

SSL AnyConnect Management VPN op FTD configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Beperkingen](#)

[Configureren](#)

[Configuraties](#)

[Stap 1. Maak AnyConnect Management VPN-profiel](#)

[Stap 2. Maak AnyConnect VPN-profiel](#)

[Stap 3. Upload AnyConnect Management VPN-profiel en AnyConnect VPN-profiel naar FMC](#)

[Stap 4. Groepsbeleid maken](#)

[Stap 5. Maak een nieuwe AnyConnect-configuratie](#)

[Stap 6. URL-object maken](#)

[Stap 7. Bepaal URL-alias](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u een Cisco AnyConnect Management-tunnel kunt configureren op een Cisco Firepower Threat Defense (FTD) die wordt beheerd door Cisco Firepower Management Center (FMC). In het voorbeeld onder Secure Socket Layer (SSL) wordt gebruikt om Virtual Private Network (VPN) tussen FTD en een Windows 10-client te maken.

Bijgedragen door Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco AnyConnect-profiel-editor
- SSL AnyConnect-configuratie via FMC.
- Verificatie van clientcertificaten

Gebruikte componenten

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

- Cisco FTD versie 6.7.0 (gebouwd 65)
- Cisco FMC versie 6.7.0 (gebouwd 65)
- Cisco AnyConnect 4.9.01095 geïnstalleerd op Windows 10-machine

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Vanaf release 6.7 ondersteunt Cisco FTD de configuratie van AnyConnect Management-tunnels. Dit maakt eerder geopende verbeteringsaanvraag [op CSCvs78215](#).

Met de functie AnyConnect Management kunt u direct nadat het eindpunt is beëindigd een VPN-tunnel maken. Het is niet nodig dat de gebruikers de AnyConnect-app handmatig starten, zodra hun systeem is ingeschakeld, detecteert de AnyConnect VPN-agent de Management VPN-functie en start een AnyConnect-sessie met behulp van de hostingvermelding die in de serverlijst van het AnyConnect Management VPN-profiel is gedefinieerd.

Beperkingen

- Alleen verificatie van clientcertificaten wordt ondersteund.
- Alleen Machine certificaatwinkel wordt ondersteund voor Windows-clients.
- Niet ondersteund op Cisco Firepower Apparaat Manager (FDM) [CSCvx90058](#).
- Niet ondersteund op Linux-klanten.

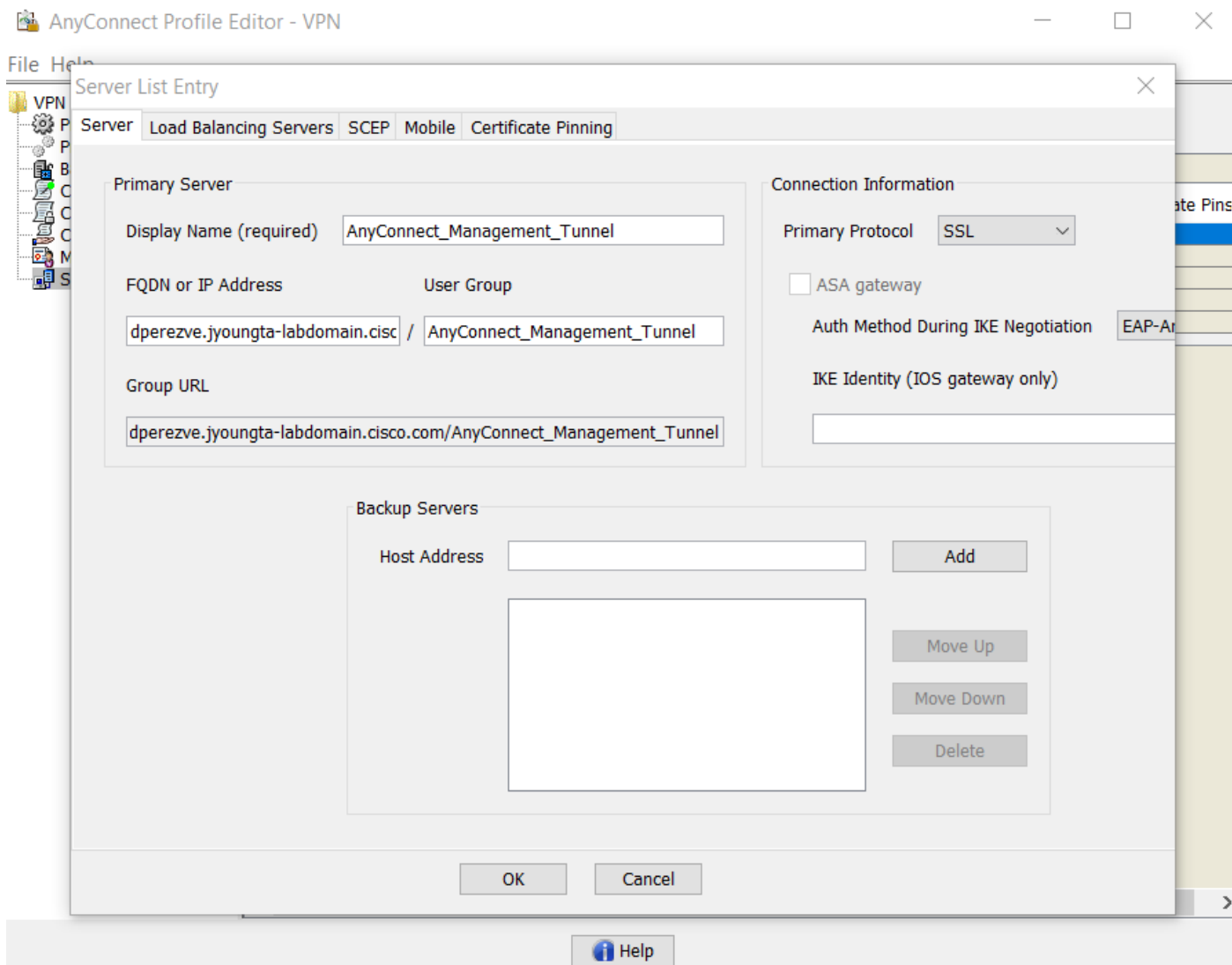
Configureren

Configuraties

Stap 1. Maak AnyConnect Management VPN-profiel

Open de AnyConnect Profile Editor om AnyConnect Management VPN-profiel te maken. Het beheerprofiel bevat alle instellingen die worden gebruikt om de VPN-tunnel te maken nadat de eindpunten zijn opgestart.

