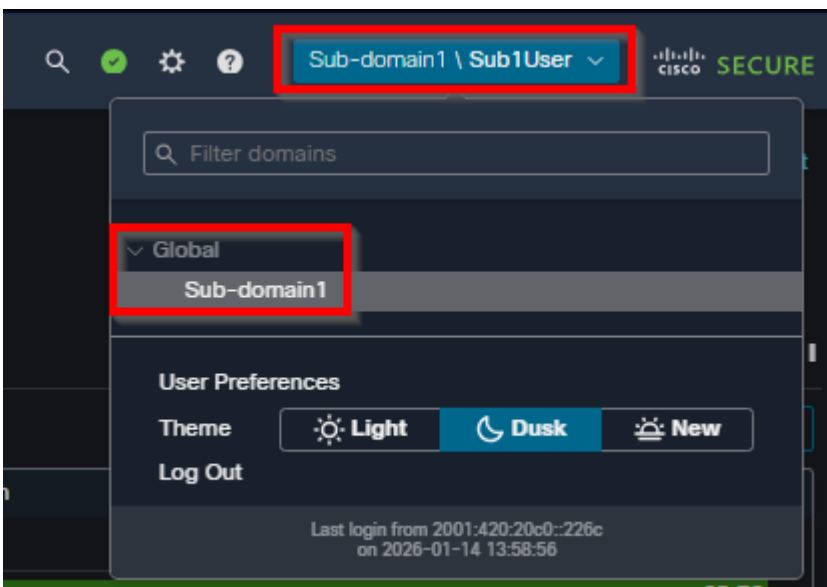


inline_image_0.png



inline_image_1.png

- Deze gebruikers moeten inloggen met behulp van de domeinspecificatie: subdomein\gebruikersnaam.
- De toegang wordt automatisch beperkt tot het domein waar de gebruiker is gemaakt:



inline_image_2.png

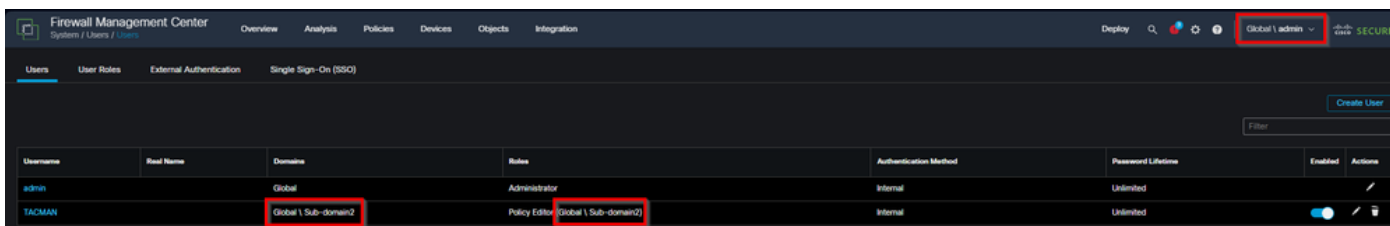
- Aangepaste rollen die in het subdomein zijn gemaakt, zijn alleen van toepassing op dat domein.

Gebruikers gemaakt in Global Domain:

- Gebruikers die zijn gemaakt van het Global-domein kunnen inloggen met alleen hun

