

Comprendre l'intégration de commutateurs via Catalyst Center Plug and Play

Table des matières

[Introduction](#)

[Description](#)

[Public](#)

[Exigences](#)

[Conditions préalables](#)

[Présentation du concept Plug-and-Play](#)

[1. Détection DHCP du serveur Plug and Play](#)

[2. Format DHCP Option 43](#)

[Option 43 Définitions des champs](#)

[3. Exemples de configuration de l'option DHCP 43](#)

[4. Comportement VLANB de démarrage PnP](#)

[Vérification du certificat CatalystCenter](#)

[Vérification GUI](#)

[Vérification CLI](#)

[Diagramme du réseau](#)

[MéthodesIntégrationCommutateur](#)

[1. Intégration à l'aide de VLAN1](#)

[2. Intégration à l'aide du VLAN personnalisé](#)

[3. Commutateur intégré utilisant le port de gestion](#)

[4. Journaux de console du commutateur](#)

[Intégration du commutateur à CatalystCenter sans les modèles du jour 0](#)

[1. Pour réclamer des commutateurs :](#)

[2. Pour nommer et mapper le commutateur :](#)

[3. AssignSoftwareImage orTemplate \(facultatif\) :](#)

[4. Modèles de provisionnement](#)

[5. Résumé](#)

[6. Surveiller le processus de demande](#)

[Intégration du commutateur à Catalyst Center avec les modèles du jour 0](#)

[1. Créer un modèle de jour 0 ou d'intégration](#)

[2. Ajouter les détails du modèle](#)

[3. Modifier le modèle](#)

[4. Créer un profil réseau](#)

[5. Ajoutez un modèle et modifiez les paramètres du profil réseau](#)

[6. Enregistrez le profil](#)

[7. Attribuez un profil de réseau au site où les commutateurs/commutateurs doivent être intégrés](#)

[8. RevendicationCommutateurs](#)

[9. Attribuez un nom au commutateur et affectez-le à un site](#)

[10. Affecter un modèle Jour-0](#)

[11. Modèles de provisionnement](#)

[12. Résumé](#)

[13. Suivre l'avancement des demandes](#)

[Vérification](#)

[Importation en masse dePériphériques dans CatalystCenterInventaire Plug-and-Play](#)

[1. Conditions préalables](#)

[2. Procédure d'importation groupée](#)

[Dépannage](#)

[1. Validation de la connectivité PnP](#)

[1.1. Accessibilité ICMPR](#)

[1.2. Validation HTTPHELLO](#)

[1.3. Récupération du certificat HTTPS](#)

[1.4. État du profil PnP](#)

[2. Validation DHCP](#)

[2.1. Vérification de l'attribution des adresses IP DHCP](#)

[2.2. Confirmer le serveur de location](#)

[2.3. Valider l'option 43 à l'aide des journaux de débogage](#)

[Meilleures pratiques](#)

Introduction

Ce document décrit Catalyst Center Plug and Play pour l'intégration automatisée des commutateurs, le cycle de vie complet, les méthodes de détection et le dépannage.

Description

Catalyst Center Plug and Play (PnP) automatise l'intégration des commutateurs Cisco Catalyst via l'agent PnP intégré Cisco IOS® XE. Ce processus permet la découverte sécurisée, l'authentification et le provisionnement initial avec un effort manuel minimal, accélérant considérablement les déploiements et améliorant la cohérence de la configuration. En prenant en charge des déploiements évolutifs via des paramètres standardisés et des modèles Day-0 en option, PnP garantit un déploiement fiable et évolutif.

Le document décrit le cycle de vie complet de l'intégration, y compris les workflows Plug and Play, les méthodes de détection, les options d'intégration et la validation des certificats. Il fournit également des conseils détaillés sur la demande, la vérification, le dépannage des périphériques et les meilleures pratiques du secteur.

Public

Ce document est destiné aux administrateurs réseau, aux ingénieurs de déploiement et aux intégrateurs système qui déploient et gèrent des commutateurs Cisco Catalyst via Catalyst Center.

Exigences

Il est préférable que les lecteurs de ce document aient une connaissance pratique de base de ces sujets :

- Centre Catalyst
- commutateurs Cisco Catalyst
- Automatisation et provisionnement du réseau
- Notions de base sur DHCP et DNS

Conditions préalables

Assurez-vous que ces conditions préalables sont remplies avant de commencer le processus d'intégration :

- Catalyst Center 2.3.7.9 ou version ultérieure est installé et opérationnel.
- Les commutateurs Cisco Catalyst exécutent un Cisco IOS XE version 16.12.x ou ultérieure pris en charge.
- La connectivité réseau est disponible entre les commutateurs Catalyst et Catalyst Center.
- Le serveur DHCP est configuré avec l'option 43 pointant vers l'adresse IP ou le nom de domaine complet de l'interface d'entreprise de Catalyst Center.
- Les commutateurs sont dans l'état par défaut (out-of-box) et la commande `pnpa service`

reset disponible sur IOS XE 16.12.1 et versions ultérieures peut être utilisée pour réinitialiser un commutateur à cet état.

Présentation du concept Plug-and-Play

Examinez ces concepts clés qui expliquent comment Catalyst Center Plug and Play intègre un nouveau commutateur.

1. Détection DHCP du serveur Plug and Play

Lorsqu'un commutateur Cisco Catalyst est mis sous tension par défaut, l'agent Plug-and-Play tente de détecter un contrôleur Plug-and-Play (comme Catalyst Center) à l'aide du protocole DHCP.

Le processus de détection utilise l'échange DHCP standard :

- Détection DHCP
- Offre DHCP
- Requête DHCP
- Accusé de réception DHCP

S'il est configuré correctement, le serveur DHCP inclut l'option 43, qui fournit au commutateur les détails de connexion du serveur Plug and Play.

2. Format DHCP Option 43

La valeur DHCP Option 43 est une chaîne ASCII séparée par des points-virgules qui spécifie comment le commutateur se connecte au serveur Plug and Play.

Exemple :

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

Option 43 Définitions des champs

- 5A1N
 - 5 - Sous-option PnP
 - A - Mode actif (le périphérique initie la communication)
 - 1 - Version du modèle d'agent Plug and Play
 - N - Débogage désactivé (D active le débogage)
- B2 - Type d'adresse IP du serveur Plug and Play
 - 1 - Nom d'hôte
 - 2 - Adresse IPv4
 - 3 - Adresse IPv6
- K4 - Protocole de transport
 - 4 - HTTP
 - 5 - HTTPS
- I - Adresse IP ou nom de domaine complet du serveur Plug and Play
- J - Numéro de port TCP

Les paramètres facultatifs sont les suivants :

- T - URL du bundle de certificats Trustpool (obligatoire pour HTTPS)
- Z - Adresse IP du serveur NTP (obligatoire lors de l'utilisation de la sécurité Trustpool)

3. Exemples de configuration de l'option DHCP 43

- Exemple 1 : Configuration IPv4 de l'option 43 : 10.127.212.43 [adresse IP de l'interface d'entreprise de Catalyst Center]

```
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
```

- Exemple 2 : Configuration du nom d'hôte Option 43 : catc1.cisco.com [FQDN de Catalyst Center]

```
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
```

- Exemple 3 : Option 43 Configuration IPv6 : 2001:60:60:60::133 [Adresse IPv6 de l'interface d'entreprise de Catalyst Center]

```
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. Comportement du VLAN de démarrage PnP

Par défaut, un commutateur réinitialisé en usine utilise le VLAN 1 pour la gestion PnP. Cisco recommande d'utiliser un VLAN de gestion dédié dans les environnements de production. Voici la commande permettant de configurer un VLAN de démarrage Plug-and-Play personnalisé :