In dit voorbeeld wordt een Server List die naar Full Qualified Domain Name (FQDN) wijst, dperezve.jyoungta-labdomein.cisco.com gedefinieerd en SSL is geselecteerd als het primaire protocol. Als u een serverlijst wilt toevoegen, navigeer dan in de **lijst met servers** en selecteer de knop **Toevoegen**, vult u de gewenste velden in en slaat u de wijzigingen op.



Naast de serverlijst moet het VPN-profiel van het beheer een aantal verplichte voorkeuren bevatten:

- **Automatische** selectie moet op **waarheid** worden ingesteld.
- **AutoReconconnect** moet worden ingesteld op **waarheid**.
- **AutoReconnectBehavior** moet worden ingesteld voor **ReconconnectAfterResume**.
- **AutoUpdate** moet op **fout** worden ingesteld.
- **BlockUnvertrouwde servers** moet op **waar** ingesteld worden.
- **certificaatwinkel** moet worden ingesteld voor **MachineStore**.
- **certificaatnummerStoreOverride** moet op **waarheid** worden ingesteld.
- **AutomatischServerSelecteren** inschakelen moet op **onjuist** zijn ingesteld.
- **Schakel de** toepassing in voor de **scripts** op **vals** moeten worden ingesteld.
- **BewaarVPNOnLogoff** moet op **waarheid** worden ingesteld.

In AnyConnect Profile Editor navigeer naar **voorkeuren (Deel 1)** en stel de instellingen als volgt in:

File Help

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Preferences (Part 1)

Profile: ...nnect -FTD-Lab1.XML Profile\AnyConnect_Management_Tunnel.xml

Use Start Before Logon User Controllable

Show Pre-Connect Message

Certificate Store

Windows **Machine** ▾

macOS **All** ▾

Certificate Store Override

Auto Connect On Start User Controllable

Minimize On Connect User Controllable

Local Lan Access User Controllable

Disable Captive Portal Detection User Controllable

Auto Reconnect User Controllable

Auto Reconnect Behavior

ReconnectAfterResume ▾

Auto Update User Controllable

RSA Secure ID Integration User Controllable

Automatic ▾

Windows Logon Enforcement

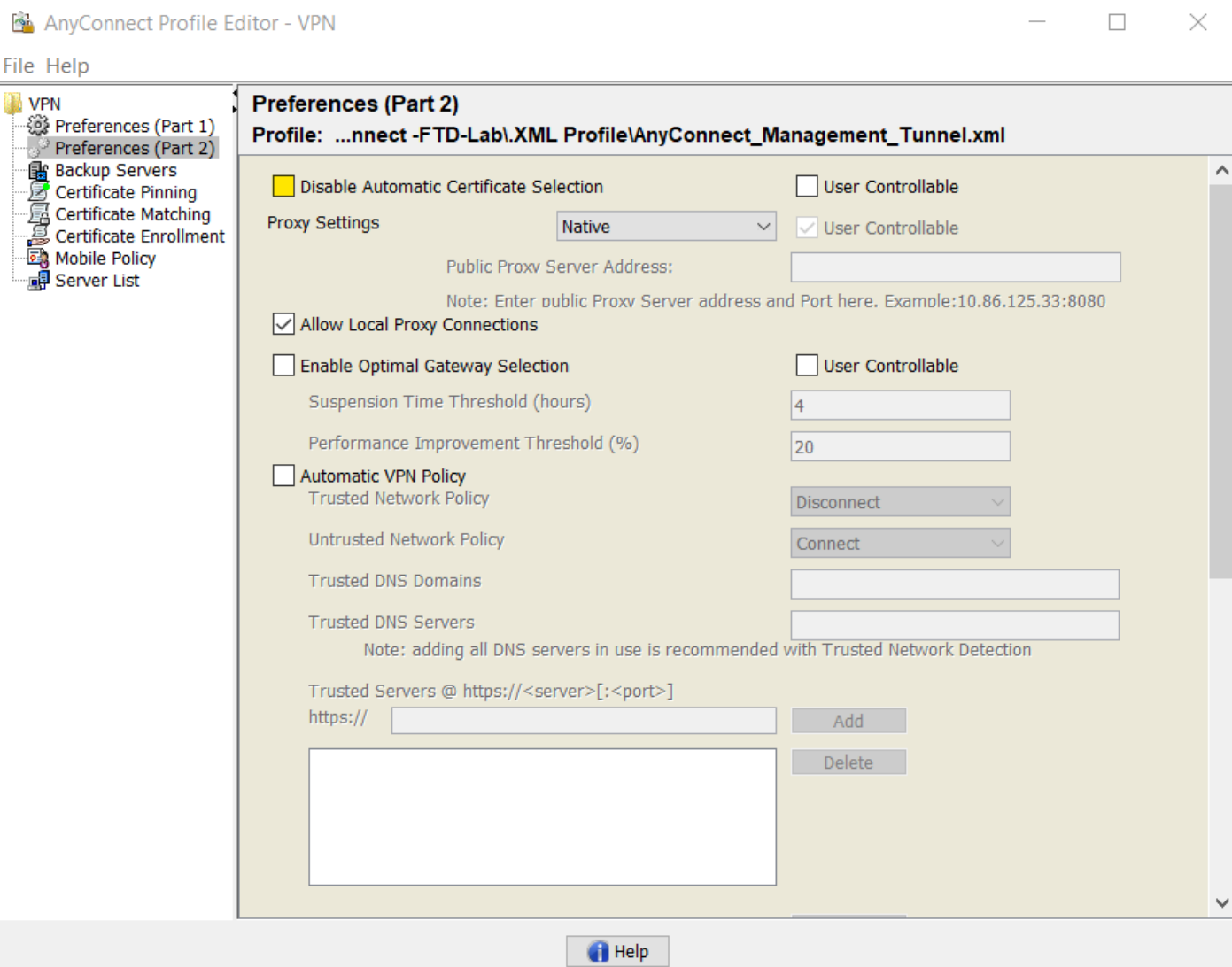
SingleLocalLogon ▾

Windows VPN Establishment

AllowRemoteUsers ▾

Help

navigeer vervolgens naar **voorkeuren (Deel 2)** en controleer de optie **Automatisch certificaat selecteren** niet.



