

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

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Traffic Flow](#)

[Configuraties](#)

[- Configuratie Duo Admin Portal](#)

[- Configuratie Duo Access Gateway \(DAG\)](#)

[- ASA-configuratie](#)

[- ISE-configuratie](#)

[Verifiëren](#)

[Gebruikerservaring](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

---

## 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

---

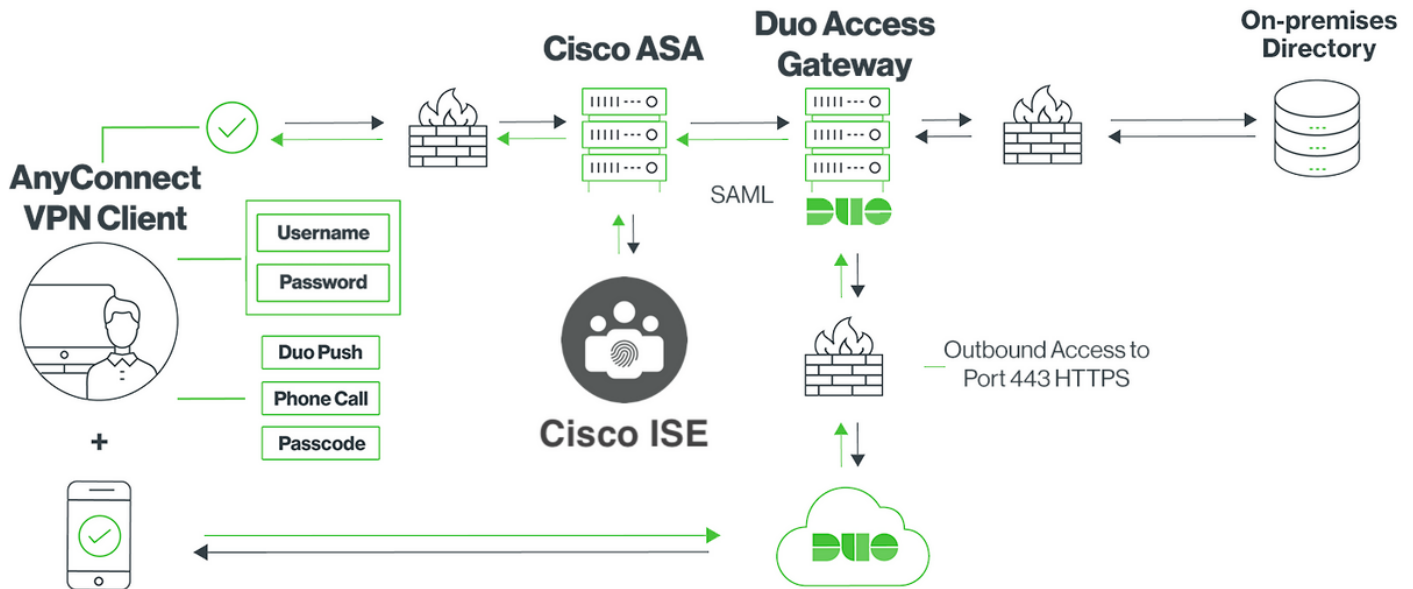
 Opmerking: AnyConnect Embedded Browser, gebruikt in deze implementatie, vereist ASA op 9.7(1)24, 9.8(2)28, 9.9(2)1 of hogere versie van elke release en AnyConnect versie 4.6 of hoger.

---

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

### Netwerkdigram



## 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

The screenshot shows the Duo Admin Portal interface. The breadcrumb trail is "Dashboard > Applications > Protect an Application". The search bar contains "ASA". The table below shows the following applications:

Application	2FA	Single Sign-On (if available)	Documentation	Action
Asana	2FA	Duo Access Gateway (self-hosted)	<a href="#">Documentation</a>	<a href="#">Protect</a>
Cisco ASA	2FA	Duo Access Gateway (self-hosted)	<a href="#">Documentation</a>	<a href="#">Protect</a>
Cisco ASA	2FA	Single Sign-On (hosted by Duo)	<a href="#">Documentation</a>	<a href="#">Configure</a>

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

The screenshot shows the 'Cisco ASA - Duo Access Gateway' configuration page. The left sidebar contains navigation options like 'Device Insight', 'Policies', 'Applications', 'Users', 'Groups', 'Endpoints', '2FA Devices', 'Administrators', 'Reports', 'Settings', 'Billing', 'Need Help?', 'Account ID', 'Deployment ID', and 'Helpful Links'. The main content area is titled 'Configure Cisco ASA' and includes a 'Reset Secret Key' button. Below this, there is a 'Service Provider' section with the following fields:

- Base URL:** firebird.cisco.com (with a red box around the input field)
- Tunnel Group:** TG\_SAML (with a red box around the input field)
- Custom attributes:**  Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.
- Mail attribute:** sAMAccountName,mail (with a red box around the input field)

At the bottom of the configuration section, there is a blue 'Save Configuration' button with a red box around it.

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

Device Insight  
Policies  
**Applications**  
Protect an Application  
Single Sign-On  
Users  
Groups  
Endpoints  
2FA Devices  
Administrators  
Reports  
Settings  
Billing

Need Help?  
Chat with Tech Support  
Email Support  
Call us at 1-855-386-2884

Account ID  
2010-1403-48  
Deployment ID  
DU057  
Helpful Links  
Documentation

## Cisco ASA - Duo Access Gateway

Authentication Log | Remove Application

### Configure Cisco ASA

Reset Secret Key

To set up this application, install the Duo Access Gateway and then configure your service provider. [View Cisco ASA SAML SSO instructions](#)

Next step: [Download your configuration file](#)

#### Service Provider

**Base URL**  
firebird.cisco.com  
Enter the Cisco ASA Base URL.

**Tunnel Group**  
TG\_SAML  
Enter the Tunnel Group you are protecting with SSO.

**Custom attributes**  Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.

**Mail attribute**  
sAMAccountName,mail  
The attribute containing the email address of the user.

Save Configuration

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

admin-77d04ebc.duosecurity.com/applications

Cisco Study | Cisco Tools | Mix | SourceFire | VPN | AAA | ASA | IFT 6.7

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48 | ciscoduobr

Dashboard > Applications

## Applications

SSO Setup Guide | Protect an Application

Export | Search

Name	Type	Application Policy	Group Policies
Cisco ASA - Duo Access Gateway	Cisco ASA - Duo Access Gateway		

1 total

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

The screenshot shows the Duo Admin console interface. On the left is a dark sidebar with the Duo logo and a menu containing: Dashboard, Device Insight, Policies, Applications, **Users** (highlighted), **Add User** (highlighted), Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, Groups, and Endpoints. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below it is a breadcrumb trail: Dashboard > Users > Add User. The main heading is "Add User". A sub-section titled "Adding Users" contains the text "Most applications allow users to enroll themselves after they complete primary authentication." and a link "Learn more about adding users". The "Username" field contains the text "duouser" and has a note below it: "Should match the primary authentication username." At the bottom of the form is a blue "Add User" button.

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

The screenshot shows the Duo Admin console interface for adding a phone. The sidebar is identical to the previous screenshot, with "Users" and "Add User" highlighted. The main content area has the same search bar and breadcrumb trail: Dashboard > Users > duouser > Add Phone. The main heading is "Add Phone". A sub-section contains a link "Learn more about Activating Duo Mobile". The "Type" field has two radio buttons: "Phone" (selected) and "Tablet". The "Phone number" field contains a dropdown menu showing the flag for the Netherlands and the text "+91 9xxx-xxx-xxx", with a link "Show extension field" to its right. Below the field is the text "Optional. Example: '+91 91234 56789'". At the bottom of the form is a blue "Add Phone" button.