```
pnp startup-vlan
```

Cette commande doit être configurée sur un commutateur en amont. Le commutateur en amont communique le VLAN de démarrage Plug-and-Play au nouveau commutateur à l'aide du protocole CDP (Cisco Discovery Protocol). Le commutateur en aval :

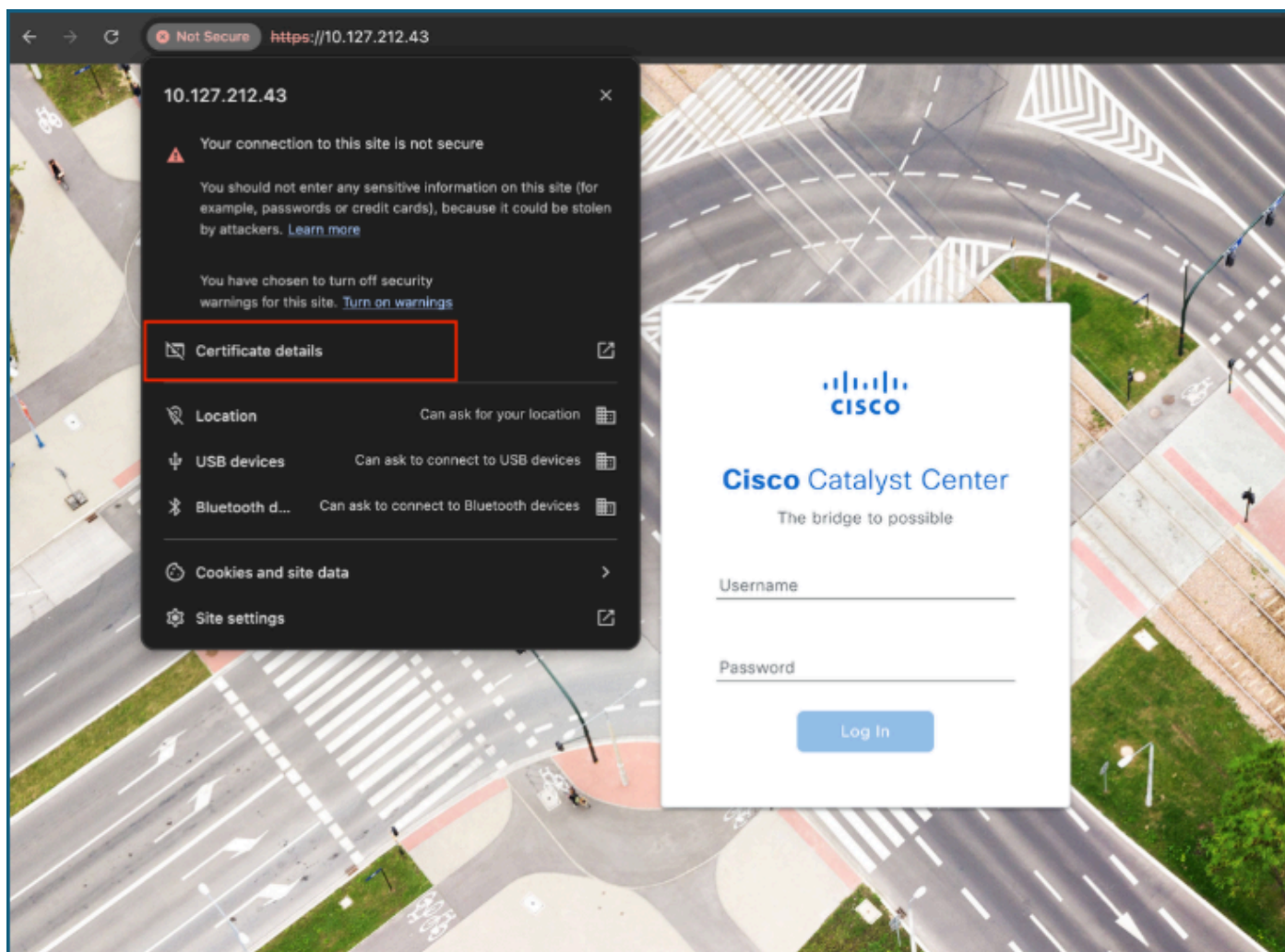
- Désactive DHCP sur VLAN 1
- Active DHCP sur le VLAN de démarrage configuré
- Met à jour l'agrégation pour autoriser le nouveau VLAN

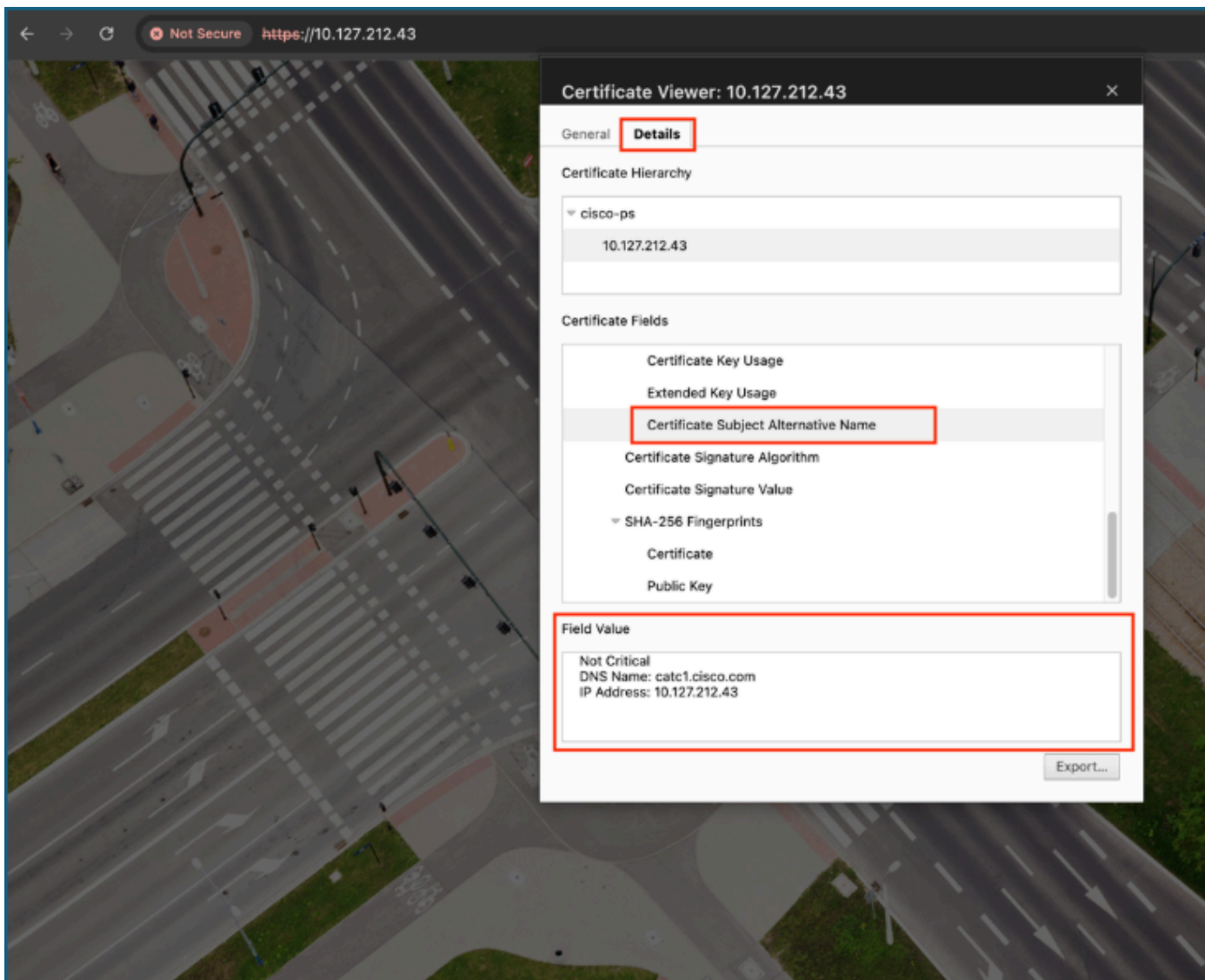
Vérification du certificat Catalyst Center

L'intégration sécurisée nécessite que le certificat SSL de Catalyst Center inclue l'adresse IP ou le nom de domaine complet (FQDN) utilisé par le commutateur dans le champ Subject Alternative Name (SAN).

Vérification GUI

1. Ouvrez la page de connexion de Catalyst Center dans un navigateur
2. Afficher les informations du site
3. Ouvrir les détails du certificat
4. Vérification des entrées SAN sous Extensions





Remarque : Si le champ SAN ou Autre nom du sujet contient :

- Only DNS Name : configurez le nom DNS dans la chaîne de l'option 43.
- Only IP Address : configurez l'adresse IP dans la chaîne de l'option 43.
- Adresse IP et nom DNS : configurez l'adresse IP dans la chaîne de l'option 43.

Vérification CLI

Pour vérifier cela, nous avons besoin de l'adresse IP de Catalyst Center et d'une machine pouvant atteindre le serveur Catalyst Center. Exécutez cette commande dans le terminal ou à l'invite de commandes.

```
echo | openssl s_client -showcerts -servername
```

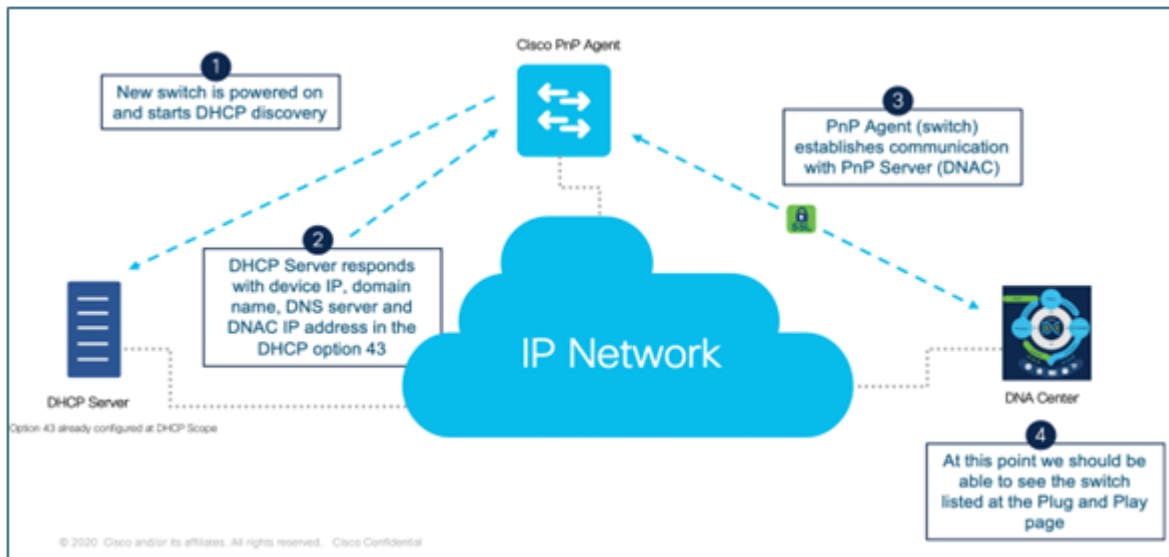
```
-connect
```

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

Vérifiez que le champ SAN contient l'adresse IP ou le nom de domaine complet approprié.

```
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:99:0e: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:e6:13:78:0e: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:e0:95:63: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
```

Diagramme du réseau



Cisco PnP automatise l'intégration des nouveaux périphériques en permettant la découverte, la configuration et la gestion avec un minimum d'effort manuel. Lorsqu'un nouveau commutateur est mis sous tension, il envoie une demande de détection DHCP et le serveur DHCP renvoie les détails du réseau, y compris l'adresse IP Catalyst Center (serveur Plug and Play) via DHCP Option 43. Grâce à ces informations, l'agent Plug and Play du commutateur se connecte en toute sécurité au serveur Plug and Play sur le réseau IP. Une fois la connexion établie, le périphérique est authentifié et identifié, puis ajouté à l'inventaire Plug-and-Play, où les administrateurs peuvent appliquer des configurations et terminer le provisionnement rapidement et de manière cohérente.

Méthodes d'intégration des commutateurs

Dans cette section, passez en revue les différentes méthodes d'intégration permettant d'intégrer un commutateur dans l'inventaire Plug-and-Play de Catalyst Center.

1. Intégration à l'aide de VLAN1

Cette méthode utilise le VLAN 1 par défaut pour la gestion PnP

Exigences

- L'interface SVI du VLAN 1 est configurée sur le commutateur en amont.
- Serveur DHCP avec option 43 configurée
- Résolution DNS pour le nom de domaine complet Catalyst Center

Procédure sur le commutateur en amont

Étape 1 : configuration de l'interface SVI du VLAN 1

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

Étape 2 : configuration d'un pool DHCP avec l'option 43 (Remarque : nous pouvons utiliser le paramètre Option 43 avec l'adresse IPv4 ou le nom de domaine complet de 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;
```