Stap 2. Maak AnyConnect VPN-profiel

Naast het VPN-profiel voor beheer moet het normale AnyConnect VPN-profiel worden geconfigureerd. Het AnyConnect VPN-profiel wordt tijdens de eerste verbindingsooging gebruikt en tijdens deze sessie wordt het Beheersprofiel gedownload van FTD.

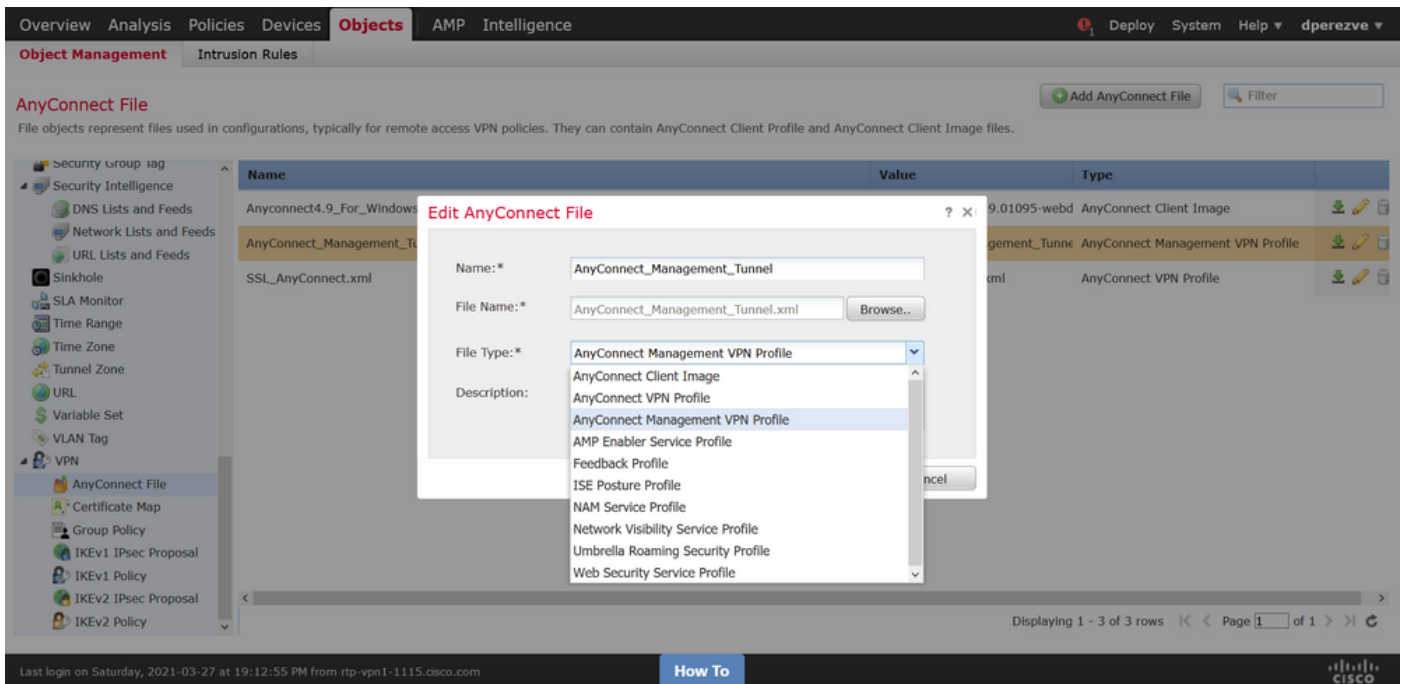
Gebruik de AnyConnect Profile Editor om het AnyConnect VPN-profiel te maken. In dit geval bevatten beide bestanden dezelfde instellingen, zodat dezelfde procedure kan worden gevolgd.

Stap 3. Upload AnyConnect Management VPN-profiel en AnyConnect VPN-profiel naar FMC

Zodra de profielen zijn gemaakt, wordt de volgende stap gezet door ze te uploaden naar het FMC, zoals AnyConnect File Objects.

