Integratie van ISE en SecureX op locatie via orkestratie

Inhoud

Inleiding

Dit document beschrijft de stappen om Identity Services Engine en SecureX via Orchestration te integreren met een workflow van Cisco Secure Gateway-hub.

Voorwaarden

Cisco raadt u aan kennis te hebben over deze onderwerpen:

- Ervaring met Cisco ISE-configuratie
- Kennis van ISE-API
- Kennis over SecureX-orkestratie

Vereisten

U moet Cisco ISE hebben geïmplementeerd in uw netwerk en over een actieve SecureX-account beschikken. De orkestratiewerkstromen worden geactiveerd via de SecureX browser extensie.

In ons voorbeeld is de werkstroom die gebruikt moet worden geïmporteerd vanuit de Cisco Secure GitHub pagina, deze procedure is ook van toepassing op een aangepaste werkstroom.

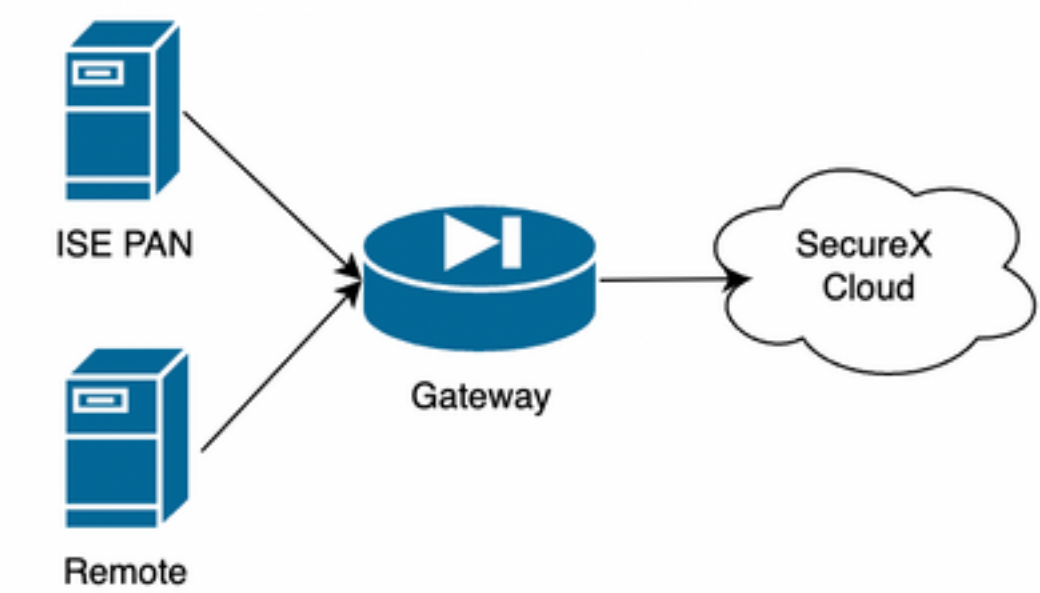
Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

- Identity Services Engine ISE-versie 3.1
- SecureX-account
- SXO Remote device versie 1.7

Configureren

Netwerkdiagram



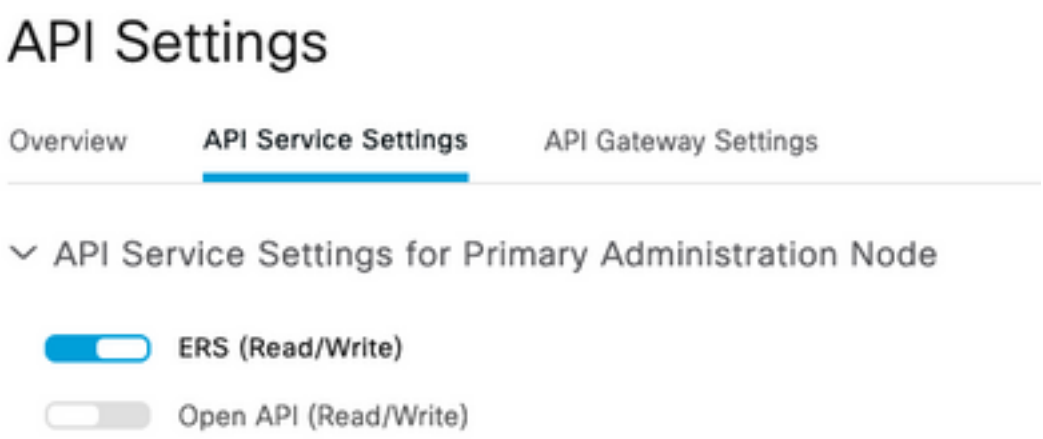
In ons voorbeeld worden ISE PAN en Remote server in hetzelfde subnetje geplaatst om directe connectiviteit te hebben.