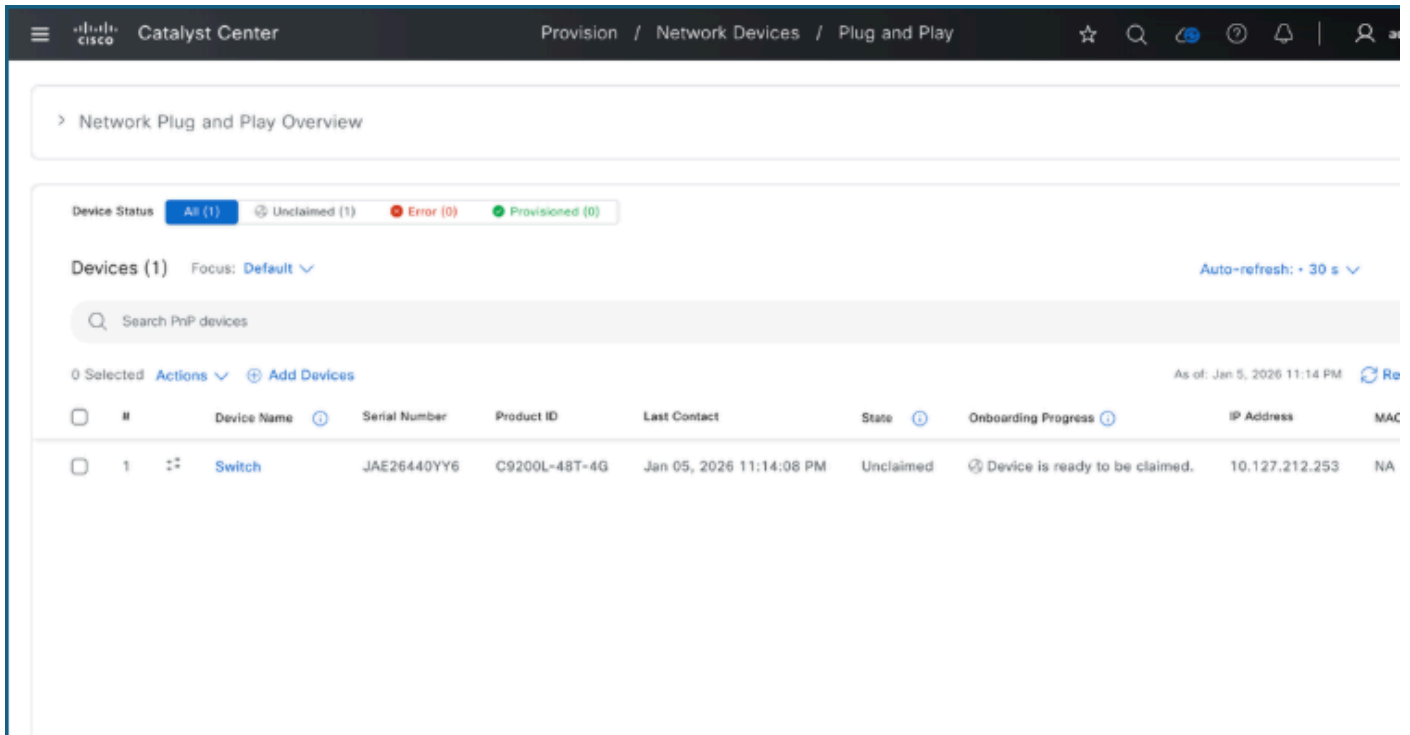
OU

```
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
```

Étape 3 : configuration d'une interface trunk vers le nouveau commutateur

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

Étape 4. Vérifiez que le commutateur apparaît sur la page Provisionnement > Plug and Play de Catalyst Center.



2. Intégration à l'aide du VLAN personnalisé

Cette méthode utilise un VLAN dédié pour la gestion.

Exigences

- SVI VLAN personnalisé configuré sur le commutateur en amont.
- Serveur DHCP avec option 43 configurée.
- Résolution DNS pour le nom de domaine complet Catalyst Center.
- L'agrégation autorise le VLAN personnalisé ainsi que tous les autres VLAN nécessaires à un autre trafic.

Procédure sur le commutateur en amont

Étape 1 : configuration de l'interface SVI du VLAN personnalisé

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

Étape 2 : configuration d'un pool DHCP avec l'option 43 (Remarque : nous pouvons utiliser le paramètre Option 43 avec l'adresse IPv4 ou le nom de domaine complet de 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;
```

OU

```
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
```

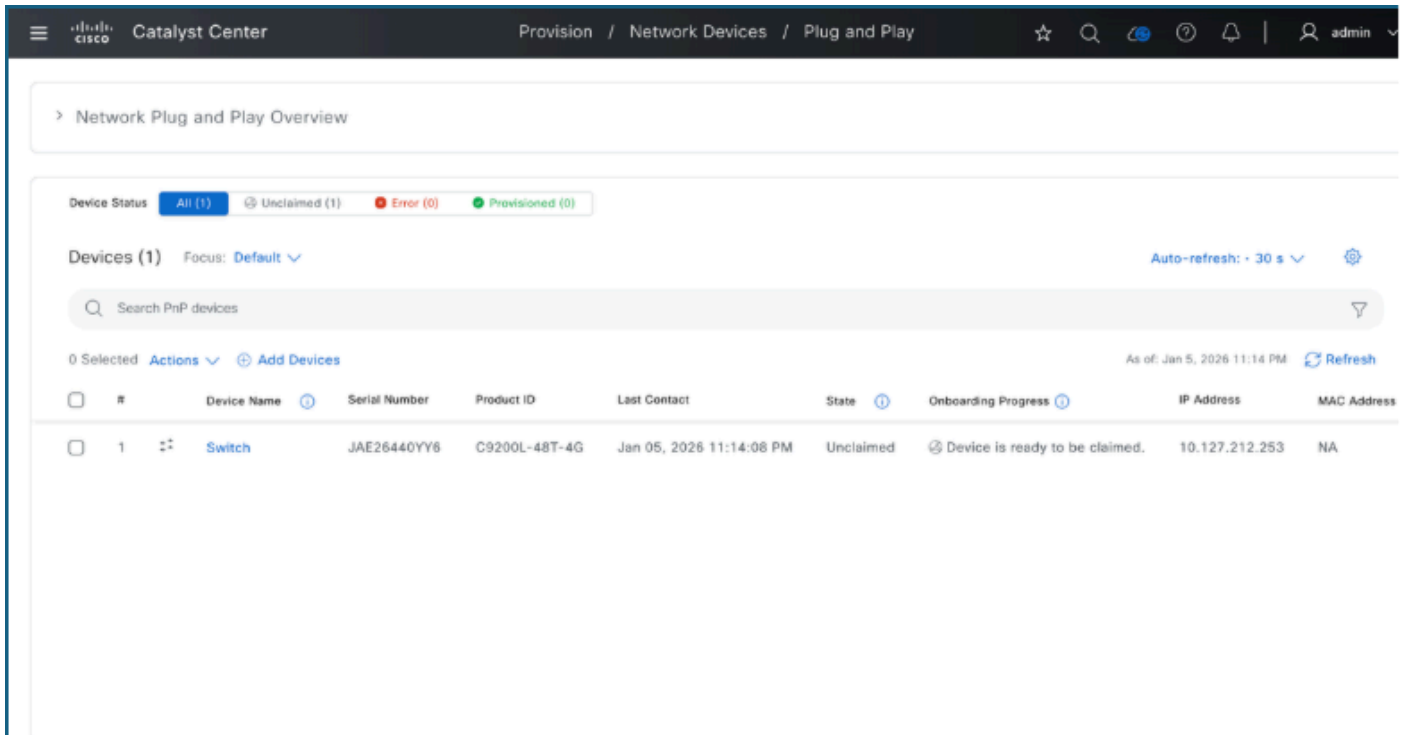
Étape 3 : configuration du VLAN personnalisé en tant que VLAN Plug-and-Play

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

Étape 4 : configuration de l'interface trunk sur le nouveau commutateur

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

Étape 5. Vérifiez que le commutateur apparaît sur la page Provisionnement > Plug and Play de Catalyst Center.



3. Commutateur intégré utilisant le port de gestion

Cette méthode utilise l'interface de gestion du commutateur.

Exigences

- SVI VLAN personnalisé configuré sur le commutateur en amont
- Serveur DHCP avec option 43 configurée
- Résolution DNS pour le nom de domaine complet Catalyst Center

Procédure sur le commutateur en amont.

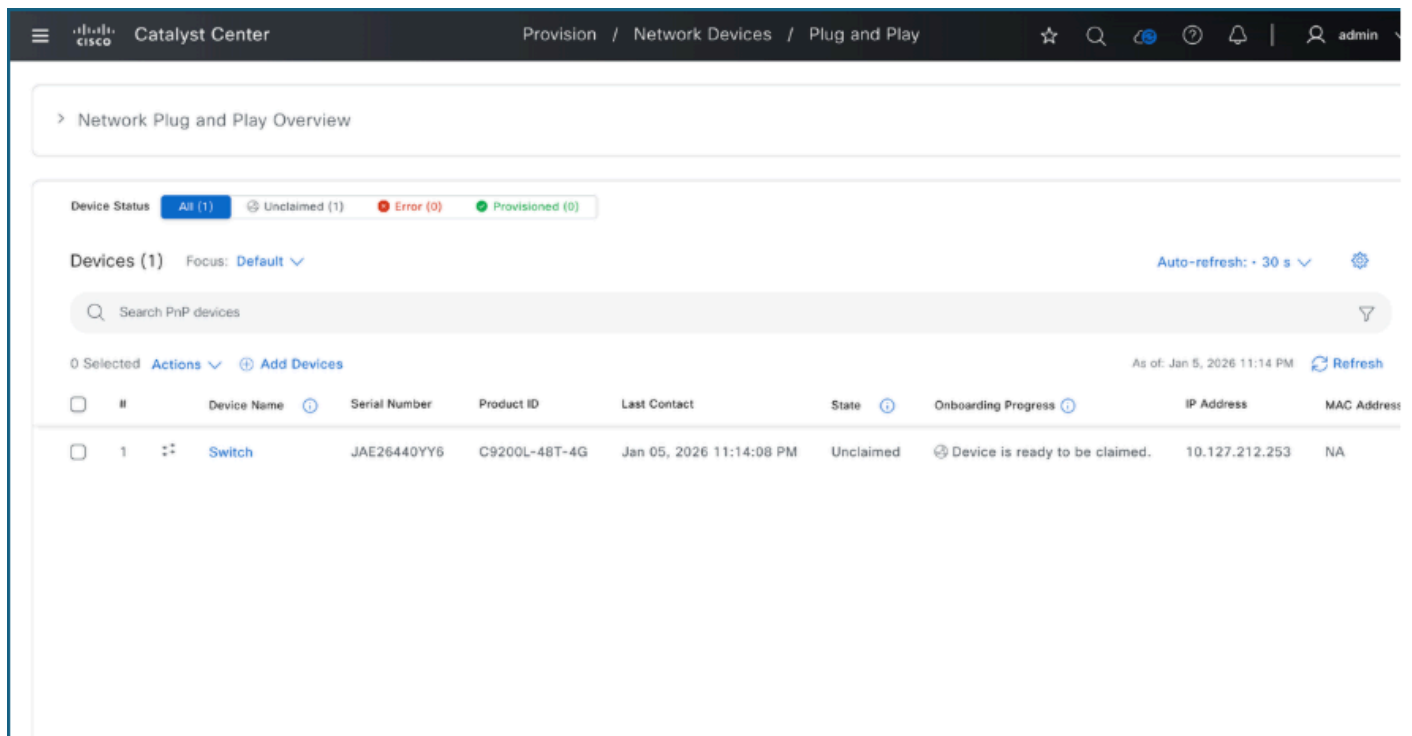
Étape 1 : configuration de l'interface SVI du VLAN

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

Étape 2 : configuration de l'interface d'accès au nouveau commutateur

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

Étape 3. Vérifiez que le commutateur apparaît sur la page Provisionnement > Plug and Play de Catalyst Center.



4. Journaux de console du commutateur

Voici ce qui apparaît sur la console du commutateur lorsque le protocole DHCP est utilisé pour Plug-and-Play.

