

SSL VPN-verificatie configureren via FTD, ISE, DUO en Active Directory

Inhoud

[Inleiding](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Configuraties](#)

[FTD-configuraties.](#)

[Een RADIUS-server integreren in het Firepower Management Center \(FMC\)](#)

[Configureer de externe VPN.](#)

[ISE-configuraties.](#)

[Integreer DUO als een Externe Radius Server.](#)

[Integreer de FTD als een netwerktoegangsapparaat.](#)

[DUO-configuraties.](#)

[DUO Proxy-installatie.](#)

[Integreren DUO Proxy met ISE en DUO Cloud.](#)

[Integreren DUO met Active Directory.](#)

[Exporteer gebruikersaccounts vanuit Active Directory \(AD\) via DUO Cloud.](#)

[Gebruikers inschrijven in de Cisco DUO Cloud.](#)

[Configuratievalidatieprocedure.](#)

[Veelvoorkomende problemen.](#)

[Werkscenario.](#)

[Fout11353 Geen externe RADIUS-servers meer: geen failover meer uitvoeren](#)

[De RADIUS-sessies worden niet weergegeven in de live ISE-logboeken.](#)

[Aanvullende probleemoplossing.](#)

Inleiding

Dit document beschrijft de integratie van SSL VPN in Firepower Threat Defence met behulp van Cisco ISE en DUO Security voor AAA.

Vereisten

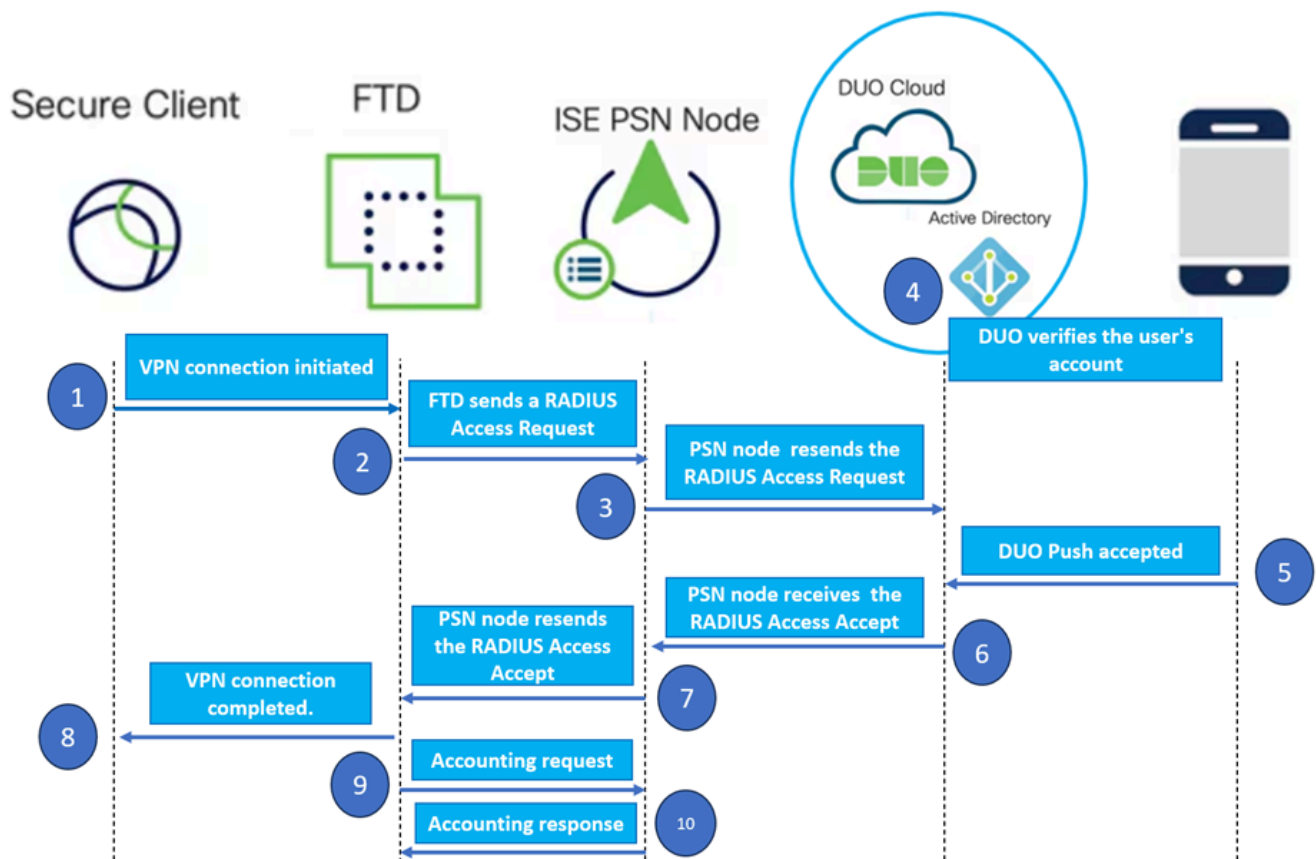
- ISE 3.0 of hoger.
- VCC 7.0 of hoger.
- FTD 7.0 of hoger.
- DUO-verificatieproxy.
- ISE Essentials-licenties
- Licentie voor DUO Essentials.

Gebruikte componenten

- ISE 3.2-patch 3
- VCC 7.2.5
- FTD 7.2.5
- Proxy DUO 6.3.0
- Any Connect 4.10.08029

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.

Netwerkdigram



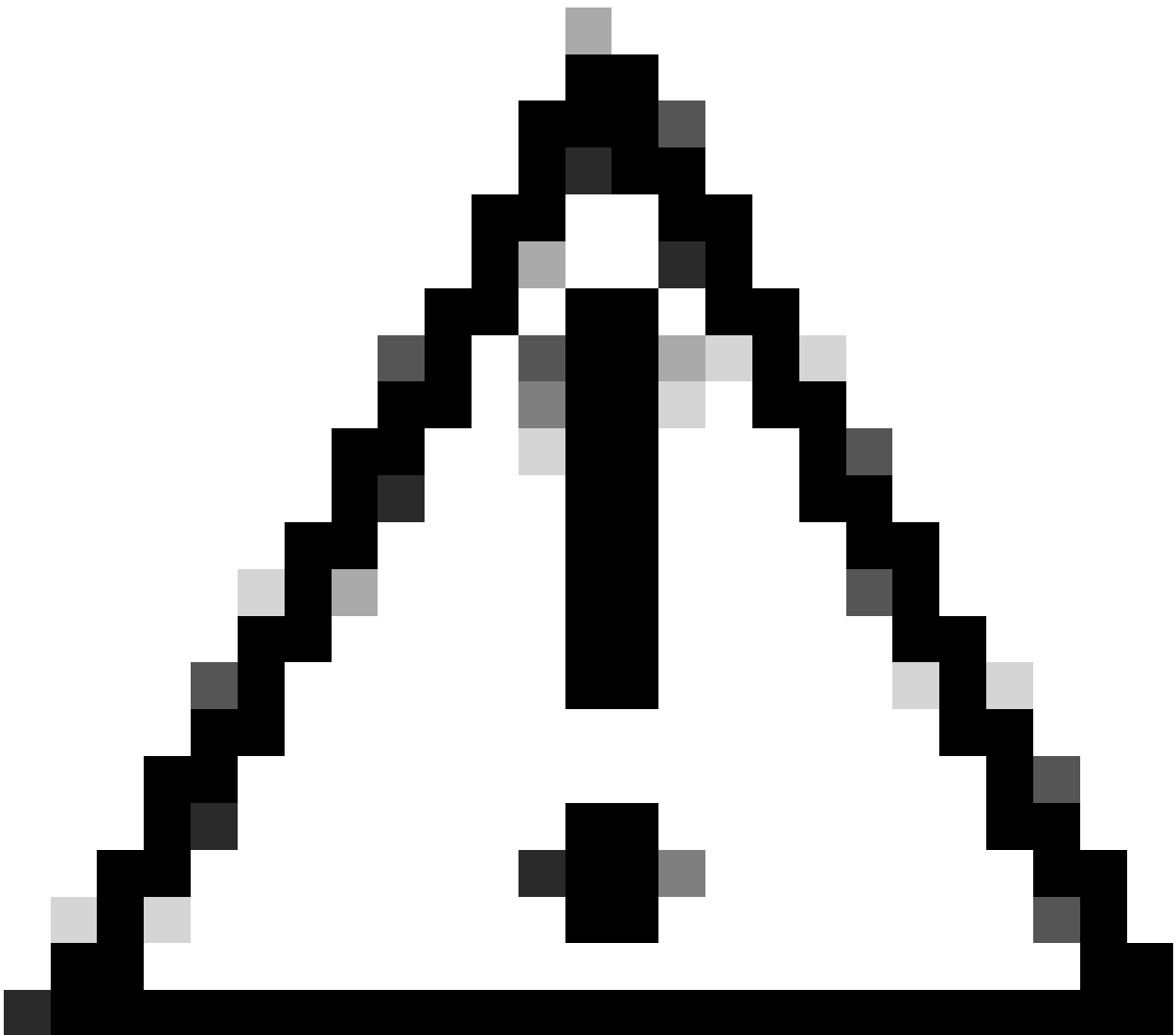
Topologie.

In onze voorgestelde oplossing is Cisco ISE een cruciale RADIUS-serverproxy. In plaats van een directe evaluatie van het verificatie- of autorisatiebeleid, is ISE geconfigureerd om de RADIUS-pakketten van de FTD naar de DUO-verificatieproxy te sturen.

De DUO-verificatieproxy fungeert als een speciale intermediair binnen deze verificatiestroom. Het is op een Windows-server geïnstalleerd en overbruggt de kloof tussen Cisco ISE en de DUO-cloud. De proxy primaire functie is het verzenden van verificatieverzoeken - ingekapseld in RADIUS-pakketten - naar de DUO Cloud. De DUO Cloud staat uiteindelijk netwerktoegang toe of ontkent

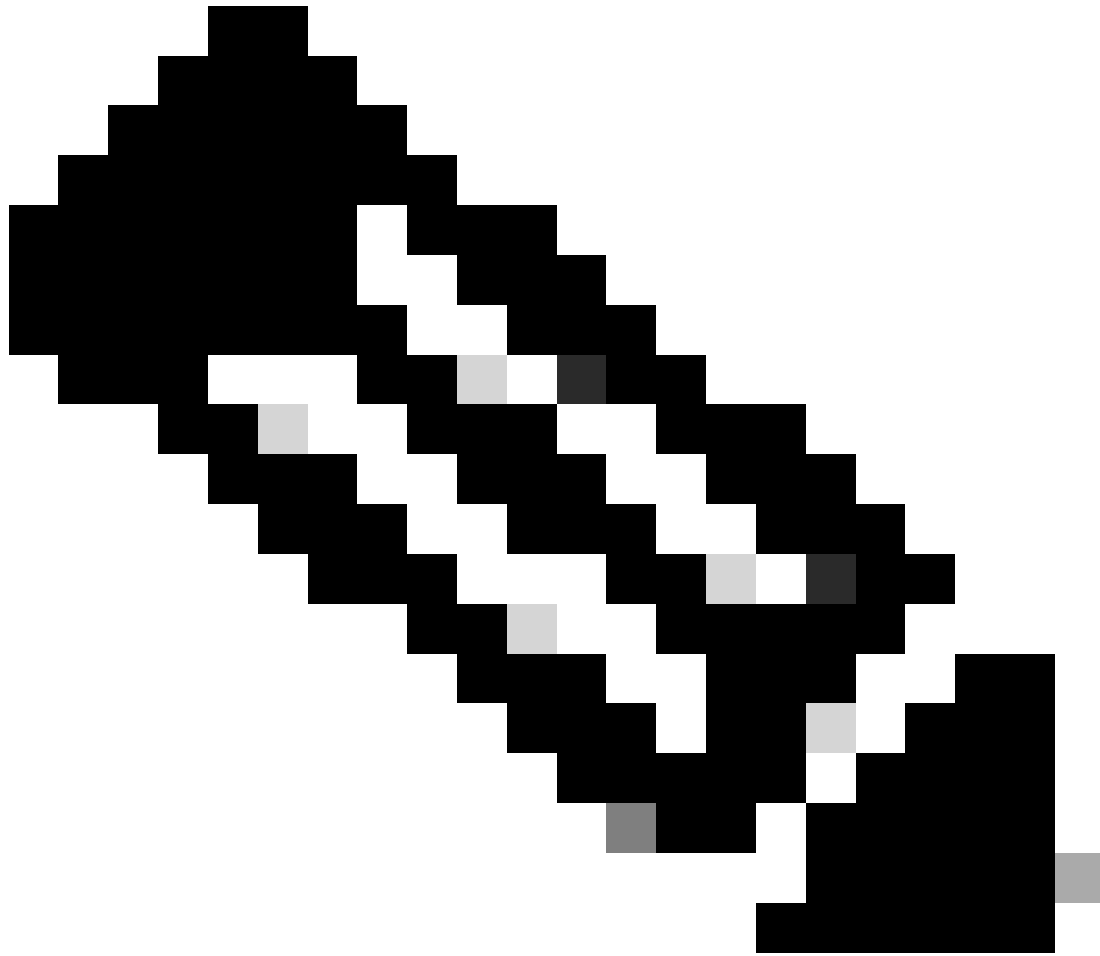
op basis van de tweevoudige verificatieconfiguraties.

