

# Duo Two-Factor verificatie configureren voor FMC Management Access

## Inhoud

- [Inleiding](#)
- [Voorwaarden](#)
- [Vereisten](#)
- [Gebruikte componenten](#)
- [Achtergrondinformatie](#)
- [Verificatiestroom](#)
- [Verificatiestroom toegelicht](#)
- [Configureren](#)
- [Configuratiestappen op FMC](#)
- [Configuratiestappen op ISE](#)
- [Configuratiestappen voor Duo Management Portal](#)
- [Verifiëren](#)
- [Problemen oplossen](#)
- [Gerelateerde informatie](#)

## 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

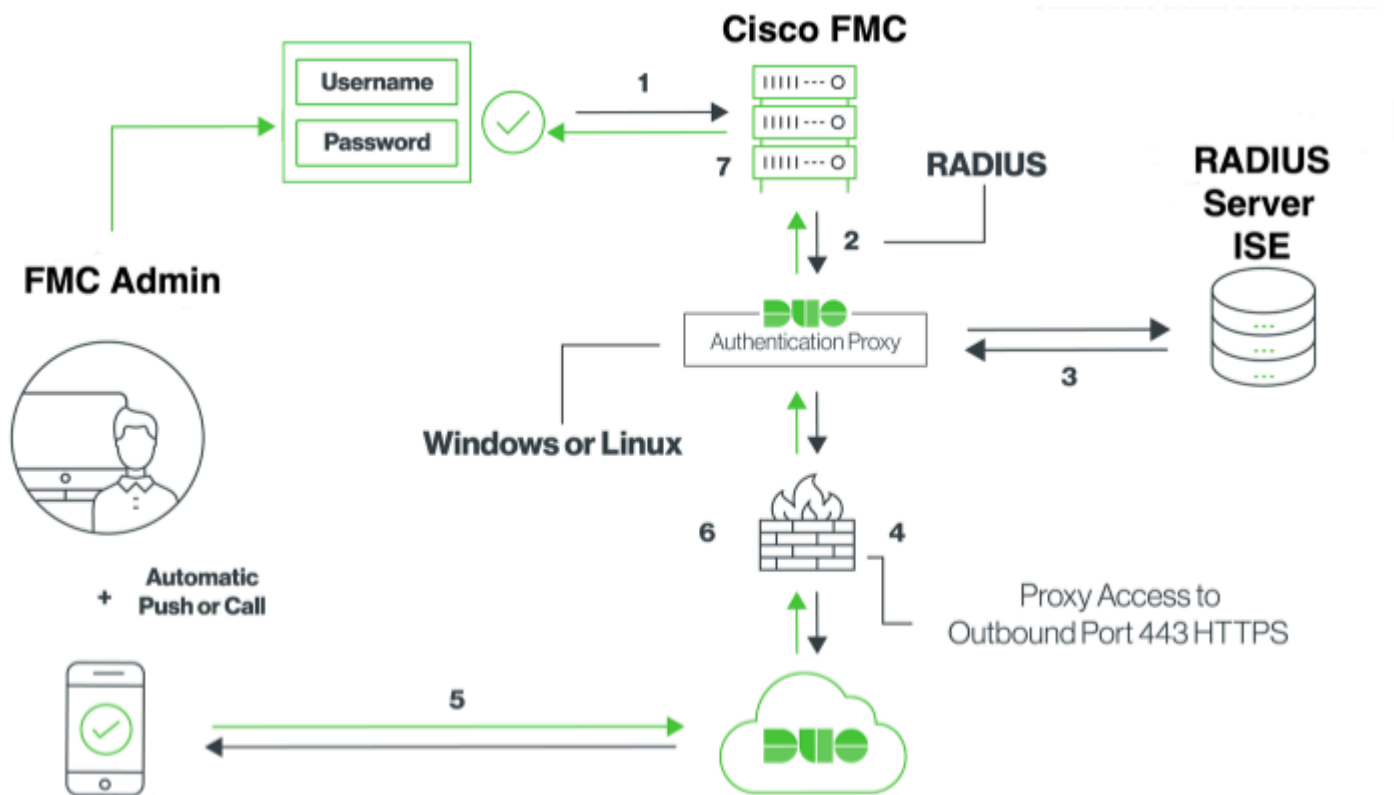
- Cisco Firepower Management Center (FMC) versie 6.3.0
- Cisco Identity Services Engine (ISE) actieve versie 2.6.0.156
- Ondersteunde versie van Windows (<https://duo.com/docs/authproxy-reference#new-proxy-install>) met een verbinding met FMC, ISE en het internet om te fungeren als de Duo Verificatie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

