

Duo-integratie configureren met Active Directory en ISE voor tweevoudige verificatie op AnyConnect/Remote Access VPN-clients

Inhoud

- [Inleiding](#)
- [Voorwaarden](#)
- [Vereisten](#)
- [Gebruikte componenten](#)
- [Achtergrondinformatie](#)
- [Netwerkdigram en -scenario](#)
- [Communicatieproces](#)
- [Active Directory-configuraties](#)
- [Twee configuraties](#)
- [Configuratie van twee autorisatieproxy](#)
- [Cisco ISE-configuraties](#)
- [Cisco ASA RADIUS/ISE-configuratie](#)
- [Cisco ASA VPN-configuratie voor externe toegang](#)
- [Testen](#)
- [Problemen oplossen](#)
- [Fouten in het werk](#)

Inleiding

In dit document wordt de duo push-integratie met AD en ISE beschreven als twee-factor verificatie voor AnyConnect-clients die met ASA zijn verbonden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- RA VPN-configuratie op ASA
- RADIUS-configuratie op ASA
- ISE
- Active Directory
- Duo-toepassingen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft 2016-server
- ASA 9.14(3)18
- ISE-server 3.0
- Duo Server

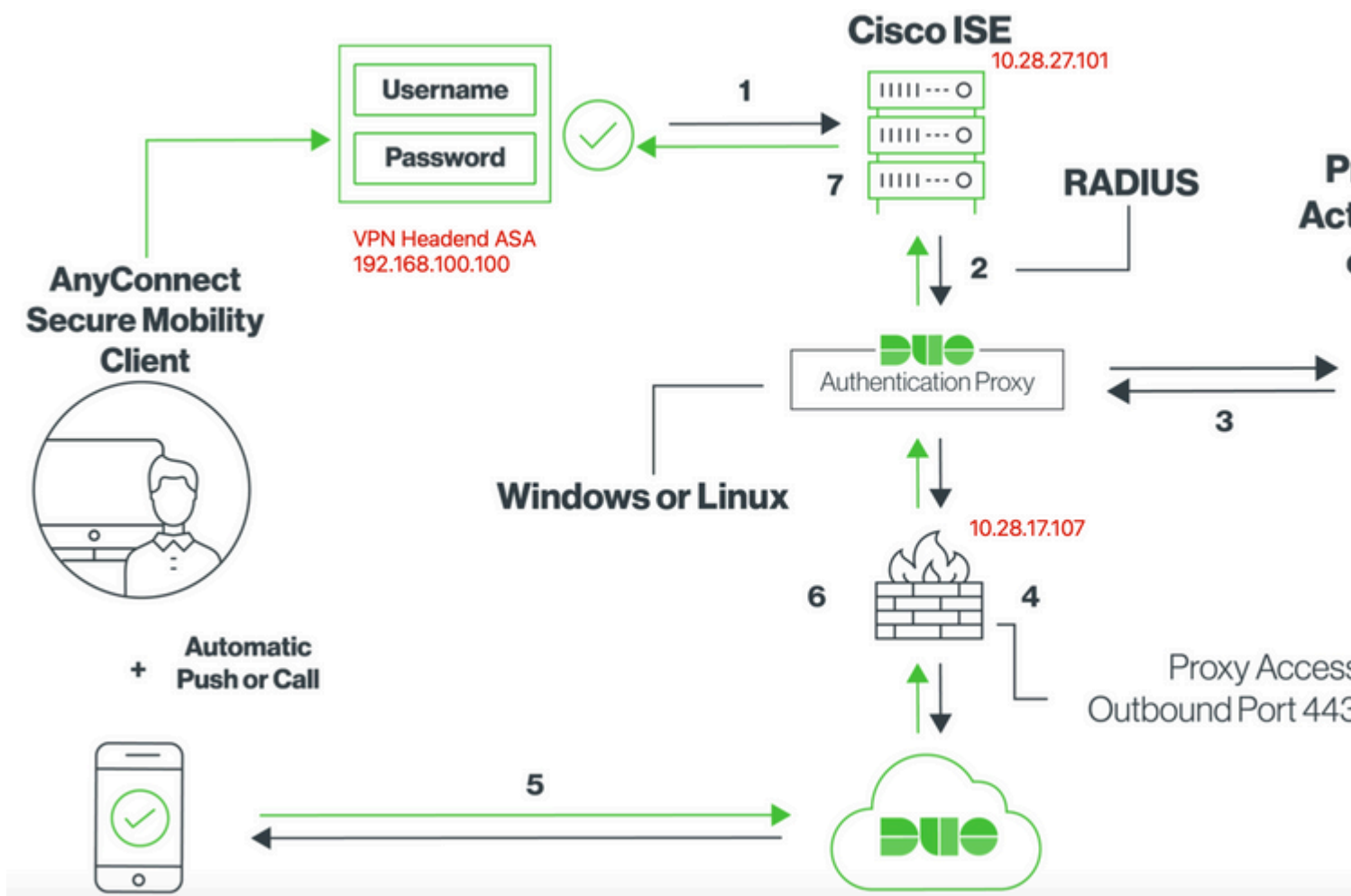
- Duo Verificatie Proxy Manager

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

Dit document beschrijft hoe u Duo push-integratie met Active Directory (AD) en Cisco Identity Service Engine (ISE) kunt configureren als tweevoudige verificatie voor AnyConnect-clients die verbinding maken met Cisco adaptieve security applicatie (ASA).

Netwerkdigram en -scenario



Communicatieproces

<https://duo.com/docs/ciscoise-radius>

1. Primaire verificatie gestart naar Cisco ISE-id
2. Cisco ISE stuurt een verificatieaanvraag naar de Duo-verificatieproxy
3. Primaire verificatie maakt gebruik van Active Directory of RADIUS
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 authenticatiereactie
7. Cisco ISE-toegang verleend

Gebruikersaccounts:

- Active Directory Admin: Dit wordt gebruikt als de directory account om de Duo Auth Proxy te laten binden aan de Active Directory-server voor primaire verificatie.
- Testgebruiker van Active Directory
- Duo testgebruiker voor secundaire verificatie

Active Directory-configuraties

Windows-server is vooraf geconfigureerd met Active Directory Domain-services.

Opmerking: Als RADIUS Duo Autor Proxy Manager op dezelfde Active Directory-hostmachine wordt uitgevoerd, moeten de NPS-rollen (Network Policy Server) worden verwijderd/verwijderd. Als beide RADIUS-services worden uitgevoerd, kunnen ze conflicten veroorzaken en gevolgen hebben voor de prestaties.

Om een AD-configuratie voor verificatie en gebruikersidentiteit op gebruikers van Remote Access VPN te realiseren, zijn een paar waarden vereist.

Al deze gegevens moeten worden gecreëerd of verzameld op de Microsoft Server voordat de configuratie kan worden uitgevoerd op de ASA- en Duo Auth-proxyserver.

De belangrijkste waarden zijn:

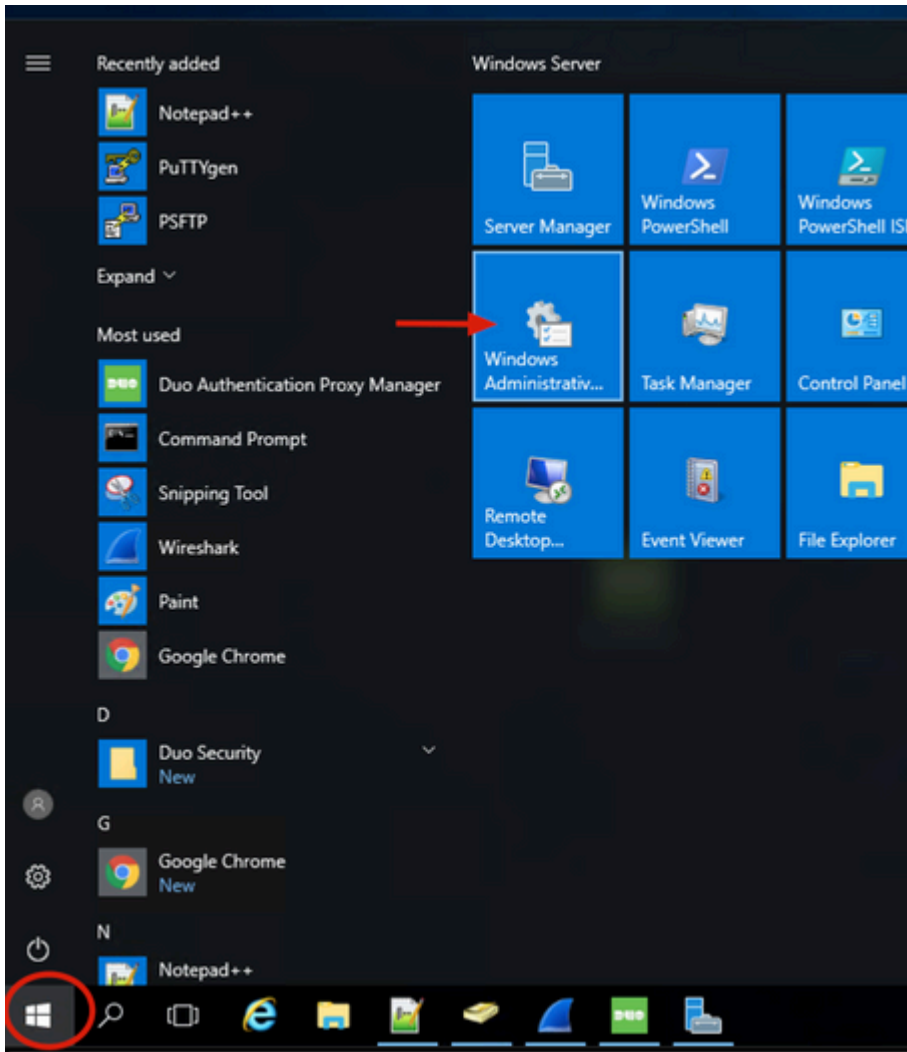
- Domeinnaam. Dit is de domeinnaam van de server. In deze configuratiehandleiding is `agarciam.cisco` de domeinnaam.
- IP/FQDN-adres van server. Het IP-adres of FQDN wordt gebruikt om de Microsoft-server te bereiken. Als een FQDN wordt gebruikt, moet een DNS-server worden geconfigureerd binnen ASA en Duo Auth proxy om de FQDN op te lossen.

