Integreer Duo SAML SSO met AnyConnect Secure Remote Access via ISE-poortadapter

Inhoud

Inleiding

Dit document beschrijft een configuratievoorbeeld voor het integreren van Duo SAML SSO met Adaptive Security Appliance (ASA) en Cisco AnyConnect Secure Mobility Client-toegang die gebruikmaakt van Cisco ISE voor een gedetailleerde postenbeoordeling. Duo SAML SSO wordt geïmplementeerd met behulp van Duo Access Gateway (DAG), die communiceert met de Active Directory voor eerste gebruikersverificatie en vervolgens communiceert met Duo Security (Cloud) voor multi-factor verificatie. Cisco ISE wordt gebruikt als een autorisatieserver voor het leveren van endpointverificatie met behulp van postenbeoordeling.

Bijgedragen door Dinesh Moudgil en Pulkit Saxena, Cisco HTTS Engineer.

Voorwaarden

Vereisten

In dit document wordt ervan uitgegaan dat de ASA volledig operationeel en geconfigureerd is zodat de Cisco Adaptive Security Device Manager (ASDM) of opdrachtregelinterface (CLI)

configuratiewijzigingen kan doorvoeren.

Cisco raadt kennis van de volgende onderwerpen aan:

- Fundamentele bepalingen voor Duo Access Gateway en Duo Security
- Basiskennis van de configuratie van VPN voor externe toegang op de ASA
- Basiskennis van ISE en posterijen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

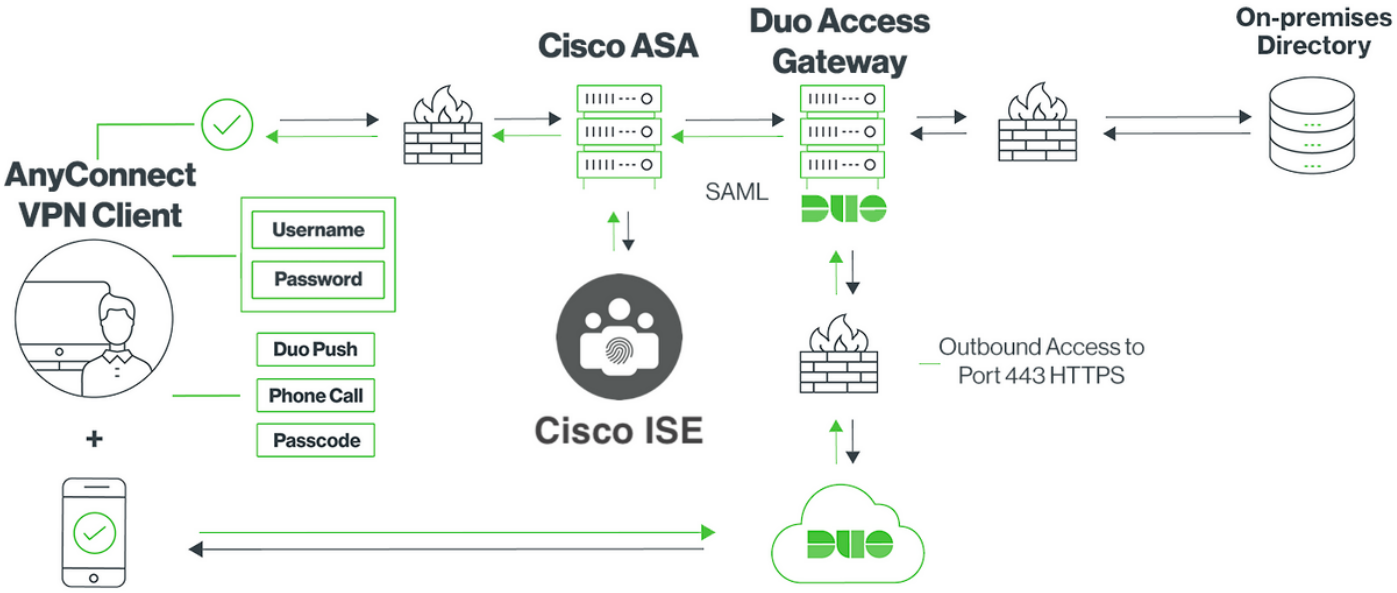
- Software voor Cisco adaptieve security applicatie, versie 9.12(3)12
- Duo Access Gateway
- Duo Security
- Cisco Identity Services Engine versie 2.6 en hoger
- Microsoft Windows 10 met AnyConnect versie 4.8.03052

Opmerking: AnyConnect Embedded Browser, gebruikt in deze implementatie, vereist ASA op 9.7(1)24, 9.8(2)28, 9.9(2)1 of hogere versie van elke release en AnyConnect versie 4.6 of hoger.

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 de potentiële impact van elke opdracht begrijpen.

Configureren

Netwerkdiagram



Traffic Flow

1. AnyConnect-client start een SSL VPN-verbinding met Cisco ASA
2. Cisco ASA, geconfigureerd voor primaire verificatie met Duo Access Gateway (DAG), leidt de ingesloten browser in AnyConnect-client om naar DAG voor SAML-verificatie
3. AnyConnect-client wordt omgeleid naar Duo Access Gateway
4. Zodra de AnyConnect-client de referenties invoert, wordt een SAML-verificatieaanvraag gebouwd en gegenereerd vanuit Cisco ASA naar Duo Access Gateway
5. Duo Access Gateway maakt gebruik van de integratie met on-site actieve directory om primaire verificatie uit te voeren voor de AnyConnect-client
6. Zodra de primaire verificatie is geslaagd, stuurt Duo Access Gateway een verzoek naar Duo Security over TCP-poort 443 om te beginnen met verificatie met twee factoren
7. De AnyConnect-client heeft een "Duo Interactive Prompt" weergegeven en de gebruiker voltooit de Duo-verificatie met twee factoren met de voorkeursmethode (push- of wachtcode)
8. Duo Security ontvangt een authenticatiereactie en retourneert de informatie naar de Duo Access Gateway
9. Op basis van de verificatiereactie maakt Duo Access Gateway een SAML-verificatiereactie die SAML-bewering bevat en reageert op de AnyConnect-client
10. AnyConnect-client geverifieerd voor SSL VPN-verbinding met Cisco ASA
11. Zodra de verificatie is geslaagd, stuurt Cisco ASA een autorisatieverzoek naar Cisco ISE

> Opmerking: Cisco ISE is alleen geconfigureerd voor autorisatie omdat Duo Access Gateway de benodigde verificatie biedt

12. Cisco ISE verwerkt het autorisatieverzoek en aangezien de status van de clientpositie onbekend is, wordt Posture via Cisco ASA omgeleid naar de beperkte toegang tot AnyConnect-client

13. Als AnyConnect-client geen compliancemodule heeft, wordt het gevraagd om deze te downloaden om verder te gaan met de beoordeling van de houding

14. Als AnyConnect-client is uitgerust met een nalevingsmodule, wordt een TLS-verbinding met Cisco ASA tot stand gebracht en wordt de stroom gestart

15. Afhankelijk van de postuur-omstandigheden die op ISE zijn geconfigureerd, worden postuur-controles uitgevoerd en details van AnyConnect-client naar Cisco ISE verzonden

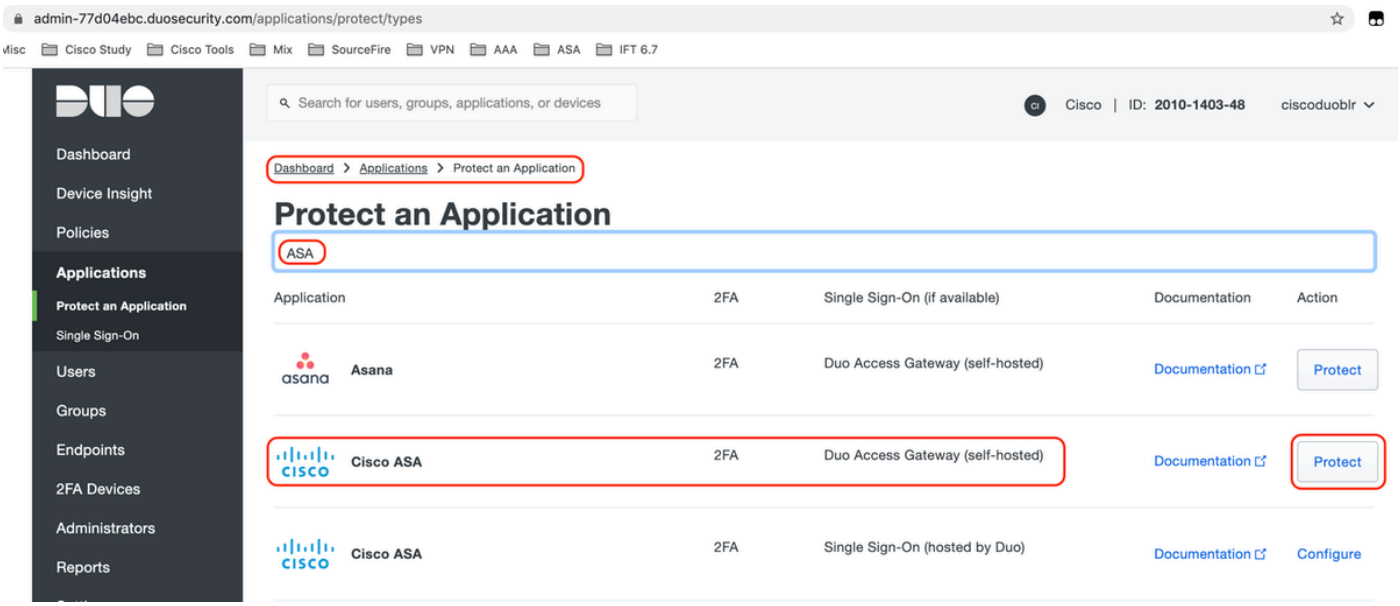
16. Als de status van de clienthouding verandert van Onbekend in conform, wordt het verzoek tot wijziging van de autorisatie (CoA) verzonden van Cisco ISE naar Cisco ASA om volledige toegang tot de client te verlenen en is VPN volledig geïnstalleerd

Configuraties

- Configuratie Duo Admin Portal

In deze sectie configureer je de ASA applicatie op de Duo Admin Portal.

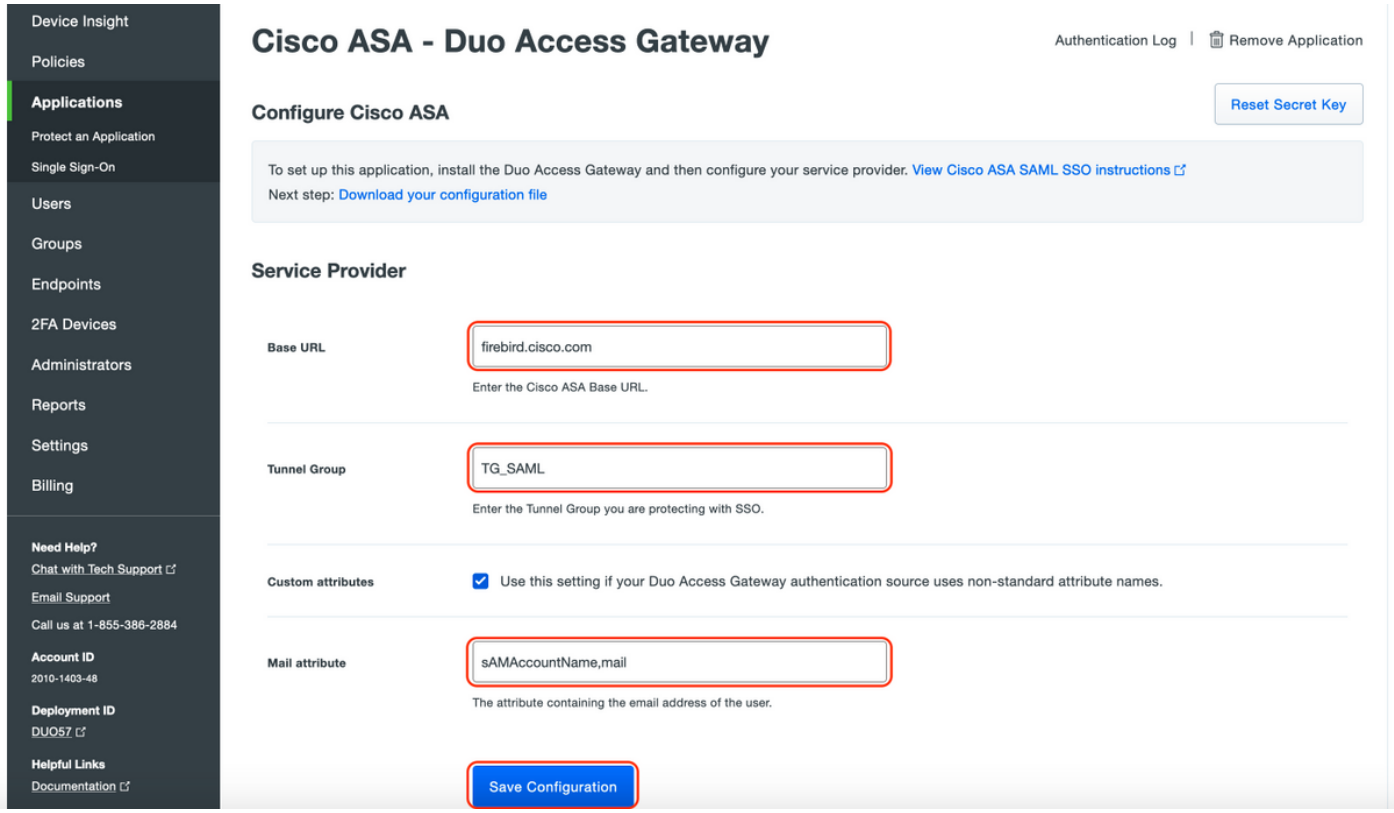
1. Log in op "Duo Admin Portal" en navigeer naar "Toepassingen > Bescherm een Toepassing", en zoek naar "ASA" met het beschermingstype "2FA met Duo Access Gateway, zelf-gehost". Klik op "Protect" uiterst rechts om Cisco ASA te configureren



2. Configureer de volgende kenmerken onder "Serviceprovider" voor de beschermde toepassing, ASA

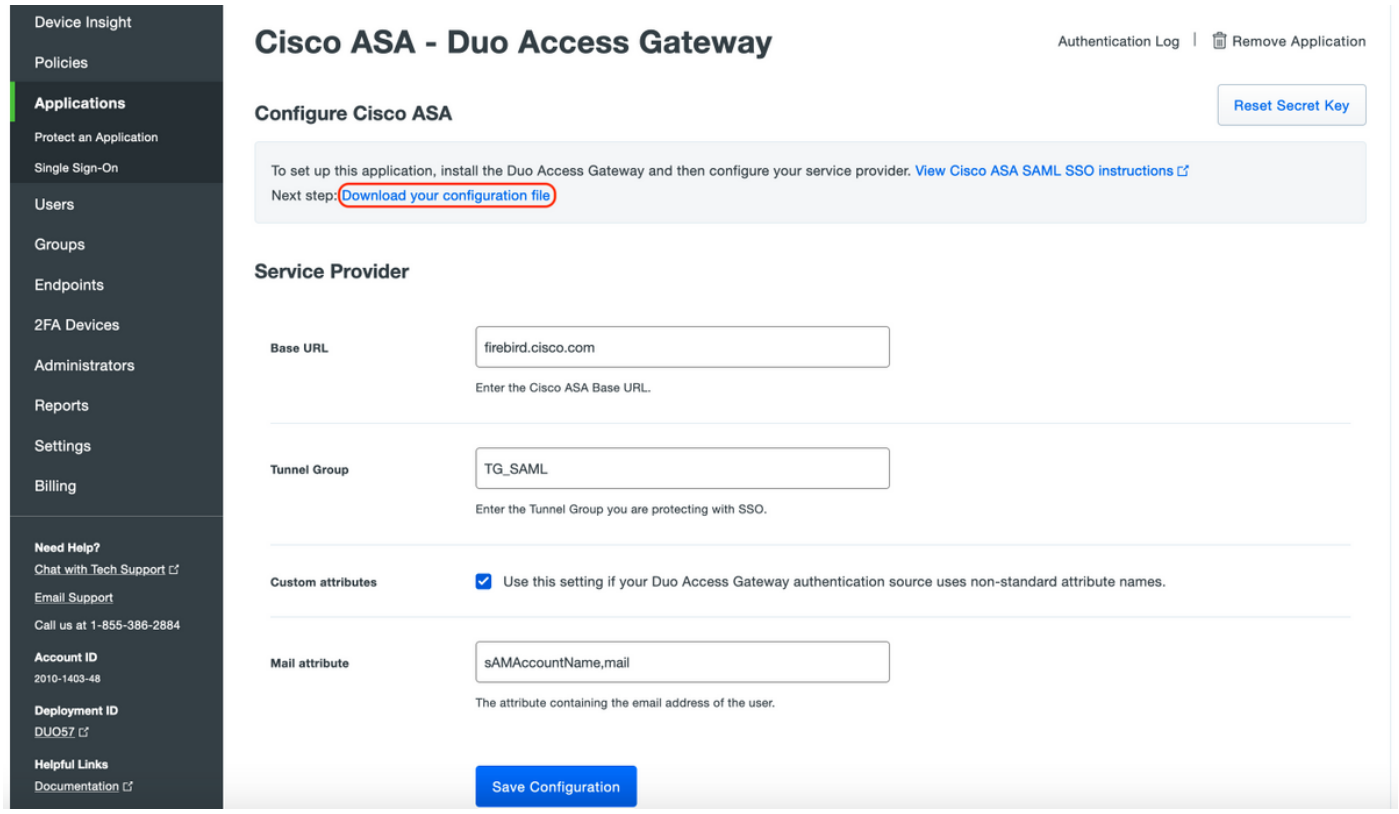
Basis-URL	firebird.cisco.com
Tunnelgroep	TG_SAML
E-mailkenmerk	Accountnaam, e-mail

Klik op "Opslaan" onderaan de pagina

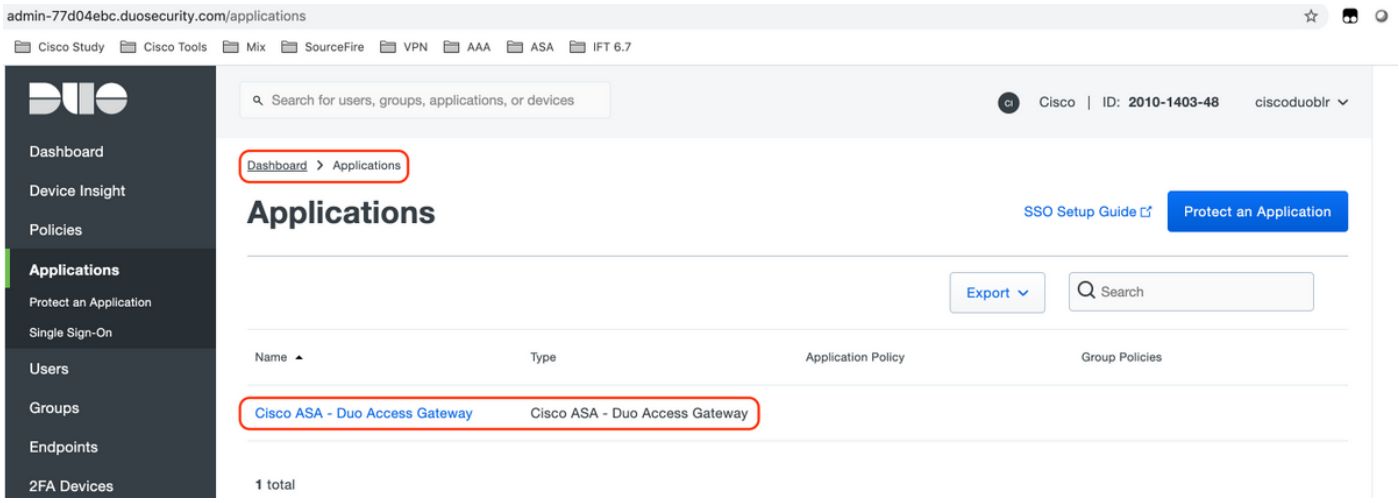


In dit document worden voor de rest van de configuratie standaardparameters gebruikt, maar deze kunnen worden ingesteld op basis van de vereisten van de klant.
Er kunnen op dit moment extra instellingen worden aangepast voor de nieuwe SAML-toepassing, zoals het wijzigen van de naam van de toepassing van de standaardwaarde, het inschakelen van zelfbediening of het toewijzen van een groepsbeleid.

