Begrijp Switch Onboarding via Catalyst Center Plug and Play

Inhoud

Inleiding

Beschrijving

publiek

Vereisten

Voorwaarden

Plug and PlayConceptOverzicht

- 1. DHCP-detectie van PnP-server
- 2. DHCP Option 43-indeling
  - Optie 43 Velddefinities
- 3. Voorbeelden van de configuratie van DHCP Option 43
- 4. PnP-opstartgedrag

CatalystCenter-certificaatverificatie

- GUI-verificatie
- CLI-verificatie

Netwerkdiagram

SwitchOnboardingMethods

- 1. Aan boord met VLAN1
- 2. Onboard met aangepaste VLAN
- 3. Switch aan boord met behulp van de beheerpoort
- 4. Logbestanden van de Switch-console

Onboarding-Switch naar CatalystCenter zonder Day-0-sjablonen

- 1. Om switch te claimen:
- 2. De switch benoemen en in kaart brengen:
- 3. SoftwareImage ofTemplate toewijzen (optioneel):
- 4. Voorzieningsmodellen
- 5. Samenvatting
- 6. Toezicht houden op de aanvraagprocedure

Onboarding Switch naar CatalystCenter met Day-0 templates

- 1. Maak een Day-0- of OnboardingTemplate
- 2. Sjabloondetails toevoegen
- 3. De template bewerken
- 4. Netwerkprofiel maken
- 5. Sjabloon toevoegen en netwerkprofielinstellingen bewerken
- 6. Het profiel opslaan
- 7. Een netwerkprofiel toewijzen aan de locatie waar de switch/switches aan boord moeten worden genomen
- 8. ClaimSwitches

9. Een naam voor de switch toewijzen en een site toewijzen
10. Een Day-0-sjabloon toewijzen
11. Templates voor voorzieningen
12. Samenvatting
13. Voortgang van de aanvraag monitoren
Verificatie
Bulkimport van apparaten in CatalystCenterPlug and Play-inventaris
1. Voorwaarden
2. Invoerprocedure in bulk
Probleemoplossing
1. PnP-connectiviteitsvalidatie
1.1. Bereikbaarheid van het ICMPR
1.2. HTTPHELLO-validatie
1.3. HTTPS-certificaat ophalen
1.4. PnP-profielstatus
2. DHCP-validatie
2.1. Toewijzing van DHCP-IP-adres controleren
2.2. Leaseserver bevestigen
2.3. Optie 43 valideren met behulp van foutopsporingslogboeken
beste praktijken

Inleiding

In dit document worden de plug-and-play van het Catalyst Center beschreven voor automatische onboarding van de switch, de volledige levenscyclus, detectiemethoden en probleemoplossing.

Beschrijving

Catalyst Center Plug and Play (PnP) automatiseert de onboarding van Cisco Catalyst switch via de Cisco IOS® XE embedded PnP-agent. Dit proces maakt veilige detectie, verificatie en initiële provisioning mogelijk met minimale handmatige inspanningen, waardoor implementaties aanzienlijk worden versneld en de consistentie van de configuratie wordt verbeterd. Door schaalbare implementaties te ondersteunen via gestandaardiseerde instellingen en optionele Day-0-sjablonen, zorgt PnP voor een betrouwbare implementatie op grote schaal.

Het document beschrijft de volledige levenscyclus van onboarding, inclusief PnP-workflows, detectiemethoden, onboardingopties en certificaatvalidatie. Het biedt ook gedetailleerde richtlijnen voor het claimen van apparaten, verificatie, probleemoplossing en best practices in de branche.

publiek

Dit document is bestemd voor netwerkbeheerders, implementatietechnici en systeemintegrators die Cisco Catalyst-switches implementeren en beheren via Catalyst Center.

Vereisten

Het verdient de voorkeur dat de lezers van dit document een fundamentele praktische kennis hebben van deze onderwerpen:

- katalysatorcentrum
- Cisco Catalyst-switches
- Netwerkautomatisering en -provisioning
- DHCP en DNS fundamentals

Voorwaarden

Zorg ervoor dat aan deze voorwaarden is voldaan voordat u het onboardingproces start:

- Catalyst Center 2.3.7.9 of hoger is geïnstalleerd en operationeel.
- Cisco Catalyst-switches voeren een ondersteunde Cisco IOS XE-release 16.12.x of hoger uit.
- Er is netwerkconnectiviteit beschikbaar tussen de Catalyst switches en het Catalyst Center.
- De DHCP-server is geconfigureerd met optie 43 die verwijst naar het IP-adres of FQDN van de bedrijfsinterface van het Catalyst Center.
- Switches zijn in de fabrieksinstellingen (out-of-box) staat, en de pnpa service reset opdracht beschikbaar op IOS XE 16.12.1 en hoger kan worden gebruikt om een switch te resetten naar deze staat.

Plug and Play Concept Overzicht

Bekijk deze kernconcepten die uitleggen hoe Catalyst Center Plug and Play aan boord van een nieuwe switch is.

1. DHCP-detectie van PnP-server

Wanneer een standaard Cisco Catalyst-switch in de fabriek wordt ingeschakeld, probeert de PnP-agent een Plug and Play-controller (zoals Catalyst Center) te vinden met behulp van DHCP.

Het detectieproces maakt gebruik van de standaard DHCP-uitwisseling:

- DHCP Discover
- DHCP-aanbieding
- DHCP-aanvraag
- DHCP-bevestiging

Indien correct geconfigureerd, bevat de DHCP-server Option 43, die de switch voorziet van verbindingsgegevens voor de PnP-server.

2. DHCP Option 43-indeling

De waarde DHCP Option 43 is een door een puntkomma gescheiden ASCII-tekenreeks die aangeeft hoe de switch verbinding maakt met de PnP-server.

Voorbeeld:

```
option 43 ascii 5A1N;B2;K4;I10.127.212.43;J80;
```

Optie 43 Velddefinities

- 5A1N
  - 5 – PnP-suboptie
  - A – Actieve modus (apparaat initieert communicatie)
  - 1 – PnP-agentsjabloonversie
  - N – Foutopsporing uitgeschakeld (D maakt foutopsporing mogelijk)
- B2 – IP-adrestype PnP-server
  - 1 – Hostnaam
  - 2 – IPv4-adres
  - 3 – IPv6-adres
- K4 – Vervoerprotocol
  - 4 – HTTP
  - 5 – HTTPS
- I – IP-adres van PnP-server of FQDN
- J – TCP-poortnummer

Optionele parameters zijn onder meer:

- T – Trustpool certificaatbundel URL (verplicht voor HTTPS)

- Z – IP-adres van de NTP-server (verplicht bij gebruik van Trustpool-beveiliging)

3. DHCP Option 43-configuratievoorbeelden

- Voorbeeld 1: Optie 43 IPv4-configuratie: 10.127.212.43 [IP-adres Catalyst Center-bedrijfsinterface]

```
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B2;K4;I10.127.212.43;J80;
  default-router 10.127.212.49
```

- Voorbeeld 2: Configuratie hostnaam optie 43: catc1.cisco.com [Catalyst Center FQDN]

```
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B1;K4;Icatc1.cisco.com;J80;
  default-router 10.127.212.49
```

- Voorbeeld 3: Optie 43 IPv6-configuratie: 2001:60:60:60:133 [IPv6-adres Catalyst Center-bedrijfsinterface]

```
ipv6 dhcp pool pnp_pool
 address prefix 2001:70:70:70::/64
 link-address 2001:70:70:70::7/64
 vendor-specific 9
  suboption 16 ascii "ciscopnp"
  suboption 17 ascii "5A1D;B3;K4;I2001:60:60:60::133;J80"
```

4. Opstartgedrag van PnP VLAN

Standaard gebruikt een fabrieksreset-switch VLAN 1 voor PnP-beheer. Cisco raadt het gebruik van een dedicated beheer-VLAN in productieomgevingen aan. Dit is de opdracht voor het configureren van een aangepast PnP-opstart-VLAN:

```
pnp startup-vlan
```

Deze opdracht moet worden geconfigureerd op een upstream-switch. De upstream-switch communiceert het PnP-opstartprotocol met behulp van Cisco Discovery Protocol (CDP) met de nieuwe switch. De stroomafwaartse switch dan:

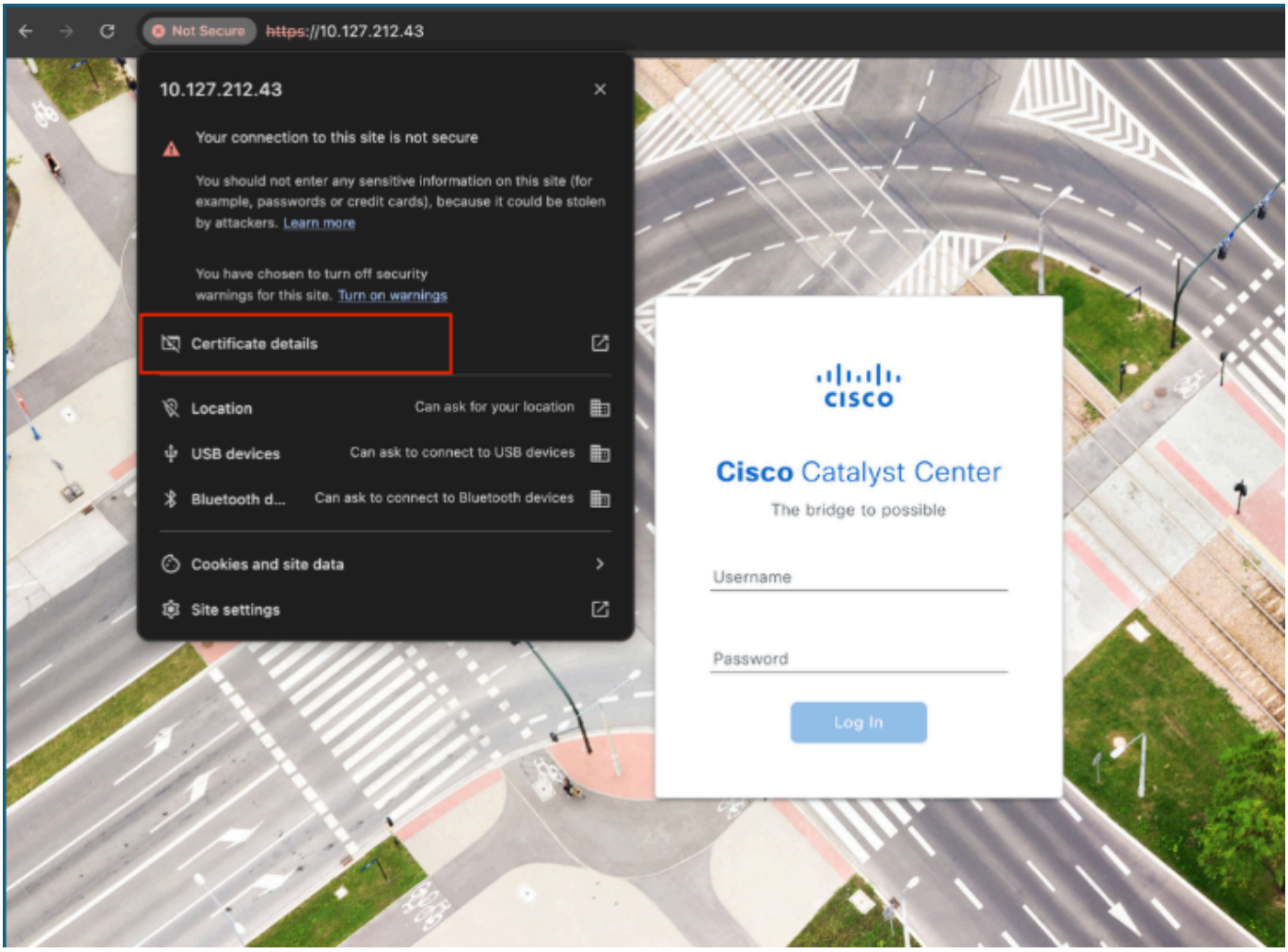
- Schakelt DHCP uit op VLAN 1
- Schakelt DHCP in op het geconfigureerde opstart-VLAN
- Hiermee wordt de trunk bijgewerkt om het nieuwe VLAN toe te staan

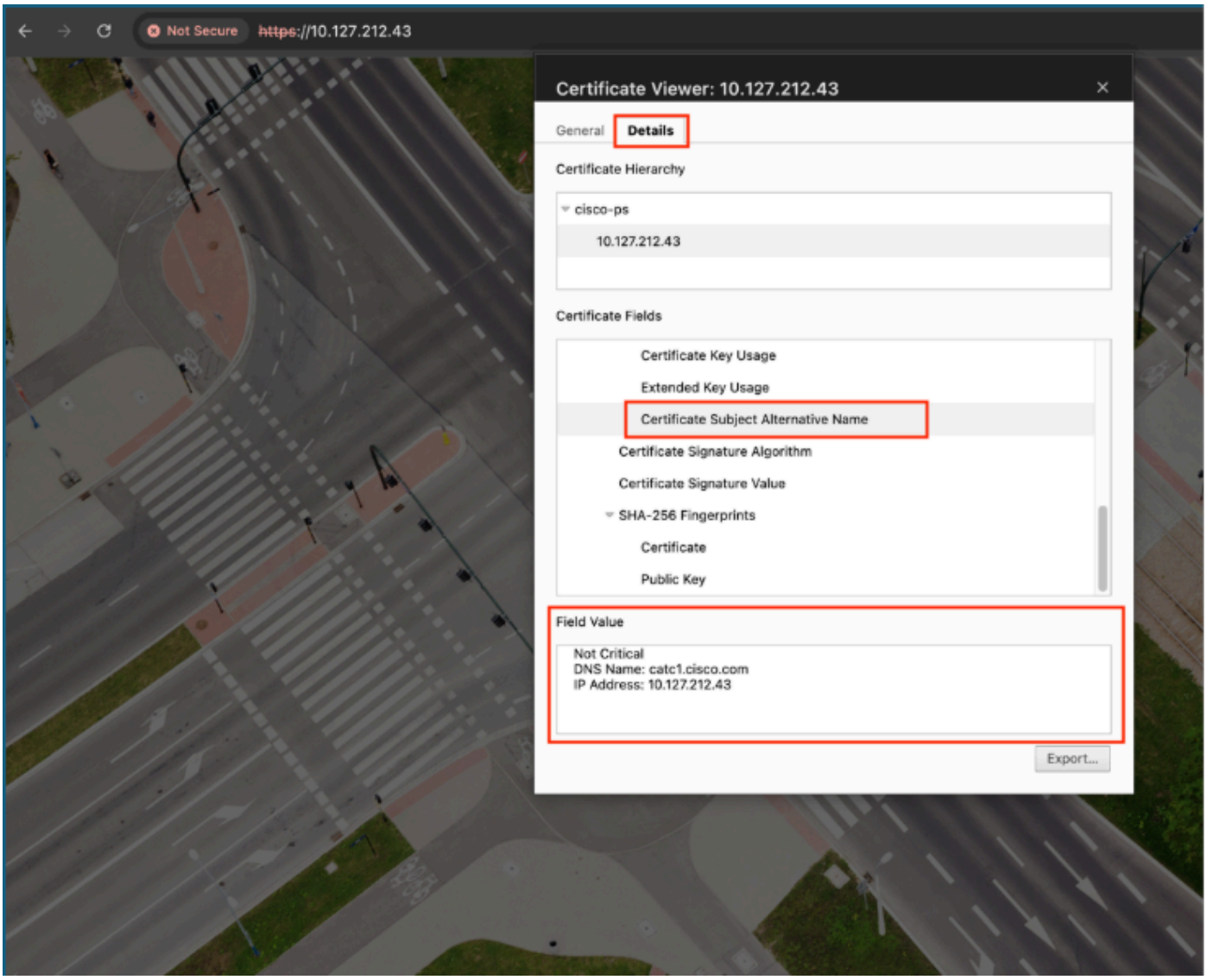
Certificaatverificatie Catalyst Center

Veilige onboarding vereist dat het SSL-certificaat van het Catalyst Center het IP-adres of de FQDN bevat die door de switch wordt gebruikt in het veld Alternatieve naam (SAN) van het onderwerp.

GUI-verificatie

1. Open de aanmeldingspagina van Catalyst Center in een browser
2. Sitegegevens bekijken
3. Open certificaatgegevens
4. SAN-items verifiëren onder Extensies





Opmerking: als het veld SAN of alternatieve onderwerpnaam het volgende bevat:

- Alleen DNS-naam – Configureer de DNS-naam in de optie 43-tekenreeks.
- Alleen IP-adres – Configureer het IP-adres in de optie 43 string.
- Zowel IP-adres als DNS-naam – Configureer het IP-adres in de optie 43-tekenreeks.

CLI-verificatie

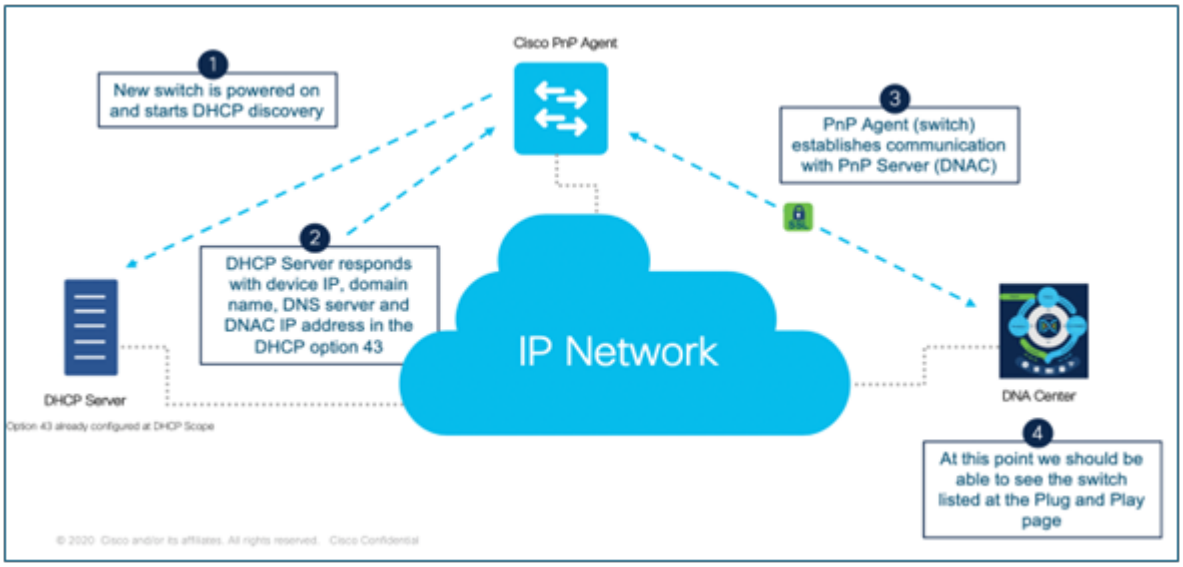
Om dit te verifiëren, hebben we het IP-adres van Catalyst Center en een machine nodig die de Catalyst Center-server kan bereiken. Voer deze opdracht uit in de terminal of bij de opdrachtprompt.

```
echo | openssl s_client -showcerts -servername

       -connect

       :443 2>/dev/null | openssl x509 -noout -text
```

Controleer of het SAN-veld het juiste IP-adres of FQDN bevat.

```
sitirkey@SITIRKEY-M-6PGJ netbox-docker % echo | openssl s_client -showcerts -servername 10.127.212.43 -connect 10.127.212.43:443 2>/dev/null | openssl x509 -inform
 pem -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 7523967389788466058 (0x686a807a31f6eb8a)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=IN, ST=Karnataka, L=Bangalore, O=cisco, OU=cisco-ps, CN=cisco-ps, emailAddress=sitirkey@cisco.com
        Validity
            Not Before: Jan  5 14:51:00 2026 GMT
            Not After : Jan  5 14:51:00 2027 GMT
        Subject: CN=10.127.212.43
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a5:ea:19:9e:b4:71:0d:97:fb:43:c5:ad:89:35:
                    69:2f:78:29:64:0a:b2:46:44:a7:89:98:a6:ff:71:
                    25:79:d2:53:0f:c0:c9:29:9d:c1:84:6a:16:4a:b4:
                    58:f5:46:ef:21:0a:79:71:b8:50:74:ff:29:86:cd:
                    6c:54:b6:91:62:8e:e4:20:5c:e9:38:66:84:40:97:
                    21:f8:73:27:49:2b:f3:09:86:08:1b:f5:d7:21:c8:
                    ad:8a:99:8e:55:9e:83:23:1e:f7:93:10:33:ee:08:
                    6b:2d:ad:57:7c:ba:af:21:44:67:d6:e4:b9:c5:e2:
                    88:b1:2f:ce:71:26:2a:68:ce:ea:29:65:6f:2b:47:
                    53:59:4d:5a:45:a3:03:1d:1c:fd:c9:58:f6:1d:c4:
                    49:b7:b9:36:0d:b7:6d:af:43:59:0c:ca:e0:d5:ef:
                    b7:86:92:31:bc:cd:66:e2:e8:ae:4c:68:7d:40:63:
                    45:c1:6a:e6:13:78:8e:cf:d5:42:07:04:2f:5f:80:
                    aa:ad:14:18:74:6f:47:f1:24:2b:93:47:a8:93:72:
                    8a:81:93:de:0b:41:b8:e7:5c:0a:10:e1:b2:46:06:
                    66:a7:9f:23:11:0d:e0:60:95:63:cb:ac:58:4f:6e:
                    04:a4:fd:d6:76:d4:5e:b4:e6:e4:25:50:04:30:07:
                    17:05
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                DNS:catc1.cisco.com, IP Address:10.127.212.43
    Signature Algorithm: sha256WithRSAEncryption
```

Netwerkdiagram



Cisco PnP automatiseert de onboarding van nieuwe apparaten door detectie, configuratie en beheer mogelijk te maken met minimale handmatige inspanning. Wanneer een nieuwe switch wordt ingeschakeld, verzendt deze een DHCP-detectieverzoek en retourneert de DHCP-server netwerkgegevens, waaronder het IP-adres van het Catalyst Center (PnP-server) via DHCP Option 43. Met behulp van deze informatie maakt de PnP-agent van de switch via het IP-netwerk een veilige verbinding met de PnP-server. Nadat de verbinding tot stand is gebracht, wordt het apparaat geverifieerd en geïdentificeerd en vervolgens toegevoegd aan de Plug and Play-inventaris, waar beheerders configuraties kunnen toepassen en de provisioning snel en consistent kunnen voltooien.