1. De gebruiker start het VPN-verificatieproces door hun unieke gebruikersnaam en wachtwoord in te voeren.
2. De Firewall Threat Defence (FTD) stuurt het verificatieverzoek naar Cisco Identity Services Engine (ISE).
3. Het Policy Services Node (PSN) stuurt het verificatieverzoek door naar de DUO-verificatieproxyserver. Vervolgens valideert de DUO-verificatieserver de referenties via de DUO Cloud-service.
4. De DUO Cloud valideert de gebruikersnaam en het wachtwoord tegen zijn gesynchroniseerde database.



Let op: de synchronisatie tussen de DUO Cloud en de organisaties Active Directory moet actief zijn om een up-to-date gebruikersdatabase in de DUO Cloud te onderhouden.

5. Na een succesvolle verificatie start de DUO Cloud een DUO Push naar de gebruikers die geregistreerd zijn op een mobiel apparaat via een beveiligde, versleutelde push-melding. De gebruiker moet dan de DUO Push goedkeuren om hun identiteit te bevestigen en verder te gaan.
6. Zodra de gebruiker de DUO Push goedkeurt, stuurt de DUO-verificatieproxy-server een bevestiging terug naar de PSN om aan te geven dat de verificatieaanvraag door de gebruiker is geaccepteerd.
7. Het PSN-knooppunt stuurt de bevestiging naar het FTD om te informeren dat de gebruiker is geauthentiseerd.
8. Het FTD ontvangt de verificatiebevestiging en stelt de VPN-verbinding met het eindpunt in met de juiste beveiligingsmaatregelen.
9. De FTD registreert de details van de succesvolle VPN-verbinding en stuurt de boekhoudgegevens veilig terug naar het ISE-knooppunt voor het bijhouden van gegevens en audits.
10. Het ISE-knooppunt registreert de boekhoudinformatie in zijn levensonderhoud en zorgt ervoor dat alle gegevens veilig worden opgeslagen en toegankelijk zijn voor toekomstige audits of nalevingscontroles.



Opmerking:

Voor de installatie in deze handleiding worden de volgende netwerkparameters gebruikt:

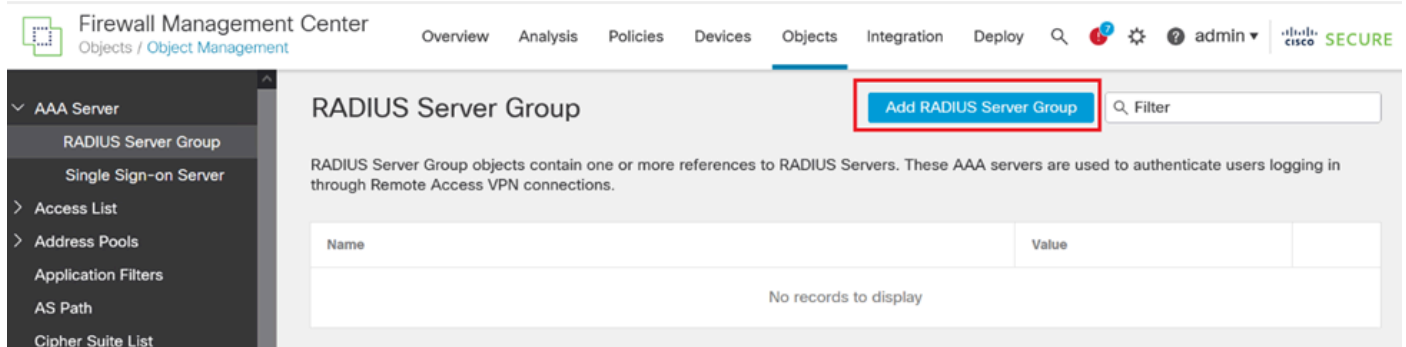
- IP-knooppunt voor primaire netwerkserver (PNS): 10.4.23.21
- FTD (Firepower Threat Defence) IP voor peer VPN: 10.4.23.53
- DUO-verificatieproxy voor IP: 10.31.126.2007
- Domeinnaam: testlab.local

Configuraties

FTD-configuraties.

Een RADIUS-server integreren in het Firepower Management Center (FMC)

1. Open het VCC door uw webbrowser te starten en het IP-adres van het VCC in te voeren om de grafische gebruikersinterface (GUI) te openen.
2. Ga naar het menu Objecten, selecteer AAA-server en ga verder naar de optie RADIUS-servergroep.
3. Klik op de knop RADIUS-servergroep toevoegen om een nieuwe groep voor RADIUS-servers te maken.



RADIUS-servergroep.

4. Voer een beschrijvende naam in voor de nieuwe AAA RADIUS-servergroep om een duidelijke identificatie binnen uw netwerkinfrastructuur te garanderen.
5. Voeg vervolgens een nieuwe RADIUS-server toe door de juiste optie te selecteren binnen de groepsconfiguratie.

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname	
No records to display	

RADIUS-server.

6. Specificeer het IP-adres van RADIUS-servers en voer de gedeelde geheime sleutel in.



Opmerking: het is van essentieel belang dat deze geheime sleutel veilig wordt gedeeld met de ISE-server om een succesvolle RADIUS-verbinding tot stand te brengen.

New RADIUS Server



IP Address/Hostname:*

10.4.23.21

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

1812

Key:*

●●●●●●●●

Confirm Key:*

●●●●●●●●

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

Connect using:

Routing Specific Interface



Cancel

Save

Nieuwe RADIUS-server.

7. Klik na het configureren van de RADIUS-servergegevens op Save om de instellingen voor de RADIUS-servergroep te bewaren.

Add RADIUS Server Group



Enable authorize only

Enable interim account update

Interval:* (1-120) hours

24

Enable dynamic authorization

Port:* (1024-65535)

1700

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

10.4.23.21



Cancel

Save

Gegevens over servergroep.

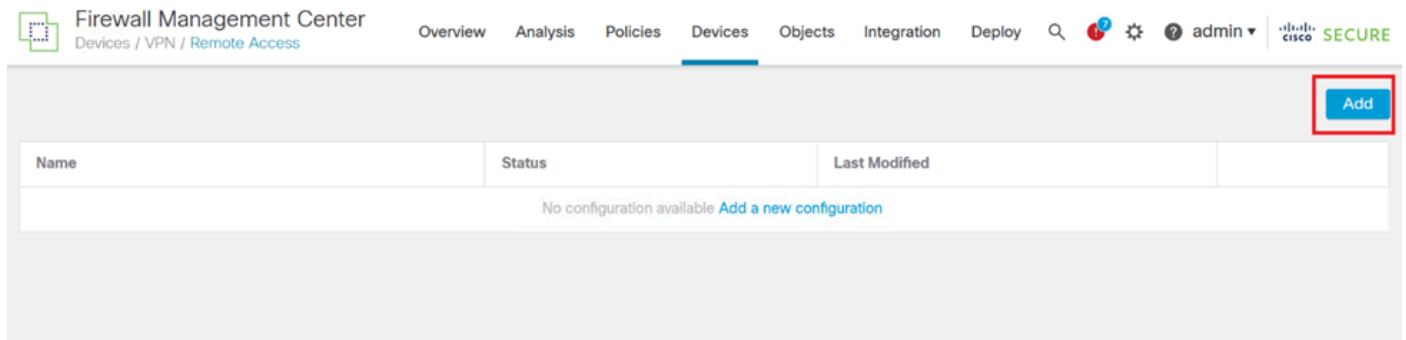
8. Als u de AAA-serverconfiguratie in uw netwerk wilt voltooien en implementeren, navigeert u naar het menu Implementeren en vervolgens selecteert u Alles implementeren om de instellingen toe te passen.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', and 'Deploy'. The 'Deploy' menu is highlighted with a red box. Below the navigation bar, the 'RADIUS Server Group' configuration page is visible. The left sidebar shows a tree view with 'AAA Server' expanded, and 'RADIUS Server Group' selected. The main content area shows the 'RADIUS Server Group' configuration, including a search bar, 'Advanced Deploy' link, and a 'Deploy All' button highlighted with a red box. The table below shows one entry: 'FTD_01' with a status of 'Ready for Deployment'.

AAA-server implementeren.

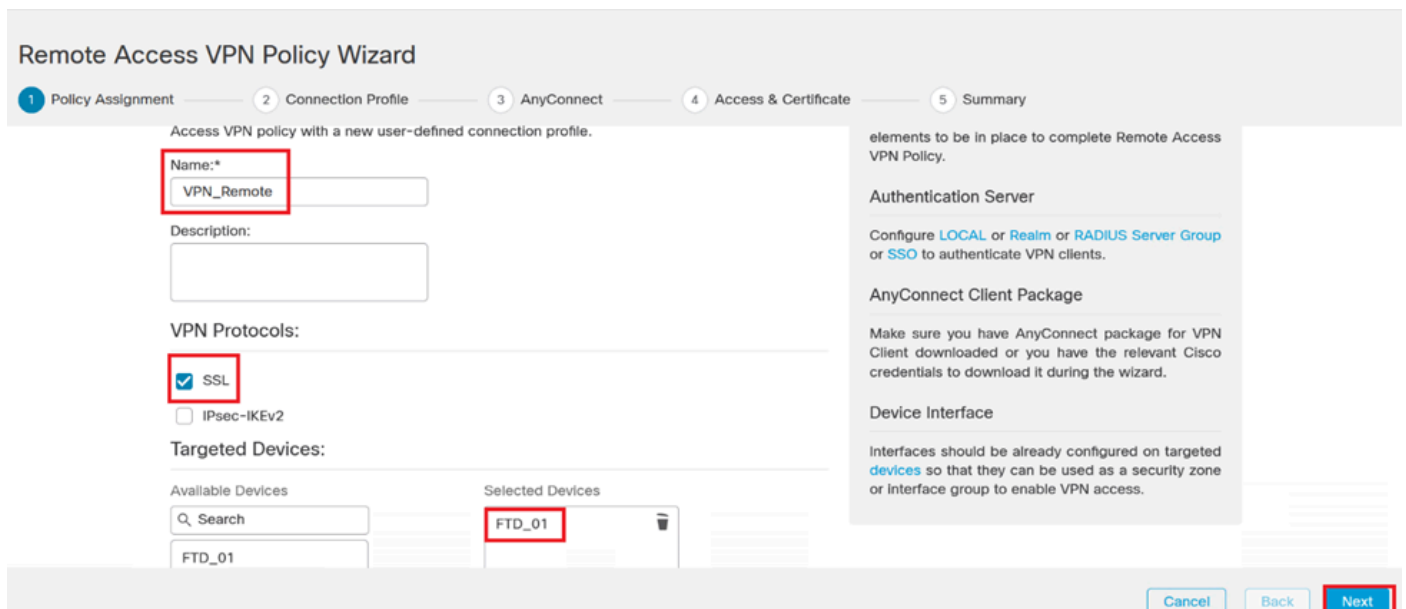
Configureer de externe VPN.

1. Ga naar Apparaten > VPN > Externe toegang in de FMC GUI om het VPN-configuratieproces te starten.
2. Klik op de knop Add om een nieuw VPN-verbindingsprofiel te maken.



VPN-verbindingsprofiel.

3. Voer een unieke en beschrijvende naam voor VPN in om de VPN binnen uw netwerkinstellingen te helpen identificeren.
4. Kies de SSL-optie om een beveiligde verbinding te garanderen met behulp van het SSL VPN-protocol.
5. Selecteer het specifieke FTD-apparaat in de lijst met apparaten.



VPN-instellingen.