In deze configuratiehandleiding is deze waarde `agarciam.cisco` (die zich oplost in `10.28.17.107`).

- Serverpoort. De poort die wordt gebruikt door de LDAP-service. Standaard gebruiken LDAP en STARTTLS TCP-poort 389 voor LDAP en gebruikt LDAP over SSL (LDAPS) TCP-poort 636.
- root-CA. Als LDAPS of STARTTLS wordt gebruikt, is de wortel CA die wordt gebruikt om het SSL certificaat te ondertekenen dat door LDAPS wordt gebruikt vereist.
- Gebruikersnaam en wachtwoord voor map Dit is het account dat door Duo Auth proxy server wordt gebruikt om te binden aan de LDAP-server en gebruikers te verifiëren en te zoeken naar gebruikers en groepen.
- Basisnaam en Groepsnaam (DN). De Base DN is het vertrekpunt voor Duo Auth proxy en vertelt de Active directory om te beginnen met zoeken naar gebruikers en hen te verifiëren.

In deze configuratiegids, wordt het worteldomein `agarciam.cisco` gebruikt aangezien de Basis DN en Groep DN Duo-GEBRUIKERS zijn.

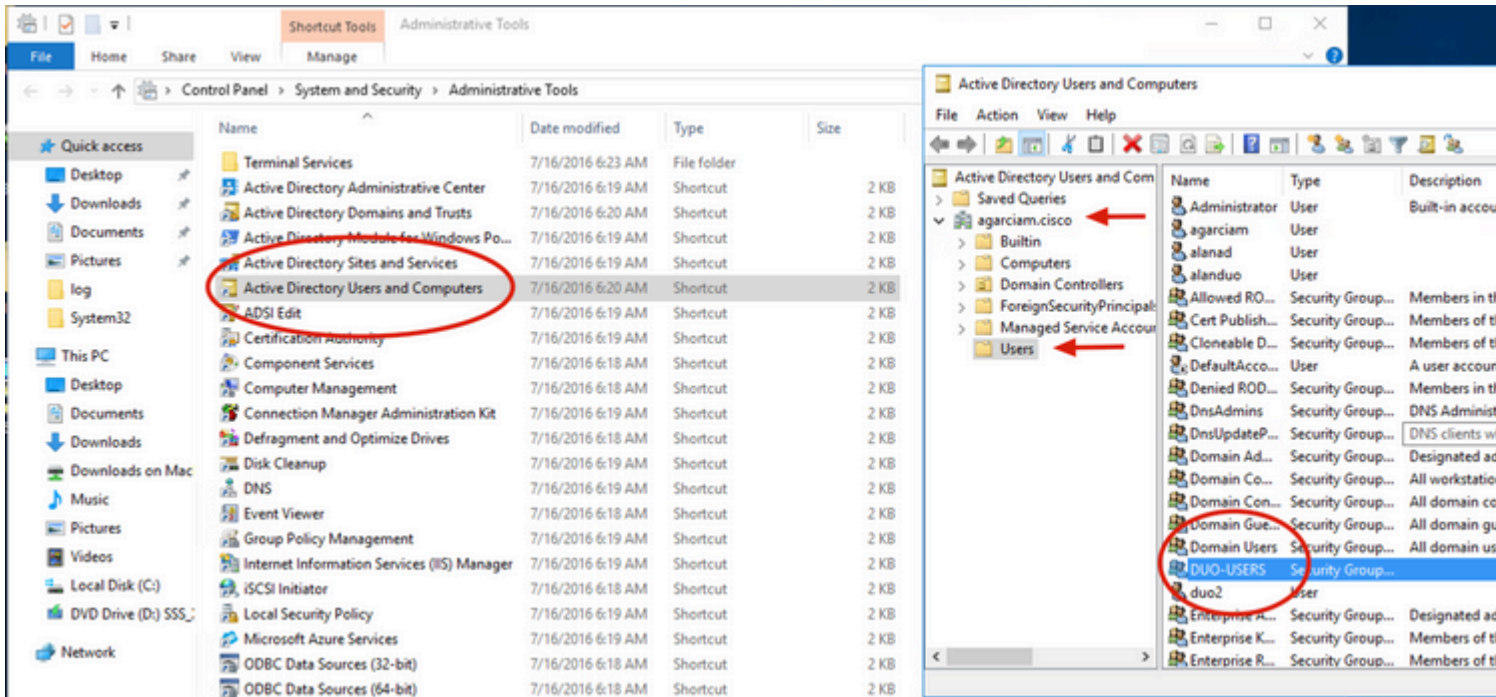
1. Om een nieuwe Duo gebruiker, op Windows Server toe te voegen, navigeer naar **Windows** pictogram linksonder en klik op **Windows-beheerprogramma's**, zoals in de afbeelding.



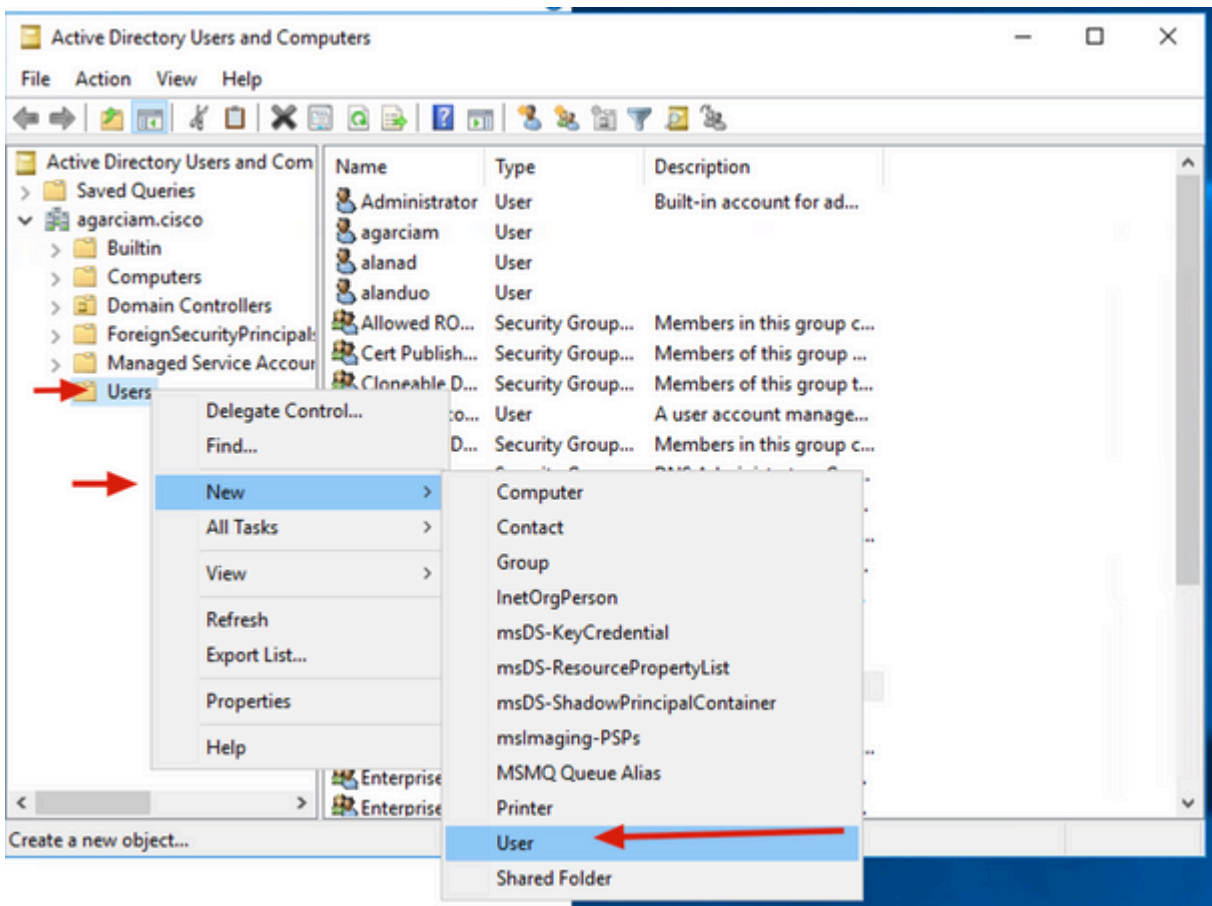
2. Ga in het venster Windows-beheertools naar **Active Directory-gebruikers en -computers**.

Vouw in het paneel Active Directory-gebruikers en -computers de domeinoptie uit en navigeer naar de map **Gebruikers**.

In dit configuratievoorbeeld wordt Duo-USER gebruikt als doelgroep voor secundaire authenticatie.



3. Klik met de rechtermuisknop op de map **Gebruikers** en selecteer **Nieuw > Gebruiker**, zoals in de afbeelding.



4. Specificeer in het venster Nieuwe gebruiker-object de identiteitskenmerken van deze nieuwe gebruiker en klik op **Volgende**, zoals in de afbeelding.