Onboarding-methoden voor switches

Bekijk de verschillende onboardingmethoden in dit gedeelte waarmee een switch kan worden ingescheept in de Plug and Play-inventaris van Catalyst Center.

1. Aan boord met VLAN1

Deze methode gebruikt de standaard VLAN 1 voor PnP-beheer

Vereisten

- VLAN 1 SVI is geconfigureerd op de upstream-switch.
- DHCP-server met optie 43 geconfigureerd
- DNS-resolutie voor het Catalyst Center FQDN

De procedure op de Upstream switch

Stap 1. SVI van VLAN 1 configureren.

```
config t
interface Vlan1
  ip address 10.127.212.49 255.255.255.0
```

Stap 2. Configureer een DHCP-pool met optie 43 (Opmerking: we kunnen de parameter Option 43 gebruiken met het IPv4-adres of FQDN van Catalyst Center).

```
config t
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B2;K4;I10.127.212.43;J80;
```

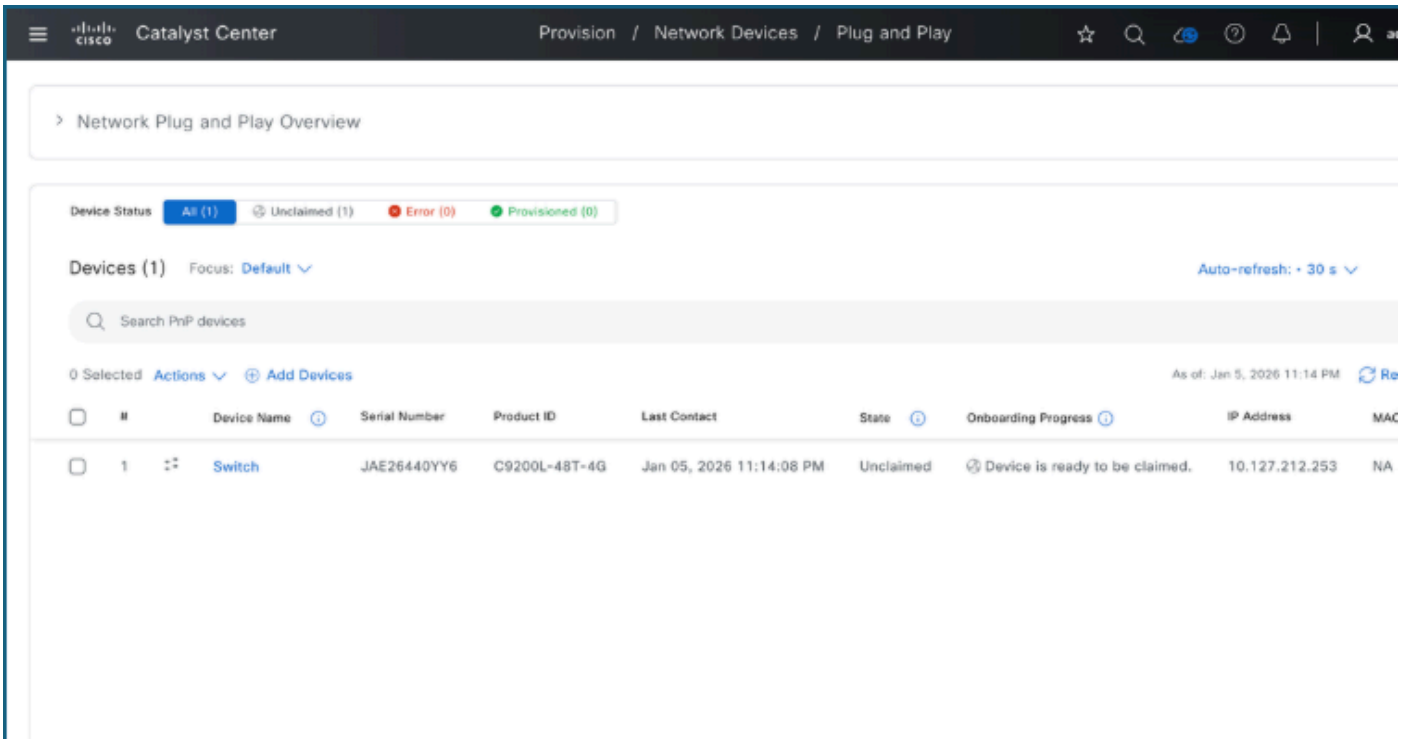
of

```
config t
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii5A1D;B1;K4;Icatc1.cisco.com;J80;
  default-router 10.127.212.49
  dns-server 10.127.212.1
```

Stap 3. Configureer een hoofdinterface voor de nieuwe switch.

```
config t
interface GigabitEthernet1/0/5
  description PnP_Trunk
  switchport mode trunk
```

Stap 4. Controleer of de switch wordt weergegeven op de pagina Voorzieningen > Plug and Play van Catalyst Center.



2. Onboard met aangepaste VLAN

Deze methode maakt gebruik van een speciaal VLAN voor beheer.

Vereisten

- Aangepaste VLAN SVI geconfigureerd op de upstream-switch.
- DHCP-server met optie 43 geconfigureerd.
- DNS-resolutie voor het Catalyst Center FQDN.
- Trunk maakt het aangepaste VLAN mogelijk, samen met andere VLAN's die nodig zijn voor ander verkeer.

Procedure op de upstream-switch

Stap 1. De SVI van het aangepaste VLAN configureren.

```
config t
interface Vlan302
  description PnP_Vlan
    ip address 10.127.212.49 255.255.255.0
```

Stap 2. Configureer een DHCP-pool met optie 43 (Opmerking: we kunnen de parameter Option 43 gebruiken met het IPv4-adres of FQDN van Catalyst Center).

```
config t
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B2;K4;I10.127.212.43;J80;
```

of

```
config t
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B1;K4;Icatc1.cisco.com;J80;
  default-router 10.127.212.49
  dns-server 10.127.212.1
```

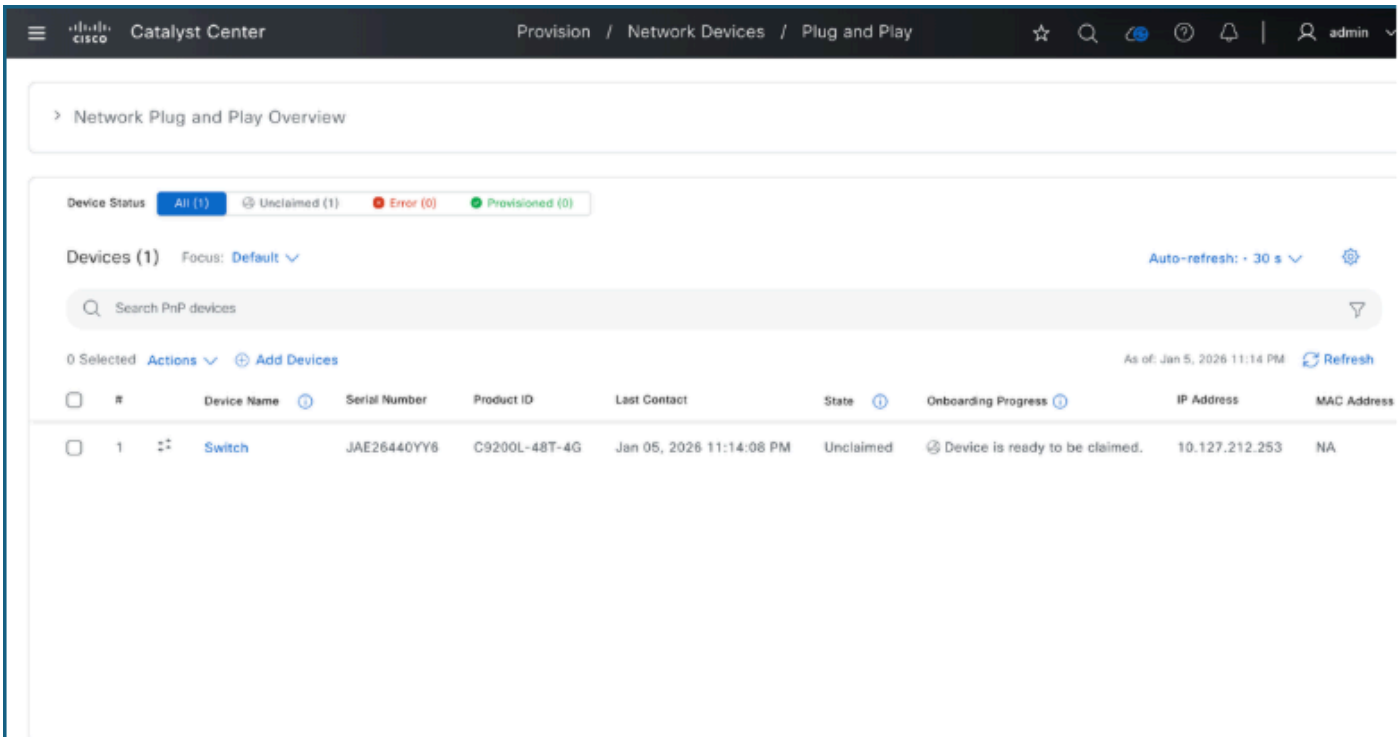
Stap 3. Configureer het aangepaste VLAN als het PnP VLAN.

```
config t
pnp startup-vlan 302
```

Stap 4. Configureer de trunkinterface naar nieuwe switch.

```
config t
interface GigabitEthernet1/0/5
  description PnP_Trunk
  switchport mode trunk
  switchport trunk allowed vlan 302
```

Stap 5.Controleer of de switch wordt weergegeven op de pagina Voorzieningen > Plug and Play van Catalyst Center.



3. Switch aan boord met behulp van de beheerpoort

Deze methode maakt gebruik van de beheerinterface van de switch.

Vereisten

- Aangepaste VLAN SVI geconfigureerd op de upstream-switch
- DHCP-server met optie 43 geconfigureerd
- DNS-resolutie voor het Catalyst Center FQDN

De procedure op de stroomopwaartse switch.

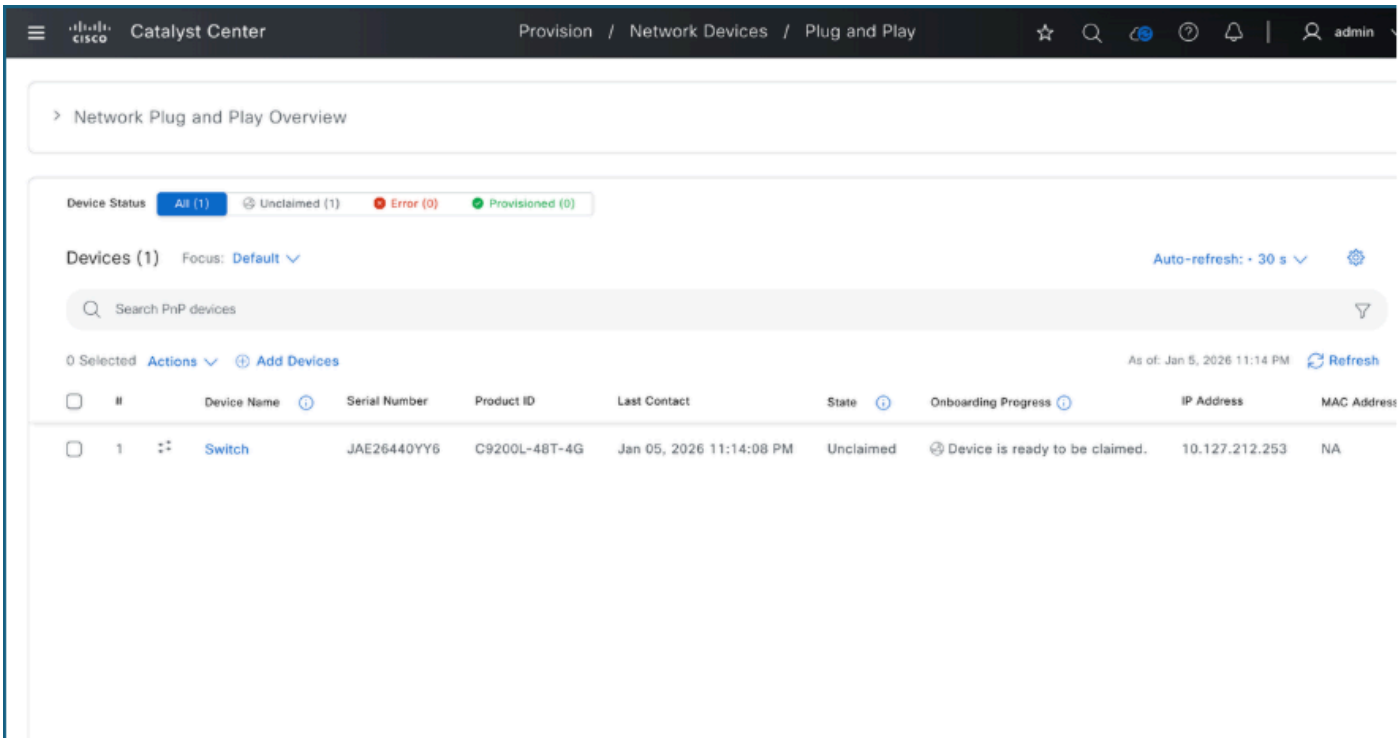
Stap 1. De SVI van het VLAN configureren.

```
config t
interface Vlan302
    ip address 10.127.212.49 255.255.255.0
    ip helper-address 10.127.212.1
```

Stap 2. Configureer de toegangsinterface naar de nieuwe switch.

```
config t
interface GigabitEthernet1/0/5
  switchport mode access
  switchport access vlan 302
```

Stap 3.Controleer of de switch wordt weergegeven op de pagina Voorzieningen > Plug and Play van Catalyst Center.



4. Logbestanden van de Switch-console

Dit is wat er op de console van de switch verschijnt wanneer DHCP wordt gebruikt voor Plug and Play.

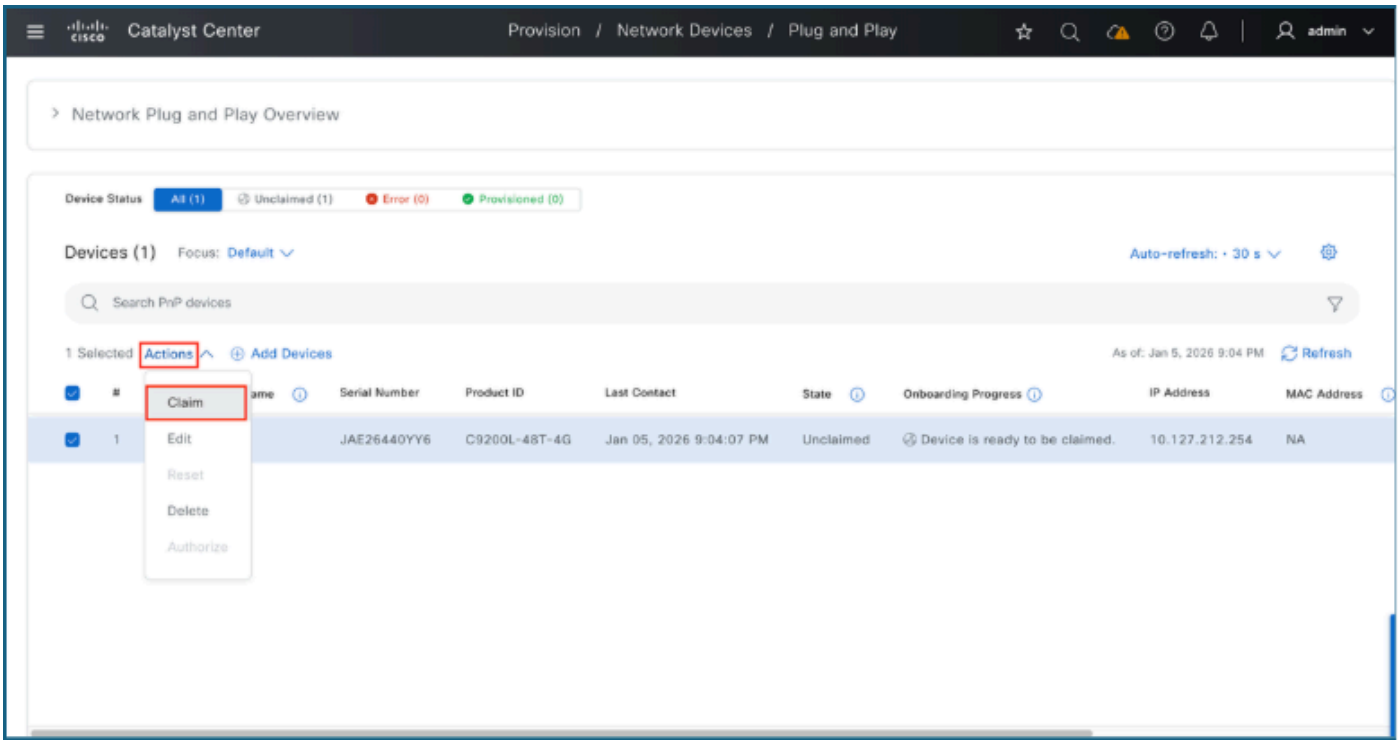
```
Base Ethernet MAC Address          : 44:64:3c:b1:2b:80
Motherboard Assembly Number        : 73-102066-04
Motherboard Serial Number          : JAE26440YY6
Model Revision Number              : D0
Motherboard Revision Number        : A0
Model Number                       : C9200L-48T-4G
System Serial Number               : JAE26440YY6


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:


Press RETURN to get started!


*Jan  5 15:28:24.332: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-2360689995 has been generated or imported by crypto-engine
*Jan  5 15:28:24.366: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jan  5 15:28:24.540: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write memory" to save new IOS PKI configuration
*Jan  5 15:28:24.543: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent Discovery from console as vty0
*Jan  5 15:28:24.895: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-2360689995.server has been generated or imported by crypto-engine
*Jan  5 15:28:26.546: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent Discovery from console as vty0
*Jan  5 15:28:26.546: %PNP-6-PNP_SAVING_TECH_SUMMARY: Saving PnP tech summary (pnp-tech-discovery-summary)... Please wait. Do not interrupt.
*Jan  5 15:28:27.574: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent Discovery from console as vty0
*Jan  5 15:28:28.589: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent Discovery from console as vty0
*Jan  5 15:28:29.604: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent Discovery from console as vty0
*Jan  5 15:28:33.230: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent Discovery from console as vty0
*Jan  5 15:28:31.023: %SYS-6-CLOCKUPDATE: System clock has been updated from 15:28:33 UTC Mon Jan 5 2026 to 15:28:31 UTC Mon Jan 5 2026, configured from console by vty0.
Jan  5 15:28:31.023: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
Jan  5 15:28:31.032: %SYS-5-CONFIG_P: Configured programmatically by process XEP_pnp-zero-touch from console as vty0
Jan  5 15:28:31.034: %SMART_LIC-5-SYSTEM_CLOCK_CHANGED: Smart Agent for Licensing System clock has been changed
Jan  5 15:28:31.910: %PNP-6-PNP_TECH_SUMMARY_SAVED_OK: PnP tech summary (pnp-tech-discovery-summary) saved successfully.
Jan  5 15:28:31.910: %PNP-6-PNP_DISCOVERY_DONE: PnP Discovery done successfully (PnP-DHCP-IPv4)
Jan  5 15:28:33.405: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: pnplabel created succesfully
Jan  5 15:28:33.419: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write memory" to save new IOS PKI configuration
Jan  5 15:28:34.718: %SYS-5-CONFIG_P: Configured programmatically by process PnP reconnect profile from console as vty0
%Error opening tftp://255.255.255.255/network-confg (Timed out)
Jan  5 15:28:39.911: AUTOINSTALL: Tftp script execution not successful for Vl302.
Jan  5 15:29:35.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 15:29:35 UTC Mon Jan 5 2026 to 15:29:35 UTC Mon Jan 5 2026, configured from console by vty0.
Jan  5 15:29:35.000: %SYS-5-CONFIG_P: Configured programmatically by process XEP_pnp-zero-touch from console as vty0
Jan  5 15:29:35.001: %PNP-6-PNP_SAVING_TECH_SUMMARY: Saving PnP tech summary (pnp-tech-error-summary)... Please wait. Do not interrupt.
Jan  5 15:29:35.001: %SMART_LIC-5-SYSTEM_CLOCK_CHANGED: Smart Agent for Licensing System clock has been changed
Jan  5 15:29:38.651: %SYS-5-CONFIG_P: Configured programmatically by process XEP_pnp-zero-touch from console as vty0
Jan  5 15:29:39.651: %PNP-6-PNP_TECH_SUMMARY_SAVED_OK: PnP tech summary (pnp-tech-error-summary) saved successfully.
Jan  5 15:29:44.698: %SYS-5-CONFIG_P: Configured programmatically by process XEP_pnp-zero-touch from console as vty0
```

Onboarding-Switch naar Catalyst Center zonder Day-0-sjablonen

Als u een nieuwe switch in de inventarislijst van het Catalyst Center wilt opnemen, voert u de vereiste procedures uit zodra het apparaat zichtbaar en opvraagbaar is op de pagina Plug and Play.

