

# Plug en afspelen configureren in RV160- en RV260-routers

## Doel

Het doel van dit document is om u te tonen hoe u Plug and Play (VPPN) en PnP-ondersteuning kunt configureren op RV160- en RV260-routers.

## Inleiding

Cisco Open Plug-n-Play (PPP)-agent is een softwaretoepassing voor Cisco Small Business-apparaten. Wanneer een apparaat wordt ingeschakeld, probeert het proces voor de ontdekking van de agent Open PnP, dat in het apparaat is ingesloten, het adres van de Open PPP-server te vinden. De Open PPP-agent gebruikt methoden als Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) en Cisco Cloud Service Discovery om het gewenste IP-adres van de Open VPN-server te verkrijgen. Vereenvoudigd implementatieproces van Cisco Small Business-apparaat automatiseert de volgende implementatiegerelateerde operationele taken:

- Het instellen van initiële netwerkconnectiviteit voor het apparaat.
- Apparaatconfiguratie leveren.
- Beelden van firmware leveren.

Ondersteuning van PnP werd geïntroduceerd in de Small Business-omgeving met FindIT 1.1, die fungeert als de PnP-server.

Sommige termen om vertrouwd te zijn met betrekking tot VPPN en FindIT:

- Een **afbeelding** is een firmware-update voor een PnP-enabled apparaat.
- Een **Configuration** is een configuratiebestand dat naar het apparaat moet worden gedownload. De configuratiebestanden bevatten alle informatie die een apparaat nodig heeft om aan een netwerk deel te nemen, zoals gateway, IP-adressen van bekende apparaten, beveiligingsinstellingen enzovoort.
- Een **apparaat dat niet wordt geclaimd** is een apparaat dat is ingeschakeld in de VPN-server, maar er is geen afbeelding of configuratie aan toegewezen.
- **Provisioning** is de handeling van het leveren van apparaten met beelden of configuraties.

