

Certificaatverificatie configureren & DUO SAML-verificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Stappen configureren op DUO](#)

[Een beleid voor toepassingsbescherming maken](#)

[Toepassingsbeleid maken](#)

[Configuratiestappen voor FMC](#)

[Identiteitscertificaat implementeren bij de FTD](#)

[IDP-certificaat implementeren in de FTD](#)

[Het SAML SSO-object maken](#)

[Configuratie voor Virtual Private Network \(RAVPN\) met externe toegang maken](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Probleem 1: Certificaat-authenticatie mislukt](#)

[Probleem 2: SAML-fouten](#)

Inleiding

In dit document wordt een voorbeeld beschreven van de implementatie van certificaatgebaseerde verificatie en dubbele SAML-verificatie.

Voorwaarden

De hulpmiddelen en apparaten die in de handleiding worden gebruikt, zijn:

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Interne certificeringsautoriteit (CA)
- Cisco DUO Premier-account
- Cisco DUO-verificatieproxy
- Cisco Secure Client (CSC)

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basic VPN,
- SSL/TLS
- infrastructuur met openbare sleutel
- Ervaring met FMC
- Cisco Secure Client
- FTD-code 7.2.0 of hoger
- Cisco DUO-verificatieproxy

Gebruikte componenten

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

- Cisco FTD (7.3.1)
- Cisco FMC (7.3.1)
- Cisco Secure Client (5.0.02075)
- Cisco DUO-verificatieproxy (6.0.1)
- Mac OS (13.4.1)
- Active Directory

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Stappen configureren op DUO

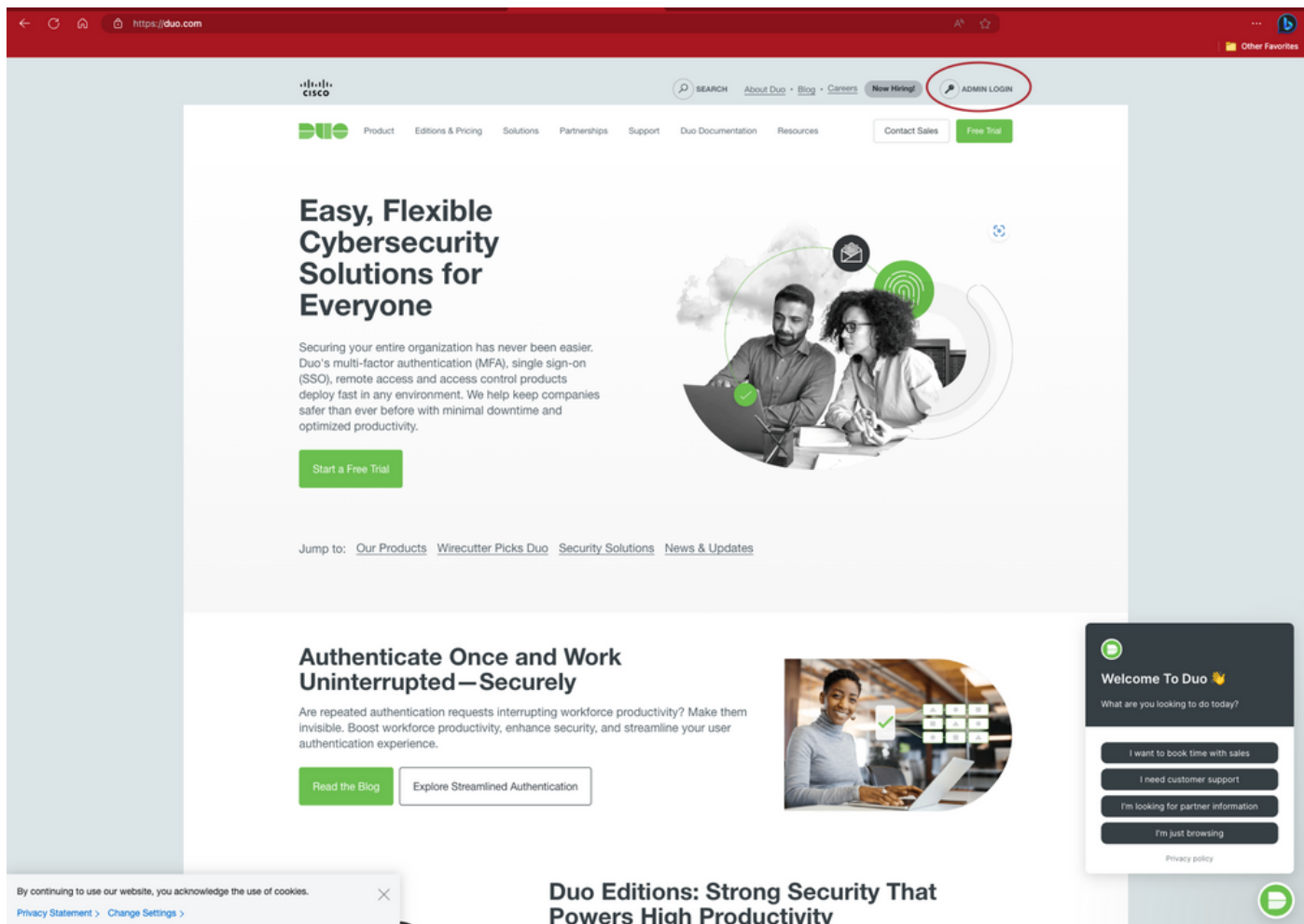
In dit gedeelte worden de stappen beschreven voor het configureren van Cisco DUO Single Sign-on (SSO). Voordat u begint, zorg ervoor dat de authenticatie proxy geïmplementeerd.