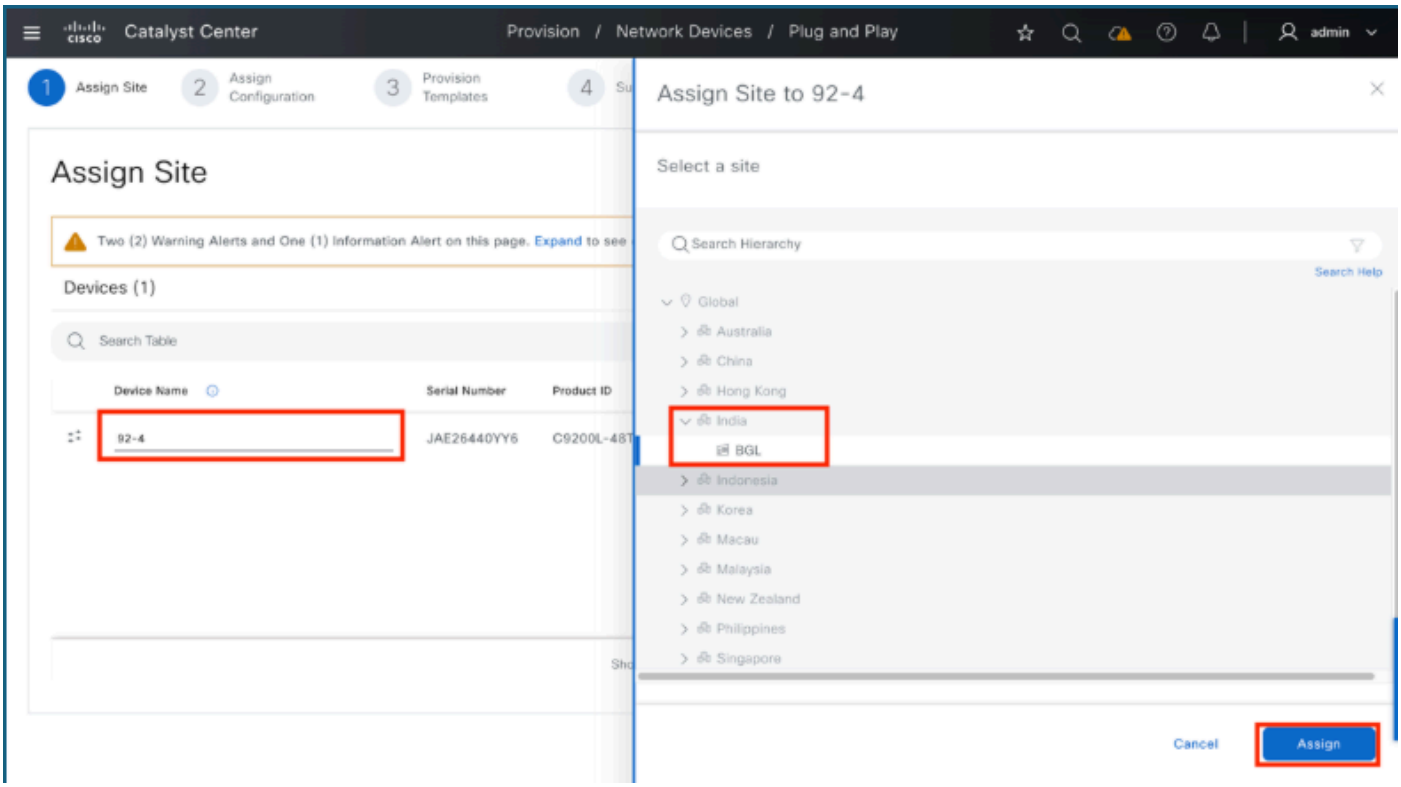
1. Om switch te claimen:

- Schakel de selectievakjes in voor de switch die moeten worden geclaimd.
- Navigeer naar Acties > Claim.



2. De switch benoemen en in kaart brengen:

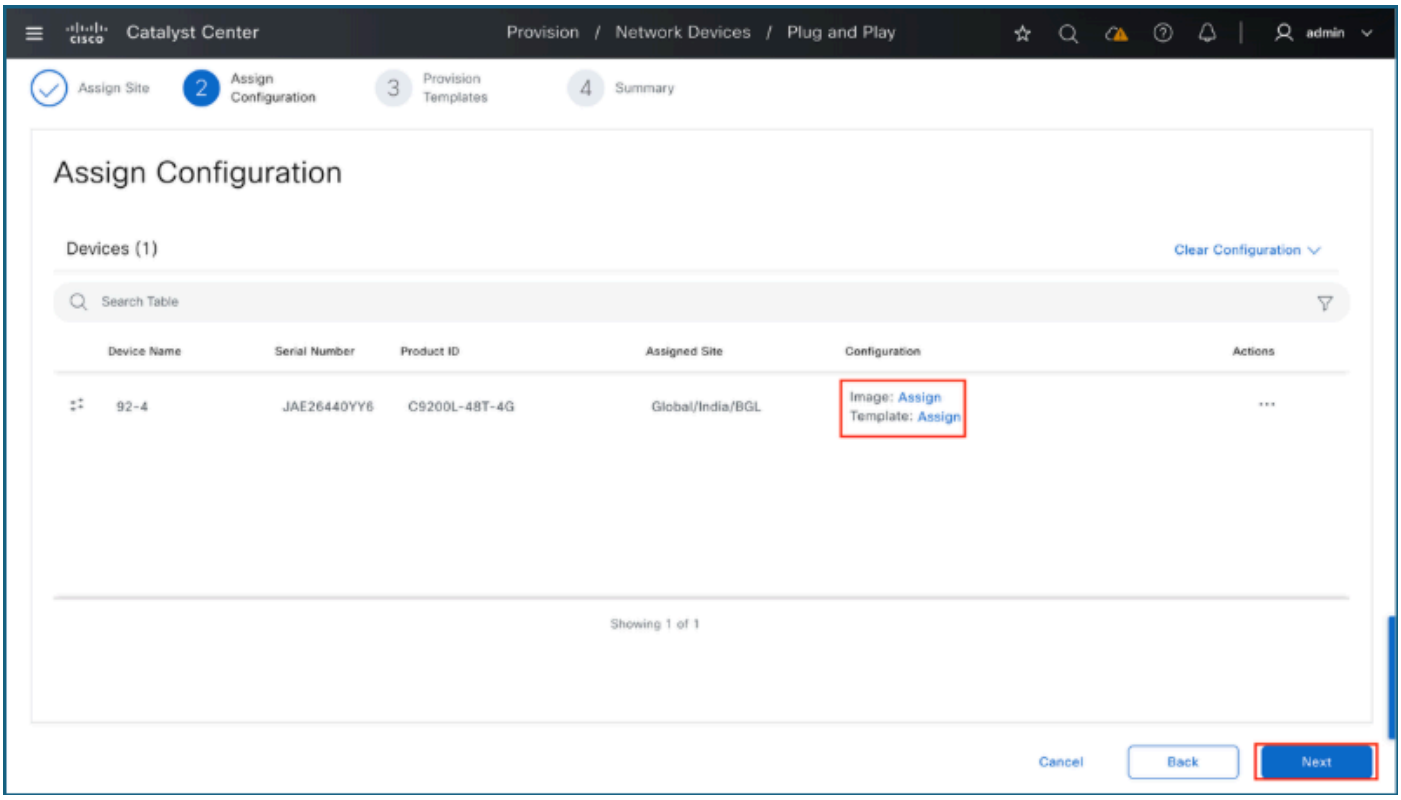
- Voer de naam in het veld Apparaatnaam in en klik op Toewijzen.
- Kies de juiste site of het juiste gebouw, klik nogmaals op Toewijzen en klik vervolgens op Volgende.



3. Software-image of -sjabloon toewijzen (optioneel):

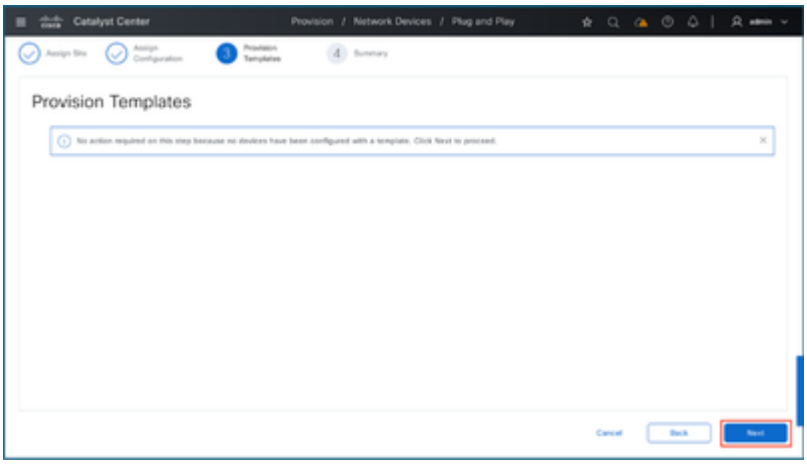
Gebruik deze stap om de switch te upgraden naar een specifieke softwareversie of een Day-0-configuratiesjabloon toe te passen.

- Klik op Toewijzen naast Image om de softwareversie op te geven.
- Klik op Toewijzen naast Sjabloon om een sjabloonconfiguratie toe te passen.
- Klik op Volgende nadat de gewenste opdrachten zijn voltooid.



4. Voorzieningsmodellen

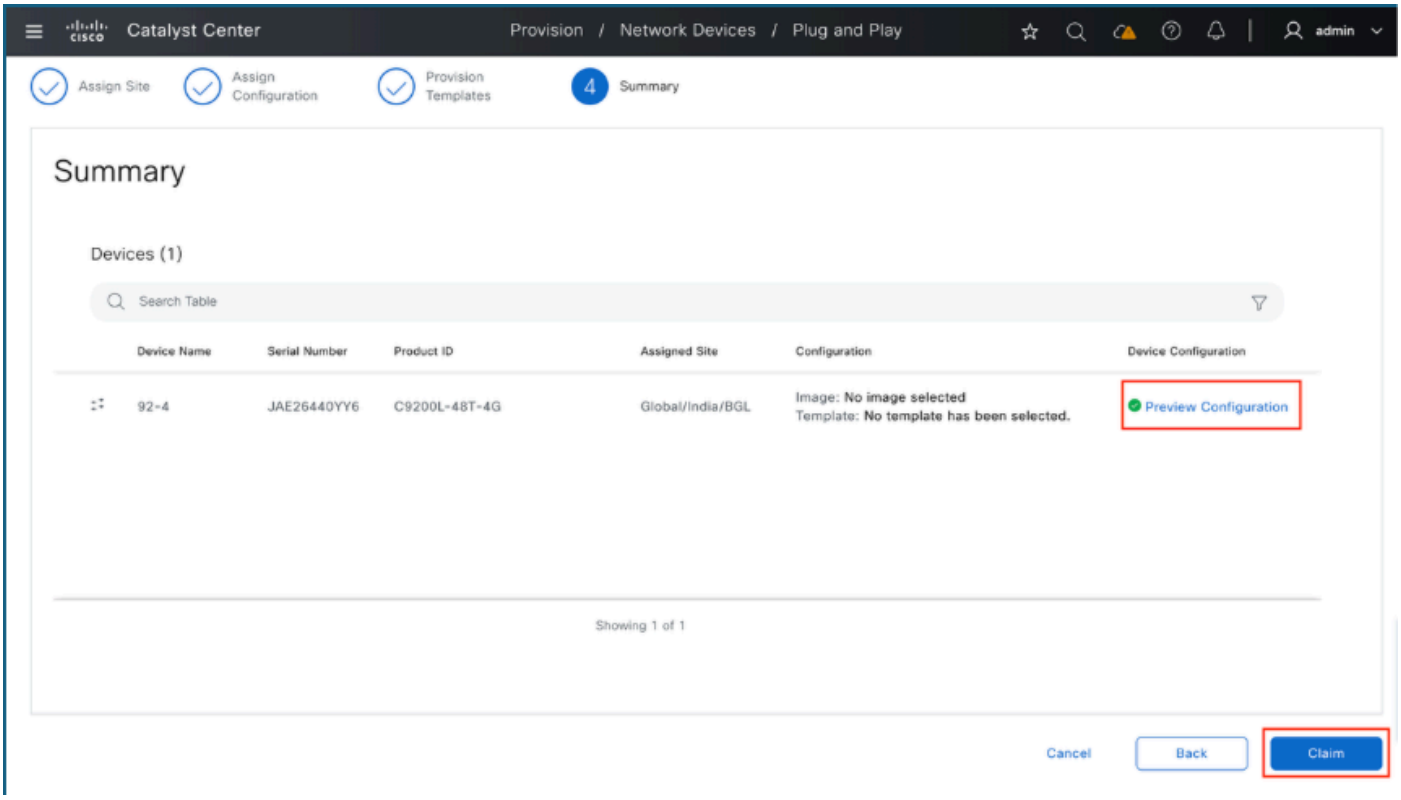
Wanneer u het apparaat claimt zonder sjablonen te gebruiken, omzeilt u deze configuratiestap door Volgende te selecteren.

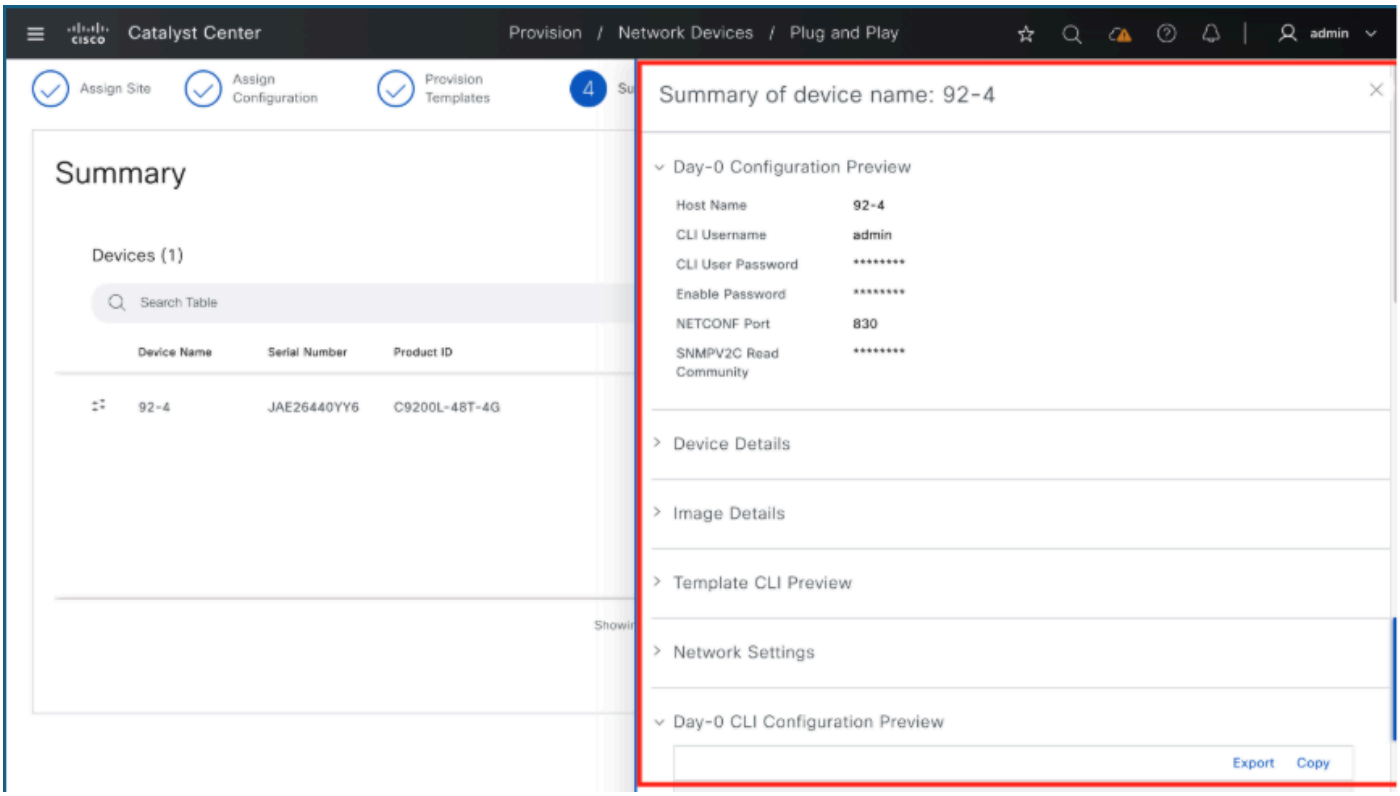


5. Samenvatting

Gebruik de overzichtspagina om de configuratie te bekijken voordat deze wordt geleverd door Catalyst Center.

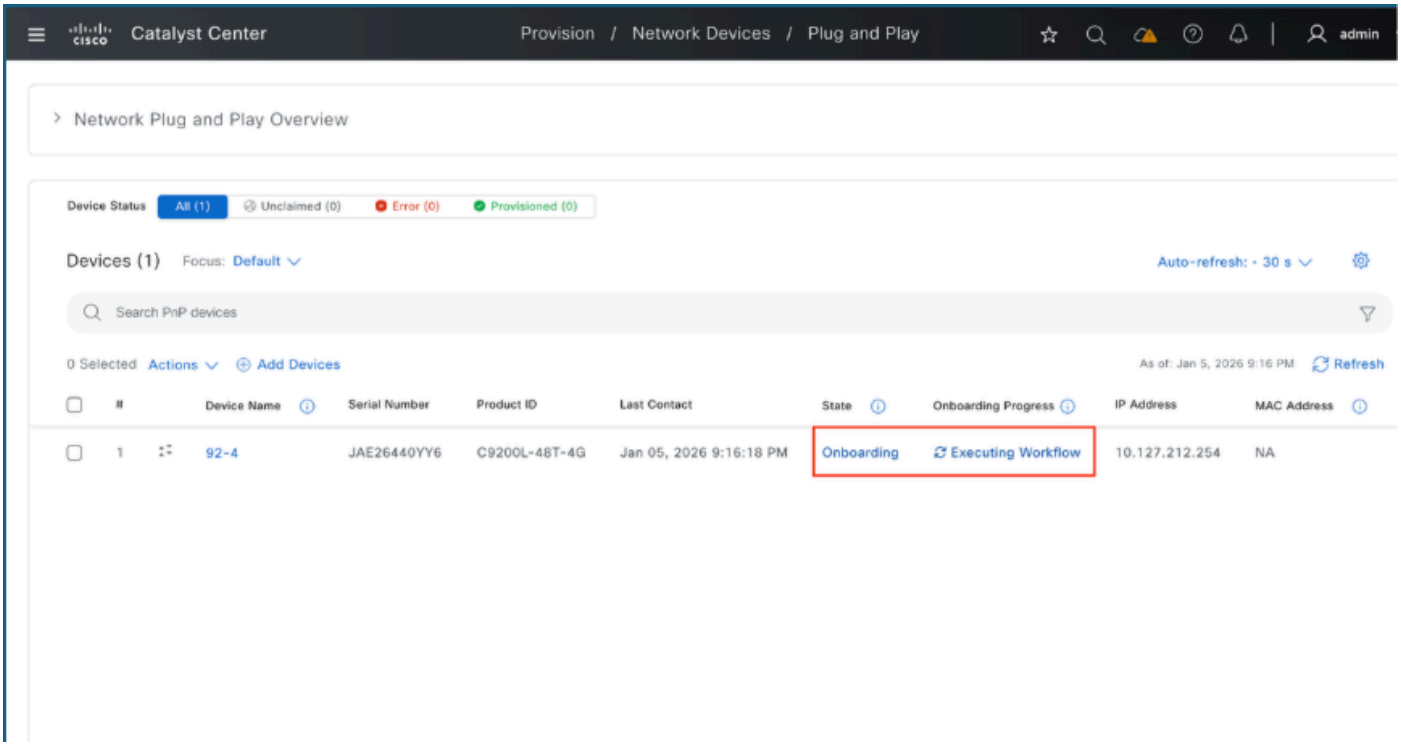
- Klik op Voorbeeldconfiguratie.
- Vouw de afzonderlijke secties uit om de instellingen te controleren.
- Klik op Claim zodra u dit hebt geverifieerd.