```
Base Ethernet MAC Address      : 44:64:3c:b1:2b:80
Motherboard Assembly Number   : 73-102866-04
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!

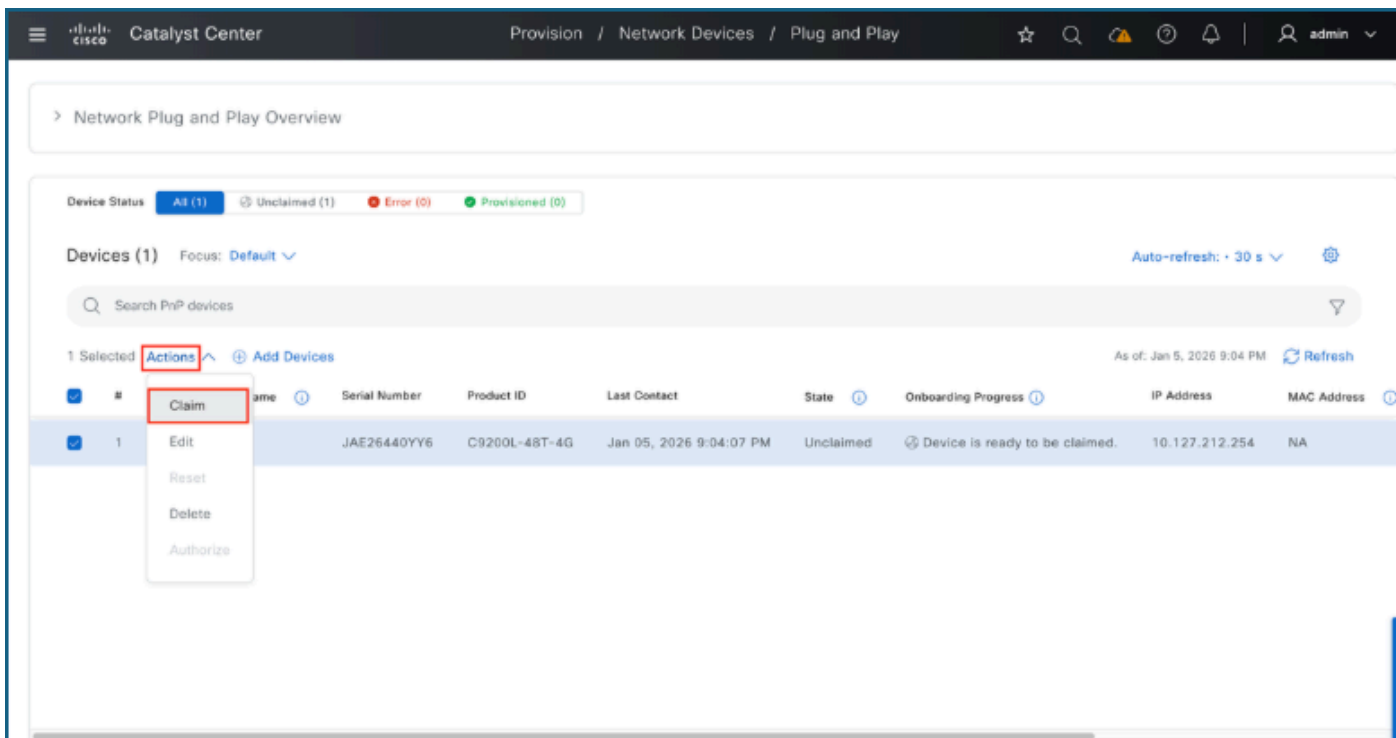
*Jan 5 15:28:24.332: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-2360689995 has been generated or imported by crypto-engine
*Jan 5 15:28:24.366: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jan 5 15:28:24.540: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write memory" to save 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: pnp-label created successfully
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-conf (Timed out)
Jan 5 15:28:39.911: AUTOINSTALL: Tftp script execution not successful for V1302.
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 15:29:44.690: %SYS-5-CONFIG_P: Configured programmatically by process XEP_pnp-zero-touch from console as vty0
```

Intégration de Switch to Catalyst Center sans modèles Day-0

Pour intégrer un nouveau commutateur dans l'inventaire de Catalyst Center, effectuez ces procédures requises une fois que le périphérique est visible et récupérable sur la page Plug-and-Play.

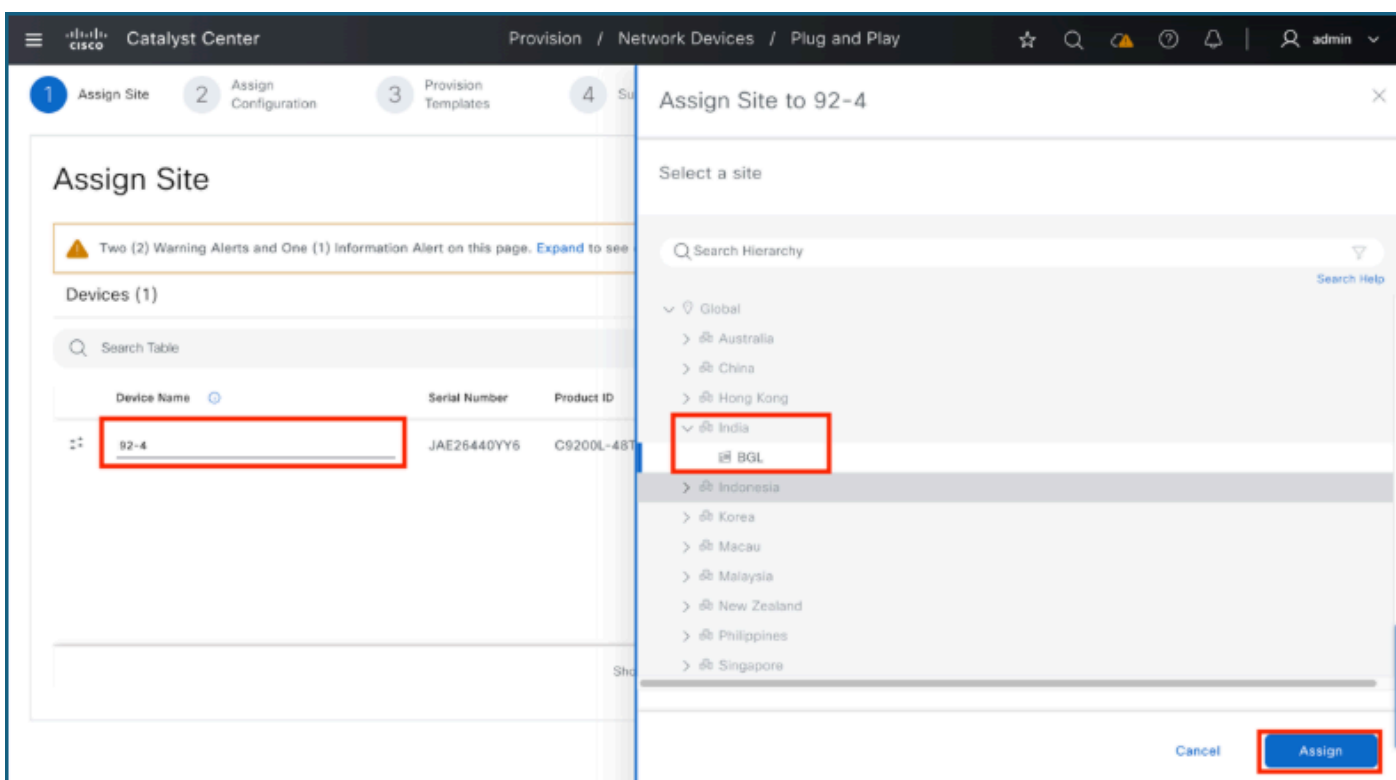
1. Pour réclamer des commutateurs :

- Cochez les cases correspondant aux commutateurs à réclamer.
- Accédez à Actions > Réclamation.



2. Pour nommer et mapper le commutateur :

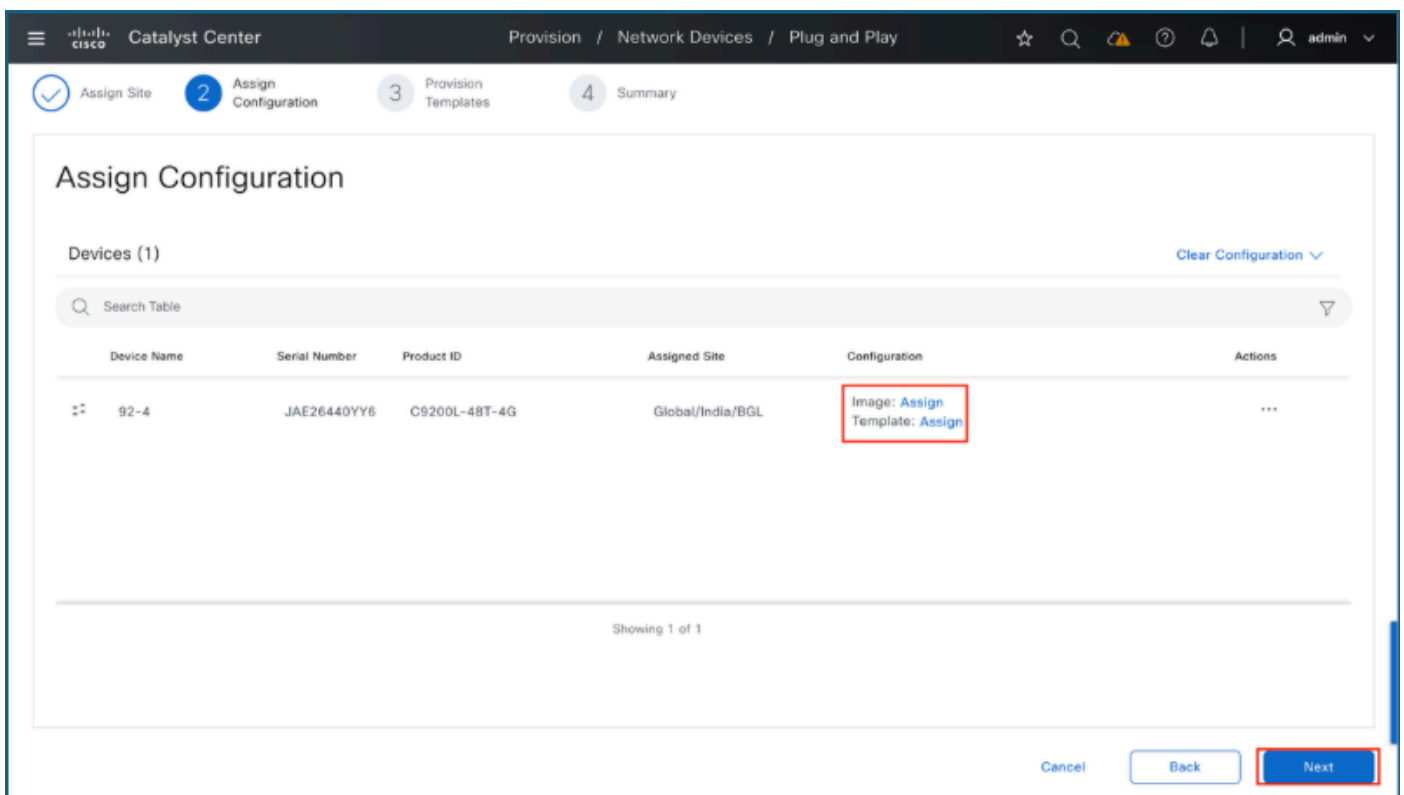
- Entrez le nom dans le champ Device Name et cliquez sur Assign.
- Choisissez le site ou le bâtiment approprié, cliquez à nouveau sur Assign, puis cliquez sur Next.