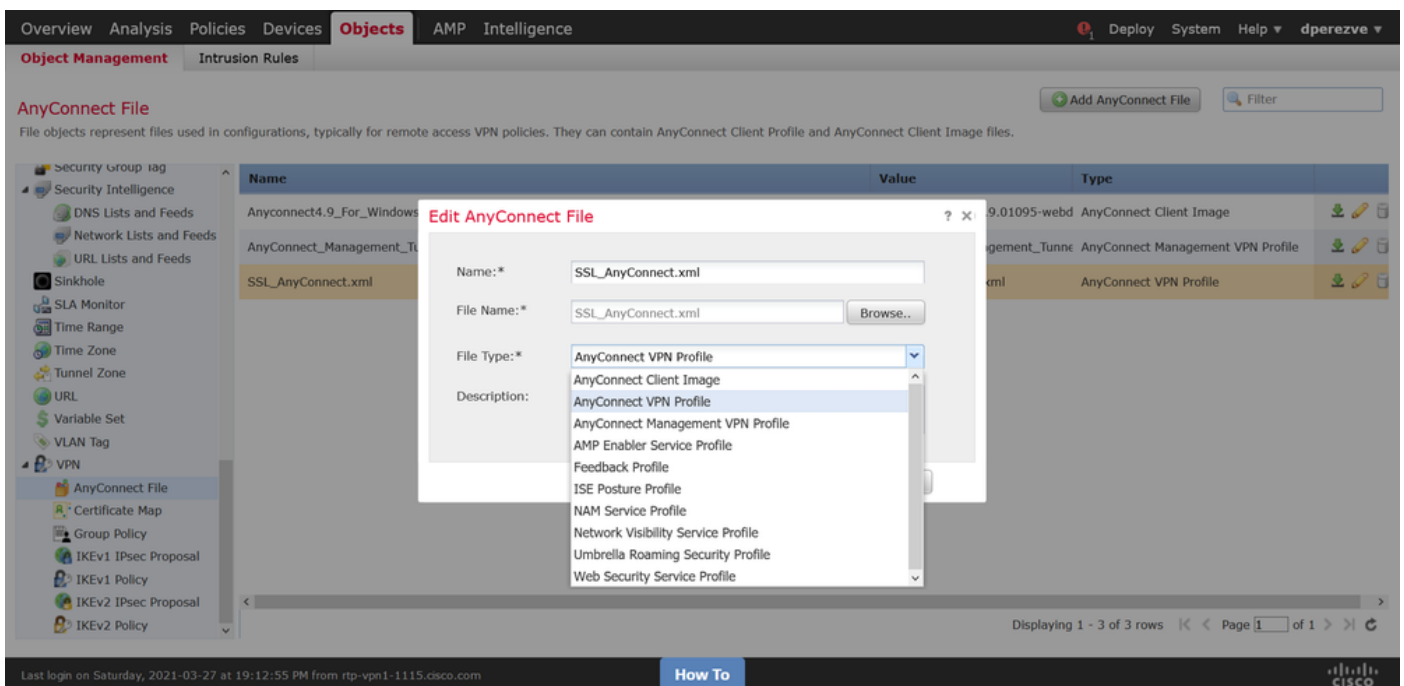
Om het nieuwe AnyConnect Management VPN-profiel naar FMC te uploaden, navigeer naar **Objecten > Objectbeheer** en kies de optie **VPN** uit de inhoudsopgave en selecteer de knop **Add AnyConnect File**.

Geef een naam voor het bestand op, kies **AnyConnect Management VPN Profile** als het bestandstype en slaat het object op.



Als u het AnyConnect VPN-profiel opnieuw wilt uploaden, navigeer dan opnieuw naar **Objecten > Objectbeheer** en kies de **VPN**-optie uit de inhoudsopgave en selecteer de knop **Add AnyConnect File**.

Geef een naam voor het bestand op maar kies nu **AnyConnect VPN Profile** als bestandstype en slaat het nieuwe object op.



profielen moeten aan de objectlijst worden toegevoegd en als **AnyConnect Management VPN-profiel** en **AnyConnect VPN-profiel** worden gemarkeerd.

Overview Analysis Policies Devices **Objects** AMP Intelligence Deploy System Help dperezve

Object Management Intrusion Rules

AnyConnect File Add AnyConnect File

File objects represent files used in configurations, typically for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image files.

Name	Value	Type	
Anyconnect4.9_For_Windows	anyconnect-win-4.9.01095-webd	AnyConnect Client Image	
AnyConnect_Management_Tunnel	AnyConnect_Management_Tunne	AnyConnect Management VPN Profile	
SSL_AnyConnect.xml	SSL_AnyConnect.xml	AnyConnect VPN Profile	

Displaying 1 - 3 of 3 rows << Page 1 of 1 >>

Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To

Stap 4. Groepsbeleid maken

Als u een nieuw Groepsbeleid wilt maken, navigeer dan naar **Objecten > Objectbeheer** en kies **VPN** optie uit de inhoudsopgave, selecteer **Groepsbeleid** en klik op de knop **Toevoegen groepsbeleid**.

Zodra het venster **Add Group Policy** wordt geopend, selecteert u een naam, definieert u een AnyConnect-pool en opent u het tabblad **AnyConnect**. Navigeren in op **Profile** en selecteer het object dat het normale AnyConnect VPN-profiel in het vervolgkeuzemenu van **Clientprofiel** vertegenwoordigt.

Overview Analysis Policies Devices **Objects** AMP Intelligence Deploy System Help dperezve

Object Management Intrusion Rules

Group Policy
A Group Policy is a set of attribute and value pairs, profile.

Edit Group Policy Name: * Description:

General **AnyConnect** **Advanced**

Profile
Management Profile
Client Modules
SSL Settings
Client Profile: **SSL_AnyConnect.xml**