6. Configureer de AAA-methode om de PSN-knooppunt in de verificatie-instellingen te gebruiken.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: **AAA Only** ▼

Authentication Server:* **ISE** ▼ +

(LOCAL or Realm or RADIUS)

Fallback to LOCAL Authentication

Authorization Server: **Use same authentication server** ▼ +

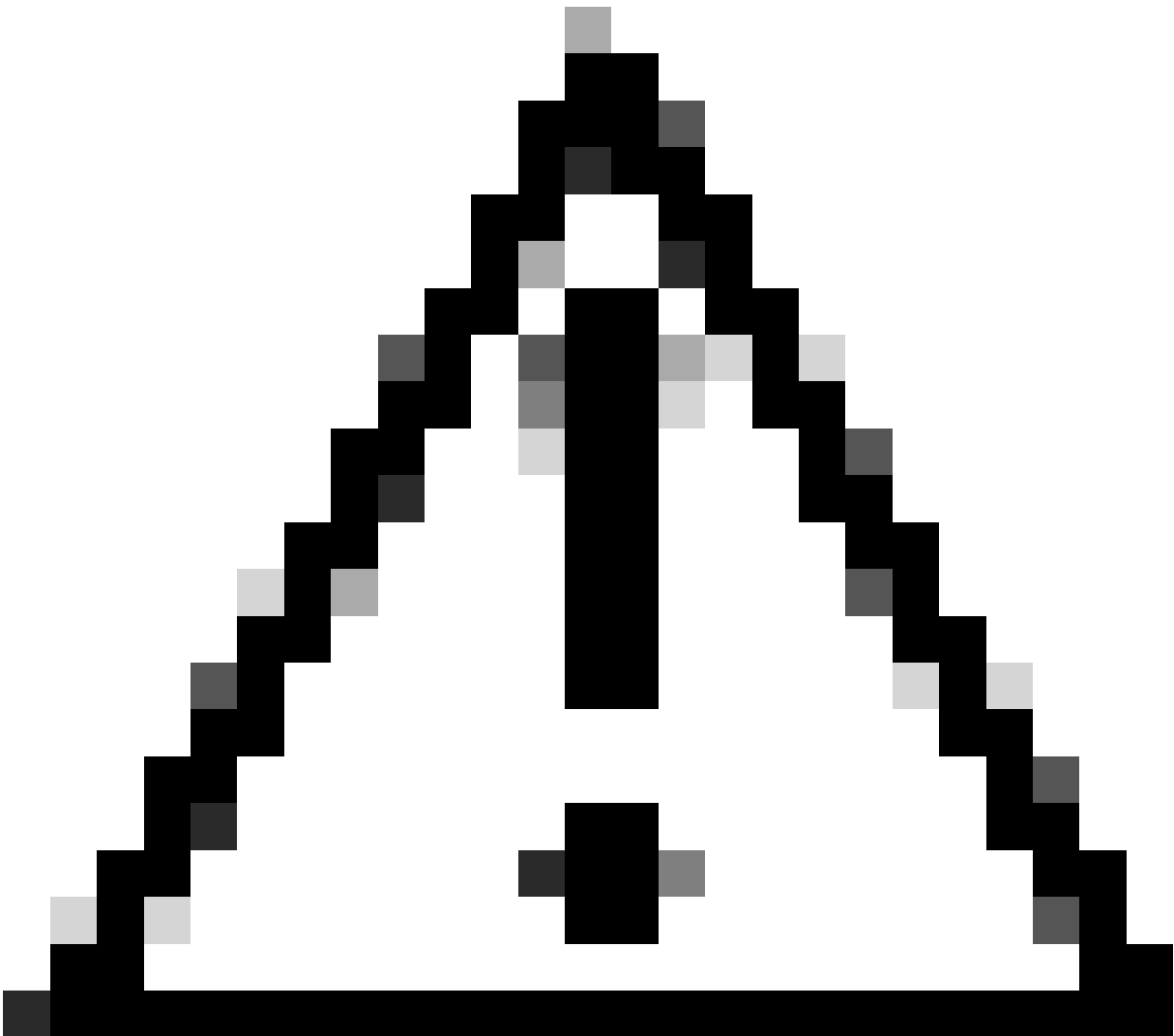
(realm or RADIUS)

Accounting Server: **ISE** ▼ +

(RADIUS)

Verbindingsprofiel.

7. Stel dynamische IP-adrestoewijzing in voor VPN.



Waarschuwing: bijvoorbeeld is de DHCP VPN-pool geselecteerd.

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: 

IPv6 Address Pools: 

IP-adresgroep.

8. Ga verder met het creëren van een nieuw groepsbeleid.

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:*  

[Edit Group Policy](#)

Groepsbeleid.

9. Controleer of in de instellingen Groepsbeleid het SSL-protocol is geselecteerd.

Add Group Policy



Name:*

VPN_Remote_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Cancel

Save

VPN-protocollen.

10. Maak een nieuwe VPN-pool of selecteer een bestaande om de reeks IP-adressen te definiëren die beschikbaar zijn voor VPN-clients.

Add Group Policy



Name:*

VPN_Remote_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IP Address Pools:



Name

IP Address Range

Cancel

Save

Pool VPN.

1. Specificeer de DNS-servergegevens voor de VPN-verbinding.

Add Group Policy



Name:*

VPN_Remote_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Primary DNS Server:



Secondary DNS Server:



Primary WINS Server:



Secondary WINS Server:



DHCP Network Scope:



Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Cancel

Save



Waarschuwing: extra functies zoals Banner, Split Tunneling, AnyConnect en Geavanceerde opties worden als optioneel beschouwd voor deze configuratie.

12. Klik na het configureren van de benodigde gegevens op Volgende om verder te gaan naar de volgende fase van de installatie.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:*

[Edit Group Policy](#)

Cancel

Back

Next

Groepsbeleid.

13. Selecteer het juiste AnyConnect-pakket voor de VPN-gebruikers. Als het vereiste pakket niet wordt vermeld, hebt u de optie om het benodigde pakket in deze fase toe te voegen.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

Select at least one AnyConnect Client image

[Show Re-order buttons](#)

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input type="checkbox"/>	anyconnect-win-4.10.08029-we...	anyconnect-win-4.10.08029-webdeploy-k9...	Windows

Cancel

Back

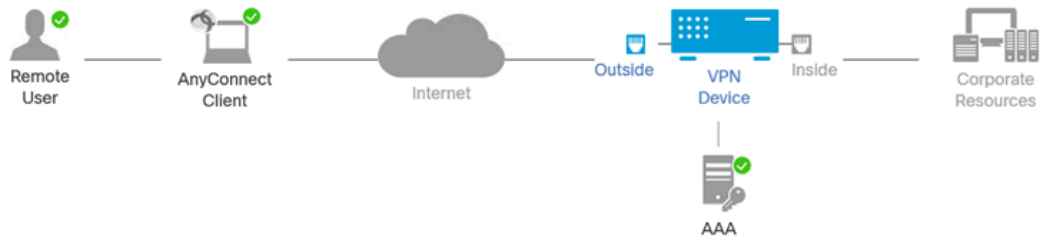
Next

Pakketinstallatie.

14. Kies de netwerkinterface op het FTD-apparaat waarin u de externe functie van VPN wilt inschakelen.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary



Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

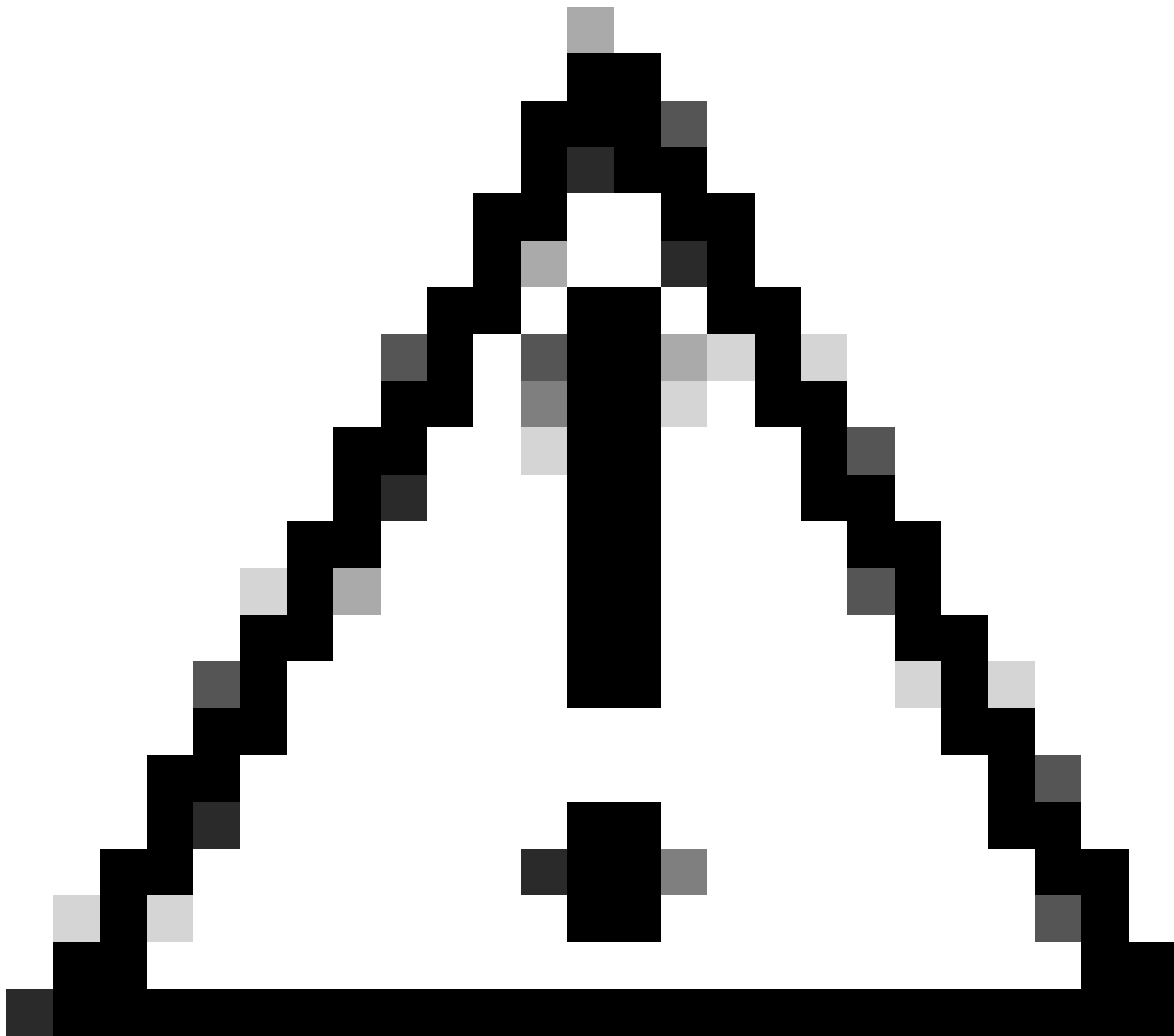
Interface group/Security Zone:* +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

VPN-interface

15. Voer een certificaatschrijvingsproces in door een van de beschikbare methoden te selecteren om het certificaat op de firewall te maken en te installeren, wat essentieel is voor beveiligde VPN-verbindingen.



Waarschuwing: in deze handleiding is bijvoorbeeld een zelfondertekend certificaat geselecteerd.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:*

 ▼ +

Apparaatcertificaat.

Add Cert Enrollment



Name*

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

SCEP

Enrollment URL:*

Self Signed Certificate

EST

Challenge Password:

SCEP

Confirm Password:

Manual

PKCS12 File

Retry Period:

1 (Range 0-60)

Retry Count:

10

(Range 0-100)

Fingerprint:

Cancel

Save

Cert-inschrijving.

16. Klik op Volgende zodra de certificaatinschrijving is geconfigureerd.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Will access for VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Overzicht van Access & services

17. Bekijk de samenvatting van al uw configuraties om er zeker van te zijn dat ze nauwkeurig zijn en uw beoogde instellingen weergeven.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	VPN_Remote
Device Targets:	FTD_01
Connection Profile:	VPN_Remote
Connection Alias:	VPN_Remote
AAA:	
Authentication Method:	AAA Only
Authentication Server:	ISE (RADIUS)
Authorization Server:	ISE (RADIUS)
Accounting Server:	ISE
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	Pool_VPN
Address Pools (IPv6):	-
Group Policy:	VPN_Remote_Policy
AnyConnect Images:	anyconnect-win-4.10.08029-webdeploy-k9.pkg
Interface Objects:	Outside
Device Certificates:	Cert_Enrollment

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration
SSL will be enabled on port 443. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.
- ▲ Network Interface Configuration
Make sure to add interface from targeted

Samenvatting van VPN-instellingen.

18. Om de configuratie van de externe VPN-toegang toe te passen en te activeren, navigeer om alles te implementeren > implementeren en voer de implementatie uit op het geselecteerde FTD-apparaat.

VPN-instellingen implementeren.

ISE-configuraties.

Integreer DUO als een Externe Radius Server.

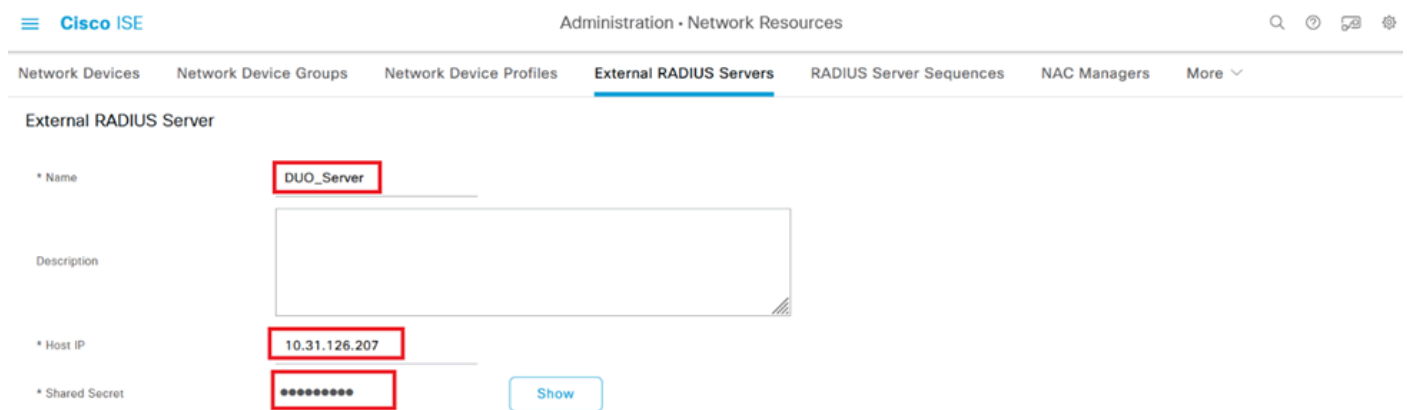
1. Navigeer naar Beheer > Netwerkbronnen > Externe RADIUS-servers in de Cisco ISE-beheerinterface.
2. Klik op de knop Add om een nieuwe externe RADIUS-server te configureren.