Aangezien ISE een on-premise-apparaten is, kan de Remote-server in contact staan met de Secure-X-cloud en de informatie doorsturen naar het ISE PAN

Configuraties

ISE-PAN-configuratie

1. Navigeer naar **Beheer > Systeem > Instellingen > API-instellingen >API-serviceinstellingen** en schakel **ERS in (Lezen/schrijven)**

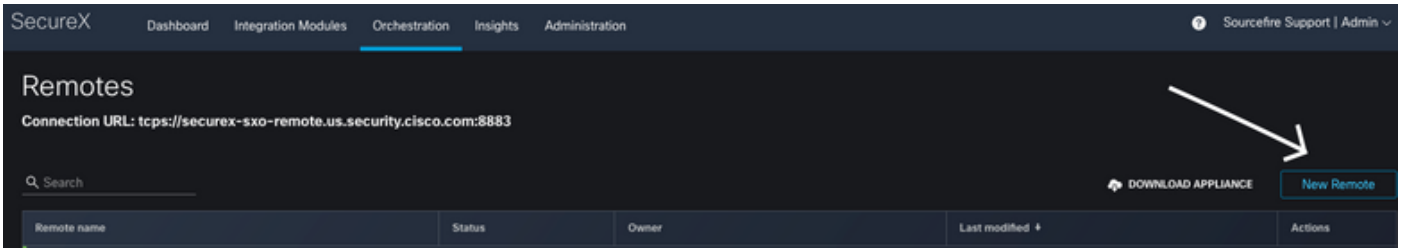


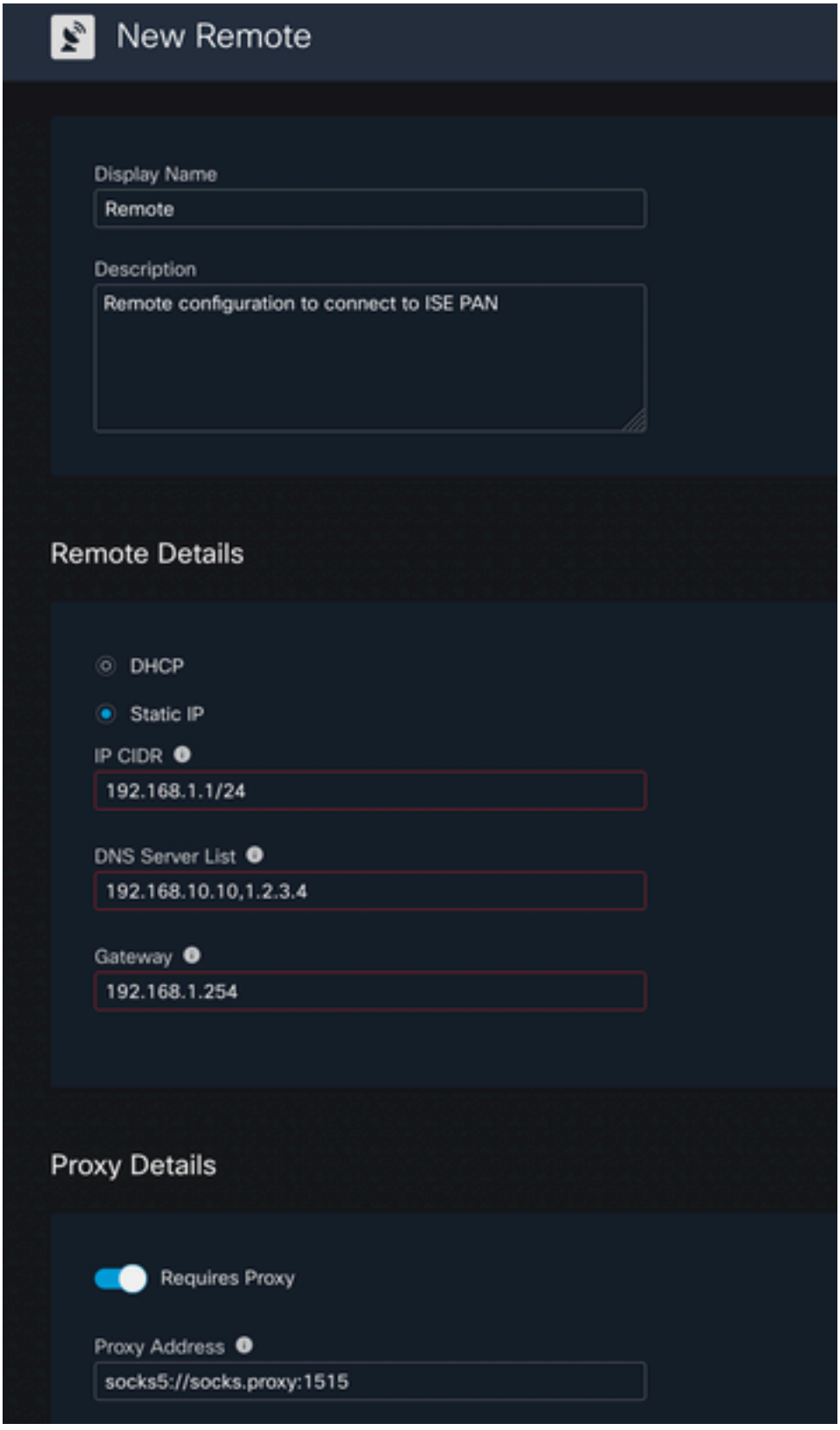
2. (Optioneel) Maak een nieuwe gebruiker voor de Secure-X-verbinding, navigeer naar **Beheer > Systeem > Admin Access > Beheerder > Beheerders** en maak een nieuwe gebruiker, deze nieuwe gebruiker moet beschikken over "ERS Admin"-rechten of het kan een super-beheerder gebruiker zijn.