Activeer "Duo Mobile" voor de specifieke gebruiker

## Device Info

[Learn more about Activating Duo Mobile](#)



Not using Duo Mobile

[Activate Duo Mobile](#)



**Model**

Unknown



**OS**

Generic Smartphone



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:



- Dashboard
- Device Insight
- Policies
- Applications
- Users
- Groups
- Endpoints
- 2FA Devices**
- Phones
- Hardware Tokens
- WebAuthn & U2F
- Administrators
- Reports
- Settings
- Billing
- Need Help?**
- [Chat with Tech Support](#)
- [Email Support](#)
- Call us at 1-855-386-2884

[Dashboard](#) > [Phone: +91](#) > [Activate Duo Mobile](#)

# Activate Duo Mobile

A new Duo Mobile activation code has been generated, and any old credentials have been invalidated. activation instructions to the user by SMS.

Phone

Installation instructions

Send installation instructions via SMS

*Welcome to Duo! Please install Duo Mobile from your app store.*

Activation instructions

Send activation instructions via SMS

*To activate the app, tap and open this link with Duo Mobile:  
<https://m-77d04ebc.duosecurity.com/activate/YB5ucEisJAq1YIBN5ZrT>*

[Send Instructions by SMS](#)

or [skip this step](#)

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

Dashboard > Phones > Phone: +91 [redacted]

+91 [redacted] Send SMS Passcodes... | [redacted]

**Shared phone**  
This phone is attached to multiple users.

**duouser** +91 [redacted] **testing 123** +91 [redacted] [Attach a user](#)

Authentication devices can share multiple users

**Device Info**  
[Learn more about Activating Duo Mobile](#)

Using Duo Mobile [Reactivate Duo Mobile](#) **Model** Unknown **OS** Generic Smartphone

## - 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"

## Configure Sources

Configure authentication source settings below. Changes made to non-active authentication sources will take effect when made active.

Source type	<input type="text" value="Active Directory"/> Specify the authentication source to configure.
Status:	<input checked="" type="checkbox"/> LDAP Bind Succeeded <input checked="" type="checkbox"/> ldap://10.197.243.110
Server	<input type="text" value="10.197"/> <input type="text" value="389"/> Hostname and port of your Active Directory. The port is typically 389 for cleartext LDAP and STARTTLS, and 636 for LDAPS. Hostnames can be comma separated for failover functionality. For example: ad1.server.com,ad2.server.com,10.1.10.150
Transport type	<input checked="" type="radio"/> CLEAR <input type="radio"/> LDAPS <input type="radio"/> STARTTLS This setting controls whether the communication between Active Directory and the Duo Access Gateway is encrypted.
Attributes	<input type="text" value="sAMAccountName,mail"/> Specify attributes to retrieve from the AD server. For example: sAMAccountName,mail.
Search base	<input type="text" value="CN=Users,DC=dmoudgil,DC=local"/> The DNs which will be used as a base for the search. Enter one per line. They will be searched in the order given.
Search attributes	<input type="text" value="sAMAccountName"/> Specify attributes the username should match against. For example: sAMAccountName,mail.
Search username	<input type="text" value="iseadmin"/> The username of an account that has permission to read from your Active Directory. We recommend creating a service account that has read-only access.
Search password	<input type="password" value="•••••"/> The password corresponding to the search username specified above.
<input type="button" value="Save Settings"/>	

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

### Set Active Source

Specify the source that end-users will use for primary authentication.

Source type

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

## Applications


### Add Application

Create a SAML application in the Duo Admin Panel. Then, download the provided configuration file and upload it here.

Configuration file

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

### Applications

Name	Type	Logo	
<input type="text" value="Cisco ASA - Duo Access Gateway"/>	Cisco ASA		<input type="button" value="Delete"/>

7. Download onder het submenu "Metadata" de XML-metadatas 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

**Metadata** [Recreate Certificate](#)

Information for configuring applications with Duo Access Gateway. [Download XML metadata.](#)

Certificate: /C=US/ST=M/I/L=Ann Arbor/O=Duo Security, Inc. [Download certificate](#)

Expiration: 2030-04-30 18:57:14

SHA-1 Fingerprint: [REDACTED]

SHA-256 Fingerprint: [REDACTED]

SSO URL	<a href="https://explorer.cisco.com/dag/saml2/idp/SSOService.php">https://explorer.cisco.com/dag/saml2/idp/SSOService.php</a>
Logout URL	<a href="https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer">https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer</a>
Entity ID	<a href="https://explorer.cisco.com/dag/saml2/idp/metadata.php">https://explorer.cisco.com/dag/saml2/idp/metadata.php</a>
Error URL	<a href="https://explorer.cisco.com/dag/module.php/duosecurity/du">https://explorer.cisco.com/dag/module.php/duosecurity/du</a>

## - ASA-configuratie

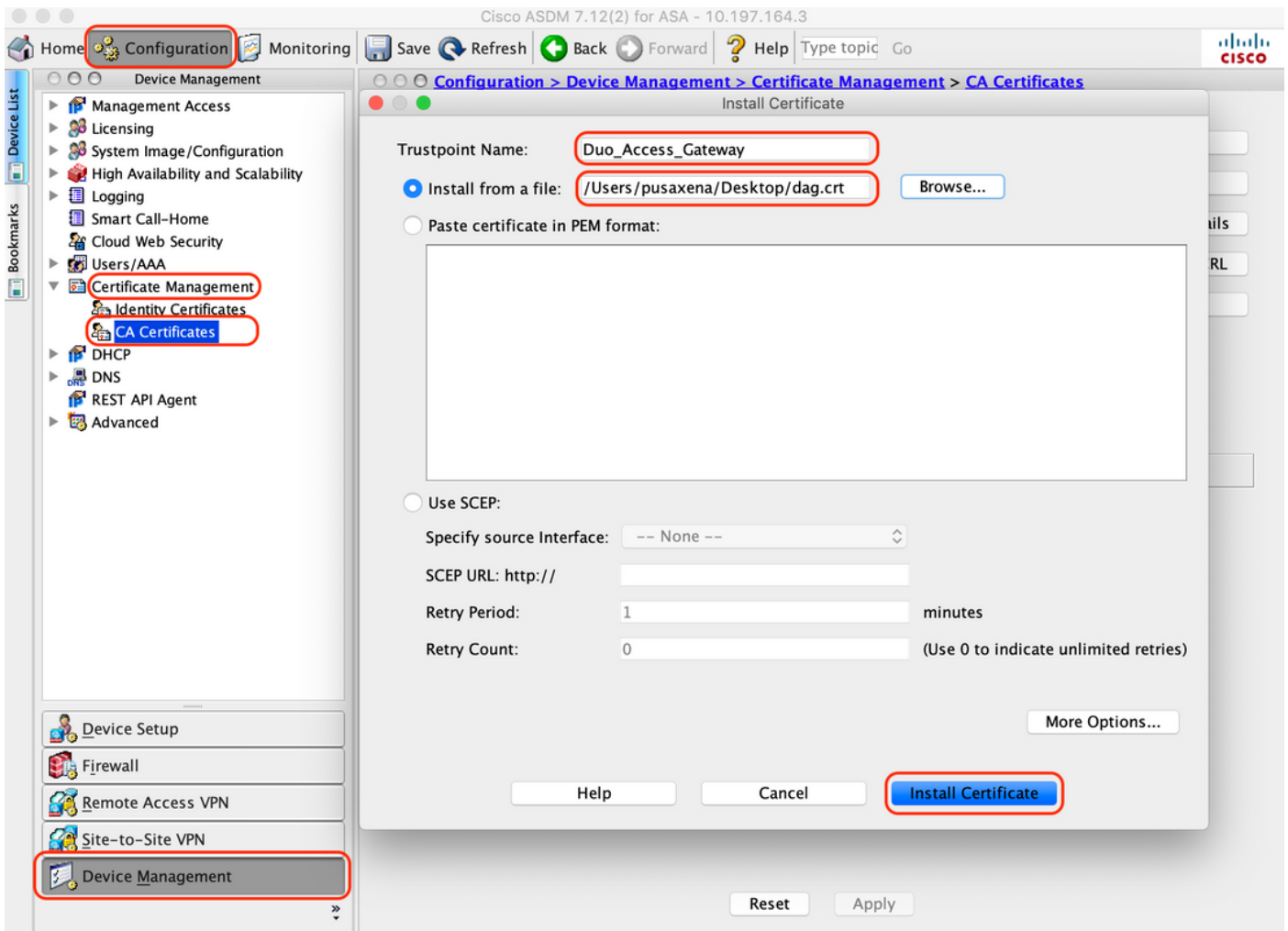
Deze paragraaf bevat informatie over het configureren van ASA voor SAML IDP-verificatie en basisconfiguratie van AnyConnect. Het document biedt ASDM-configuratiestappen en CLI-loopconfiguratie voor het overzicht.