Externe RADIUS-servers

3. Voer een naam in voor de Proxy DUO Server.
4. Voer het juiste IP-adres in voor de Proxy DUO Server om een juiste communicatie tussen de ISE en de DUO-server te waarborgen.
5. Stel de gedeelde geheime sleutel in.

Opmerking: deze gedeelde geheime sleutel moet in de Proxy DUO Server worden geconfigureerd om een RADIUS-verbinding tot stand te brengen.

6. Zodra alle details correct zijn ingevoerd, klikt u op **Indienen** om de nieuwe Proxy DUO Server-configuratie op te slaan.



The screenshot shows the Cisco ISE Administration interface for configuring an External RADIUS Server. The breadcrumb trail is Administration > Network Resources > External RADIUS Servers. The configuration form includes the following fields:

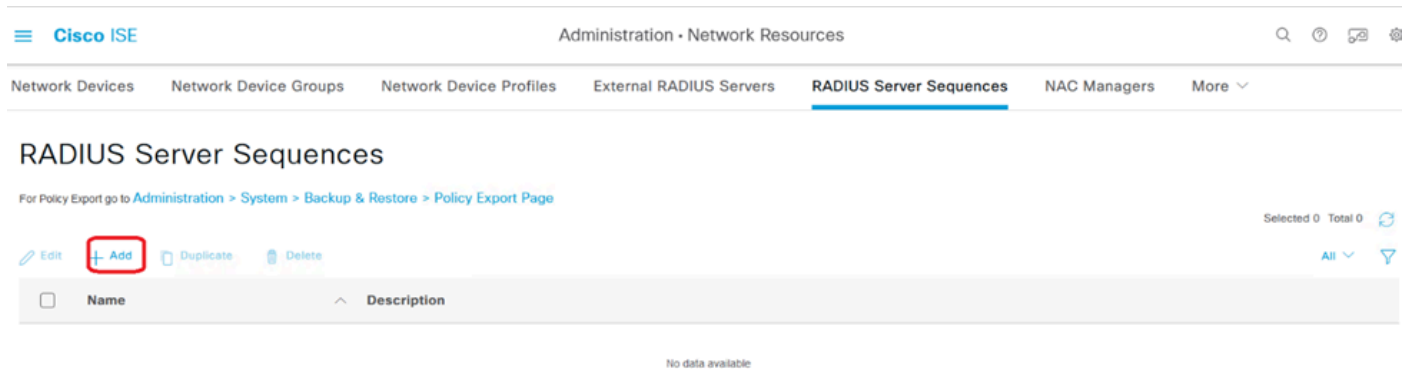
- * Name:** DUO_Server
- Description:** (Empty text area)
- * Host IP:** 10.31.126.207
- * Shared Secret:** (Masked with asterisks)

A "Show" button is located next to the Shared Secret field.

Externe RADIUS-servers

7. Ga verder naar Beheer > RADIUS-serverreeks.

8. Klik op Add om een nieuwe RADIUS-serverreeks te maken.

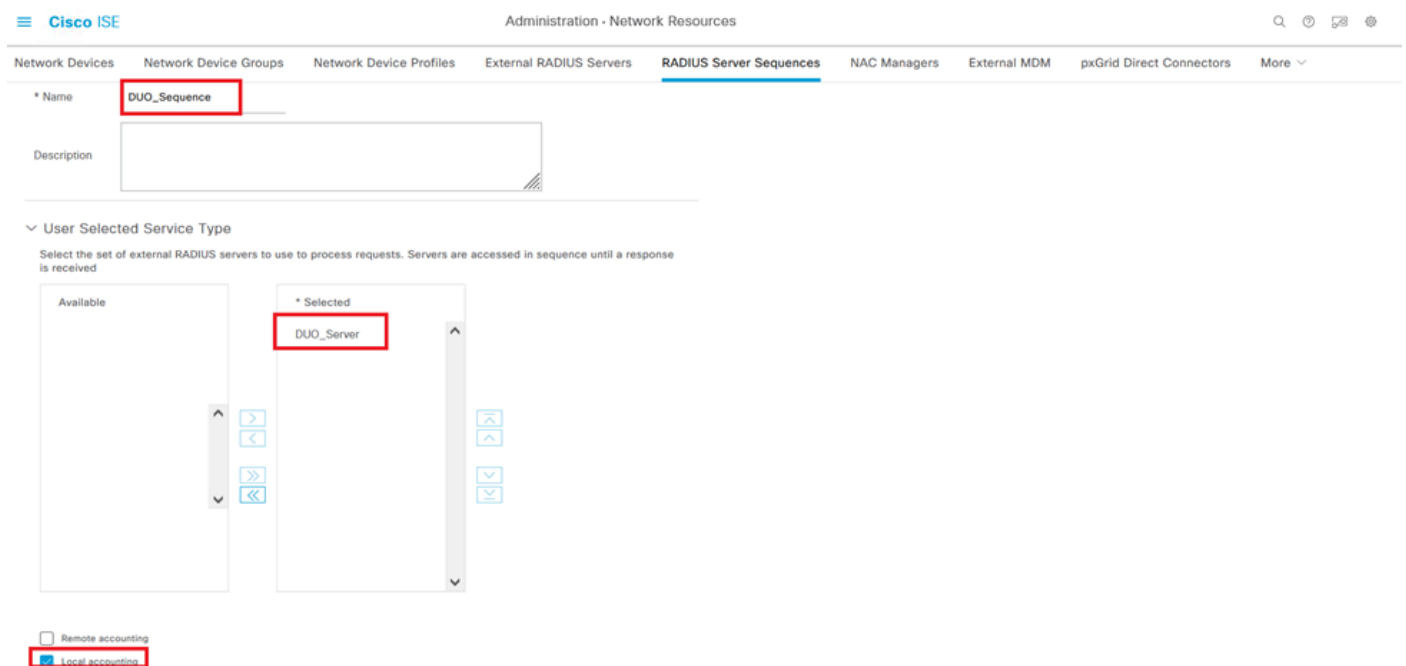


RADIUS-serversequenties

9. Geef een duidelijke naam voor de RADIUS-serverreeks voor eenvoudige identificatie.

10. Zoek de eerder geconfigureerde DUO RADIUS-server, DUO_Server genoemd in deze handleiding, en verplaats deze naar de geselecteerde lijst rechts om deze in de reeks op te nemen.

11. Klik op Indienen om de configuratie van de RADIUS-serverreeks te voltooien en op te slaan.

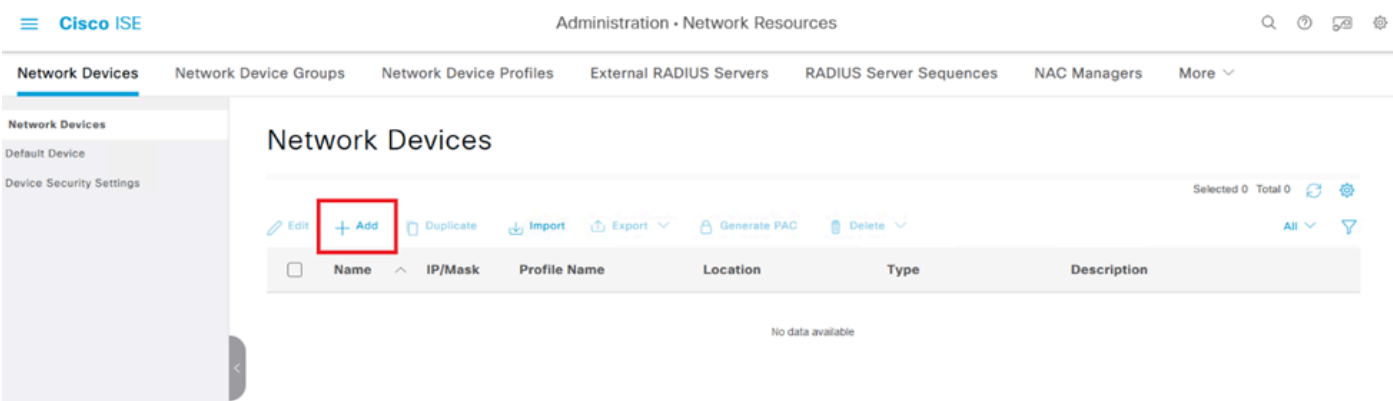


Configuratie van de RADIUS-serverreeks.

Integreer de FTD als een netwerktoegangsapparaat.

1. Navigeer naar het gedeelte Beheer in uw systeeminterface en selecteer vervolgens Network Resources om toegang te krijgen tot het configuratiegebied voor netwerkapparaten.

2. Zoek en klik in het gedeelte Network Resources eenmaal op de knop Add om het proces voor het toevoegen van een nieuw netwerktoegangsapparaat te starten.



Netwerkttoegangsapparaten.

3. Voer in de daarvoor bestemde velden de naam van het netwerkttoegangsapparaat in om het apparaat in uw netwerk te identificeren.
4. Specificeer vervolgens het IP-adres van het FTD-apparaat (Firepower Threat Defence).
5. Voer de sleutel in die eerder is ingesteld tijdens de installatie van het VCC (Firepower Management Center). Deze sleutel is essentieel voor veilige communicatie tussen apparaten.
6. Voltooi de procedure door op de knop **Indienen** te klikken.

[Network Devices List](#) > **FTD**

Network Devices

Name

FTD

Description

IP Address

* IP :

10.4.23.53

/

32



FTD toevoegen als NAD.

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret [Show](#)

Use Second Shared Secret [i](#)

Second Shared Secret [Show](#)

CoA Port **1700** [Set To Default](#)

RADIUS-instellingen

DUO-configuraties.

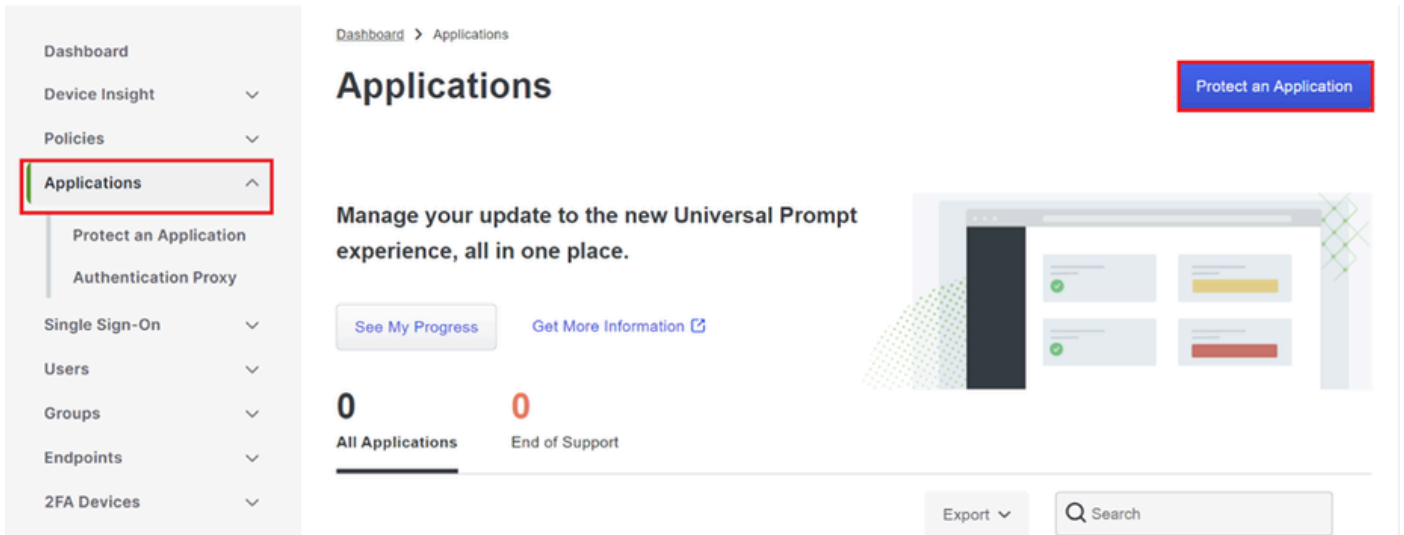
DUO Proxy-installatie.