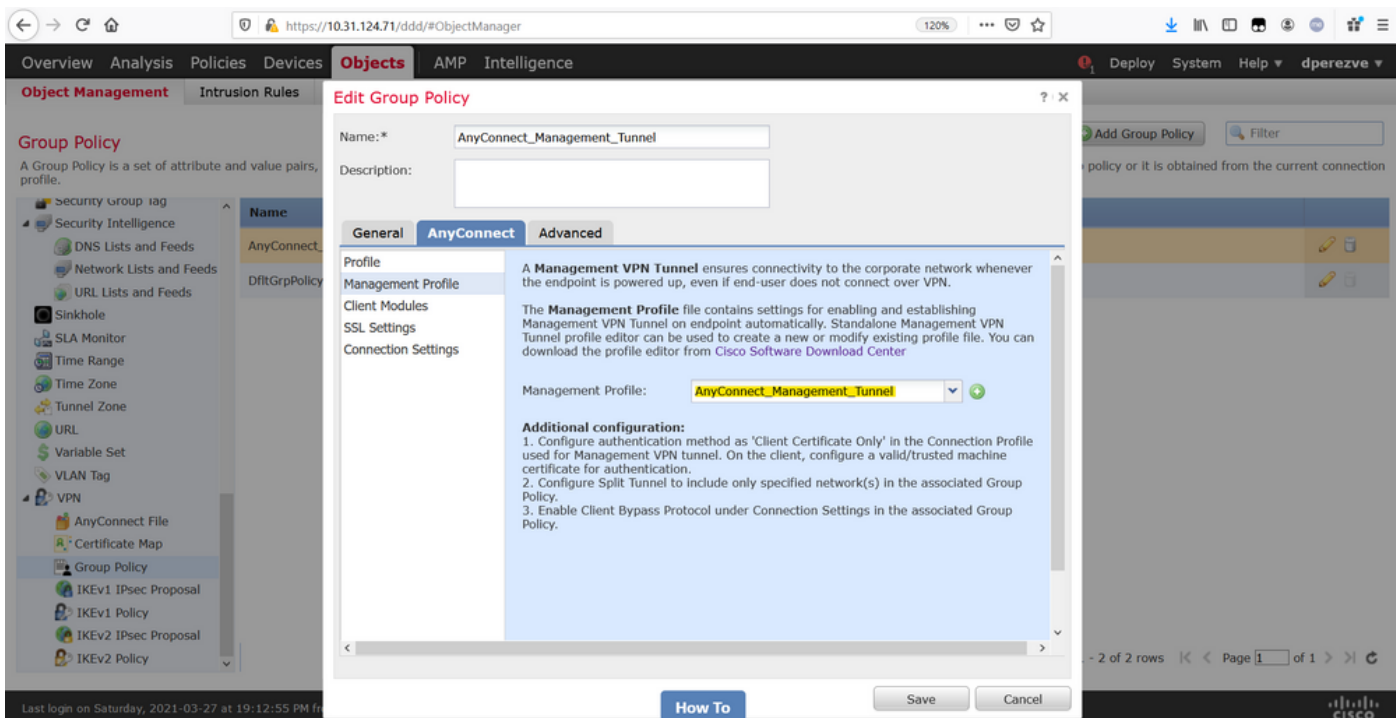
Standalone profile editor can be used to create a new or modify existing AnyConnect profile. You can download the profile editor from [Cisco Software Download Center](#).

Save Cancel

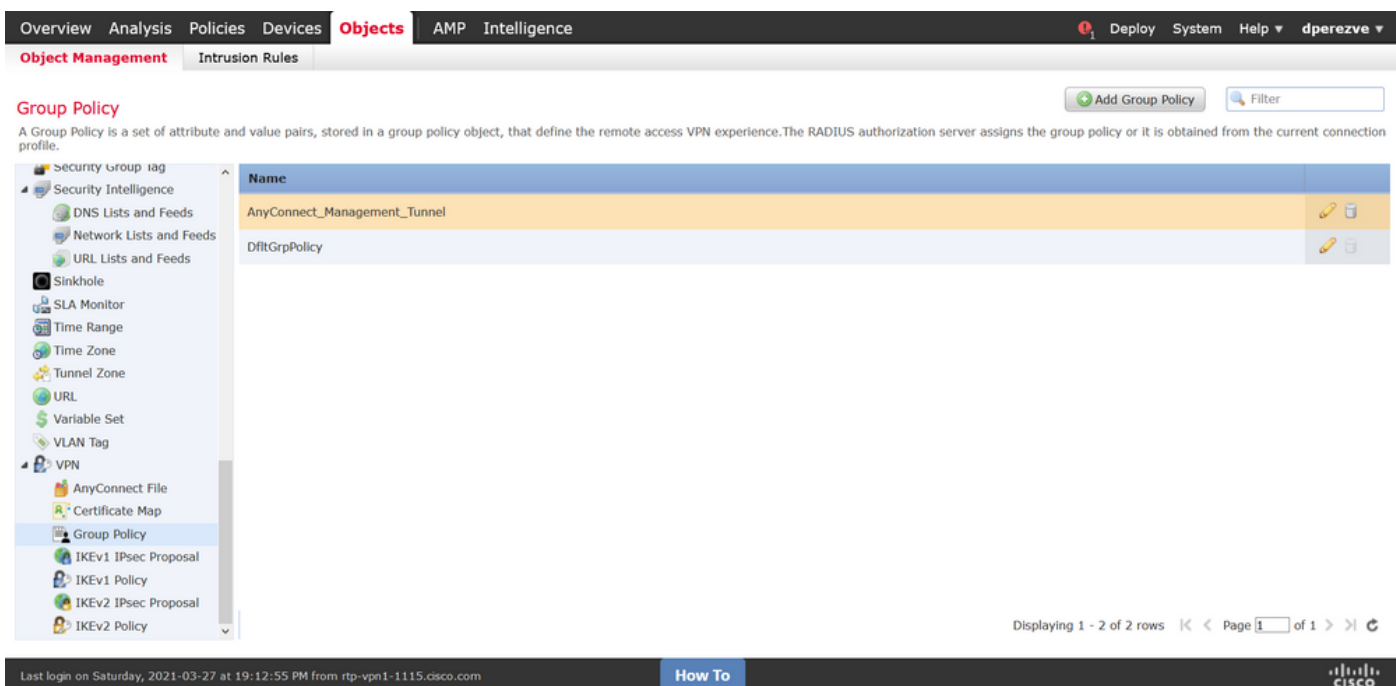
Displaying 2 of 2 rows << Page 1 of 1 >>

Last login on Saturday, 2021-03-27 at 19:12:55 PM How To

navigeren naar het tabblad **Management Profile** en selecteer het object dat het VPN-profiel beheren in het vervolgkeuzemenu **Management Profile** bevat.



Sla de wijzigingen op om het nieuwe object aan het bestaande groepsbeleid toe te voegen.



Stap 5. Maak een nieuwe AnyConnect-configuratie

De configuratie van SSL AnyConnect in FMC is samengesteld uit 4 verschillende stappen. Om AnyConnect te configureren stuurt u naar **Apparaten > VPN > Externe toegang** en selecteert u de knop **Add**. Hierdoor moet de **VPN-beleidswizard Externe toegang** openen.