### 1. Certificaat voor Duo Access Gateway uploaden

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

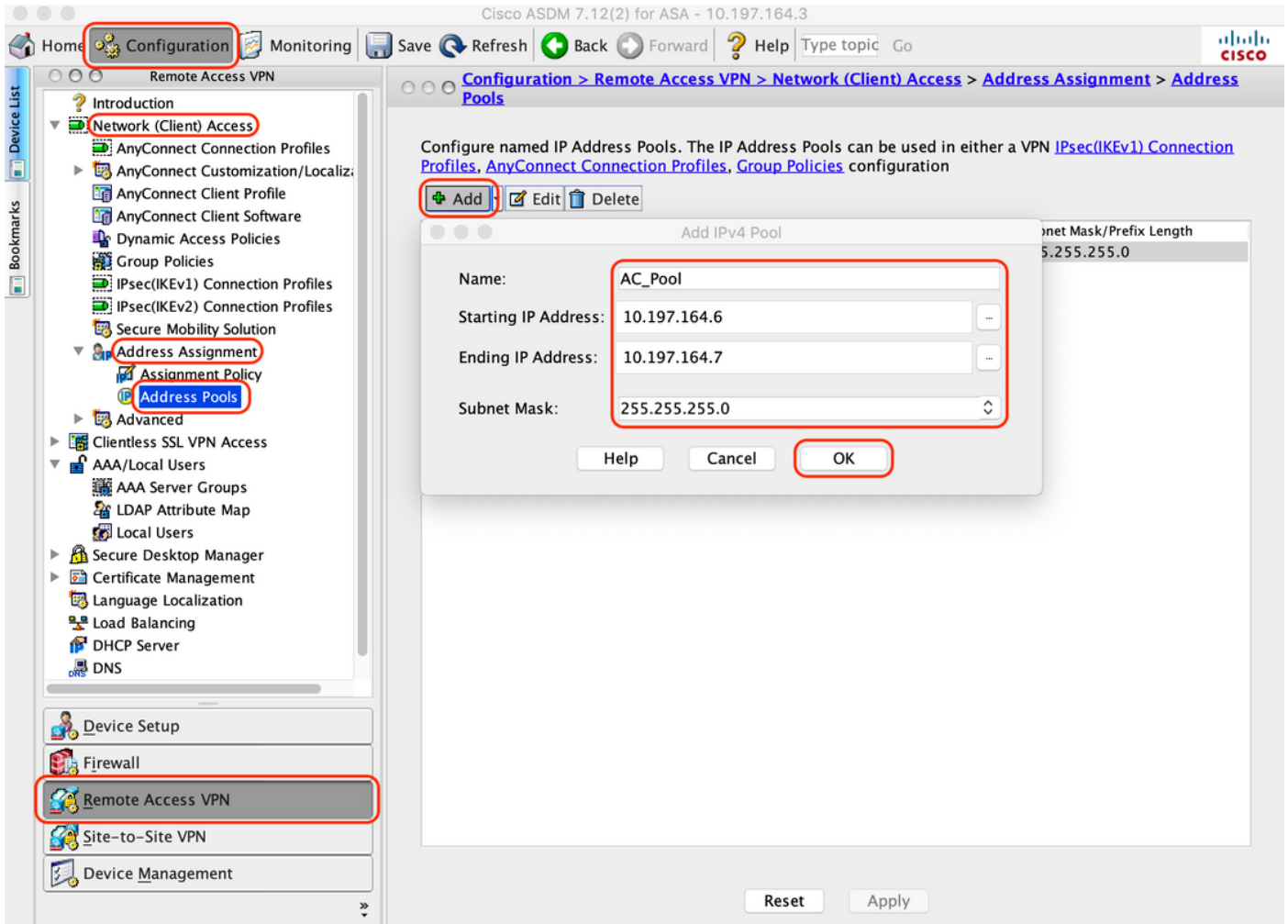
B. Configureer op de "Install Certificate Page" de Trustpoint Name: Duo\_Access\_Gateway

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 > Netwerктоegang (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"

The screenshot shows the Cisco Configuration Assistant interface. The left sidebar contains a navigation tree with 'Remote Access VPN' selected. The main window displays the 'AAA Server Groups' configuration page. A modal dialog box titled 'Add AAA Server Group' is open, showing the following configuration:

- Server Group: ISE
- Protocol: RADIUS
- Accounting Mode: Single (selected)
- Reactivation Mode: Depletion (selected)
- 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: [Dropdown]

The 'OK' button is highlighted with a red box. The 'Remote Access VPN' and 'AAA Server Groups' menu items in the sidebar are also highlighted with red boxes.

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



Cisco ASDM 7.12(2) for ASA - 10.197.164.3

Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

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

Add AAA Server

Server Group: ISE

Interface Name: outside

Server Name or IP Address: 10.106.44.77

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key: [Redacted]

Common Password: [Redacted]

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable:

