Duo Two-Factor verificatie configureren voor FMC Management Access

Inhoud

Inleiding

In dit document worden de stappen beschreven die moeten worden uitgevoerd om externe verificatie met twee factoren voor beheertoegang te configureren op Firepower Management Center (FMC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Objectconfiguratie van Firepower Management Center (FMC)
- Beheer van Identity Services Engine (ISE)

Gebruikte componenten

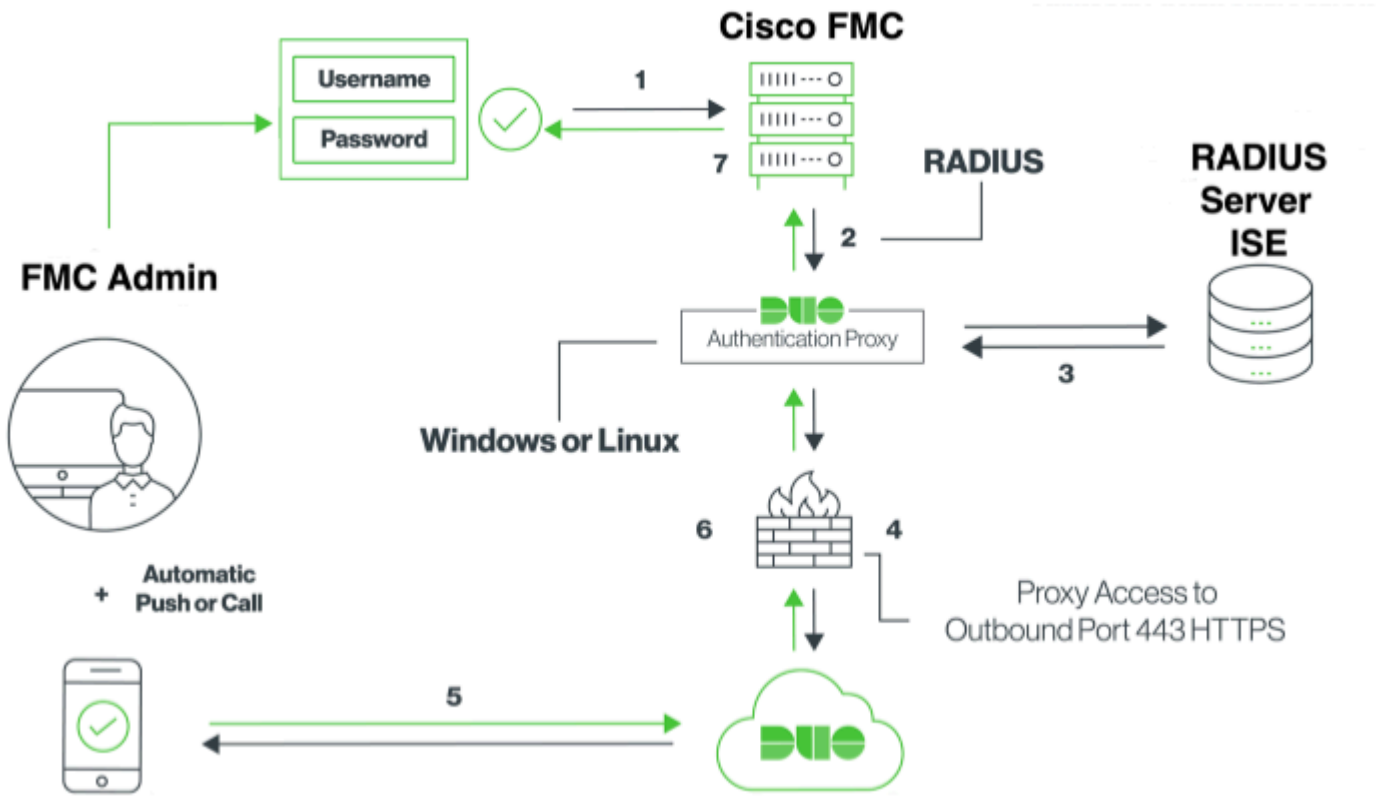
- Cisco Firepower Management Center (FMC) versie 6.3.0
- Cisco Identity Services Engine (ISE) actieve versie 2.6.0.156
- Ondersteunde versie van Windows (https://duo.com/docs/authproxy-reference#new-proxy-install) met een verbinding met FMC, ISE en het internet om te fungeren als de Duo Verificatie proxyserver
- Windows Machine om toegang te krijgen tot FMC-, ISE- en Duo-beheerportal
- Duo-webaccount

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.

Achtergrondinformatie

De FMC-beheerder verifieert via de ISE-server en een extra verificatie in de vorm van een push-melding wordt door de Duo-verificatieproxy-server naar het mobiele apparaat van de beheerder gestuurd.

Verificatiestroom



Verificatiestroom toegelicht

1. Primaire verificatie gestart op Cisco FMC.
2. Cisco FMC stuurt een verificatieaanvraag naar de Duo-verificatieproxy.
3. Voor primaire verificatie moet Active Directory of RADIUS worden gebruikt.
4. Duo Authenticatie Proxy-verbinding ingesteld met Duo Security over TCP-poort 443.
5. Secundaire authentificatie via de dienst van Duo Security.
6. Duo authenticatie proxy ontvangt de authenticatiereactie.
7. Cisco FMC GUI-toegang wordt verleend.