Externe server configureren en implementeren

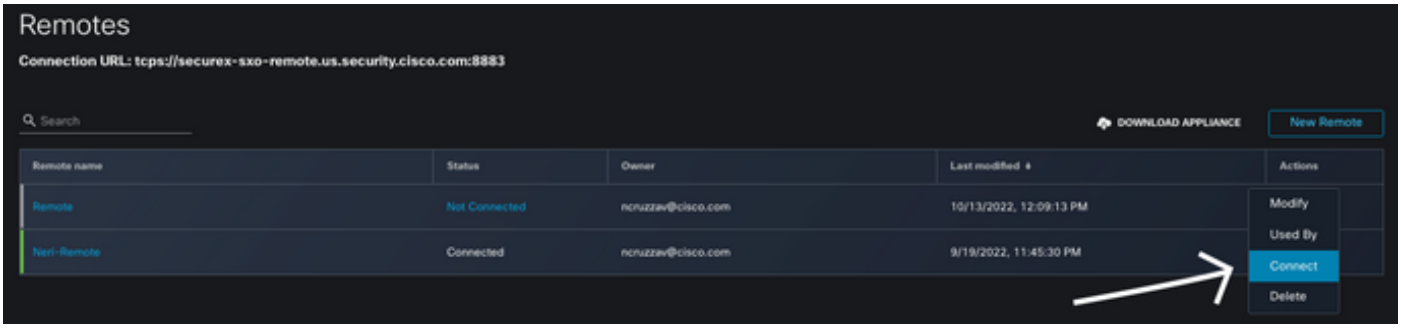
1. Configureer de externe server op de Secure-X-console naar **Orchestration > Admin > Remote Configuration** en selecteer optie **New Remote,** de IP-adresinformatie moet worden gebruikt wanneer de VM wordt gemaakt en moet zich bevinden in hetzelfde subnetje waar het ISE-PAN wordt geïmplementeerd.

> **Opmerking:** Als de verbinding met de cloud gebeurt via een proxy, wordt momenteel alleen een SOCKS5 proxy voor dit doel ondersteund.

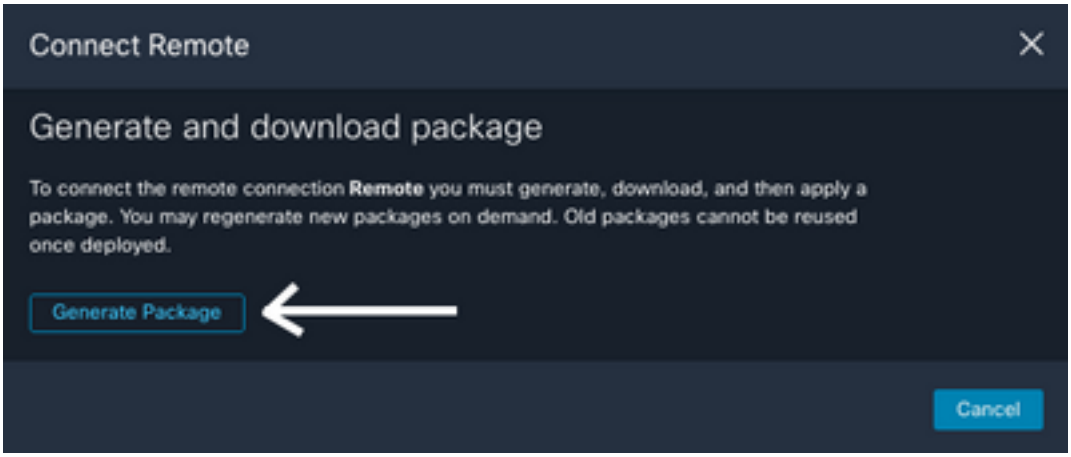




2. Download de instellingen die voor de VM-implementatie moeten worden gebruikt. Zodra de informatie is opgeslagen, verschijnt de afstandsbediening als "**Not Connected"**, navigeer onder acties en selecteer **Connect**



Selecteer **Generate Package,** deze actie downloadt een .zip-bestand dat de informatie bevat die zojuist is geconfigureerd om te worden gebruikt wanneer de VM wordt geïmplementeerd.

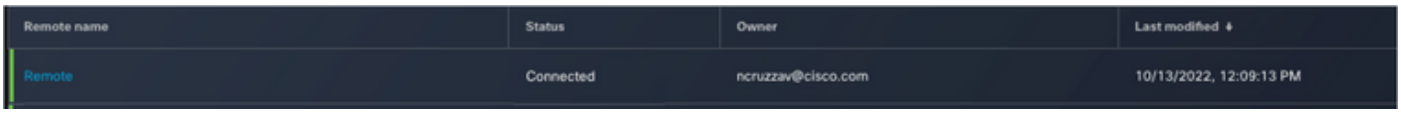


3. Download en installeer de VM, naast **New Remote** selecteer **DOWNLOAD APPLICATIE** deze actie downloadt een OVA image dat u moet gebruiken om de externe server te implementeren.