SDI Messages

Message Table

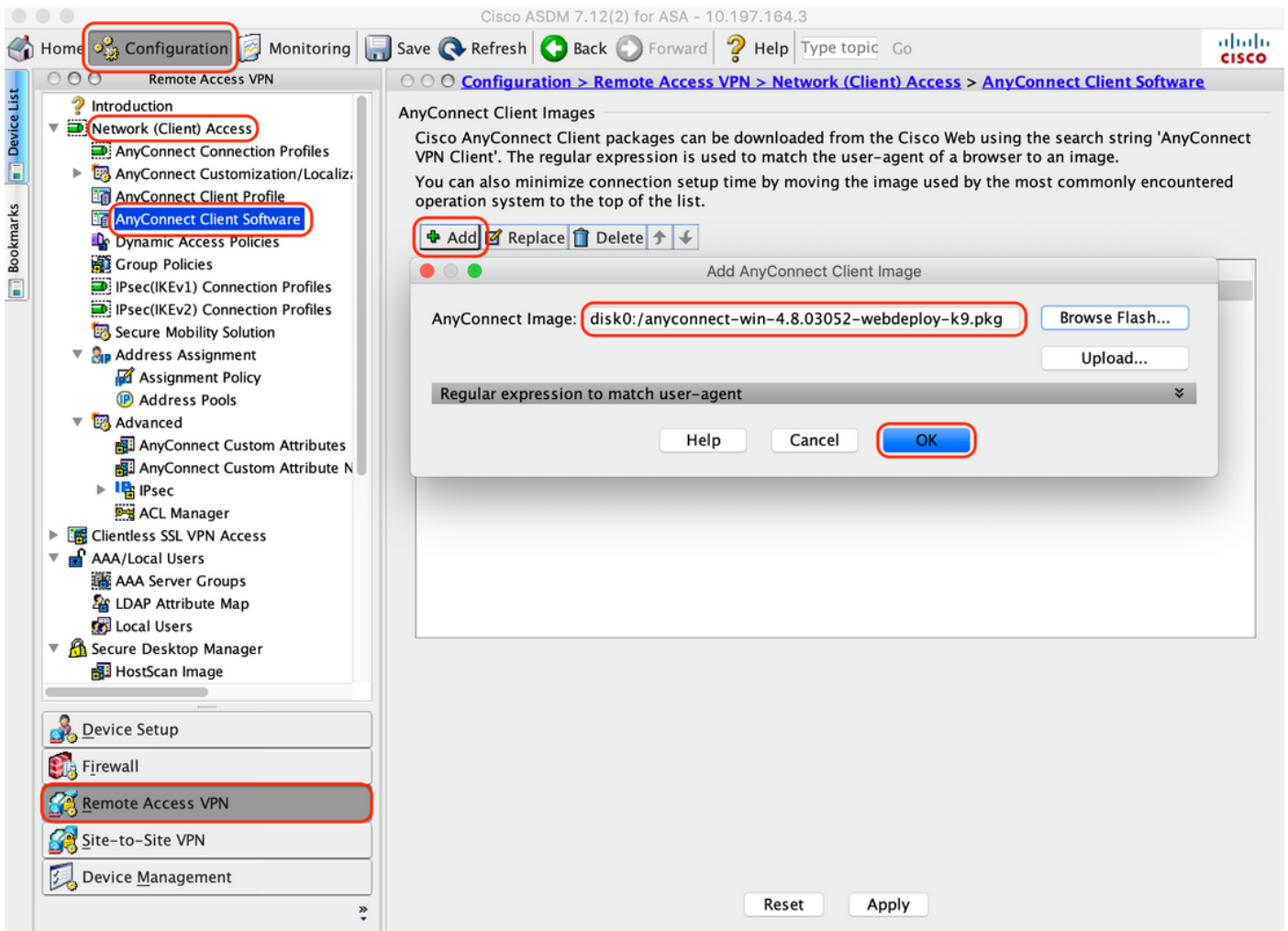
Help Cancel OK

Reset Apply

#### 4. Toewijzing van AnyConnect-clientsoftware

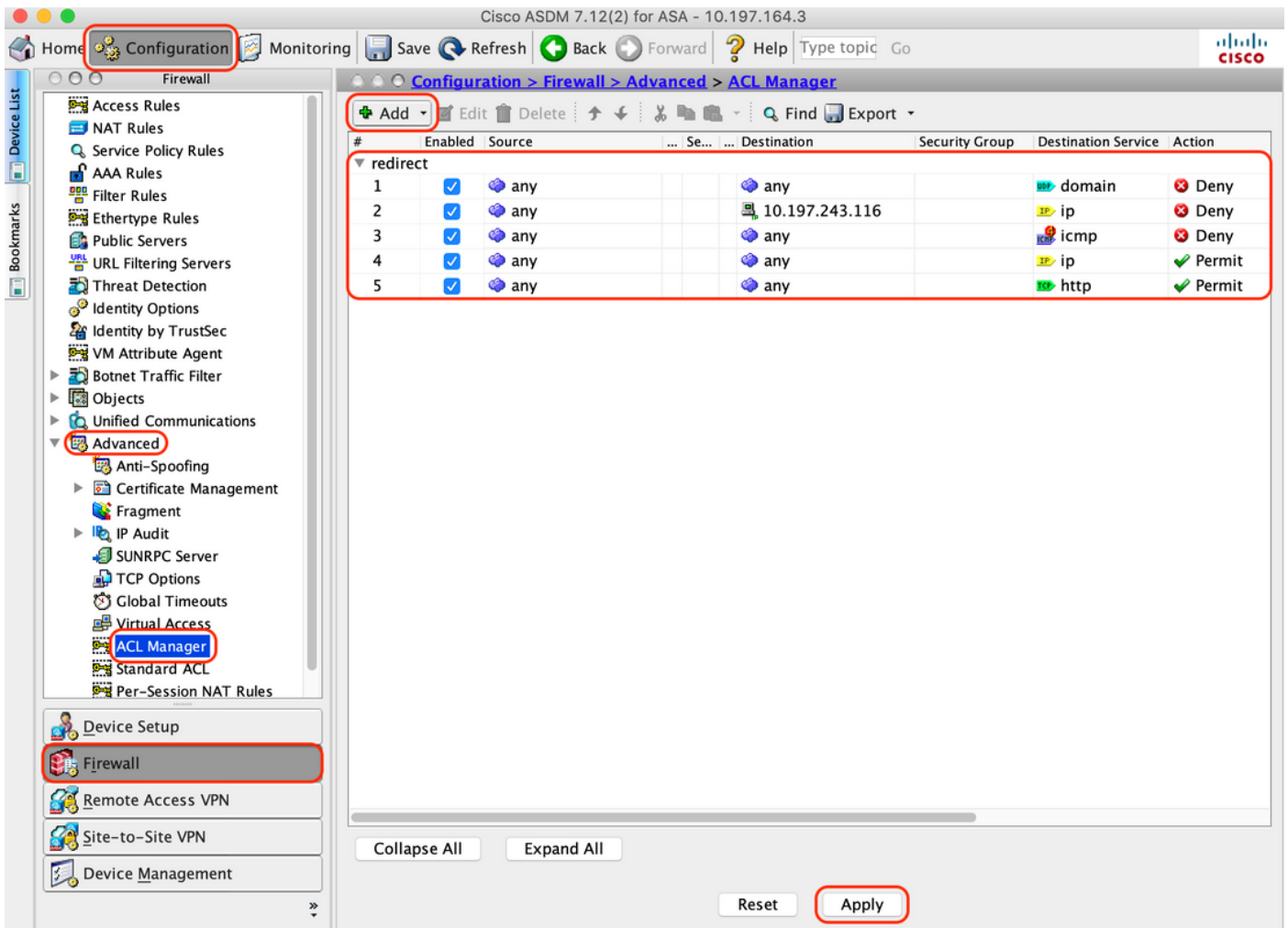
A. Breng de AnyConnect-clientsoftware in kaart met webimplementatieafbeelding 4.8.03052 voor Windows die voor WebVPN moet worden gebruikt

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



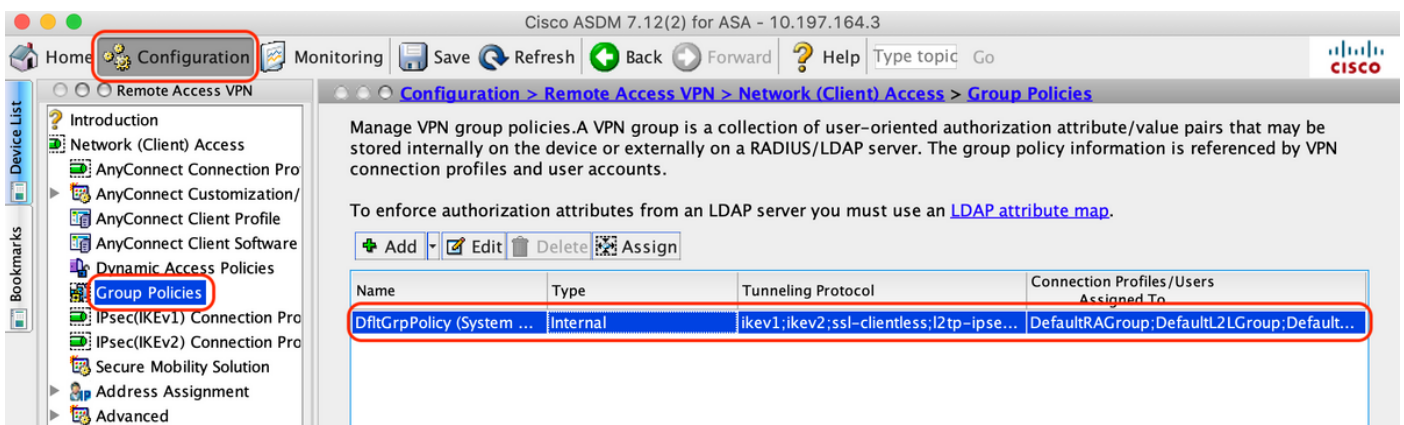
5. Configureer de omleiding van ACL die als resultaat van ISE is ingedrukt