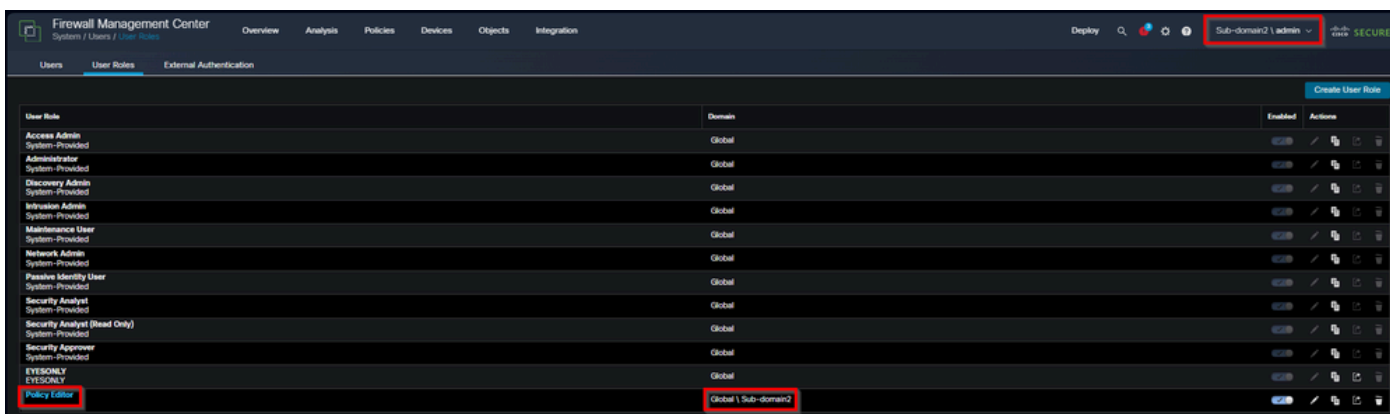
gebruikersnaam, zelfs als hun rollen alleen in subdomeinen zijn.

- Deze gebruikers blijven zichtbaar in de gebruikerslijst van het Global Domain:



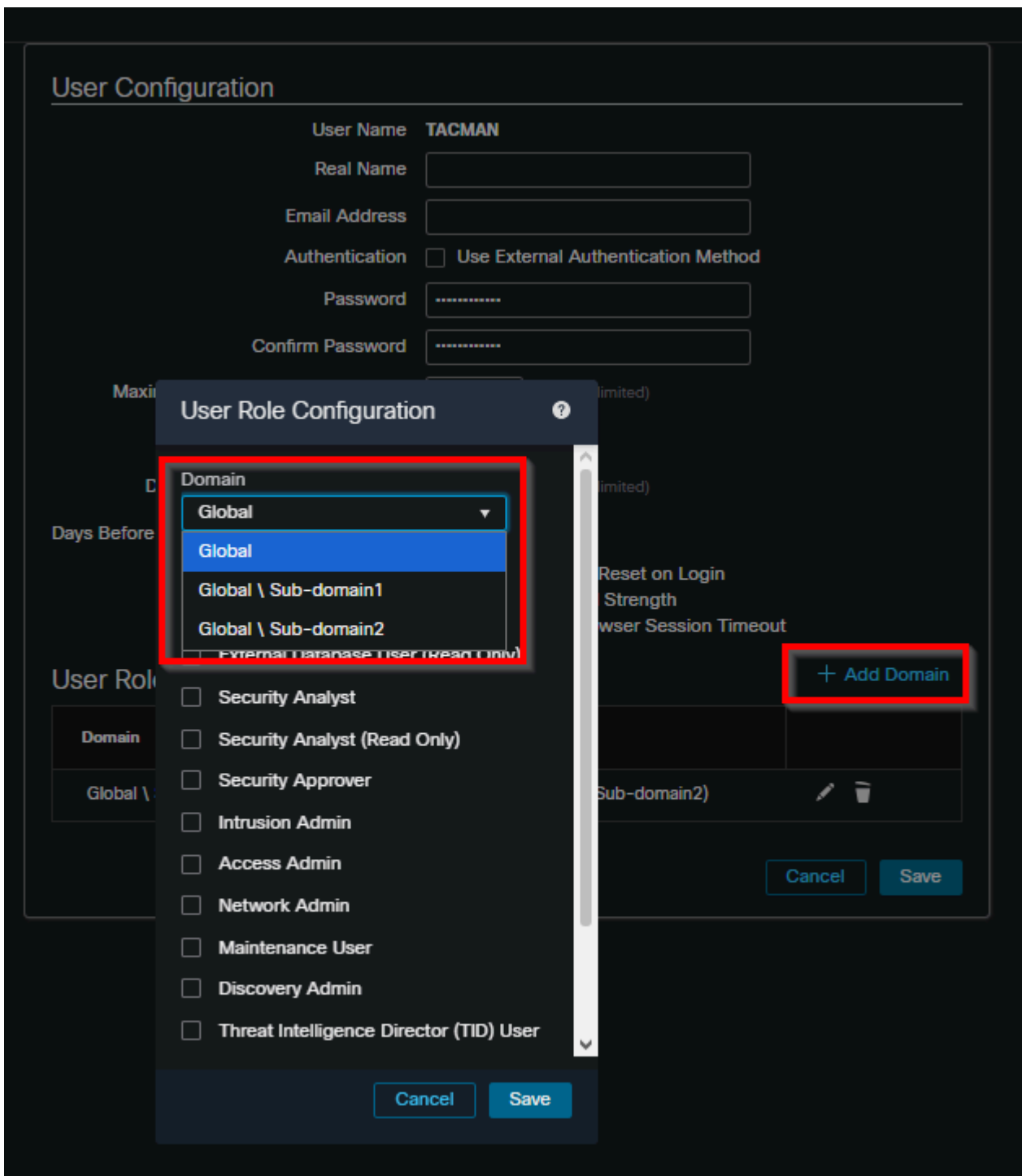
inline_image_3.png

- Roltoewijzingen kunnen worden gemaakt voor elk afstammingsdomein:



inline_image_4.png

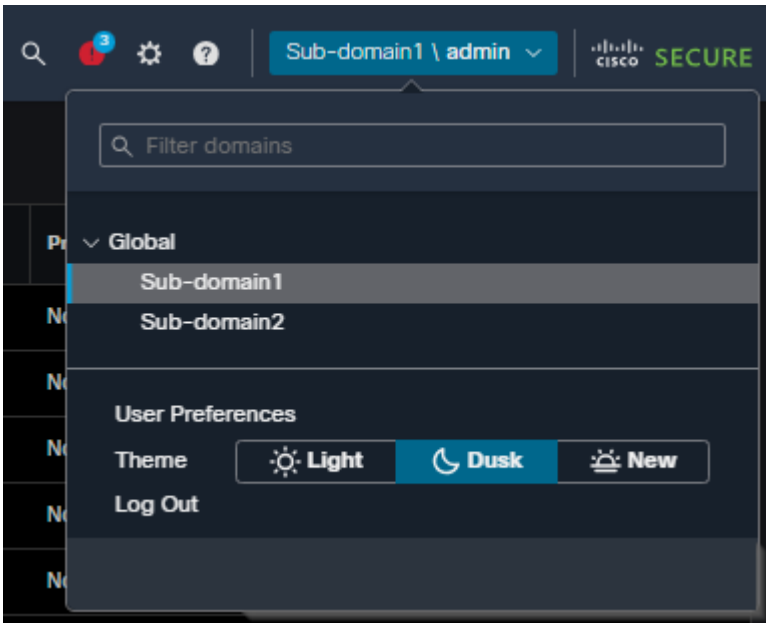
- Toegang kan worden beperkt tot specifieke subdomeinen door roltoewijzing:



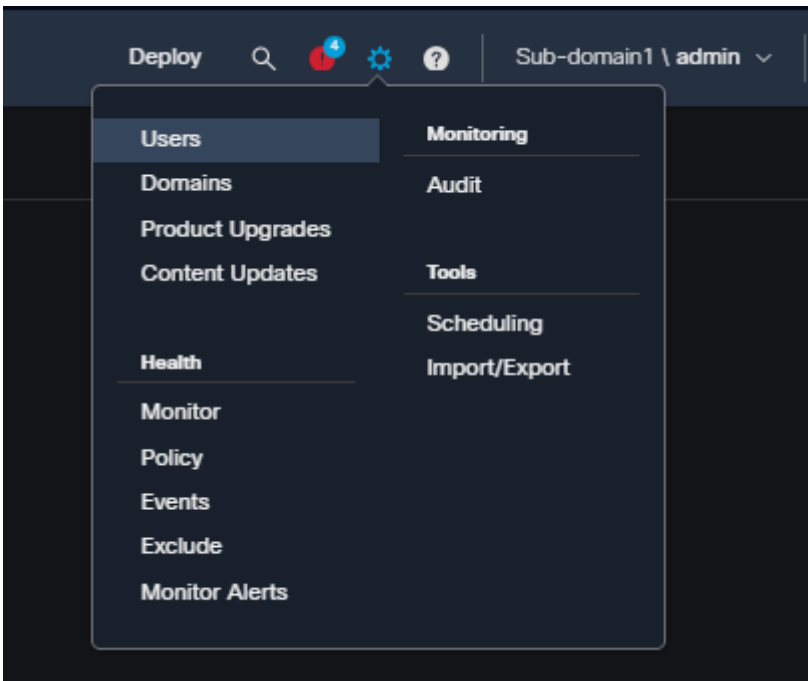
inline_image_5.png

Configuratiestappen voor gebruikersbeperking subdomein

- Navigeer naar het specifieke subdomein waar de toegang moet worden beperkt en maak de gebruikersaccount aan onder System / Gebruikers.



inline_image_6.png



inline_image_7.png

User Configuration

User Name

Real Name

Email Address

Authentication Use External Authentication Method

Password

Confirm Password

Maximum Number of Failed Logins (0 = Unlimited)

Minimum Password Length

Days Until Password Expiration (0 = Unlimited)

Days Before Password Expiration Warning

Options

- Force Password Reset on Login
- Check Password Strength
- Exempt from Browser Session Timeout

User Role Configuration

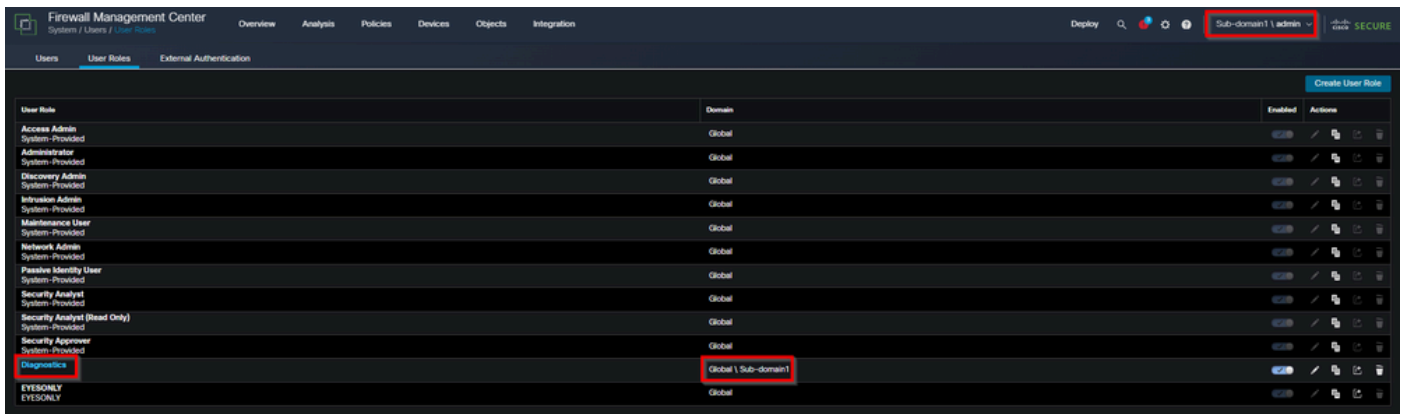
Default User Roles

- Administrator
- Security Analyst
- Security Analyst (Read Only)
- Security Approver
- Intrusion Admin
- Access Admin
- Network Admin
- Maintenance User
- Discovery Admin
- Passive Identity User