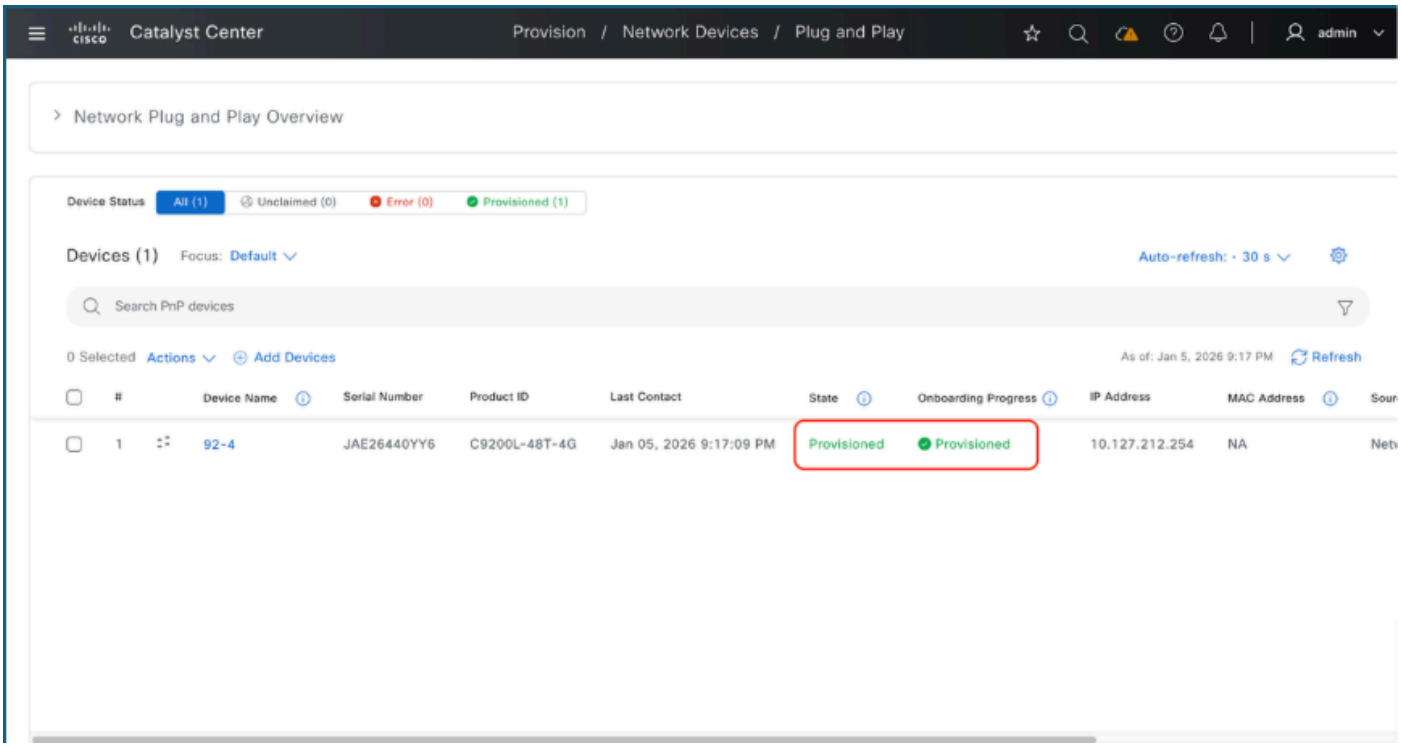




6. Toezicht houden op het claimproces

Na het starten van de claim keert de interface terug naar het Plug and Play-dashboard. De apparaatstatus bewaken, een overgang naar Provisioned geeft aan dat de switch is geclaimd en toegevoegd aan de inventarisatie van het Catalyst Center.



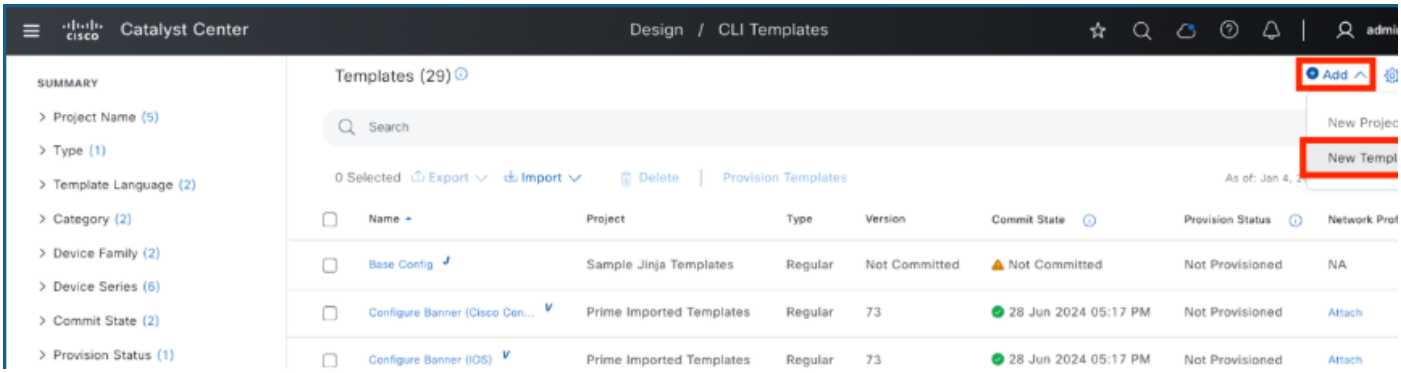


Onboarding Switch naar Catalyst Center met Day-0 templates

Wanneer de nieuwe switch klaar is om te worden geclaimd op de Plug and Play-pagina van Catalyst Center, past u een Day-0-sjabloon toe om extra configuratie toe te voegen tijdens het claimproces.

1. Sjabloon voor dag 0 of onboarding maken

- Navigeer naar Ontwerp > CLI-sjablonen.
- Selecteer Toevoegen > Nieuwe template.

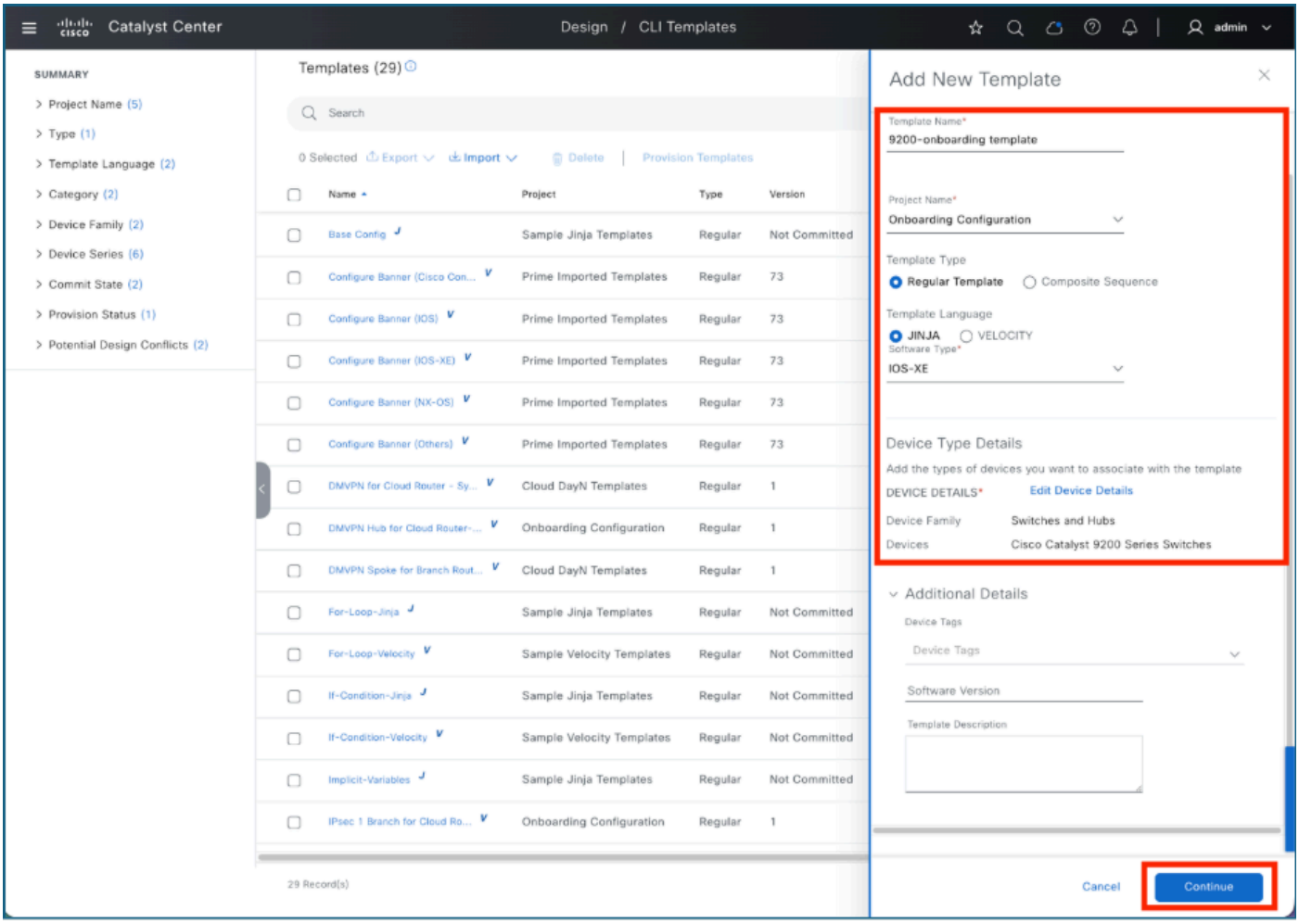


2. Sjabloondetails toevoegen

Voer in het zijpaneel de volgende sjabloonspecificaties in:

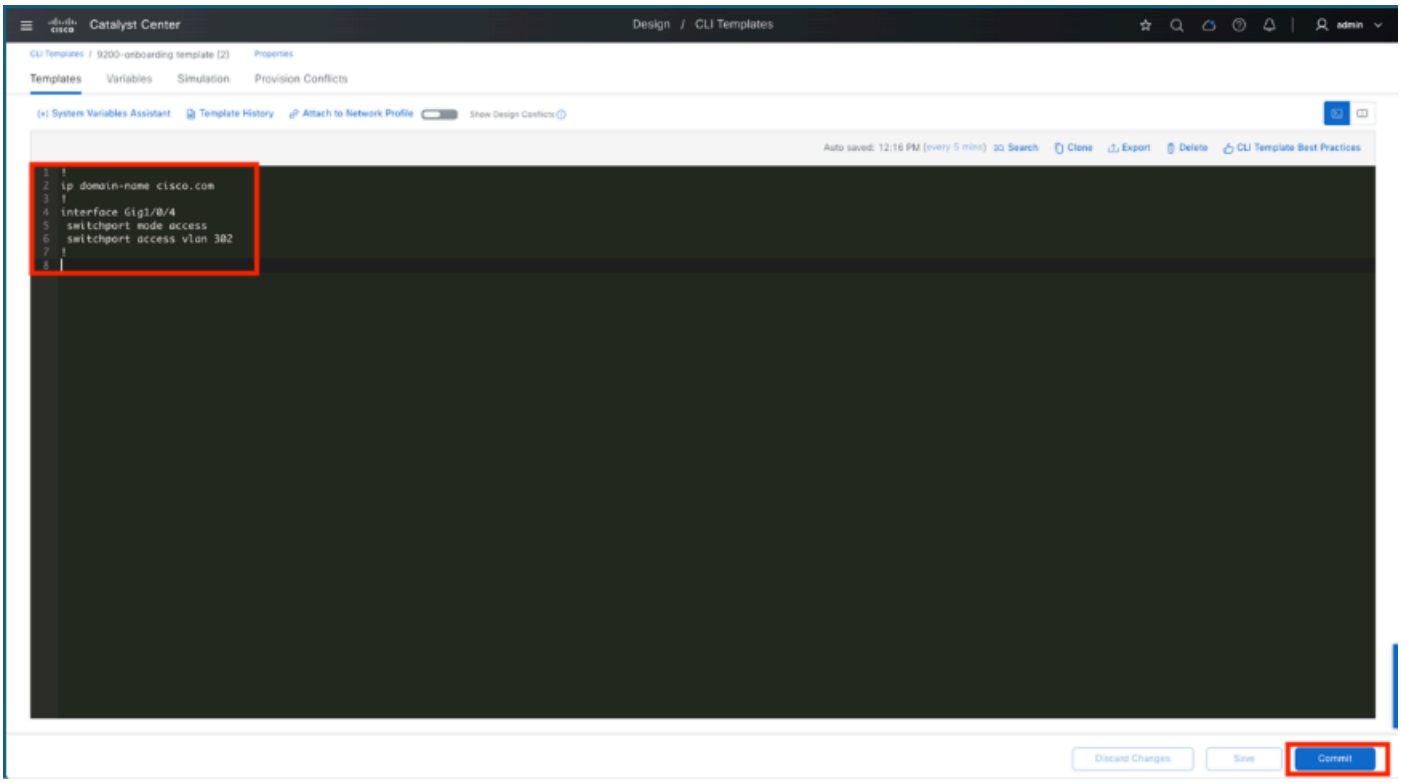
- Naam template
- Projectnaam: Selecteer voor sjablonen van dag 0 altijd Onboarding Configuration.

- Sjabloontype, taal en softwaretype: Selecteer de juiste waarden in de menu's.
- Klik op Doorgaan om verder te gaan.



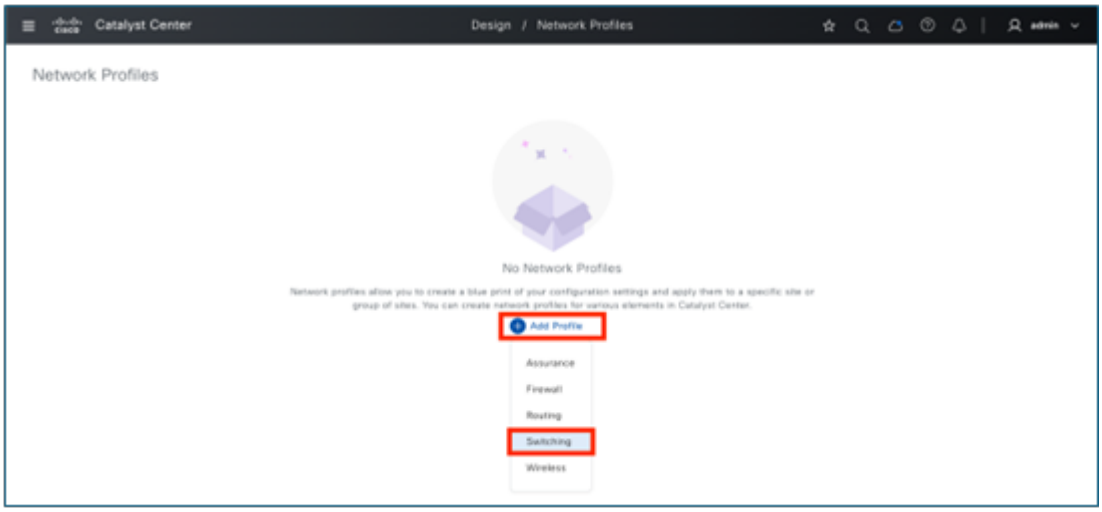
3. De template bewerken

Geef de configuratie op die moet worden geïmplementeerd in de switch in de CLI-sjablooneditor. In dit voorbeeld worden een domeinnaam en een toegangspoort geconfigureerd. Nadat u de configuratie aan de CLI-sjablooneditor hebt toegevoegd, klikt u op Opslaan en vervolgens op Vastleggen om de wijzigingen te voltooien.



4. Netwerkprofiel maken

- Navigeer naar het menu Ontwerp en selecteer Netwerkprofielen.
- Klik op de knop Profiel toevoegen.
- Kies het juiste profieltype uit de lijst (bijvoorbeeld Schakelen).



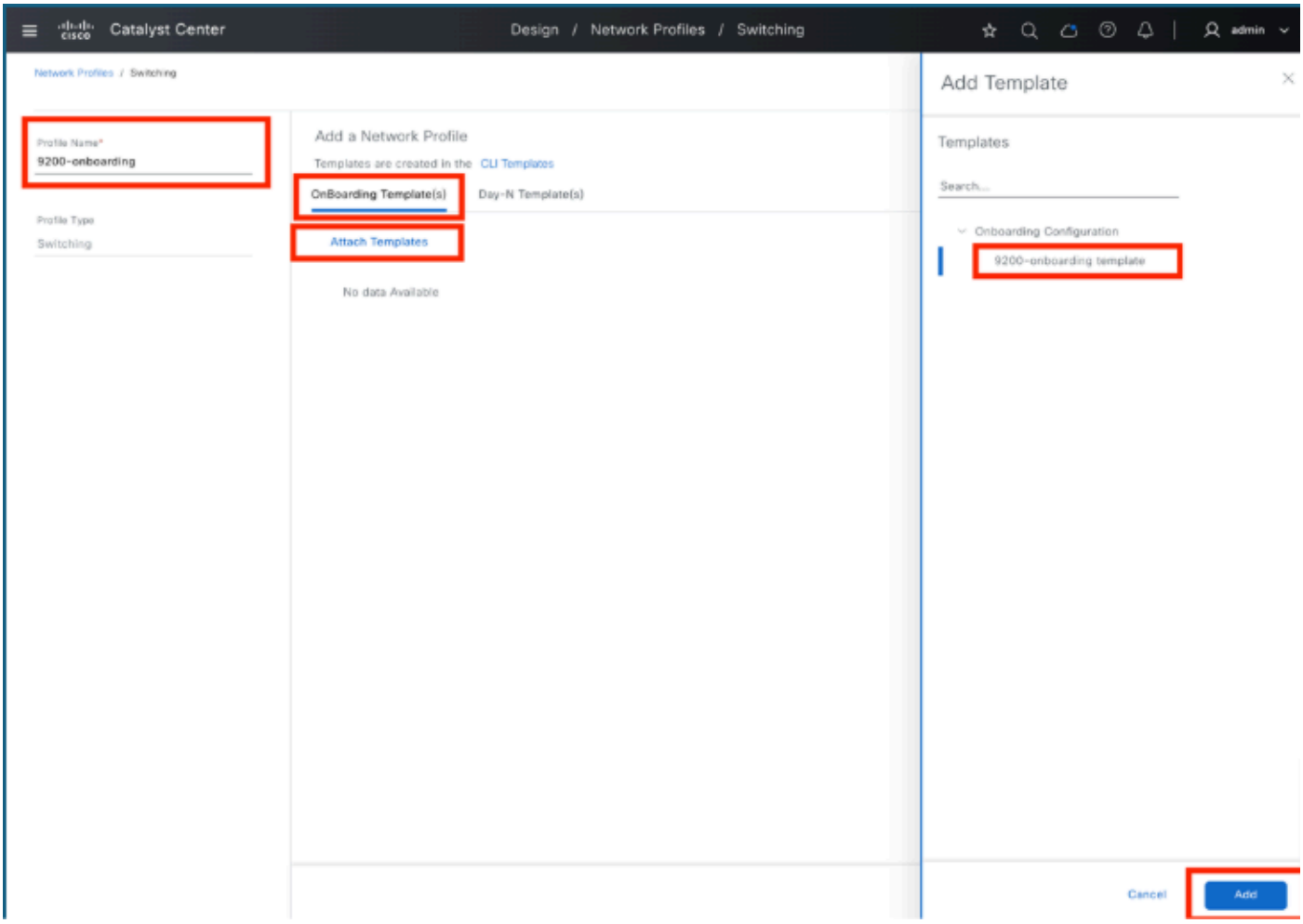
5. Sjabloon toevoegen en netwerkprofielinstellingen bewerken

- Profielnaam invoeren: Geef een naam op voor het netwerkprofiel.