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

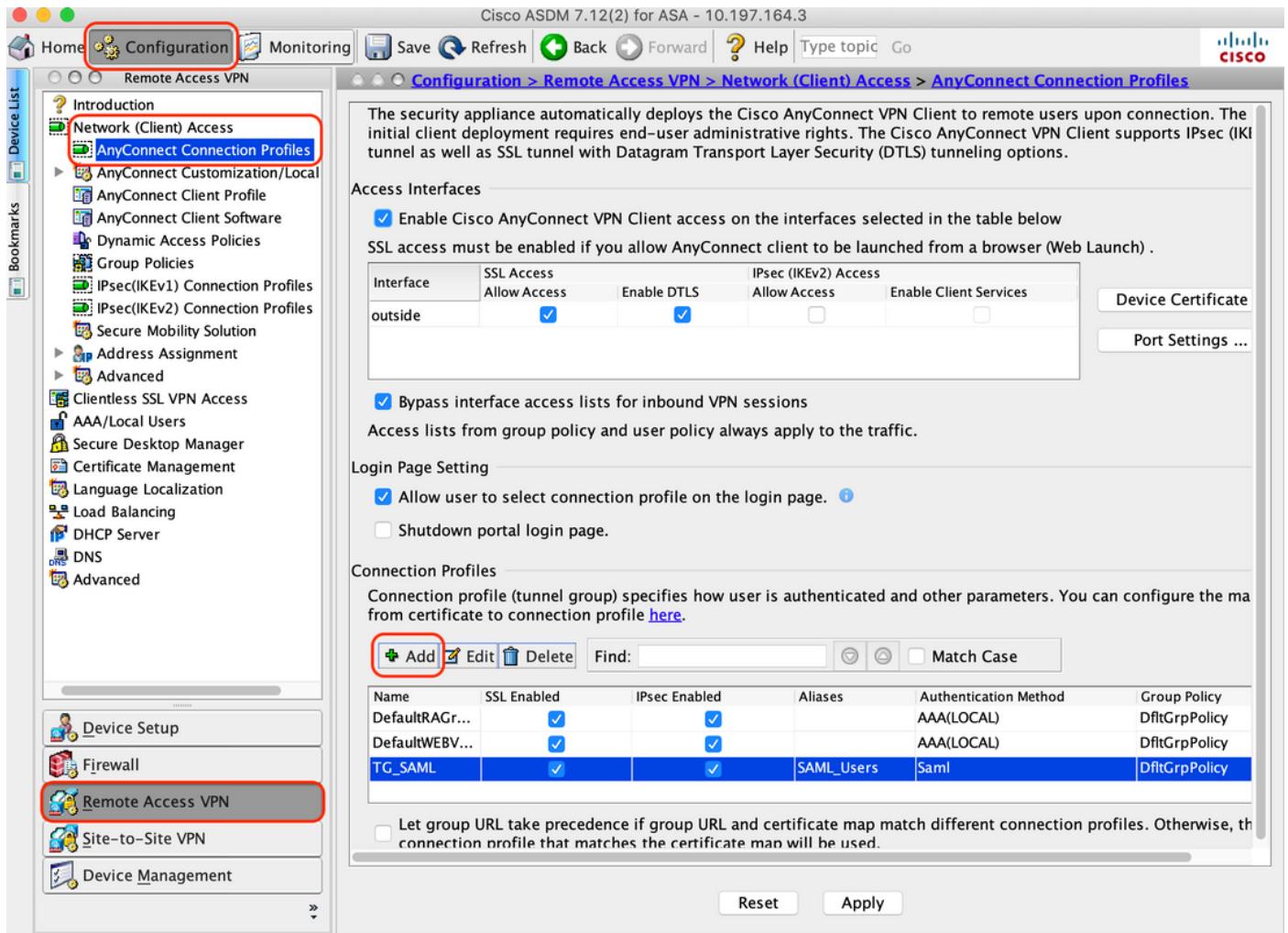
A. Bij deze instelling wordt gebruikgemaakt van het standaardgroepsbeleid dat kan worden bekeken op: "Configuration > Remote Access VPN > Network (Client) Access > Group Policies"



## 7. Verbindingsprofiel configureren

A. Een nieuw verbindingprofiel 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

The screenshot shows the configuration page for a SAML Identity Provider. The left sidebar has 'Basic' selected and 'Advanced' collapsed. The main area contains the following sections:

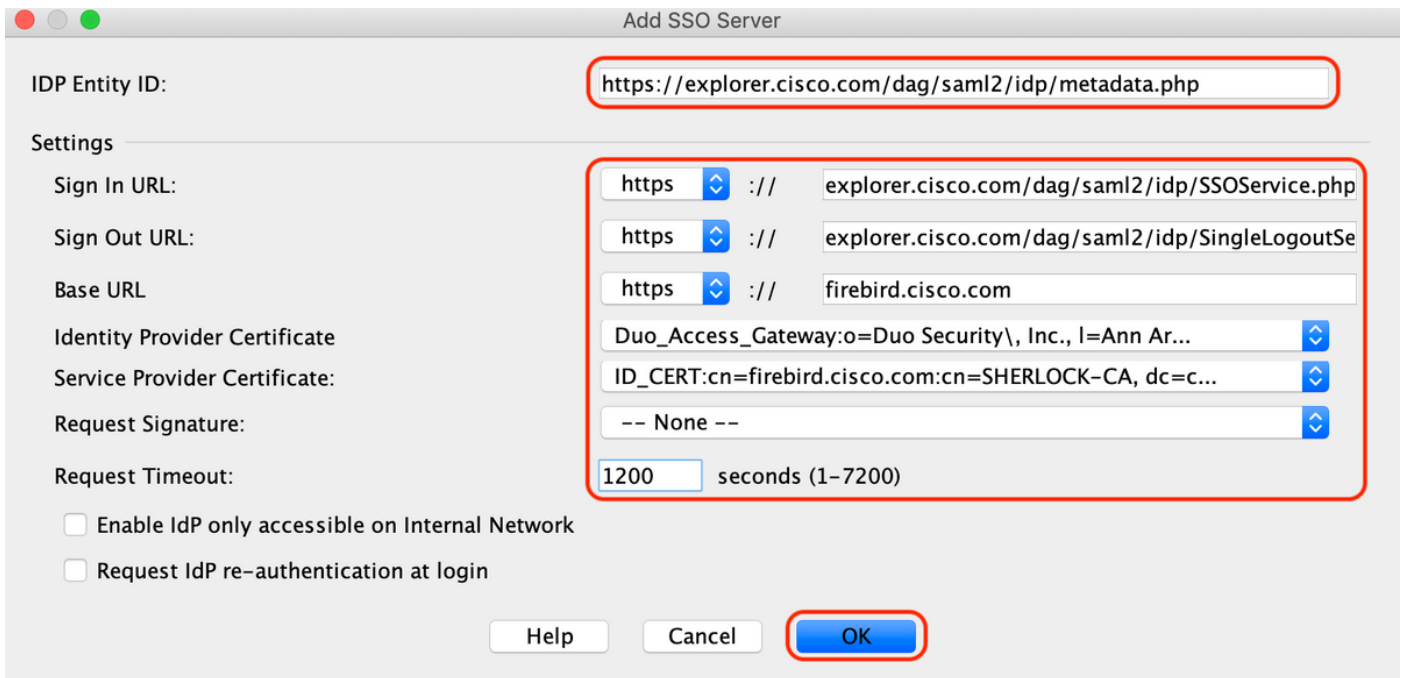
- Name:** TG\_SAML
- Aliases:** SAML\_Users
- Authentication:**
  - Method:** SAML
  - AAA Server Group:** LOCAL (with a 'Manage...' button and a checkbox for 'Use LOCAL if Server Group fails')
- SAML Identity Provider:**
  - SAML Server:** https://explorer.cisco.com/dag/saml2/idp/metadata.php (with a 'Manage...' button)
- Client Address Assignment:**
  - DHCP Servers:** (empty field)
  - None** (selected), DHCP Link, DHCP Subnet
  - Client Address Pools:** AC\_Pool (with a 'Select...' button)
  - Client IPv6 Address Pools:** (empty field, with a 'Select...' button)
- Default Group Policy:**
  - Group Policy:** DfltGrpPolicy (with a 'Manage...' button)
  - (Following fields are linked to attribute of the group policy selected above.)
  - Enable SSL VPN client protocol
  - Enable IPsec(IKEv2) client protocol
  - DNS Servers:** (empty field)
  - WINS Servers:** (empty field)
  - Domain Name:** (empty field)