Raadpleeg de handleiding [SecureX Remote Setup voor](#) de specificaties van de externe VM

De gedownloade informatie in het ZIP-bestand moet op de **gecodeerde gebruikersgegevens** worden gebruikt wanneer de VM wordt gemaakt. Hierdoor wordt de geconfigureerde externe informatie in de server ingevuld zodra deze wordt opgestart.

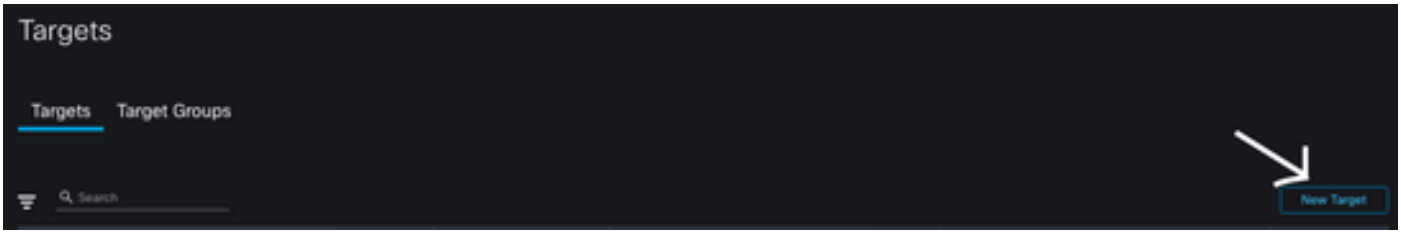
4. Zodra de VM is geïnstalleerd, maakt deze automatisch verbinding met de SecureX-account om te controleren of de verbinding is geactiveerd. Onder de configuratie van de afstandsbediening moet u een verandering zien van de status naar **"Connected"**



Het doel op SecureX configureren

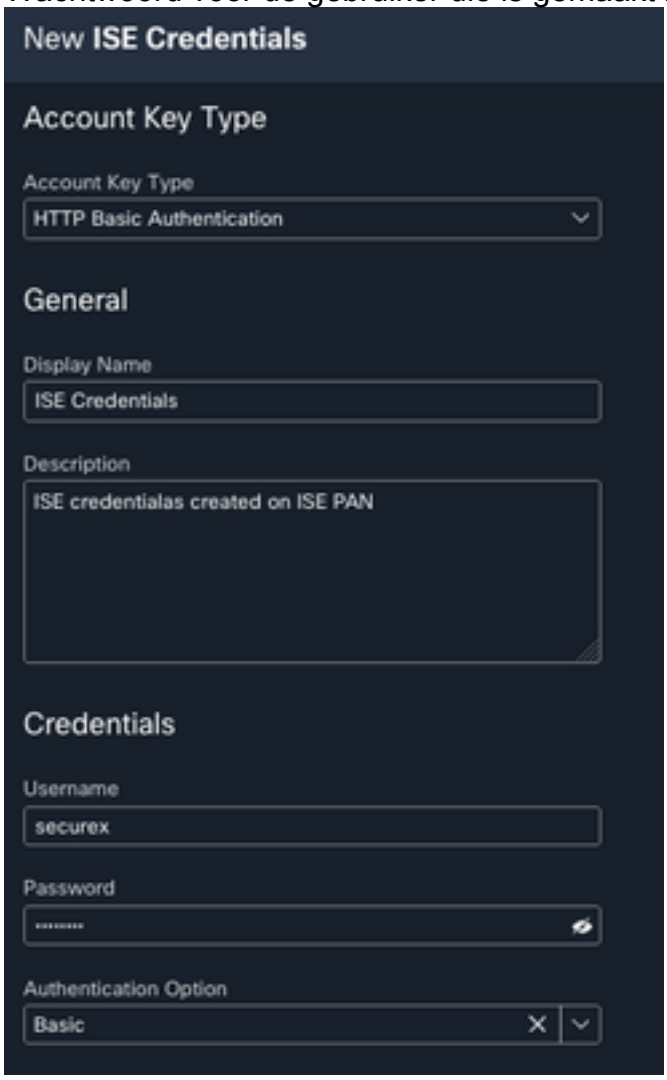
Voor Orchestratie om met een apparaat te werken is belangrijk om een **Doel** te configureren, Secure X gebruikt dit Doel om de API-oproepen te verzenden en met het apparaat te communiceren via Orchestratie