3. Attribuer une image ou un modèle de logiciel (facultatif) :

Utilisez cette étape pour mettre à niveau le commutateur vers une version logicielle spécifique ou appliquer un modèle de configuration du jour 0.

- Cliquez sur Assign en regard de Image pour spécifier la version du logiciel.
- Cliquez sur Affecter en regard de Modèle pour appliquer une configuration de modèle.
- Cliquez sur Next une fois les affectations souhaitées terminées.

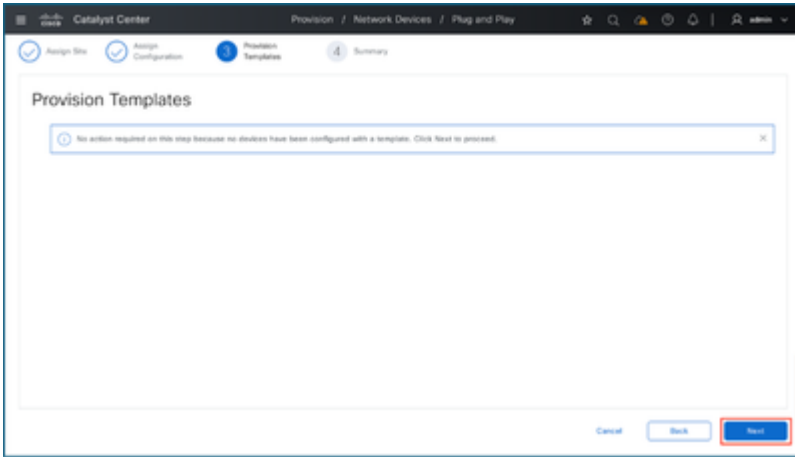


The screenshot shows the 'Assign Configuration' step in the Cisco Catalyst Center interface. The breadcrumb navigation at the top indicates the path: Provision / Network Devices / Plug and Play. The workflow progress bar shows four steps: 1. Assign Site (checked), 2. Assign Configuration (active), 3. Provision Templates, and 4. Summary. The main content area is titled 'Assign Configuration' and displays a table with one device. The table has columns for Device Name, Serial Number, Product ID, Assigned Site, Configuration, and Actions. The 'Configuration' column for the device '92-4' shows 'Image: Assign' and 'Template: Assign', with a red box highlighting these options. At the bottom right, there are three buttons: 'Cancel', 'Back', and 'Next', with 'Next' highlighted in blue.

Device Name	Serial Number	Product ID	Assigned Site	Configuration	Actions
92-4	JAE26440YY6	C9200L-48T-4G	Global/India/BGL	Image: Assign Template: Assign	...

4. Modèles de provisionnement

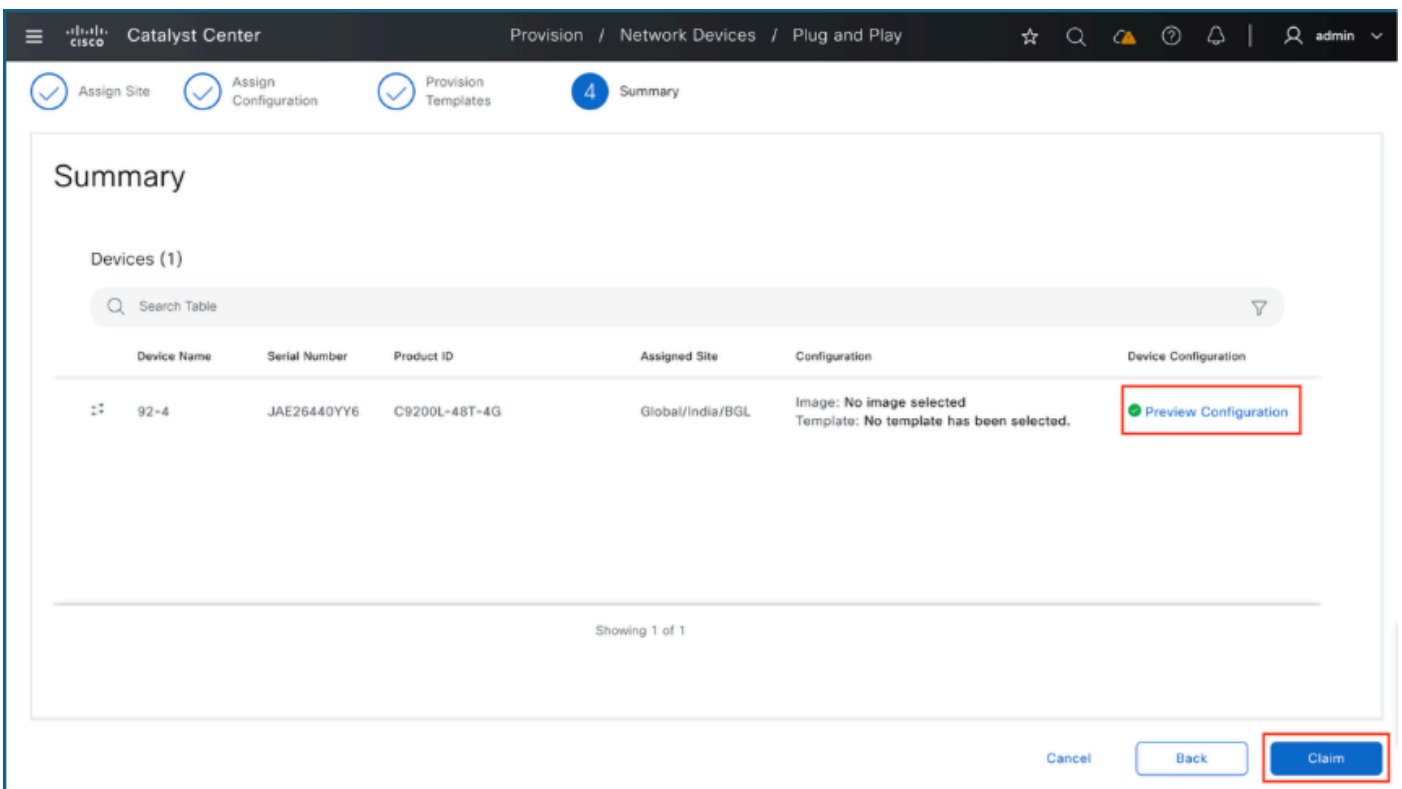
Lorsque vous demandez le périphérique sans utiliser de modèles, ignorez cette étape de configuration en sélectionnant Next (Suivant).