At the bottom, there is a 'Find:' search bar, 'Next' and 'Previous' navigation buttons, and 'Help', 'Cancel', and 'OK' buttons.

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

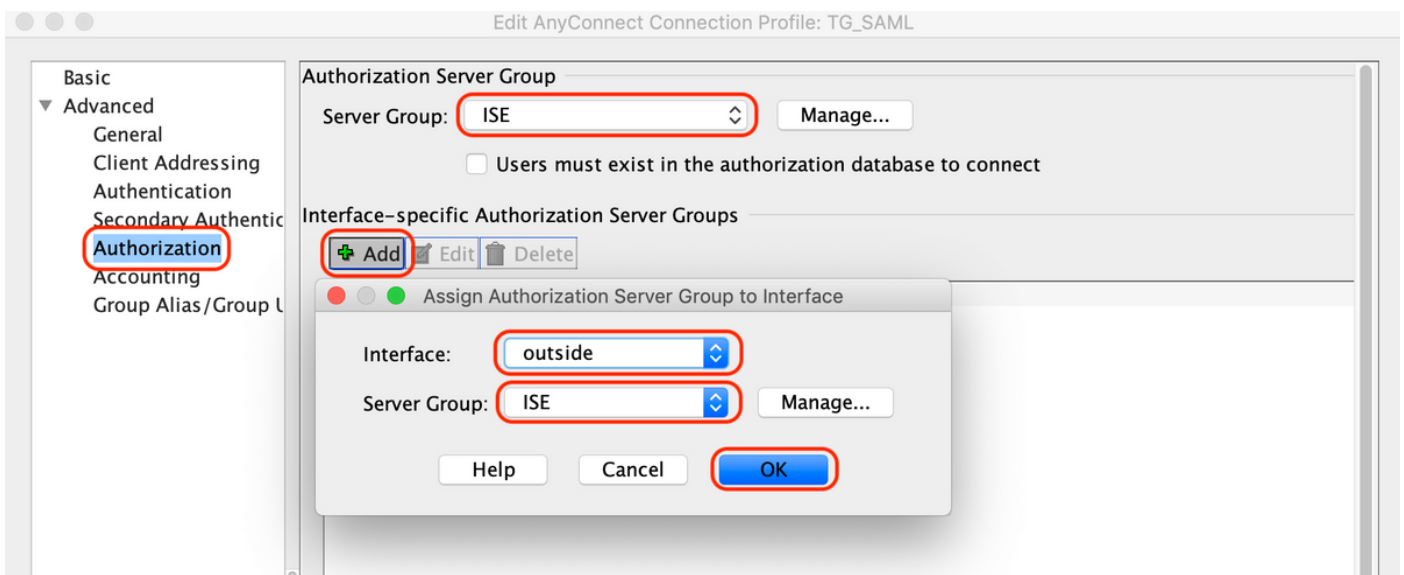
ID IDP-entiteit	<a href="https://explorer.cisco.com/dag/saml2/idp/metadata.php">https://explorer.cisco.com/dag/saml2/idp/metadata.php</a>
URL voor aanmelding	<a href="https://explorer.cisco.com/dag/saml2/idp/SSOService.php">https://explorer.cisco.com/dag/saml2/idp/SSOService.php</a>
URL voor uitloggen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

E. Klik op "Beheer > Toevoegen"



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

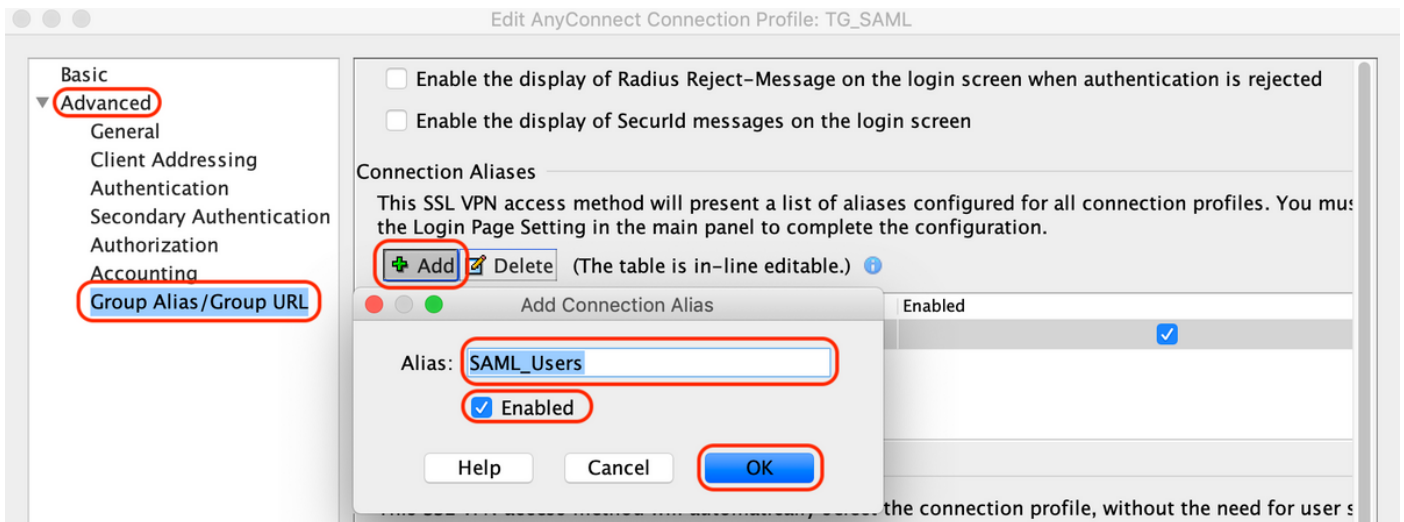
Navigeer naar "Geavanceerd > Autorisatie" en klik op "Toevoegen"



G. Onder Groepsalias de verbindingssalias 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
cr1 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

\* Name   
Description

IP Address  /

\* Device Profile    
Model Name   
Software Version

\* Network Device Group

Location    
IPSEC    
Device Type



▼ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**  
\* Shared Secret    
Use Second Shared Secret    
CoA Port

RADIUS DTLS Settings ⓘ

DTLS Required  ⓘ  
Shared Secret  ⓘ  
CoA Port    
Issuer CA of ISE Certificates for CoA  ⓘ  
DNS Name

General Settings

Enable KeyWrap  ⓘ  
\* Key Encryption Key    
\* Message Authenticator Code Key    
Key Input Format  ASCII  HEXADECIMAL



▶ TACACS Authentication Settings



▶ SNMP Settings



▶ Advanced TrustSec Settings

## 2. Installeer de laatste updates

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

### Posture Updates

Web

Offline

\* Update Feed URL

Proxy Address

Proxy Port  HH MM SS

Automatically check for updates starting from initial delay    every  hours

### ▼ Update Information

Last successful update on	2020/05/07 15:15:05 <input type="button" value="i"/>
Last update status since ISE was started	No update since ISE was started. <input type="button" value="i"/>
Cisco conditions version	224069.0.0.0
Cisco AV/AS support chart version for windows	171.0.0.0
Cisco AV/AS support chart version for Mac OSX	91.0.0.0
Cisco supported OS version	41.0.0.0

## 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 compliancmodule en "anyconnect-win-4.8.03052-webimplementation-k9.pkg" als AnyConnect Head-end implementatiepakket.