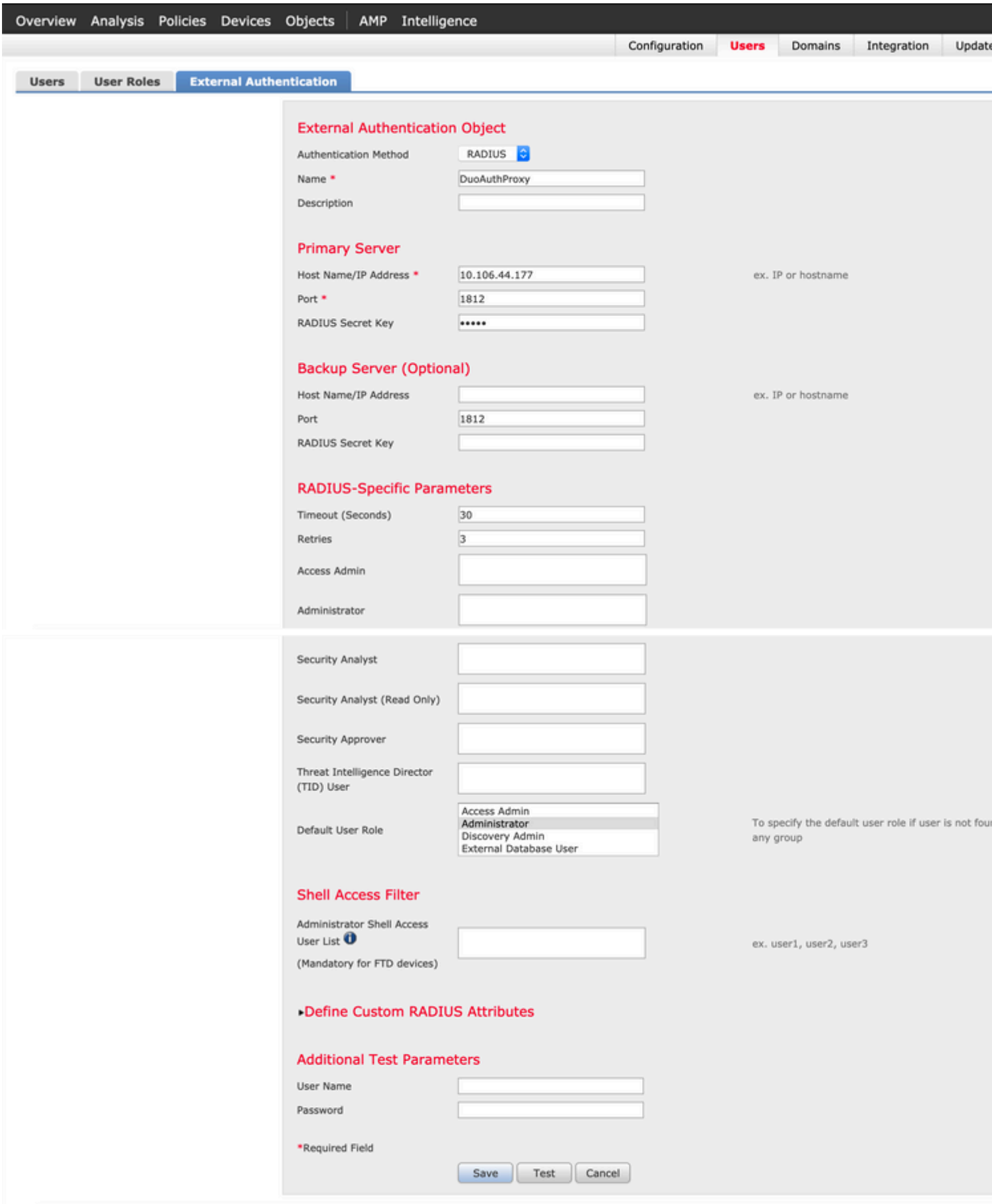
Configureren

Om de configuratie te voltooien, moet u rekening houden met deze secties:

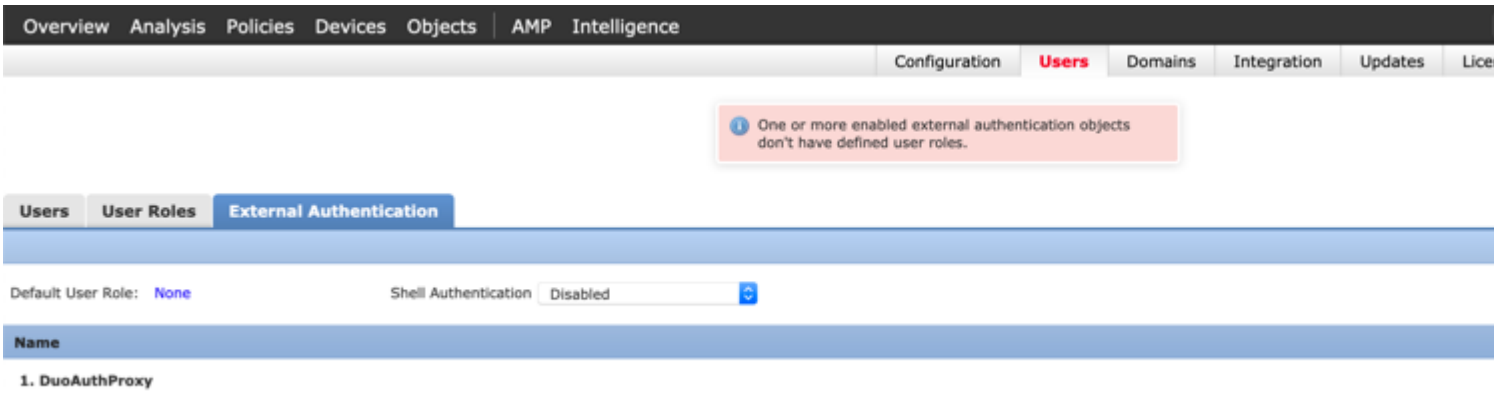
Configuratiestappen op FMC

Stap 1. Navigeer naar **Systeem > Gebruikers > Externe verificatie**. Maak een extern verificatieobject en stel de verificatiemethode in als RADIUS. Zorg ervoor dat de beheerder is geselecteerd onder de standaard gebruikersrol zoals in het afbeelding:

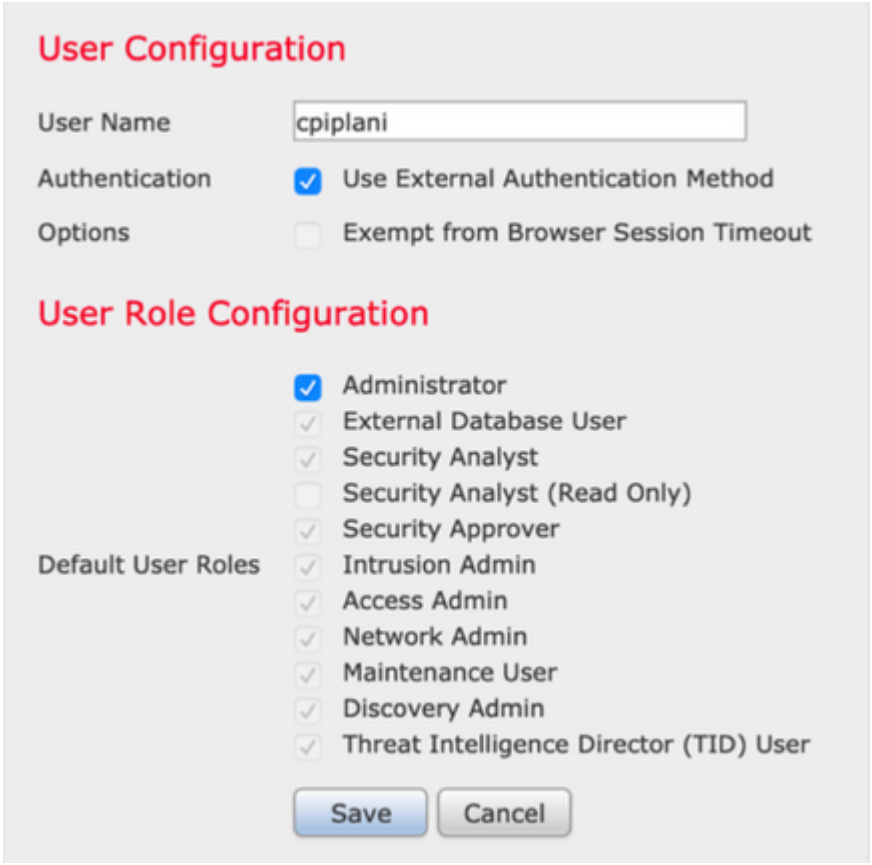
Opmerking: 10.106.44.177 is het voorbeeldadres van het IP-adres van de Duo-verificatieproxyserver.



Klik op **Opslaan** en **Toepassen**. Negeer de waarschuwing zoals weergegeven in het beeld:



Stap 2. Ga naar **Systeem > Gebruikers > Gebruikers**. Maak een gebruiker en controleer de verificatiemethode als extern zoals in de afbeelding:



Stap 1. Duo-verificatieproxyserver downloaden en installeren.

Log in op de Windows-machine en installeer de Duo Verificatie Proxy Server

Aanbevolen wordt een systeem te gebruiken met minimaal 1 CPU, 200 MB schijfruimte en 4 GB RAM

Opmerking: dit apparaat moet toegang hebben tot FMC, RADIUS-server (in ons geval) en Duo Cloud (internet)

Stap 2. Configureer het bestand **authproxy.cfg**.

Open dit bestand in een teksteditor zoals Kladblok++ of WordPad.

> Opmerking: De standaardlocatie is te vinden op C:\Program Files (x86)\Duo Security Verification Proxy\conf\authproxy.cfg

---

Bewerk het bestand **authproxy.cfg** en voeg deze configuratie toe:

<#root>

```
[radius_client]
```

host=10.197.223.23 Sample IP Address of the ISE server

secret=cisco

Password configured on the ISE server in order to register the network device

Het IP-adres van het VCC moet worden geconfigureerd in combinatie met de RADIUS-geheime sleutel.

<#root>

```
[radius_server_auto]
ikey=xxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxxx.duosecurity.com
```