- Toegangssjablonen: Klik op Onboarding Template(s) en selecteer vervolgens Bijvoegen Templates.

- Kies Sjabloon: Zoek en selecteer de gewenste sjabloon in de directory Onboarding Configuration.

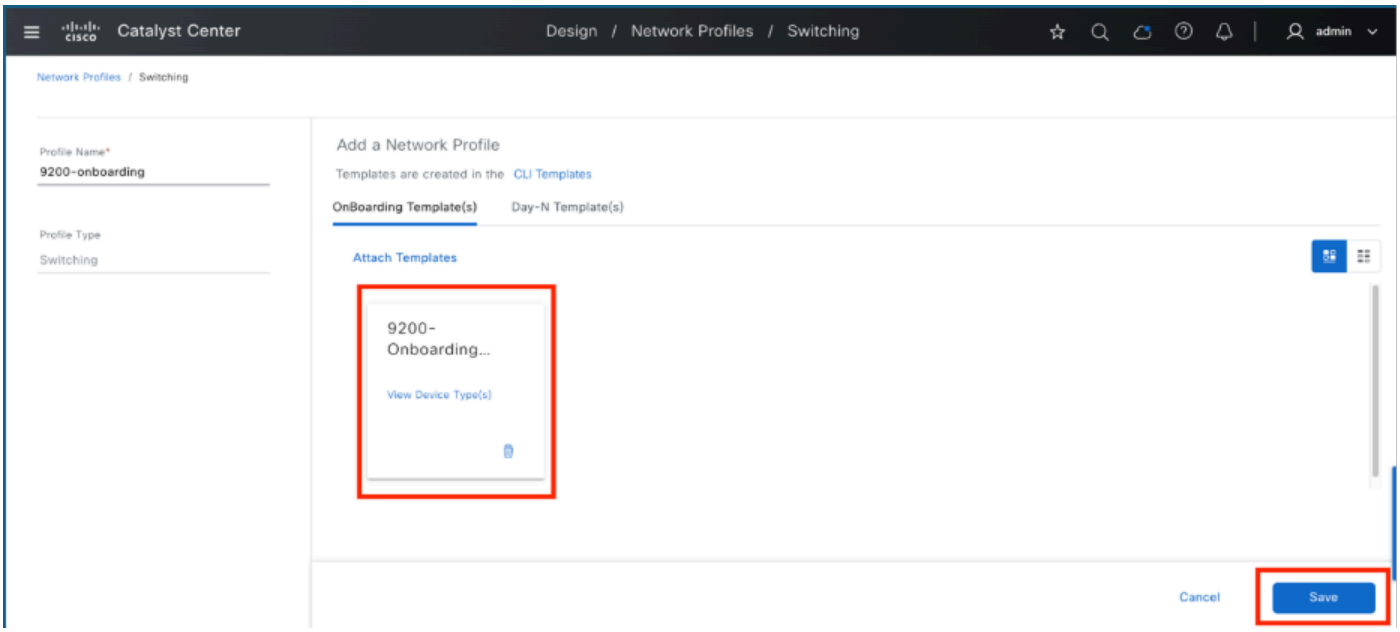
- Voltooien: Klik op de knop Toevoegen om het proces te voltooien.



6. Het profiel opslaan

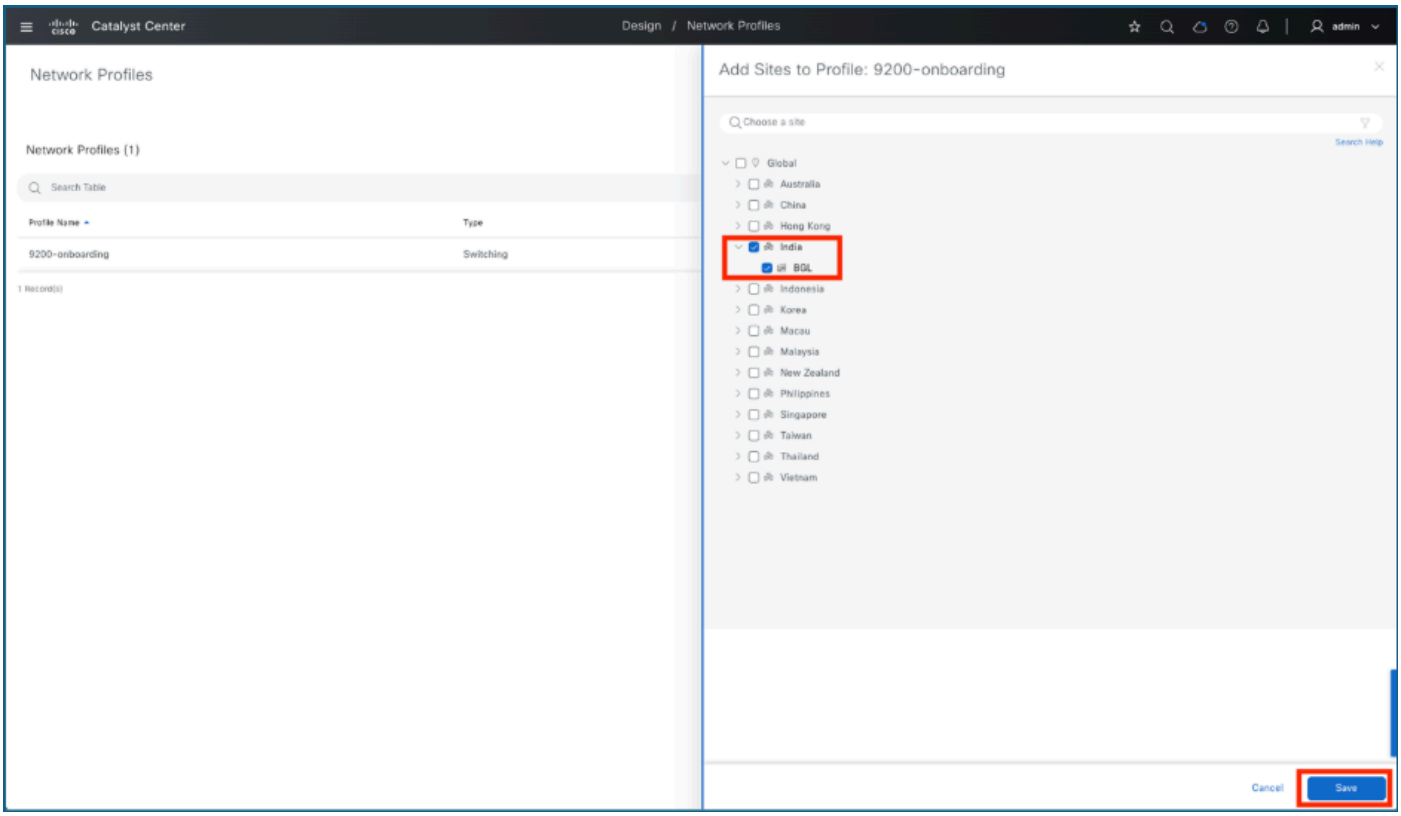
- Sjabloon verifiëren: zorg ervoor dat de sjabloon wordt weergegeven in de lijst onder Sjabloon(len) voor onboarding.

- Profiel opslaan: Klik op de knop Opslaan om de profielinstellingen te voltooien en op te slaan.



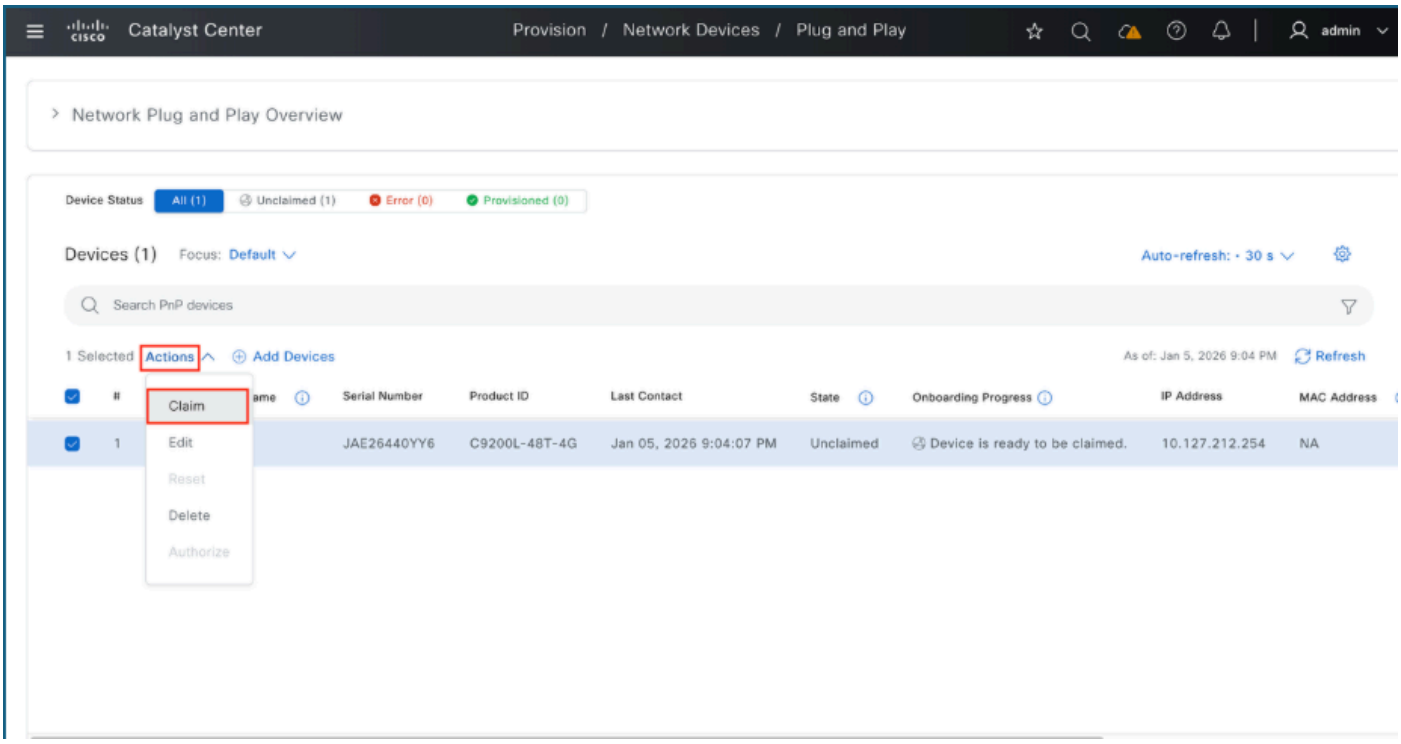
7. Een netwerkprofiel toewijzen aan de locatie waar de switch/switches aan boord moeten worden genomen

- Toewijzing starten: Klik op de optie Site toewijzen voor het netwerkprofiel dat zojuist is gemaakt.
- Kies de site: Selecteer de specifieke site waar de switches aan boord moeten worden genomen.
- Bevestigen: Klik op Opslaan om de toewijzing te voltooien.



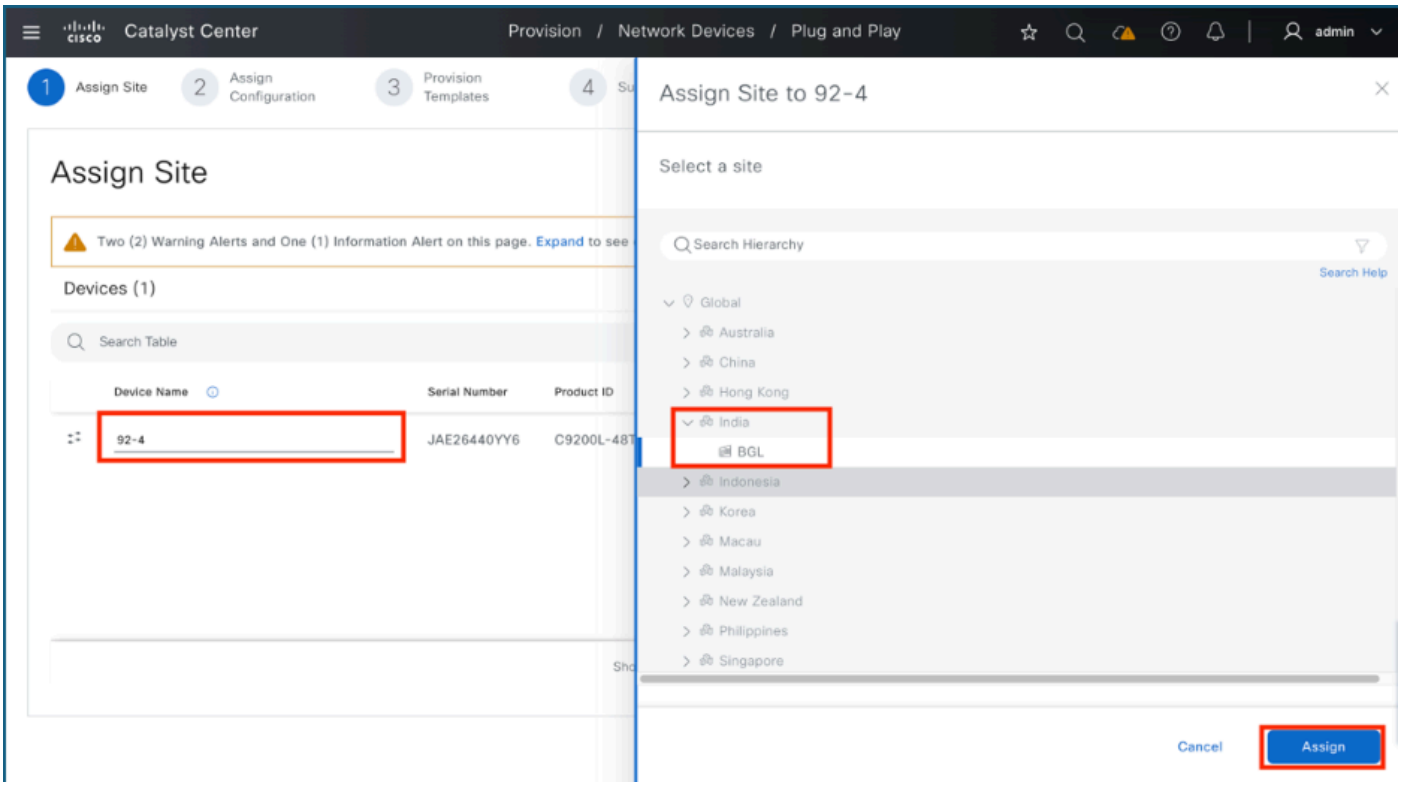
8. Claim-Switches

- Navigeer naar Plug and Play: Ga naar het menu Provision en selecteer Plug and Play.
- Apparaten selecteren: Zoek de switch of switches die moeten worden geclaimd en klik op het selectievakje naast de naam van elke switch.
- Claim starten: Navigeer naar het menu Acties en selecteer Claim.



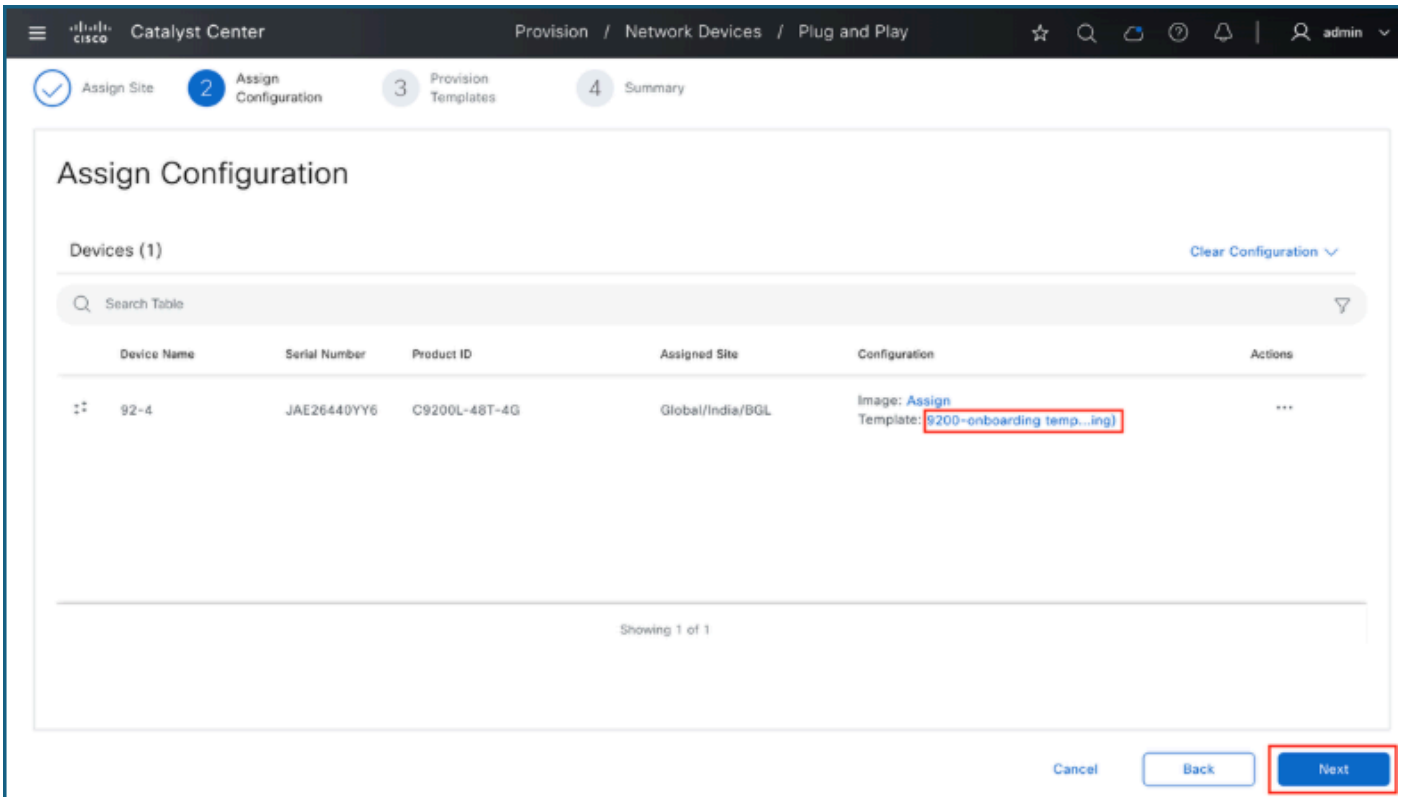
9. Een naam voor de switch toewijzen en een site toewijzen

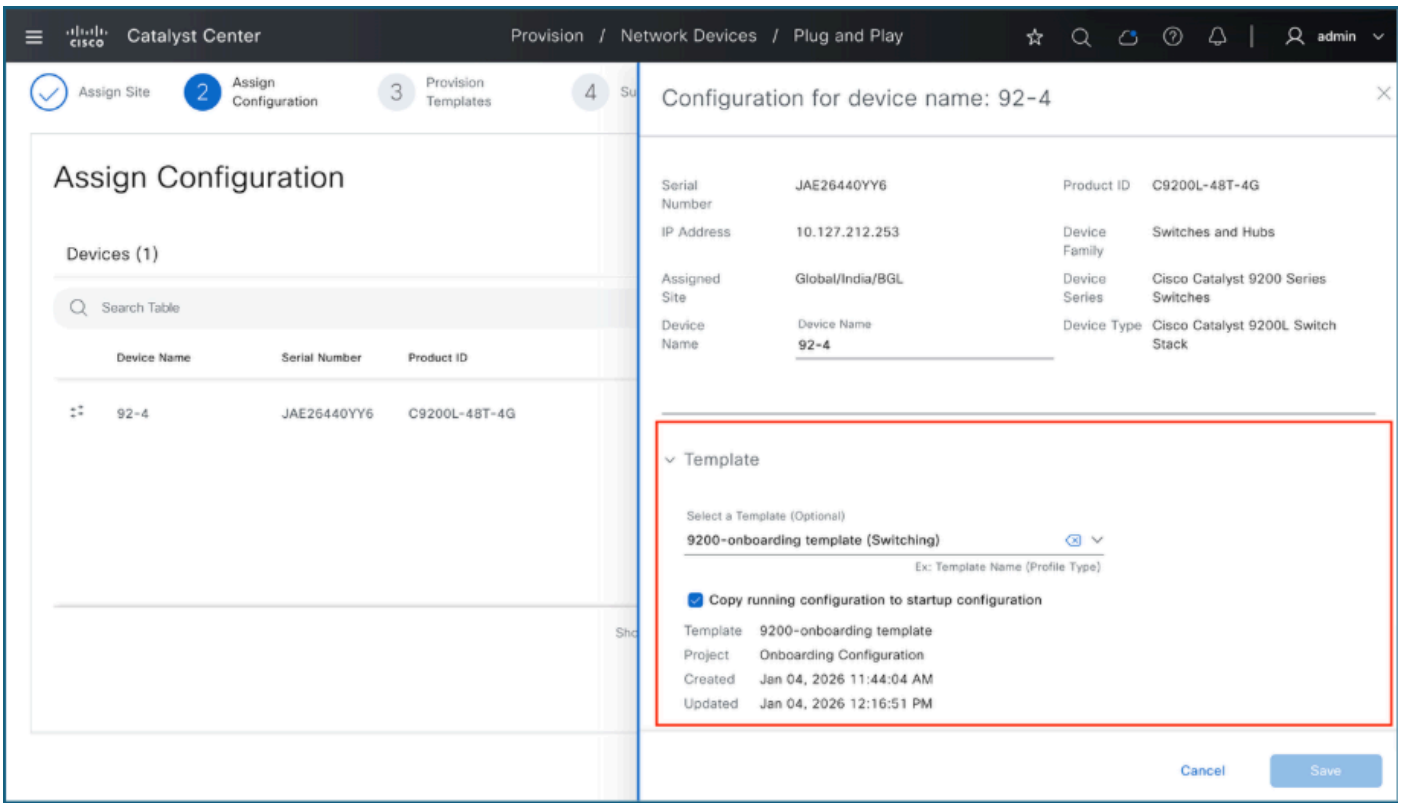
- Apparaatnaam: Voer de gewenste naam voor de switch in het veld Apparaatnaam in.
- Toewijzing starten: Klik op de knop Toewijzen.
- Selecteer Locatie: Kies de juiste locatie of het juiste gebouw, klik nogmaals op Toewijzen en klik vervolgens op Volgende om verder te gaan.