1. Navigeren naar **orkestratie > Doelstellingen > Nieuw doel**

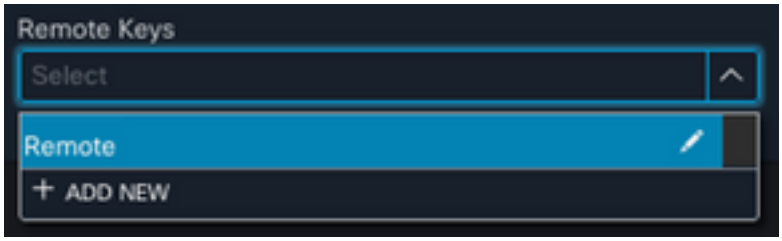


2. Vul de doelinformatie in met de volgende richtsnoeren

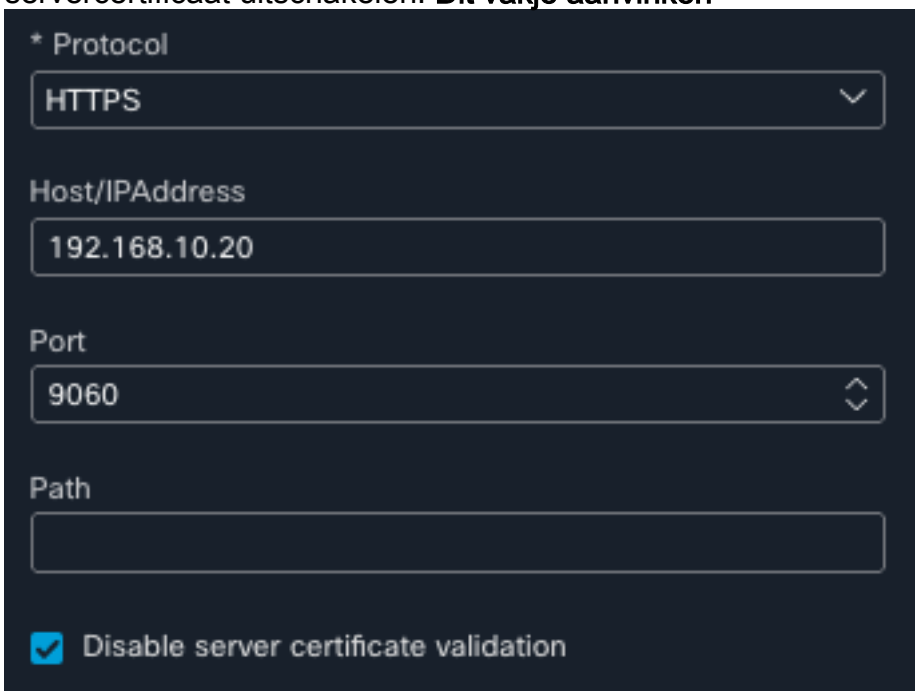
- Display naam: Doelcode
- Beschrijving: Een korte beschrijving om het doel van het doel te identificeren
- Rekeningsleutels: Hier moet u de gebruiker/het wachtwoord configureren voor toegang tot ISE via API Geen accountsleutels: **Onjuist**Standaardaccountsleutels: Selecteer **Nieuwe toevoegen** Type rekeningsleutel: **HTTP-basisverificatie**Display naam: Identificatiecode rekeningsleutelUsername: Gebruiker gemaakt op **ISE PAN** als ERS-beheerderWachtwoord: Wachtwoord voor de gebruiker die is gemaakt met **ISE PAN**Verificatieoptie: **Basis**



- Afstandsbediening: Hier moet u de eerder geconfigureerde externe verbinding selecteren Remote-toetsen: selecteer uw afstandsbediening in het uitrolmenu



- HTTP: Hier moet u de API-informatie voor het **ISE-PAN** configureren Protocol: **HTTPS**Host/IP-adres: **ISE-PAN privé-IP**Port: **9060**Pad: Laat het leegVerificatie servercertificaat uitschakelen: **Dit vakje aanvinken**



- Proxy: Aangezien de proxyconfiguratie in de externe configuratie is opgenomen, kunt u deze sectie leeg laten
- Selecteer **Indienen**

De workflow vanuit Cisco Secure GitHub importeren

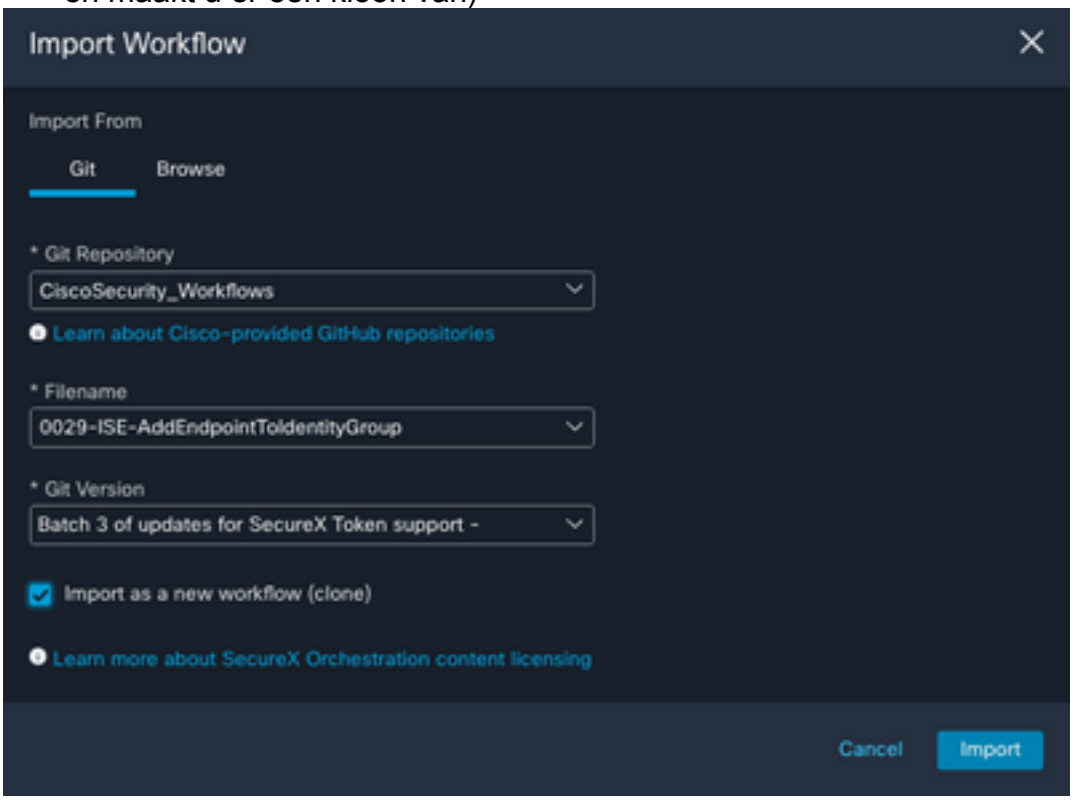
In dit voorbeeld is de werkstroom die moet worden gebruikt "Add Endpoint to Identity Group". U kunt een van de werkstromen op de Cisco Secure GitHub-pagina gebruiken of u kunt een aangepaste werkstroom maken.