radius_ip_1=10.197.223.76

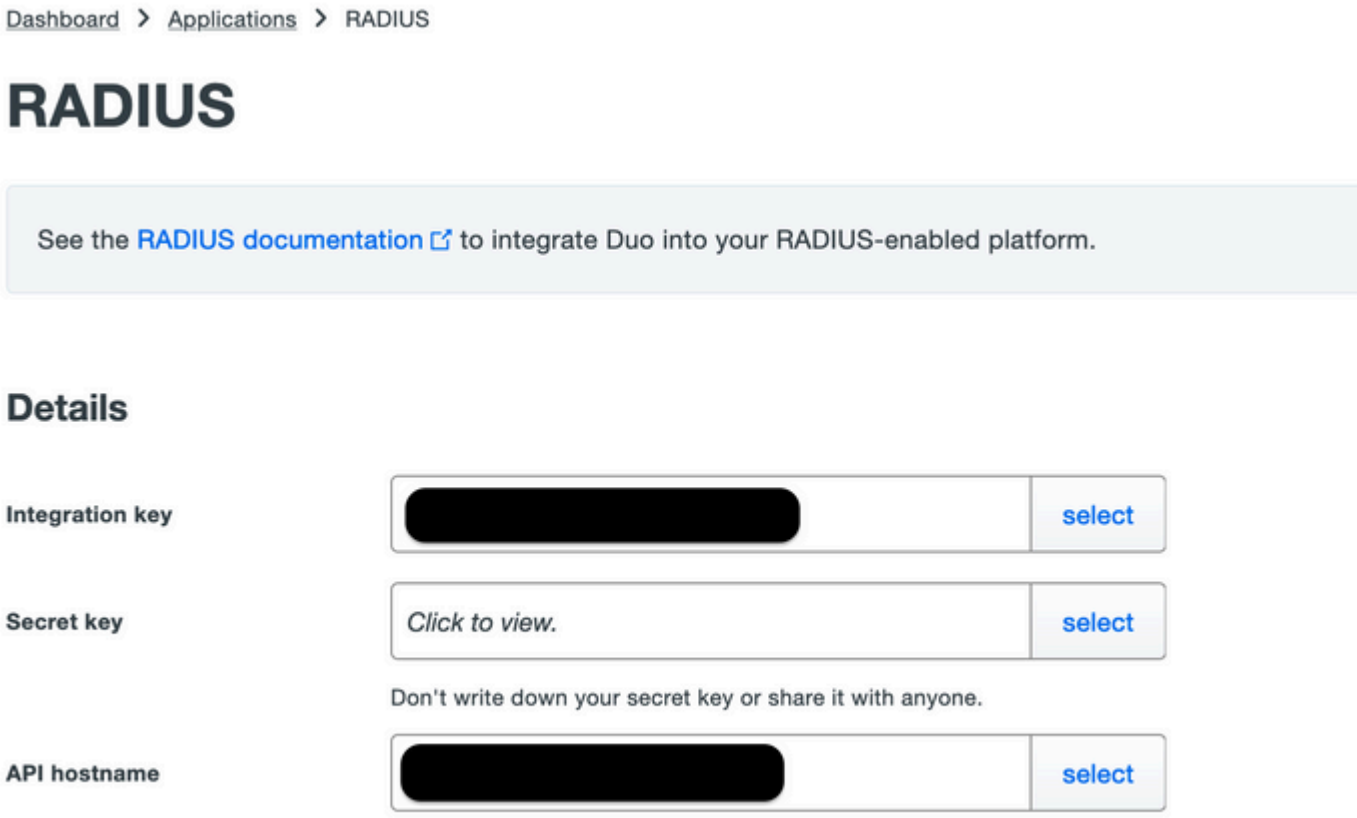
IP of FMC

radius_secret_1=cisco

Radius secret key used on the FMC

```
failmode=safe
client=radius_client
port=1812
api_timeout=
```

Verzeker u ervan dat u de parameters key, skey en api_host configureert. Meld u aan bij uw Duo-account (Duo Admin Login) en navigeer naar **Toepassingen > Bescherm een Toepassing** om deze waarden te verkrijgen. Selecteer vervolgens de RADIUS-verificatietoepassing zoals in de afbeelding:



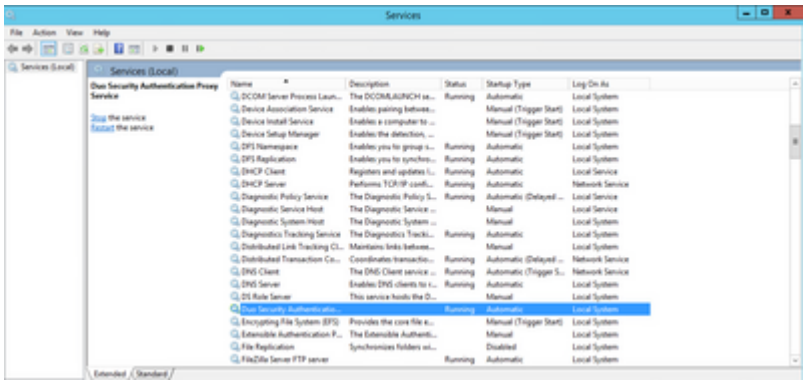
Integratiesleutel = ikey

geheime sleutel = sleutel

API-hostnaam = api_host

Stap 3. Start de Duo Security Verification Proxy-service opnieuw. **Sla** het bestand op en **start** de Duo-service opnieuw op de Windows-machine.

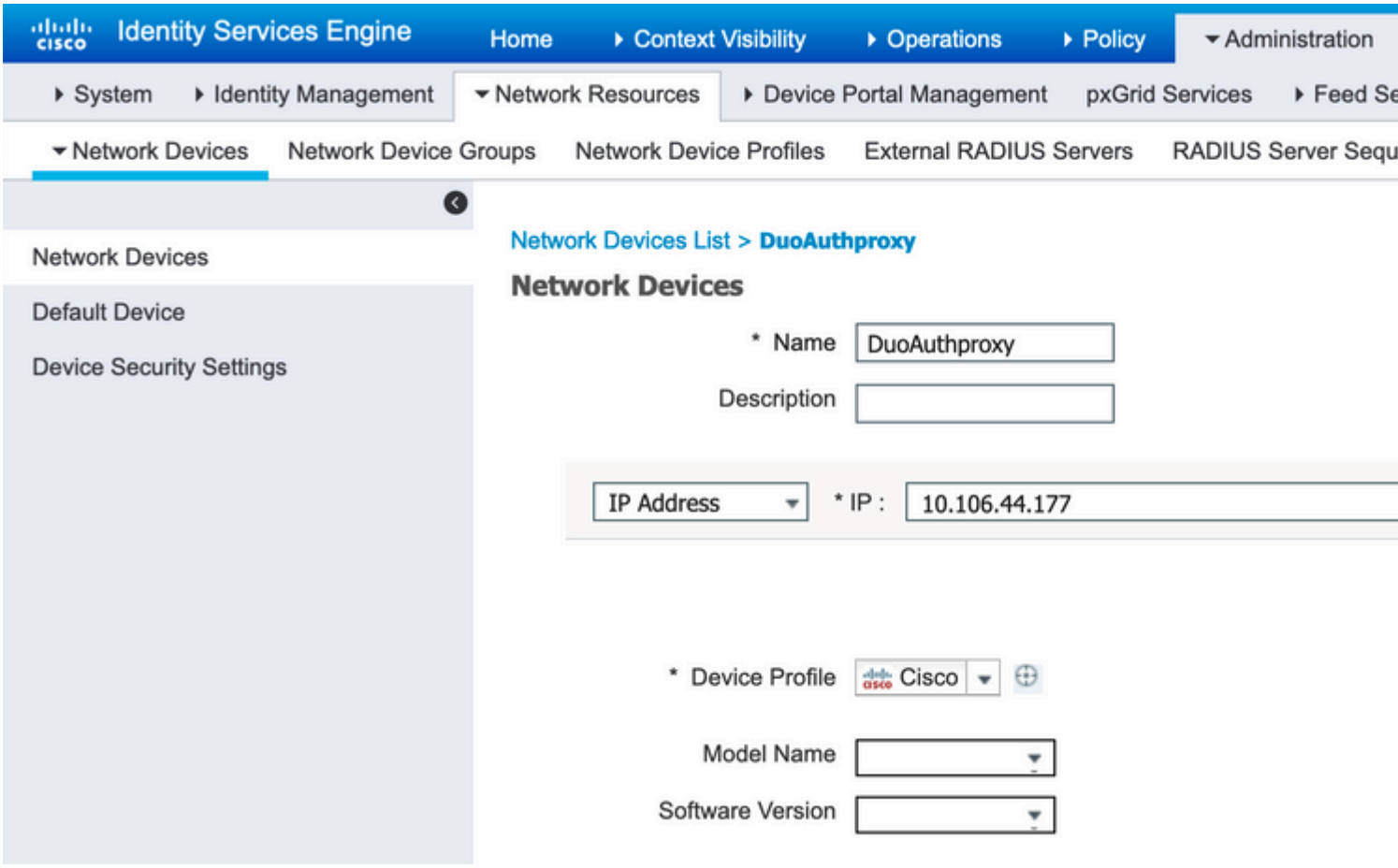
Open de Windows Services console (services.msc). Zoek de **Duo Security Verification Proxy-service** in de lijst met services en klik op **Opnieuw starten** zoals in de afbeelding:



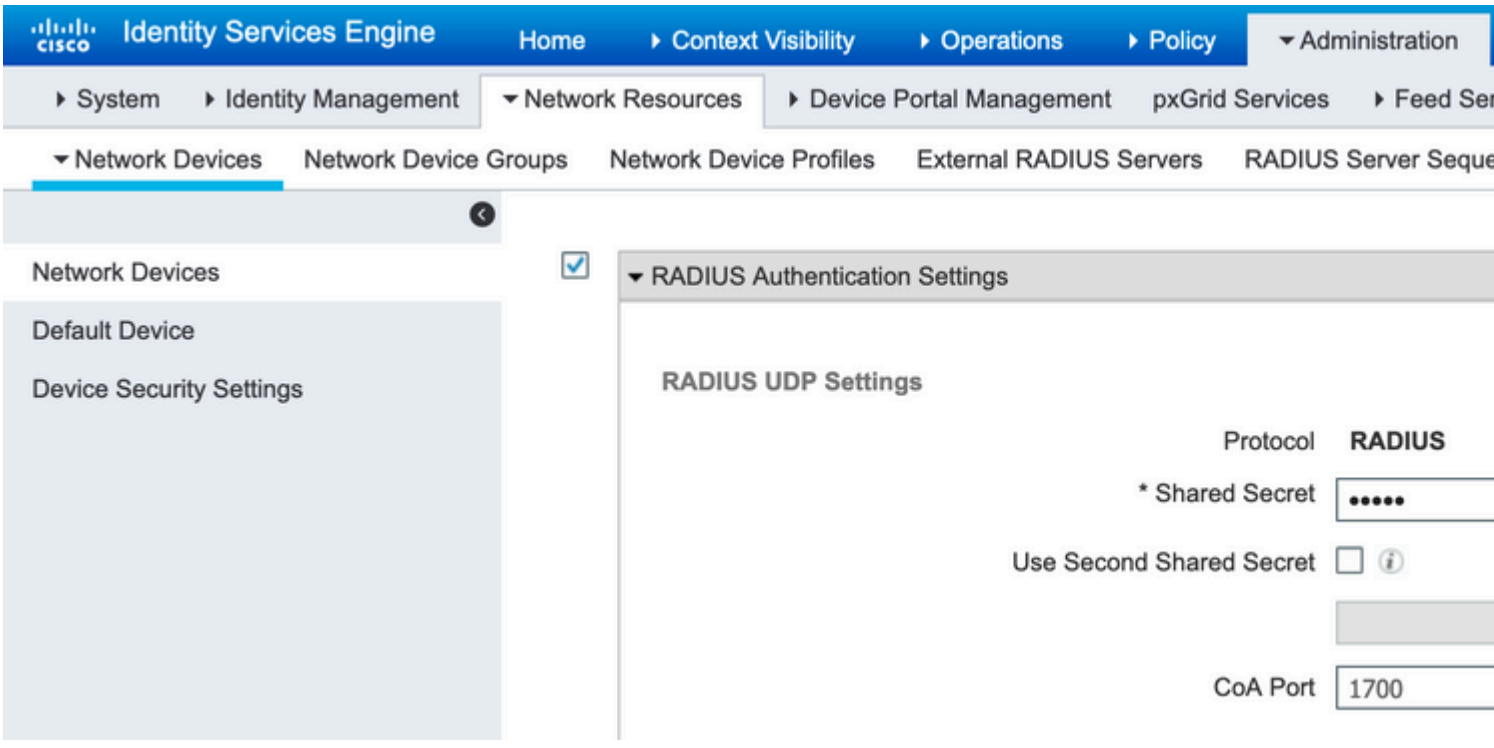
Configuratiestappen op ISE

Stap 1. Blader naar **Beheer > Netwerkapparaten en** klik op **Toevoegen** om het netwerkapparaat te configureren zoals in de afbeelding:

Opmerking: 10.106.44.177 is het voorbeeldadres van het IP-adres van de Duo-verificatieproxyserver.