Toegang tot de DUO Proxy Download en Installatie Gids door te klikken op de volgende link:

<https://duo.com/docs/authproxy-reference>

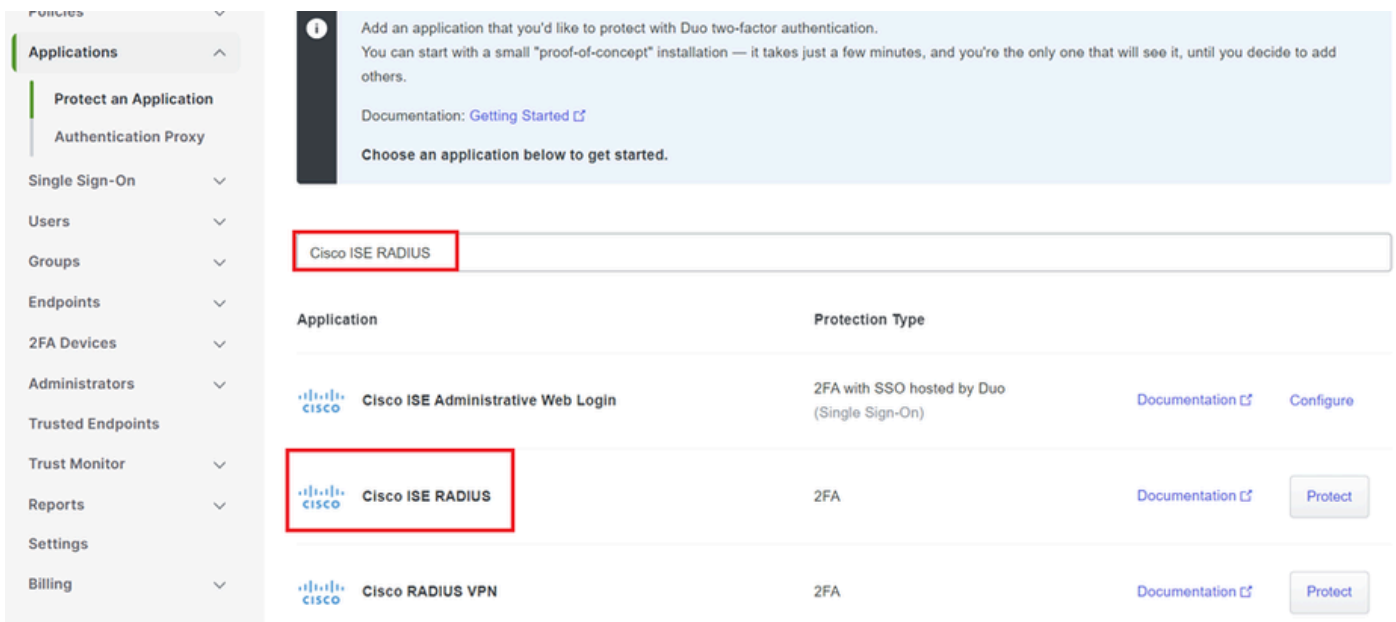
Integreren DUO Proxy met ISE en DUO Cloud.

1. Log in op de DUO Security website op <https://duo.com/> met behulp van uw referenties.
2. Navigeer naar het gedeelte Toepassingen en selecteer Bescherm een toepassing om door te gaan.



DUO-toepassingen

3. Zoek naar de "Cisco ISE RADIUS"-optie in de lijst en klik op Protect om deze aan uw toepassingen toe te voegen.



ISE-RADIUS-optie

4. Als de toevoeging succesvol is, zult u de details van de DUO-applicatie zien. Blader naar beneden en klik op Opslaan.

5. Kopieer de meegeleverde integratiesleutel, geheime sleutel en API hostname; deze zijn cruciaal voor de komende stappen.



Application modified successfully.

[Dashboard](#) > [Applications](#) > Cisco ISE RADIUS

Cisco ISE RADIUS

[Authentication Log](#) | [Remove Application](#)

Follow the [Cisco ISE RADIUS instructions](#).

Details

[Reset Secret Key](#)

Integration key

DIX [redacted] [Copy](#)

Secret key

.....ywLM [Copy](#)

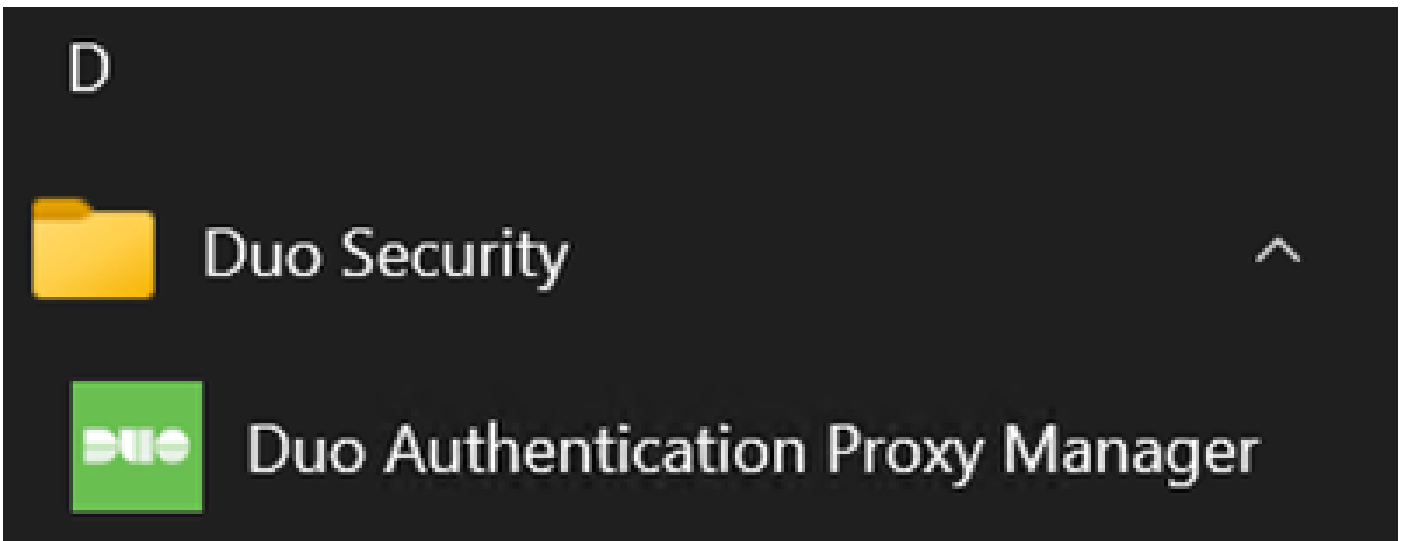
Don't write down your secret key or share it with anyone.

API hostname

[redacted] duosecurity.com [Copy](#)

ISE-servergegevens

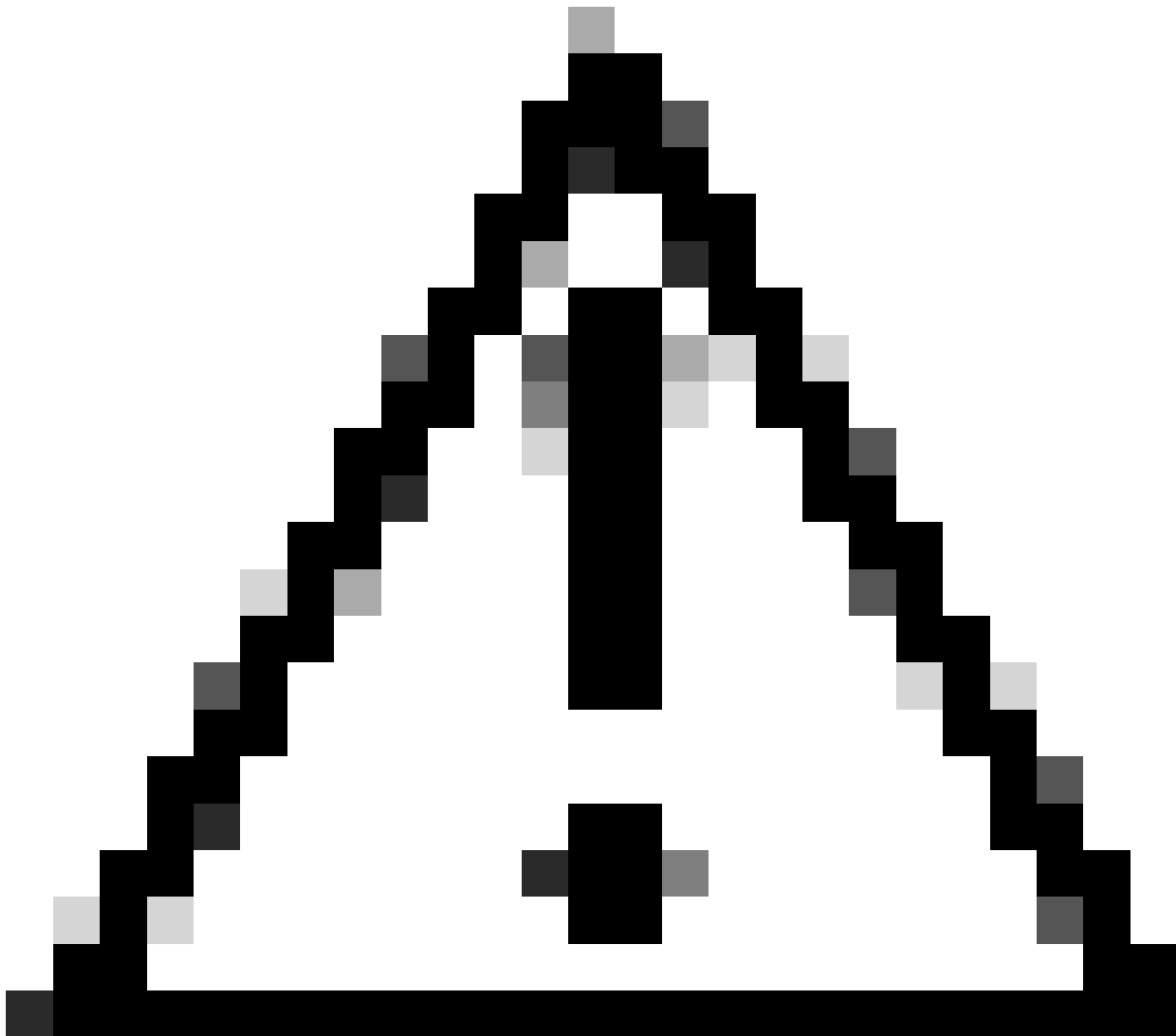
6. Start de DUO Proxy Manager op uw systeem om door te gaan met de setup.



DUO Proxy Manager

7. (Optioneel) Als uw DUO Proxy Server een proxy-configuratie nodig heeft om verbinding te maken met de DUO Cloud, voert u de volgende parameters in:

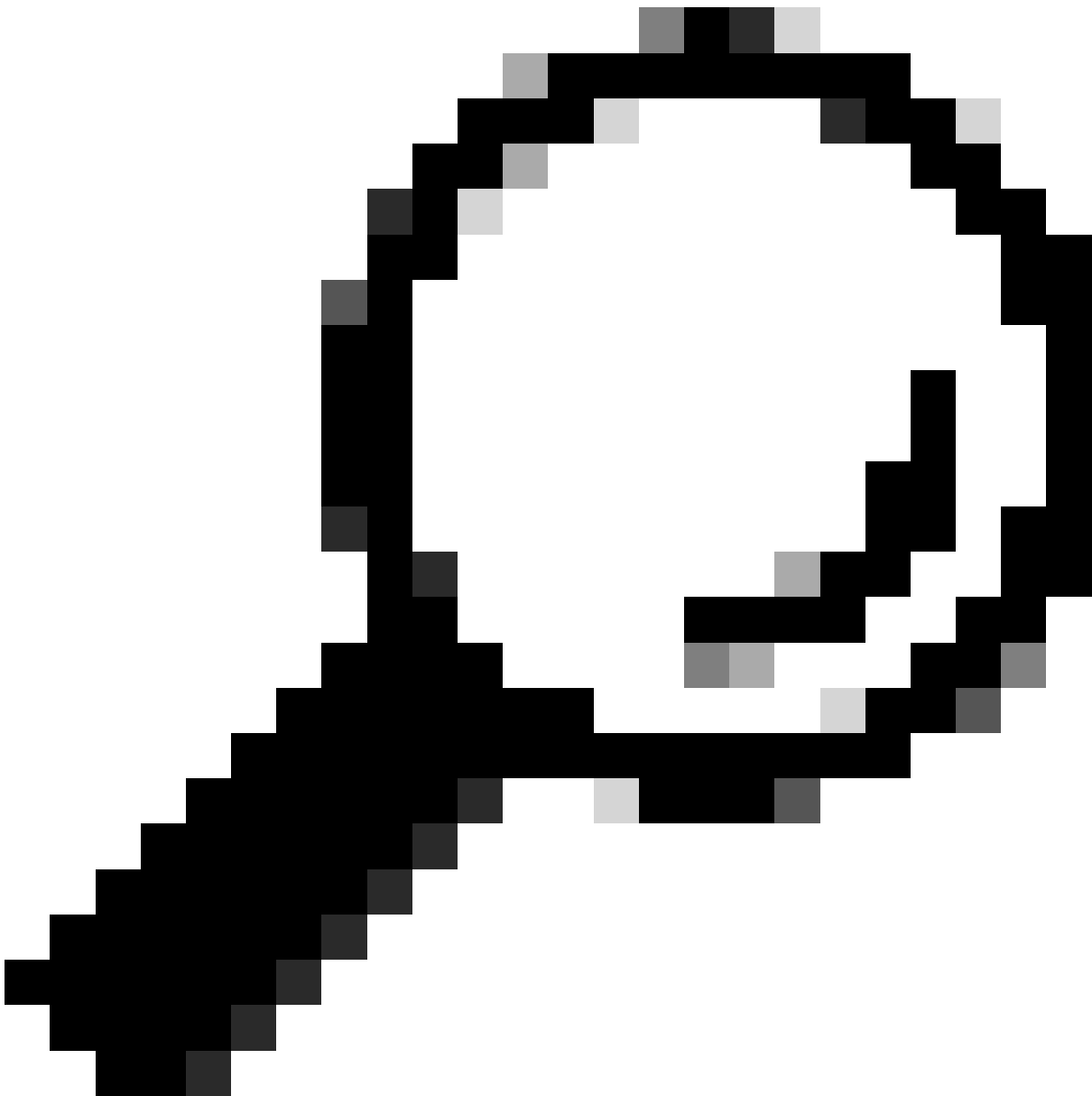
```
[main]
http_proxy_host=<Proxy IP Address or FQDN >
http_proxy_port=<port>
```



Waarschuwing: Zorg ervoor dat u vervangt en met uw daadwerkelijke volmachtsdetails.