Waarschuwing: Als een verificatieproxy niet is geïmplementeerd, bevat deze link de handleiding voor deze taak. [DUO Authentication Proxy Guide](#)

Een beleid voor toepassingsbescherming maken

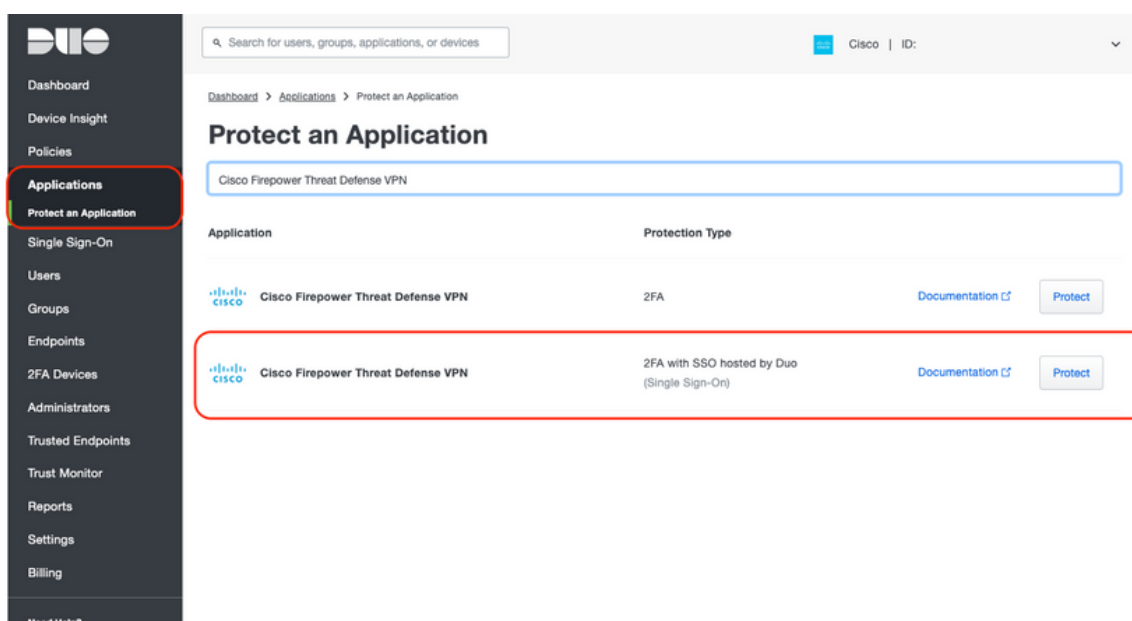
Stap 1. Meld u aan bij het beheerpaneel via deze link [Cisco Duo](#)



Cisco DUO-homepage

Stap 2. Navigeer naar Dashboard > Toepassingen > Een toepassing beveiligen.

Voer in de zoekbalk "Cisco Firepower Threat Defense VPN" in en selecteer "Protect".



Een screenshot van een toepassing beveiligen

Selecteer de optie met alleen het beschermingstype "2FA met SSO gehost door Duo".

Stap 3: Kopieer deze URL-informatie onder Metadata.

- Identiteitsleverancier Entiteit-ID
- SSO-URL
- Afmeldings-URL

See the [Cisco ASA SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID

Copy

Sign In URL

Copy

Sign Out URL

Copy

Voorbeeld van te kopiëren informatie



Opmerking: de links zijn weggelaten uit de screenshot.

Stap 4. Selecteer "Download certificaat" om het Identity Provider Certificate te downloaden onder Downloads.

Stap 5. Vul de informatie van de serviceprovider in

Cisco Firepower Base URL - De FQDN die wordt gebruikt om de FTD te bereiken

Naam van verbindingsprofiel - de naam van de tunnelgroep

Toepassingsbeleid maken

Stap 1: Als u een toepassingsbeleid wilt maken onder Beleid, selecteert u "Een beleid toepassen op alle gebruikers" en selecteert u "Of, een nieuw beleid maken", zoals in de afbeelding wordt weergegeven.

Policy

Policy defines when and how users will authenticate when accessing this application. Your global policy always applies, but you can override its rules with custom policies.

Group policies

Apply a policy to groups of users

Application policy

Apply a policy to all users

Voorbeeld van het maken van een toepassingsbeleid

Apply a Policy



Policy

Select a Policy



[Or, create a new Policy.](#)

Apply Policy

Voorbeeld van het maken van een toepassingsbeleid

Stap 2. Voer onder Beleidsnaam de gewenste naam in, selecteer "Verificatiebeleid" onder Gebruikers en selecteer "2FA afdwingen." Sla vervolgens op met "Beleid maken".

Create a New Policy

Policy name

MFA

Users

New User policy

Authentication policy

User location

Devices

Trusted Endpoints

Device Health application

Remembered devices

Operating systems

Browsers

Plugins

Networks

Authorized networks

Anonymous networks

Authenticators

Risk-based factor selection

Authentication methods

Duo Mobile app

Tampered devices

Screen lock

Full-disk encryption

Mobile device biometrics

Authentication policy

Enforce 2FA

Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

Bypass 2FA

Skip two-factor authentication and enrollment, unless there is a superseding policy configured.

Deny access

Deny authentication to all users.

When enabled, this affects all users.

Choose another rule on the left to add to this policy.

Create Policy

Voorbeeld van het maken van een toepassingsbeleid

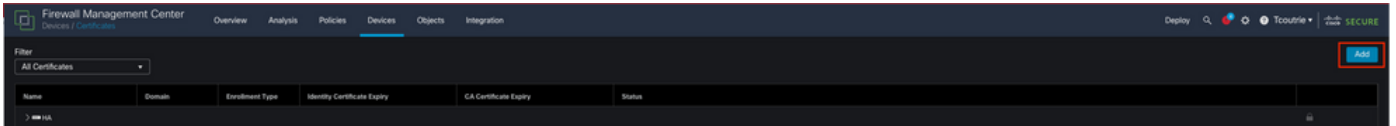
Stap 3. Pas het beleid toe met "Beleid toepassen" in het volgende venster. Blader vervolgens naar de onderkant van de pagina en selecteer "Opslaan" om de DUO-configuraties te voltooien

Configuratiestappen voor FMC

Identiteitscertificaat implementeren bij de FTD

In deze sectie wordt beschreven hoe het identiteitscertificaat moet worden geconfigureerd en geïmplementeerd in de FTD die nodig is voor certificaatverificatie. Voordat u begint, moet u alle configuraties implementeren.