10. Een Day-0-sjabloon toewijzen

- Selecteer de sjabloon: Klik op de sjabloon die automatisch is geselecteerd naast de optie Sjabloon.
- Details bekijken: Controleer de configuratiedetails van de toegewezen sjabloon zorgvuldig.
- Doorgaan: Klik op Volgende zodra u de toewijzing van de template hebt bevestigd.





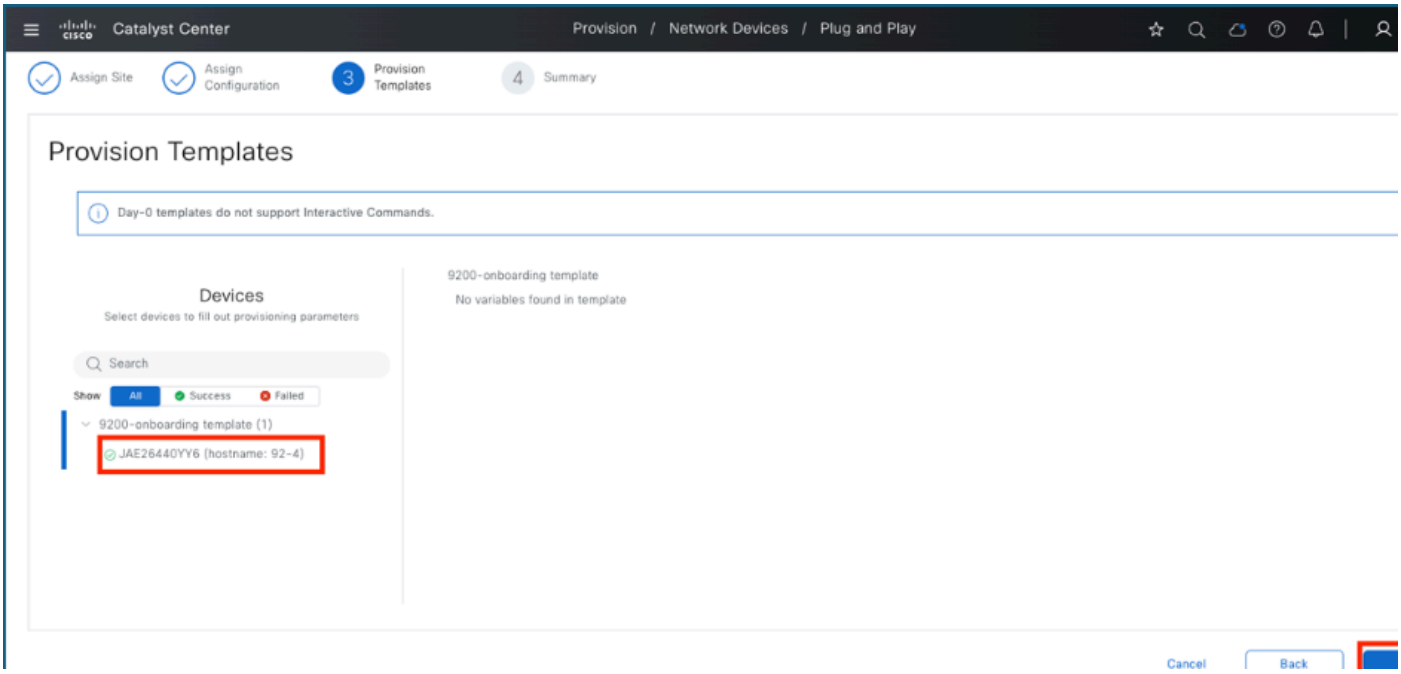
11. Templates voor voorzieningen

- Selecteer Apparaat: Klik in het gedeelte Sjabloon op het specifieke apparaat dat u configureert.

- Variabelen identificeren: controleren op de vereiste waarden voor variabelen die aan de sjabloon zijn gekoppeld.

- Waarden invoeren: Als variabelen verplicht zijn, vult u de benodigde waarden in.

- Doorgaan: Klik op Volgende om naar de volgende stap te gaan.



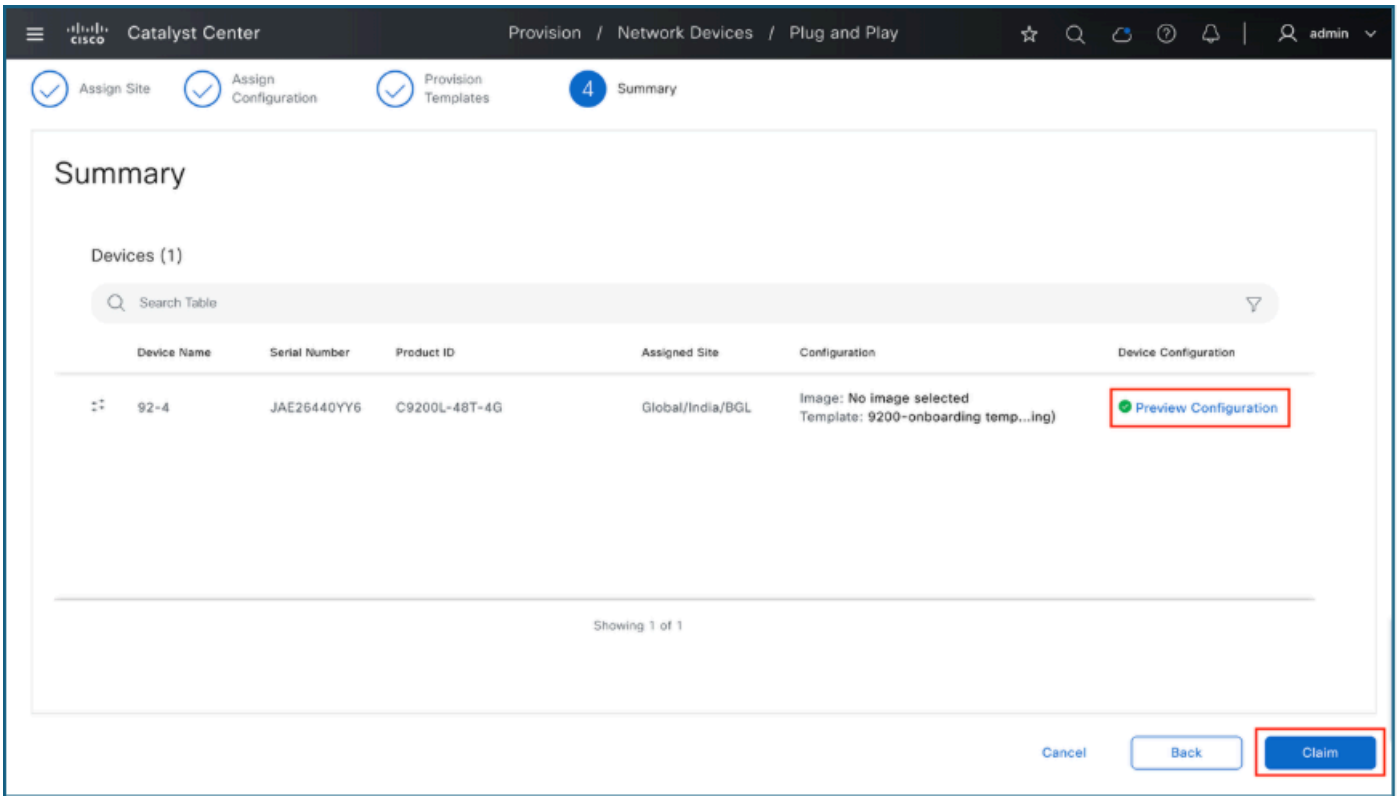
12. Samenvatting

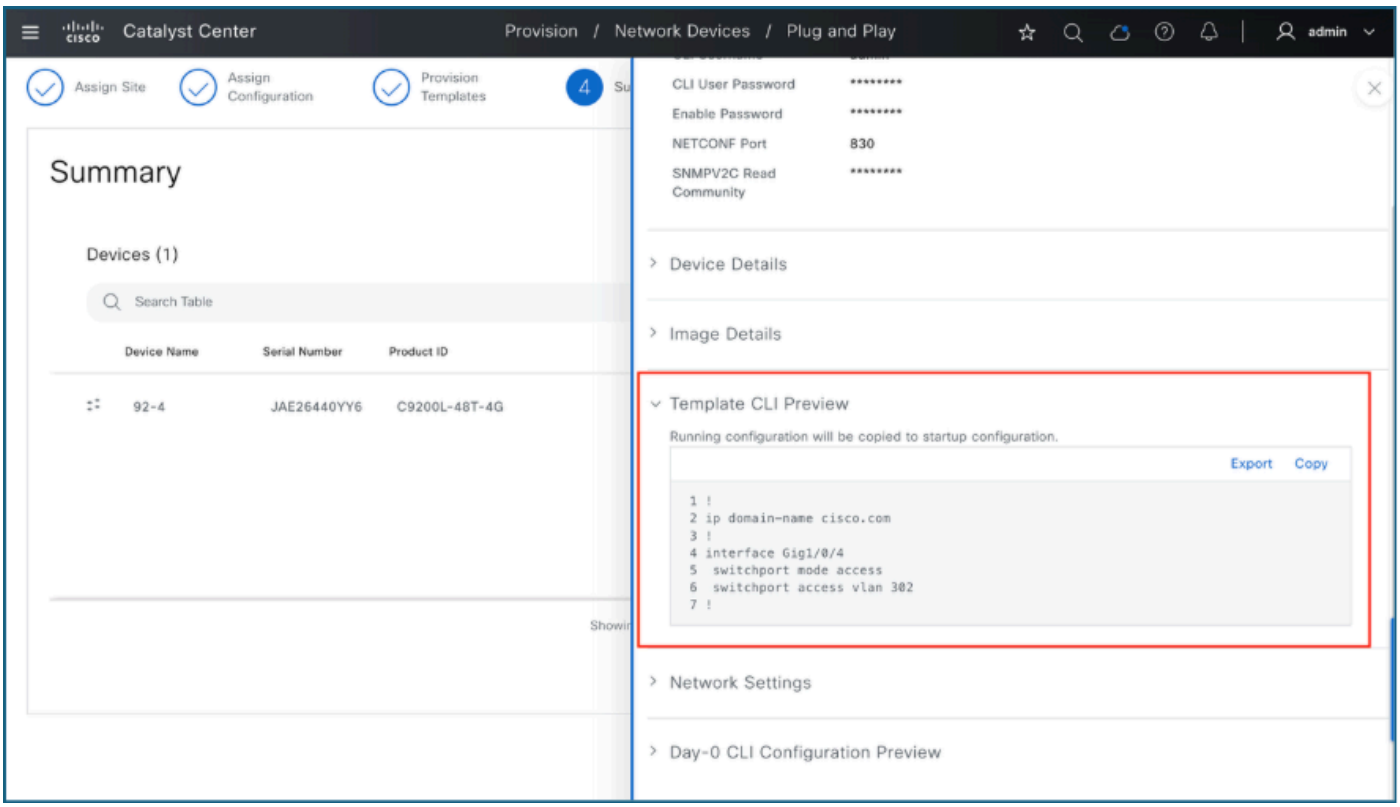
- Configuratie controleren: controleer op de pagina Overzicht de configuratie-instellingen die zijn voorbereid door Catalyst Center.

- Voorbeelddetails: Klik op Voorbeeldconfiguratie om de wijzigingen in behandeling te bekijken.

- Secties verifiëren: Vouw elke sectie uit om de specifieke configuratiedetails te bekijken.

- Voltooien: Nadat u de instellingen hebt geverifieerd, klikt u op Claim om door te gaan.

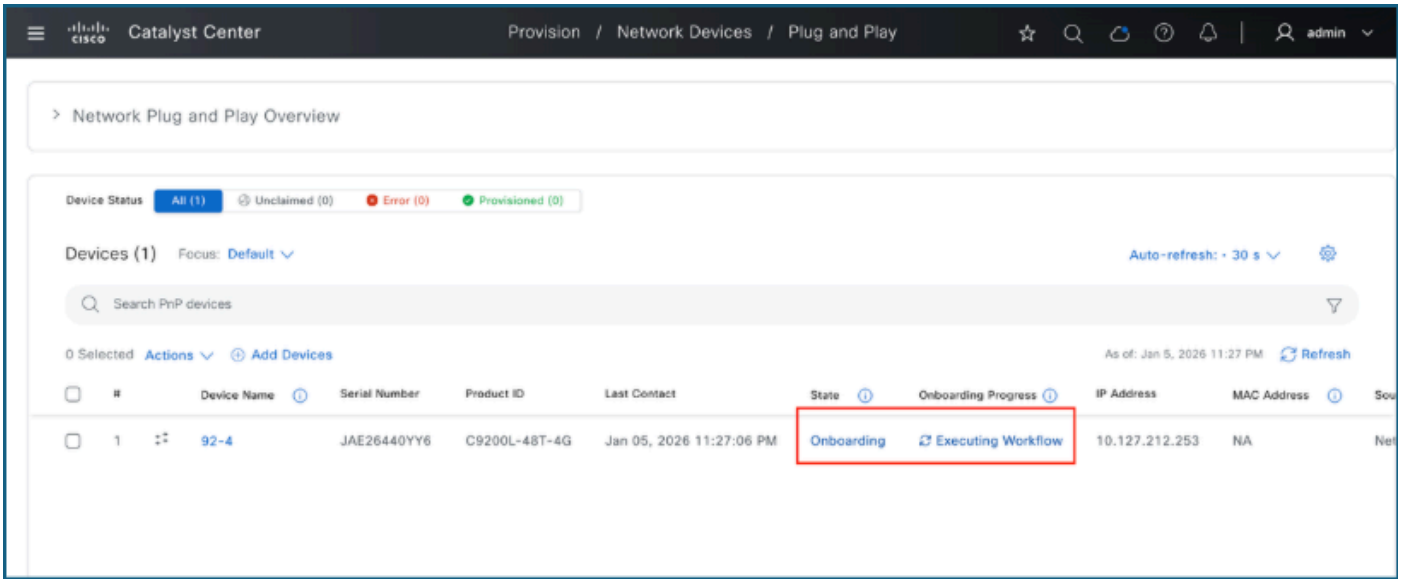


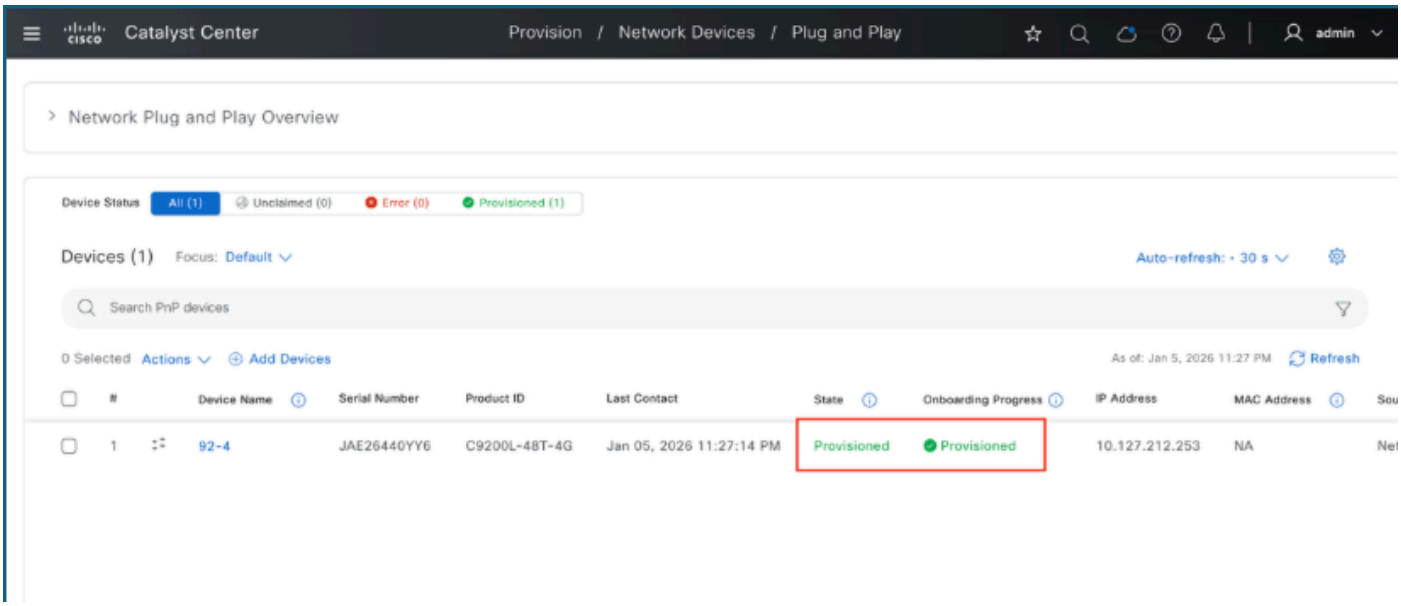


13. Voortgang van de aanvraag monitoren

U wordt doorgestuurd naar de pagina Plug and Play om de voortgang van het apparaat te volgen.

- Monitorstatus: Observeer de apparaatstatus terwijl het claimproces wordt uitgevoerd.
- Voltooiing bevestigen: wanneer de status wordt bijgewerkt naar Provisioned, is de switch geclaimd en opgenomen in de Catalyst Center-inventarisatie.



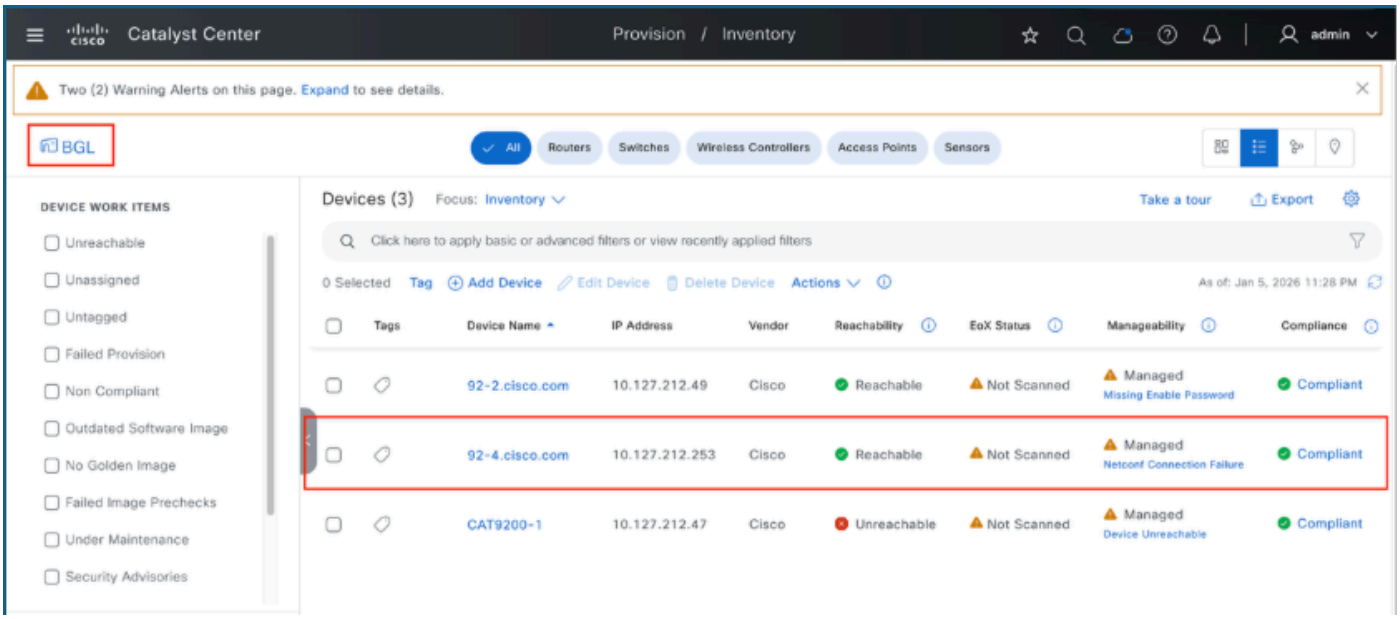


Verificatie

- Toegang tot het menu Voorzieningen: Open het tabblad Voorzieningen op de hoofdpagina.