## Toepasselijke apparaten

- RV160
- RV260

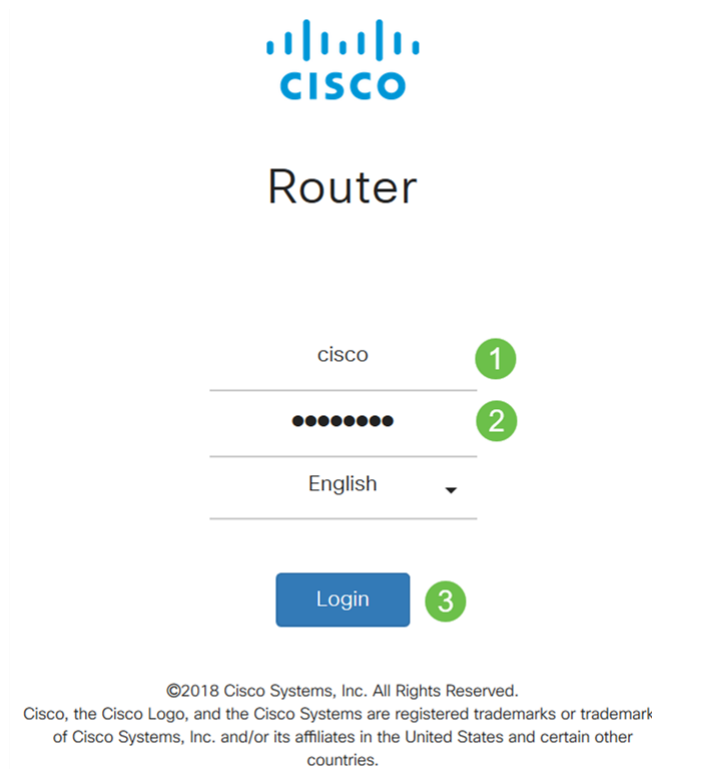
## Softwareversie

- 1.0.00.15

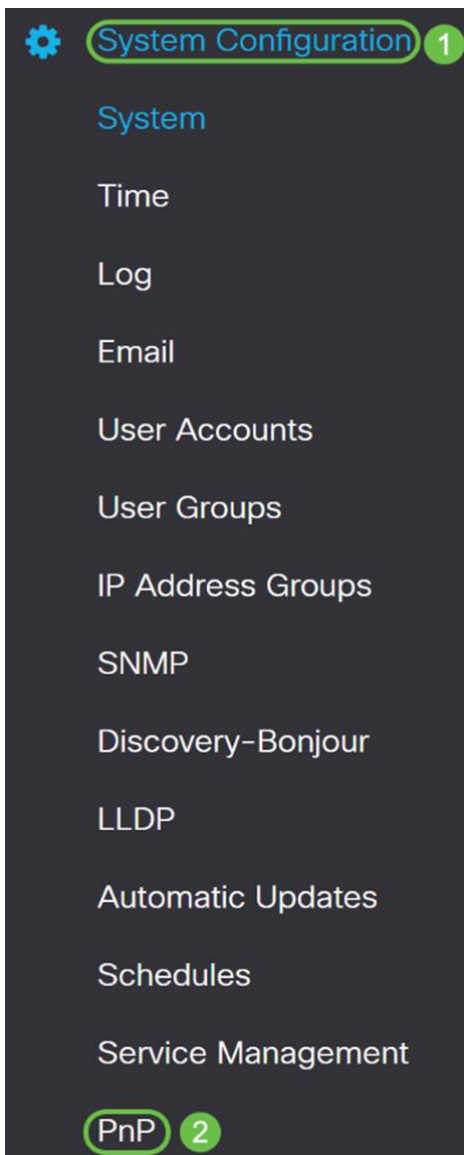
# PPPoP-routerconfiguratie

Apparaten moeten eerst worden geconfigureerd om in te checken op de VPN-server om provisioning te ontvangen. Om de router te configureren om in de FindIT Manager te controleren ter ondersteuning van VPNP, voert u de volgende stappen uit.

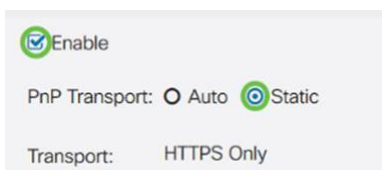
Stap 1. Meld u aan bij de webconfiguratie van uw router.



Stap 2. Navigeer naar **systemconfiguratie > PPP**.



Stap 3. Standaard is PnP in de router ingeschakeld en *PnP-transport* is ingesteld op *Auto* om de PnP-server automatisch te ontdekken. In dit voorbeeld was **Static** geselecteerd als de *PnP Transport* optie.



Opmerking: Anders dan switches ondersteunen de RV160/RV260-Series routers alleen gecodeerde VPN-communicatie (Hyper-Text Transfer Protocol Secure).

Stap 4. Voer het IP-adres in of de Full Qualified Domain Name (FQDN) van de FindIT-beheerder en het poortnummer als deze iets anders gebruikt dan Port 443. Standaard zal de router elk reeds vertrouwd certificaat van de certificaatinstantie (CA) vertrouwen. Indien gewenst kunt u ervoor kiezen alleen certificaten van een bepaalde certificeringsinstantie te vertrouwen door slechts één certificaat voor hoofdlettergebruik te selecteren.

In dit voorbeeld:

*IP/FQDN* is **FindIT.xxxx.net**.

*Port* is **443**.

*CA-certificaat* is **alles**.

IP/FQDN: findit. net **1**

Port: 443 **2**

CA Certificate: All **3**

Stap 5. Klik op **Toepassen**.

PnP Apply Cancel

Enable

PnP Transport:  Auto  Static

Transport: HTTPS Only

IP/FQDN: findit. net

Port: 443

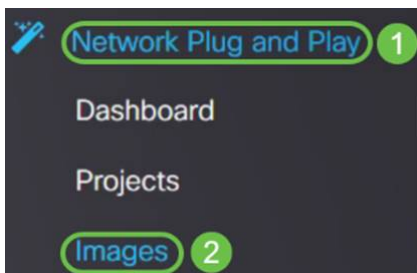
CA Certificate: All

## Afbeelding of configuratie uploaden

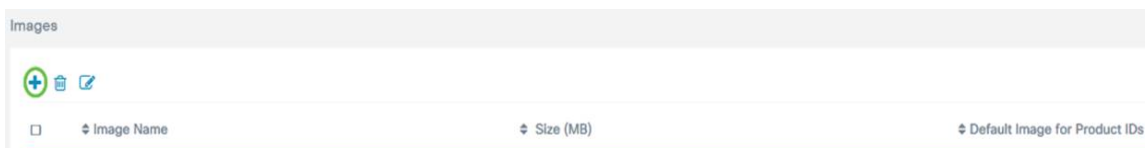
Om een lage temperatuur te bereiken, of geen aanraakimplementaties, moeten de configuratie- of beeldbestanden beschikbaar zijn aan het apparaat voordat u het apparaat voor het eerst inschakelt. Voer de volgende stappen uit om een afbeelding of een configuratie te uploaden naar de FindIT Manager om deze in VPN-apparaten in te zetten.