Selecteer in het tabblad **Policy Assignatie** het FTD-apparaat in handen, definieer een naam voor het verbindingsprofiel en controleer het SSL-selectieteken.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Dashboards Reporting Summary

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 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-IKEv2

Targeted Devices:

Available Devices:
 ftdv-dperezve
 ftdv-fejimene

Selected Devices: ftdv-dperezve

Before You Start

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

Authentication Server
Configure [Realm](#) or [RADIUS Server Group](#) or [SSO](#) to authenticate VPN clients.

AnyConnect Client Package
Make sure you have AnyConnect 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.

Last login on Thursday, 2021-03-25 at 17:01:05 PM from rtp-vpn6-107.cisco.com How To

Selecteer in **Connection Profile** alleen het **Clientcertificaat** als verificatiemethode. Dit is de enige echtheidscontrole die voor de functie wordt ondersteund.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

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

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

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:

Username From Certificate: (Distinguished Name) as username

Primary Field:

Secondary Field:

Authorization Server: (Realm or RADIUS)

Accounting Server: (RADIUS)

Client Address Assignment:

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

Use AAA Server (Realm or RADIUS only) ?

Use DHCP Servers

Use IP Address Pools

Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To

Selecteer vervolgens het object Group Policy dat in stap 3 is gemaakt in de vervolgkeuzelijst **Groepsbeleid**.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

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

Authorization Server: (Realm or RADIUS)

Accounting Server: (RADIUS)

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

Use AAA Server (Realm or RADIUS only) i

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

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

Group Policy:*

^

v

Back Next Cancel

Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To

Selecteer op **AnyConnect** het **AnyConnect File Object** op het eindpunt in overeenstemming met het besturingssysteem.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

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

AAA

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

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

[Show Re-order buttons](#)

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	Anyconnect4.9_For_Windows	anyconnect-win-4.9.01095-webdeploy-k9.pkg	Windows <input type="text" value="Windows"/>