1. Navigeren naar **Orchestration > Mijn werkstromen > Werkstroom importeren**

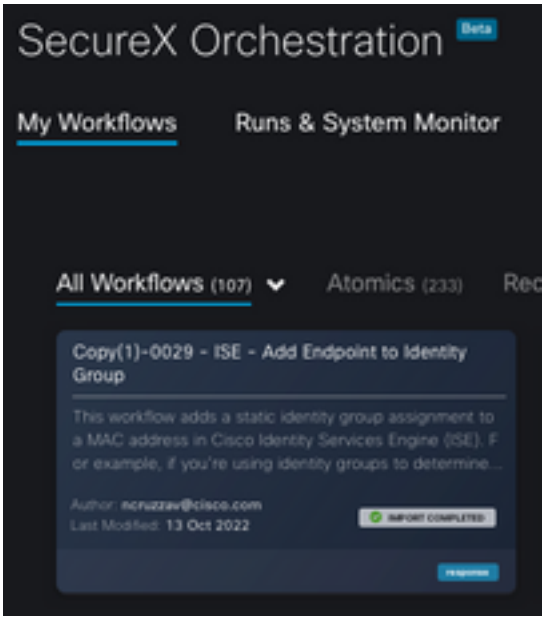
2. Om het werkschema te importeren, vul de informatie als volgt in en selecteer **Importeren;** om de te importeren workflow te identificeren, kunt u zoeken op naam of op werkstroomnummer

- Git Repository: **Cisco Security_Workflows** (waar de workflow zich bevindt)
- Bestandsnaam: **0029-ISE-AddEndpointToIdentityGroup** (selecteer het aantal werkstromen dat

u wilt gebruiken)
- Git versie: **Batch 3 van updates voor SecureX-token ondersteuning** (laatste versie)
- Importeren als een nieuwe werkstroom (kloon): **Controleer** (Hiermee importeert u de workflow en maakt u er een kloon van)

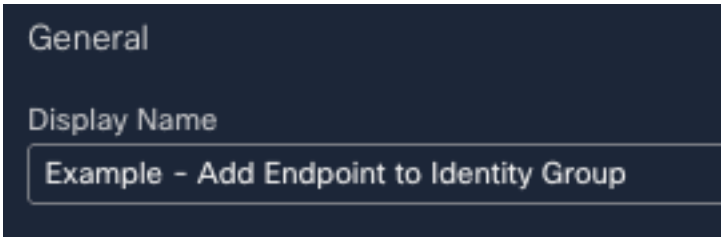


3. Zodra de nieuwe sjabloon is geïmporteerd, wordt deze weergegeven onder **Mijn werkstromen.** Selecteer de nieuwe werkstroom om de parameters te bewerken, zodat deze kunnen werken met **ISE**