New Object - User

Create in: agarciam.cisco/Users

First name: duovpn Initials:

Last name:

Full name: duovpn

User logon name: duovpn @agarciam.cisco

User logon name (pre-Windows 2000): AGARCIAM\ duovpn

< Back Next > Cancel

5. Bevestig het wachtwoord en klik op **Volgende. Voltoeien** zodra de gebruikersinformatie is geverifieerd.

New Object - User

Create in: agarciam.cisco/Users

Password:

Confirm password:

User must change password at next logon

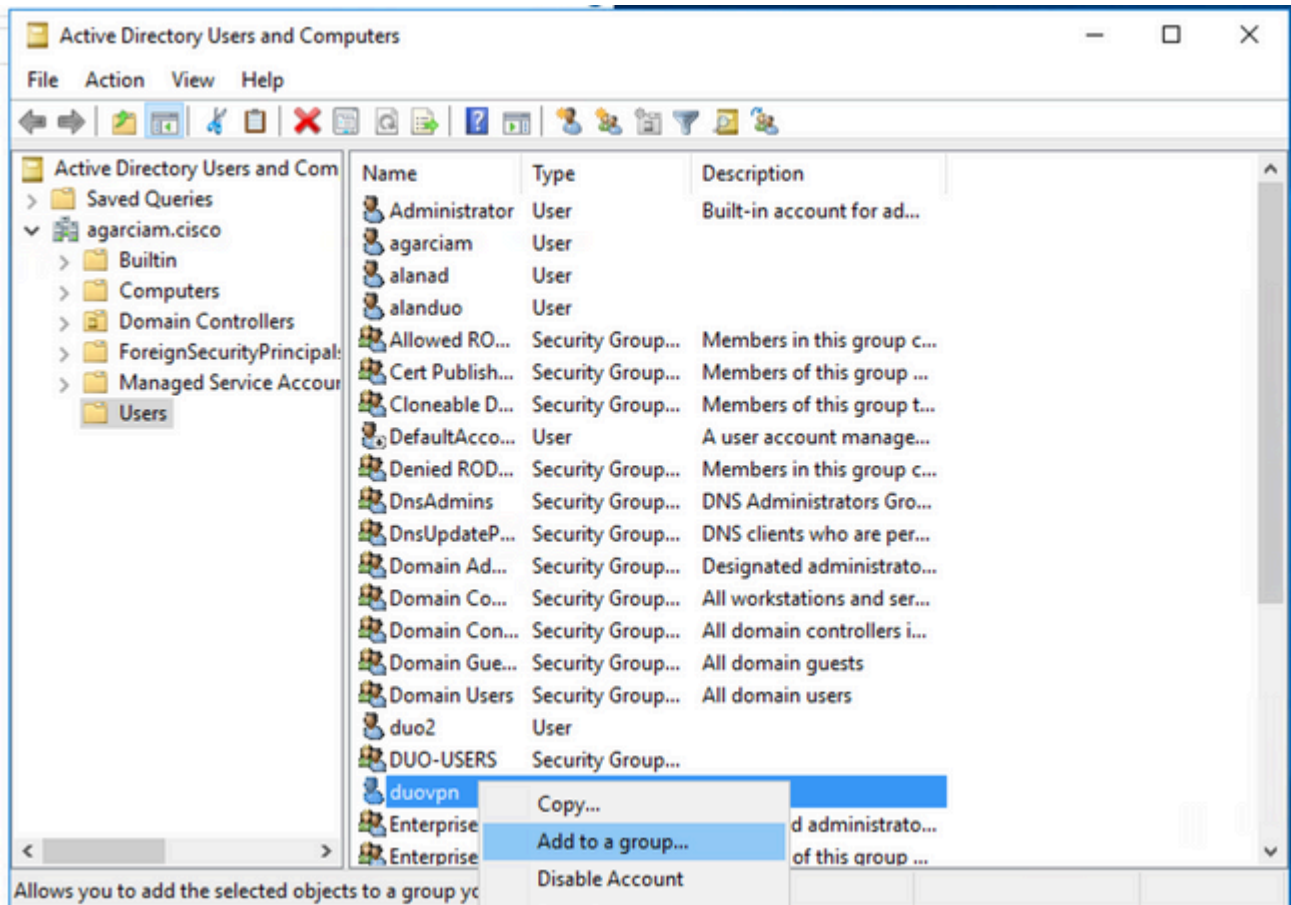
User cannot change password

Password never expires

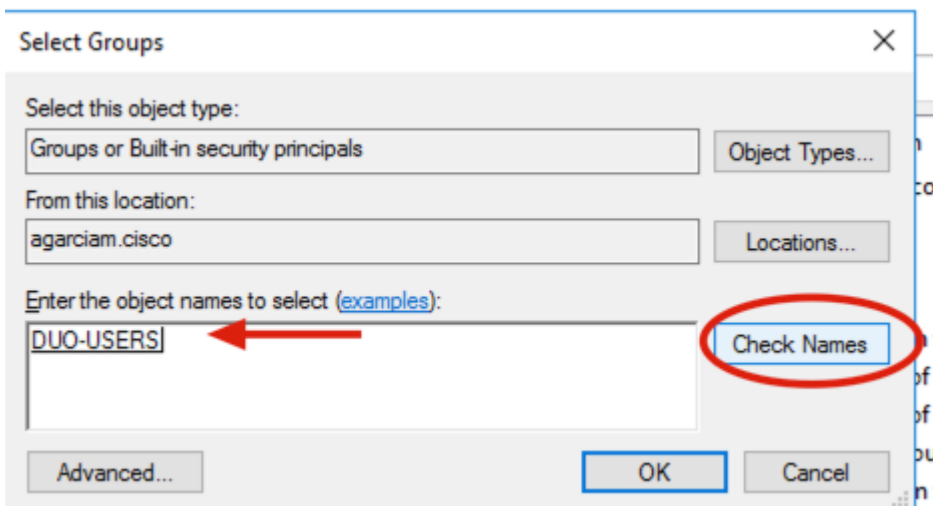
Account is disabled

< Back Next > Cancel

6. Wijs de nieuwe gebruiker toe aan een specifieke groep, klik met de rechtermuisknop op de groep en selecteer **Toevoegen aan een groep**, zoals in de afbeelding.



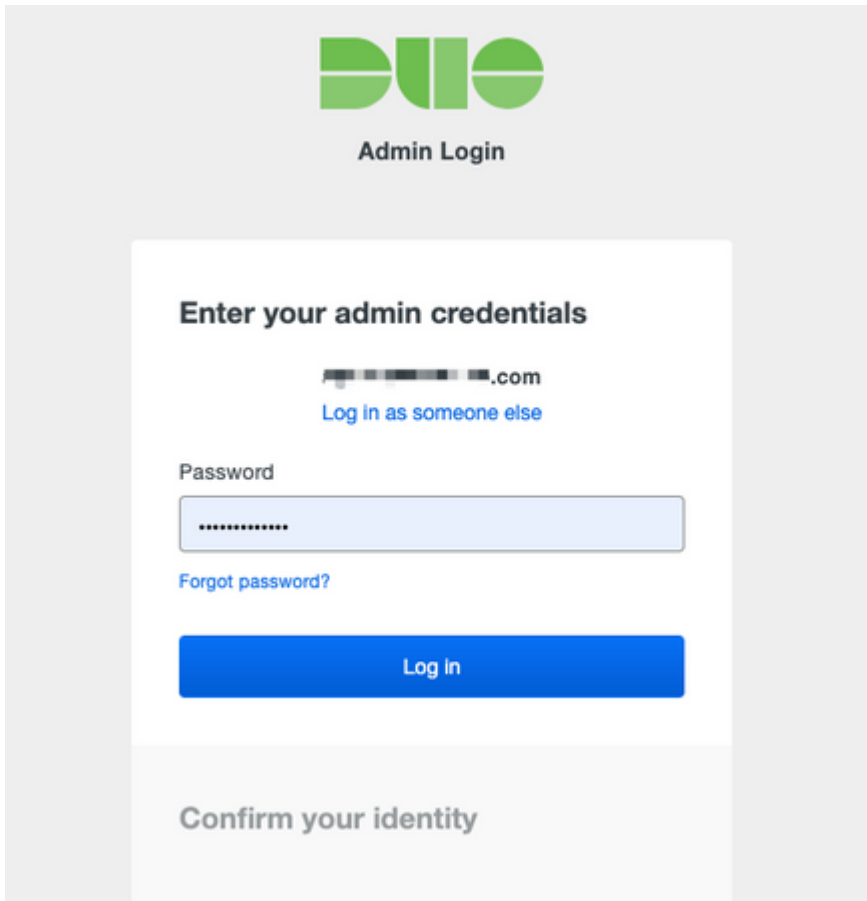
7. Typ in het paneel Groepen selecteren de naam van de gewenste groep en klik op **Namen controleren**.
 Selecteer vervolgens de naam die overeenkomt met uw criteria en klik op **OK**.



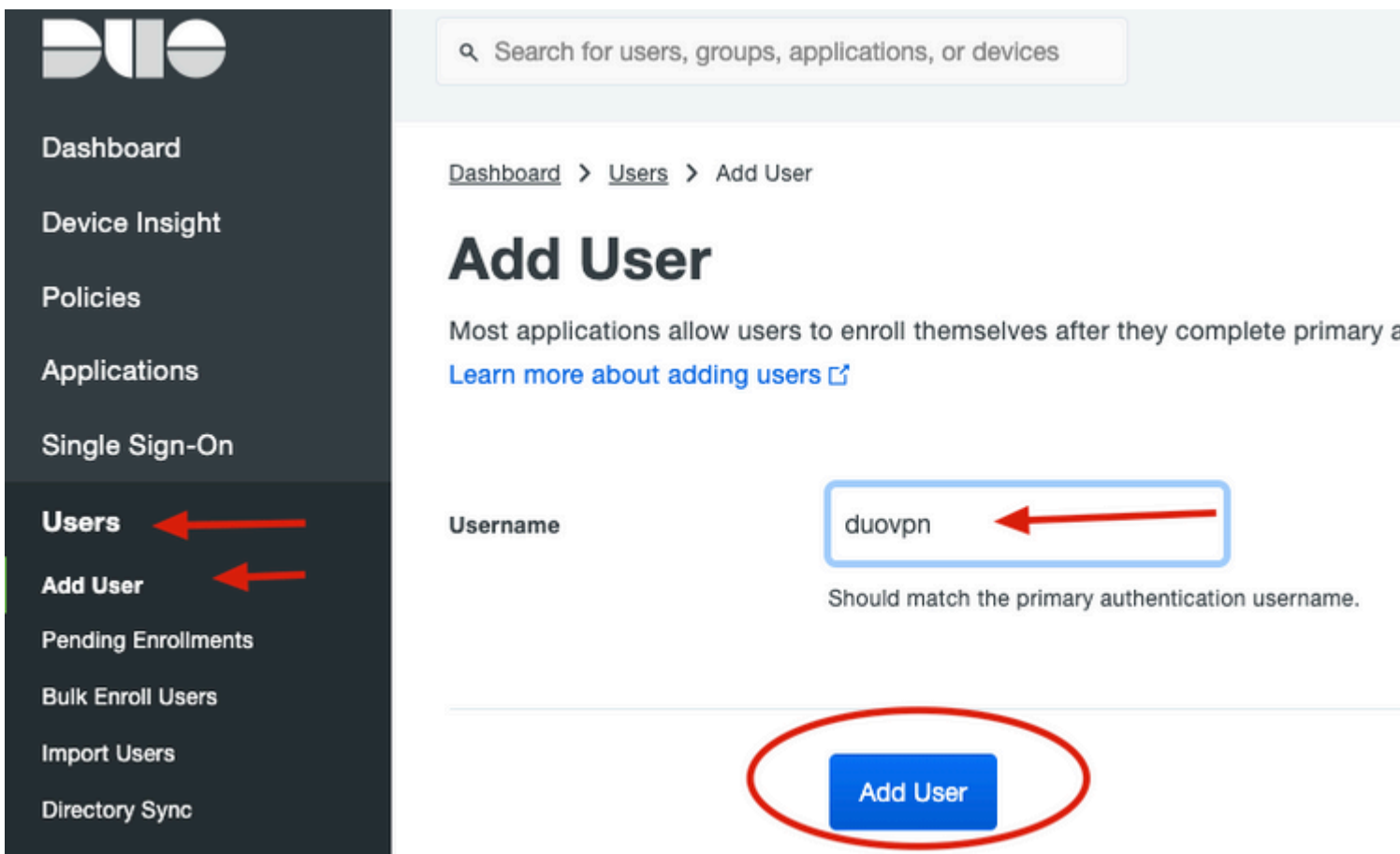
8. Dit is de gebruiker die in dit document als voorbeeld wordt gebruikt.