- Voorraad bekijken: selecteer de optie Voorraad.

- Status verifiëren: controleer de lijst om te bevestigen dat de switches zijn geleverd.



Apparaten in bulk importeren in plug-and-play-inventaris van Catalyst Center

Om de uitrol van grote netwerken te stroomlijnen, ondersteunt Catalyst Center een methode voor het importeren van bulk voor het vooraf faseren van apparaten. Dit proces omvat het uploaden van apparaat-ID's zoals PID's, serienummers en optionele site- of sjabloongegevens, waardoor het systeem automatisch apparaten aan boord kan nemen zodra ze worden ingeschakeld en aangesloten.

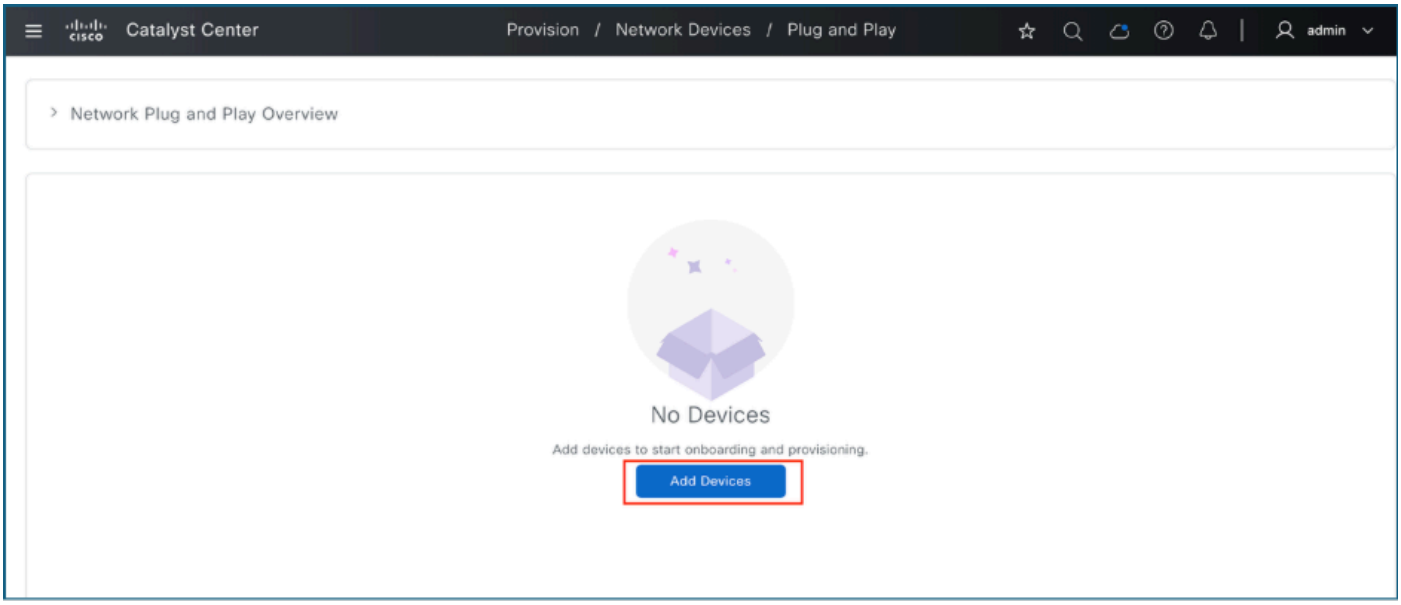
1. Voorwaarden

Om een succesvolle bulkinvoer te garanderen, moet aan deze vereisten worden voldaan:

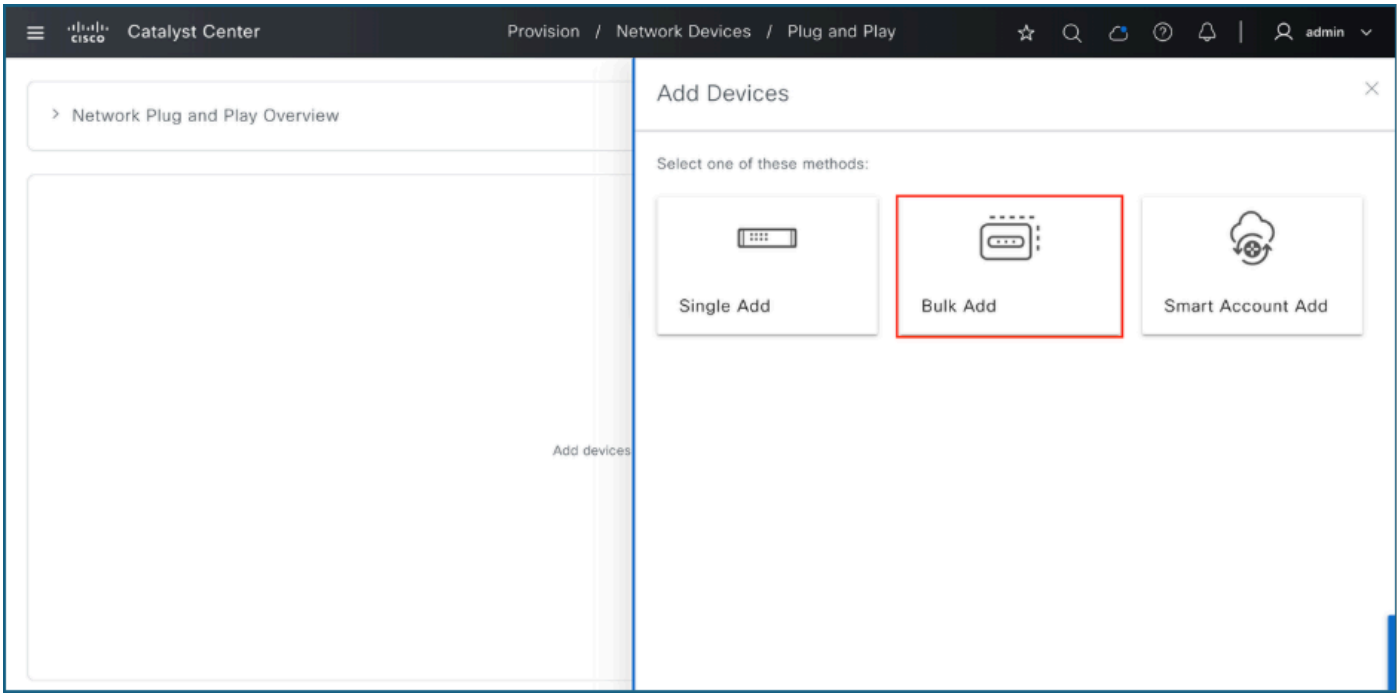
- De instantie Catalyst Center moet bereikbaar en operationeel zijn.
- Hardware moet officieel worden ondersteund door de Cisco Plug and Play-service.
- Apparaatserienummers en PID's moeten toegankelijk zijn.
- Doelsitehiërarchieën moeten vooraf worden geconfigureerd in de Catalyst Center-omgeving.

2. Invoerprocedure in bulk

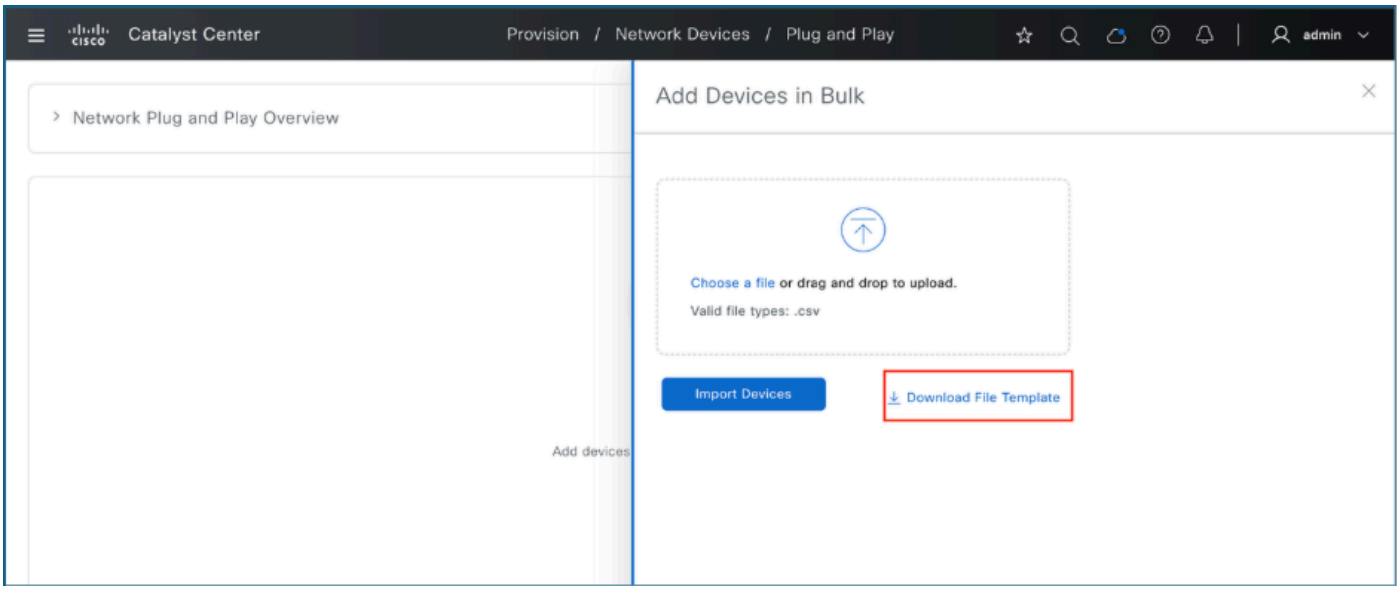
1. Aanmelden bij Catalyst Center
2. Navigeer naar Voorzieningen > Plug and Play
3. Klik op Apparaten toevoegen



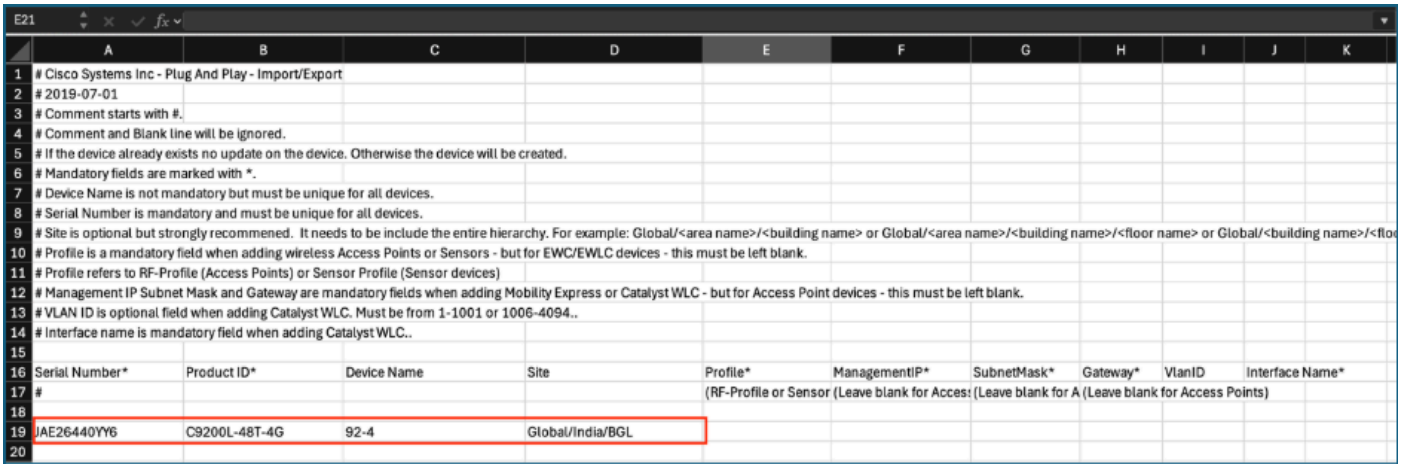
4. Klik op Bulksgewijs toevoegen



5. Klik op Bestandssjabloon downloaden om het voorbeeld CSV-bestand te downloaden

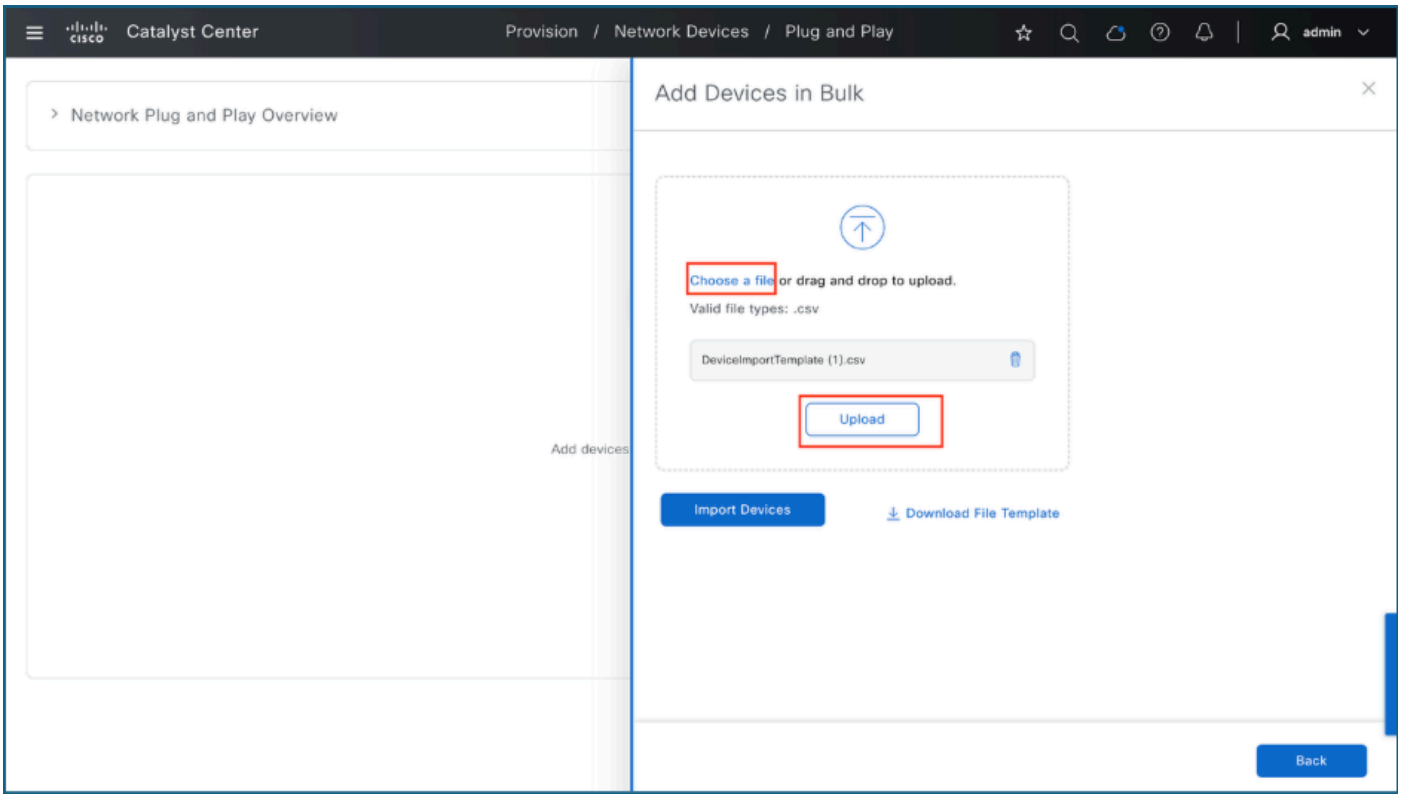


6. Vul het CSV-bestand in met de vereiste apparaatgegevens.

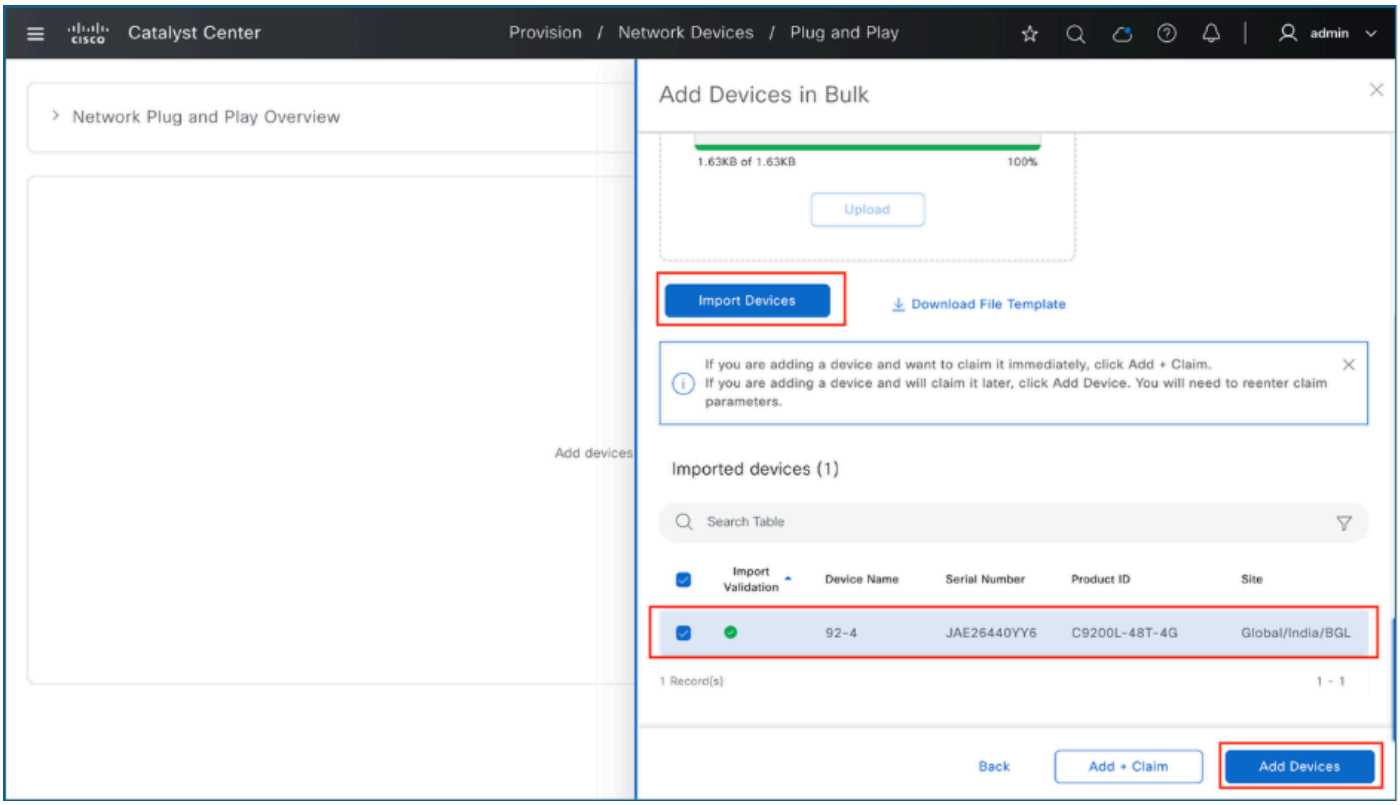


	A	B	C	D	E	F	G	H	I	J	K
1	# Cisco Systems Inc - Plug And Play - Import/Export										
2	# 2019-07-01										
3	# Comment starts with #.										
4	# Comment and Blank line will be ignored.										
5	# If the device already exists no update on the device. Otherwise the device will be created.										
6	# Mandatory fields are marked with *.										
7	# Device Name is not mandatory but must be unique for all devices.										
8	# Serial Number is mandatory and must be unique for all devices.										
9	# Site is optional but strongly recommened. It needs to be include the entire hierarchy. For example: Global/<area name>/<building name> or Global/<area name>/<building name>/<floor name> or Global/<building name>/<flo										
10	# Profile is a mandatory field when adding wireless Access Points or Sensors - but for EWC/EWLC devices - this must be left blank.										
11	# Profile refers to RF-Profile (Access Points) or Sensor Profile (Sensor devices)										
12	# Management IP Subnet Mask and Gateway are mandatory fields when adding Mobility Express or Catalyst WLC - but for Access Point devices - this must be left blank.										
13	# VLAN ID is optional field when adding Catalyst WLC. Must be from 1-1001 or 1006-4094..										
14	# Interface name is mandatory field when adding Catalyst WLC..										
15											
16	Serial Number*	Product ID*	Device Name	Site	Profile*	ManagementIP*	SubnetMask*	Gateway*	VlanID	Interface Name*	
17	#				(RF-Profile or Sensor	(Leave blank for Acces	(Leave blank for A	(Leave blank for Access Points)			
18											
19	JAE26440YY6	C9200L-48T-4G	92-4	Global/India/BGL							
20											