Stap 1. Navigeer naar Apparaten > Certificaat en kies Toevoegen, zoals weergegeven in de afbeelding.



Screenshot van apparaten/certificaten

Stap 2: Kies het FTD-toestel uit de keuzelijst Apparaten. Klik op het + pictogram om een nieuwe certificaatinschrijvingsmethode toe te voegen.

A screenshot of the 'Add New Certificate' dialog box. The title 'Add New Certificate' is at the top. Below it, a message states: 'Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.' There are two main fields: 'Device*' with a dropdown menu showing 'HA', and 'Cert Enrollment*' with a dropdown menu showing 'Select a certificate enrollment object'. To the right of the 'Cert Enrollment*' dropdown is a red box around a '+' button. At the bottom right, there are 'Cancel' and 'Add' buttons.

Schermafbeelding van Nieuw certificaat toevoegen

Stap 3: Kies de optie die de voorkeursmethode is om certificaten in de omgeving te verkrijgen via het "inschrijvingstype", zoals weergegeven in de afbeelding.

Add Cert Enrollment



Name*

FTD04-16

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

PKCS12 File



PKCS12 File*:

test.p12



Browse PKCS12 File

Passphrase:

.....



Validation Usage:



IPsec Client



SSL Client



SSL Server



Skip Check for CA flag in basic constraints of the CA Certificate



Allow Overrides

Cancel

Save

Screenshot van nieuwe pagina voor certificaatschrijving



Tip: De beschikbare opties zijn: Self Signed Certificate - Genereer lokaal een nieuw certificaat, SCEP - Use Simple Certificate Enrollment Protocol to obtain a certificate from a CA, Manual - Installeer het Root and Identity-certificaat, PKCS12 - Upload encrypted certificate bundle with root, identity, and private key.

IDP-certificaat implementeren in de FTD

In deze sectie wordt beschreven hoe het IDP-certificaat wordt geconfigureerd en geïmplementeerd in de FTD. Voordat u begint, moet u alle configuraties implementeren.

Stap 1: Navigeer naar Apparaten > Certificaat en kies Toevoegen."

Stap 2: Kies het FTD-toestel uit de keuzelijst Apparaten. Klik op het + pictogram om een nieuwe certificaatinschrijvingsmethode toe te voegen.

Stap 3: Voer in het venster Cert Enrollment toevoegen de vereiste informatie in zoals weergegeven in de afbeelding en vervolgens "Opslaan" zoals weergegeven in de afbeelding.

- Naam: Naam van het object
- Type inschrijving: Handleiding
- Selectievakje ingeschakeld: alleen CA
- CA-certificaat: Pem-formaat van het certificaat

Add Cert Enrollment

Name*

duocert

Description

CA Information
Certificate Parameters
Key
Revocation

Enrollment Type

Manual

☒ CA Only
Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

OC957DUc7tc4
b79bVzOXuqz5ZpaJHqtXV8fLOH
eIPYblyYBwSstXB+k75VHs0Voz
AkeySJCWRQXF
ISSRGu8DpUIKzKu2zd55322+wd
fkyy/WMXUJWmSXXKnnHEsOqL
GCxmfd+5OsWlo
ICCMGa5gYgEv8EHF3Y++sFg=
-----END CERTIFICATE-----

Validation Usage:
☒ IPsec Client
☐ SSL Client
☒ SSL Server
☐ Skip Check for CA flag in basic constraints of the CA Certificate