Custom User Roles EYESONLY (Global)

inline_image_8.png

- Maak aangepaste rollen binnen het subdomein onder Systeem / Gebruikersrollen. Aangepaste gebruikersrollen die in een subdomein zijn gemaakt, zijn alleen beschikbaar binnen dat domein en kunnen niet worden geopend vanuit andere domeinen.



inline_image_9.png

- Wijs de aangepaste rol toe aan de gebruiker. De gebruiker erft alleen rechten voor het domein waar zowel de gebruiker als de rol zijn gemaakt.

The image shows two overlapping dialog boxes. The top one is titled "User Configuration" and contains fields for "User Name" (Sub1User), "Real Name" (Sub1User), "Email Address", "Authentication" (Use External Authentication Method), "Password", "Confirm Password", "Maximum Number of Failed Logins" (5), "Minimum Password Length" (8), "Days Until Password Expiration" (0), "Days Before Password Expiration Warning" (0), and "Options" (Force Password Reset on Login, Check Password Strength, Exempt from Browser Session Timeout). The bottom dialog box is titled "User Role Configuration" and contains "Default User Roles" (Administrator, Security Analyst, Security Analyst (Read Only), Security Approver, Intrusion Admin, Access Admin, Network Admin, Maintenance User, Discovery Admin, Passive Identity User) and "Custom User Roles" (Diagnostics (Global \ Sub-domain1), EYESONLY (Global)). Both dialog boxes have "Cancel" and "Save" buttons at the bottom right.

inline_image_10.png

- Gebruikersaanmeldingsformaat voor subdomeingebruikers. Gebruikers die in subdomeinen zijn gemaakt, moeten dit aanmeldingsformaat gebruiken:

Gebruikersnaam: Subdomein\gebruikersnaam

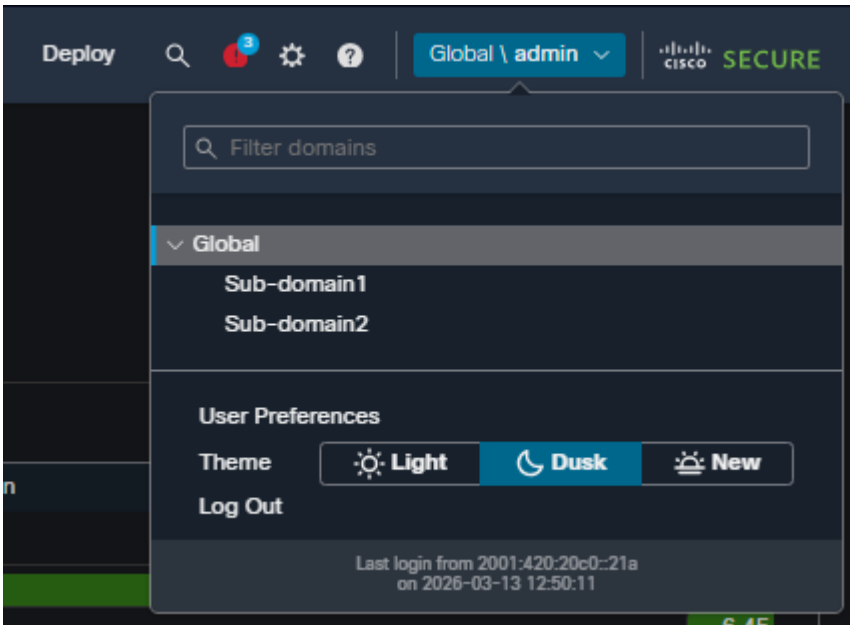
Wachtwoord: [gebruikerswachtwoord]