3. Klik op de koppeling "Download your Configuration file" om de Cisco ASA-toepassingsinstellingen te verkrijgen (als JSON-bestand). Dit bestand wordt in latere stappen naar Duo Access Gateway geüpload

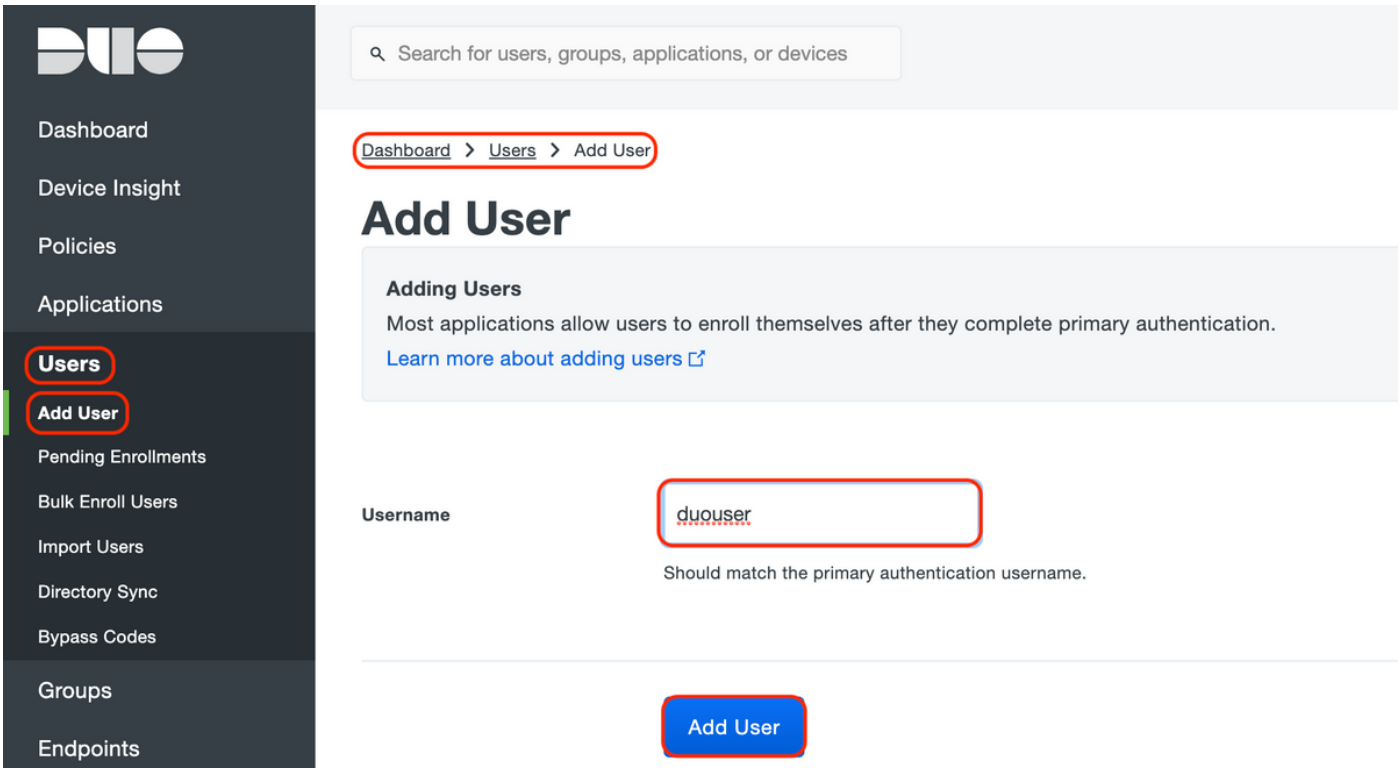


4. Onder "Dashboard > Toepassingen" ziet de nieuwe ASA-toepassing eruit zoals in de onderstaande afbeelding:

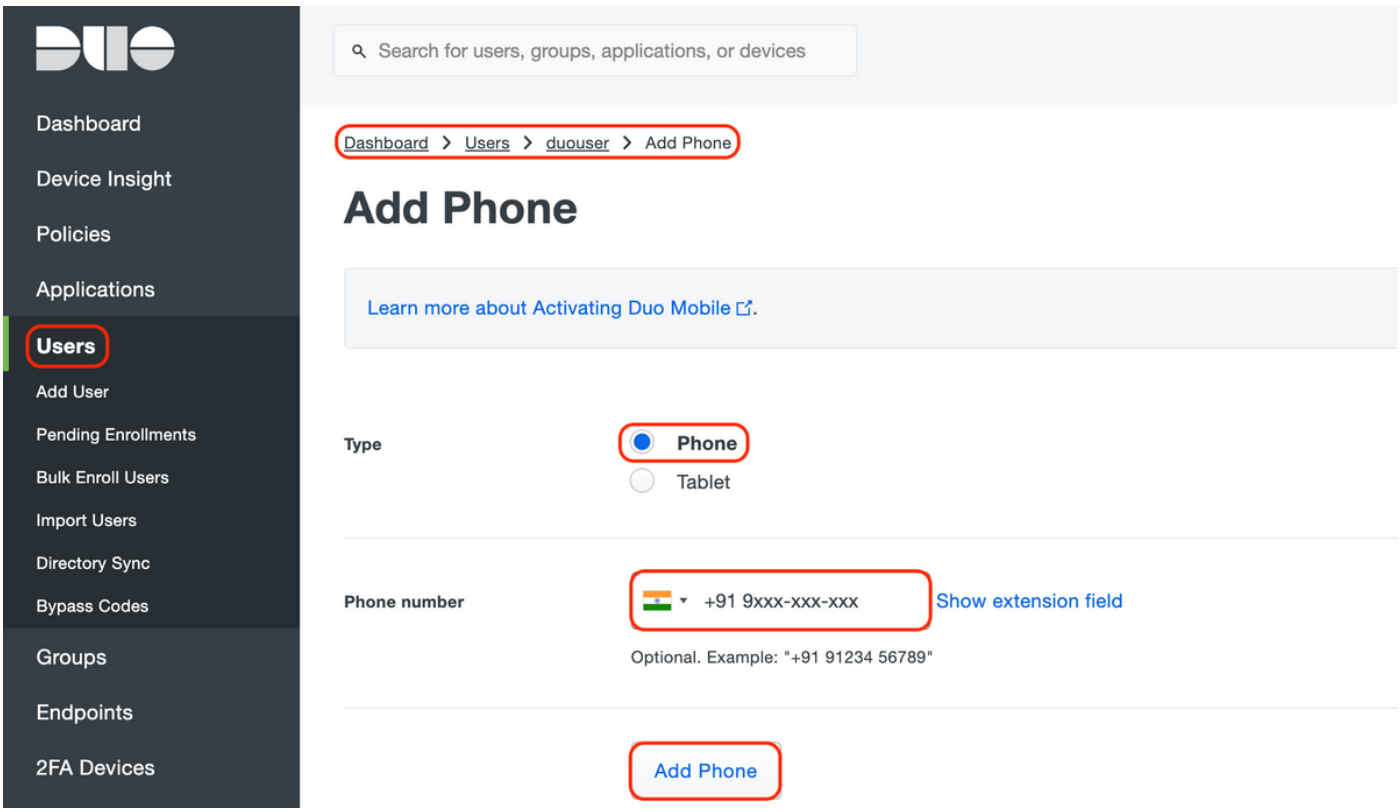


5. Navigeer naar "Gebruikers > Gebruiker toevoegen" zoals in de afbeelding:

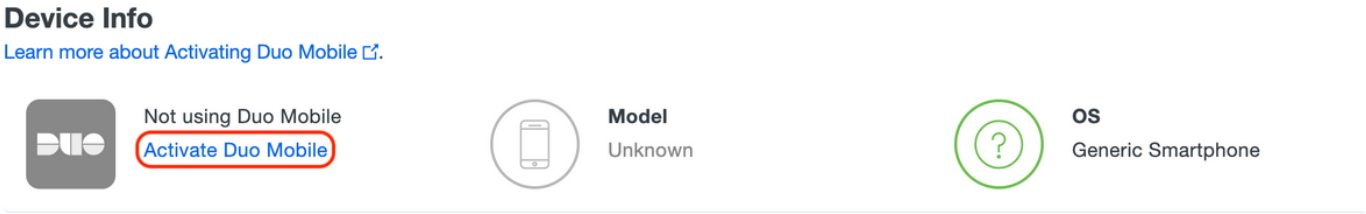
Maak een gebruiker met de naam "DuoSer" aan voor AnyConnect Remote Access-verificatie en activeer Duo Mobile op het eindgebruikerapparaat



Als u het telefoonnummer wilt toevoegen zoals in de afbeelding, selecteert u de optie "Telefoon toevoegen".

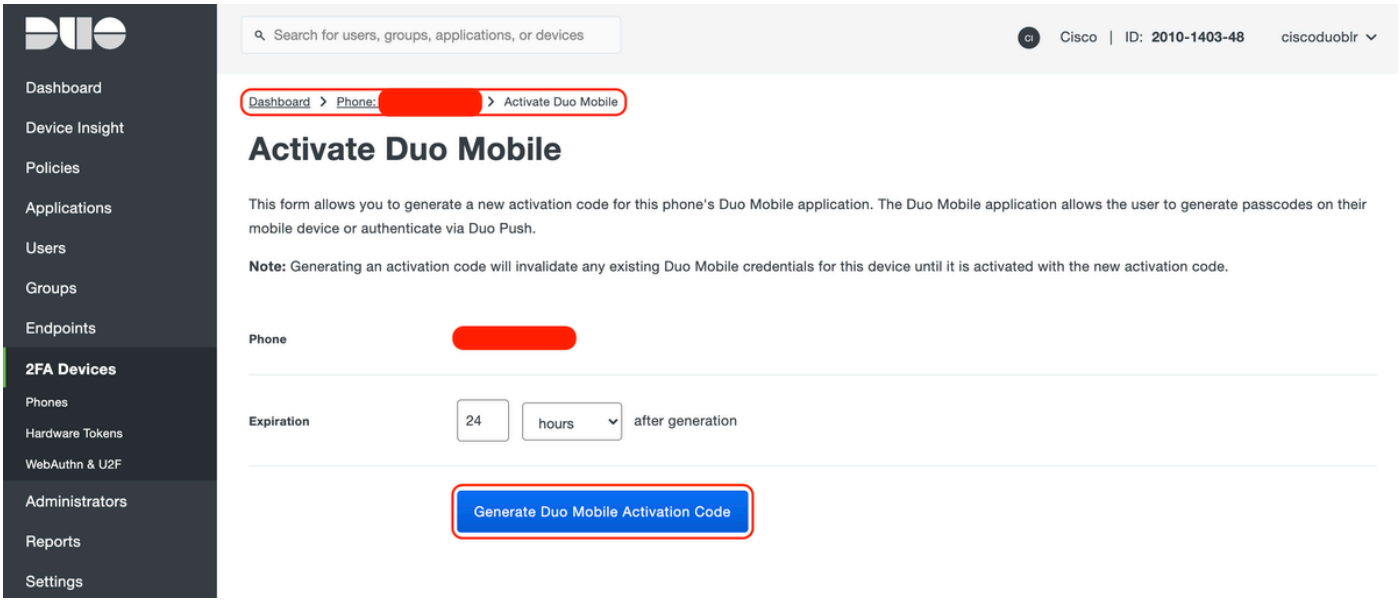


Activeer "Duo Mobile" voor de specifieke gebruiker

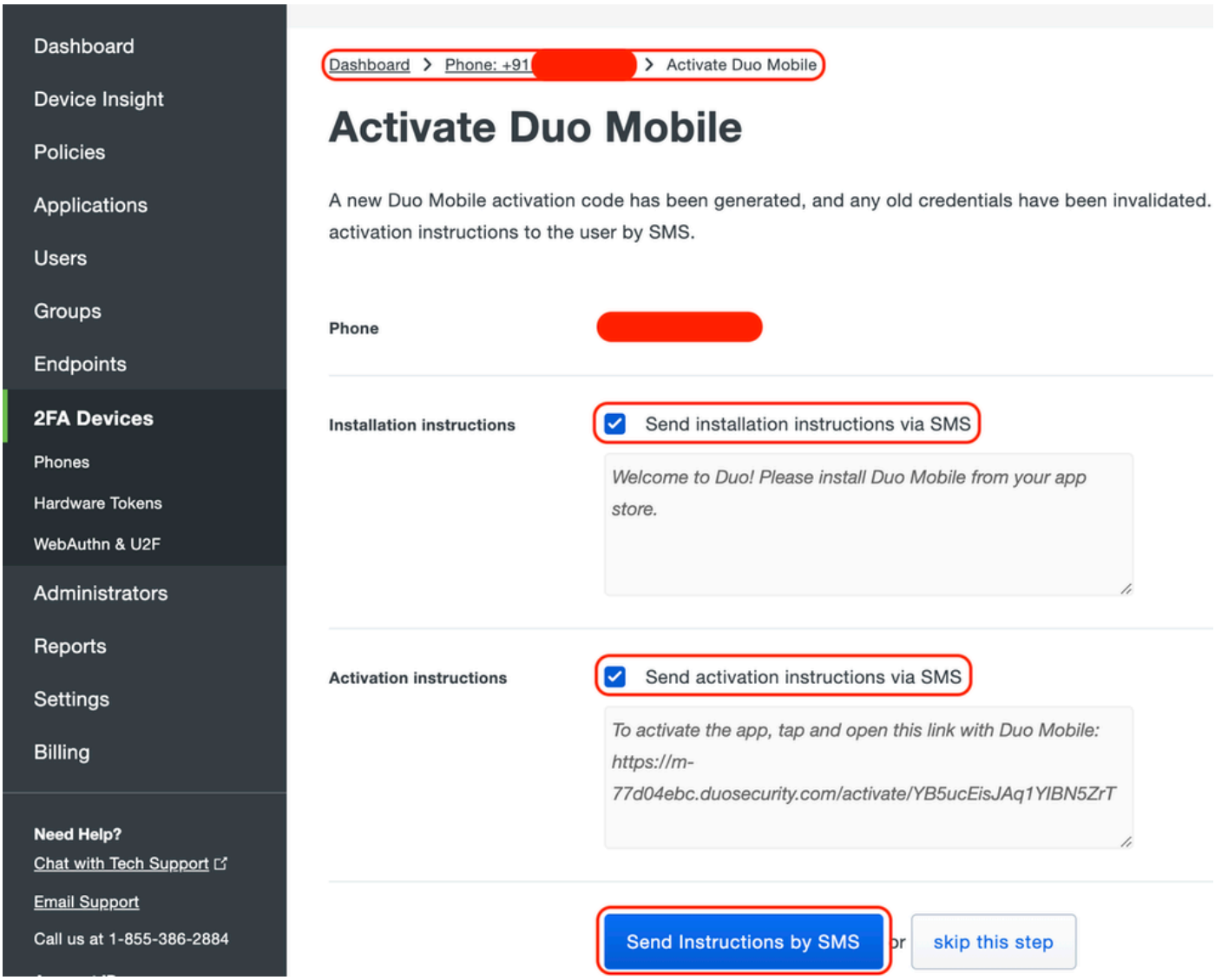


Opmerking: zorg ervoor dat "Duo Mobile" is geïnstalleerd op het apparaat van de eindgebruiker.
Handmatige installatie van Duo-toepassing voor IOS-apparaten
Handmatige installatie van Duo-toepassing voor Android-apparaten

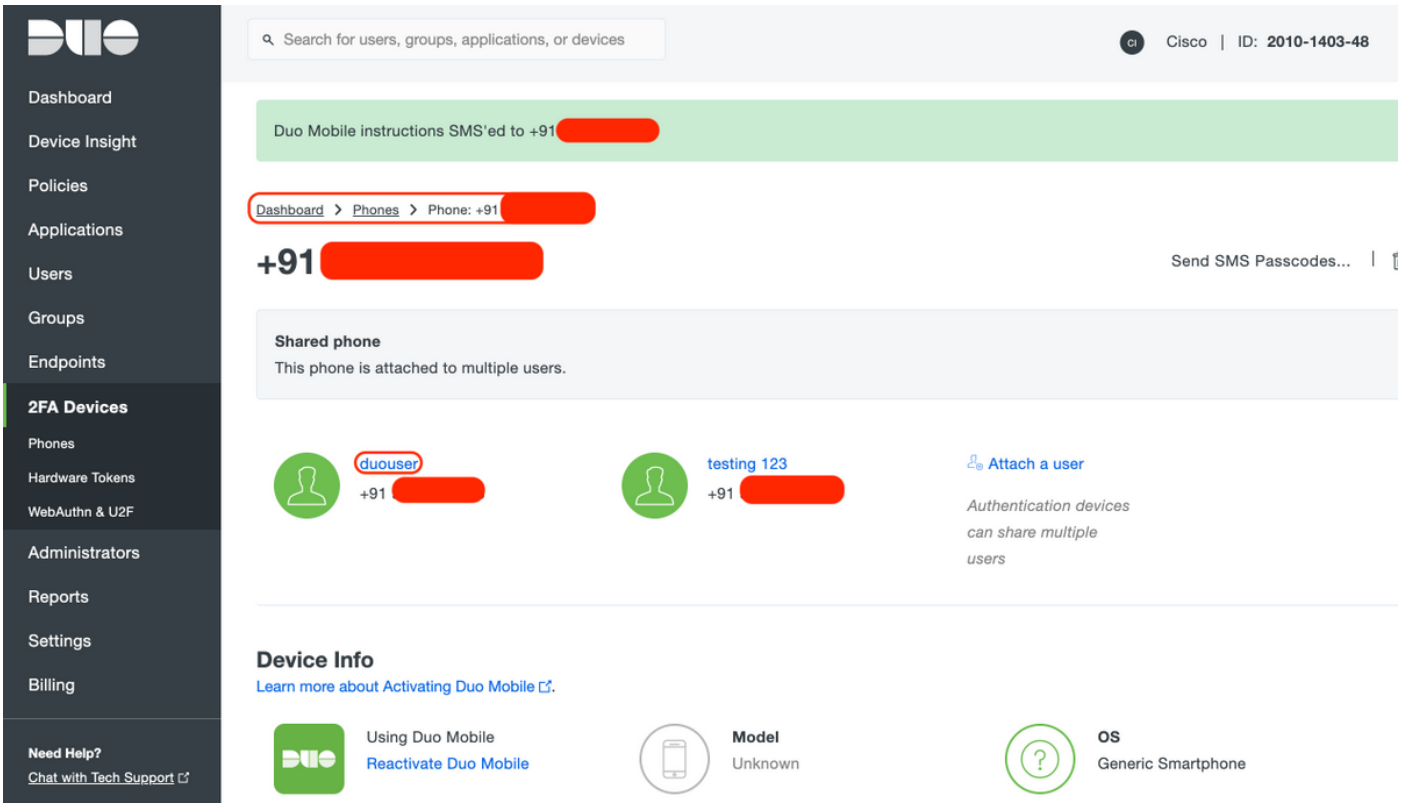
Selecteer "Generate Duo Mobile Activeringscode" zoals in de afbeelding:



Selecteer "Instructies per sms verzenden" zoals in de afbeelding:



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



- Configuratie Duo Access Gateway (DAG)

1. Duo Access Gateway (DAG) implementeren op een server in uw netwerk

---

Opmerking: Volg de onderstaande documenten voor implementatie:

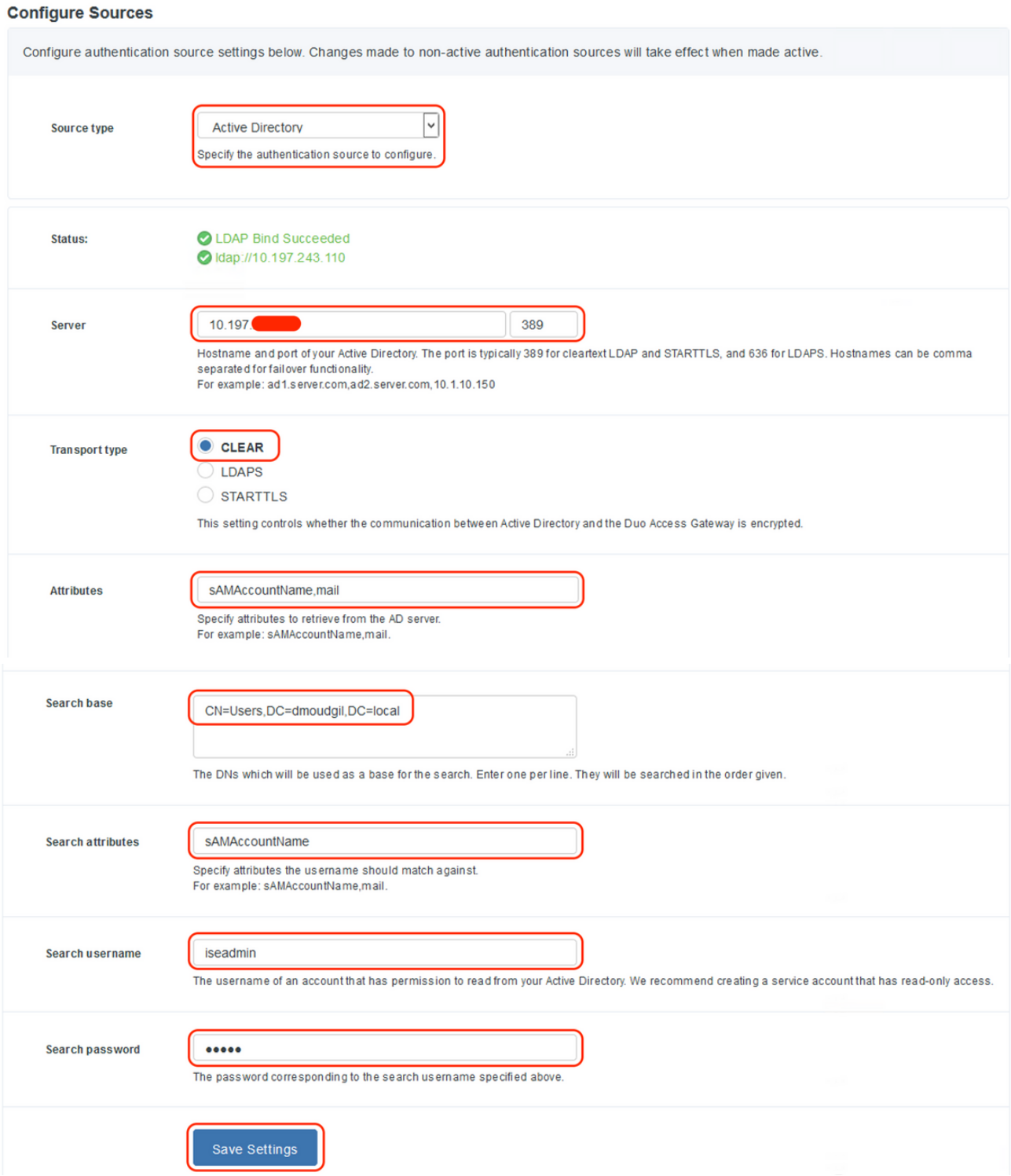
Duo Access Gateway voor Linux
https://duo.com/docs/dag-linux

Duo Access Gateway voor Windows
https://duo.com/docs/dag-windows

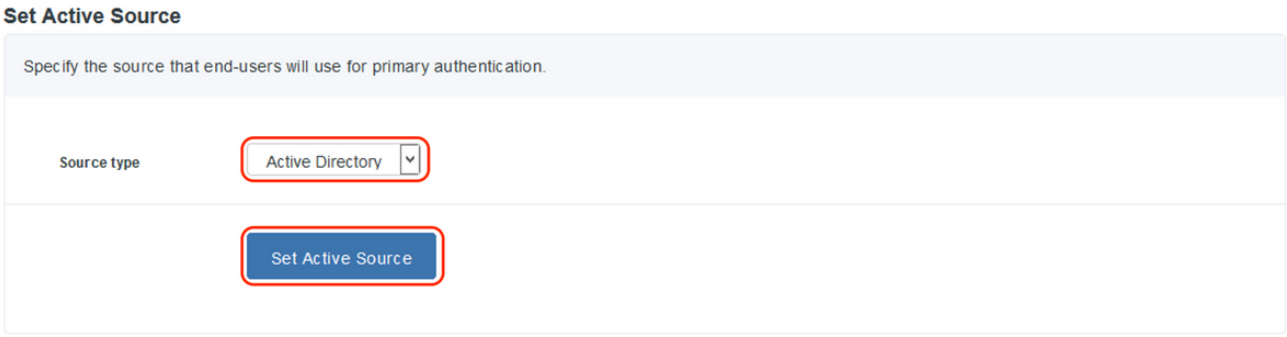
---

2. Ga op de startpagina van Duo Access Gateway naar "Verificatiebron"

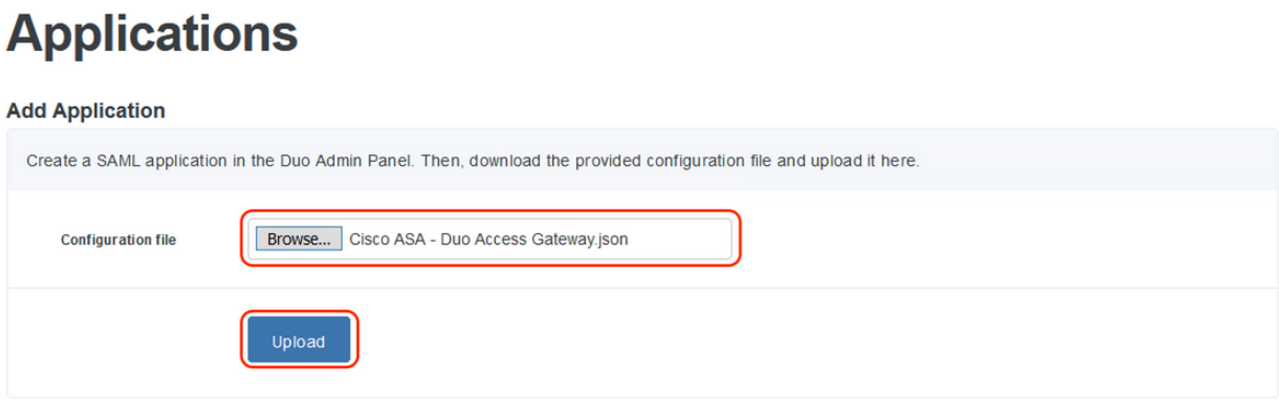
3. Voer onder "Bronnen configureren" de volgende kenmerken in voor uw Active Directory en klik op "Instellingen opslaan"



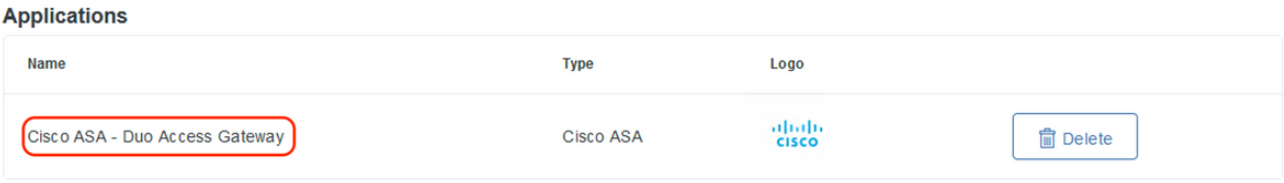
4. Selecteer onder "Actieve bron instellen" het brontype als "Actieve map" en klik op "Actieve bron instellen"



5. Navigeer naar "Toepassingen", onder het submenu "Add Application" het .json bestand uploaden dat gedownload is van Duo Admin Console binnen de sectie "Configuration file". Het corresponderende .json-bestand is gedownload in Stap 3 onder Duo Admin Portal Configuration

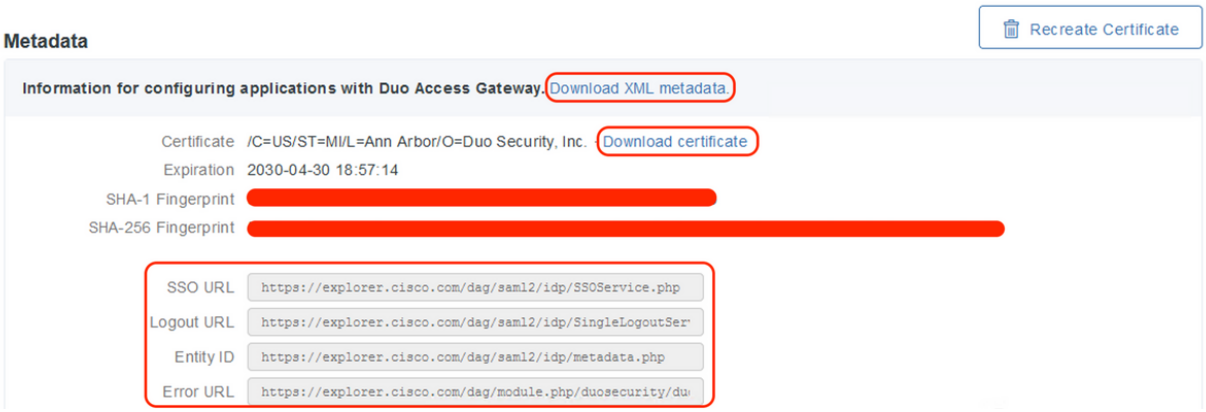


6. Zodra de applicatie succesvol is toegevoegd, verschijnt deze onder het submenu "Toepassingen"



7. Download onder het submenu "Metadata" de XML-metadata en het IDp certificaat en noteer de volgende URL's die later op de ASA zijn geconfigureerd

    1. DSB-URL
    2. Uitloggen-URL
    3. Entiteits-ID
    4. Fout URL



- ASA-configuratie

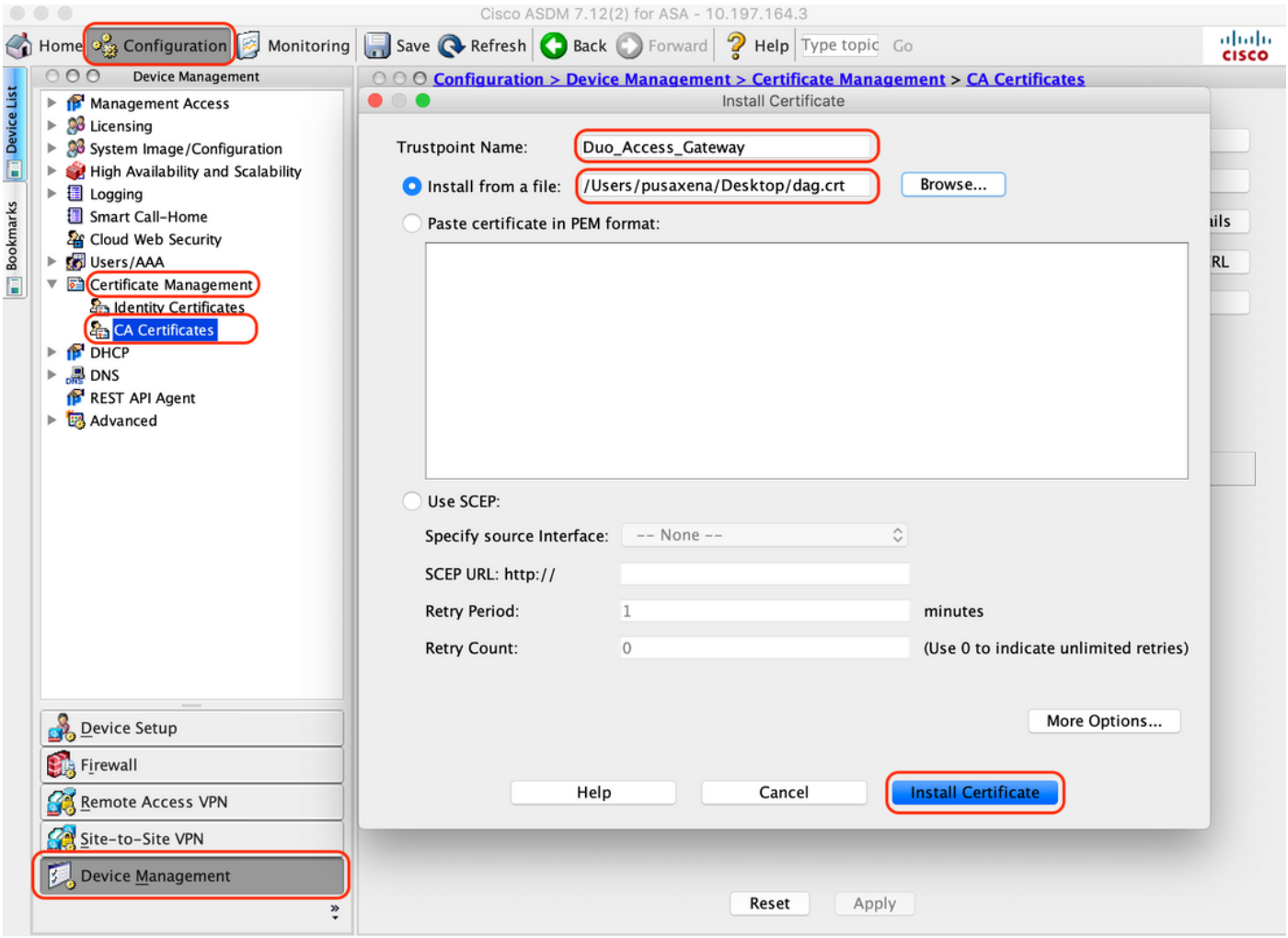
Deze paragraaf bevat informatie over het configureren van ASA voor SAML IDP-verificatie en basisconfiguratie van AnyConnect. Het document biedt ASDM-configuratiestappen en CLI-loopconfiguratie voor het overzicht.

1. Certificaat voor Duo Access Gateway uploaden

A. Navigeer naar "Configuratie > Apparaatbeheer > Certificaatbeheer > CA-certificaten" en klik op "Toevoegen"

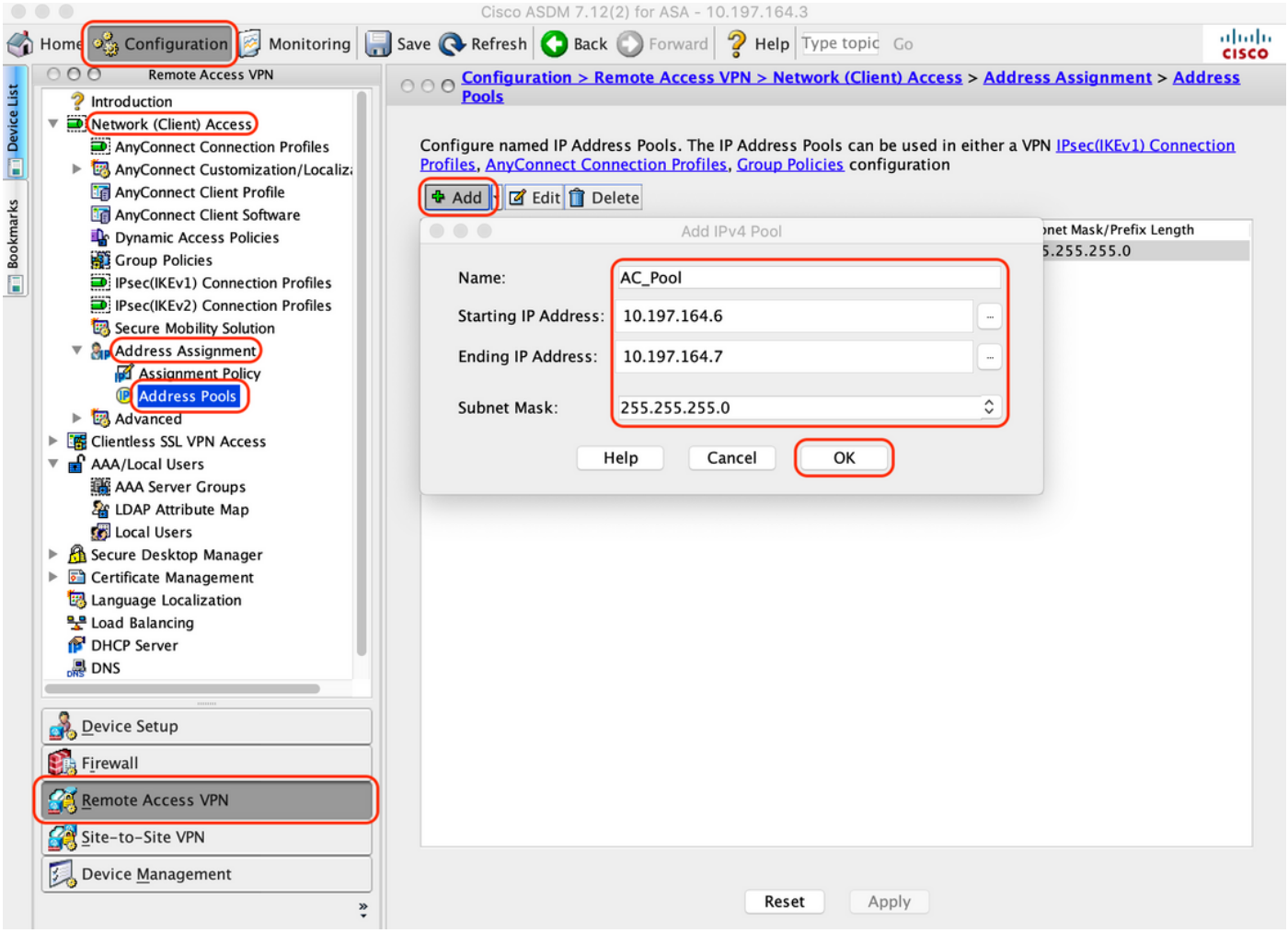
B. Configureer op de "Install Certificate Page" de Trustpoint Name: Duo_Access_Gateway

C. Klik op "Bladeren" om het pad te selecteren dat aan het DAG-certificaat is gekoppeld en klik na het selecteren op "Installatiecertificaat"



2. IP Local Pool maken voor AnyConnect-gebruikers

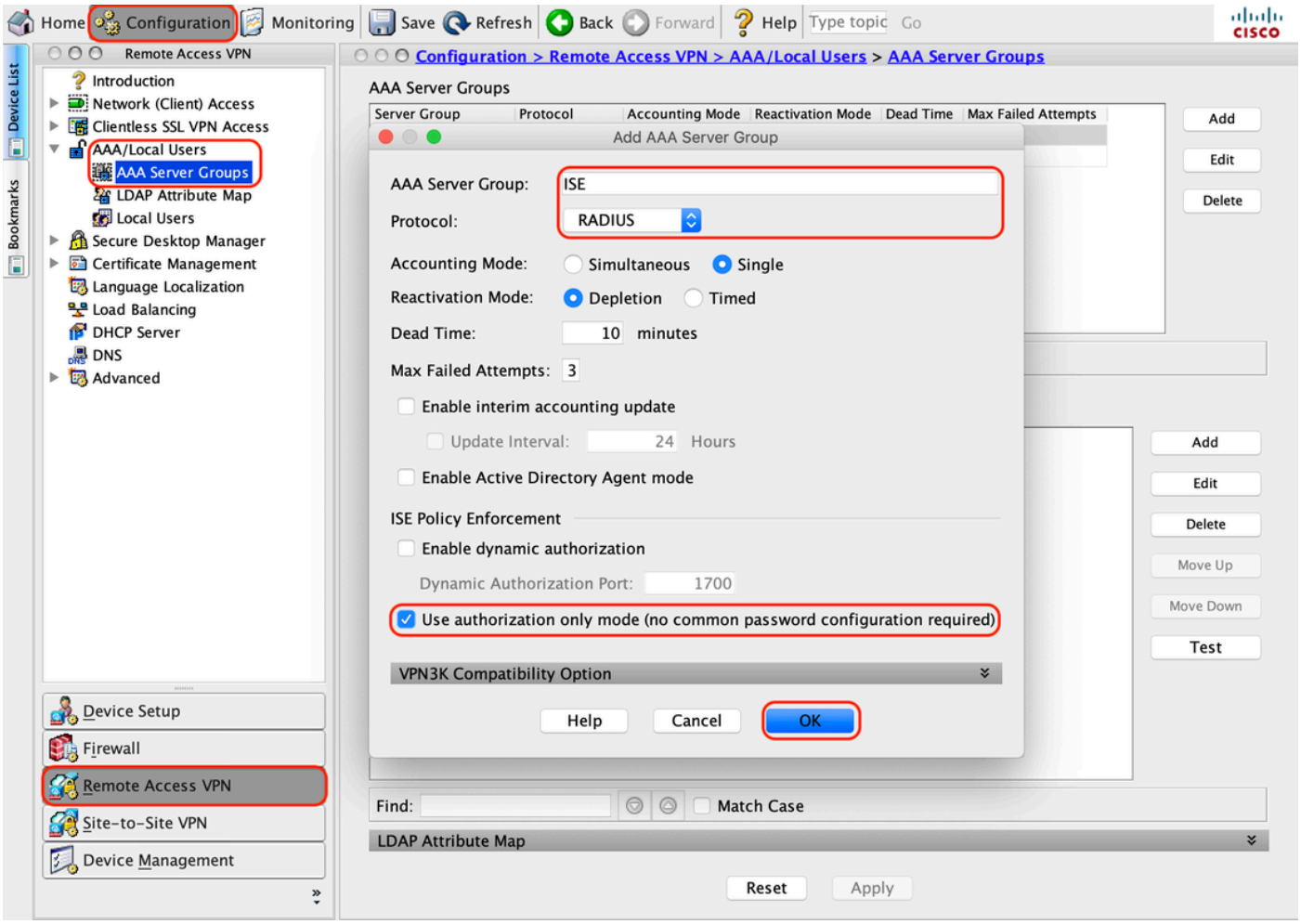
Navigeer naar "Configuratie > Externe toegang VPN > Netwerktoegang (client) > Adrestoewijzing > Adrespools", klik op "Toevoegen"