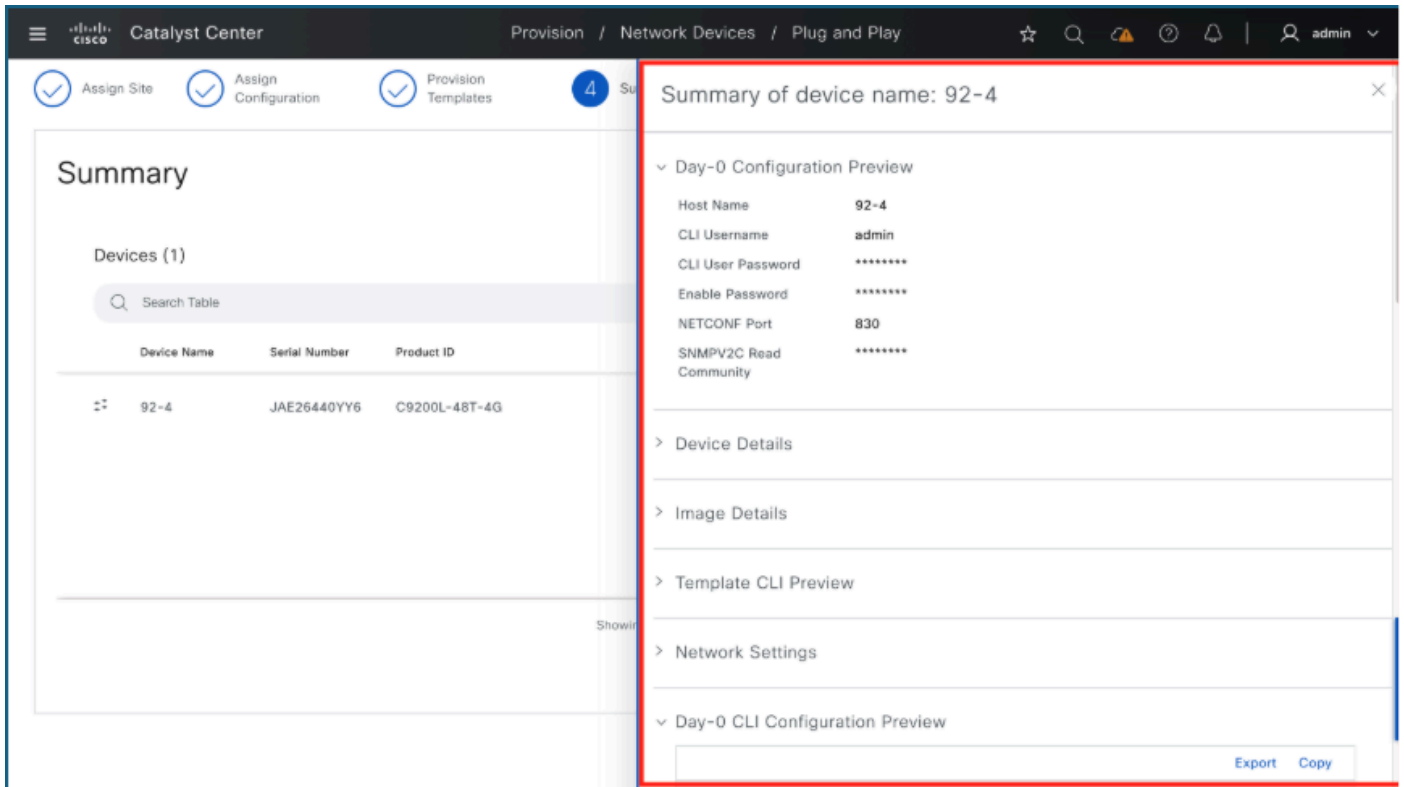


5. Résumé

Utilisez la page Récapitulatif pour vérifier la configuration avant qu'elle ne soit provisionnée par Catalyst Center.

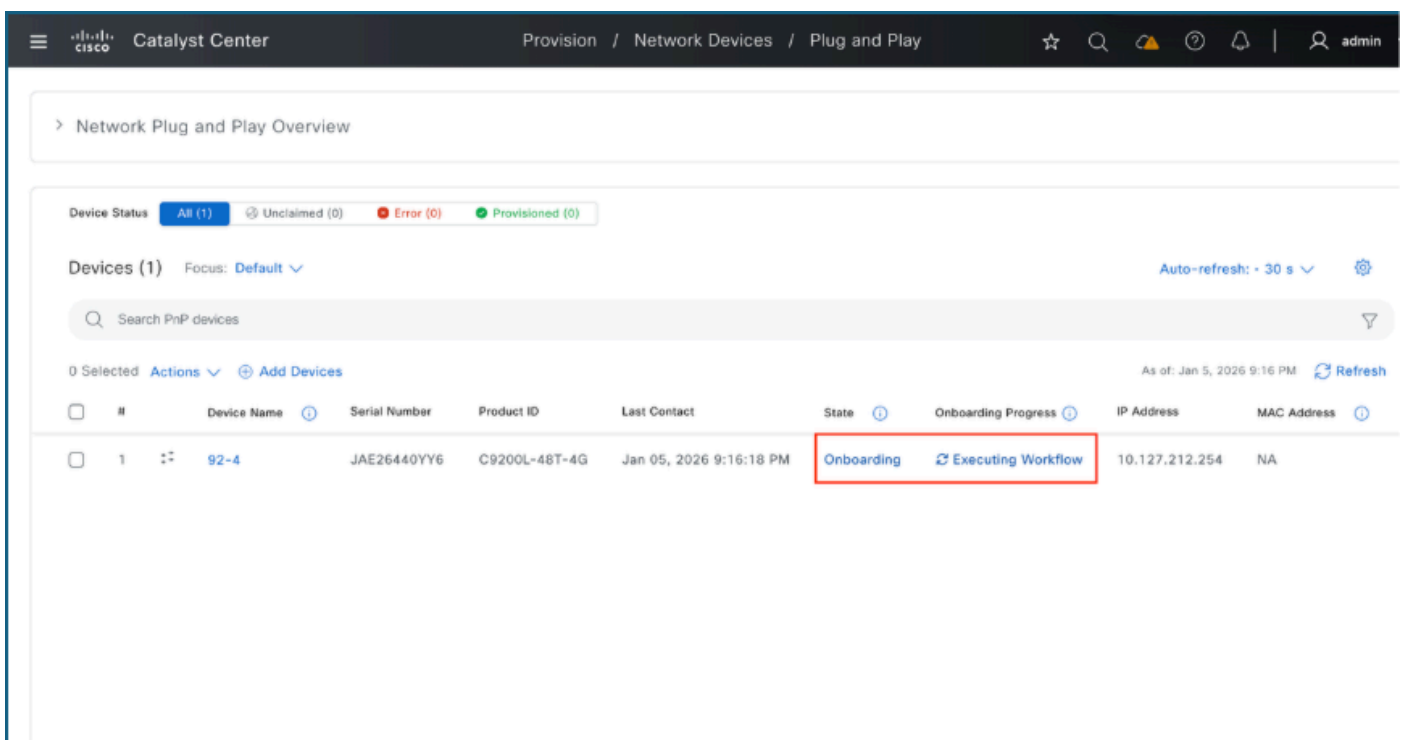
- Cliquez sur Preview Configuration.
- Développez les sections individuelles pour vérifier les paramètres.
- Une fois la vérification effectuée, cliquez sur Demande.

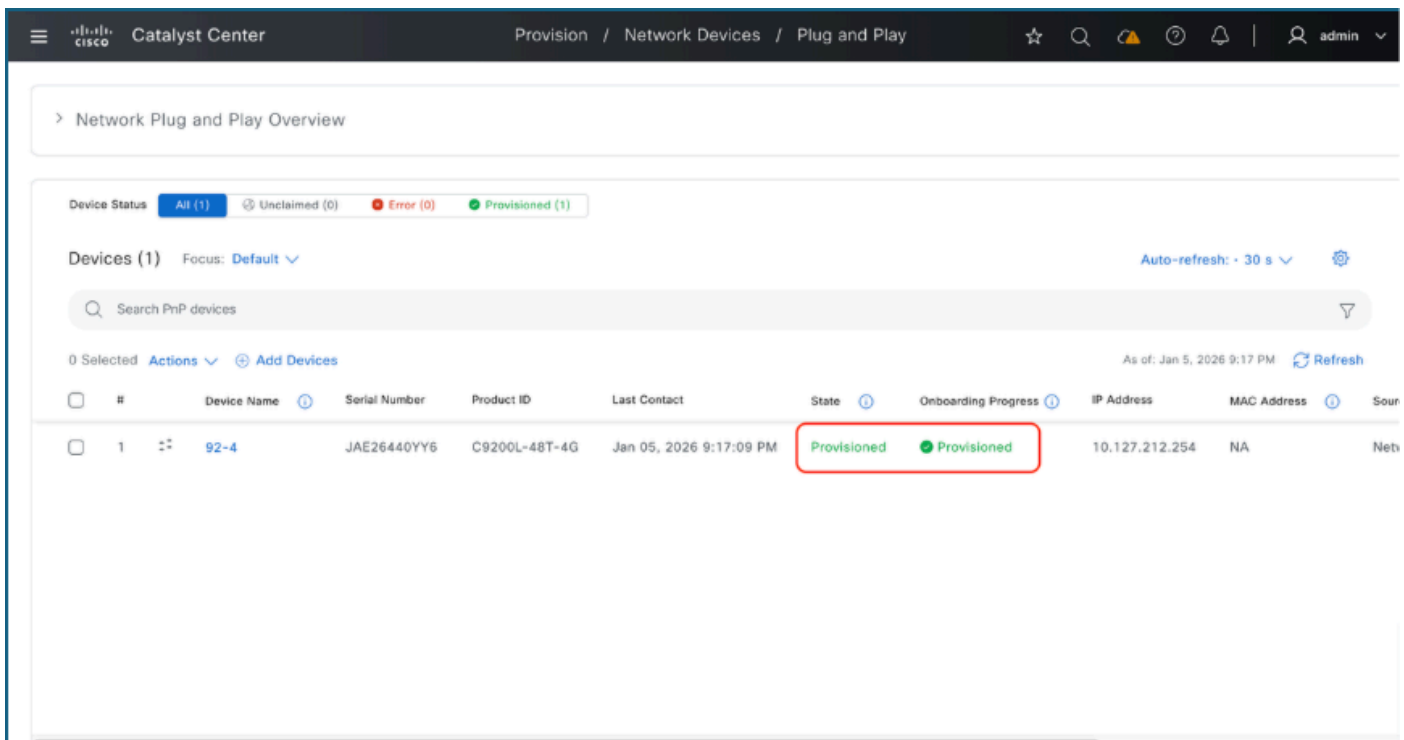




6. Surveiller le processus de réclamation

Lors de l'établissement de la demande, l'interface retourne au tableau de bord Plug-and-Play. Si vous surveillez l'état du périphérique, une transition vers Provisioned indique que le commutateur a été correctement revendiqué et ajouté à l'inventaire de Catalyst Center.



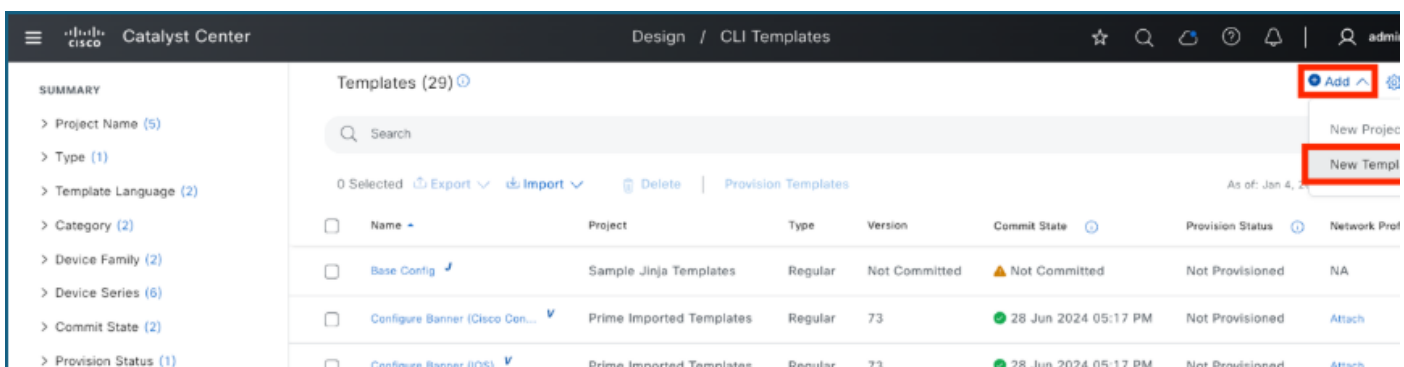


Intégration du commutateur à Catalyst Center avec les modèles du jour 0

Lorsque le nouveau commutateur est prêt à être réclamé sur la page Plug and Play de Catalyst Center, appliquez un modèle Jour 0 pour inclure une configuration supplémentaire pendant le processus de réclamation.

1. Créer un modèle de jour 0 ou d'intégration

- Accédez à Design > CLI Templates.
- Sélectionnez Ajouter > Nouveau modèle.



2. Ajouter les détails du modèle

Dans le panneau latéral, entrez les spécifications de gabarit suivantes :

- Nom du modèle
- Nom du projet : Pour les modèles du jour 0, sélectionnez toujours Onboarding Configuration.
- Type de modèle, Langue et Type de logiciel : Sélectionnez les valeurs appropriées dans les menus.
- Cliquez sur Continue pour continuer.

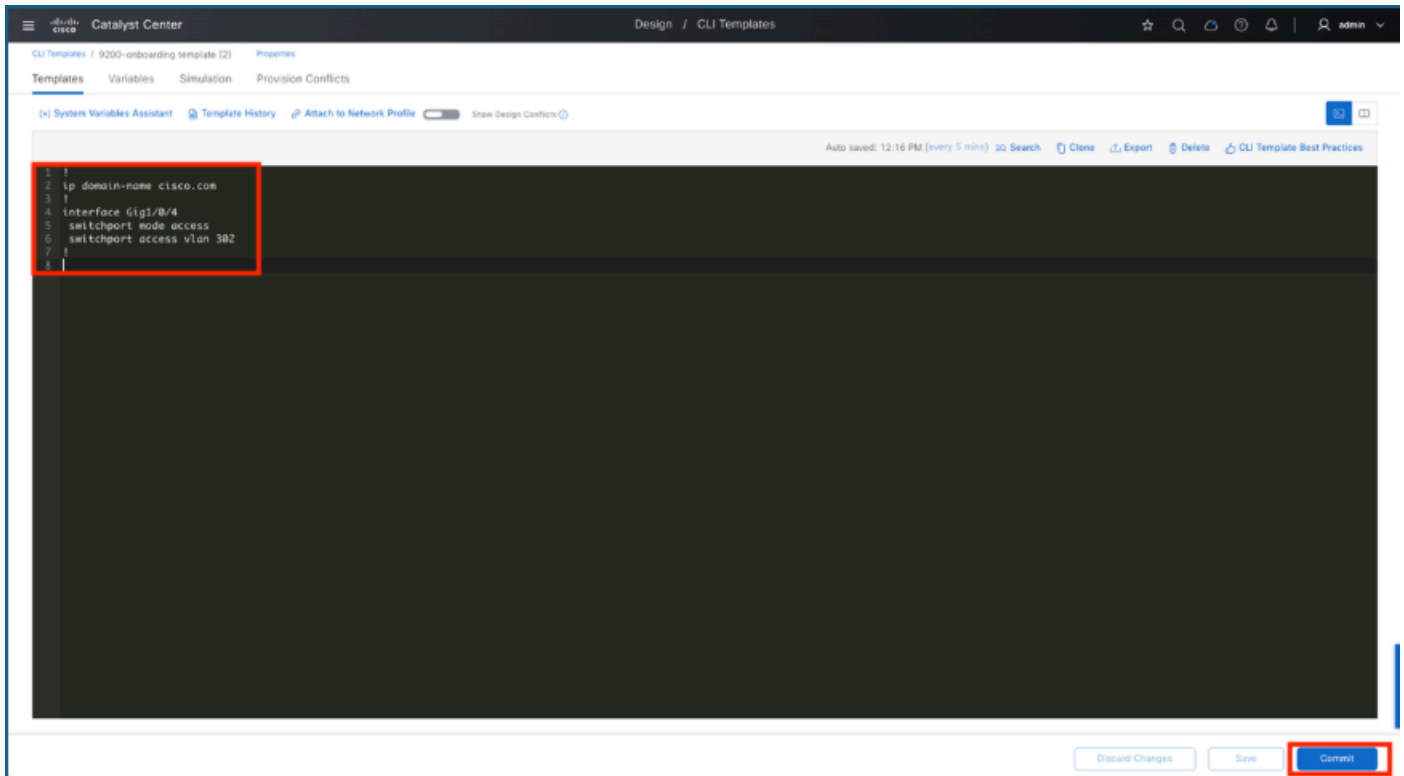