inline_image_11.png

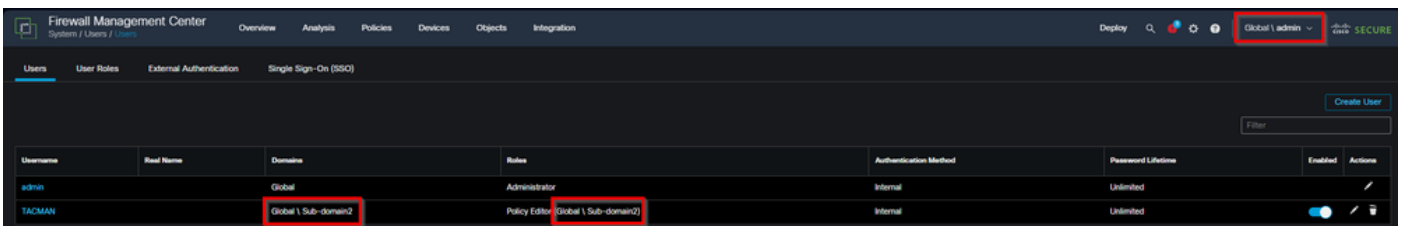
Configuratiestappen voor gebruikers met een wereldwijd domein met subdomeinbeperkingen

- Maak de gebruiker aan in het globale domein onder Systeem / Gebruikers. Gebruik een beheerdersaccount met globale domeintoegang om de gebruiker aan te maken.

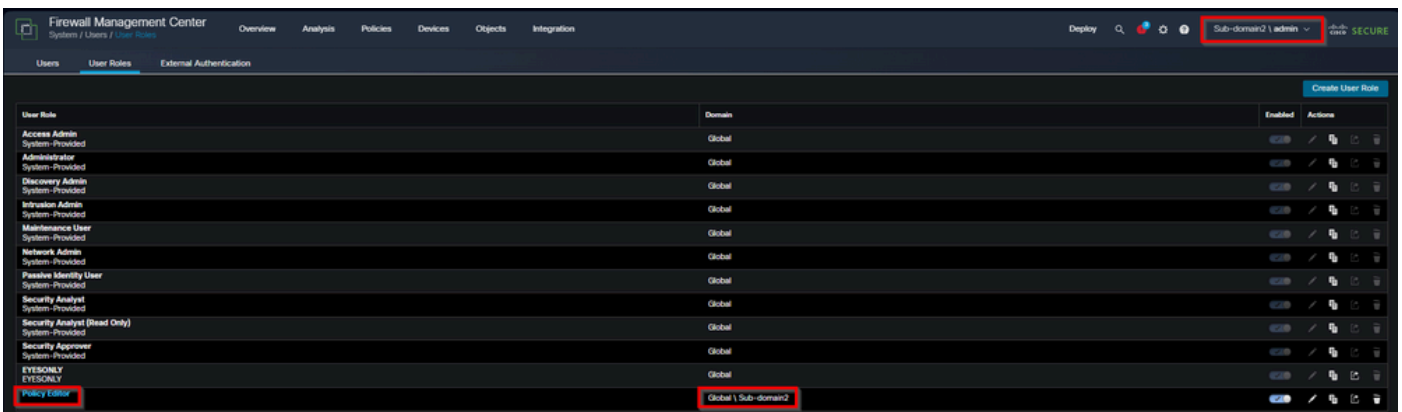


inline_image_12.png

- Wijs alleen rollen toe voor specifieke subdomeinen onder Systeem / Gebruikers. Wijs in de gebruikersconfiguratie rollen uitsluitend toe aan het (de) doelsubdomein(en) zonder globale domeinmachtigingen te verstrekken.



inline_image_3.png



inline_image_14.png

- Deze gebruikers kunnen alleen inloggen met hun gebruikersnaam, zonder domeinspecificatie:

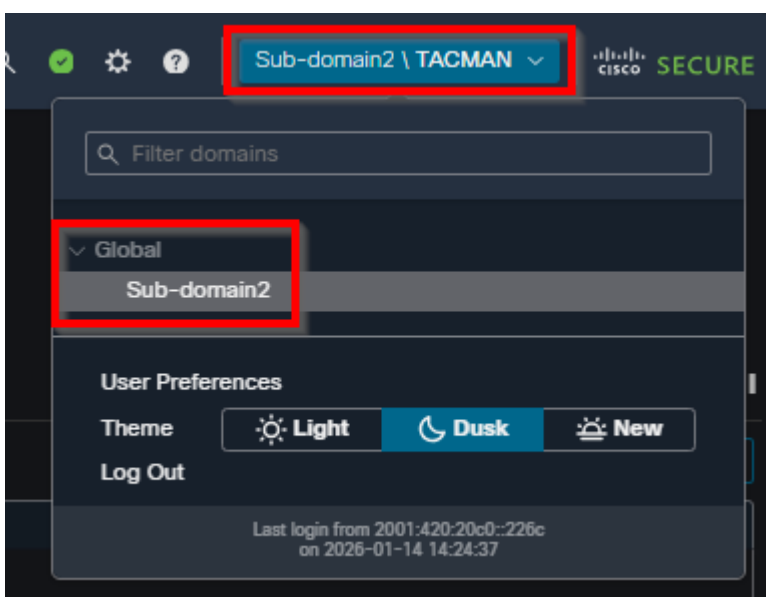
Gebruikersnaam: gebruikersnaam

Wachtwoord: [gebruikerswachtwoord]



inline_image_15.png

- De gebruiker heeft alleen toegang tot de subdomeinen waar rollen specifiek zijn toegewezen, zonder toegang tot Global domain of andere subdomeinen.



Flexibiliteit van roltoewijzing

Gebruikers kunnen in elk domein verschillende rechten hebben:

- Alleen-lezen rechten in het globale domein met beheerdersrechten in een afstammingsdomein
- Geen globale domeintoegang met volledige beheerdersrechten in specifieke subdomeinen
- Rechten voor beleidseditor in één subdomein zonder toegang tot andere subdomeinen

Overwegingen van externe gebruikers

Voor externe gebruikers (LDAP- of RADIUS-verificatie):

- Als gebruikersrollen worden toegewezen via groepslidmaatschap of gebruikerskenmerken, kunnen de minimale toegangsrechten niet worden verwijderd.
- Extra rechten kunnen een groter bereik krijgen dan de standaardgebruikersrol.
- Externe verificatieobjecten zijn alleen beschikbaar in het domein waarin ze zijn gemaakt.
- Individuele gebruikersmachtigingen moeten worden geconfigureerd op een groter bereik dan de rol van standaardgebruiker voor de juiste beperking.

Beperkingen en overwegingen

- Aangepaste gebruikersrollen die zijn gemaakt in voorouderdomeinen kunnen niet worden bewerkt vanuit afstammingsdomeinen.
- Shell Authentication is alleen beschikbaar in Global domain, niet in subdomeinen.
- Gebruikersvoorkeuren en dashboardinstellingen zijn van toepassing op alle domeinen waartoe het account toegang heeft.
- Toestemmingswijzigingen voor gebruikers worden afzonderlijk geconfigureerd en niet in groepen of in bulkmethoden.

Oorzaak

De vereiste vloeit voort uit de noodzaak om granulaire toegangscontrole te implementeren in FMC-implementaties met meerdere domeinen waarbij gebruikers verschillende toegangsniveaus tot globale en subdomeinen nodig hebben, met specifieke beperkingen tussen domeinen om de veiligheidsgrenzen te handhaven.

Verwante inhoud

- [Beheerdershandleiding Cisco Secure Firewall Management Center, 7.6: Gebruikers](#)
- [Beheerdershandleiding van het Cisco Secure Firewall Management Center, 7.6: Aangepaste gebruikersrollen maken](#)
- [Beheerdershandleiding Cisco Secure Firewall Management Center, 7.6: Een interne gebruiker toevoegen of bewerken](#)
- [Beheerdershandleiding van het Cisco Secure Firewall Management Center, 7.6: Gebruikers en domeinen](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.