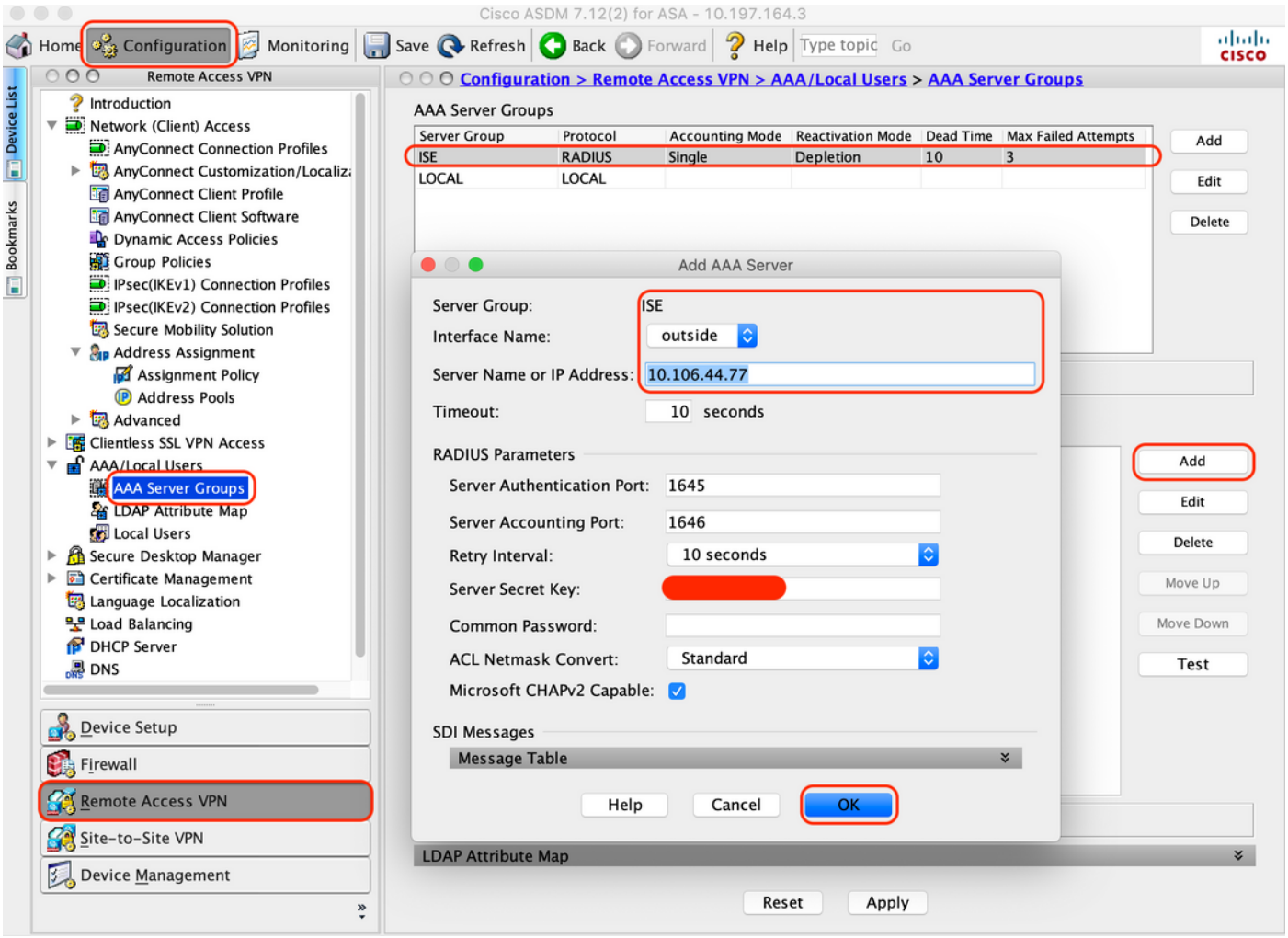
3. AAA-servergroep configureren

A. In deze sectie, configureer de AAA-servergroep en geef details over de specifieke AAA-server die de autorisatie uitvoert

B. Navigeer naar "Configuratie > Externe toegang VPN > AAA/Lokale gebruikers > AAA-servergroepen", klik op "Toevoegen"



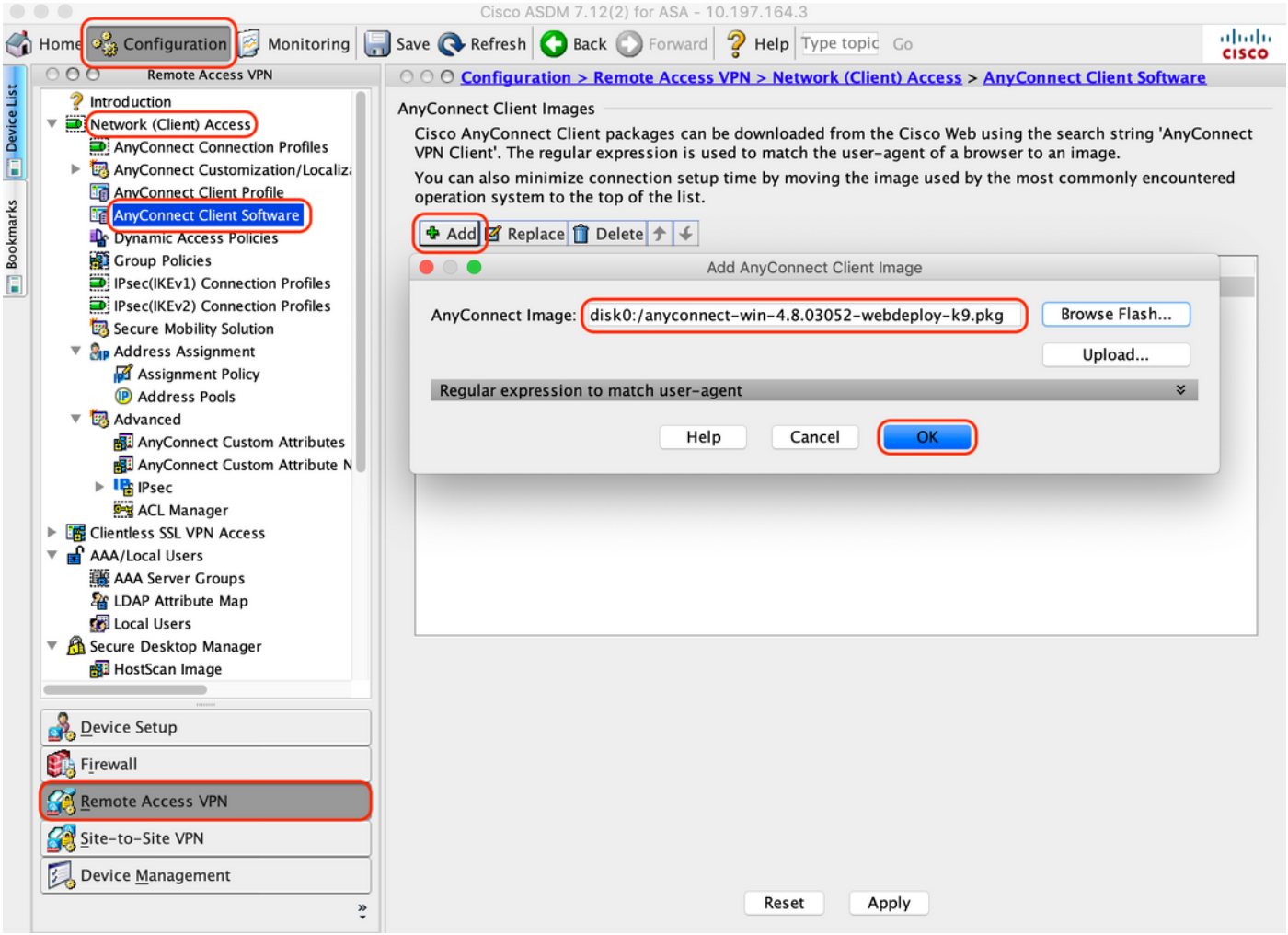
C. Klik op dezelfde pagina onder de sectie "Servers in de geselecteerde groep" op "Add" en geef IP-adresdetails van de AAA-server op



4. Toewijzing van AnyConnect-clientsoftware

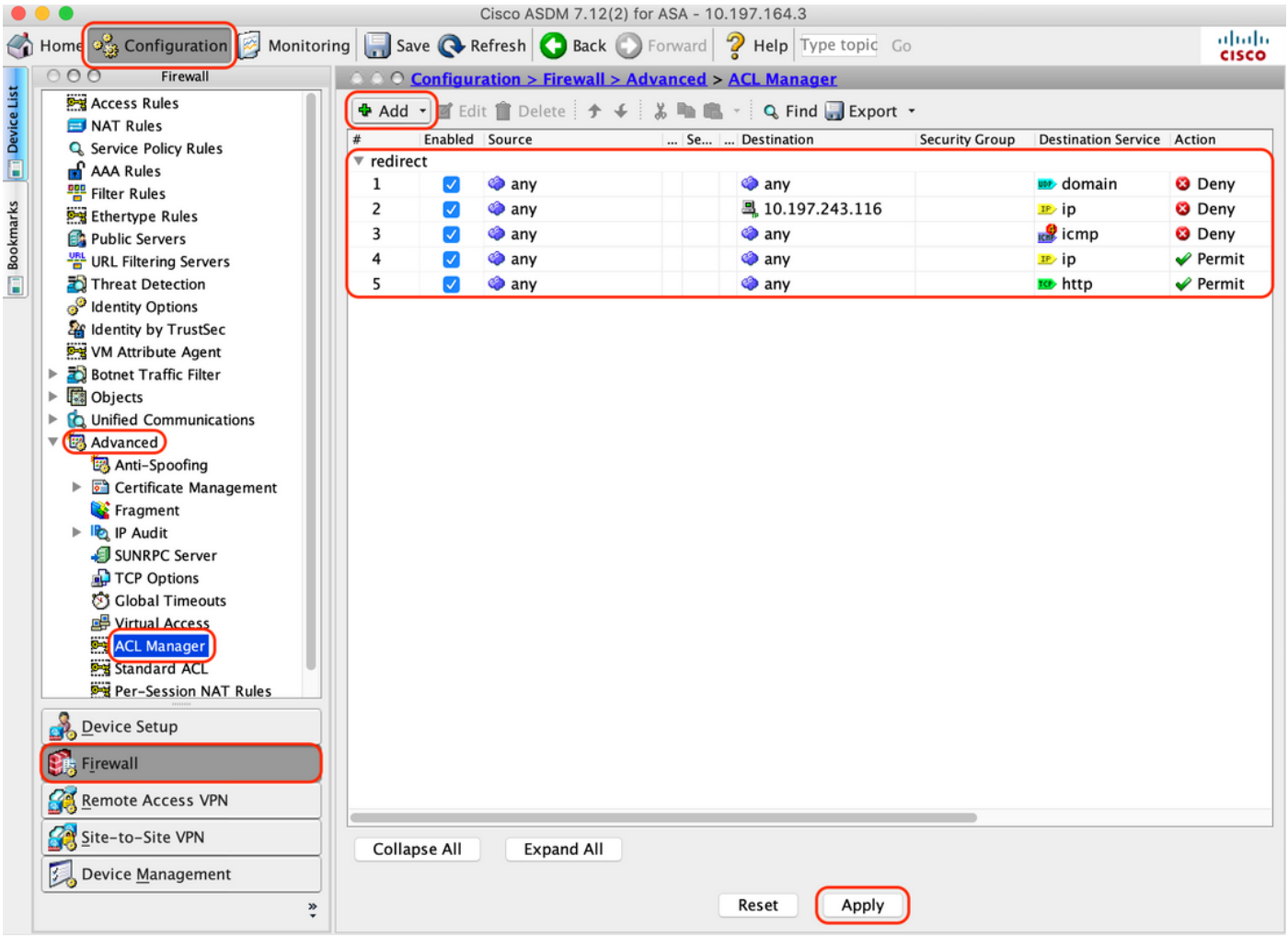
A. Breng de AnyConnect-clientsoftware in kaart met webimplementatieafbeelding 4.8.03052 voor Windows die voor WebVPN moet worden gebruikt

B. Navigeer naar "Configuration > Remote Access VPN > Network (Client) Access > AnyConnect-clientsoftware" en klik op "Add"



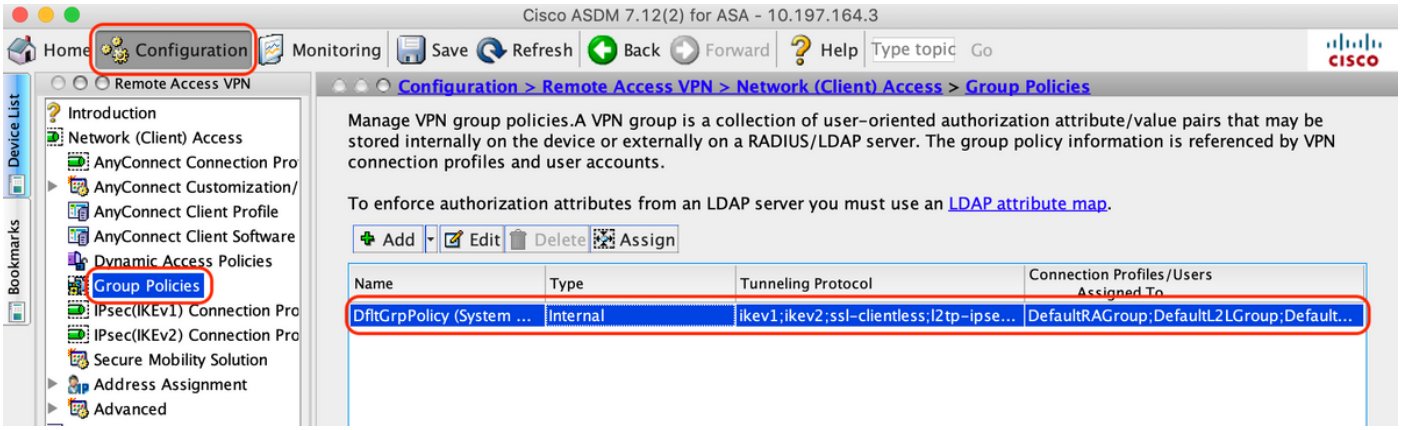
5. Configureer de omleiding van ACL die als resultaat van ISE is ingedrukt

A. Navigeer naar "Configuratie > Firewall > Geavanceerd > ACL-beheer". Klik op Toevoegen om de omleiding van ACL toe te voegen. De ingangen, zodra geconfigureerd, zien zoals hieronder:



6. Bestaand groepsbeleid valideren

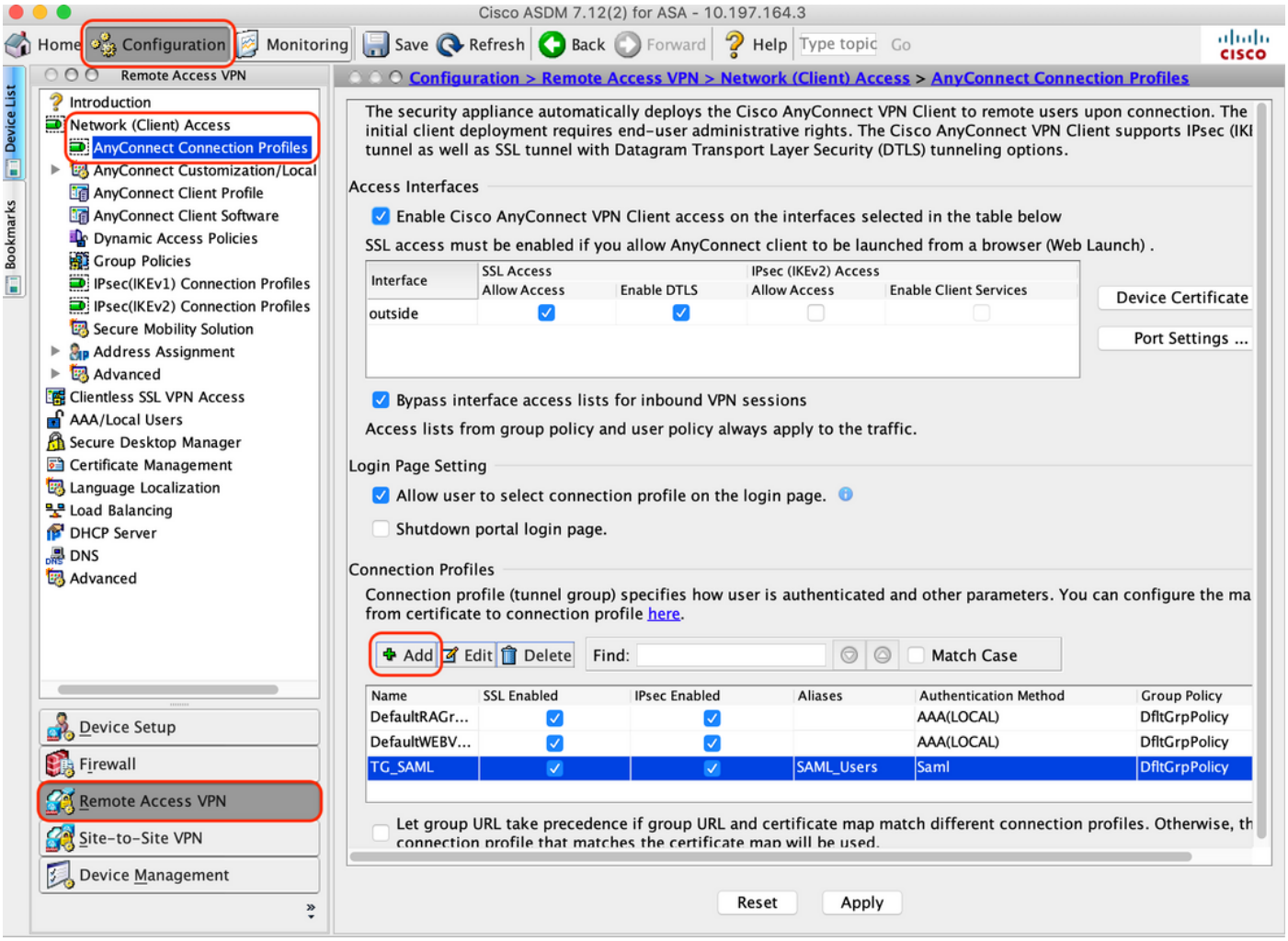
A. Bij deze instelling wordt gebruikgemaakt van het standaardgroepsbeleid dat kan worden bekeken op: "Configuration > Remote Access VPN > Network (Client) Access > Group Policies"