☐ Allow Overrides

Cancel

Save

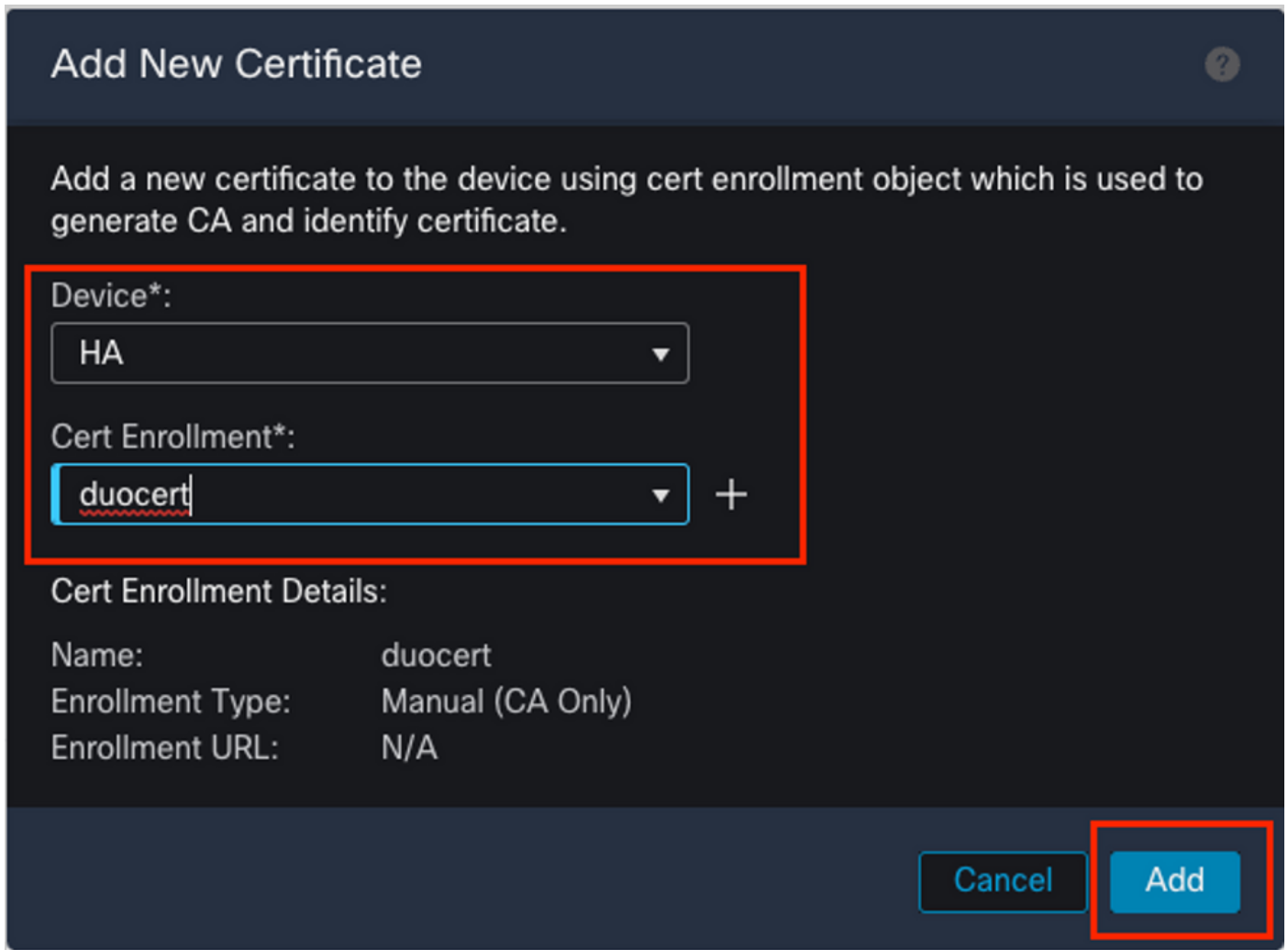
Voorbeeld van het maken van een object voor certificaatschrijving



Waarschuwing: "Controleer voor CA-markering in basisbeperkingen van het CA-certificaat" kan indien nodig worden gebruikt. Gebruik deze optie met voorzichtigheid.

Stap 4: Selecteer het nieuw gemaakte object voor certificaatschrijving onder "Inschrijving

certificeren*:" en selecteer vervolgens "Toevoegen" zoals weergegeven in de afbeelding.



Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: HA

Cert Enrollment*: duocert

Cert Enrollment Details:

Name:	duocert
Enrollment Type:	Manual (CA Only)
Enrollment URL:	N/A

Cancel Add

Schermafbeelding van toegevoegd object voor inschrijving van certificaat en apparaat



Opmerking: zodra het certificaat is toegevoegd, wordt 'onmiddellijk geïmplementeerd'.

Het SAML SSO-object maken

In dit gedeelte worden de stappen beschreven voor het configureren van SAML SSO via FMC. Voordat u begint, moet u alle configuraties implementeren.

Stap 1. Navigeer naar Objects > AAA Server > Single Sign-on Server en selecteer "Add Single Sign-on Server".

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? Tcourtrie

AAA Server
RADIUS Server Group
Single Sign-on Server
Access List
Address Pools
Application Filters
AS Path
bfd Template
Cipher Suite List
Community List
DHCP IPv6 Pool
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List
Route Map

Single Sign-on Server

Add Single Sign-on Server 🔍 Filter

Single Sign-on Server contains parameters for SAML based authentication. These Single Sign-on Servers are used to authenticate users logging in through Remote Access VPN connections.

Name	
AZ	✎ 🗑
DUO	✎ 🗑

Displaying 1 - 2 of 2 rows | < > Page 1 of 1

Voorbeeld van een nieuw SSO-object maken

Stap 2. Voer de vereiste informatie in vanuit "Een toepassingsbeschermingsbeleid maken"

". Als u wilt doorgaan nadat u klaar bent, selecteert u "Opslaan".

- Naam*: Naam van het object
- Identiteitsprovider Entiteit-ID*: Entiteit-ID vanaf stap 3
- SSO-URL*: URL voor aanmelden gekopieerd uit stap 3
- Afmeldings-URL: afmeldings-URL gekopieerd van stap 3
- Basis-URL: Gebruik dezelfde FQDN als "Cisco Firepower Base-URL" in stap 5
- Certificaat van identiteitsprovider*: geïmplementeerd IDP-certificaat
- Serviceleverancierscertificaat: Certificaat op de externe interface van de FTD

New Single Sign-on Server?

Name*

duosso

Identity Provider Entity ID*

SSO URL*

Logout URL

Base URL

https://vpn.ciscoexample.com

Identity Provider Certificate*

duocert

+

Service Provider Certificate

FTD04-16

+

Request Signature

--No Signature--

Request Timeout

Use the timeout set by the provide

seconds (1-7200)

☐ Enable IdP only accessible on Internal Network

☒ Request IdP re-authentication on Login

☐ Allow Overrides

Cancel

Save

Voorbeeld van een nieuw SSO-object.



Opmerking: de links Entity ID, SSO URL en Logout URL zijn weggelaten uit de screenshot

Configuratie voor Virtual Private Network (RAVPN) met externe toegang maken

In dit gedeelte worden de stappen beschreven voor het configureren van RAVPN met behulp van de wizard.

Stap 1. Navigeer naar Apparaten > Externe toegang Selecteer "Toevoegen."

Stap 2. Voer in de wizard de naam in van de nieuwe RAVPN-beleidswizard, selecteer SSL onder VPN-protocollen: Voeg de doelapparaten toe, zoals weergegeven in de afbeelding. Selecteer "Volgende" zodra deze is voltooid.