Stap 1. Sluit aan op de FindIT Network Manager en ga naar **Network Plug en Play** en kies *Afbeeldingen of Configuraties*.

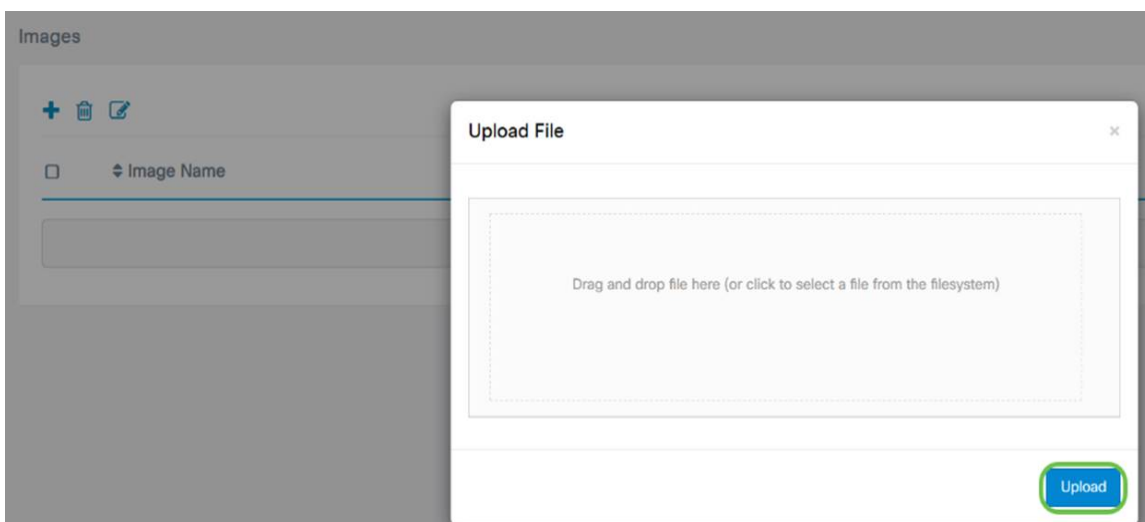
In dit voorbeeld zijn **Afbeeldingen** geselecteerd.



Stap 2. Klik op het pictogram **Add** om een beeldbestand toe te voegen.



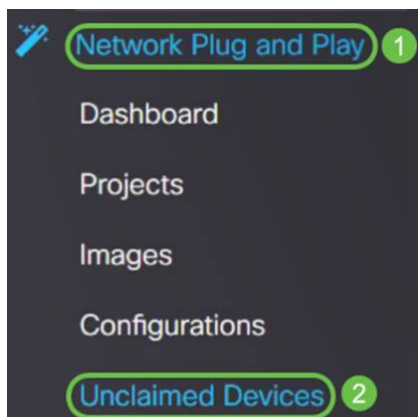
Stap 3. Sleep het firmware-bestand van een map naar het browser en kies **Upload**.



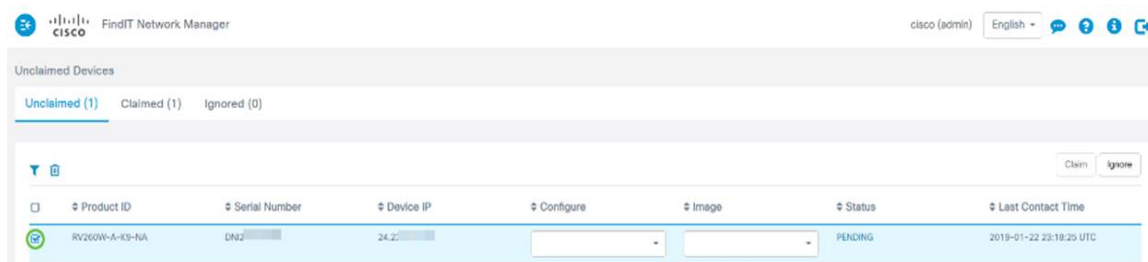
# Apparaten opeisen

Nadat de firmware of de configuratie is geüpload, kunt u een apparaat opvragen dat is ingeschakeld. Door een apparaat op te eisen, kan een FindIT-server een configuratie of afbeelding voor dat apparaat inzetten.