The screenshot shows the Cisco Catalyst Center interface for managing CLI Templates. The main panel displays a list of 29 templates with columns for Name, Project, Type, and Version. The 'Add New Template' dialog box is open on the right, with a red border highlighting its fields. The dialog contains the following information:

- Template Name***: 9200-onboarding template
- Project Name***: Onboarding Configuration
- Template Type**: Regular Template, Composite Sequence
- Template Language**: JINJA, VELOCITY
- Software Type***: IOS-XE
- Device Type Details**:
 - DEVICE DETAILS***: [Edit Device Details](#)
 - Device Family**: Switches and Hubs
 - Devices**: Cisco Catalyst 9200 Series Switches
- Additional Details**:
 - Device Tags**: Device Tags
 - Software Version**: [Empty field]
 - Template Description**: [Empty text area]

At the bottom of the dialog, there are 'Cancel' and 'Continue' buttons, with the 'Continue' button highlighted by a red box.

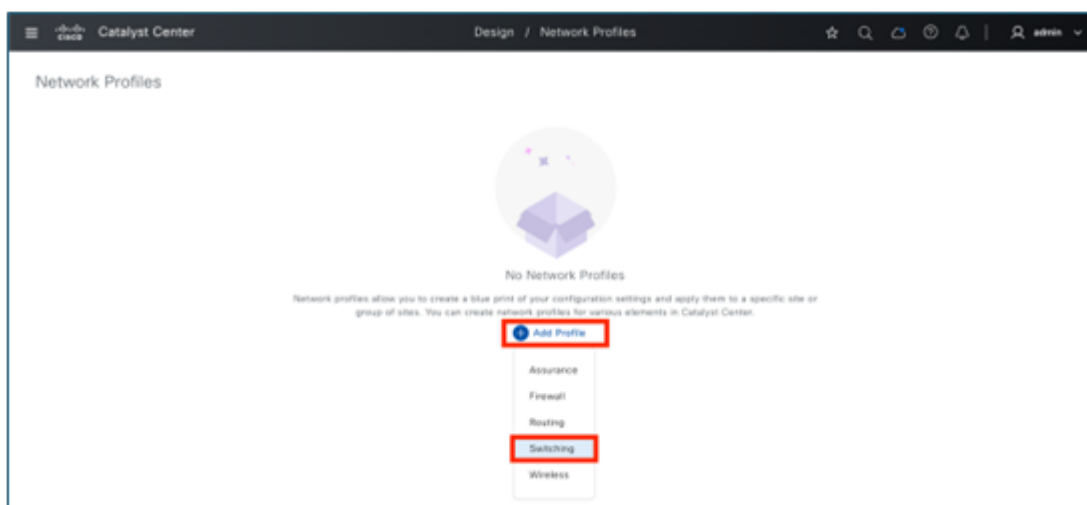
3. Modifier le modèle

Entrez la configuration à déployer sur le commutateur dans l'Éditeur de modèle CLI. Dans cet exemple, un nom de domaine et un port d'accès sont configurés. Après avoir ajouté la configuration à l'Éditeur de modèle CLI, cliquez sur Enregistrer, puis sur Valider pour finaliser les modifications.



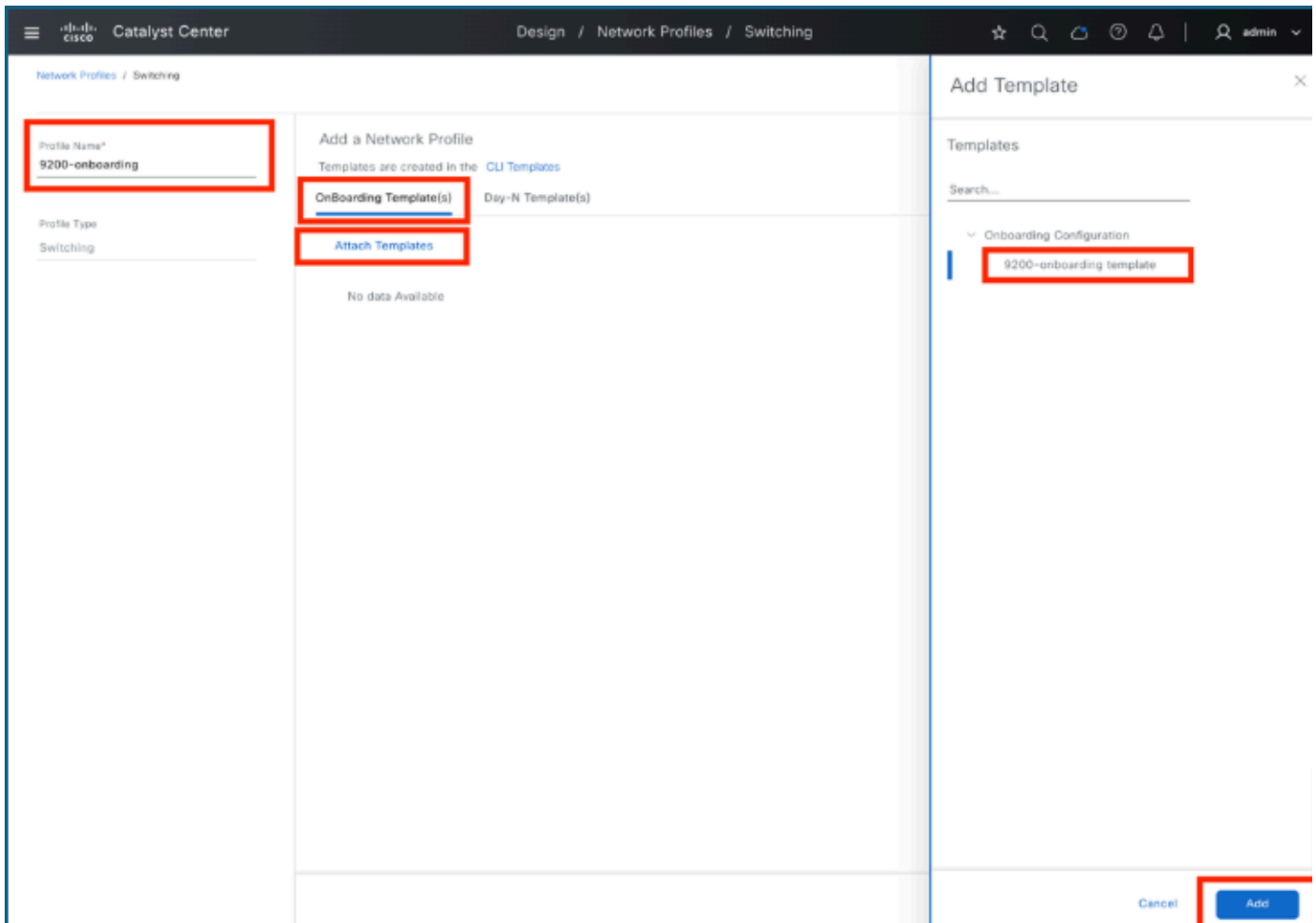
4. Créer un profil réseau

- Accédez au menu Design et sélectionnez Network Profiles.
- Cliquez sur le bouton Add Profile.
- Choisissez le type de profil approprié dans la liste (par exemple, Commutation).



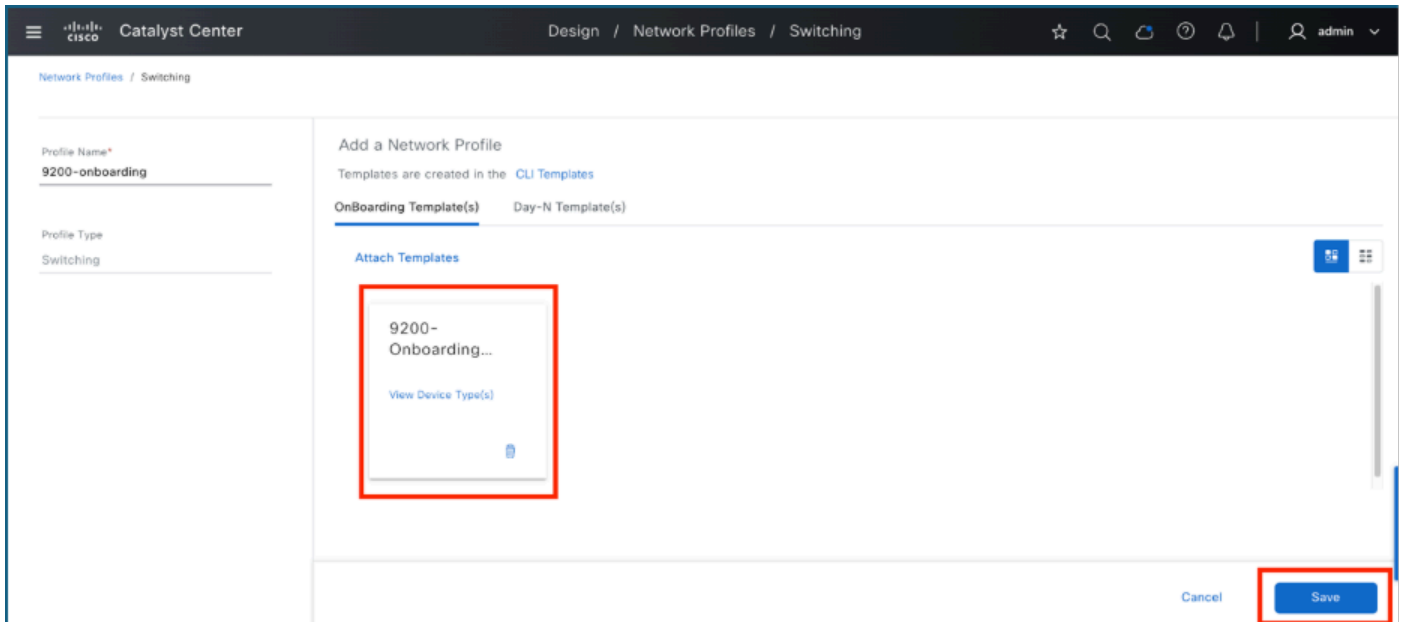