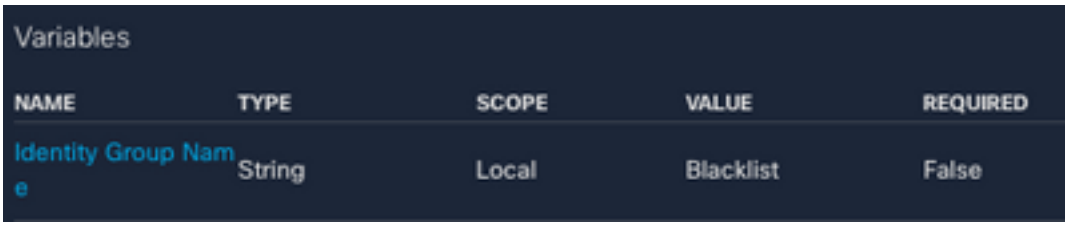


4. Aangezien dit een pre-build workflow is, hoeft u slechts 3 delen van de workflow te wijzigen:

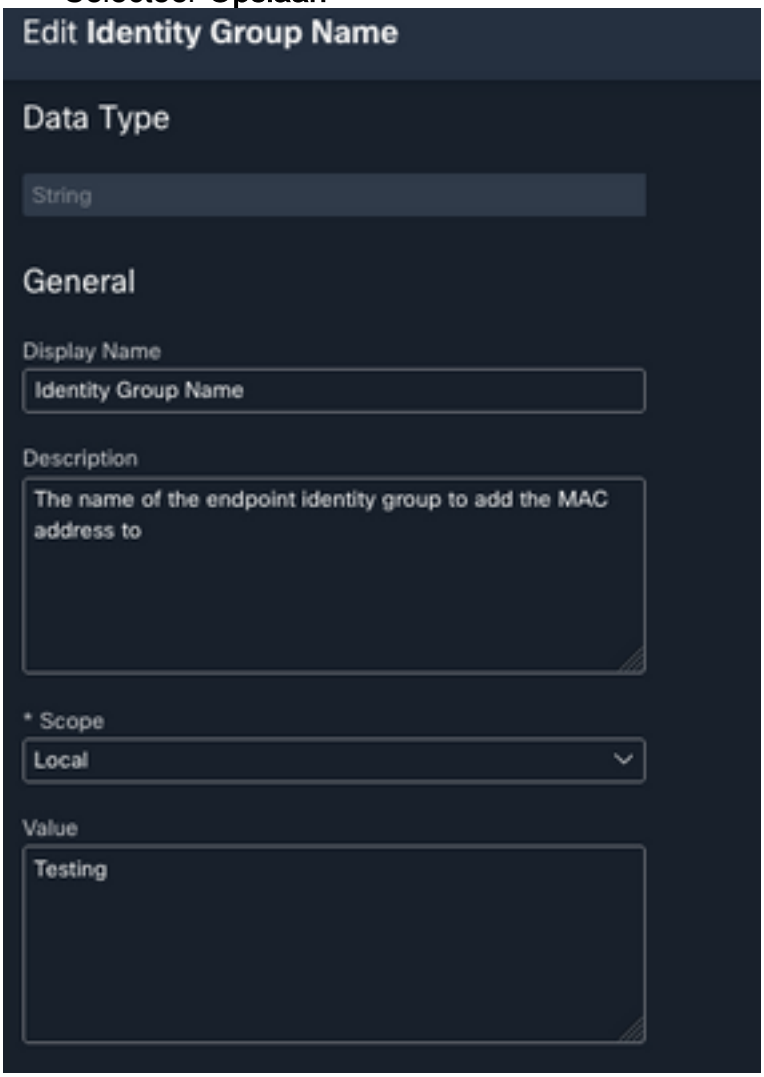
- Naam: Verander de naam van het display voor een betere identificatie



- Variabele voor identiteitsgroep Bewerk onder Variabelen de standaard **Identity Group Variable** is **Balcklist,** selecteer de variabele en configureer de Identity Group Name die u wilt wijzigen via Orchestration



- Selecteer **Opslaan**



- Doel: Eerder geconfigureerd voor het **doel** Doeltype: **HTTP-endpoint**Doel: **Naam van het geconfigureerde doel**

Verifiëren

Als alles is geconfigureerd is het tijd om de werkstroom te testen

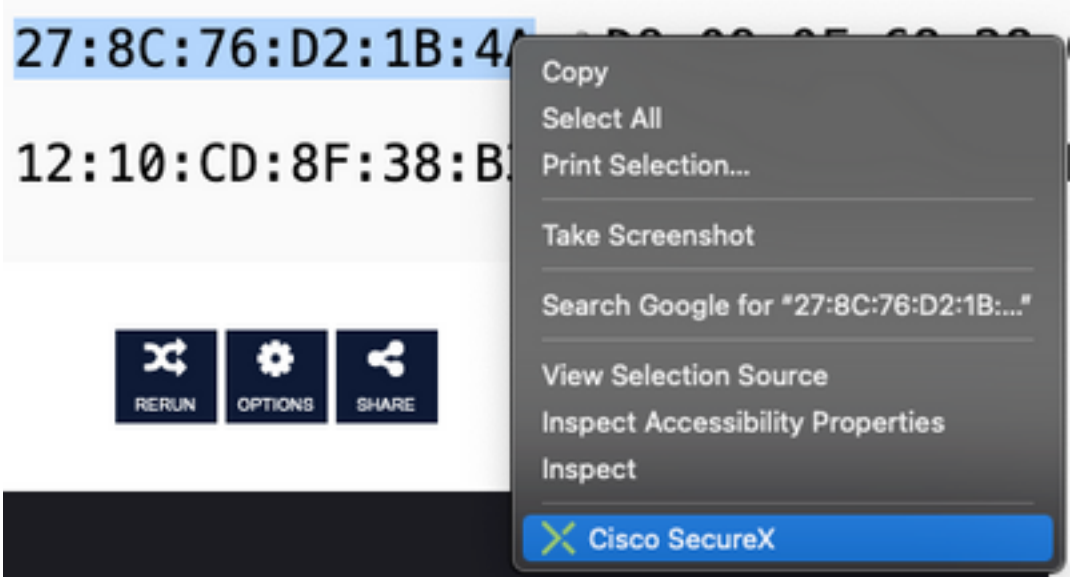
De workflow voor de test voert deze actie uit: als u een MAC-adres in een webpagina vindt, kan dit op ISE zelf of een andere webpagina zoals Threat Response; via de SecureX-browser-extensie zoekt de workflow naar dat MAC-adres in de ISE-database via API, als de MAC niet bestaat, wordt de waarneembare toegevoegd aan de Endpoint Identity Group zonder dat de waarde en de toegang tot ISE moeten worden gekopieerd.