Remote Access VPN Policy Wizard

Policy Assignment | Connection Profile | Secure Client | Access & Certificate | Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:

Description:

VPN Protocols:

☒ SSL

☐ IPsec-IPv2

Targeted Devices:

Available Devices: HA

Selected Devices: HA

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure LOCAL or RADIUS or RADIUS Server Group or SSO to authenticate VPN clients.

Secure Client Package

Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

Cancel | Back | **Next**

Stap 1 van de RAVPN wizard

Stap 2. Voor het profiel Verbinden stelt u de opties in (hier weergegeven): Selecteer "Volgende" zodra deze is voltooid.

- Naam van verbindingsprofiel: gebruik de naam van de tunnelgroep in stap 5 van "Een toepassingsbeschermingsbeleid maken".

Authenticatie, autorisatie en boekhouding (AAA):

- Verificatiemethode: Clientcertificaat en SAML
- Verificatieserver:* Selecteer het SSO-object dat is gemaakt tijdens het maken van het SAML SSO-object.

Toewijzing van klantadres:

- AAA-server gebruiken (alleen Realm of RADIUS) - Radius of LDAP
- DHCP-servers gebruiken - DHCP-server
- IP-adresgroepen gebruiken - Lokale pool op de FTD

Firewall Management Center Overview Analysis Policies **Devices** Objects Integration Deploy Tcoutlife **SECURE**

Remote Access VPN Policy Wizard

Policy Assignment Connection Profile **Secure Client** Access & Certificate Summary

Connection Profile Name:

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

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

Authentication Method:

Authentication Server:

SAML Login Experience: ☒ VPN client embedded browser ☐ Default OS Browser

☐ Allow connection only if username from certificate and SAML are the same

☐ Use username from client certificate for Authorization

Username from Certificate:

Primary Field:

Secondary Field:

Authorization Server:

Accounting Server:

Client Address Assignment:

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

☐ Use AAA Server (RADIUS or RADIUS only)

☒ Use DHCP Servers

Use DHCP Servers:

☐ Use IP Address Pools

Group Policy:

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

Group Policy:

[Edit Group Policy](#)

Cancel Back **Next**

Stap 2 van de RAVPN wizard



Tip: Voor dit lab wordt een DHCP-server gebruikt.

Stap 3. Selecteer "+" om een web-deploy image van de te implementeren Cisco Secure Client te uploaden. Schakel vervolgens het selectievakje in van het te implementeren CSC-image. Zoals te zien is op de afbeelding. Selecteer "Volgende" zodra deze is voltooid.

Firewall Management Center Overview Analysis Policies **Devices** Objects Integration Deploy Tcoutlife **SECURE**

Remote Access VPN Policy Wizard

Policy Assignment Connection Profile Secure Client **Access & Certificate** Summary

Remote User Secure Client Internet Gateway VPN Device Corporate Resources AAA

Secure Client Image

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

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

Secure Client File Object Name	Secure Client Package Name	Operating System
☒ cisco-secure-client-macos-5.0...	cisco-secure-client-macos-5.0.02075-web...	Mac OS
☒ cisco-secure-client-win-5.0.020...	cisco-secure-client-win-5.0.02075-webde...	Windows

Cancel Back **Next**

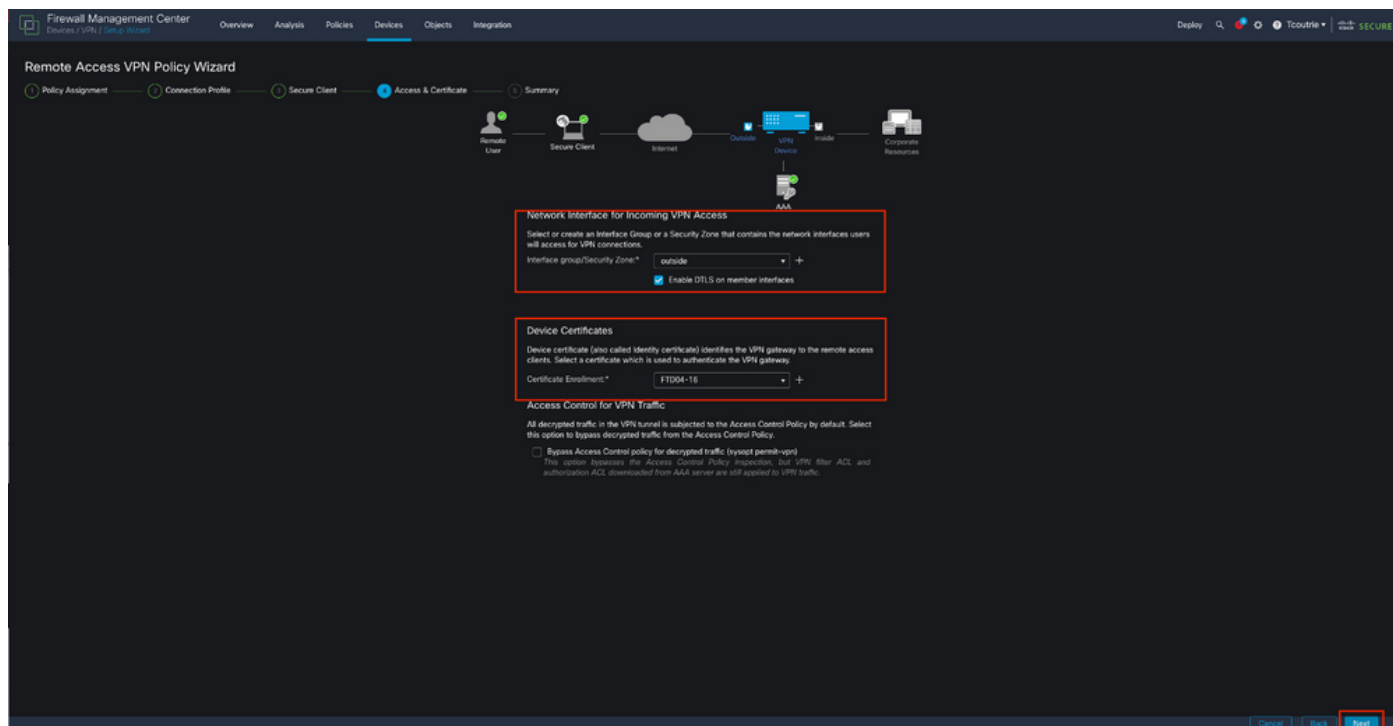
Stap 3 RAVPN-wizard

Stap 4. Stel deze objecten in (zoals te zien in de afbeelding): Selecteer "Volgende" zodra deze is voltooid.