---

**External Authentication Object**

Authentication Method

Name \*

Description

**Primary Server**

Host Name/IP Address \*  ex. IP or hostname

Port \*

RADIUS Secret Key

**Backup Server (Optional)**

Host Name/IP Address  ex. IP or hostname

Port

RADIUS Secret Key

**RADIUS-Specific Parameters**

Timeout (Seconds)

Retries

Access Admin

Administrator

Security Analyst

Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Default User Role  To specify the default user role if user is not found in any group

**Shell Access Filter**

Administrator Shell Access User List  ex. user1, user2, user3

(Mandatory for FTD devices)

**Define Custom RADIUS Attributes**

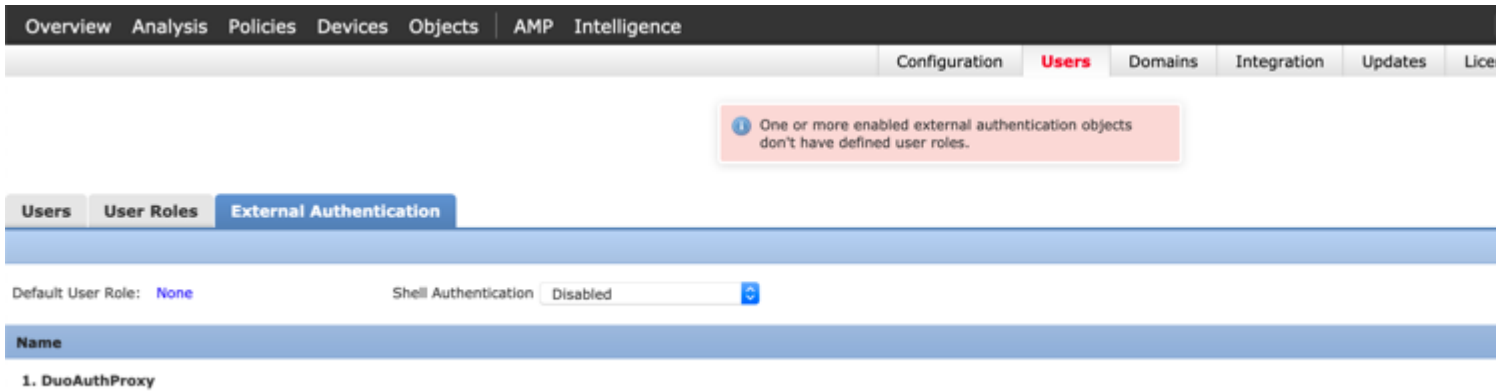
**Additional Test Parameters**

User Name

Password

\*Required Field

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=xxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxx.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:

# RADIUS

See the [RADIUS documentation](#) to integrate Duo into your RADIUS-enabled platform.