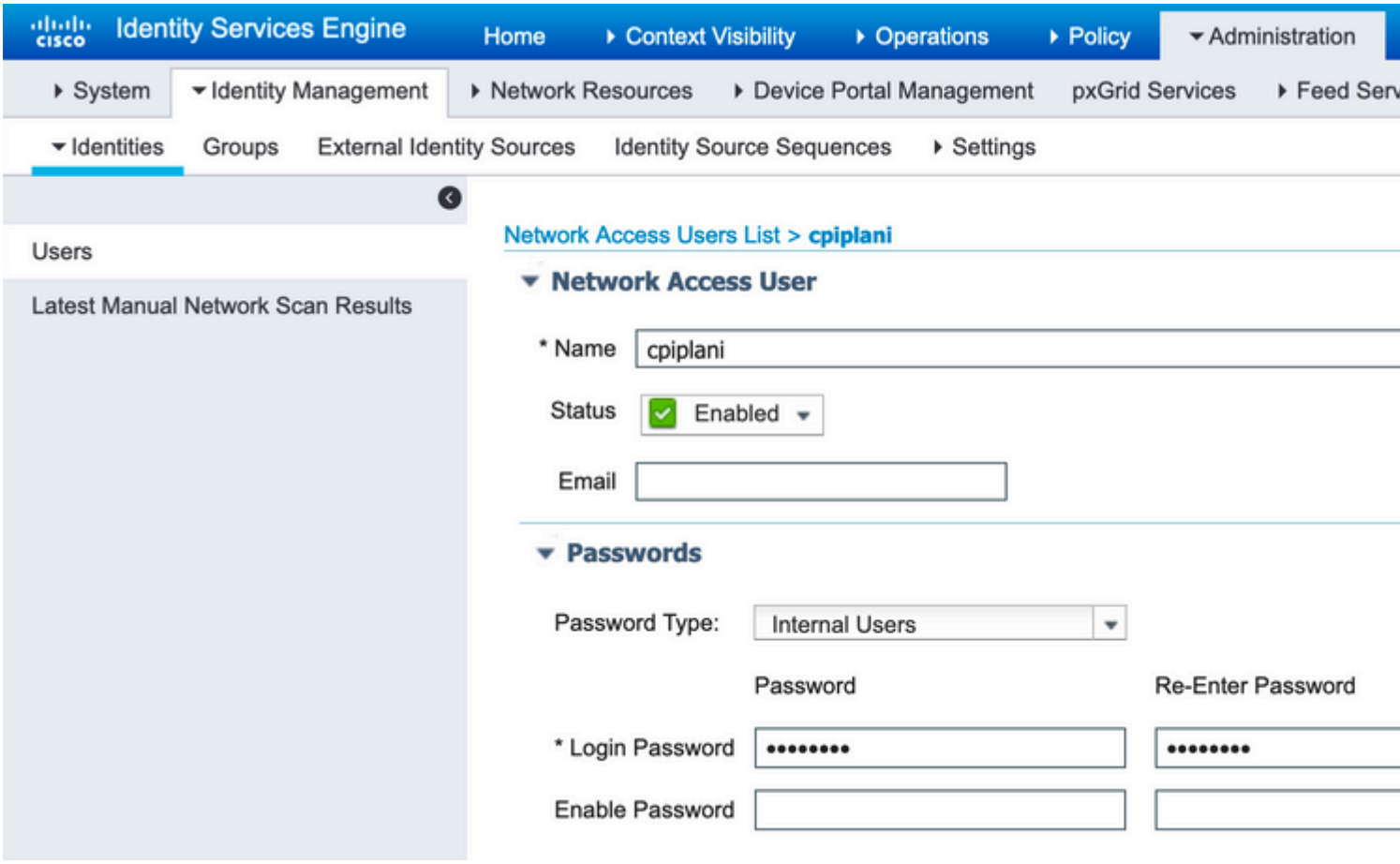


Configureer het **gedeelde geheim** zoals vermeld in **auteproxy.cfg** in het **geheim** zoals weergegeven in de afbeelding:



Stap 2. Ga naar **Beheer > Identiteiten**. Klik op **Add** om de Identity-gebruiker te configureren zoals in de

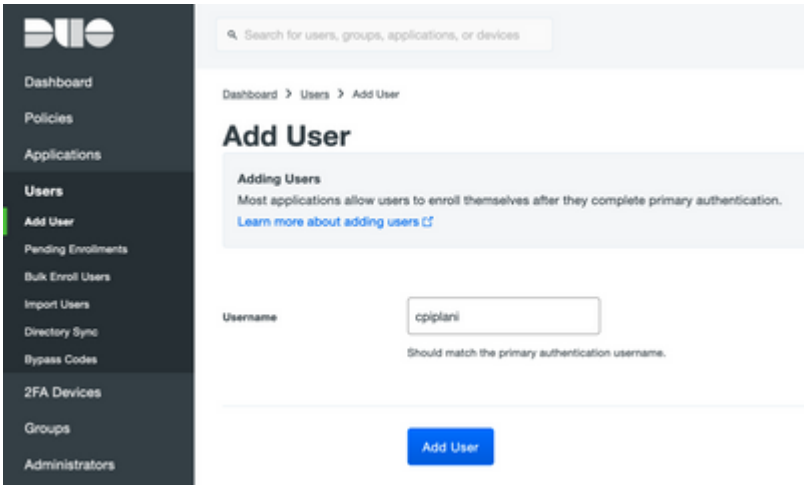
afbeelding:



Configuratiestappen voor Duo Management Portal

Stap 1. Maak een gebruikersnaam aan en activeer Duo Mobile op het eindapparaat.