Interfacegroep/Beveiligingszone: *: Buiteninterface

"Certificaatinschrijving: *": Identiteitscertificaat dat is gemaakt tijdens het gedeelte

"Identiteitscertificaat implementeren bij de FTD" van deze handleiding

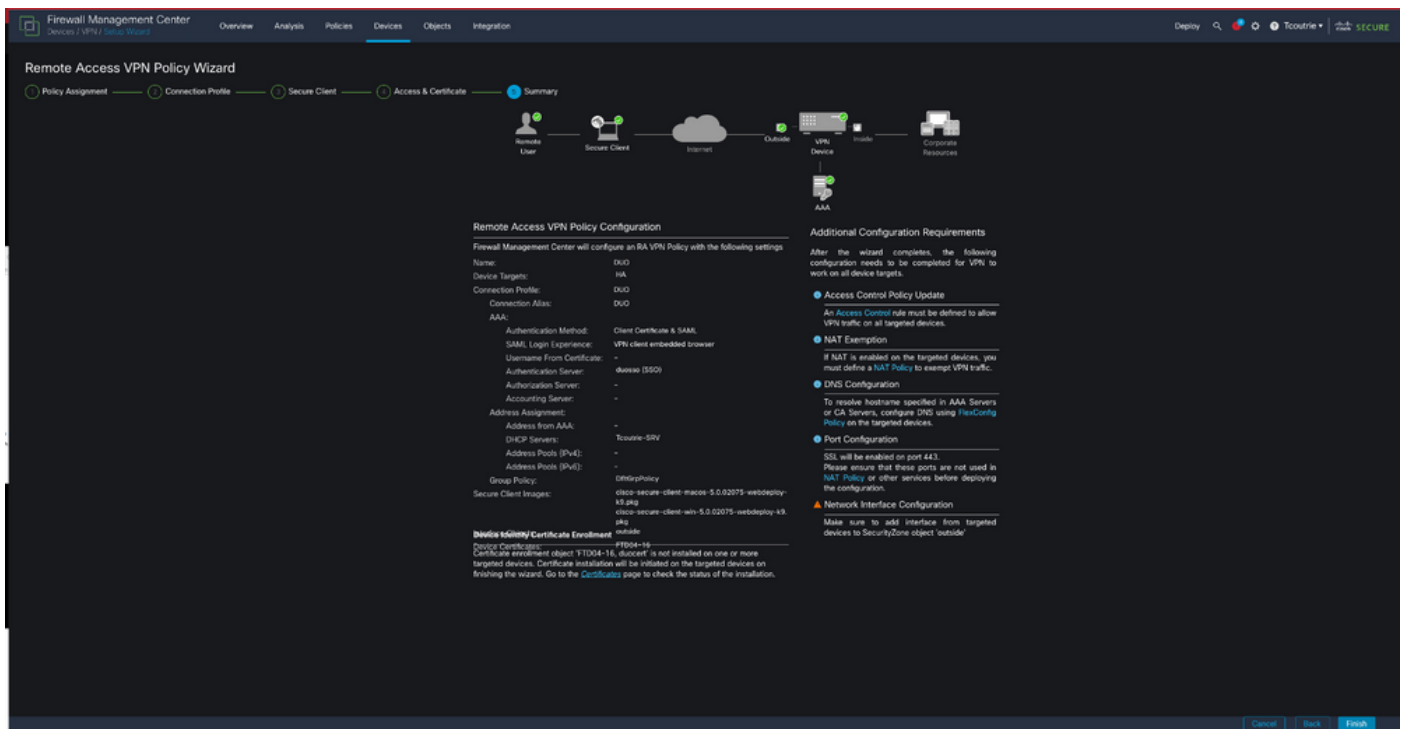


Stap 4 van de RAVPN wizard

 **Tip:** Als dit niet is gemaakt, voegt u een nieuw object voor certificaatinschrijving toe door "+" te selecteren.

Stap 6. Samenvatting

Controleer alle informatie. Als alles klopt, ga dan verder met 'Voltooien'.