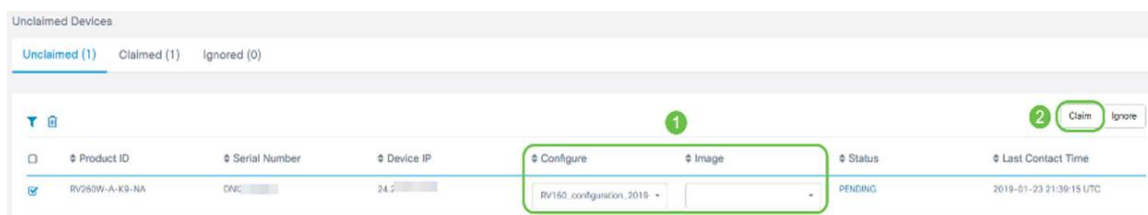
Stap 1. Meld u aan bij FindIT Manager en navigeer naar **Network Plug en Play > Unclaimapparaten**.



Stap 2. Pak het apparaat vast onder *Niet-geclaimde* apparaten en selecteer het.



Stap 3. Kies de configuratie of het beeld dat u wilt toepassen en klik op **claimen**. In dit voorbeeld is een configuratiebestand geselecteerd. Hierdoor wordt het apparaat van het tabblad *Unclaimd* naar het tabblad verplaatst en wordt de configuratie van de machine de volgende keer dat het apparaat controleert op de server.



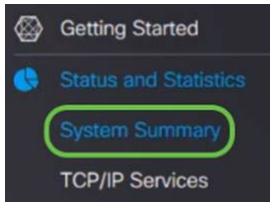
## PnP omkeren

Standaard is PnP ingeschakeld op de RV160/RV260-routers en is deze ingesteld om de VPN-server automatisch te detecteren. Dit kan voorkomen vanaf een DHCP-server, DNS-query of Cisco's apparaatHelp-website.

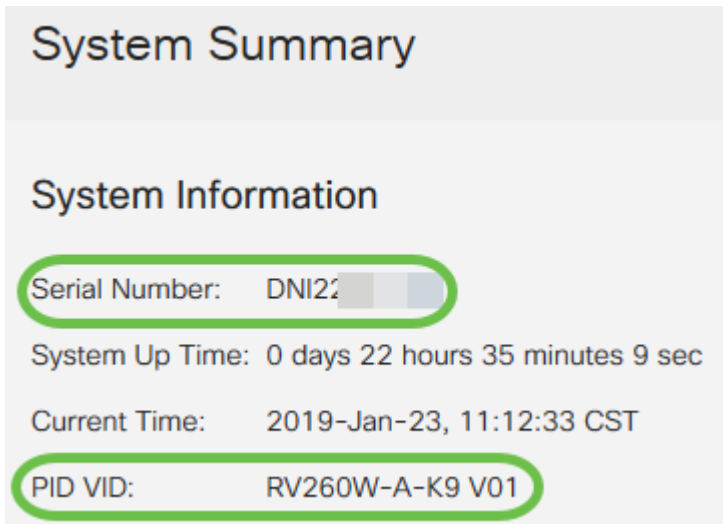
Dankzij de automatische omleiding van VPN kunt u de website van de hulp van Cisco-apparaat (<https://software.cisco.com>) gebruiken om apparaten die PnP-functie hebben ingeschakeld van meerdere netwerken automatisch aan te sluiten op de gewenste PnP-server. U kunt de configuraties en afbeeldingen van een groot aantal apparaten extern verwerken.

Voer de volgende stappen uit om de VPN-omleiding te configureren.

Stap 1. Meld u aan bij het webprogramma van de router. Navigeer naar **systemoverzicht**.



Stap 2. Verkrijg het *serienummer* en modelnummer (*PID VID*) van de router uit de *systeminformatie*.