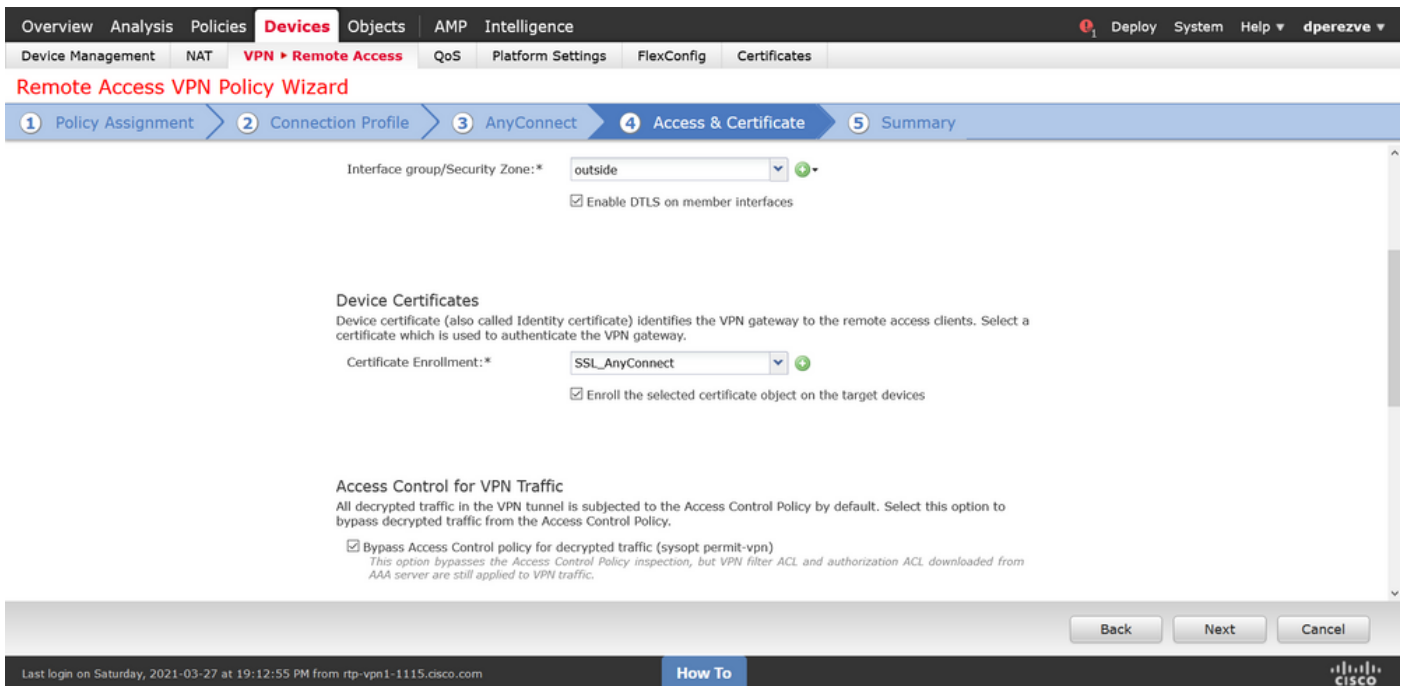
Back Next Cancel

Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To

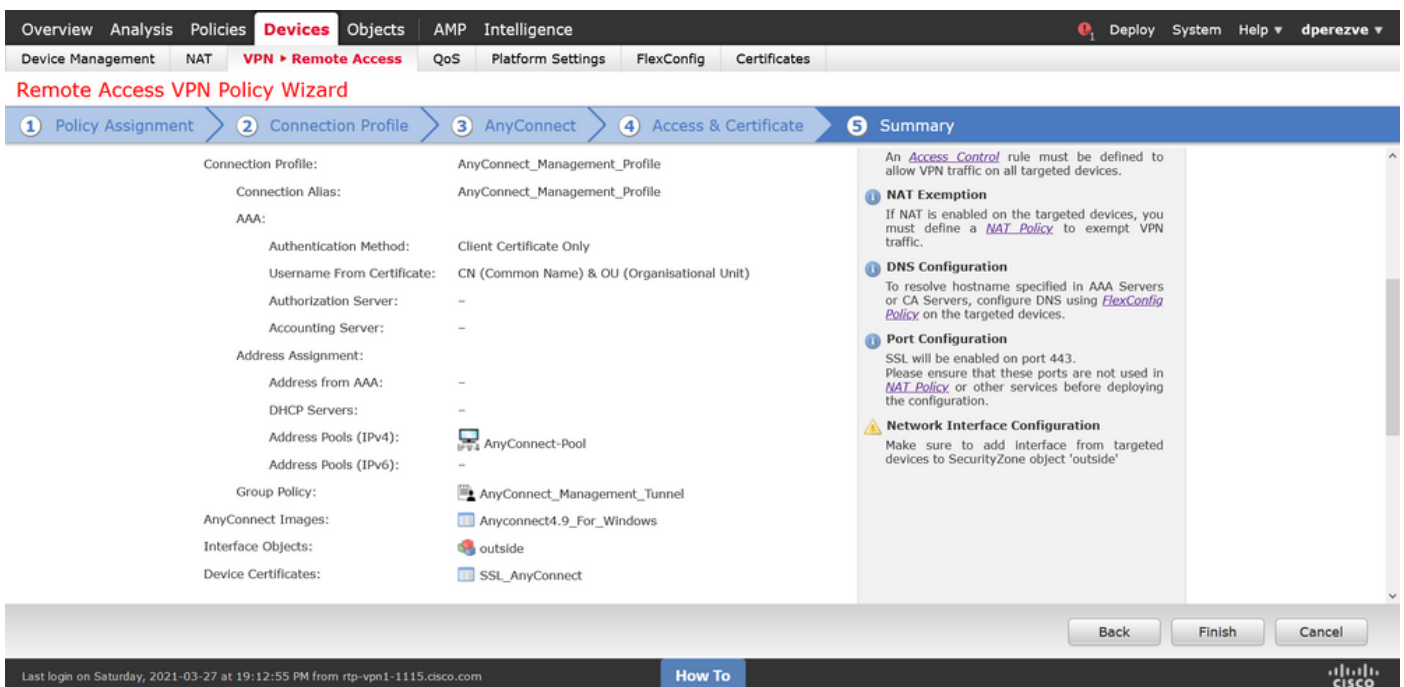
Specificeer op **Access & Certificate** dat door de FTD moet worden gebruikt om zijn identiteit aan de Windows-client te controleren.

Opmerking: Aangezien gebruikers geen contact moeten opnemen met AnyConnect-app wanneer ze de functie Management VPN gebruiken, moet het certificaat volledig worden vertrouwd en mag u geen waarschuwingsbericht afdrucken.

Opmerking: Om fouten in de validering van certificaten te voorkomen, moet het veld Gemeenschappelijke Naam (GN) dat in de Onderwerp Naam van het certificaat is opgenomen, overeenkomen met de FQDN die is gedefinieerd in de lijst van XML-profielen van de server (Stap 1 en Stap 2).



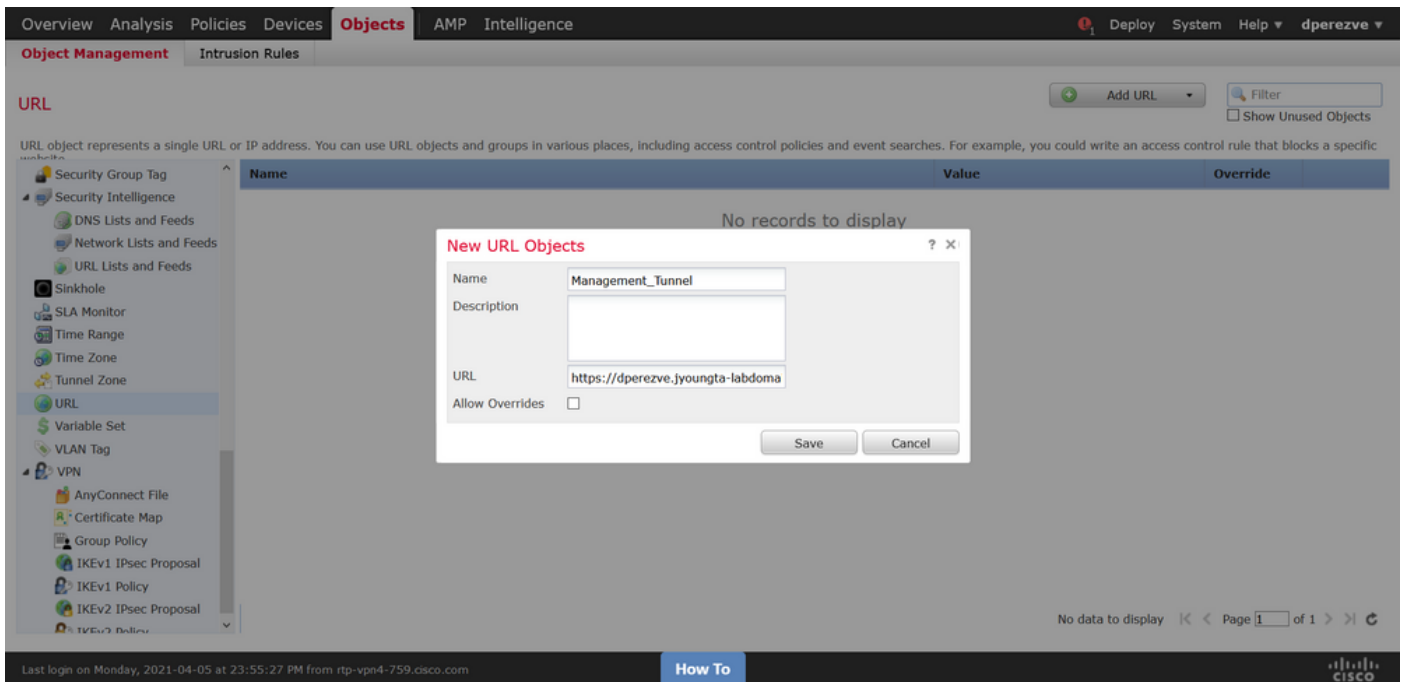
Tenslotte selecteert u de knop **Voltooien** in het **tabblad Samenvatting** om de nieuwe AnyConnect-configuratie toe te voegen.