Overzichtspagina

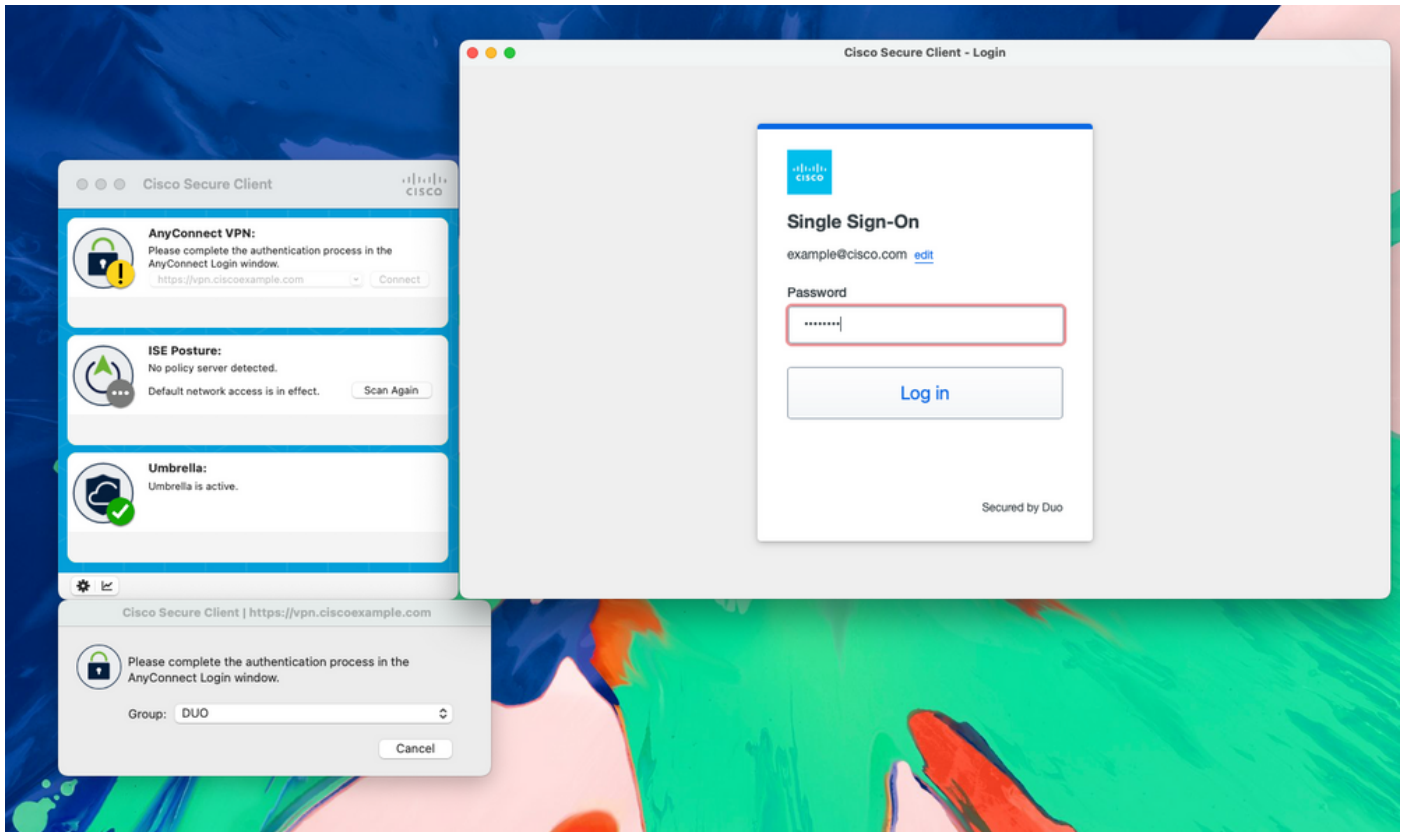
Stap 7. Implementeer de nieuw toegevoegde configuraties.

Verifiëren

In dit gedeelte wordt beschreven hoe u een succesvolle verbindingspoging verifieert.

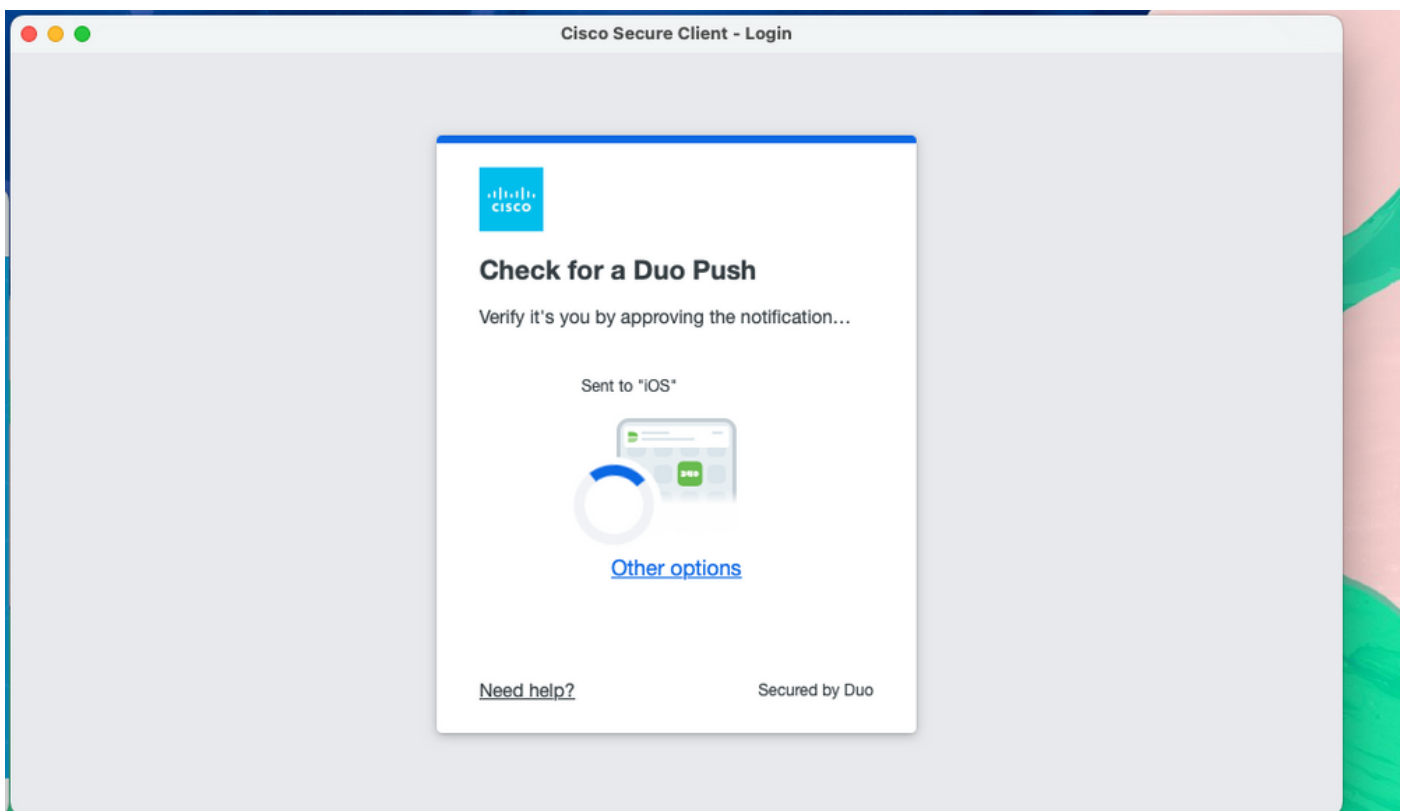
Open Cisco Secure Client en voer het FQDN van de FTD in en maak verbinding.