7. Verbindingsprofiel configureren

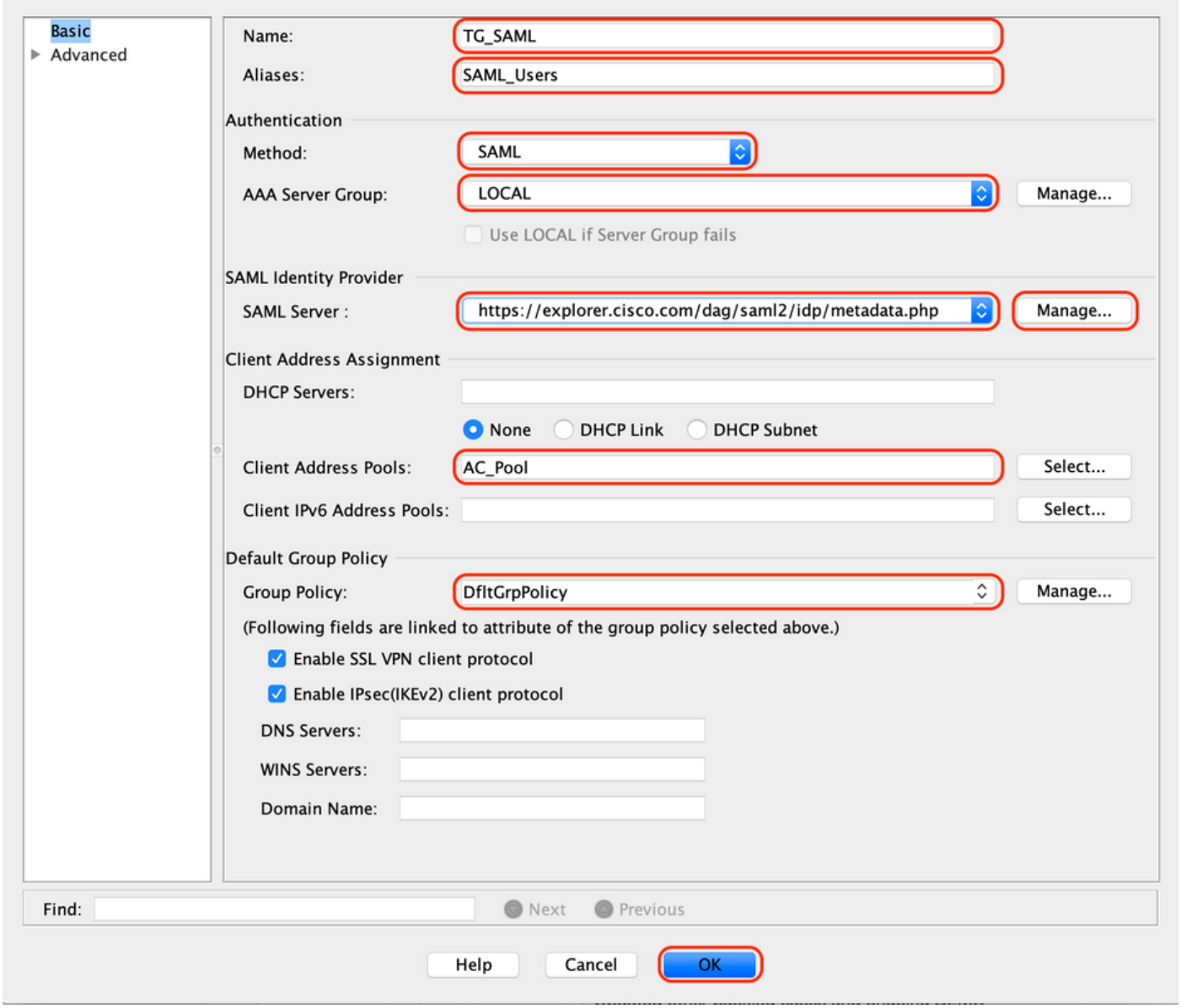
A. Een nieuw verbindingsprofiel maken waarmee AnyConnect-gebruikers verbinding maken

B. Navigeer naar "Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles", klik op "Add"



C. Configureer de onderstaande gegevens die aan het verbindingsprofiel zijn gekoppeld:

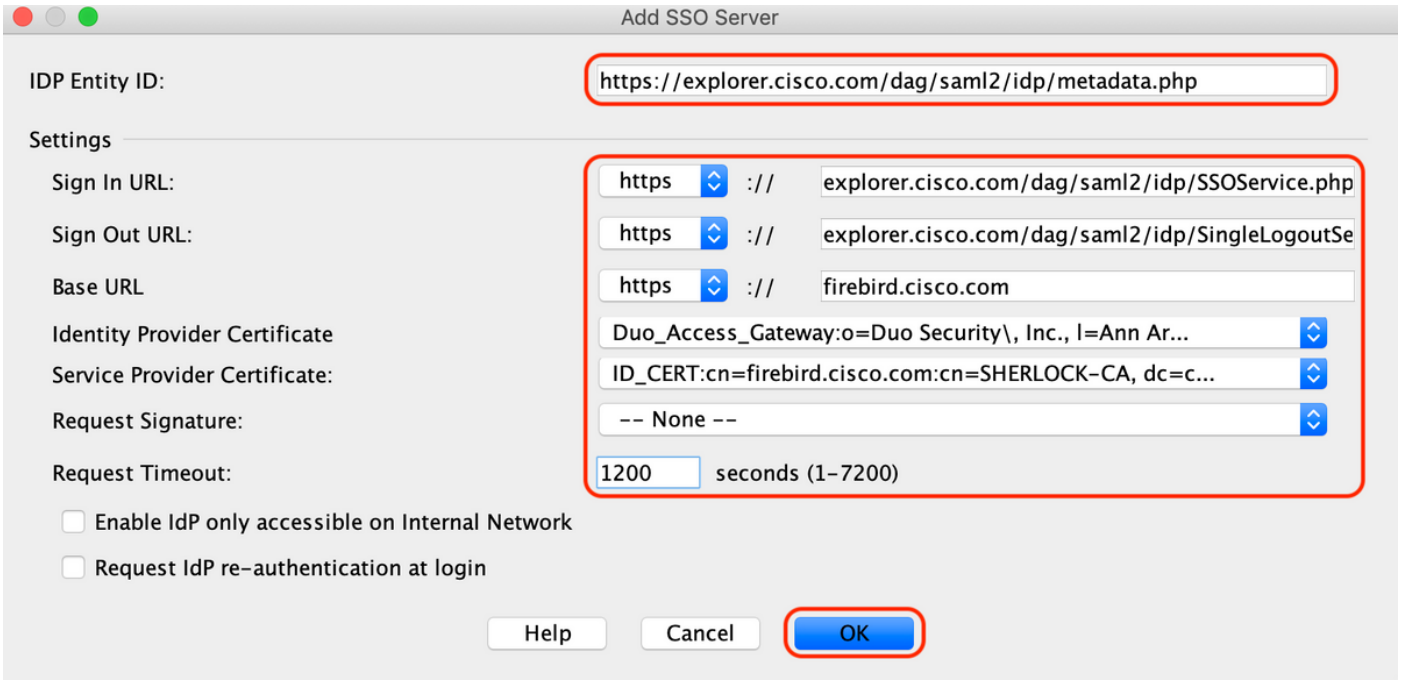
Naam	TG_SAML
Bijnamen	SAML_Gebruikers
Methode	SAML
AAA-servergroep	Lokaal
Clientadrespools	AC_pool
Groepsbeleid	DFLG-beleid



D. Op dezelfde pagina kunt u de gegevens van de SAML Identity Provider configureren zoals hieronder wordt getoond:

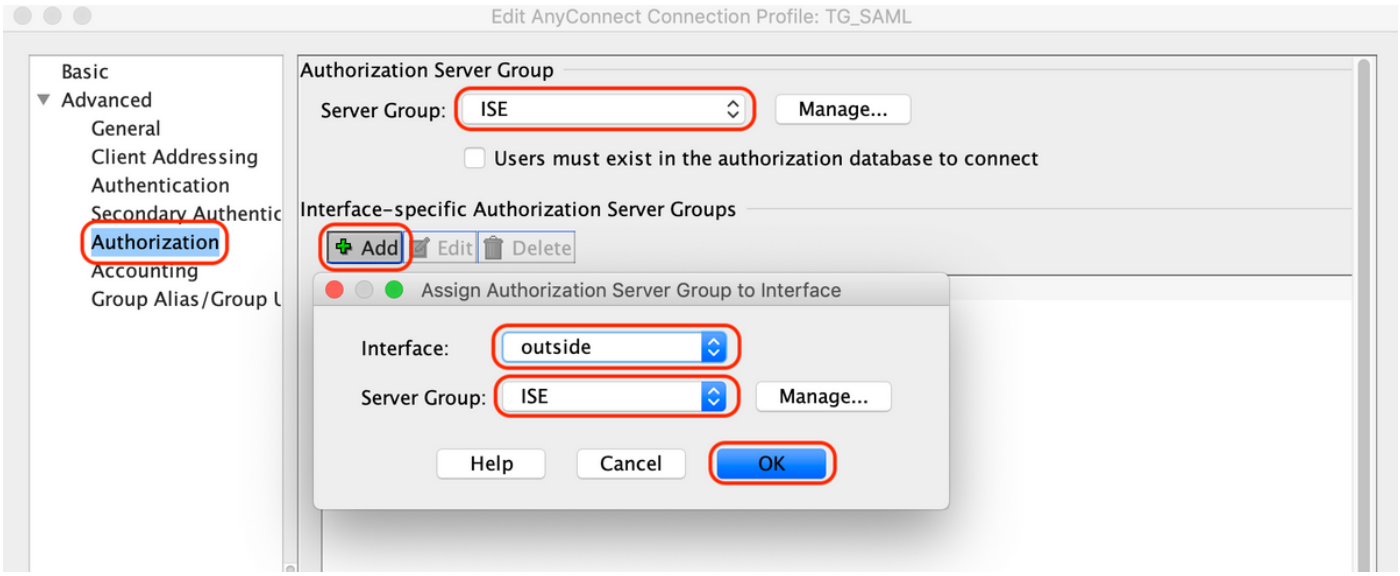
ID IDP-entiteit	https://explorer.cisco.com/dag/saml2/idp/metadata.php
URL voor aanmelding	https://explorer.cisco.com/dag/saml2/idp/SSOService.php
URL voor uitloggen	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explore
Basis-URL	https://firebird.cisco.com

E. Klik op "Beheer > Toevoegen"



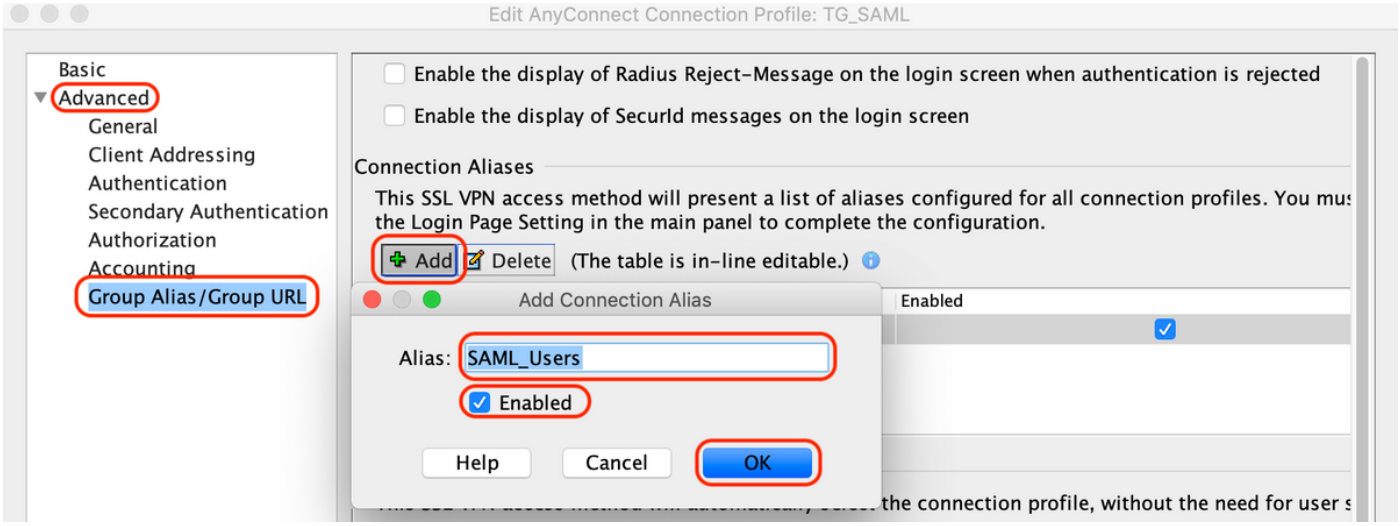
F. Definieer onder de sectie Geavanceerd voor het verbindingsprofiel de AAA-server voor autorisatie

Navigeer naar "Geavanceerd > Autorisatie" en klik op "Toevoegen"



G. Onder Groepsalias de verbindingsalias definiëren

Navigeer naar "Geavanceerd > Groepsalias/GroepsURL" en klik op "Toevoegen"



H. Dit voltooit de ASA configuratie, hetzelfde ziet er uit zoals hieronder op de opdrachtregel interface (CLI)

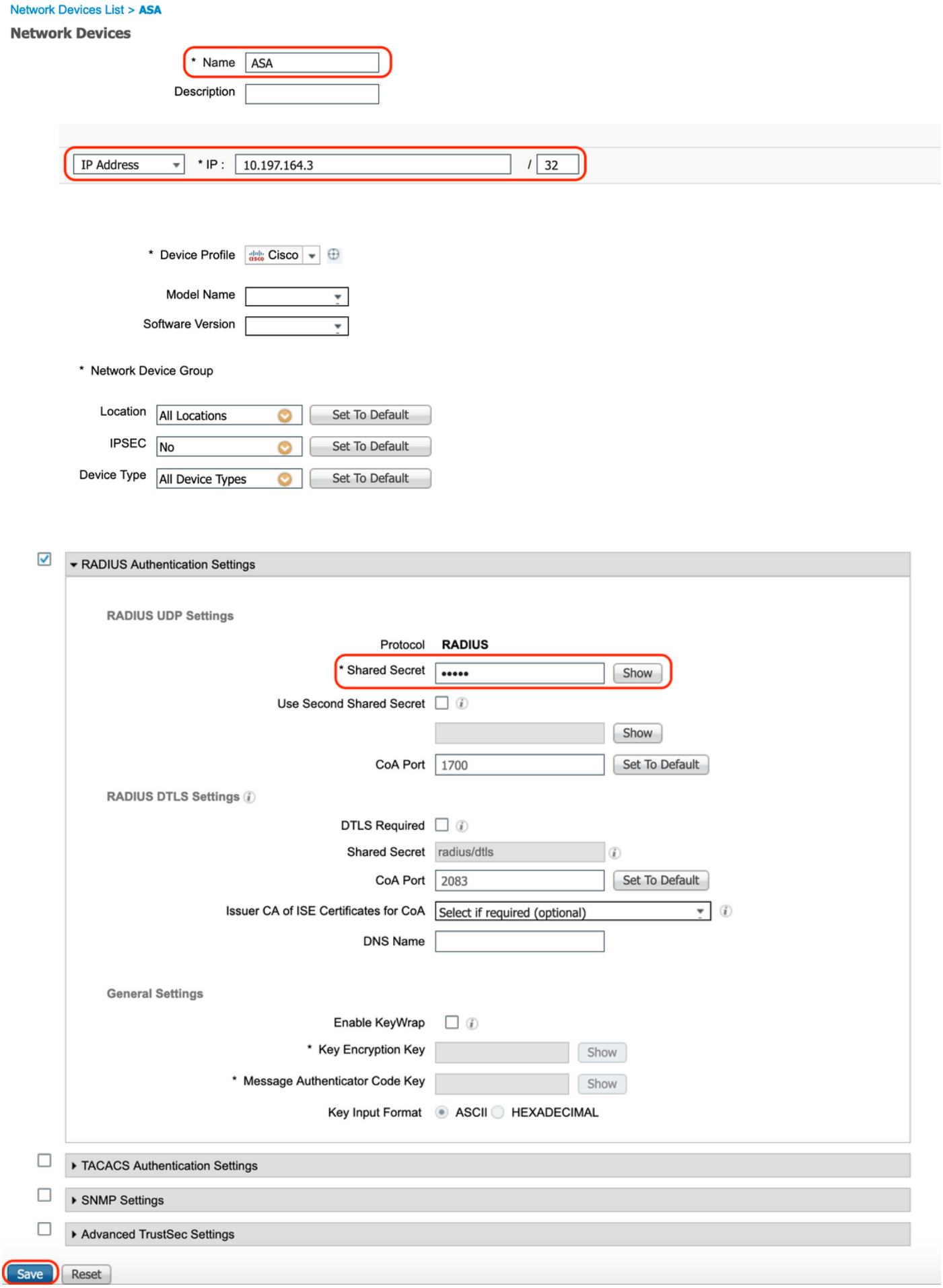
```
!
hostname firebird
domain-name cisco.com
!
!
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
!
!--------------------Client pool configuration--------------------
!
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
!
!--------------------Redirect Access-list-------------------------
!
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.197.243.116
access-list redirect extended deny icmp any any
access-list redirect extended permit ip any any
access-list redirect extended permit tcp any any eq www
!
!--------------------AAA server configuration---------------------
!
aaa-server ISE protocol radius
 authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE (outside) host 10.106.44.77
 key *****
!
!-----Configure Trustpoint for Duo Access Gateway Certificate-----
!
crypto ca trustpoint Duo_Access_Gateway
 enrollment terminal
 crl configure
!
!-------Configure Trustpoint for ASA Identity Certificate---------
!
crypto ca trustpoint ID_CERT
 enrollment terminal
 fqdn firebird.cisco.com
```

```
 subject-name CN=firebird.cisco.com
 ip-address 10.197.164.3
 keypair ID_RSA_KEYS
 no ca-check
 crl configure
!
!------Enable AnyConnect and configuring SAML authentication------
!
webvpn
 enable outside
 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 anyconnect image disk0:/anyconnect-win-4.8.03052-webdeploy-k9.pkg 1
 anyconnect enable
 saml idp https://explorer.cisco.com/dag/saml2/idp/metadata.php
  url sign-in https://explorer.cisco.com/dag/saml2/idp/SSOService.php
  url sign-out https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explor
  base-url https://firebird.cisco.com
  trustpoint idp Duo_Access_Gateway
  trustpoint sp ID_CERT
  no signature
  no force re-authentication
  timeout assertion 1200
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
!--------------------Group Policy configuration--------------------
!
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
!
!----------Tunnel-Group (Connection Profile) Configuraiton----------
!
tunnel-group TG_SAML type remote-access
tunnel-group TG_SAML general-attributes
 address-pool AC_Pool
 authorization-server-group ISE
 accounting-server-group ISE
tunnel-group TG_SAML webvpn-attributes
 authentication saml
 group-alias SAML_Users enable
 saml identity-provider https://explorer.cisco.com/dag/saml2/idp/metadata.php
!
```

- ISE-configuratie

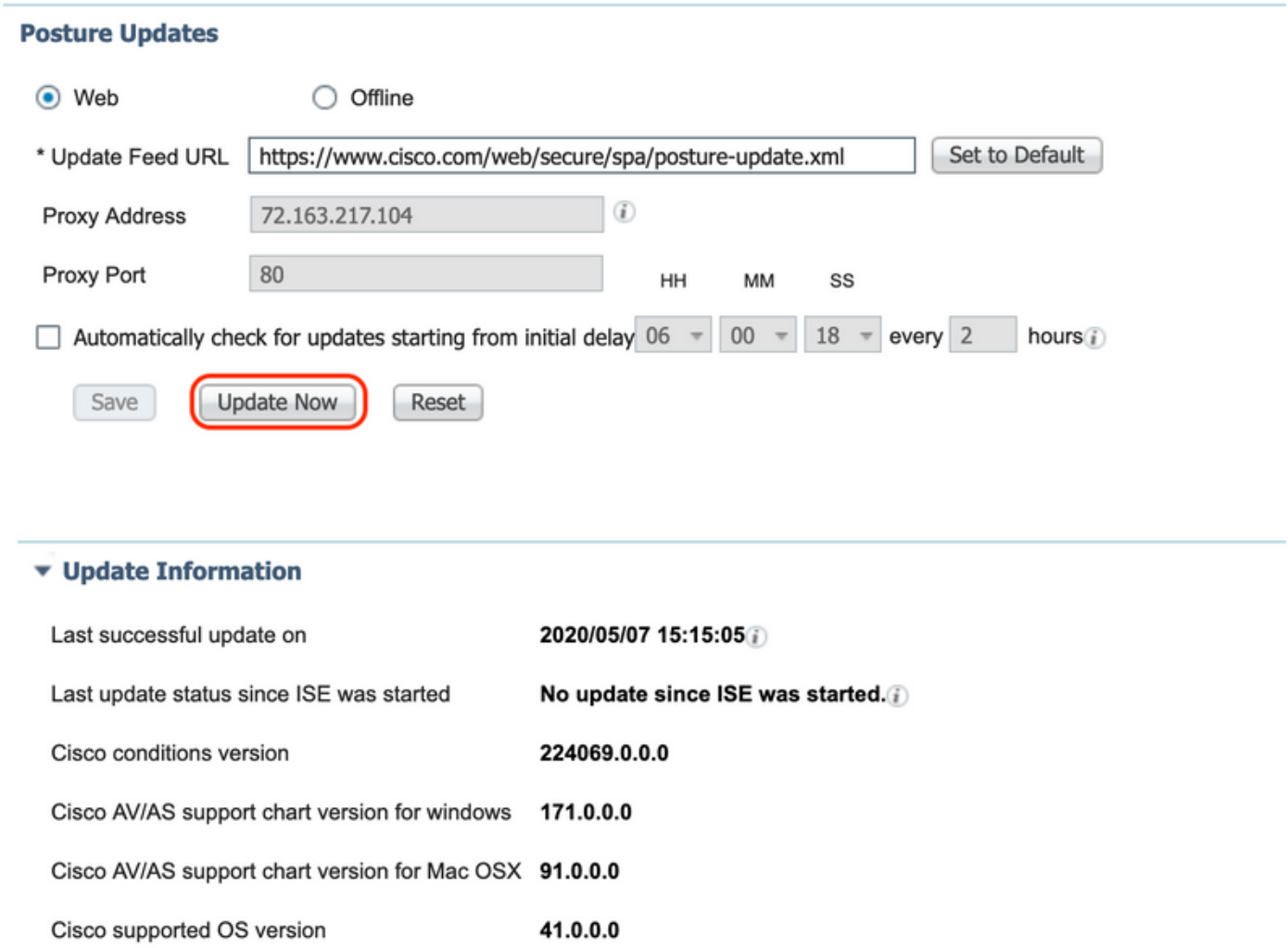
1. Cisco ASA toevoegen als netwerkapparaat