Twee configuraties

1. Log in op uw Dudo Admin portal.



2. In het linker zijpaneel, navigeer naar **Gebruikers**, klik op **Add User** en typ de naam van de gebruiker die overeenkomt met onze Active Domain-gebruikersnaam, en klik vervolgens op **Add User**.



3. Vul in het nieuwe gebruikerspaneel de spatie in met alle benodigde informatie.

Policies

Applications

Single Sign-On

Users

Add User

Pending Enrollments

Bulk Enroll Users

Import Users

Directory Sync

Bypass Codes

Groups

Endpoints

2FA Devices

Trusted Endpoints

Trust Monitor

Reports

Settings

Need Help?

[Chat with Tech Support](#)

[Email Support](#)

Call us at 1-855-386-2884

Versioning

Core Authentication Service:

D235.6

Admin Panel:

D235.6

[Read Release Notes](#)

Account ID

2910-6030-53

Deployment ID

[DUO63](#)

Helpful Links

[Documentation](#)

[User Guide](#)

[Dashboard](#) > [Users](#) > duovpn

duovpn



This user has not enrolled yet. See our [enrollment documentation](#) to learn

Username

duovpn



Username aliases

[+ Add a username alias](#)

Users can have up to 8 aliases.

Optionally, you may choose to reserve using an alias number for (e.g., Username alias 1 should only be used for Employee ID).

Full name

test ypn user



Email

[redacted]@[redacted].com

Status

Active



Require multi-factor authentication (default).

Bypass

Allow users to skip two-factor authentication and log in w

Disabled

Automatically deny access

This controls the user's two-factor authentication process.

Groups

You don't have any editable groups. [Add one.](#)

Groups can be used for management, reporting, and policy. [Le](#)

Notes

:In dit document wordt de methode Duo push for mobile devices gebruikt, dus moet er een telefoonapparaat worden toegevoegd.

Klik op **Telefoon toevoegen**.

Phones
You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#) ↗.

This user has no phones. [Add one.](#)

Endpoints

This user has no devices.

Hardware Tokens [Add Hardware Token](#)

This user has no hardware tokens. [Add one.](#)

Bypass Codes [Add Bypass Code](#)

This user has no bypass codes. [Add one.](#)

WebAuthn & U2F [Add U2F Device](#)

5. Typ het telefoonnummer van de gebruiker en klik op **Telefoon toevoegen**.

Add Phone



[Learn more about Activating Duo Mobile](#)

Type

- Phone
 Tablet

Phone number





[Show extension field](#)

Optional. Example: "+52 1 222 123 4567"



Add Phone

6. Navigeer naar **Gebruikers** op het linkerpaneel Duo Admin en klik op de nieuwe gebruiker.


- Dashboard
- Device Insight
- Policies
- Applications
- Single Sign-On
- Users** 
- Add User
- Pending Enrollments
- Bulk Enroll Users
- Import Users
- Directory Sync
- Bypass Codes
- Groups
- Endpoints
- 2FA Devices
- Trusted Endpoints
- Trust Monitor
- Reports
- Settings
- Need Help?
Chat with Tech Support 

Dashboard > Users

Users

Directory Sync | Im

i You have users who have not activated Duo Mobile. [Click here to send them activation links.](#)

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#) .

5

Total Users

0

Not Enrolled

2



Inactive Users


1








Trash

0

By

Select (0)  

[Export](#) 

	Username 	Name	Email	Phones	Tokens
<input type="checkbox"/>				1	
<input type="checkbox"/>				1	
<input type="checkbox"/>				1	
<input type="checkbox"/>	duovpn		 @i.com	1	
<input type="checkbox"/>			 @o.com	1	

Opmerking:In het geval u op dit moment geen toegang hebt tot uw telefoon, kunt u de e-mailoptie selecteren.

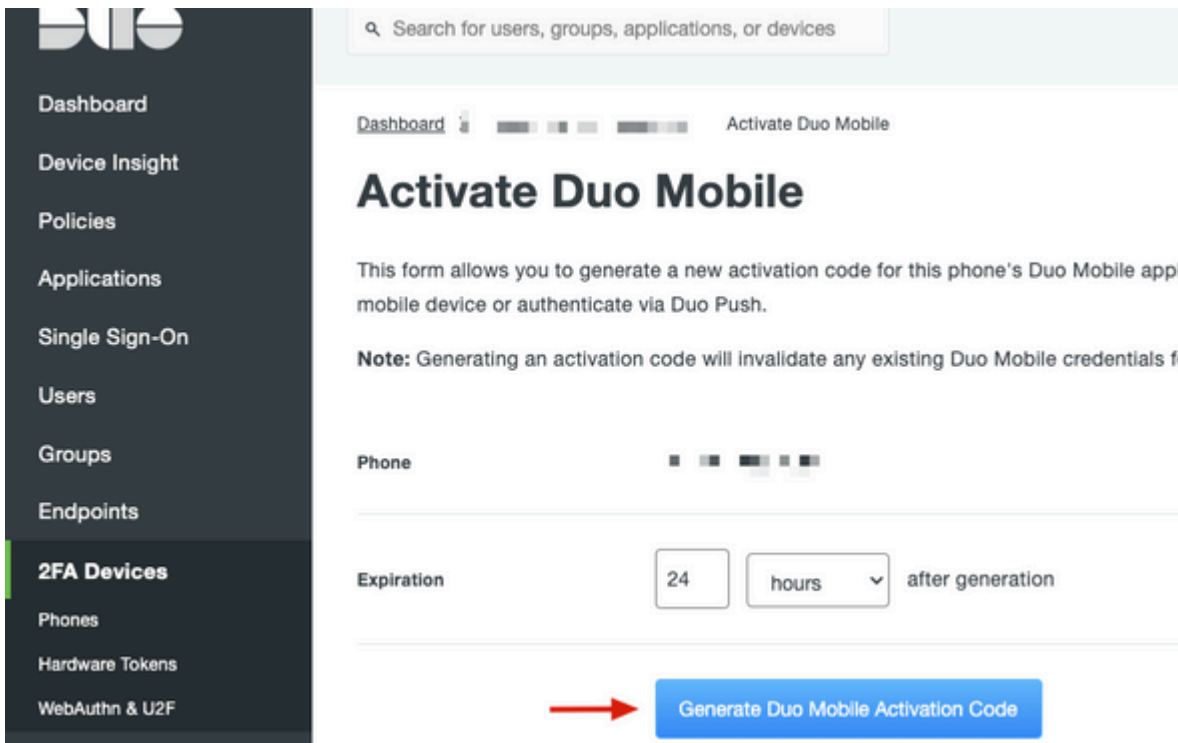
7. Navigeren naar **telefoons** sectie en klik op **Duo Mobile activeren**.

Phones

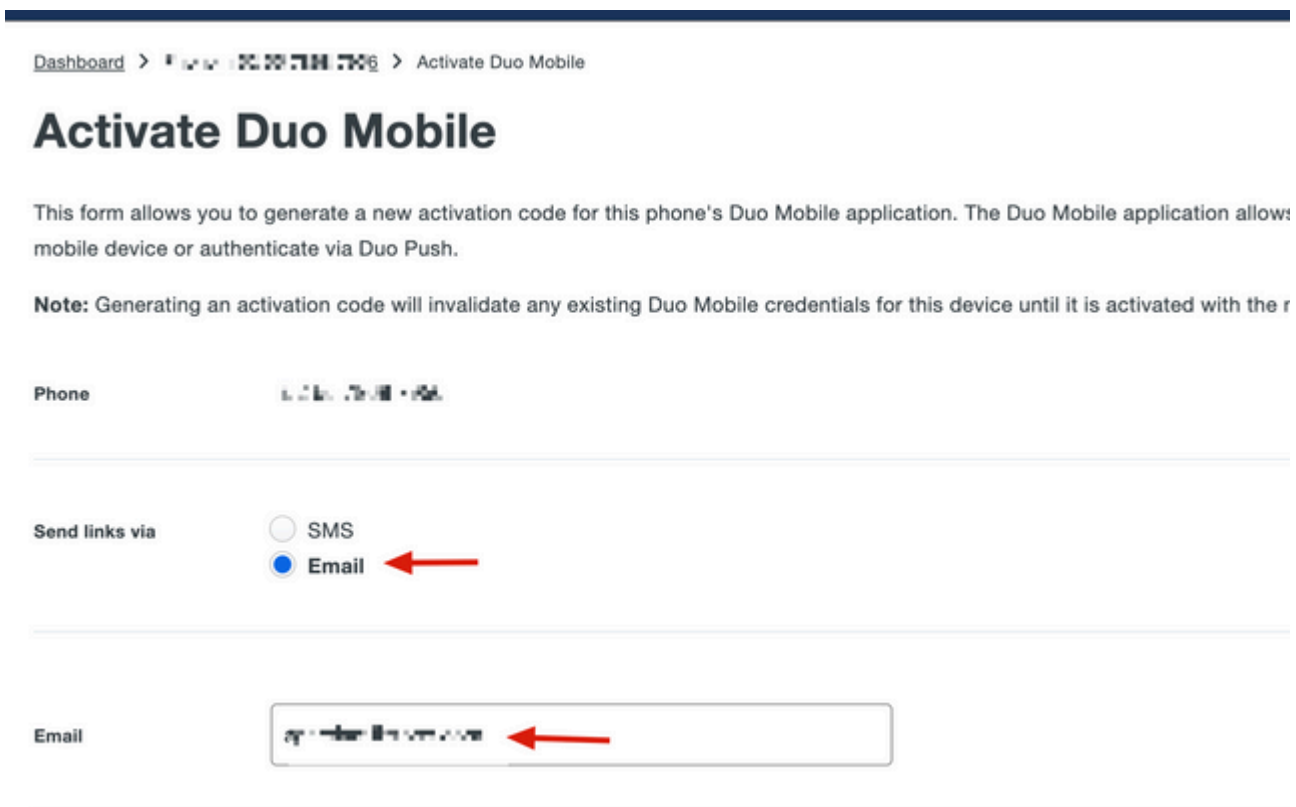
You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#) .