Voeg de gebruiker toe op de Duo cloud administratie webpagina. Navigeer naar **Gebruikers > Gebruikers toevoegen** zoals in de afbeelding:



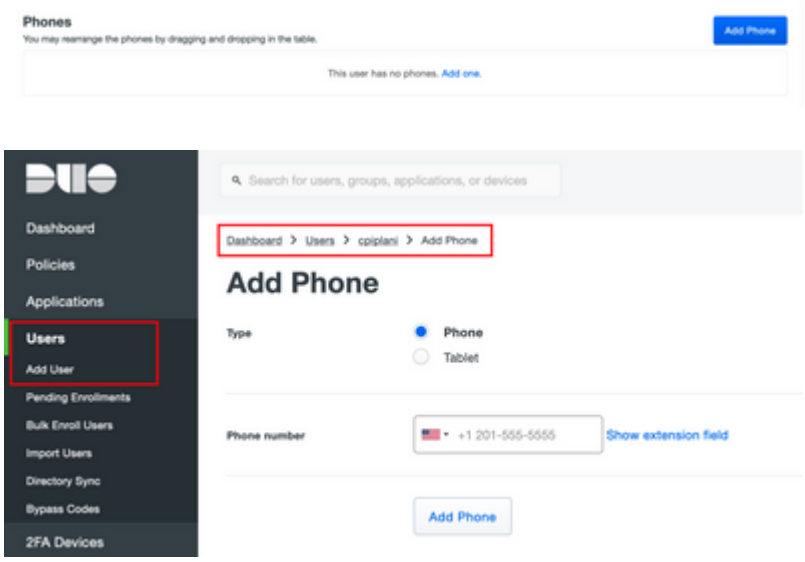
Opmerking: Zorg ervoor dat de eindgebruiker de Duo-app heeft geïnstalleerd.

[Handmatige installatie van Duo-toepassing voor IOS-apparaten]

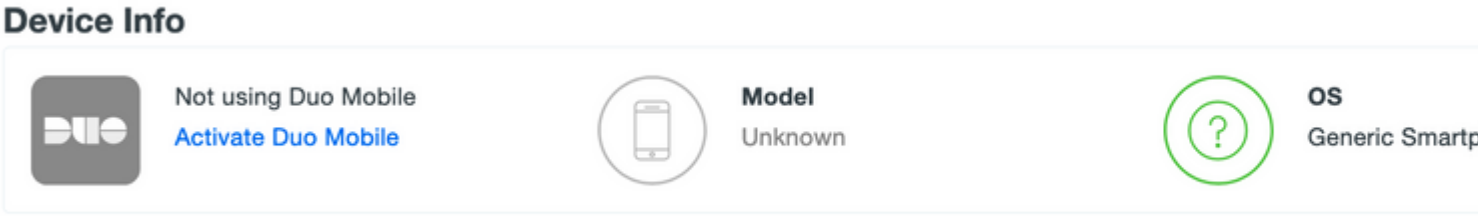
[Handmatige installatie van Duo-toepassing voor Android-apparaten]

Stap 2. Automatische generatie van code.

Voeg het telefoonnummer van de gebruiker toe zoals in de afbeelding:



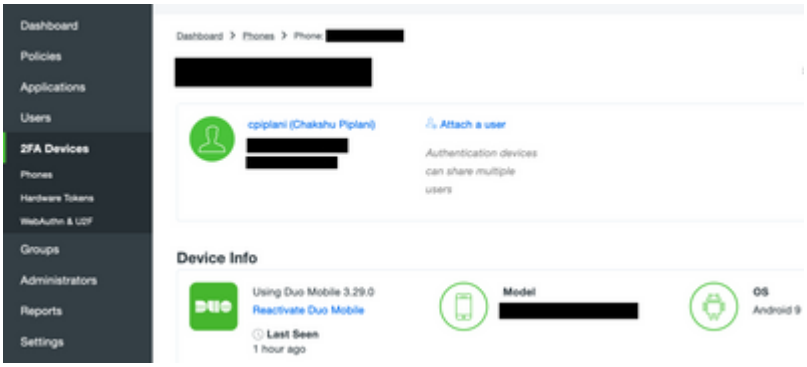
Kies **Duo Mobile activeren** zoals in de afbeelding:



Kies **Duo Mobile Activeringscode genereren** zoals in de afbeelding:

Kies **Instructies per sms verzenden** zoals in de afbeelding:

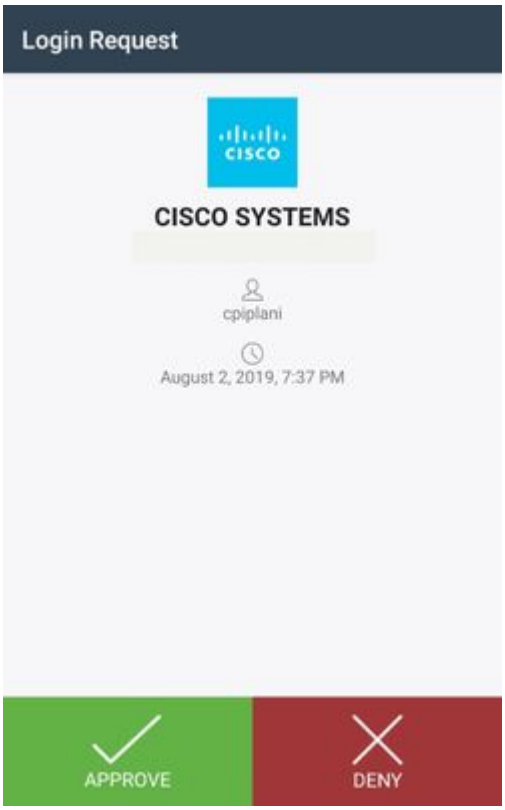
Klik op de koppeling in de SMS en Duo app wordt gekoppeld aan de gebruikersaccount in het gedeelte Apparaatinfo, zoals in de afbeelding:



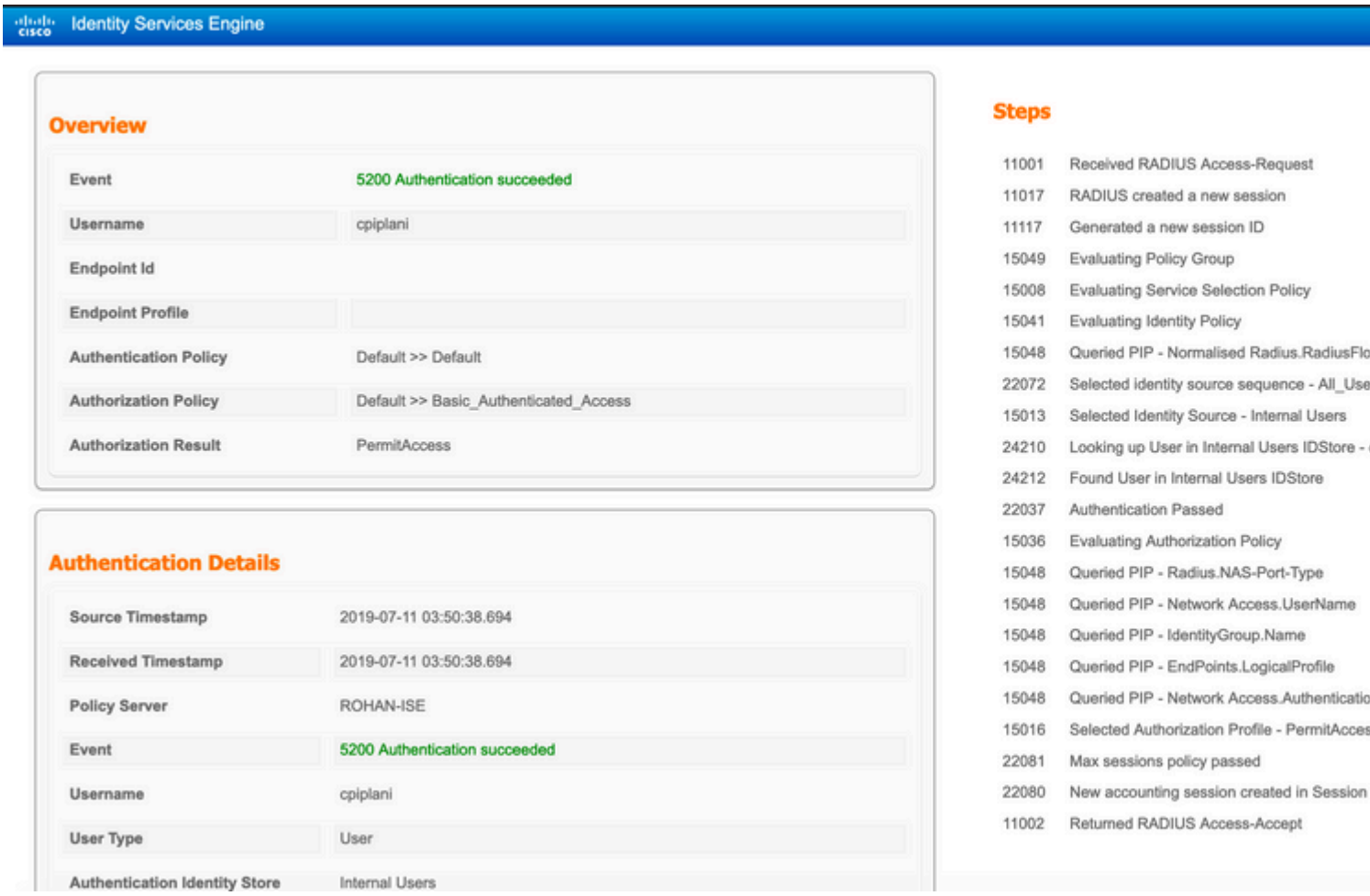
Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Log in bij het VCC met uw gebruikersreferenties die zijn toegevoegd op de ISE-pagina met gebruikersidentiteiten. U moet een Duo PUSH melding krijgen over uw eindpunt voor Two Factor Authenticatie (2FA), goedkeuren, en FMC zou inloggen zoals in het beeld:



Ga op de ISE-server naar **Operations > RADIUS > Live logs**. Zoek de gebruikersnaam die gebruikt wordt voor de verificatie op het VCC en selecteer het detailverificatierapport onder de kolom Details. In dit geval moet u controleren of de verificatie is geslaagd, zoals in de afbeelding:



Problemen oplossen

Deze sectie bevat informatie voor het troubleshooten van de configuratie.

- Controleer de debugs op Duo Authenticatie Proxy Server. De logbestanden bevinden zich onder deze locatie:

C:\Program Files (x86)\Duo Security verificatie proxy\log

Open het bestand **authproxy.log** in een tekseditor zoals Notepad++ of WordPad.

Log snippets als er onjuiste referenties worden ingevoerd en verificatie wordt geweigerd door de ISE-server.

<#root>

2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request from

10.197.223.76

to radius_server_auto

10.197.223.76 is the IP of the FMC

2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Received new request id 4 from ('10.197.223.76', 34524
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34524), 4):

login attempt for username u'cpiplani'

2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.2
2019-08-04T18:54:17+0530 [RadiusClient (UDP)]

Got response

for id 199 from ('

10.197.223.23

', 1812);

code 3 10.197.223.23 is the IP of the ISE Server.

2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Primary credentials rejecte
2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4):

Returning response code 3: AccessReject

2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Sending response

- Ga op ISE naar **Operations > RADIUS > Live logs** om de verificatiegegevens te verifiëren.

Log fragmenten van succesvolle verificatie met ISE en Duo:

<#root>

2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request from

10.197.223.76

to radius_server_auto

```
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Received new request id 5 from ('10.197.223.76', 34095
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34095), 5): login attempt for usern
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.2
2019-08-04T18:56:16+0530 [RadiusClient (UDP)] Got response for id 137 from ('

10.197.223.23

', 1812);

code 2                          <<<< At this point we have got successful authentication from ISE Server.

2019-08-04T18:56:16+0530 [RadiusClient (UDP)] http POST to https://api-f754c261.duosecurity.com:443/rest
2019-08-04T18:56:16+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPCl
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5): G
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] Invalid ip. Ip was None
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] http POST to https://api-f754c26
2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPCl
2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPCl
2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):

 Duo authentication returned 'allow': 'Success. Logging you in...

'
2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):

Returning response code 2: AccessAccept             <<<< At this point, user has hit the approve button

2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5): S
2019-08-04T18:56:30+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPCl
```

Gerelateerde informatie

- **RA VPN-verificatie met Duo**
- **Technische ondersteuning en documentatie â€“ Cisco Systems**

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.