### Agent Resources From Local Disk

Category  ⓘ

Browse...

▼ AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.8.30...	AnyConnectDesktopWindows	4.8.3052.0	AnyConnect Secure Mobility Clie...

#### 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"

### ISE Posture Agent Profile Settings > Anyconnect Posture Profile

\* Name:

Description:

## Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	<input type="text" value="120"/> secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	<input type="text" value="60"/> secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	<input type="text" value="4"/>	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host	<input type="text"/>	IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to
Server name rules	<input type="text" value="*"/>	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	<input type="text"/>	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	<input type="text" value="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"

\* Select AnyConnect Package **AnyConnectDesktopWindows 4.8.3052.0** ▼

\* Configuration Name **AnyConnect Configuration**

Description:

**DescriptionValue**

\* Compliance Module **AnyConnectComplianceModuleWindows 4.3.1250.614** ▼

Notes

**AnyConnect Module Selection**

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Umbrella Roaming Security

Start Before Logon

**Diagnostic and Reporting Tool**

**Profile Selection**

\* ISE Posture **Anyconnect Posture Profile** ▼

VPN ▼

Network Access Manager ▼

Web Security ▼

AMP Enabler ▼

Network Visibility ▼

Umbrella Roaming Security ▼

Customer Feedback ▼

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"

**Client Provisioning Policy**

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:  
 For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.  
 For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows_10	If Any	and Windows 10 (All)	and Condition(s)	then AnyConnect Configuration
Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOS X 4.7.00135 And MacOsXSPWizard 2.1.0.42 And Cisco-ISE-NSP
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

Save Reset

## 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

**File Conditions List > VPN\_Posture\_File\_Check**

**File Condition**

\* Name: VPN\_Posture\_File\_Check

Description:

\* Operating System: Windows 10 (All)

Compliance Module: Any version

\* File Type: FileExistence

\* File Path: ABSOLUTE\_PATH

\* File Operator: Exists

C:\custom.txt

Save Reset

## 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

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
requirement_vvsn					
Default_Hardware_Attributes_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Hardware_Attributes_Check	then Select Remediations
Default_Firewall_Requirement_Win	for Windows All	using 4.x or later	using AnyConnect	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win
Default_Firewall_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac
USB_Block_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if USB_Check	then Message Text Only
Any_AM_Installation_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if ANY_am_win_inst	then Message Text Only
Any_AM_Installation_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if ANY_am_mac_inst	then Message Text Only
Default_AppVis_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Win	then Select Remediations
Default_AppVis_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Mac	then Select Remediations
Default_Hardware_Attributes_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations
Default_Hardware_Attributes_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations
Default_Firewall_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win
Default_Firewall_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac
<input checked="" type="checkbox"/> VPN_Posture_Requirement	for Windows 10 (All)	using 4.x or later	using AnyConnect	met if VPN_Posture_File_Check	then Message Text Only

Note: Remediation Action is filtered based on the operating system and stealth mode selection. Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.

Save Reset

## 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

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
⊙	Policy Options	Default_AppVis_Policy_Win	Any	Windows All	4.x or later	AnyConnect		Default_AppVis_Requirement_Win
⊙	Policy Options	Default_AppVis_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_AppVis_Requirement_Win_temporal
⊙	Policy Options	Default_Firewall_Policy_Mac	Any	Mac OSX	4.x or later	AnyConnect		Default_Firewall_Requirement_Mac
⊙	Policy Options	Default_Firewall_Policy_Mac_temporal	Any	Mac OSX	4.x or later	Temporal Agent		Default_Firewall_Requirement_Mac_temporal
⊙	Policy Options	Default_Firewall_Policy_Win	Any	Windows All	4.x or later	AnyConnect		Default_Firewall_Requirement_Win
⊙	Policy Options	Default_Firewall_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_Firewall_Requirement_Win_temporal
⊙	Policy Options	Default_Hardware_Attributes_Policy_Mac	Any	Mac OSX	4.x or later	AnyConnect		Default_Hardware_Attributes_Requirement_Mac
⊙	Policy Options	Default_Hardware_Attributes_Policy_Mac_temporal	Any	Mac OSX	4.x or later	Temporal Agent		Default_Hardware_Attributes_Requirement_Mac_temporal
⊙	Policy Options	Default_Hardware_Attributes_Policy_Win	Any	Windows All	4.x or later	AnyConnect		Default_Hardware_Attributes_Requirement_Win
⊙	Policy Options	Default_Hardware_Attributes_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_Hardware_Attributes_Requirement_Win_temporal
⊙	Policy Options	Default_USB_Block_Policy_Win	Any	Windows All	4.x or later	AnyConnect		USB_Block
⊙	Policy Options	Default_USB_Block_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		USB_Block_temporal
✔	Policy Options	VPN_Posture_Policy_Win	Any	Windows 10 (All)	4.x or later	AnyConnect		VPN_Posture_Requirement

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

Navigeer naar "Policy > Policy Elements > Results > Authorisation > Downloadable 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

Downloadable ACL List > PostureUnknown

**Downloadable ACL**

\* Name: PostureUnknown

Description: [Empty]

IP version:  IPv4  IPv6  Agnostic

\* DACL Content:

```

1234567 permit udp any any eq domain
8910111 permit ip any host 10.106.44.77
2131415 permit tcp any any eq 80
1617181 permit tcp any any eq 443
9202122
2324252
6272629
3031323
3343536
    
```

Check DAACL Syntax

Save Reset



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

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Authorization' > 'Downloadable ACLs' selected. The main content area is titled 'Downloadable ACL List > PostureNonCompliant' and 'Downloadable ACL'. The configuration details are as follows:

- \* Name: PostureNonCompliant
- Description: (empty field)
- IP version:  IPv4  IPv6  Agnostic
- \* DACL Content:

```
1234567 deny ip any 10.0.0.0 255.0.0.0
8910111 deny ip any 172.16.0.0 255.240.0.0
2131415 deny ip any 192.168.0.0 255.255.0.0
1617181 permit ip any any
9202122
2324252
6272829
3031323
3343536
```
- Buttons: Save, Reset

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

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Authorization' > 'Downloadable ACLs' selected. The main content area is titled 'Downloadable ACL List > PostureCompliant' and 'Downloadable ACL'. The configuration details are as follows:

- \* Name: PostureCompliant
- Description: (empty field)
- IP version:  IPv4  IPv6  Agnostic
- \* DACL Content:

```
1234567 permit ip any any
8910111
2131415
1617181
9202122
2324252
6272829
3031323
3343536
```
- Buttons: Save, Reset

## 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)

The screenshot shows the configuration page for an Authorization Profile named "Posture Redirect" in the Cisco Identity Services Engine (ISE) interface. The profile is configured with the following settings:

- Name:** Posture Redirect
- Description:** (empty)
- Access Type:** ACCESS\_ACCEPT
- Network Device Profile:** Cisco
- Service Template:** (unchecked)
- Track Movement:** (unchecked)
- Passive Identity Tracking:** (unchecked)

**Common Tasks:**

- DACL Name:** PostureUnknown
- Web Redirection (CWA, MDM, NSP, CPP):** (checked)
- Client Provisioning (Posture):** (selected)
- ACL:** redirect
- Value:** Client Provisioning Portal (default)

**Advanced Attributes Settings:** (empty)

**Attributes Details:**

```
Access Type = ACCESS_ACCEPT
DACL = PostureUnknown
cisco-av-pair = uri-redirect-ac=redirect
cisco-av-pair = uri-redirect=https://ip:port/portal/gateway?sessionId=SessionId&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp
```

Buttons: Save, Reset

## B. Vergunningsprofiel voor niet-conforme post

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

The screenshot shows the configuration page for an Authorization Profile named "Posture Non Compliant" in the Cisco Identity Services Engine (ISE) interface. The profile is configured with the following settings:

- Name:** Posture Non Compliant
- Description:** (empty)
- Access Type:** ACCESS\_ACCEPT
- Network Device Profile:** Cisco
- Service Template:** (unchecked)
- Track Movement:** (unchecked)
- Passive Identity Tracking:** (unchecked)

**Common Tasks:**

- DACL Name:** PostureNonCompliant

**Attributes Details:**

```
Access Type = ACCESS_ACCEPT
DACL = PostureNonCompliant
```

Buttons: Save, Reset

## C. Vergunningsprofiel voor de vervulling van de functie

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

The screenshot shows the configuration page for an Authorization Profile in Cisco ISE. The profile is named "Full Access" and has an access type of "ACCESS\_ACCEPT". The "Common Tasks" section shows the "DACL Name" set to "PostureCompliant". The "Attributes Details" section shows "Access Type = ACCESS\_ACCEPT" and "DACL = PERMIT\_ALL\_IPV4\_TRAFFIC".

## 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

The screenshot shows the Policy Sets configuration page in Cisco ISE. The "Authorization Policy (15)" section is expanded, showing three policies:

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Anyconnect Posture Compliant	Session PostureStatus EQUALS Compliant	Full Access	Select from list	6	⚙️
✓	Anyconnect Posture Non Compliant	Session PostureStatus EQUALS NonCompliant	Posture Non Compliant	Select from list	0	⚙️
✓	Anyconnect Posture Unknown	AND Network Access-Device IP Address EQUALS 10.197.164.3 Session PostureStatus EQUALS Unknown	Posture Redirect	Select from list	13	⚙️

# 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&p  
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  
Filter Name :

Pkts Rx Drop : 0

#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.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Pro...	Posture St...	IP Address	Network Device
Jun 14, 2020 07:44:59.975 AM			0	_585b5291f01484d1...	00:50:56:A0:D6:97	Windows10-...	Default	Anyconnect ...	Full Access	Compliant	10.197.164.7	ASA
Jun 14, 2020 07:44:59.975 AM				#ACSACL#-IP-PERMI...	10.197.243.143			Anyconnect ...	Full Access	Compliant		ASA
Jun 14, 2020 07:44:34.963 AM				#ACSACL#-IP-Posture...				Default >> A...	Posture Redirect	Pending		ASA
Jun 14, 2020 07:44:34.958 AM				_585b5291f01484d1...	00:50:56:A0:D6:97	Windows10-...	Default	Default >> A...	Posture Redirect	Pending		ASA



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>

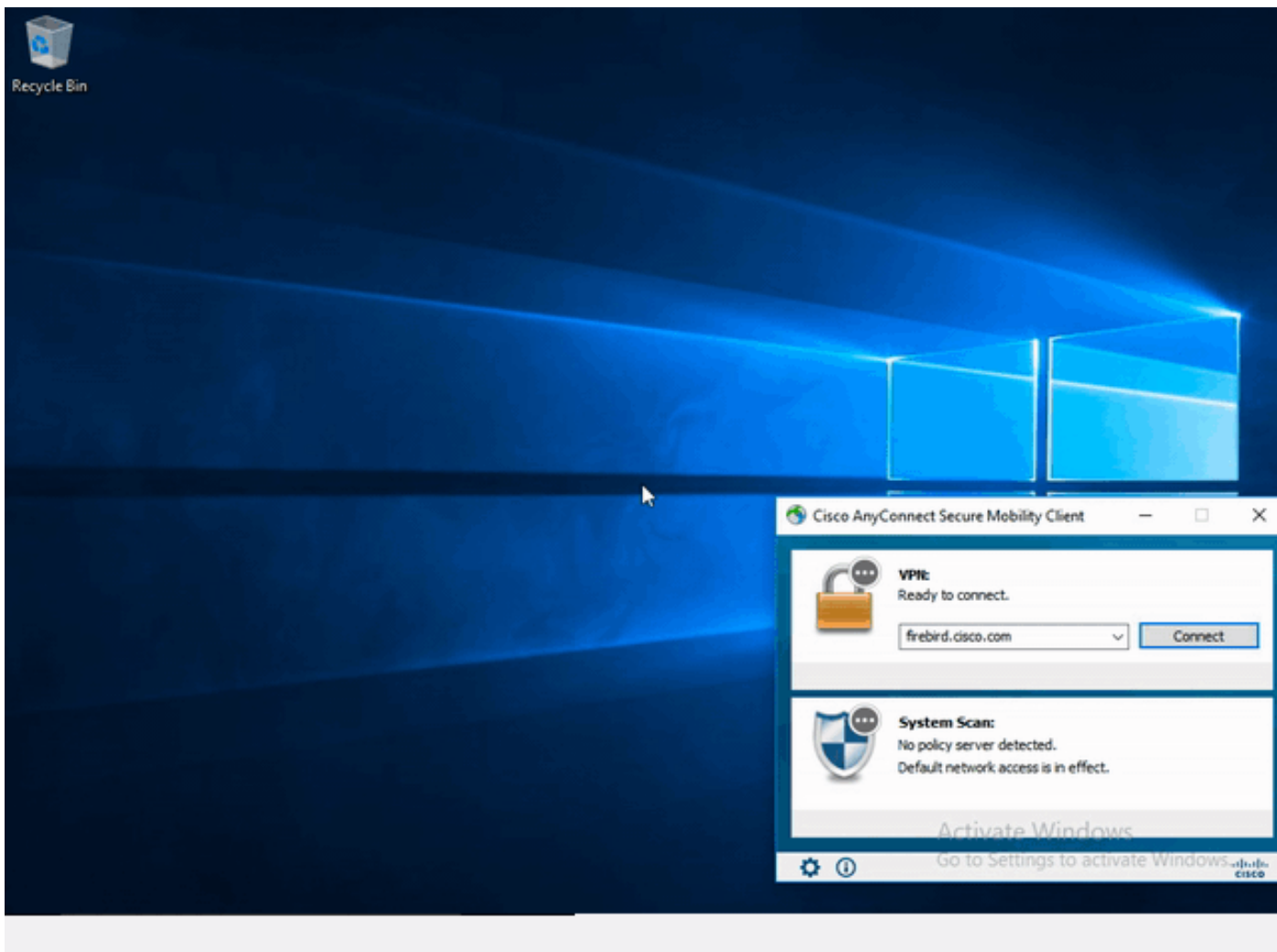
Om de verificatiestatus op het Duo Admin Portal te verifiëren, klikt u op de "Reports" aan de linkerkant van het Admin Panel dat het Verificatielogboek toont.

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](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](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-access.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.