Alias	Device	Platform	Model	Security Warnings	
phone1		Android 10		✓ No warnings	Activate Duo Mobile 

8. Klik op **Generate Duo Mobile Activeringscode**.



9. Selecteer **E-mail** om de instructies via e-mail te ontvangen, typ uw e-mailadres en klik op **Instructies per e-mail verzenden**.



10. U ontvangt een e-mail met de instructies, zoals getoond in de afbeelding.

This is an automated email from Duo Security.

Your organization invites you to set up Duo Mobile on your phone. You will find instructions from your Duo administrator below. If you have questions, please reach out to your organization's IT or help desk team.

This email will help you add your Cisco account to Duo Mobile on this device:



Just tap this link from + [redacted] or copy and paste it into Duo Mobile manually:



If you're not reading this from + [redacted] Duo Mobile on your phone and scan this barcode:



Don't have Duo Mobile yet? Install it first:

iPhone: <https://itunes.apple.com/us/app/duo-mobile/id422663827>

Android: <https://play.google.com/store/apps/details?id=com.duosecurity.duomobile>

11. Open de Duo Mobile App vanaf uw mobiele apparaat en klik op **Add** dan selecteer **Use QR code** en scan de code uit de instructies e-mail.

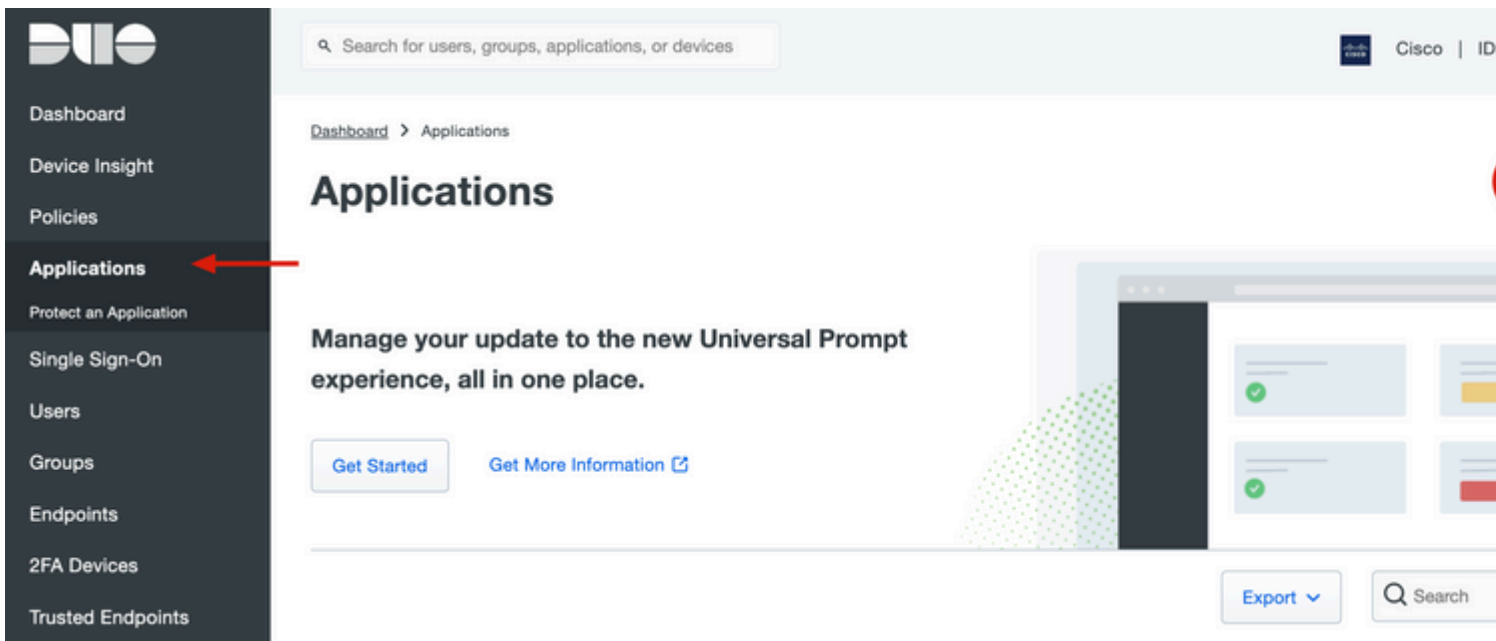
12. Nieuwe gebruiker wordt toegevoegd aan uw Duo Mobile App.

Configuratie van twee autorisatieproxy

1. Download en installeer Duo Auth Proxy Manager van <https://duo.com/docs/authproxy-reference>.

Opmerking:In dit document is Duo Auth Proxy Manager geïnstalleerd op dezelfde Windows-server waarop Active Directory-services worden gehost.

2. Navigeer in het Duo Admin-paneel naar **toepassingen** en klik op **Protect a Application**.



3. Zoek in de zoekbalk naar Cisco ISE-straal.



Protect an Application

i Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others.

Documentation: [Getting Started](#)

Choose an application below to get started.

ise

Application	Protection Type		
 Akamai Enterprise Application Access	2FA	Documentation	Protect
 Cisco ISE RADIUS	2FA	Documentation	Protect

4. Kopieer de integratiesleutel, de beveiligingssleutel en de API Hostname. U hebt deze gegevens nodig voor de configuratie van de Duo-verificatieproxy.

Duo Authentication Proxy Manager

● Authentication Proxy is **running** Up since: 3/5/2022, 9:23:04 AM ⚠ Version: 5.6.0
[Update your Authentication Proxy](#) [Rest](#)

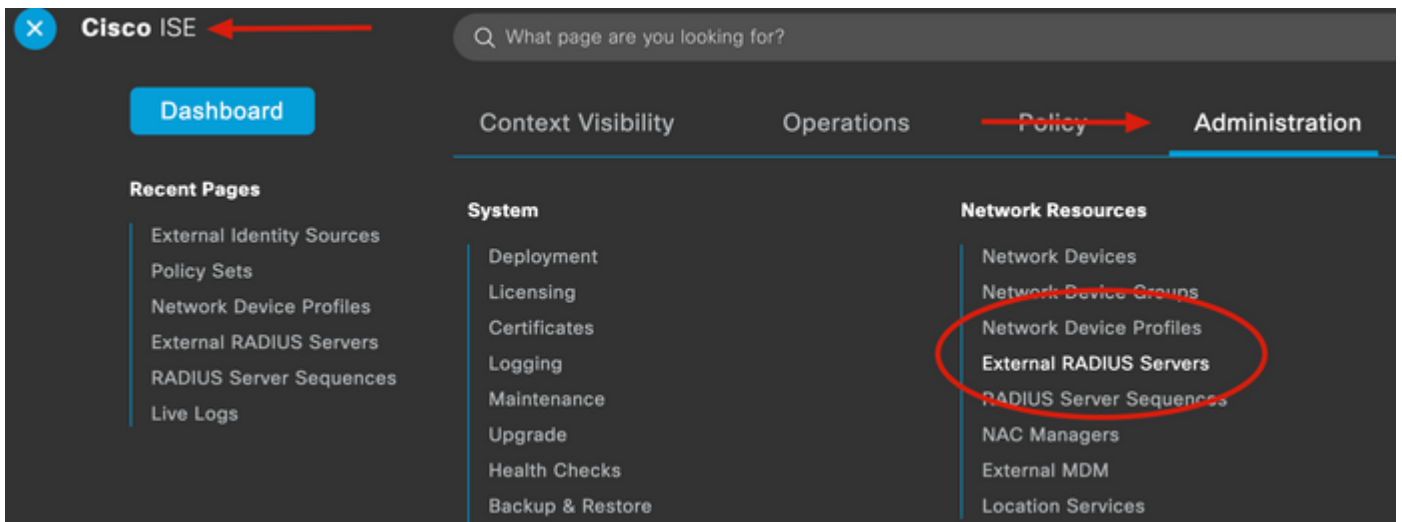
✓ **Validation passed**
Configuration has passed validation and is ready to be saved ←

Configure: authproxy.cfg	Unsaved Changes	Output
<pre>18 ; number to the section name (e.g. [ad_client2]) 19 20 [ad_client] 21 host=10.28.17.107 22 service_account_username=Administrator 23 service_account_password= 24 search_dn=DC=agarciam,DC=cisco 25 26 [radius_server_auto] 27 ikey= 28 skey= 29 api_host=api 30 radius_ip_1=10.28.17.101 31 radius_secret_1= 32 failmode=safe 33 client=ad_client 34 port=1812 35 36</pre>		<pre>Running The Duo Authentication Proxy Connection several minutes... [info] Testing section 'main' with configuration [info] {'debug': 'True', 'log_max_files': '10', 'log_max_size': '20971520', 'test_connectivity_on_startup': 'true'} [info] There are no configuration problems [info] ----- [info] Testing section 'ad_client' with configuration [info] {'debug': 'True', 'host': '10.28.17.107', 'search_dn': 'DC=agarciam,DC=cisco', 'service_account_password': '*****', 'service_account_username': 'Administrator'} [info] There are no configuration problems [info] ----- [info] Testing section 'radius_server_auto' with configuration</pre>

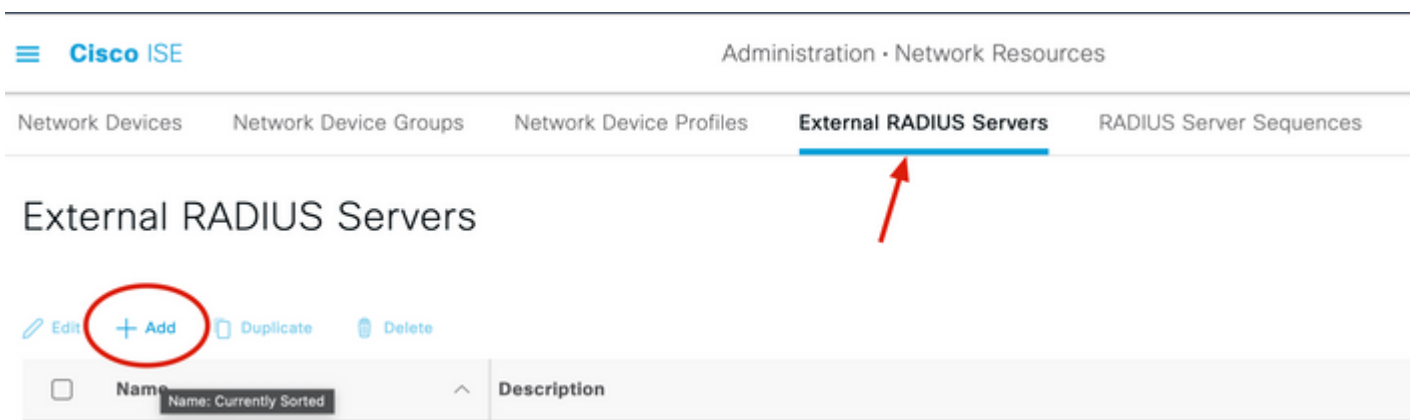
Validate Save [Learn how to c](#)

Cisco ISE-configuraties

1. Log in op het ISE-beheerportal.
2. Breid het tabblad Cisco ISE uit en navigeer naar **beheer**, klik vervolgens op **Network Resources** en klik op **Externe RADIUS-servers**.