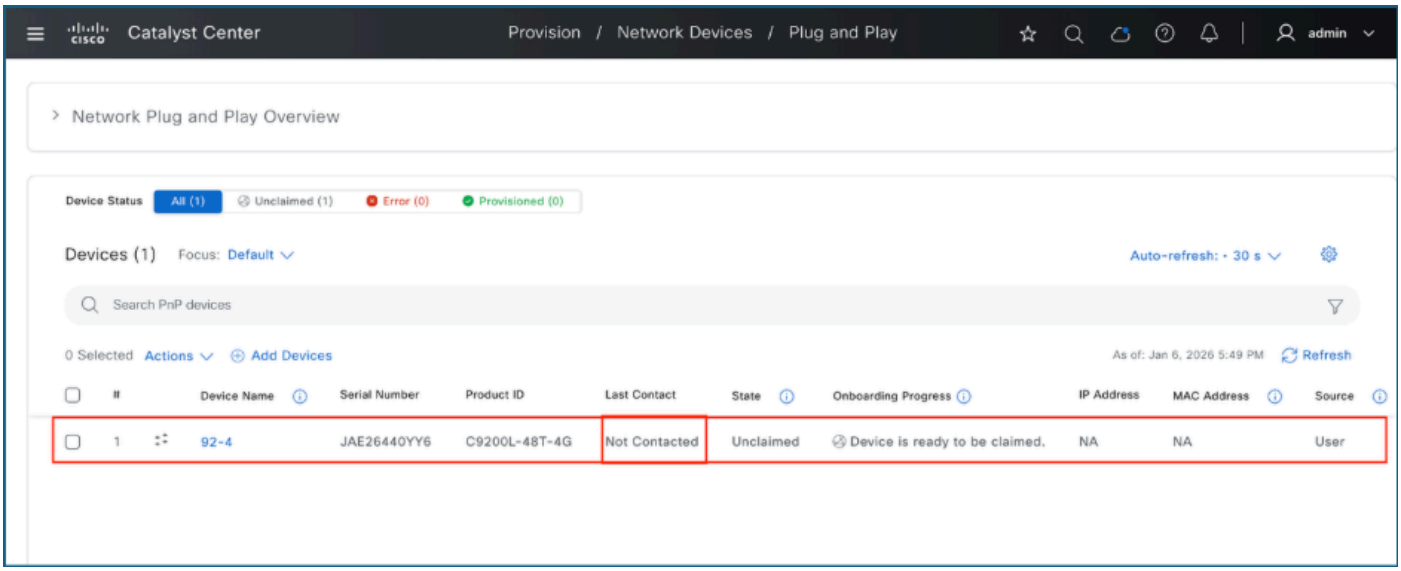
7. Upload het ingevulde CSV-bestand.



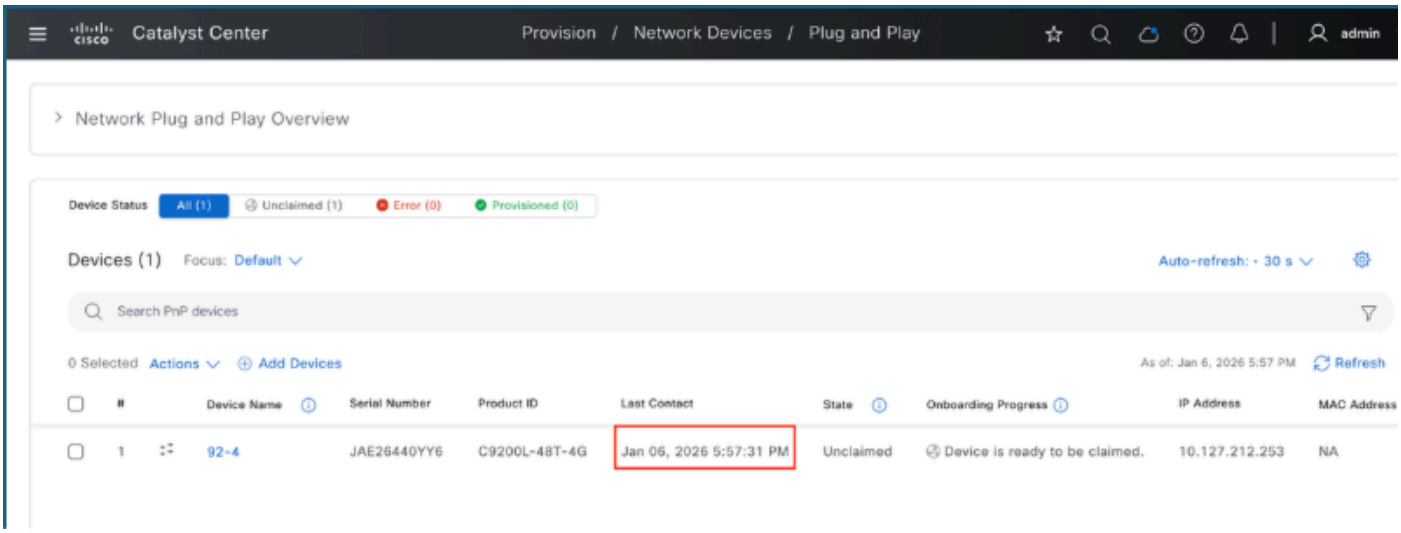
8. Importeer de apparaten uit het CSV-bestand en voeg ze toe aan de PnP-inventaris



9. De apparaten worden in de inventaris weergegeven als Niet gecontacteerd.



10. Zodra het apparaat contact opneemt met Catalyst Center, kan het worden geclaimd.



Probleemoplossing

Als de switch niet wordt weergegeven op de pagina Plug and Play van Catalyst Center, zijn dit de stappen om het probleem te identificeren en op te lossen.

1. PnP-connectiviteitsvalidatie

Met deze opdrachten wordt PnP-connectiviteit met Catalyst Center gevalideerd.

1.1. Bereikbaarheid ICMP

Controleer de ICMP-connectiviteit door het IP- of VIP-adres (Virtual IP) van Catalyst Center vast te pingen. Zorg ervoor dat het Catalyst Center bereikbaar is via ping.

```
Switch#ping 10.127.212.43
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.127.212.43, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch#
```

1.2. HTTP HELLO-validatie

Plug and Play (PnP) mislukt als Catalyst Center niet reageert op HELLO-validatieverzoeken. Om de connectiviteit te verifiëren, voert u deze opdracht uit vanaf een apparaatterminal of opdrachtprompt: curl -v http://<Catalyst Center IP>/pnp/HELLO

Bevestig dat er een "HALLO"-reactie is ontvangen.

```
sitirkey@SITIRKEY-M-6PGJ netbox-docker % curl -v http://10.127.212.43/pnp/HE
*   Trying 10.127.212.43:80...
* Connected to 10.127.212.43 (10.127.212.43) port 80
> GET /pnp/HELLO HTTP/1.1
> Host: 10.127.212.43
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Sun, 04 Jan 2026 07:51:20 GMT
< Content-Type: text/plain;charset=iso-8859-1
< Content-Length: 5
< Connection: keep-alive
<
* Connection #0 to host 10.127.212.43 left intact
```

1.3. HTTPS-certificaatophalen

De PnP-functionaliteit mislukt als het certificaat van de Catalyst Center-server niet handmatig via HTTPS kan worden opgehaald. Gebruik deze opdracht om dit te verifiëren: kopieer https://<catc-ip-address>/ca/pem mypem2

Bevestig dat de bestandsoverdracht zonder fouten wordt voltooid.

```
92-4#copy https://10.127.212.43/ca/pem mypem2
Destination filename [mypem2]?
Accessing https://10.127.212.43/ca/pem...
Loading https://10.127.212.43/ca/pem
1472 bytes copied in 0.060 secs (24533 bytes/sec)
92-4#
```

1.4. PnP-profielstatus

Als een switch niet wordt weergegeven op de PnP-pagina van Catalyst Center, onderzoekt u de PnP HTTP-connectiviteit door de opdracht uit te voerenPNP-profiel weergeven

- Controleer of PnP de juiste Active-URL gebruikt.

- Bevestig dat "Mislukte tellers" in de HTTP-statistieken 0 is. Een waarde groter dan 0 duidt op bereikbaarheidsproblemen tussen de switch en het katalysatorcentrum. Deze afbeelding illustreert een scenario met bereikbaarheidsproblemen.

```
Switch#show pnp profile
PnP Profiles: Active:0, Created:0, Deleted:0, Hidden:0

Name            CBType Node     Primary-Path           Primary-Trans  Backup-Trans

-------------- show pnp http tracking ---------------

PNP-T3-Discovery: Active-Name=[PnP-Discovery-Proc], Last-Name=[PnP-Discovery-Proc]
        Active-URL=[http://10.127.212.43:80/pnp/HELLO], Last-URL=[http://10.127.212.43:80/pnp/HELLO]
        SID=7, Last-SID=6, TID=4294967295, last-TID=4294967295, Head-Date=[-], Status-Code=0, Get-Status=0, Get-Watch=7F6CDC0EF0
        HTTP-Register Stats: Total=3, OK=3, Failed=0, Ignored=0
        HTTP-Unregister Stats: Total=2, OK=2, Failed=0, Ignored=0
        HTTP-Resp-Data-Alloc Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Free Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Proc Stats: Total=6, OK=0, Failed=6, Ignored=0
        HTTP-Get-Watch-Init Stats: Total=6, OK=6, Failed=0, Ignored=0
        HTTP-Get-Wait-Complete Stats: Total=6, OK=6, Failed=0, Ignored=0
        HTTP-Send-Get Stats: Total=6, OK=0, Failed=6, Ignored=0
        HTTP-Send-Head Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Hello Stats: Total=0, OK=0, Failed=0, Ignored=0
        SSL-Handshake Stats: Total=0, OK=0, Failed=0, Ignored=0
        Server-ID-Check Stats: Total=0, OK=0, Failed=0, Ignored=0

PNP-HTTP-Tracker: Active-Name=[-], Last-Name=[-]
        Active-URL=[-], Last-URL=[-]
        SID=0, Last-SID=0, TID=0, last-TID=0, Head-Date=[-], Status-Code=0, Get-Status=0, Get-Watch=0
        HTTP-Register Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Unregister Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Alloc Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Free Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Proc Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Get-Watch-Init Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Get-Wait-Complete Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Get Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Head Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Hello Stats: Total=0, OK=0, Failed=0, Ignored=0
        SSL-Handshake Stats: Total=0, OK=0, Failed=0, Ignored=0
        Server-ID-Check Stats: Total=0, OK=0, Failed=0, Ignored=0
Switch#
```

Dit voorbeeld illustreert een scenario zonder problemen met bereikbaarheid.

```
PNP-T1-Discovery: Active-Name=[PnP-Discovery-Proc], Last-Name=[-]
        Active-URL=[http://catc1.cisco.com:80/pnp/HELLO], Last-URL=[-]
        SID=5, Last-SID=0, TID=1, last-TID=0, Head-Date=[Mon, 05 Jan 2026 15:28:17 GMT], Status-Code=200, Get-Status=8, Get-Watch=4B881114
        HTTP-Register Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Unregister Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Alloc Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Resp-Data-Free Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Resp-Data-Proc Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Get-Watch-Init Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Get-Wait-Complete Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Send-Get Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Send-Head Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Hello Stats: Total=0, OK=0, Failed=0, Ignored=0
        SSL-Handshake Stats: Total=0, OK=0, Failed=0, Ignored=0
        Server-ID-Check Stats: Total=0, OK=0, Failed=0, Ignored=0

PNP-T1-pnp-zero-touch: Active-Name=[PnP-pnp-zero-touch], Last-Name=[-]
        Active-URL=[https://catc1.cisco.com:443/pnp/HELLO], Last-URL=[-]
        SID=8, Last-SID=0, TID=8, last-TID=0, Head-Date=[Mon, 05 Jan 2026 15:28:34 GMT], Status-Code=200, Get-Status=8, Get-Watch=4B881570
        HTTP-Register Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Unregister Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Alloc Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Resp-Data-Free Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Resp-Data-Proc Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Get-Watch-Init Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Get-Wait-Complete Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Send-Get Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Send-Head Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Hello Stats: Total=1, OK=1, Failed=0, Ignored=0
        SSL-Handshake Stats: Total=0, OK=0, Failed=0, Ignored=0
        Server-ID-Check Stats: Total=0, OK=0, Failed=0, Ignored=0
```

2. DHCP-validatie

Deze opdrachten helpen de DHCP-configuratie en -connectiviteit te valideren.

2.1. Toewijzing van DHCP-IP-adres controleren

Voer de opdracht uit: toon een IP-interfacebrief om te controleren of de PnP VLAN SVI met succes een IP-adres van de DHCP-server heeft ontvangen.

```
Switch#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES unset  administratively down down
Vlan302                10.127.212.254  YES DHCP   up                    up
GigabitEthernet0/0     unassigned      YES unset  up                    up
```

2.2. Leaseserver bevestigen

Voer de opdracht show dhcp lease uit om de gegevens van de DHCP-leaseserver te verifiëren.

```
Switch#show dhcp lease
Temp IP addr: 10.127.212.254  for peer on Interface: Vlan302
Temp  sub net mask: 255.255.255.0
   DHCP Lease server: 10.127.212.49, state: 5 Bound
   DHCP transaction id: 23F1
   Lease: 86400 secs,  Renewal: 43200 secs,  Rebind: 75600 secs
Temp default-gateway addr: 10.127.212.49
   Next timer fires after: 11:52:27
   Retry count: 0   Client-ID: cisco-4464.3cb1.2bf7-Vl302
   Client-ID hex dump: 636973636F2D343436342E336362312E
                       326266372D566C333032
   Hostname: Switch
```

2.3. Optie 43 valideren met behulp van foutopsporingslogboeken

Als u optie 43 wilt valideren, schakelt u DHCP-foutopsporing in met de opdracht foutopsporing dhcp-details. Na het inschakelen van de foutopsporing voert u een uitschakeling en geen uitschakeling uit op de interface om het DHCP-proces opnieuw te starten. Zoek in de logs de sectie "DHCP: Scan: Vendor specific option 43:". Kopieer de hex string zoals getoond in deze sectie, converteer deze naar tekst met behulp van een geschikte hex-naar-ASCII converter en controleer of de resulterende string correct naar Catalyst Center wijst.

```
000344: Jan  4 08:55:39.247: DHCP Offer Message   Offered Address: 10.127.212.254
000345: Jan  4 08:55:39.247: DHCP: Lease Seconds: 86400    Renewal secs:  43200    Rebind secs:   75600
000346: Jan  4 08:55:39.247: DHCP: Server ID Option: 10.127.212.49
000347: Jan  4 08:55:39.247: DHCP: offer received from 10.127.212.49
000348: Jan  4 08:55:39.247: DHCP: SRequest attempt # 1 for entry:
000349: Jan  4 08:55:39.247: Temp IP addr: 10.127.212.254  for peer on Interface: Vlan302
000350: Jan  4 08:55:39.247: Temp  sub net mask: 255.255.255.0
000351: Jan  4 08:55:39.247:    DHCP Lease server: 10.127.212.49, state: 4 Requesting
000352: Jan  4 08:55:39.247:    DHCP transaction id: A62
000353: Jan  4 08:55:39.247:    Lease: 86400 secs,  Renewal: 0 secs,  Rebind: 0 secs
000354: Jan  4 08:55:39.247:    Next timer fires after: 00:00:03
000355: Jan  4 08:55:39.247:    Retry count: 1   Client-ID: cisco-4464.3cb1.2bf7-Vl302
000356: Jan  4 08:55:39.247:    Client-ID hex dump: 636973636F2D343436342E336362312E
000357: Jan  4 08:55:39.247:                        326266372D566C333032
000358: Jan  4 08:55:39.248:    Hostname: Switch
000359: Jan  4 08:55:39.248: DHCP: SRequest- Server ID option: 10.127.212.49
000360: Jan  4 08:55:39.248: DHCP: SRequest- Requested IP addr option: 10.127.212.254
000361: Jan  4 08:55:39.248: DHCP: SRequest placed lease len option: 86400
000362: Jan  4 08:55:39.248: DHCP: SRequest placed class-id option: 636973636F706E70
000363: Jan  4 08:55:39.248: DHCP: SRequest: 323 bytes
000364: Jan  4 08:55:39.248: DHCP: SRequest: 323 bytes
000365: Jan  4 08:55:39.248:             B'cast on Vlan302 interface from 0.0.0.0
000366: Jan  4 08:55:39.254: DHCP: Received a BOOTREP pkt
000367: Jan  4 08:55:39.254: DHCP: Scan: Message type: DHCP Ack
000368: Jan  4 08:55:39.254: DHCP: Scan: Client ID: cisco-4464.3cb1.2bf7-Vl302
000369: Jan  4 08:55:39.254: DHCP: Scan: Server ID Option: 10.127.212.49 = A7FD431
000370: Jan  4 08:55:39.254: DHCP: Scan: Lease Time: 86400
000371: Jan  4 08:55:39.254: DHCP: Scan: Renewal time: 43200
000372: Jan  4 08:55:39.254: DHCP: Scan: Rebind time: 75600
000373: Jan  4 08:55:39.254: DHCP: Scan: Subnet Address Option: 255.255.255.0
000374: Jan  4 08:55:39.254: DHCP: Scan: Vendor specific option 43: 3541314E3B42323B4B343B4931302E3132372E3231322E34333B4A38303B
000375: Jan  4 08:55:39.254: DHCP: Scan: Router Option: 10.127.212.49
000376: Jan  4 08:55:39.254: DHCP: rcvd pkt source: 10.127.212.49,  destination:  255.255.255.255
000377: Jan  4 08:55:39.254:    UDP  sport: 43,  dport: 44,  length: 349
000378: Jan  4 08:55:39.255:    DHCP op: 2, htype: 1, hlen: 6, hops: 0
000379: Jan  4 08:55:39.255:    DHCP server identifier: 10.127.212.49
000380: Jan  4 08:55:39.255:         xid: A62, secs: 0, flags: 8000
000381: Jan  4 08:55:39.255:         client: 0.0.0.0, your: 10.127.212.254
000382: Jan  4 08:55:39.255:         srvr:   0.0.0.0, gw: 0.0.0.0
000383: Jan  4 08:55:39.255:         options block length: 101

000384: Jan  4 08:55:39.255: DHCP Ack Message
000385: Jan  4 08:55:39.255: DHCP: Lease Seconds: 86400    Renewal secs:  43200    Rebind secs:   75600
000386: Jan  4 08:55:39.255: DHCP: Server ID Option: 10.127.212.49
000387: Jan  4 08:55:40.232: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan302, changed state to up
000388: Jan  4 08:55:42.256: DHCP: Offered Address has no conflicts
000389: Jan  4 08:55:42.259: DHCP: Releasing ipl options:
000390: Jan  4 08:55:42.259: DHCP: Applying DHCP options:
000391: Jan  4 08:55:42.259:   Setting default_gateway to 10.127.212.49
000392: Jan  4 08:55:42.260:   Adding default route 10.127.212.49
000393: Jan  4 08:55:43.259: DHCPC: Notifying other components about option 43
000394: Jan  4 08:55:43.259: DHCP: Sending notification of ASSIGNMENT:
000395: Jan  4 08:55:43.259:   Address 10.127.212.254 mask 255.255.255.0
```

beste praktijken

- Zorg ervoor dat de switch zich in de fabrieksinstellingen bevindt. Als deze eerder is geleverd, gebruikt u de opdracht pnpa service reset om deze opnieuw in te stellen.
- Onderbreek het PnP-proces niet via de console.

- Controleer certificaten en DNS-resolutie voorafgaand aan implementatie.

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.