Stap 6. URL-object maken

Navigeer aan **Exemplaar > Objectbeheer** en selecteer **URL** uit de inhoudsopgave. Selecteer vervolgens **Object toevoegen** in de vervolgkeuzelijst **URL** toevoegen.

Geef een naam voor het object op en definieer de URL met behulp van dezelfde FQDN/gebruikersgroep die in de Lijst van VPN-profiel van beheer is gespecificeerd (Stap 2). In dit voorbeeld moet URL `dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel` zijn.

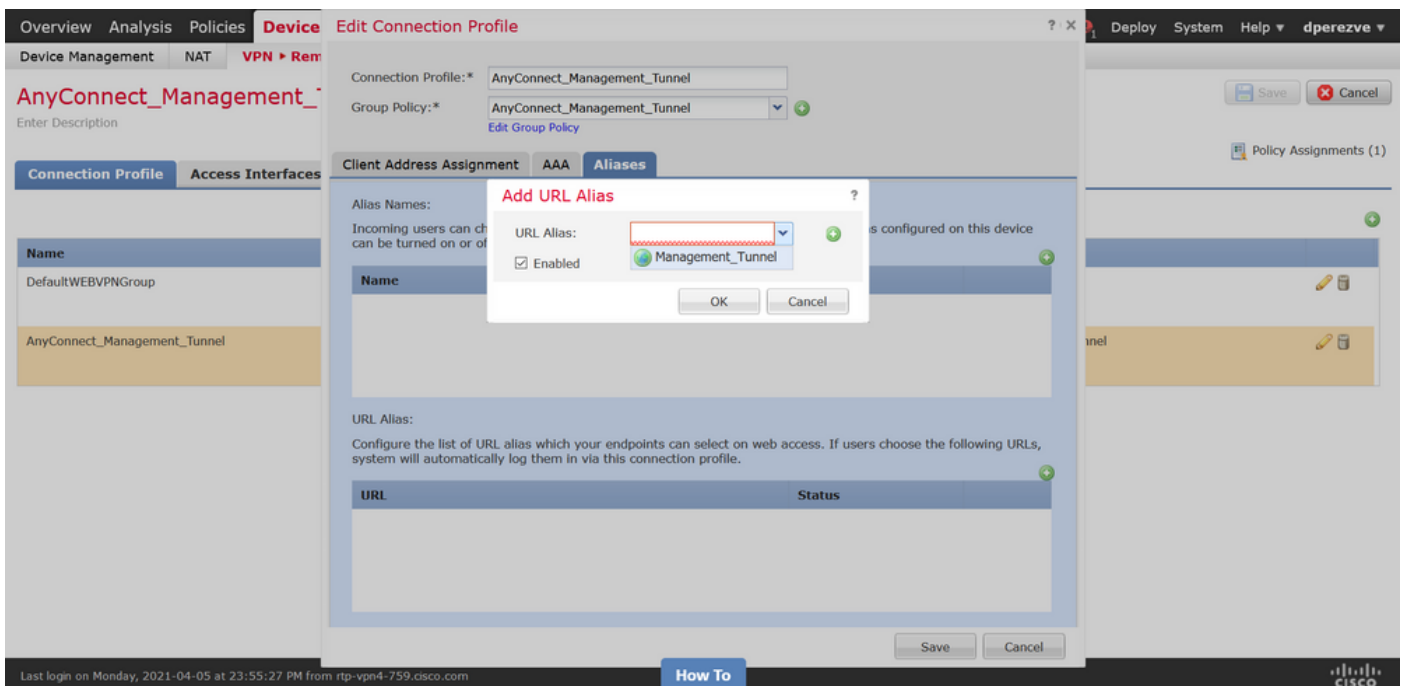


Sla de wijzigingen op om het object aan de lijst toe te voegen.

Stap 7. Bepaal URL-alias

Om de URL-alias in de AnyConnect-configuratie in te schakelen, navigeert u op **Apparaten > VPN > Externe toegang** en klikt u op het potlood-pictogram om te bewerken.

Vervolgens selecteert u op het tabblad **Connection Profile** de configuratie in uw hand, navigeer naar **Aliases**, klik op **Add** en selecteer u het **URL-object** in de lijst **URL Alias**. Zorg ervoor dat het aankruisvakje **Ingeschakeld** is geselecteerd.



Wijzigingen opslaan en configuraties op FTD implementeren.

Verifiëren

Nadat de implementatie is voltooid, is er een eerste handmatige AnyConnect-verbinding met het AnyConnect VPN-profiel nodig. Tijdens deze verbinding wordt het VPN-profiel van het beheer gedownload van FTD en opgeslagen in **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**. Vanaf dit punt moeten de volgende verbindingen via het VPN-profiel van het beheer zonder enige gebruikersinteractie worden geïnitieerd.

Problemen oplossen

Voor fouten in certificatie:

- Zorg ervoor dat het basiscertificaat voor de certificeringsinstantie (CA) op het FTD is geïnstalleerd.
- Zorg ervoor dat een identiteitsbewijs dat is ondertekend door dezelfde CA is geïnstalleerd in Windows Machine Store.
- Zorg ervoor dat het GN-veld in het certificaat is opgenomen en hetzelfde is als de FQDN die is gedefinieerd in de serverlijst van het VPN-profiel van het beheer en FQDN die is gedefinieerd in URL-alias.

Voor niet geïnitieerde beheertunnel:

- Zorg ervoor dat het VPN-profiel van het beheer is gedownload en opgeslagen in **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**.
- Zorg ervoor dat de naam voor het VPN-profiel van het beheer is **VPNMgmtTunProfile.xml**.

Voor aansluitingsproblemen verzamelt u DART-bundel en neemt u contact op met Cisco TAC voor verder onderzoek.