3. Klik op het tabblad **Externe RADIUS-servers** op **Toevoegen**.



4. Vul de spatie in met de RADIUS-configuratie die wordt gebruikt in de Duo Authenticatie Proxy Manager en klik op **Indienen**.

Network Devices Network Device Groups Network Device Profiles **External RADIUS Servers** RADIUS Server Sequences

* Name: DUO_NEW

Description: [Empty text area]

* Host IP: 10.28.17.107

* Shared Secret:| [Show](#)

Enable KeyWrap: ⓘ

* Key Encryption Key: [Empty text area] [Show](#)

* Message Authenticator Code Key: [Empty text area] [Show](#)

Key Input Format: ASCII HEXADECIMAL

* Authentication Port: 1812 (Valid Range 1 to 65535)

* Accounting Port: 1813 (Valid Range 1 to 65535)

* Server Timeout: 5 Seconds (Valid Range 1 to 120)

* Connection Attempts: 3 (Valid Range 1 to 9)

Radius ProxyFailover Expiration: 300 ⓘ (valid Range 1 to 600)

5. Navigeer naar het tabblad **RADIUS-serversequenties** en klik op **Add**.

Cisco ISE Administration · Network Resources

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers **RADIUS Server Sequences**

RADIUS Server Sequences

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

[Edit](#) **+ Add** [Duplicate](#) [Delete](#)

6. Specificeer de naam van de reeks en wijs de nieuwe externe RADIUS-server toe. Klik op **Indienen**.

RADIUS Server Sequence

General

Advanced Attribute Settings

* Name

DUO_Sequence

Description

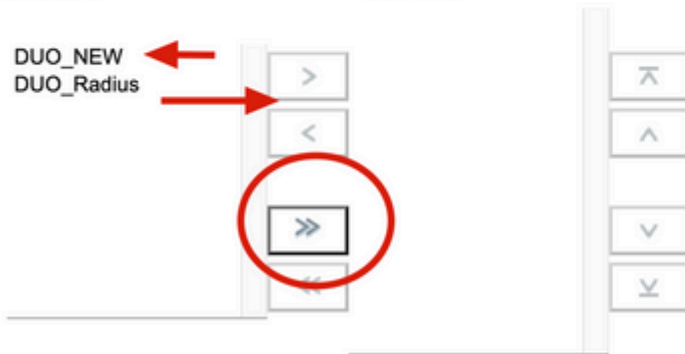
▼ User Selected Service Type

Select the set of external RADIUS servers to use to process requests. Servers are accessed in sequence until a response is r

Available

* Selected

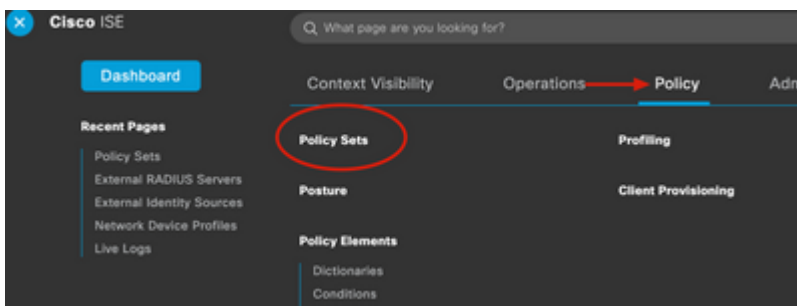
DUO_NEW
DUO_Radius



Remote accounting

Local accounting

7. Navigeer van het menu Dashboard naar **Beleid** en klik op **Beleidssets**.



8. Wijs de RADIUS-sequentie toe aan het standaardbeleid.

Opmerking: In dit document wordt de Duo-reeks op alle verbindingen toegepast, dus wordt het standaardbeleid gebruikt. De beleidstoe wijzing kan naar behoefte variëren.

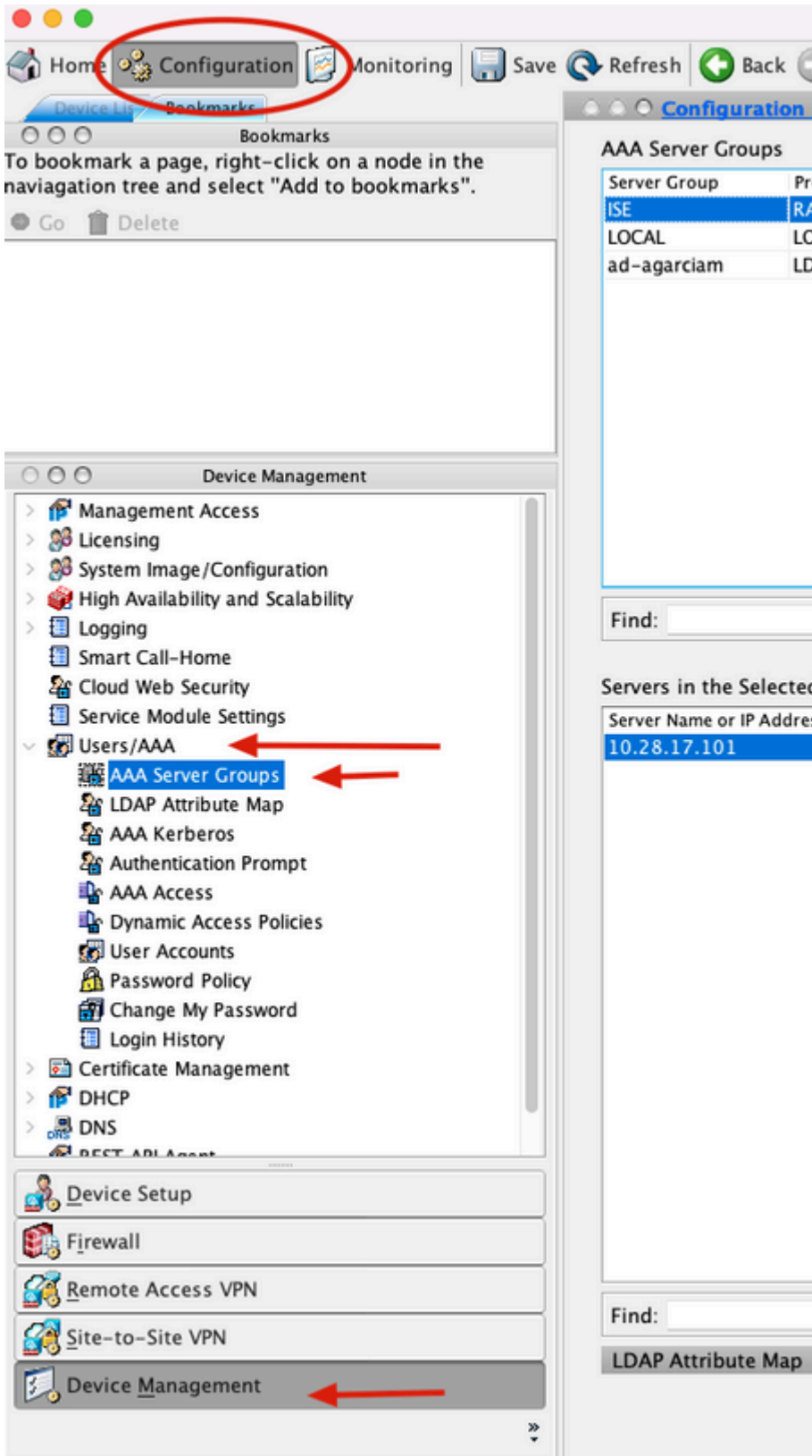
Policy Sets

Status	Policy Set Name	Description	Conditions
✓			Radius-User-Name EQUALS isevpn
✓			Radius-NAS-Port-Type EQUALS Virtual
✓	Default	Default policy set	



Cisco ASA RADIUS/ISE-configuratie

1. Configureer ISE RADIUS-server onder AAA-servergroepen, navigeer naar **Configuration** en klik vervolgens op **Apparaatbeheer** en vouw het gedeelte **Gebruikers/AAA uit**, selecteer **AAA-servergroepen**.



2. Klik in het paneel AAA-servergroepen op Add.

The screenshot shows the Cisco configuration interface for AAA Server Groups. The breadcrumb navigation is Configuration > Device Management > Users/AAA > AAA Server Groups. The main section is titled "AAA Server Groups" and contains a table with the following columns: Server Group, Protocol, Accounting Mode, Reactivation Mode, Dead Time, and Max Failed Attempts. The table is currently empty. To the right of the table are three buttons: "Add", "Edit", and "Delete". The "Add" button is circled in red. Below the table is a search bar with a "Find:" label, a search input field, and a "Match Case" checkbox. The bottom section is titled "Servers in the Selected Group" and contains a table with the following columns: Server Name or IP Address, Interface, and Timeout. This table is also empty. To the right of this table are six buttons: "Add", "Edit", "Delete", "Move Up", "Move Down", and "Test".

3. Selecteer de naam van de servergroep en specificeer **RADIUS** als het te gebruiken protocol en klik vervolgens op **OK**.