Stap 3. Ga naar de Cisco Software Central-website (<https://software.cisco.com>)

Stap 4. Meld u aan bij uw Cisco Smart-account en navigeer naar *Plug en Play Connect*.



## Network Plug and Play

### Plug and Play Connect

Device management through Plug and Play Connect portal

[Learn about Network Plug and Play](#)

Training, documentation and videos

Stap 5. Navigeer naar **Controller profielen** om details betreffende de server toe te voegen.

[Cisco Software Central](#) > **Plug and Play Connect**

## Plug and Play Connect

Devices | **Controller Profiles** | Network | Certificates

Stap 6. Klik op *Add Profile...*

<input type="checkbox"/>	Profile Name	Controller Type
	<input type="text"/>	Any

Stap 7. Selecteer *Controller type* als **PNP-SERVER** en klik op **Volgende**.

Add Controller Profile ×

STEP 1 **Profile Type**    ...    Conditional Steps

Choose the type of Profile to be created:

\* Controller Type:  Cancel

Stap 8. Voer de verplichte velden in die *Profielnaam*, *Primaire controller* (om de URL op te nemen) bevatten en uploadde het Secure Socket Layer (SSL)-certificaat.

Profile Settings:

\* Profile Name:

Description:

Default Profile:


\* Primary Controller:

Host Name:     Protocol:     Port:

\* SSL Certificate:

Een voorbeeld van een *controllerprofiel* moet als volgt worden weergegeven:

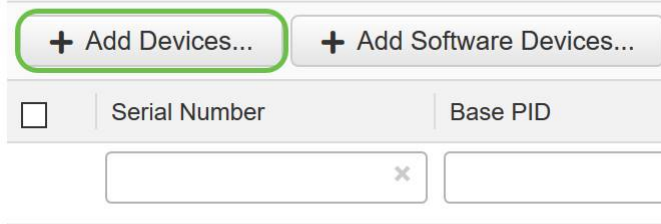
## Controller Profile

Profile Name:	TEST
Description:	Test profile
Deployment Type:	onPrem
Primary Host Name:	FindIT. 
Primary Protocol:	https
Primary Port:	443
Primary Certificate:	Uploaded
Controller Type:	PNP SERVER

Stap 9. Zodra het profiel is gebouwd, kunt u het apparaat toevoegen. U navigeert als volgt

naar *Apparaten* en klikt op **Apparaten toevoegen...**

**Devices** | Controller Profiles | Network | Certificates



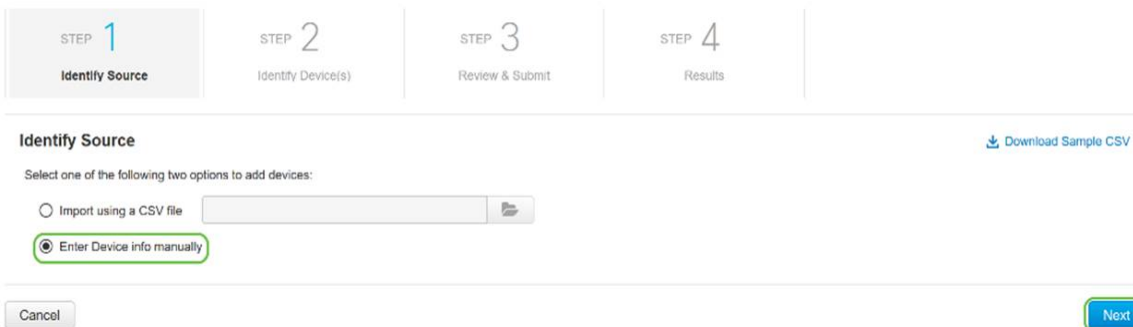
Stap 10. Voeg apparaten toe met behulp van *een CSV-bestand of Voer handmatig apparaatinformatie in.*

Opmerking: Als u een groot aantal apparaten wilt toevoegen, gebruikt u de optie *Importeren met een CSV-bestand.*

In dit voorbeeld wordt **handmatig Voer** apparaatinformatie in.