8. Gebruik nu de informatie die u eerder hebt gekopieerd om de integratieconfiguratie te voltooien.

```
[radius_server_auto]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
radius_ip_1=<ISE IP address>
radius_secret_1=<secret key configured in the external RADIUS server section>
failmode=safe
port=1812
client=ad_client
```



Tip: De lijn `client=ad_client` is een indicatie dat de DUO Proxy authenticceert met behulp van een Active Directory-account. Zorg ervoor dat deze informatie correct is om de synchronisatie met de Active Directory te voltooien.

Integreren DUO met Active Directory.

1. Integreer de DUO-verificatieproxy met uw Active Directory.

```
[ad_client]
host=<AD IP Address>
service_account_username=<service_account_username>
service_account_password=<service_account_password>
search_dn=DC=<domain>,DC=<TLD>
```

2. Sluit je aan bij je Active Directory met DUO cloud services. Log in op <https://duo.com/>.

3. Navigeer naar "Gebruikers" en selecteer "Directory Sync" om de synchronisatie-instellingen te beheren.

Dashboard > Users

Users

Directory Sync | Import Users | Bulk Enroll Users | Add User

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

0	0	0	0	0	0
Total Users	Not Enrolled	Inactive Users	Trash	Bypass Users	Locked Out

Select (0) ... Export Search

No users shown based on your search.

Directory-sync

4. Klik op "Add New Sync" en kies "Active Directory" in de geboden opties.

Dashboard > Users > Directory Sync

Directory Sync

Add New Sync

Directory Syncs | Connections

You don't have any directories yet.

Nieuwe sync toevoegen

5. Selecteer Nieuwe verbinding toevoegen en klik op Doorgaan.

Dashboard > Users > Directory_Sync > New Active Directory Sync

New Active Directory Sync

Connection
Set up a new connection using a new Authentication Proxy.

Reuse existing connection
 Add new connection
 You will be redirected to a new page

[Continue](#)

Directory Sync Setup

Waiting for connection to directory

Sync setup is disabled until a connection to the directory has been established.

Directory Sync Setup

- Connect to AD
- Add groups
- Review synced attributes

[Complete Setup](#)

Nieuwe Active Directory toevoegen

6. Kopieer de gegenereerde integratiesleutel, geheime sleutel en API-hostnaam.

Authentication Proxy

[Delete Connection](#) [No Changes](#)

Configuration metadata

- To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#)
- Configure your Authentication Proxy. Update the `ikey`, `skey`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).
- If you are using NTLM or plain authentication, update the `[cloud]` section of your configuration with the username and password for the LDAP account that has read access for your LDAP directory.

Integration key [Copy](#)

Secret key [Copy](#)

Don't write down your secret key or share it with anyone.

[Reset Secret Key](#)

API hostname [Copy](#)

Status

Not connected

- Add Authentication Proxy
- Configure Directory

Connected Directory Syncs

User Syncs

[AD Sync](#)

Details van verificatieproxy

7. Ga terug naar de configuratie van de DUO-verificatieproxy en configureer de sectie `[cloud]` met de nieuwe parameters die u hebt verkregen, evenals de referenties van de serviceaccount voor een Active Directory-beheerder:

```
[cloud]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
service_account_username=<your domain>\<service_account_username>
service_account_password=<service_account_password>
```


8. Valideer uw configuratie door de optie "valideren" te selecteren om er zeker van te zijn dat alle instellingen correct zijn.

```
1 [main]
2 http_proxy_host=cx[redacted]
3 http_proxy_port=3128
4
5 [radius_server_auto]
6 ikey=DIX[redacted]
7 skey=[redacted]uXWYwLM
8 api_host=a[redacted].duosecurity.com
9 radius_ip_1=10.4.23.21
10 radius_secret_1=po[redacted]
11 failmode=safe
12 port=1812
13 client=ad_client
14
15 [ad_client]
16 host=10.4.23.42
17 service_account_username=administrator
18 service_account_password=[redacted]
```

Configuratie van Proxy DUO.

9. Na validatie slaat u uw configuratie op en start u de DUO-verificatieproxy opnieuw om wijzigingen toe te passen.

```
Running The Duo Authentication Proxy Connectivity Tool. This may take
several minutes...
[info] Testing section 'main' with configuration:
[info] {'http_proxy_host': 'cx[redacted]',
'http_proxy_port': '3128'}
[info] There are no configuration problems
[info]
[info] Testing section 'radius_server_auto' with configuration:
[info] {'api_host': '[redacted].duosecurity.com',
'client': 'ad_client',
'failmode': 'safe',
'http_proxy_host': '[redacted]',
'http_proxy_port': '3128',
'key': 'DIX[redacted]'}
```

Serviceoptie opnieuw starten.

10. Terug in het DUO-beheerdashboard, voer het IP-adres van uw Active Directory-server in samen met de Base-DN voor gebruikerssynchronisatie.

Directory Configuration

Domain controller(s)

Hostname or IP address (1) *

10.4.23.42

Port (1) *

389

[+ Add Domain controller](#)

The port is typically 389 for cleartext LDAP or STARTTLS, and 636 for LDAPS.

Base DN *

DC=testlab,DC=local

Enter the full distinguished name (DN) of the directory location to search for users and groups. We recommend setting this to the directory root (example: DC=domain,DC=local). If specifying the DN of an OU or container, ensure it is **above both the users and groups to sync**.

Directory-instellingen.

1. Selecteer de optie Laagbaar maken om het systeem te configureren voor niet-NTLMv2-verificatie.

Authentication type



Integrated

Performs Windows authentication from a domain-joined system.



NTLMv2

Performs Windows NTLMv2 authentication.



Plain

Performs username-password authentication.

Type verificatie.

12. Sla uw nieuwe instellingen op om er zeker van te zijn dat de configuratie wordt bijgewerkt.

 Delete Connection

Save

Status

Not connected

Add Authentication Proxy



Configure Directory

Connected Directory Syncs

User Syncs

[AD Sync](#)

Opslaan, optie

13. Gebruik de "testverbinding"-functie om te verifiëren dat de DUO Cloud-service kan

communiceren met uw Active Directory.

Authentication Proxy

1. To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#)
2. Configure your Authentication Proxy. Update the `key`, `secret_key`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).

Integration key [Copy](#)

Secret key [Copy](#)

Don't write down your secret key or share it with anyone.

[Reset Secret Key](#)

API hostname [Copy](#)

3. If you are using NTLM or plain authentication, update the `[cloud]` section of your configuration with the username and password for the LDAP account that has read access for your LDAP directory.

```
service_account_username=myusername  
service_account_password=mypassword
```

4. Restart your Authentication Proxy.

5. [Test Connection](#).

Verbindingsoptie testen.

14. Bevestig dat de status van de Active Directory wordt weergegeven als "Connected", wat wijst op een geslaagde integratie.

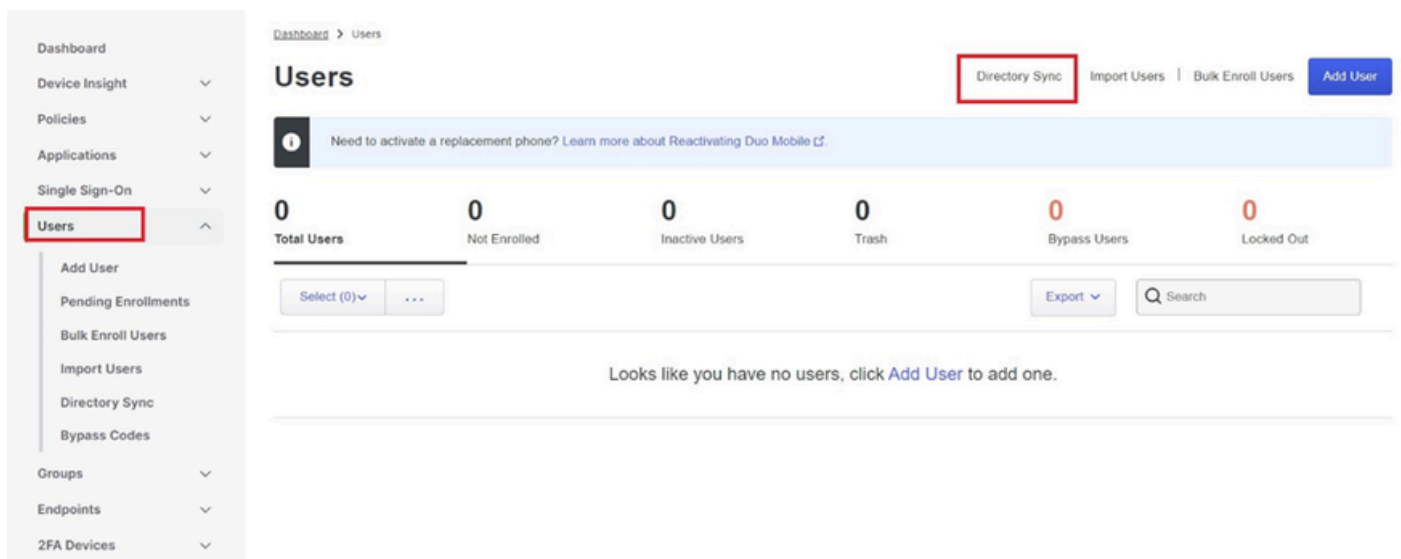
Status

Connected

Status geslaagd.

Exporteer gebruikersaccounts vanuit Active Directory (AD) via DUO Cloud.

1. Navigeer naar Gebruikers > Directory Sync binnen het Duo Admin Panel om de instellingen te vinden die betrekking hebben op directory synchronisatie met Active Directory.

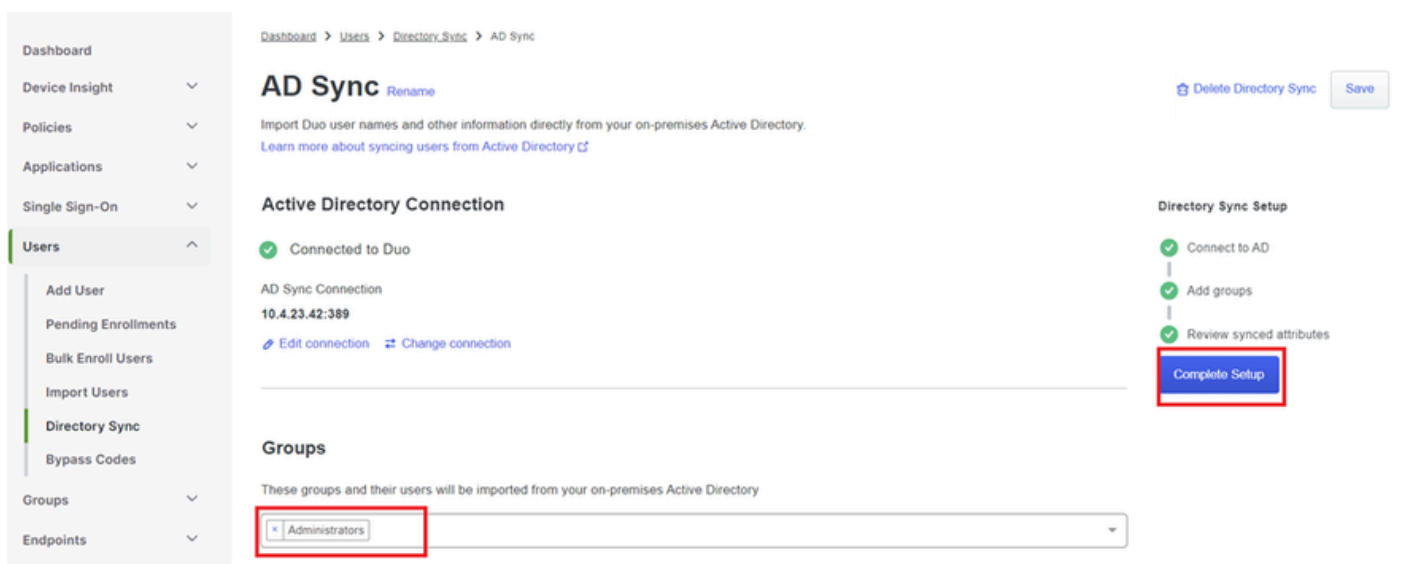


Gebruikerslijst.

2. Selecteer de Active Directory-configuratie die u wilt beheren.

3. Identificeer en kies binnen de configuratie-instellingen de specifieke groepen in Active Directory die u wilt synchroniseren met de Duo Cloud. Overweeg de filteropties voor uw selectie te gebruiken.

4. Klik op Complete Setup.



AD Sync.

5. Klik op Nu synchroniseren om de synchronisatie te starten. Dit exporteert de gebruikersaccounts van de opgegeven groepen in Active Directory naar de Duo Cloud, zodat ze kunnen worden beheerd binnen de Duo Security omgeving.

AD Sync Rename

Delete Directory Sync No Changes

Import Duo user names and other information directly from your on-premises Active Directory.
[Learn more about syncing users from Active Directory](#)

Sync Controls

Sync status

Scheduled to automatically synchronize every 12 hours, next around 2:00 AM UTC [Pause automatic syncs](#)

Sync Now

Troubleshooting ▼

Active Directory Connection

✓ Connected to Duo

AD Sync Connection

10.4.23.42:389

[Edit connection](#)

[Change connection](#)

Startsynchronisatie

Gebruikers inschrijven in de Cisco DUO Cloud.