## Details

Integration key	<input type="text" value="REDACTED"/>	<a href="#">select</a>
Secret key	<a href="#">Click to view.</a>	<a href="#">select</a>
Don't write down your secret key or share it with anyone.		
API hostname	<input type="text" value="REDACTED"/>	<a href="#">select</a>

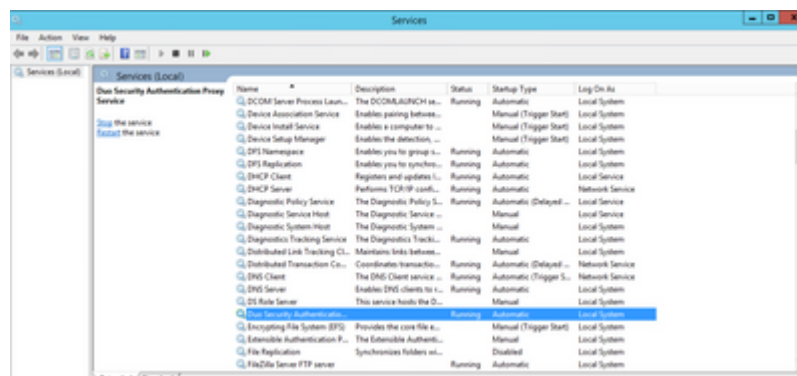
Integratiesleutel = ikey

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.

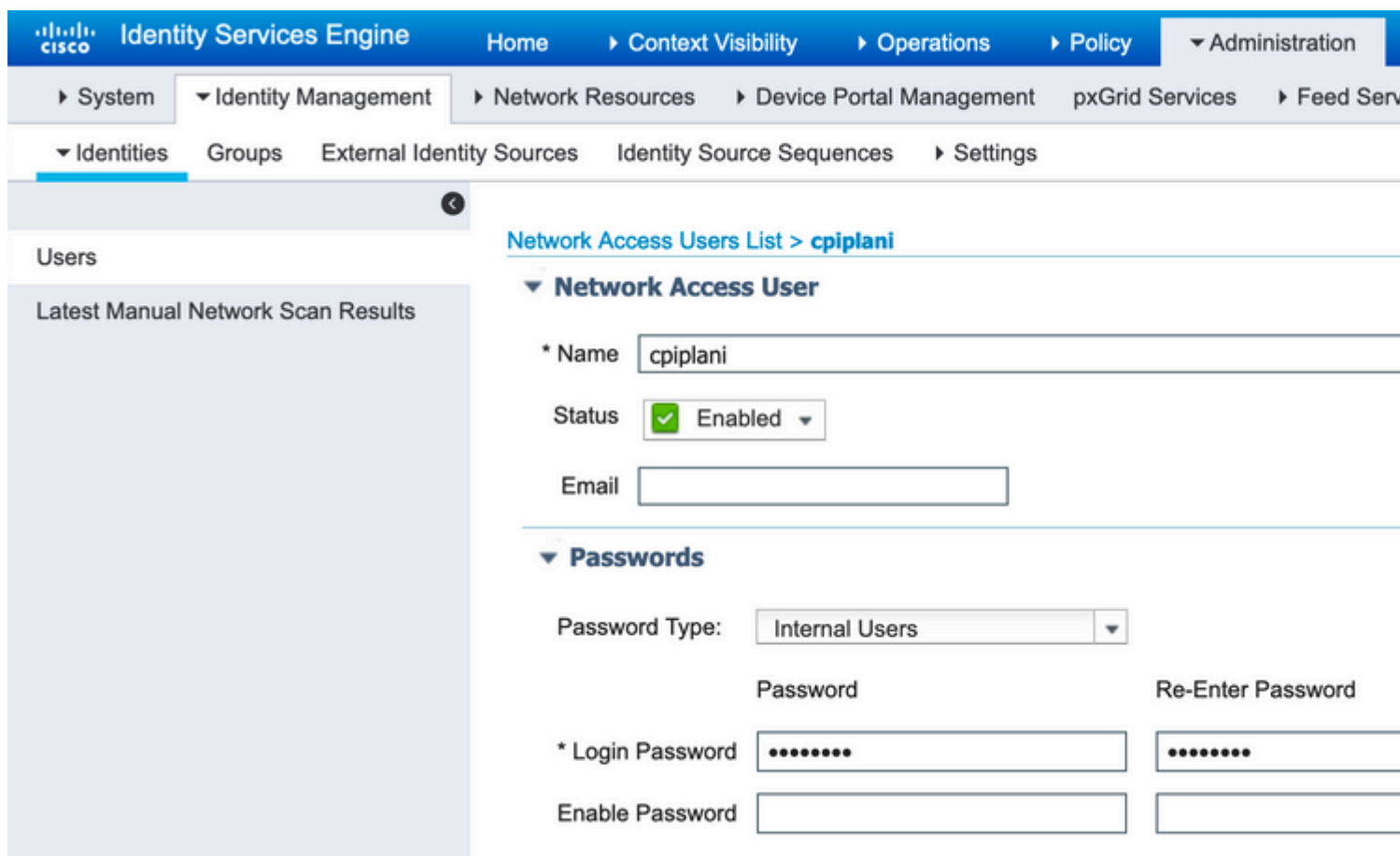
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Network Resources > Network Devices. The left sidebar shows 'Network Devices' selected. The main content area is titled 'Network Devices List > DuoAuthproxy' and 'Network Devices'. The configuration fields are: Name: DuoAuthproxy; Description: (empty); IP Address: (dropdown menu); \* IP: 10.106.44.177; \* Device Profile: Cisco; Model Name: (dropdown menu); Software Version: (dropdown menu).