Klik onder "Beheer > Netwerkbronnen > Netwerkapparaten" op "Toevoegen".
Configureer de naam van het netwerkapparaat, het bijbehorende IP-adres en voer onder "Instellingen voor RADIUS-verificatie" het gedeelde geheim in en klik op "Opslaan"


Network Devices List > ASA
Network Devices
* Name
ASA
Description
IP Address
* IP :
10.197.164.3
/ 32
* Device Profile
Cisco
Model Name
Software Version
* Network Device Group
Location
All Locations
Set To Default
IPSEC
No
Set To Default
Device Type
All Device Types
Set To Default
RADIUS Authentication Settings
RADIUS UDP Settings
Protocol
RADIUS
* Shared Secret
Show
Use Second Shared Secret
Show
CoA Port
1700
Set To Default
RADIUS DTLS Settings
DTLS Required
Shared Secret
radius/dtls
CoA Port
2083
Set To Default
Issuer CA of ISE Certificates for CoA
Select if required (optional)
DNS Name
General Settings
Enable KeyWrap
* Key Encryption Key
Show
* Message Authenticator Code Key
Show
Key Input Format
ASCII
HEXADECIMAL
TACACS Authentication Settings
SNMP Settings
Advanced TrustSec Settings
Save
Reset

2. Installeer de laatste updates

Navigeer naar "Beheer > Systeem > Instellingen > Houding > Updates" en klik op "Nu bijwerken"

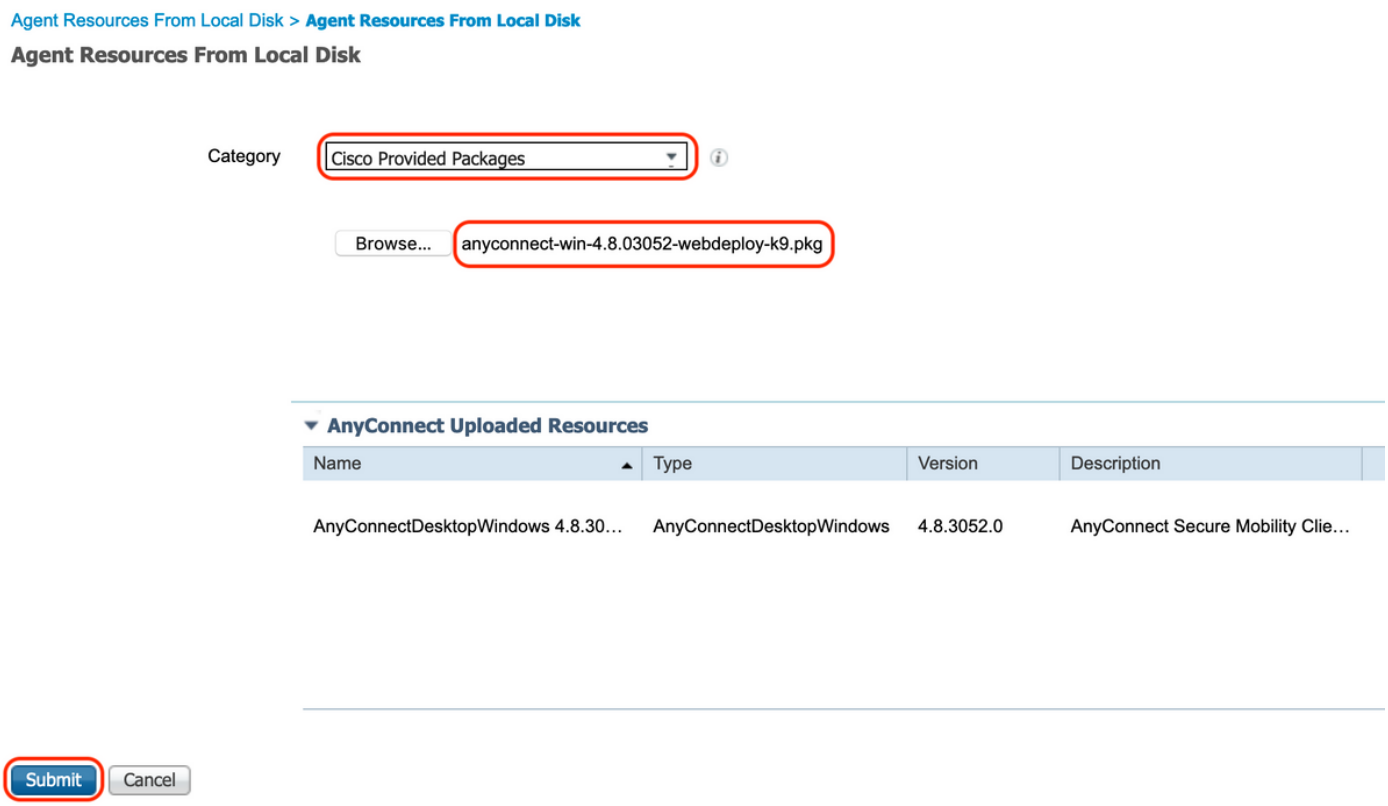


3. Upload de Compliance Module en AnyConnect Head-end implementatiepakket op ISE-kaart

Ga naar "Beleid > Beleidselementen > Resultaten > Clientprovisioning > Resources". Klik op "Add" en selecteer "Agent resources from local disk" of "Agent resources from Cisco site" op basis van de vraag of de bestanden moeten worden opgehaald van het lokale werkstation of de Cisco-site.

In dit geval, om bestanden te uploaden vanaf een lokaal werkstation onder Category, selecteert u "Cisco Provided Packages", klikt u op "Bladeren" en selecteert u de gewenste pakketten en klikt u op "Submit".

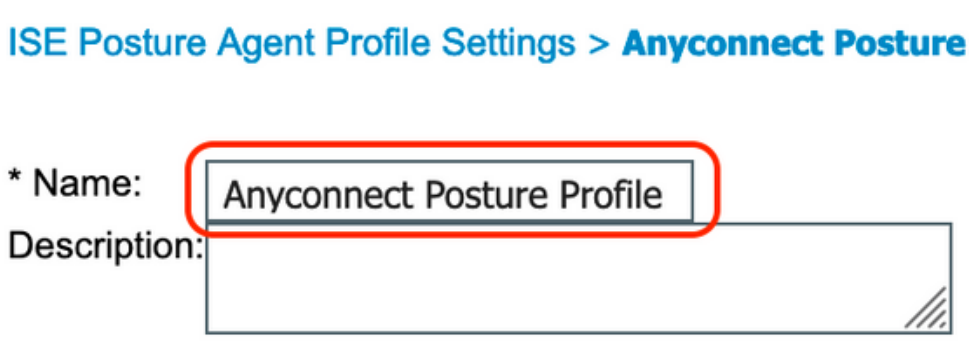
Dit document gebruikt "anyconnect-win-4.3.1012.6145-iscompliance-webimplementation-k9.pkg" als compliancemodule en "anyconnect-win-4.8.03052-webimplementation-k9.pkg" als AnyConnect Head-end implementatiepakket.



4. Een AnyConnect-poortprofiel maken

A. Navigeer naar "Beleid > Beleidselementen > Resultaten > Clientprovisioning > Bronnen". Klik op "Add" en selecteer "AnyConnect Posture Profile"

B. Voer de naam in voor het AnyConnect Posture-profiel en configureer de servernaam als "*" onder Servernaamregels en klik op "Opslaan"



Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List		List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

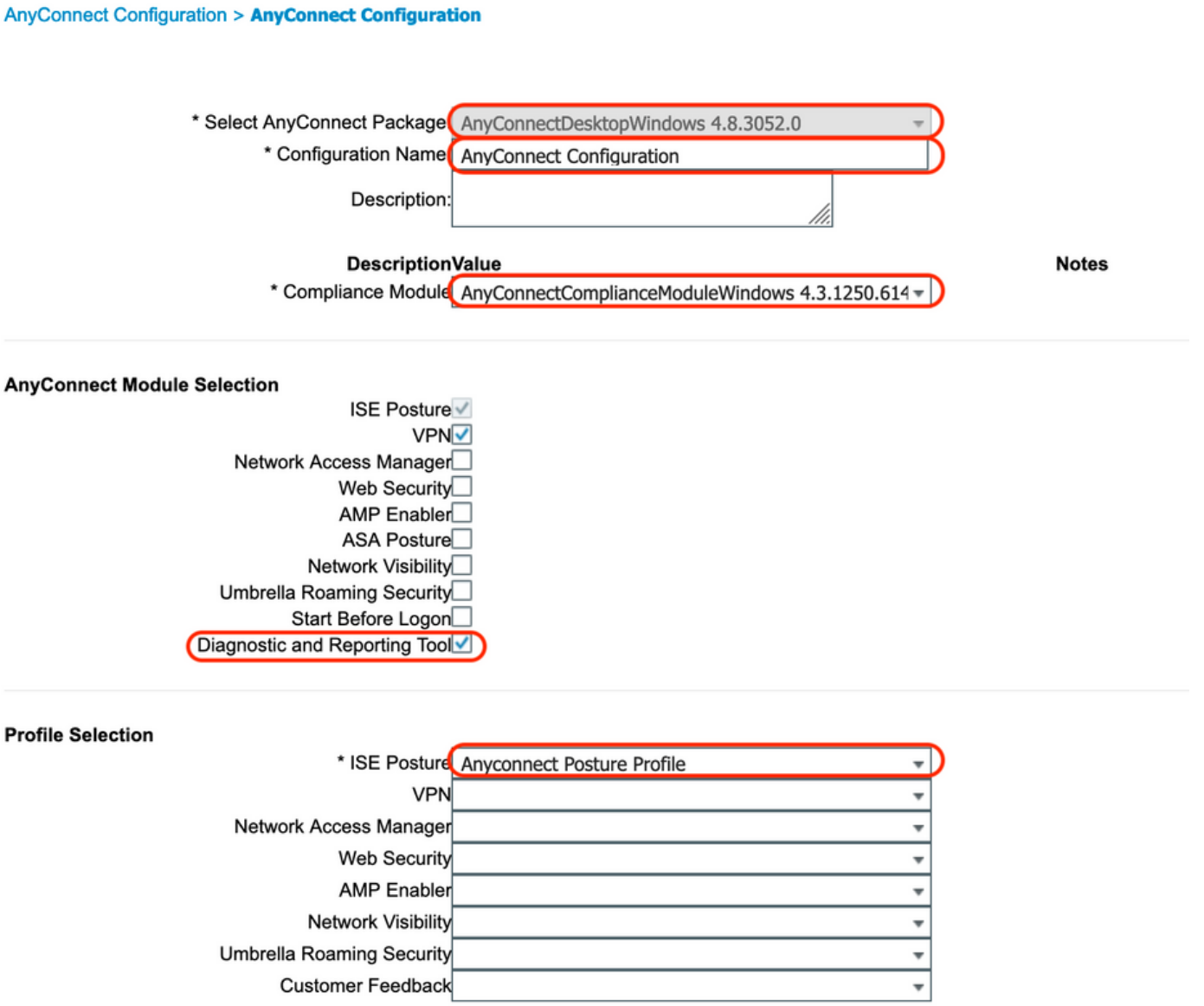
5. Configuratie AnyConnect maken

A. Navigeer naar "Beleid > Beleidselementen > Resultaten > Clientprovisioning > Bronnen". Klik op "Add" en selecteer "AnyConnect Configuration".

B. Selecteer AnyConnect-pakket, voer een configuratienaam in en selecteer de gewenste nalevingsmodule

C. Controleer onder "AnyConnect-moduleselectie" het programma 'Diagnostic and Reporting Tool'

D. Selecteer onder "Profielselectie" het selectieprofiel en klik op "Opslaan"

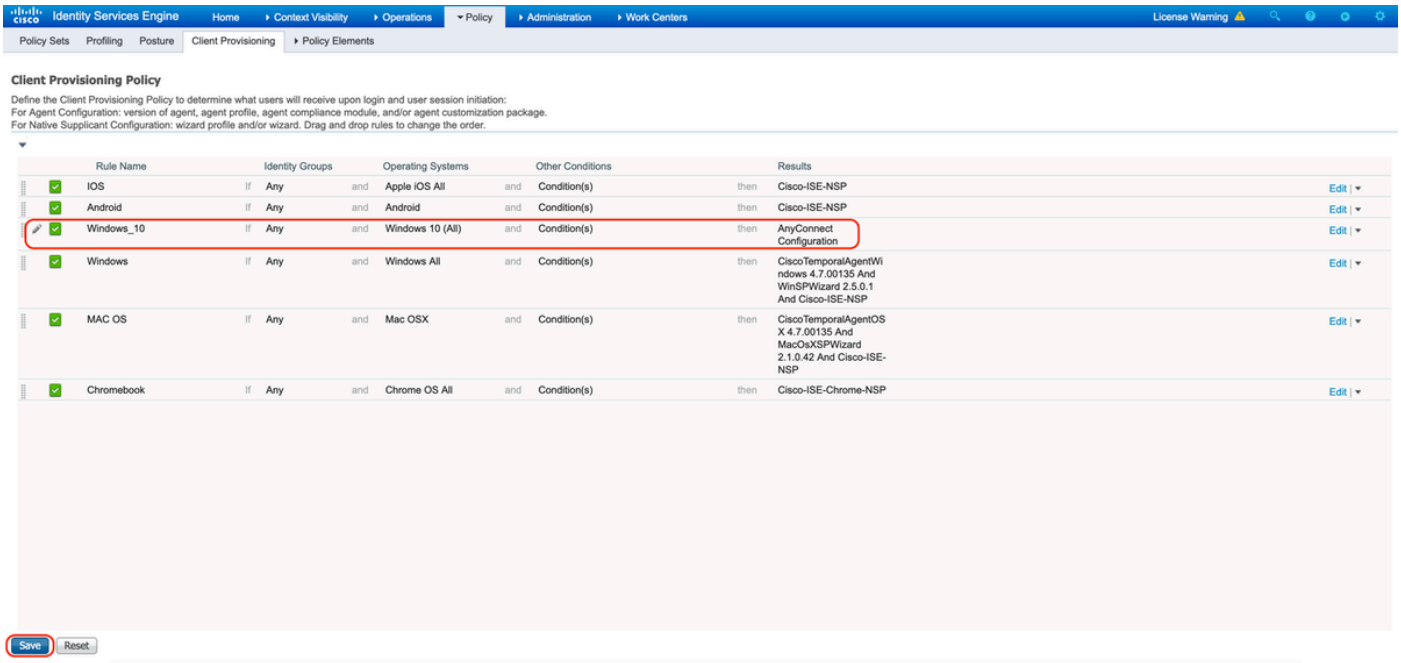


6. Clientprovisioningbeleid maken

A. Navigeer naar "Beleid > Clientprovisioning"

B. Klik op "Bewerken" en selecteer "Regel hierboven invoegen".

C. Voer de naam van de regel in, selecteer het gewenste besturingssysteem en selecteer onder Resultaten (binnen "Agent" > "Agent Configuration"), "AnyConnect Configuration" die in Stap 5 is gemaakt en klik op "Opslaan"

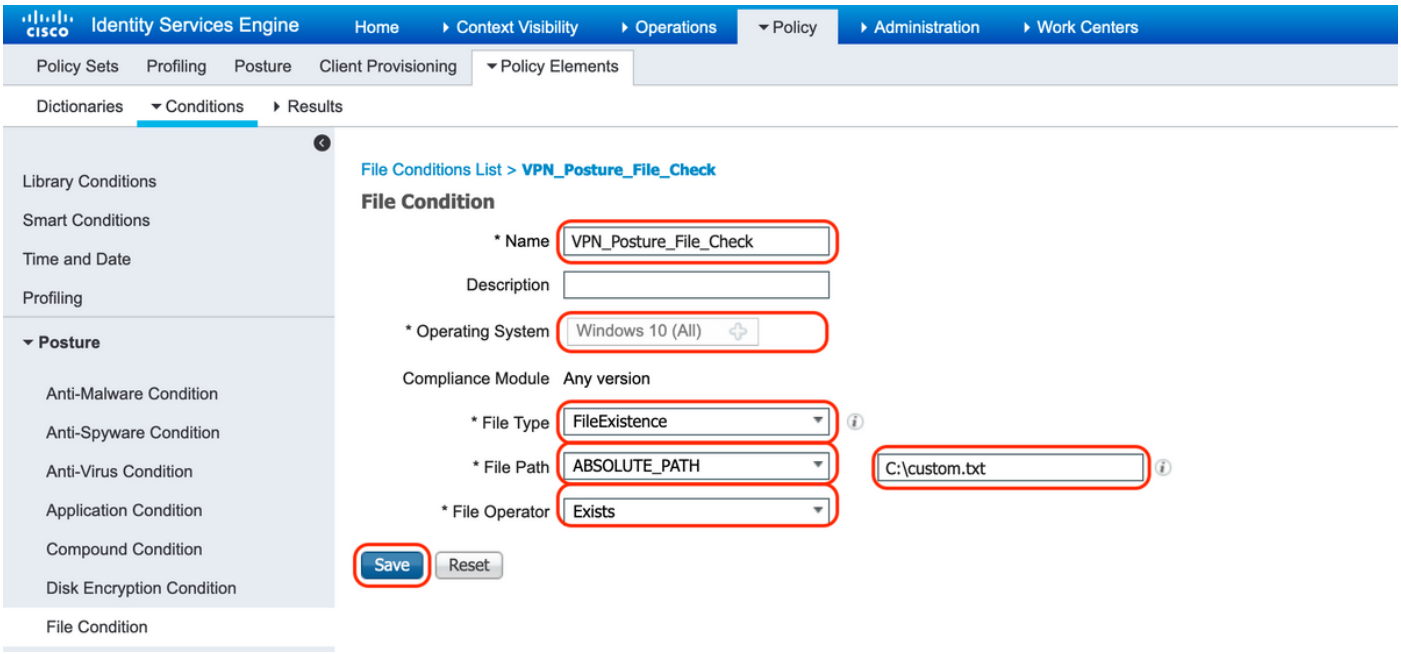


7. Een houdingsvoorwaarde maken

A. Navigeer naar "Beleid > Beleidselementen > Voorwaarden > Houding > Bestandsvoorwaarden"

B. Klik op "Add" en configureer de voorwaardelijke naam "VPN_Posture_File_Check", het gewenste besturingssysteem als "Windows 10(All)", bestandstype als "FileExistence", bestandspad als "ABSOLUTE_PATH", en het volledige pad en de bestandsnaam als "C:\custom.txt", selecteer File Operator als "Exists"

C. In dit voorbeeld wordt de aanwezigheid van een bestand met de naam "custom.txt" onder C: drive gebruikt als de bestandsvoorwaarde



8. Oplossingsactie voor houding aanmaken

Navigeer naar "Beleid > Beleidselementen > Resultaten > Houding > Oplossingsacties" om een corresponderende actie voor bestandsherstel te maken. In dit document wordt "Alleen tekst bericht" gebruikt als herstelacties die in de volgende stap zijn geconfigureerd.