Door gebruikers in te schrijven, kan identiteit worden geverifieerd via verschillende methoden, zoals code toegang, DUO push, SMS codes en tokens.

1. Navigeer naar de sectie Gebruikers in het Cisco Cloud-dashboard.
2. Zoek en selecteer de account van de gebruiker die u wilt inschrijven.

Dashboard > Users

Users Directory Sync | Import Users | Bulk Enroll Users [Add User](#)

1 Total Users **1** Not Enrolled **1** Inactive Users **0** Trash **0** Bypass Users **0** Locked Out

Select (0) ... Export

<input type="checkbox"/>	Username	Name	Email	Phones	Tokens	Status	Last Login
<input checked="" type="checkbox"/>	administrator		oteg [REDACTED]			Active	Never authenticated

1 total

Gebruikersaccountlijst.

3. Klik op de knop Email inschrijving verzenden om het inschrijvingsproces te starten.

administrator

Logs

Send Enrollment Email

Sync This User



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



This user was synced from the directory **AD Sync**. Some fields are read-only.

Username

administrator

Username aliases

[+ Add a username alias](#)

Users can have up to 8 aliases.

Optionally, you may choose to reserve using an alias number for a specific alias

(e.g., Username alias 1 should only be used for Employee ID).

Inschrijving via e-mail.

4. Controleer de e-mail inbox en open de inschrijvingsuitnodiging om het authenticatieproces te voltooien.

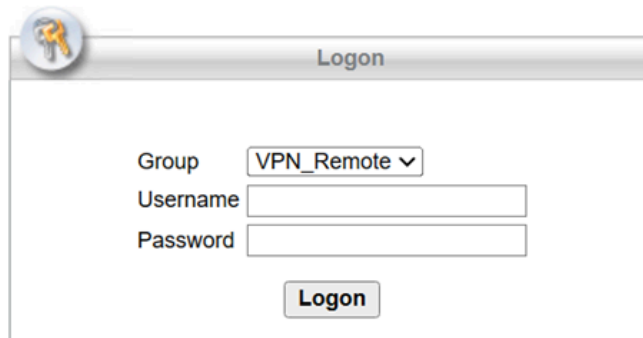
Voor extra details betreffende het inschrijvingsproces, gelieve te verwijzen naar deze middelen:

- Universele Inschrijvingsgids: <https://guide.duo.com/universal-enrollment>
- Traditionele inschrijvingsgids: <https://guide.duo.com/traditional-enrollment>

Configuratievalidatieprocedure.

Om ervoor te zorgen dat uw configuraties nauwkeurig en operationeel zijn, valideert u de volgende stappen:

1. Start een webbrowser en voer het IP-adres van het FTD-apparaat (Firepower Threat Defence) in om toegang te krijgen tot de VPN-interface.

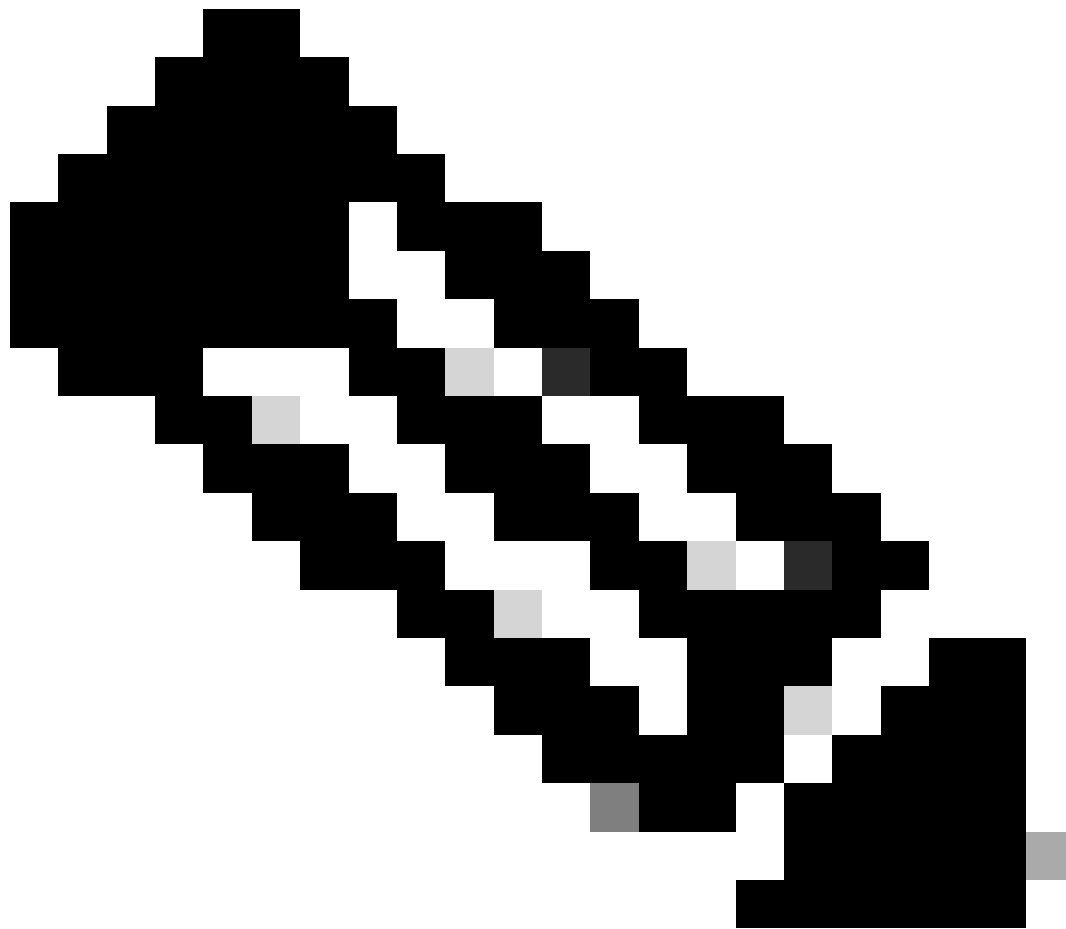


The screenshot shows a web browser window with a title bar that says "Logon". Inside the window, there is a form with the following elements:

- A "Group" label followed by a dropdown menu showing "VPN_Remote".
- A "Username" label followed by a text input field.
- A "Password" label followed by a text input field.
- A "Logon" button located below the input fields.

VPN-aanmelding.

2. Voer uw gebruikersnaam en wachtwoord in als hierom wordt gevraagd.



Opmerking: de referenties maken deel uit van de Active Directory-accounts.

3. Wanneer u een DUO Push-melding ontvangt, keurt u deze goed met behulp van de DUO Mobile-software om verder te gaan met het validatieproces.

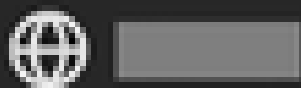


(1) Login request waiting.

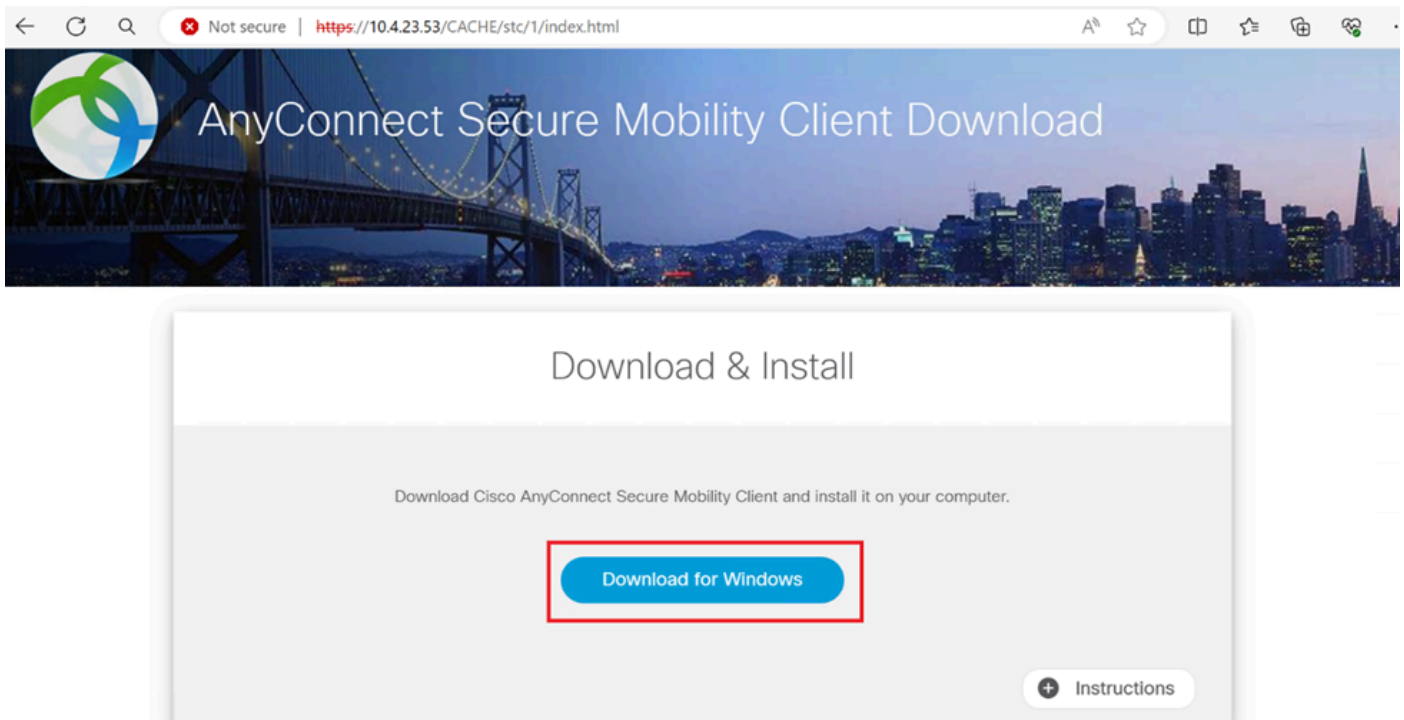
[Respond](#)



Are you logging in to Cisco ISE
RADIUS?



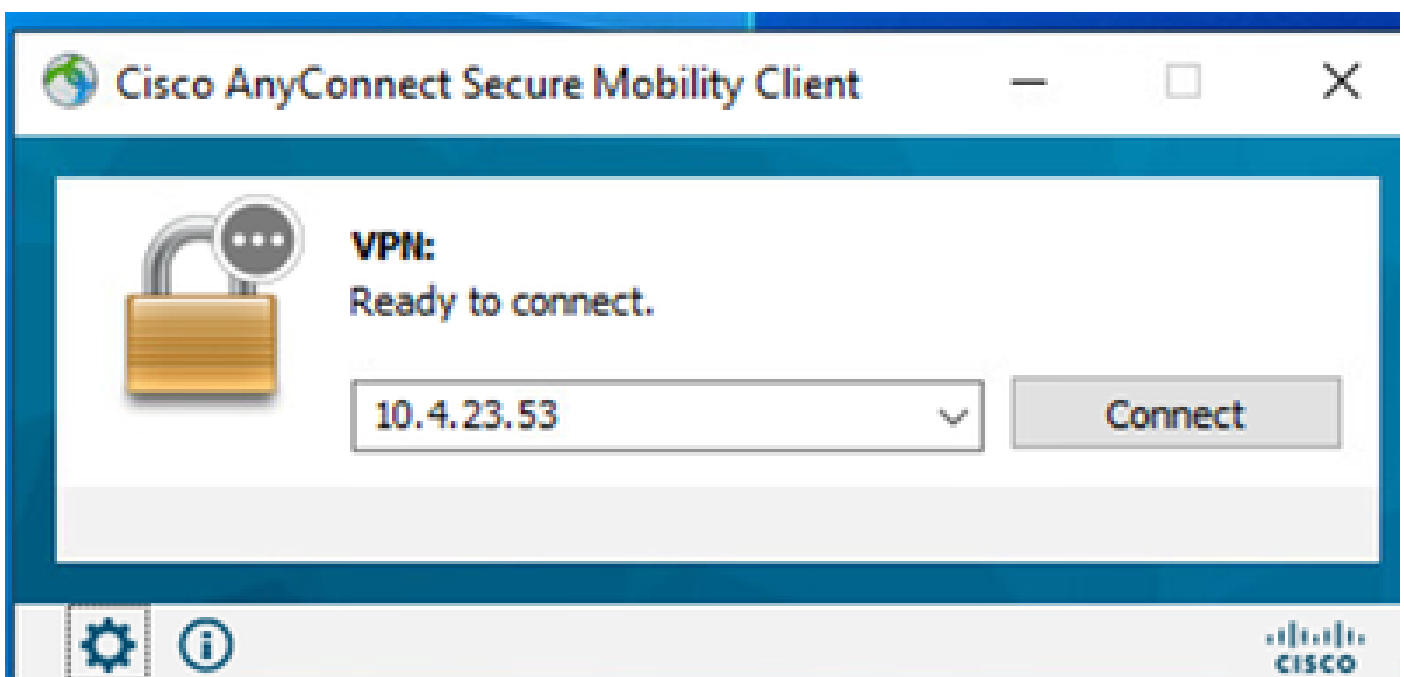
Zoek en download het Cisco AnyConnect VPN-clientpakket dat geschikt is voor Windows-systemen.