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

The screenshot shows the RADIUS Authentication Settings configuration page in Cisco ISE. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Network Resources > Network Devices. The left sidebar shows 'Network Devices' selected. The main content area is titled 'RADIUS Authentication Settings' and 'RADIUS UDP Settings'. The configuration fields are: Protocol: RADIUS; \* Shared Secret: (masked with dots); Use Second Shared Secret: (checkbox, unchecked); CoA Port: 1700.

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

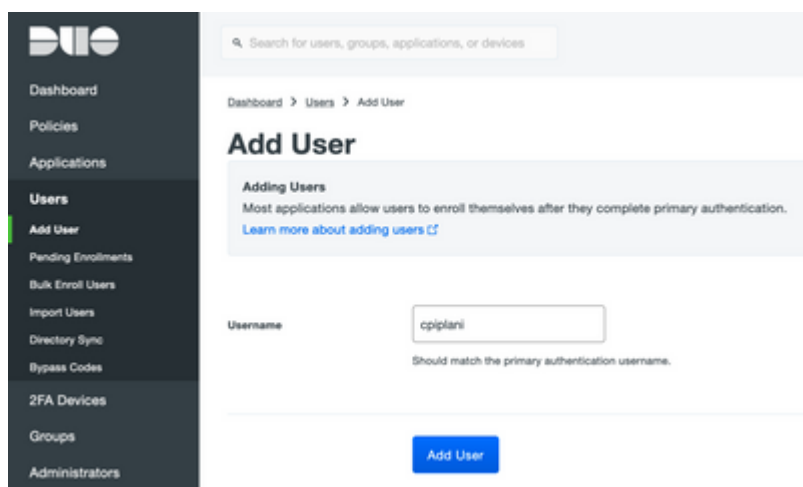
afbeelding:



## 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.

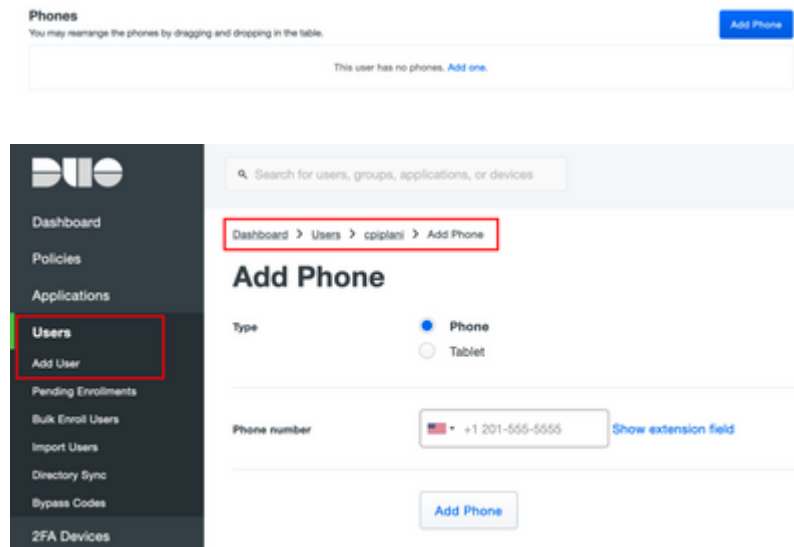


[Handmatige installatie van Duo-toepassing voor IOS-apparaten](#)

[Handmatige installatie van Duo-toepassing voor Android-apparaten](#)

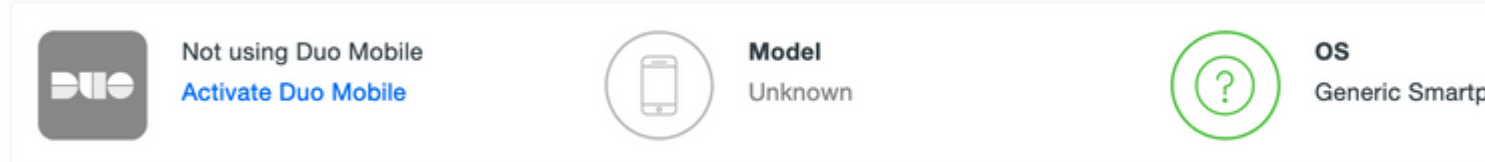
**Stap 2.** Automatische generatie van code.

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

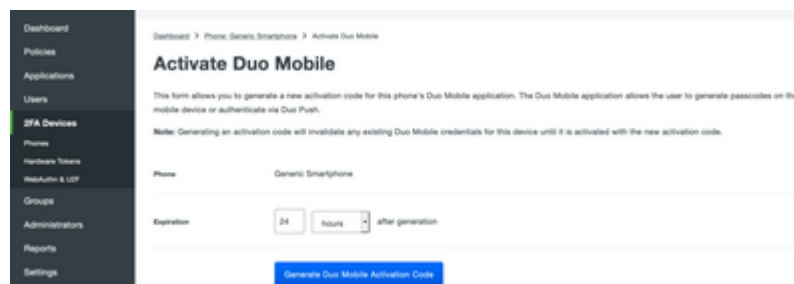


Kies **Duo Mobile activeren** zoals in de afbeelding:

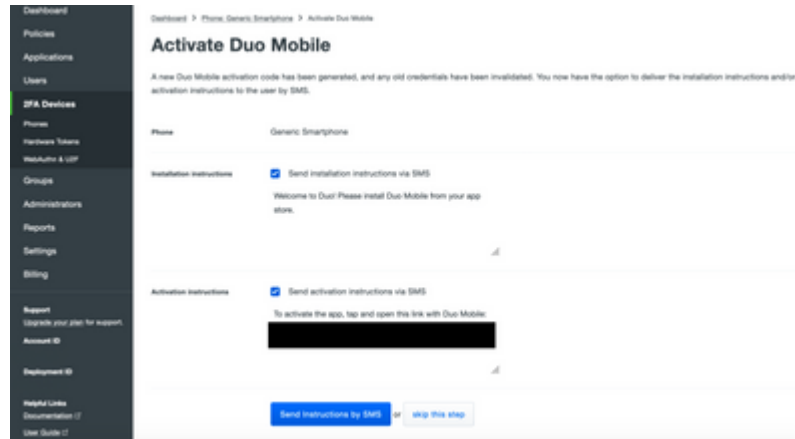
## Device Info



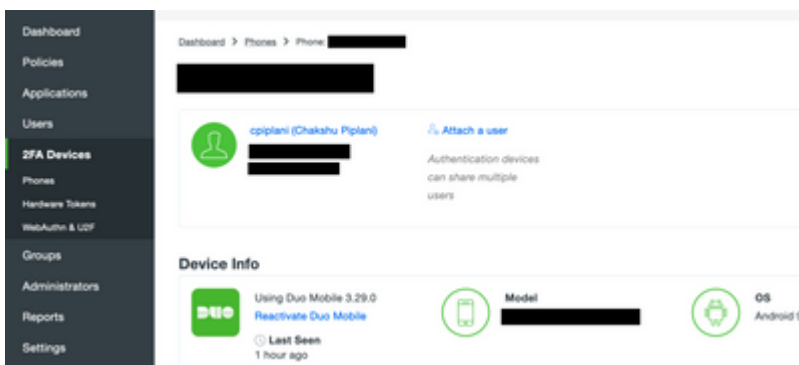
Kies **Duo Mobile Activeringscode genereren** zoals in de afbeelding:



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



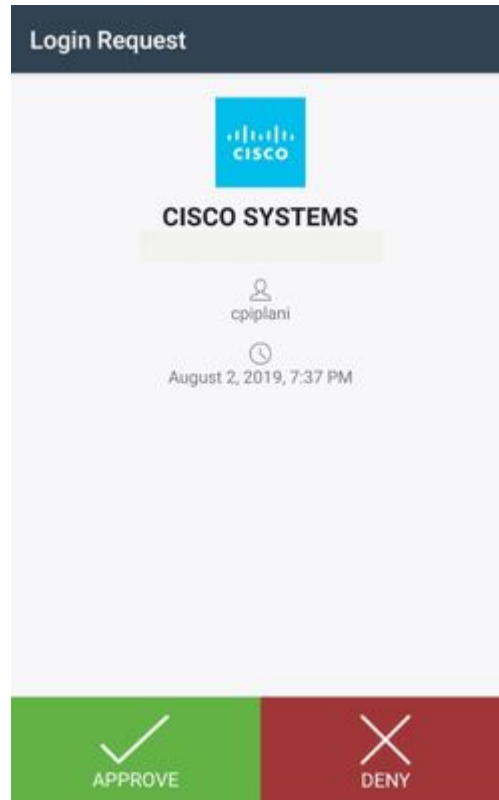
**Klik op** de koppeling in de SMS en Duo app wordt gekoppeld aan de gebruikersaccount in het gedeelte Apparaatinfo, zoals in de afbeelding:



## 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:

Identity Services Engine

### Overview

Event	5200 Authentication succeeded
Username	cpiplani
Endpoint Id	
Endpoint Profile	
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

### Authentication Details

Source Timestamp	2019-07-11 03:50:38.694
Received Timestamp	2019-07-11 03:50:38.694
Policy Server	ROHAN-ISE
Event	5200 Authentication succeeded
Username	cpiplani
User Type	User
Authentication Identity Store	Internal Users

### Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 11117 Generated a new session ID
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15041 Evaluating Identity Policy
- 15048 Queried PIP - Normalised Radius.RadiusFlo
- 22072 Selected identity source sequence - All\_Use
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore -
- 24212 Found User in Internal Users IDStore
- 22037 Authentication Passed
- 15036 Evaluating Authorization Policy
- 15048 Queried PIP - Radius.NAS-Port-Type
- 15048 Queried PIP - Network Access.UserName
- 15048 Queried PIP - IdentityGroup.Name
- 15048 Queried PIP - EndPoints.LogicalProfile
- 15048 Queried PIP - Network Access.Authentication
- 15016 Selected Authorization Profile - PermitAcces
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session
- 11002 Returned RADIUS Access-Accept

# 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 teksteditor 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 ('10.197.223.76', 34524)  
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 rejected  
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 user
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 <_DuoHTTPC
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5): C
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 <_DuoHTTPC
2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPC
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 <_DuoHTTPC
```

## 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.