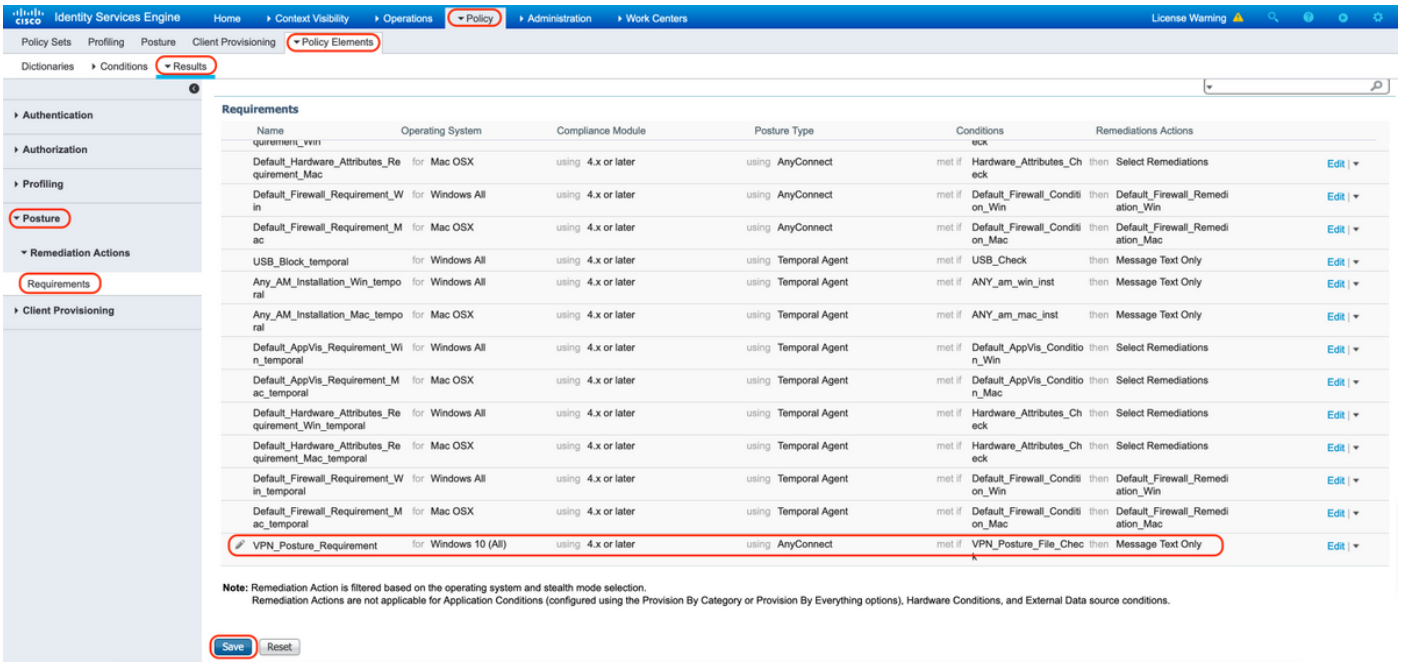
9. Opdrachtregel aanmaken

A. Navigeer naar "Beleid > Beleidselementen > Resultaten > Houding > Vereisten"

B. Klik op "Bewerken" en selecteer "Nieuwe eis invoegen"

C. Configureer de voorwaardelijke naam "VPN_Posture_Requirement", vereist besturingssysteem als "Windows 10(All)", Compliance Module als "4.x of hoger", Posture Type als "AnyConnect"

D. Voorwaarden als "VPN_Posture_File_Check" (aangemaakt in stap 7) en onder Remediations Actions selecteert u Actie als "Alleen tekst bericht" en voert u het aangepaste bericht in voor Agent-gebruiker

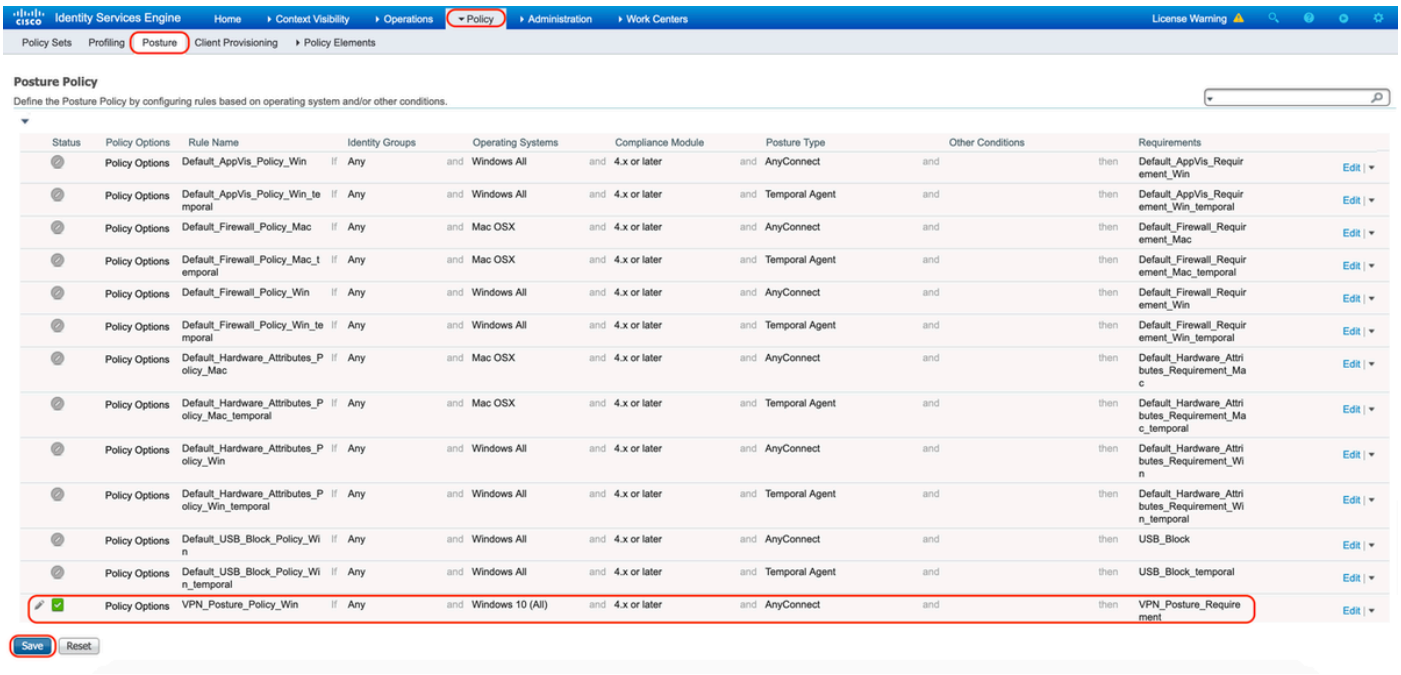


10. Een posteriebeleid maken

A. Navigeer naar "Beleid > houding"

B. Configureer de naam van de regel als "VPN_Posture_Policy_Win", vereist besturingssysteem als "Windows 10(All)", compliance module als "4.x of hoger", houding type als "AnyConnect" en

vereisten als "VPN_Posture_Requirement" zoals geconfigureerd in stap 9

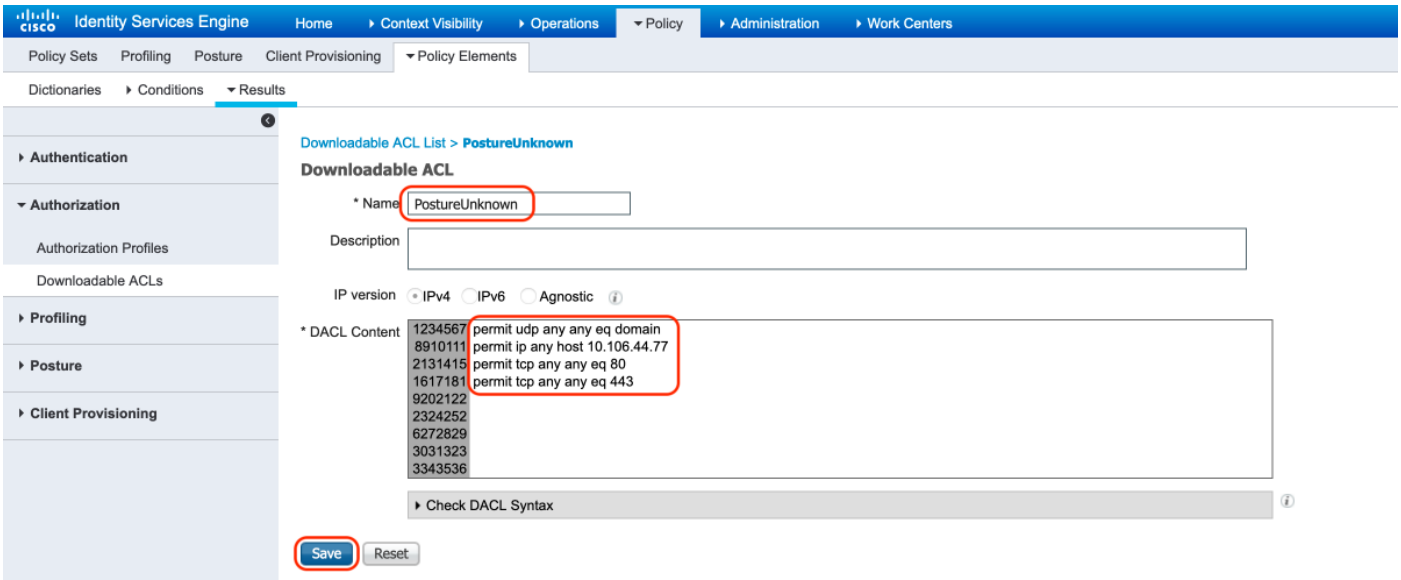


1. Dynamische ACL's (DACL's) maken

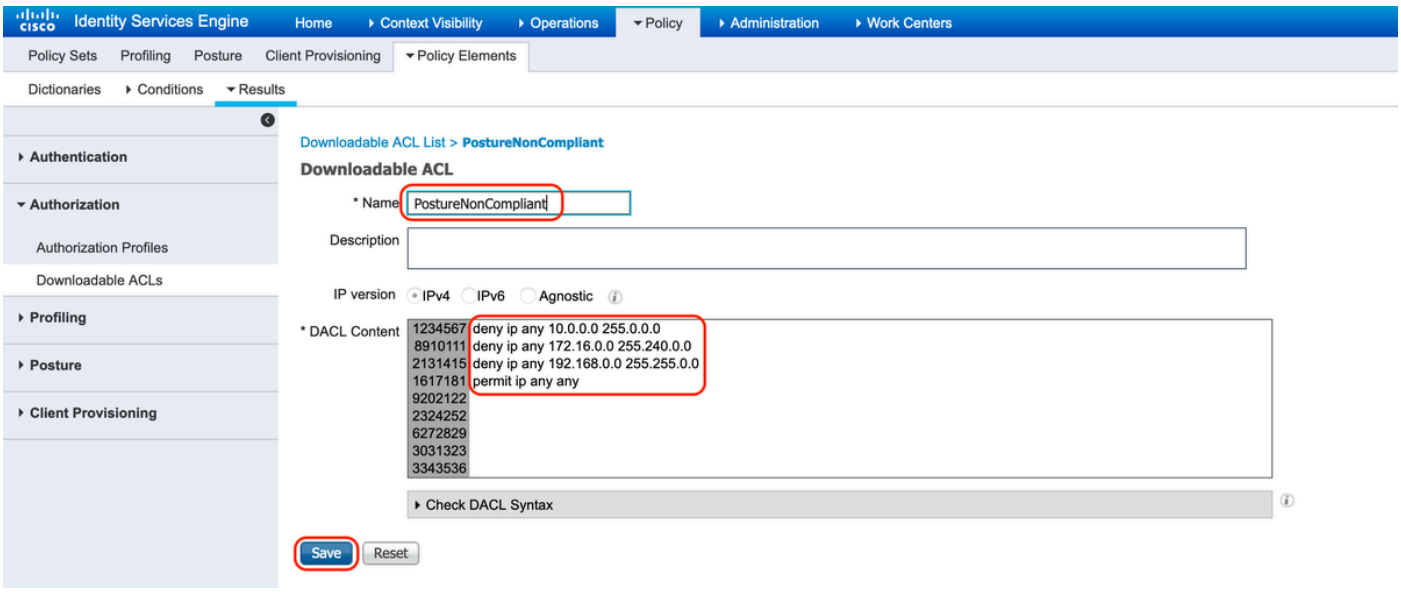
Navigeer naar "Policy > Policy Elements > Results > Authorisation > Downlodable ACLS" en maak de DACL's voor verschillende postuur statussen.

Dit document gebruikt de volgende DACL's.

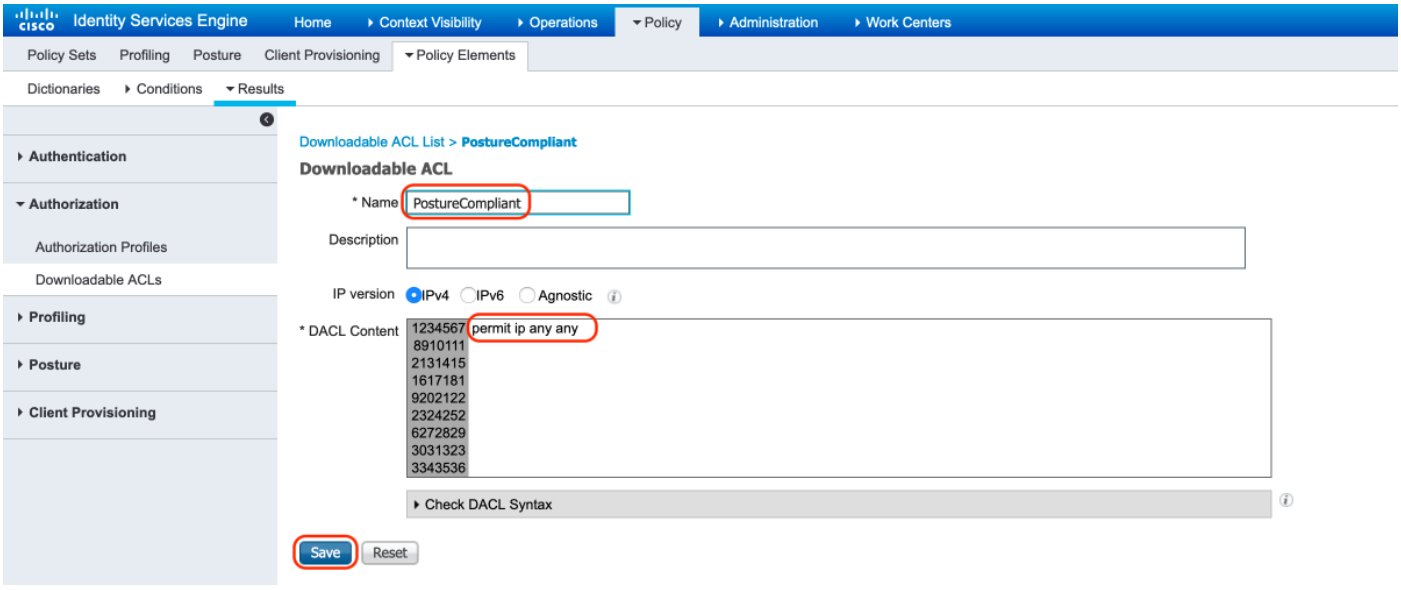
A. Positie Onbekend: maakt verkeer mogelijk naar DNS-, PSN-, HTTP- en HTTPS-verkeer



B. Houding niet conform: ontzegt toegang tot privé-subnetten en staat alleen internetverkeer toe



C. Posture Conformant: staat al verkeer voor Posture Conforme eindgebruikers toe



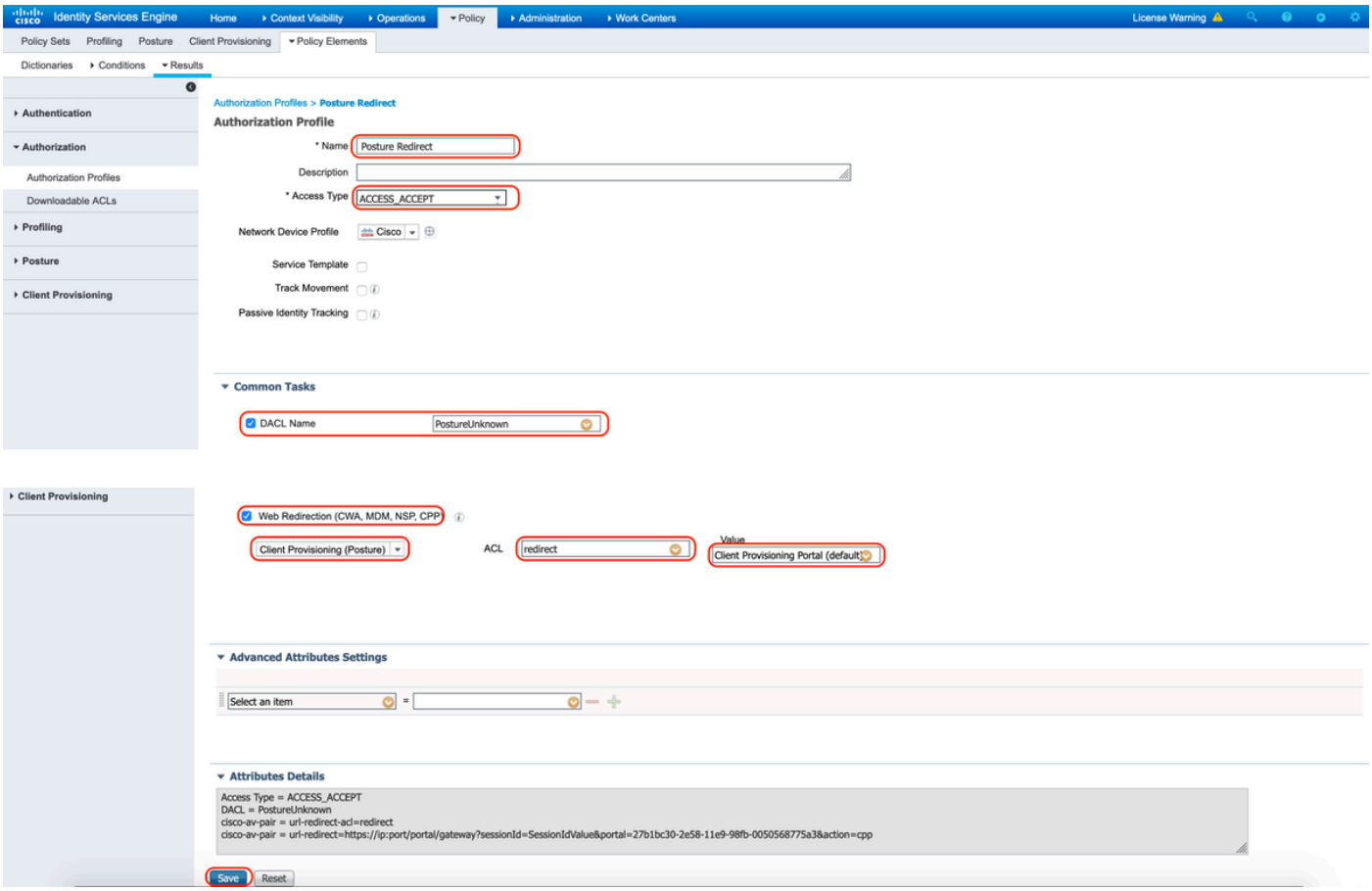
12. Autorisatieprofielen maken

Blader naar "Beleid > Beleidselementen > Resultaten > Autorisatie > Autorisatieprofielen".