Om dit aan te tonen, neem een kijkje in het volgende voorbeeld:

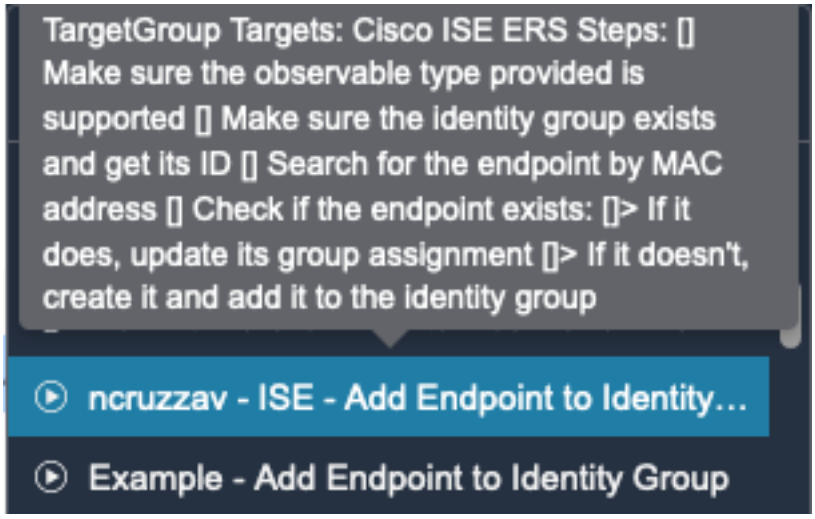
1. De geselecteerde workflow werkt met het waarneembare type **"MAC-adres"**

2. Zoek een MAC-adres op een webpagina en voer een rechtsklik uit.

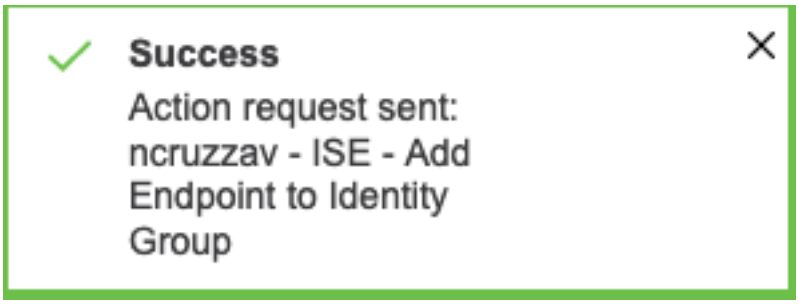
3. Selecteer de optie **SecureX**



4. Selecteer het **Workflow** dat voor u is gemaakt

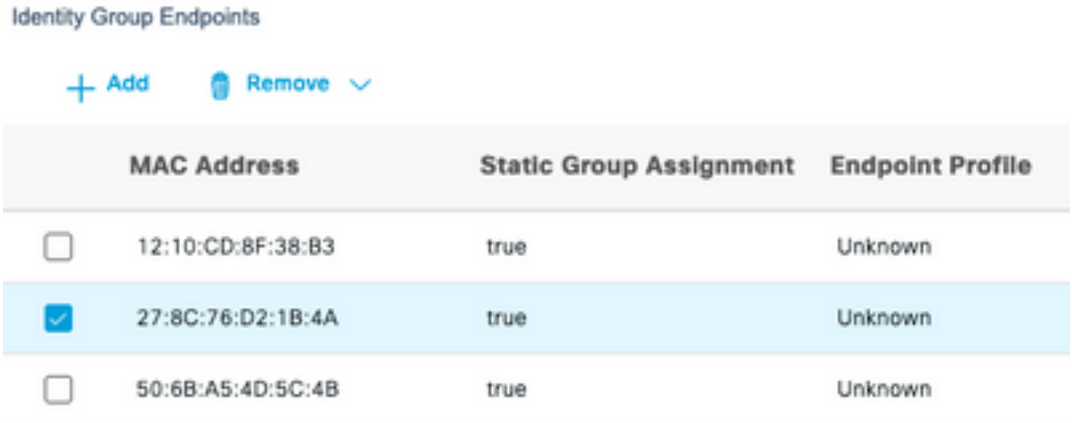


5. Bevestig dat de taak met succes is uitgevoerd



6. Navigeer op het **ISE PAN** naar **Beheer > Identity Management > Groepen > Endpoint Identity Groups > (De groep geconfigureerd op de workflow)**

7. Open de **Endpoint Identity Group** die in de workflow is geconfigureerd en bevestig dat de MAC Address-selectie is toegevoegd aan die MAC Address List



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.