Klik op **Volgende.**

Add Device(s)



Stap 1. Klik op **Apparaat identificeren...**

Add Device(s)



### Identify Devices

Enter device details by clicking Identify Device button and click Next to p



Stap 12. Voer het *serienummer, Base PID, Controller informatie over het profiel en beschrijving in.*

Klik op **Opslaan.**



## Identify Device



\* Serial Number **1**

\* Base PID **2**

Controller Profile **3**

Description **4**

Cancel

Save

Stap 13. Controleer de instellingen en klik op **Indienen**.

Add Device(s)

STEP 1 ✓ Identify Source

STEP 2 ✓ Identify Device(s)

STEP 3 Review & Submit

STEP 4 Results

### Review & Submit

Submit action will submit following 1 newly identified device(s).

Row	Serial Number	Base PID	Certificate Serial Number	SDWAN Type	Controller	Description
1	DNI2-	RV260W-A-K9-NA	--	--	TEST	RV260W-Test

Showing 1 Record

Cancel

Back

Submit

Stap 14. Er verschijnt een resultaat scherm over de geslaagde toevoeging van het apparaat. Klik op **Klaar**.

Add Device(s)

STEP 1 ✓ Identify Source

STEP 2 ✓ Identify Device(s)

STEP 3 ✓ Review & Submit

STEP 4 Results

### Attempted to add 1 device(s)



Successfully added 1 device(s) 1

It may take a few minutes for the new devices to show up in the Devices table. Please wait a minute or two and refresh the page as needed.

Done

Stap 15. Kort na de router zal u inchecken op de server. Regelmatig zal de router zich na het herstarten aansluiten op de server. Dus is omleiding niet nodig. Dit duurt een paar minuten.

[+ Add Devices...](#)
[+ Add Software Devices...](#)
[/ Edit Selected...](#)
[Delete Selected...](#)
↻

<input type="checkbox"/>	Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
<input type="checkbox"/>	DN12	RV260W-A-K9-NA	Router	TEST	2019-Jan-23, 15:43:33	Pending (Redirection)	Show Log... ▼

Showing 1 Record

Wanneer de router de server contacteert, zult u het volgende scherm zien.

[+ Add Devices...](#)
[+ Add Software Devices...](#)
[/ Edit Selected...](#)
[Delete Selected...](#)
↻

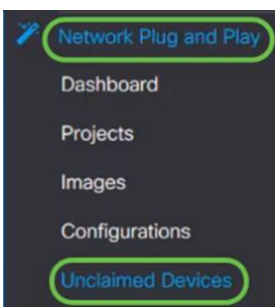
<input type="checkbox"/>	Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
<input checked="" type="checkbox"/>	DN12	RV260W-A-K9-NA	Router			Contacted	Show Log... ▼

U krijgt het volgende scherm zodra de omleiding is geslaagd.

[+ Add Devices...](#)
[+ Add Software Devices...](#)
[/ Edit Selected...](#)
[Delete Selected...](#)
↻

<input type="checkbox"/>	Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
<input type="checkbox"/>	DN12	RV260W-A-K9-NA	Router			Redirect Successful	Show Log... ▼

Stap 16. Om te zien of het apparaat in de FindIT Manager is ingeschakeld, gaat u naar FindIT Manager. Blader naar **netwerkstekker en afspelen > Niet-geclaimde apparaten**.



Stap 17. Zie dat het apparaat was ingecheckt bij de FindIT-beheerder. U kunt vervolgens de configuraties of afbeeldingen beheren voor de RV160 of RV260.

Unclaimed Devices

[Unclaimed \(1\)](#) [Claimed \(1\)](#) [Ignored \(0\)](#)

<input type="checkbox"/>	Product ID	Serial Number	Device IP	Configure	Image	Status
<input type="checkbox"/>	RV260W-A-K9-NA	DN12	24.2			PENDING

## Conclusie

U had nu met succes een PPP op de RV160/RV260-routers moeten configureren.

Voor het configureren van VPNP in RV34x Series routers, klik [hier](#).

Klik [hier](#) voor meer informatie over FindIT Network Management.

Als u meer wilt weten over FindIT en Network VPNP, klikt u [hier](#).

Klik [hier](#) voor meer informatie over hoe u een slimme account kunt aanvragen.

Als u meer wilt weten over het registreren van FindIT Network Manager op Cisco Smart-account, klikt u [hier](#).

## Bekijk een video gerelateerd aan dit artikel...

[Klik hier om andere Tech Talks uit Cisco te bekijken](#)