Add AAA Server Group

AAA Server Group: ISE

Protocol: RADIUS

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

Enable interim accounting update

Update Interval: 24 Hours

Enable Active Directory Agent mode

ISE Policy Enforcement

Enable dynamic authorization

Dynamic Authorization Port: 1700

Use authorization only mode (no common password configuration required)

VPN3K Compatibility Option

Help Cancel OK

5. Selecteer uw nieuwe servergroep en klik op **Add** onder de **Server in het paneel Geselecteerde groep**, zoals in de afbeelding.

Configuration > Device Management > Users/AAA > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
ISE	RADIUS	Single	Depletion	10	3
LOCAL	LOCAL			10	4

Find: Match Case

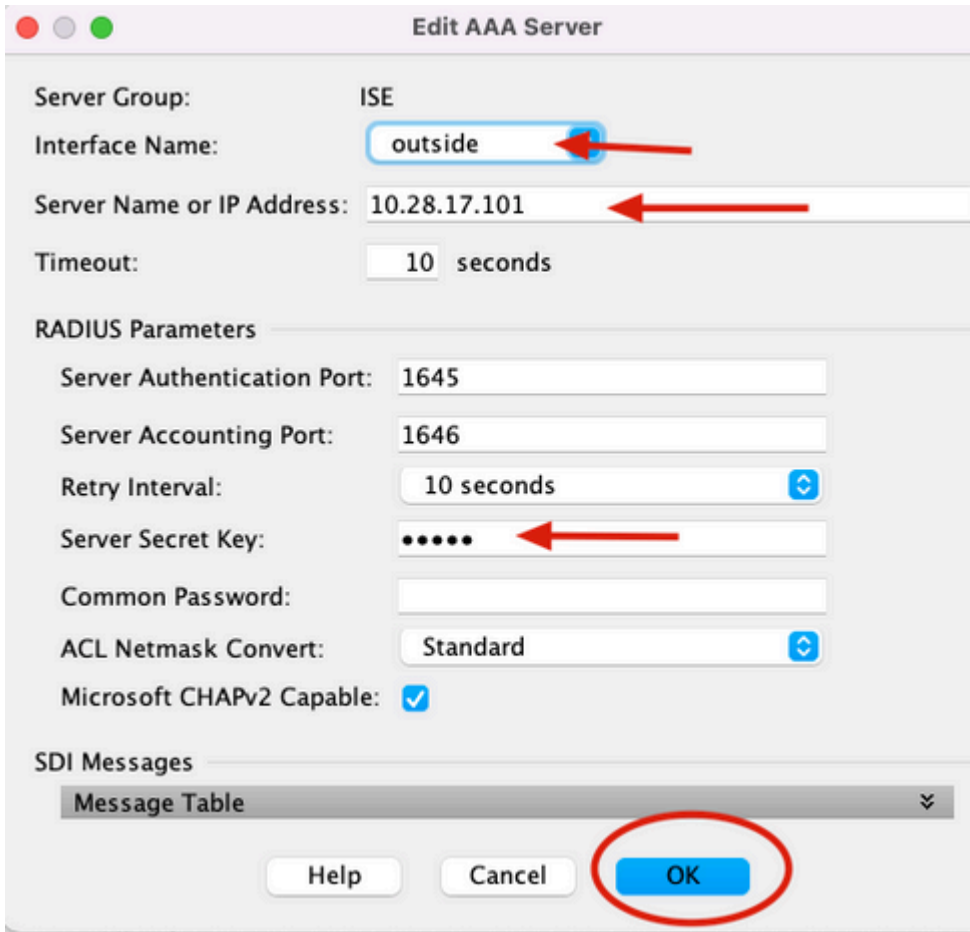
Servers in the Selected Group

Server Name or IP Address	Interface	Timeout

Buttons: Add, Edit, Delete, Move Up, Move Down

6. Selecteer in het venster **AAA-server bewerken** de interfacenaam, geef het IP-adres van de ISE-server op, typ de geheime RADIUS-toets en klik op **OK**.

Opmerking: al deze informatie moet overeenkomen met de informatie die in Duo Verification Proxy Manager is opgegeven.



CLI-configuratie.

```
aaa-server ISE protocol radius
dynamic-authorization
aaa-server ISE (outside) host 10.28.17.101
key *****
```

Cisco ASA VPN-configuratie voor externe toegang

```
ip local pool agarciam-pool 192.168.17.1-192.168.17.100 mask 255.255.255.0
```

```
group-policy DUO internal
group-policy DUO attributes
banner value This connection is for DUO authorized users only!
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split-agarciam
address-pools value agarciam-pool
```

```
tunnel-group ISE-users type remote-access
tunnel-group ISE-users general-attributes
address-pool agarciam-pool
authentication-server-group ISE
```

```
default-group-policy DUO
tunnel-group ISE-users webvpn-attributes
group-alias ISE enable
dns-group DNS-CISCO
```

Testen

1. Open de **AnyConnect**-app op uw pc-apparaat. Specificeer de hostnaam van de VPN ASA Head-end en log in met de gebruiker die is gemaakt voor Duo secundaire verificatie en klik op **OK**.