A. Vergunningprofiel voor onbekend gedrag

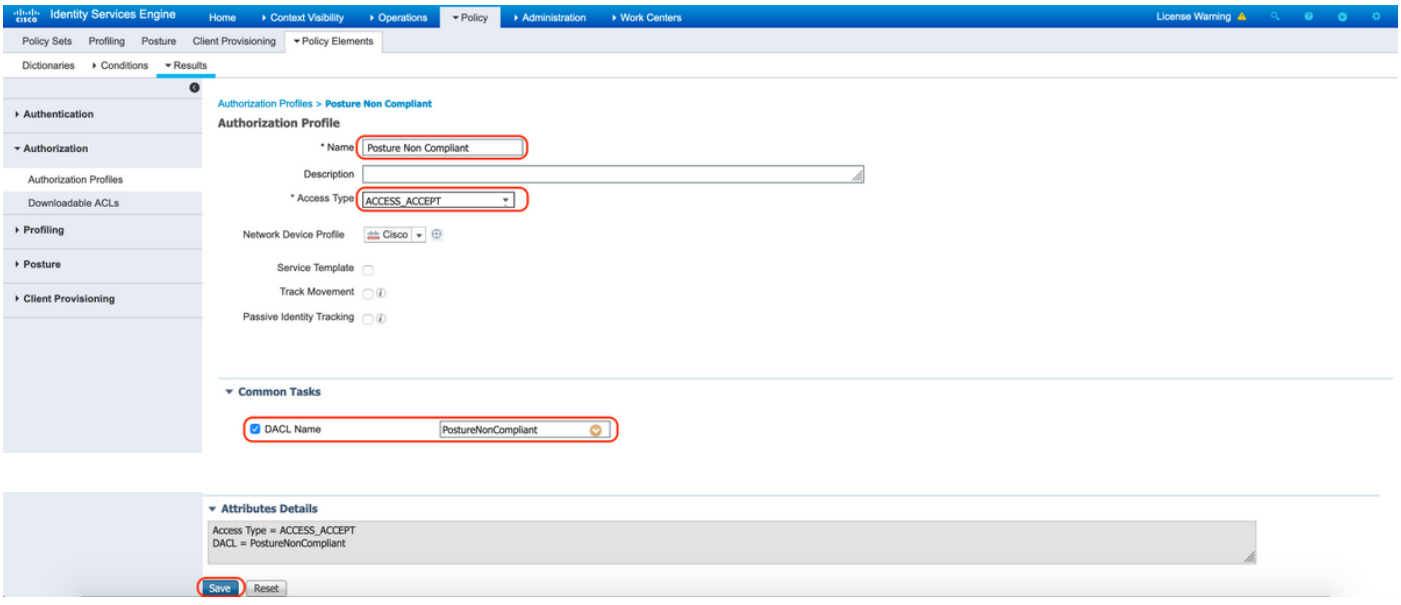
Selecteer DACL "PostureUnknown", controleer Web Redirection, selecteer Client Provisioning (Posture), configureer Redirect ACL-naam "redirect" (om te configureren op de ASA) en selecteer

het Client Provisioning-portal (standaard)



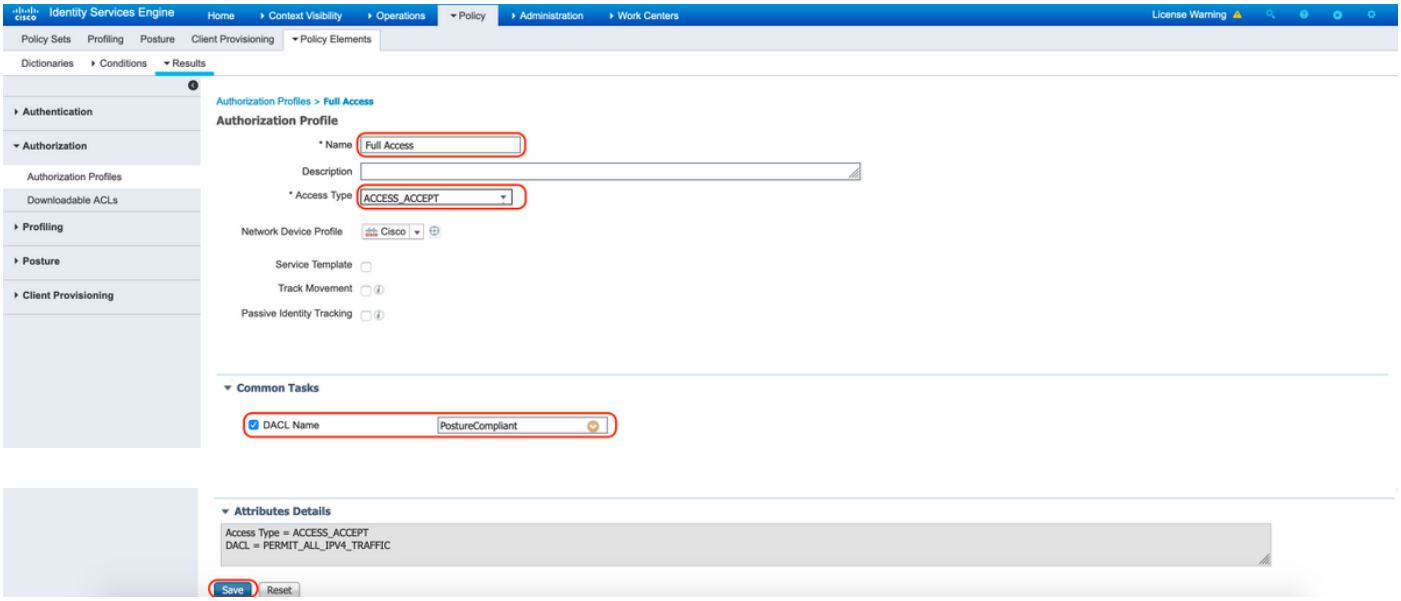
B. Vergunningsprofiel voor niet-conforme post

Selecteer DACL "PostureNonCompliant" om toegang tot het netwerk te beperken



C. Vergunningsprofiel voor de vervulling van de functie

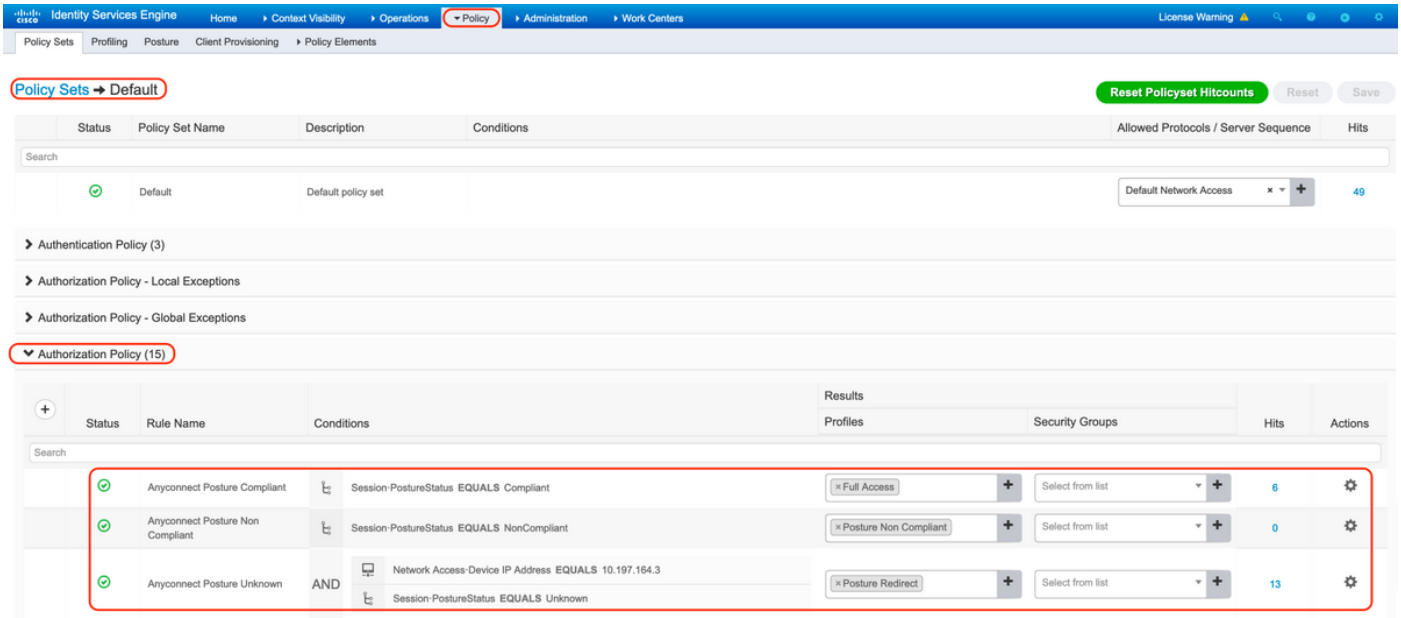
Selecteer DACL "PostureCompliant" om volledige toegang tot het netwerk mogelijk te maken



12. Vergunningsbeleid configureren

Gebruik de autorisatieprofielen die in de vorige stap zijn geconfigureerd om 3 autorisatiebeleid te configureren voor Posture Compliant, Posture Non-Compliant en Posture Unknown.

Algemene voorwaarde "Session: Posture Status" wordt gebruikt om de resultaten voor elk beleid te bepalen



Verifiëren

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

Om te verifiëren of de gebruiker is geverifieerd, voert u de volgende opdracht uit op de ASA.

<#root>

```
firebird(config)#
```

show vpn-sess detail anyconnect

```
Session Type: AnyConnect Detailed

Username     : _585b5291f01484dfd16f394be7031d456d314e3e62
Index        : 125
Assigned IP  : explorer.cisco.com     Public IP    : 10.197.243.143
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 16404                  Bytes Rx     : 381
Pkts Tx      : 16                     Pkts Rx      : 6
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy               Tunnel Group :
```

TG_SAML

```
Login Time   : 07:05:45 UTC Sun Jun 14 2020
Duration     : 0h:00m:16s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0ac5a4030007d0005ee5cc49
Security Grp : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 125.1
  Public IP    : 10.197.243.143
  Encryption   : none                   Hashing      : none
  TCP Src Port : 57244                  TCP Dst Port : 443
  Auth Mode    : SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : win
  Client OS Ver: 10.0.15063
  Client Type  : AnyConnect
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03052
  Bytes Tx     : 7973                   Bytes Rx     : 0
  Pkts Tx      : 6                      Pkts Rx      : 0
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
  Tunnel ID    : 125.2
```

```
  Assigned IP  : explorer.cisco.com     Public IP    : 10.197.243.143
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-RSA-AES256-GCM-SHA384
  Encapsulation: TLSv1.2                TCP Src Port : 57248
  TCP Dst Port : 443                    Auth Mode    : SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03052
  Bytes Tx     : 7973                   Bytes Rx     : 0
  Pkts Tx      : 6                      Pkts Rx      : 0
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  : #ACSACL#-IP-PostureUnknown-5ee45b05

DTLS-Tunnel:
  Tunnel ID    : 125.3
  Assigned IP  : explorer.cisco.com     Public IP    : 10.197.243.143
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2               UDP Src Port : 49175
  UDP Dst Port : 443                    Auth Mode    : SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03052
  Bytes Tx     : 458                    Bytes Rx     : 381
  Pkts Tx      : 4                      Pkts Rx      : 6
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  :
```

#ACSACL#-IP-PostureUnknown-5ee45b05

```
ISE Posture:
  Redirect URL : https://ise261.pusaxena.local:8443/portal/gateway?sessionId=0ac5a4030007d0005ee5cc49&po
  Redirect ACL : redirect
```

Nadat de posteringstoetsing is voltooid, wordt de gebruikerstoegang gewijzigd in volledige toegang zoals waargenomen in de DACL die in het veld "Filternaam" wordt gedrukt

<#root>

```
firebird(config)#
```

show vpn-sess detail anyconnect

```
Session Type: AnyConnect Detailed

Username     : _585b5291f01484dfd16f394be7031d456d314e3e62
Index        : 125
Assigned IP  : explorer.cisco.com     Public IP    : 10.197.243.143
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
```

```
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 16404                  Bytes Rx     : 381
Pkts Tx      : 16                     Pkts Rx      : 6
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy               Tunnel Group :
```

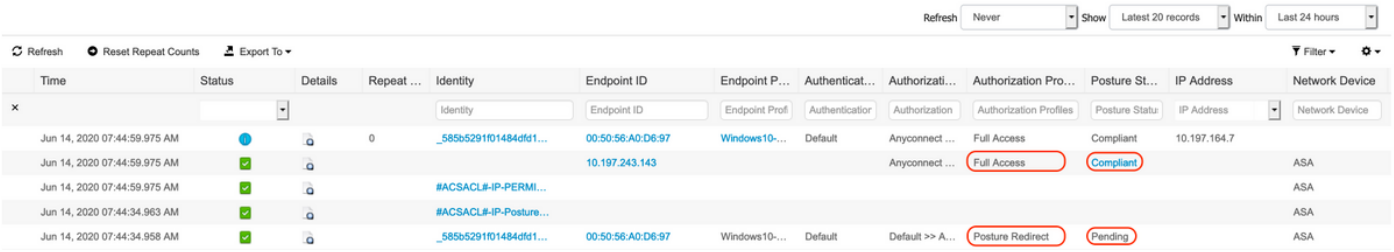
TG_SAML

```
Login Time   : 07:05:45 UTC Sun Jun 14 2020
Duration     : 0h:00m:36s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0ac5a4030007d0005ee5cc49
Security Grp : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 125.1
  Public IP    : 10.197.243.143
  Encryption   : none                   Hashing      : none
  TCP Src Port : 57244                  TCP Dst Port : 443
  Auth Mode    : SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : win
  Client OS Ver: 10.0.15063
  Client Type  : AnyConnect
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03052
  Bytes Tx     : 7973                   Bytes Rx     : 0
  Pkts Tx      : 6                      Pkts Rx      : 0
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
  Tunnel ID    : 125.2
  Assigned IP  : explorer.cisco.com     Public IP    : 10.197.243.143
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-RSA-AES256-GCM-SHA384
  Encapsulation: TLSv1.2                TCP Src Port : 57248
  TCP Dst Port : 443                    Auth Mode    : SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03052
  Bytes Tx     : 7973                   Bytes Rx     : 0
  Pkts Tx      : 6                      Pkts Rx      : 0
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

DTLS-Tunnel:
  Tunnel ID    : 125.3
  Assigned IP  : explorer.cisco.com     Public IP    : 10.197.243.143
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2               UDP Src Port : 49175
  UDP Dst Port : 443                    Auth Mode    : SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03052
  Bytes Tx     : 458                    Bytes Rx     : 381
  Pkts Tx      : 4                      Pkts Rx      : 6
```

```
  Pkts Tx Drop : 0                    Pkts Rx Drop : 0
  Filter Name  :

#ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3
```

Om te verifiëren of de autorisatie met succes is uitgevoerd op ISE, navigeer dan naar "Operations > RADIUS > Live logs"

In dit deel wordt de relevante informatie over de gemachtigde gebruiker weergegeven, d.w.z. identiteit, autorisatieprofiel, autorisatiebeleid en postuur.

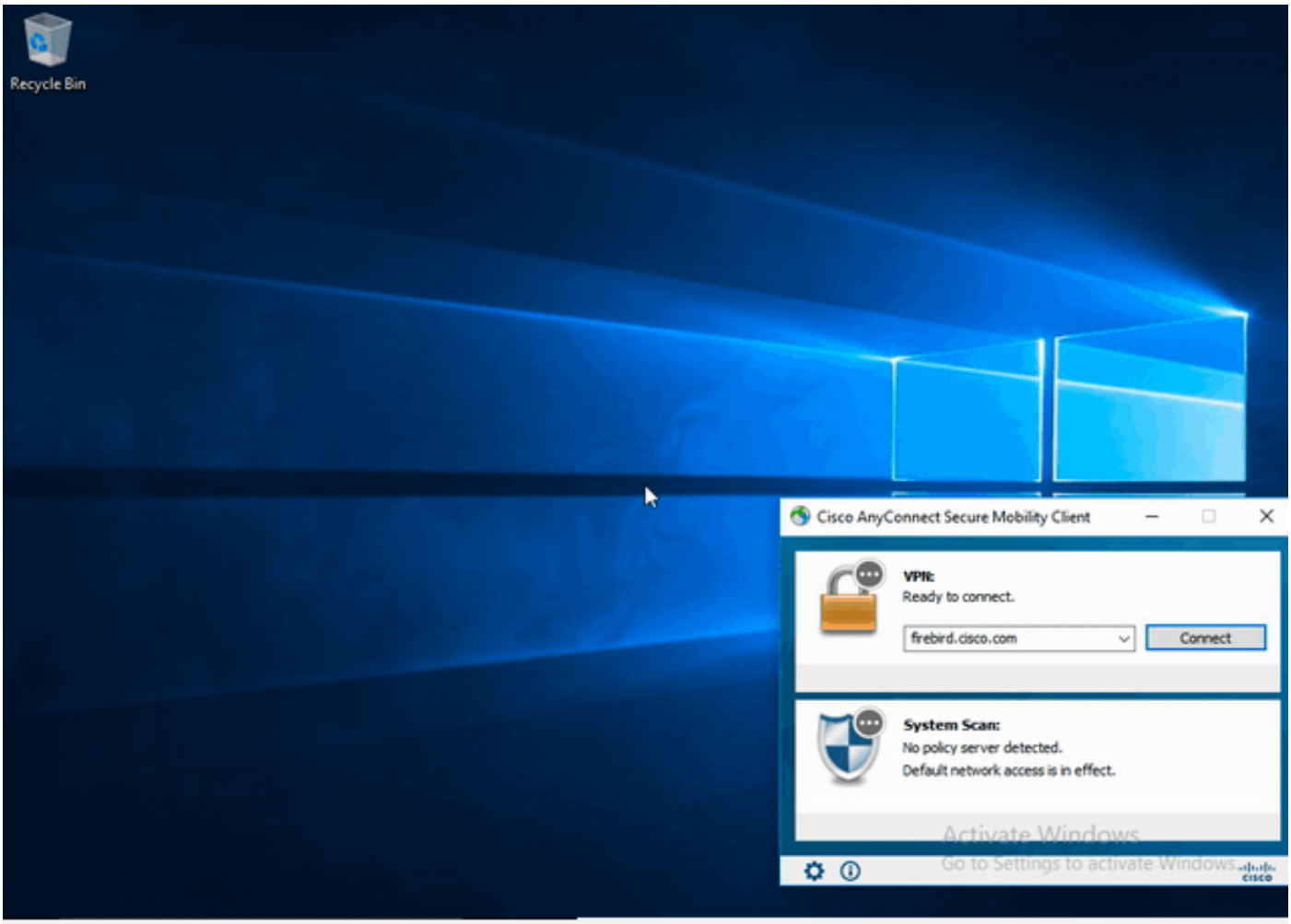


Opmerking: voor aanvullende posture validatie op ISE, raadpleegt u de volgende documentatie: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-acces.html#anc7

Om de verificatiestatus op het Duo Admin Portal te verifiëren, klikt u op de "Reports" aan de linkerkant van het Admin Panel dat het Verificatielogboek toont.
Meer informatie: https://duo.com/docs/administration#reports

Gebruik de volgende link om debug-vastlegging voor Duo Access Gateway te bekijken: https://help.duo.com/s/article/1623?language=en_US

Gebruikerservaring



Problemen oplossen

Deze sectie bevat informatie voor het troubleshooten van de configuratie.

Opmerking: raadpleeg Belangrijke informatie over debug-opdrachten voordat u debug-opdrachten gebruikt.

Let op: op de ASA kunt u verschillende debugniveaus instellen, standaard wordt niveau 1 gebruikt. Als u het debug-niveau wijzigt, kan de hoeveelheid debug-informatie toenemen. Wees hier voorzichtig mee, vooral in productieomgevingen.

Bij de meeste problemen met SAML gaat het om een fout-configuratie die u kunt vinden door de SAML-configuratie te controleren of door debugs uit te voeren.

"debug webvpn saml 255" kan worden gebruikt om de meeste problemen op te lossen, maar in scenario's waar dit debug geen nuttige informatie biedt, kunnen extra debugs worden uitgevoerd:

```
debug webvpn 255
debug webvpn anyconnect 255
debug webvpn session 255
debug webvpn request 255
```

Als u problemen met verificatie en autorisatie bij ASA wilt oplossen, gebruikt u de volgende debug-opdrachten:

```
debug radius all
debug aaa authentication
debug aaa authorization To troubleshoot Posture related issues on ISE, set the following attributes to
```

```
posture (ise-psc.log)
portal (guest.log)
provisioning (ise-psc.log)
runtime-AAA (prrt-server.log)
nsf (ise-psc.log)
nsf-session (ise-psc.log)
swiss (ise-psc.log)
```

Opmerking: voor een gedetailleerde postenstroom en probleemoplossing voor AnyConnect en ISE raadpleegt u de volgende link:
ISE-poortstijlvergelijking voor Pre en Post 2.2

Foutopsporingslogboeken voor Duo Access Gateway interpreteren en problemen oplossen
https://help.duo.com/s/article/5016?language=en_US

Gerelateerde informatie

https://www.youtube.com/watch?v=W6bE2GTU0Is&
https://duo.com/docs/cisco#asa-ssl-vpn-using-saml

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-acces.html#anc0

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.