Voer de referenties in op de SSO-pagina.



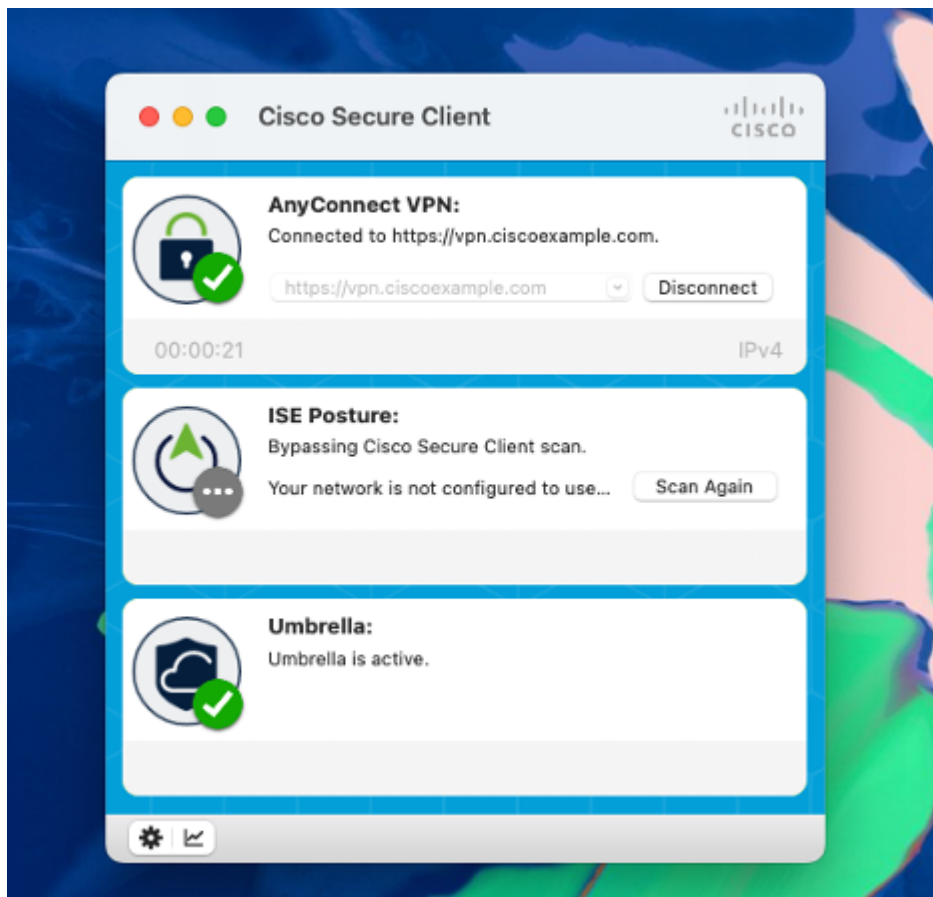
SSO-pagina via Cisco Secure Client

Accepteer de DUO-push naar het geregistreerde apparaat.



DUO-duw

Succesvolle verbinding.



Verbonden met FTD

Controleer de verbinding op de FTD met de opdracht: vpn-sessiondb detail anyconnect tonen

```

tcoutrie-ftd2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username      :                               Index      : 1916
Assigned IP   :                               Public IP   :
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128  DTLS-Tunnel:
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SH
Bytes Tx      : 390964                        Bytes Rx      : 124114
Pkts Tx       : 1216                          Pkts Rx       : 1223
Pkts Tx Drop  : 0                            Pkts Rx Drop  : 0
Group Policy  :                               Tunnel Group :
Login Time    : 23:54:41 UTC Tue Jul 18 2023
Duration      : 0h:11m:28s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                          VLAN          : none
Audt Sess ID  : 0a7aa95d0077c00064b72641
Security Grp  : none                          Tunnel Zone   : 0

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

AnyConnect-Parent:
Tunnel ID     : 1916.1
Public IP     :
Encryption    : none                        Hashing       : none
TCP Src Port  : 53859                       TCP Dst Port  : 443
Auth Mode     : Certificate and SAML
Idle Time Out: 30 Minutes                   Idle TO Left  : 18 Minutes
Client OS     : mac-intel

```

In het uitvoervoorbeeld is enige informatie weggelaten

Problemen oplossen

Dit zijn mogelijke problemen die zich voordoen na de implementatie.

Probleem 1: Certificaat-authenticatie mislukt.

Zorg ervoor dat het basiscertificaat op de FTD is geïnstalleerd;

Gebruik deze debugs:

debug crypto ca 14

debug aaa shim 128

debug AAA Common 128

Probleem 2: SAML-fouten

Deze foutmeldingen kunnen worden ingeschakeld om problemen op te lossen:

debug aaa shim 128

debug AAA Common 128

debug webvpn anyconnect 128

Foutopsporing WebVPN SAML 255

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.