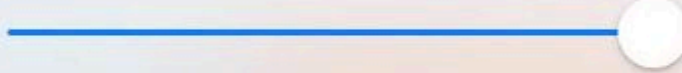


2. U hebt een Duo-push-melding ontvangen op het opgegeven Duo Mobile-apparaat.

3. Open de Duo Mobile App-melding en klik op **Goedkeuren**.

14:41

Lunes, 14 de marzo

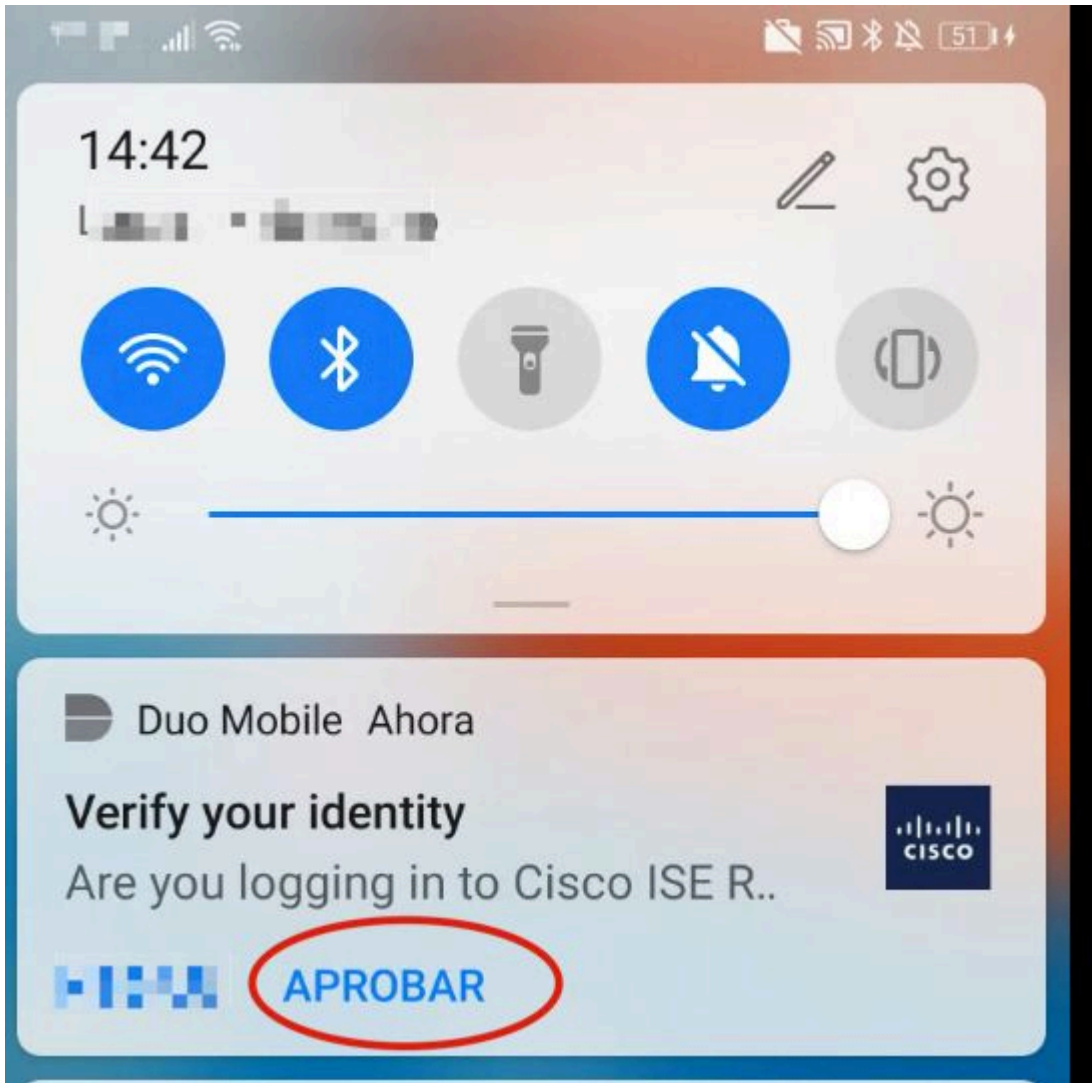


Duo Mobile Ahora

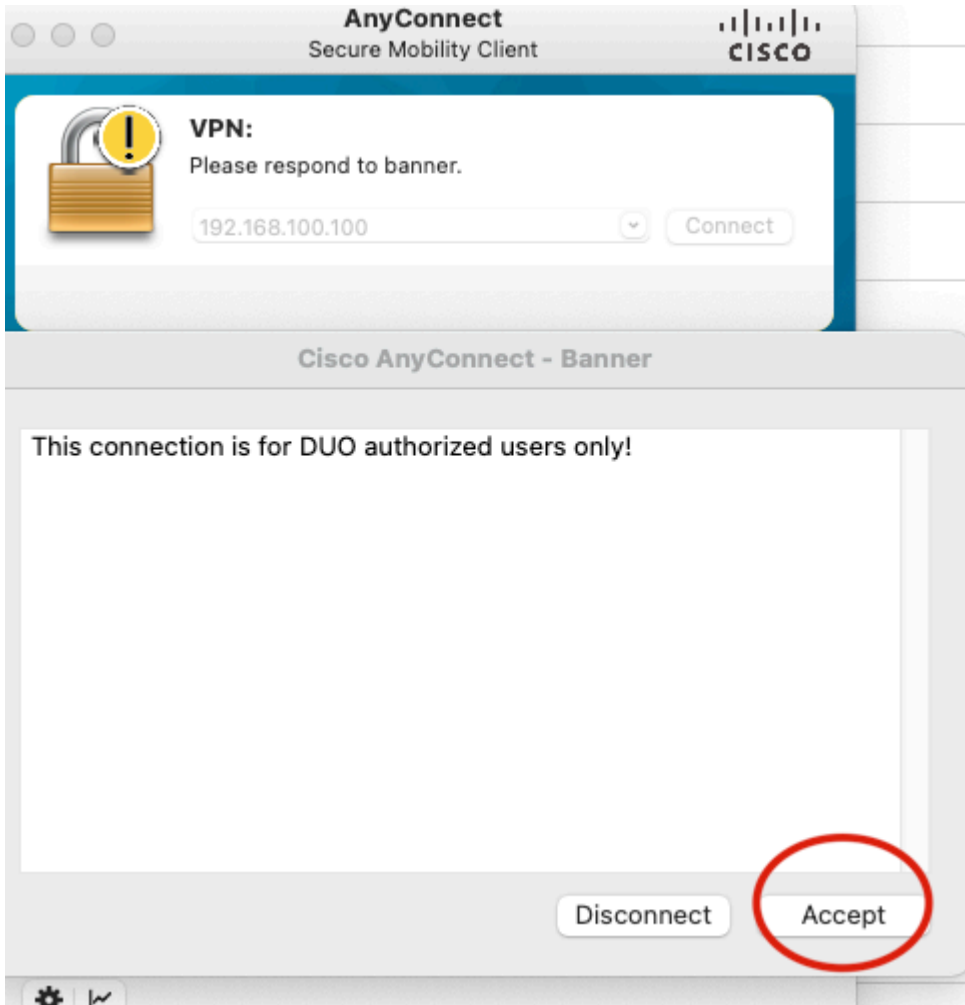
Verify your identity

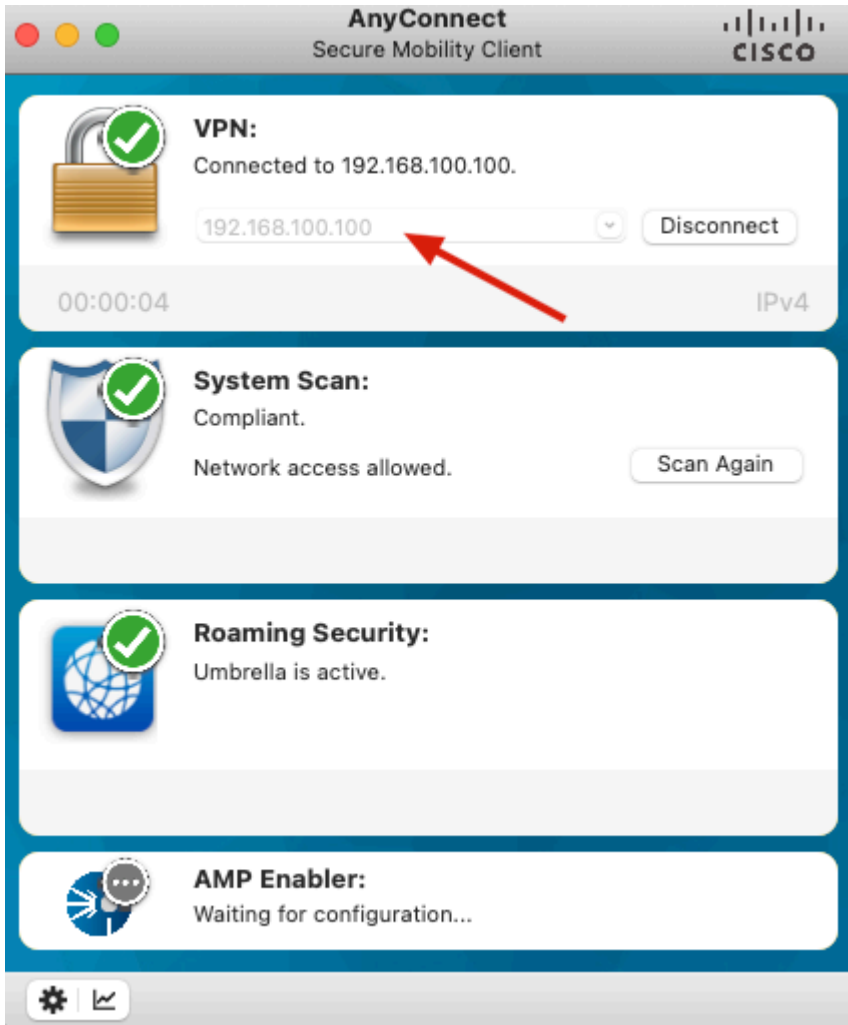
Are you logging in to Cisco ISE R..





4. Accepteer de banner en er wordt een verbinding tot stand gebracht.





Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

De Duo-verificatieproxy wordt geleverd met een debug-tool die de redenen voor fouten en fouten weergeeft.

Fouten in het werk

Opmerking: De volgende informatie wordt opgeslagen in C:\Program Files\Duo Security Authenticatie Proxy\log\connectiviteit_tool.log.

Output

Running The Duo Authentication Proxy Connectivity Tool. This may take several minutes...

[info] Testing section 'main' with configuration:

```
[info] {'debug': 'True',  
      'log_max_files': '10',  
      'log_max_size': '20971520',  
      'test_connectivity_on_startup': 'true'}
```

[info] There are no configuration problems

[info] -----

[info] Testing section 'ad_client' with configuration:

```
[info] {'debug': 'True',  
      'host': '10.28.17.107',  
      'search_dn': 'DC=agarciam,DC=cisco',  
      'service_account_password': '****',  
      'service_account_username': 'Administrator'}
```

[info] There are no configuration problems

[info] -----

[info] Testing section 'radius_server_auto' with configuration:

```
[info] {'api_host': '10.28.17.107',  
      'client': 'ad_client',  
      'debug': 'True',  
      'failmode': 'safe',  
      'ikey': 'XXXXXXXXXXXXXXXXXXXX',  
      'port': '1812',  
      'radius_ip_1': '10.28.17.101',  
      'radius_secret_1': '****',  
      'skey': '****[40]'}
```

[info] There are no configuration problems

[info] Testing section 'main' with configuration:

```
[info] {'debug': 'True',  
      'log_max_files': '10',  
      'log_max_size': '20971520',  
      'test_connectivity_on_startup': 'true'}
```

[info] There are no connectivity problems with the section.

```

[info] There are no connectivity problems with the section.
[info] -----
[info] Testing section 'ad_client' with configuration:
[info] {'debug': 'True',
      'host': '10.28.17.107',
      'search_dn': 'DC=agarciam,DC=cisco',
      'service_account_password': '*****',
      'service_account_username': 'Administrator'}
[info] The LDAP Client section has no connectivity issues.
[info] -----
[info] Testing section 'radius_server_auto' with configuration:
[info] {'api_host': 'api-adsync.wa.wa.dso.cisco.com',
      'client': 'ad_client',
      'debug': 'True',
      'failmode': 'safe',
      'ikey': 'XXXXXXXXXXXXXXXXXXXX',
      'port': '1812',
      'radius_ip_1': '10.28.17.101',
      'radius_secret_1': '*****',
      'skey': '*****[40]'}
[info] The RADIUS Server has no connectivity problems.
[info] -----
[info] SUMMARY
[info] No issues detected

```

1. Connectiviteitsproblemen, verkeerde IP, onoplosbare FQDN/Hostname op Active Directory-configuratie.

```

[ad_client]
host=10.28.17.106
service_account_username=Administrator
service_account_password=XXXXXXXXXXXX
search_dn=DC=agarciam,DC=cisco

```

```

Output
      'host': '10.28.17.106',
      'search_dn': 'DC=agarciam,DC=cisco',
      'service_account_password': '*****',
      'service_account_username': 'Administrator'}
[warn] The LDAP Client section has connectivity problems.
[warn] The LDAP host clear connection to 10.28.17.106:389 has
connectivity problems.
[error] The Auth Proxy was not able to establish a connection to 10
.28.17.106:389.

```

2. Verkeerd wachtwoord voor beheerder op Active Directory.

```
[ad_client]
host=10.28.17.107
service_account_username=Administrator
service_account_password=!@#$%^&*12345 ←
search_dn=DC=agarciam,DC=cisco
```

Debugs.

```
[info] The Auth Proxy was able to establish a connection to 10.28.17.107:389.
[info] The Auth Proxy was able to establish an LDAP connection to 10.28.17.107:389.
[error] The Auth Proxy was unable to bind as Administrator.
[error] Please ensure that the provided service account credentials are correct.
[debug] Exception: invalidCredentials: 8009030C: LdapErr: DSID-0C090516, comment: AcceptSecurityContext error, data 52e, v3839
[warn] The Auth Proxy did not run the search check because of the problem(s) with the bind check. Resolve that issue and rerun the tester.
```

3. Wrong Base Domain.

```
[ad_client]
host=10.28.17.107
service_account_username=Administrator
service_account_password=!@#$%^&*12345
search_dn=DC=agarciam,DC=ciscoo ←
```

Debugs.

```
[info] The Auth Proxy was able to bind as Administrator.
[error] The Auth Proxy got an error searching for 'agarciam,ciscoo'.
[debug] Exception: referral: 0000202B: RefErr: no such object
1 access points
ref 1: 'agarciam.ciscoo'
```


700	20.866684	10.28.17.3	10.28.17.107	RADIUS	88 Access-Request id=13, Duplicate Request
737	22.184895	10.28.17.107	10.28.17.3	RADIUS	90 Access-Accept id=13

> Frame 700: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF_{CA092CEE-552B-4E0A-9310-2D523160DD60}, id 0
> Ethernet II, Src: VMware_b3:f2:72 (00:50:56:b3:f2:72), Dst: VMware_b3:b4:3e (00:50:56:b3:b4:3e)
> Internet Protocol Version 4, Src: 10.28.17.3, Dst: 10.28.17.107
> User Datagram Protocol, Src Port: 51188, Dst Port: 1812
v RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0xd (13)
Length: 46
Authenticator: 20202020202031363436393335333230
[\[Duplicate Request Frame Number: 532\]](#)
[\[The response to this request is in frame 737\]](#)
v Attribute Value Pairs
> AVP: t=User-Name(1) l=8 val=duovpn
> AVP: t=User-Password(2) l=18 val=Encrypted

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.