Downloaden en installeren.

5. Voer het gedownloadde AnyConnect-installatiebestand uit en ga verder met de instructies die het installatieprogramma op uw Windows-apparaat heeft gegeven.

6. Open de Cisco AnyConnect Secure Mobility-clientsoftware. Maak verbinding met VPN door het IP-adres van het FTD-apparaat in te voeren.



Any Connect-software.

7. Voer, wanneer hierom wordt gevraagd, uw VPN-toegangsreferenties in en autoriseer nogmaals

het DUO Push-bericht om uw verbinding te verifiëren.



(1) Login request waiting.

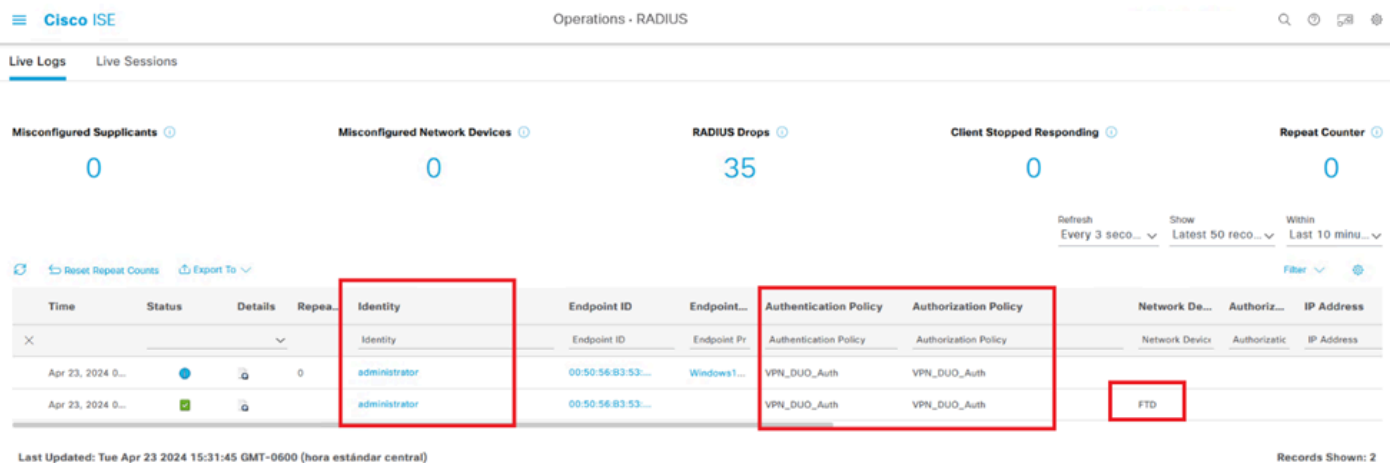
[Respond](#)



Are you logging in to Cisco ISE
RADIUS?

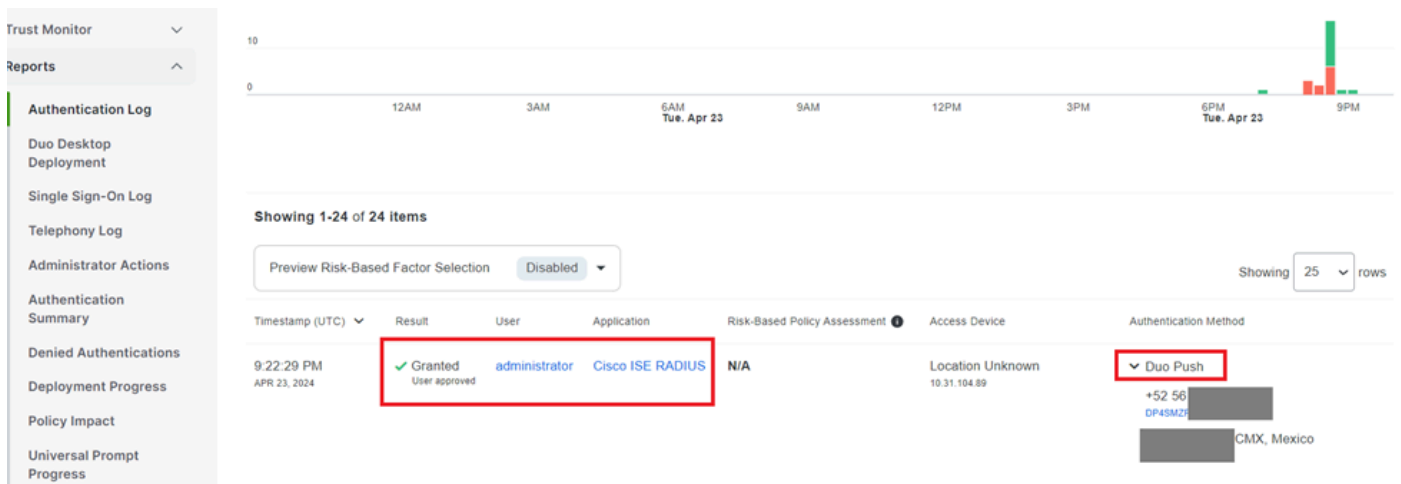


om realtime-activiteit te controleren en de juiste connectiviteit te verifiëren, toegang te krijgen tot de live logs in de Cisco Identity Services Engine (ISE).



De reddingsboei.

9. Ga naar Rapporten > Verificatielogboeken om de verificatielogboeken in het DUO Admin Panel te bekijken om te bevestigen dat de verificaties zijn geslaagd.



Verificatielogboeken.

Veelvoorkomende problemen.

Werkscenario.

Alvorens u specifieke fouten in verband met deze integratie onderzoekt, is het van cruciaal belang om het algemene werkscenario te begrijpen.

In de ISE-livelogs kunnen we bevestigen dat ISE de RADIUS-pakketten doorstuurde naar de DUO Proxy, en zodra de gebruiker de DUO Push accepteerde, werd de RADIUS Access Accept ontvangen van de DUO Proxy Server.

Overview

Event	5200 Authentication succeeded
Username	administrator
Endpoint Id	00:50:56:B3:53:D6
Endpoint Profile	
Authentication Policy	VPN_DUO_Auth
Authorization Policy	VPN_DUO_Auth
Authorization Result	

Authentication Details

Source Timestamp	2024-04-24 20:03:33.142
Received Timestamp	2024-04-24 20:03:33.142
Policy Server	asc-ise32p3-1300
Event	5200 Authentication succeeded
Username	administrator
Endpoint Id	00:50:56:B3:53:D6
Calling Station Id	10.31.104.89
Audit Session Id	000000000002e000662965a9
Network Device	FTD

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Network Access.NetworkDeviceName
- 11358 Received request for RADIUS server sequence.
- 11361 Valid incoming authentication request
- 11355 Start forwarding request to remote RADIUS server
- 11365 Modify attributes before sending request to external radius server
- 11100 RADIUS-Client about to send request - (port = 1812)
- 11101 RADIUS-Client received response (Step latency=5299 ms)
- 11357 Successfully forwarded request to current remote RADIUS server
- 11002 Returned RADIUS Access-Accept

Successverificatie.

CiscoAVPair

```
mdm-tlv=device-platform=win,  
mdm-tlv=device-mac=00-50-56-b3-53-d6,  
mdm-tlv=device-type=VMware, Inc. VMware7,1,  
mdm-tlv=device-platform-version=10.0.19045 ,  
mdm-tlv=device-public-mac=00-50-56-b3-53-d6,  
mdm-tlv=ac-user-agent=AnyConnect Windows 4.10.08029,  
mdm-tlv=device-uid-  
global=4CEBE2C21A8B81F490AC91086452CF3592593437,  
mdm-tlv=device-  
uid=3C5C68FF5FD3B6FA9D364DDB90E2B0BFA7E44B0EAAA  
CA383D5A8CE0964A799DD,  
audit-session-id=000000000002e000662965a9,  
ip:source-ip=10.31.104.89  
coa-push=true,  
proxy-flow=[10.4.23.53,10.4.23.21]
```

Result

Reply-Message Success. Logging you in...

Resultaat geslaagd.

Een pakketopname van de ISE-kant toont de volgende informatie:

Source	Destination	Protocol	Length	Info	
10.4.23.53	10.4.23.21	RADIUS	741	Access-Request id=138	→ The FTD sends the RADIUS request to ISE
10.4.23.21	10.31.126.207	RADIUS	883	Access-Request id=41	→ ISE resends the same RADIUS requests to the DUO Proxy
10.31.126.207	10.4.23.21	RADIUS	190	Access-Accept id=41	→ DUO Proxy sends the RADIUS accept (DUO push approved)
10.4.23.21	10.4.23.53	RADIUS	90	Access-Accept id=138	→ ISE resend the RADIUS accept to the FTD
10.4.23.53	10.4.23.21	RADIUS	739	Accounting-Request id=139	→ FTD sends the accounting for the current VPN connection
10.4.23.21	10.4.23.53	RADIUS	62	Accounting-Response id=139	→ ISE registered the accounting on its dashboard

ISE-pakketopname.

Fout11368 Controleer de logbestanden op de externe RADIUS-server om de precieze reden van de fout te bepalen.

Event	5400 Authentication failed
Failure Reason	11368 Please review logs on the External RADIUS Server to determine the precise failure reason.
Resolution	Please review logs on the External RADIUS Server to determine the precise failure reason.
Root cause	Please review logs on the External RADIUS Server to determine the precise failure reason.

Error 11368.

Probleemoplossing:

- Controleer of de RADIUS gedeelde geheime sleutel in ISE dezelfde is als de ingestelde sleutel in het VCC.

1. Open de ISE-GUI.
 2. Beheer > Netwerkbronnen > Netwerkapparaten.
 3. Kies de DUO Proxy Server.
 4. Klik naast het gedeelde geheim op "Weergeven" om de toets in onbewerkte tekst weer te geven.
 5. Open de GUI van het VCC.
 6. Objecten > Objectbeheer > AAA-server > RADIUS-servergroep.
 7. Kies de ISE-server.
 8. Voer de geheime sleutel opnieuw in.
- Controleer de Active Directory-integratie in DUO.

1. Open de DUO-verificatieproxy Manager.
2. Bevestig de gebruiker en het wachtwoord onder de sectie [ad_client].
3. Klik op Valideren om te bevestigen dat de huidige referenties correct zijn.

Fout 1353 Geen externe RADIUS-servers meer; kan geen failover uitvoeren

Event	5405 RADIUS Request dropped
Failure Reason	11353 No more external RADIUS servers; can't perform failover
Resolution	Verify the following: At least one of the remote RADIUS servers in the ISE proxy service is up and configured properly ; Shared secret specified in the ISE proxy service for every remote RADIUS server is same as the shared secret specified for the ISE server ; Port of every remote RADIUS server is properly specified in the ISE proxy service.
Root cause	Failover is not possible because no more external RADIUS servers are configured. Dropping the request.

Error 11353.

Probleemoplossing:

- Controleer of de RADIUS gedeelde geheime sleutel in ISE dezelfde is als de ingestelde sleutel in de DUO Proxy Server.

1. Open de ISE-GUI.
2. Beheer > Netwerkbronnen > Netwerkapparaten.
3. Kies de DUO Proxy Server.
4. Klik naast het gedeelde geheim op "Weergeven" om de toets in onbewerkte tekst weer te geven.
5. Open de DUO-verificatieproxy Manager.
6. Controleer de sectie [radius_server_auto] en vergelijk de gedeelde geheime sleutel.

De RADIUS-sessies worden niet weergegeven in de live ISE-logboeken.

Probleemoplossing:

- Controleer de DUO-configuratie.

1. Open de DUO-verificatieproxy Manager.

2. Controleer het ISE-IP-adres in het gedeelte [radius_server_auto]

- de configuratie van het VCC controleren.

1. Open de GUI van het VCC.

2. Ga naar Objecten > Objectbeheer > AAA-server > RADIUS-servergroep.

3. Kies de ISE-server.

4. Controleer het IP-adres van de ISE.

- Neem een pakket op in ISE om de ontvangst van de RADIUS-pakketten te bevestigen.

1. Ga naar Operations > Probleemoplossing > Diagnostische tools > TCP-pomp

Aanvullende probleemoplossing.

- Schakel de volgende componenten in het PSN in als debug:

Beleidsmachine

Prt-JNI

runtime-AAA

Voor verdere probleemoplossing in de DUO-verificatieproxy Manager, controleer dan de volgende link:

https://help.duo.com/s/article/1126?language=en_US

DUO Template.

U kunt de volgende sjabloon gebruiken om de configuratie in uw DUO Proxy Server te voltooien.

```
[main] <--- OPTIONAL
http_proxy_host=<Proxy IP address or FQDN>
http_proxy_port=<Proxy port>
[radius_server_auto]
ikey=xxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=xxxxxxxxxxxxxxxxxxxxxxxx
radius_ip_1=<PSN IP Address>
radius_secret_1=xxxxxxxxxx
failmode=safe
port=1812
client=ad_client
```

```
[ad_client]
host=<AD IP Address>
service_account_username=xxxxxxxx
```

service_account_password=xxxxxxxxxx
search_dn=DC=xxxxxx,DC=xxxx

[cloud]

apikey=xxxxxxxxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=xxxxxxxxxxxxxxxxxxxxxx
service_account_username=<your domain\username>
service_account_password=xxxxxxxxxxxx

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.