5. Ajoutez un modèle et modifiez les paramètres du profil réseau

- Enter a Profile Name : saisissez un nom pour le profil réseau.
- Access Templates : cliquez sur Onboarding Template(s) et sélectionnez Attach Templates.
- Choisissez Modèle : Localisez et sélectionnez le modèle requis dans le répertoire Onboarding Configuration.
- Finalize : cliquez sur le bouton Add pour terminer le processus.



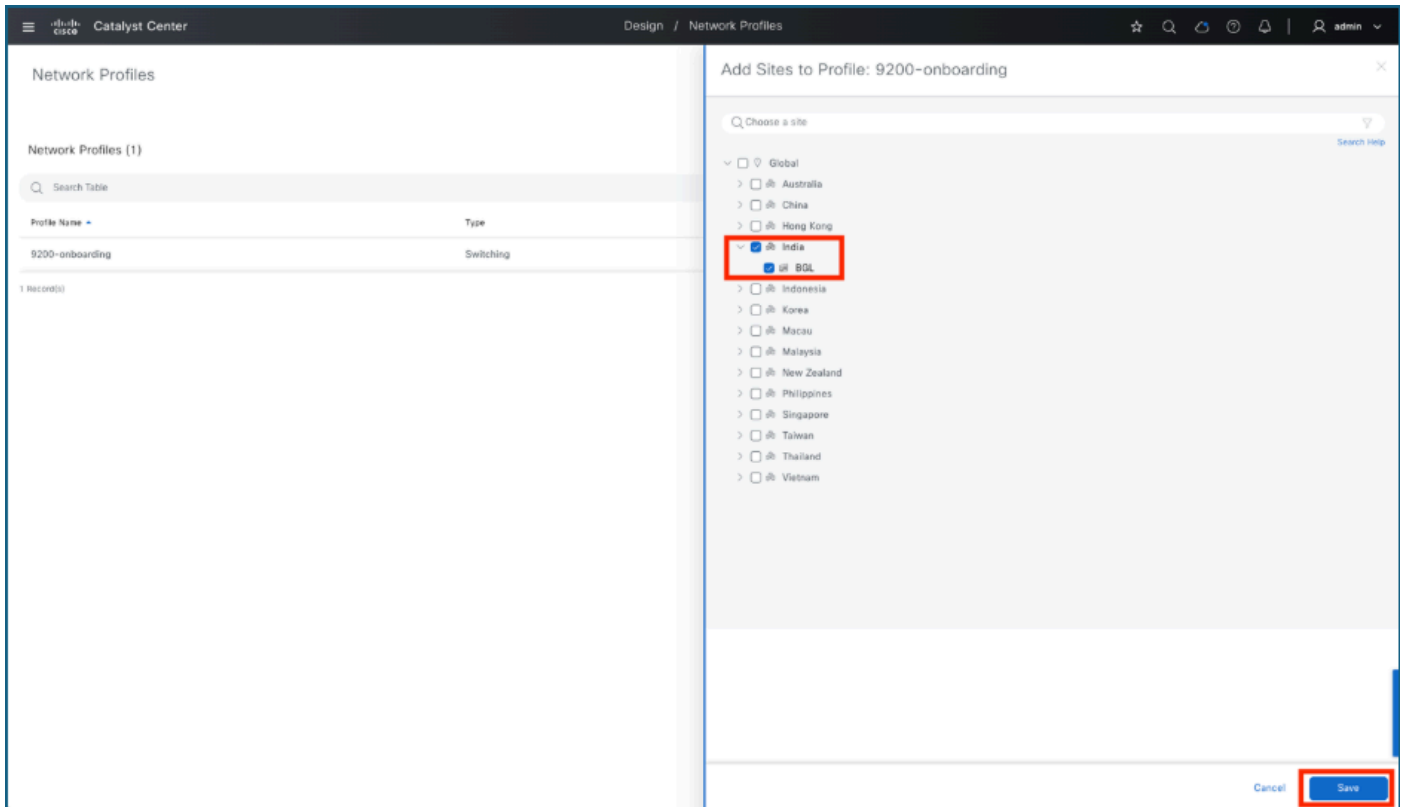
6. Enregistrez le profil

- Vérifier le modèle : après avoir ajouté le modèle, assurez-vous qu'il apparaît dans la liste sous Modèles d'intégration.
- Save Profile: Cliquez sur le bouton Save pour finaliser et stocker les paramètres de profil.



7. Attribuez un profil de réseau au site où les commutateurs/commutateurs doivent être intégrés

- Initiate Assignment : cliquez sur l'option Assign Site pour le profil réseau qui vient d'être créé.
- Choisir le site : sélectionnez le site spécifique où les commutateurs doivent être intégrés.
- Confirmer : cliquez sur Enregistrer pour finaliser l'affectation.



8. Commutateurs de demande

- Accédez au menu Plug-and-Play : Accédez au provisionnement et sélectionnez Plug-and-Play.
- Select Devices : localisez le ou les commutateurs à réclamer et cochez la case en regard du nom de chaque commutateur.
- Lancer la demande : accédez au menu Actions et sélectionnez Demande.

Catalyst Center Provision / Network Devices / Plug and Play

> Network Plug and Play Overview

Device Status: All (1) Unclaimed (1) Error (0) Provisioned (0)

Devices (1) Focus: Default Auto-refresh: 30 s

Search PnP devices

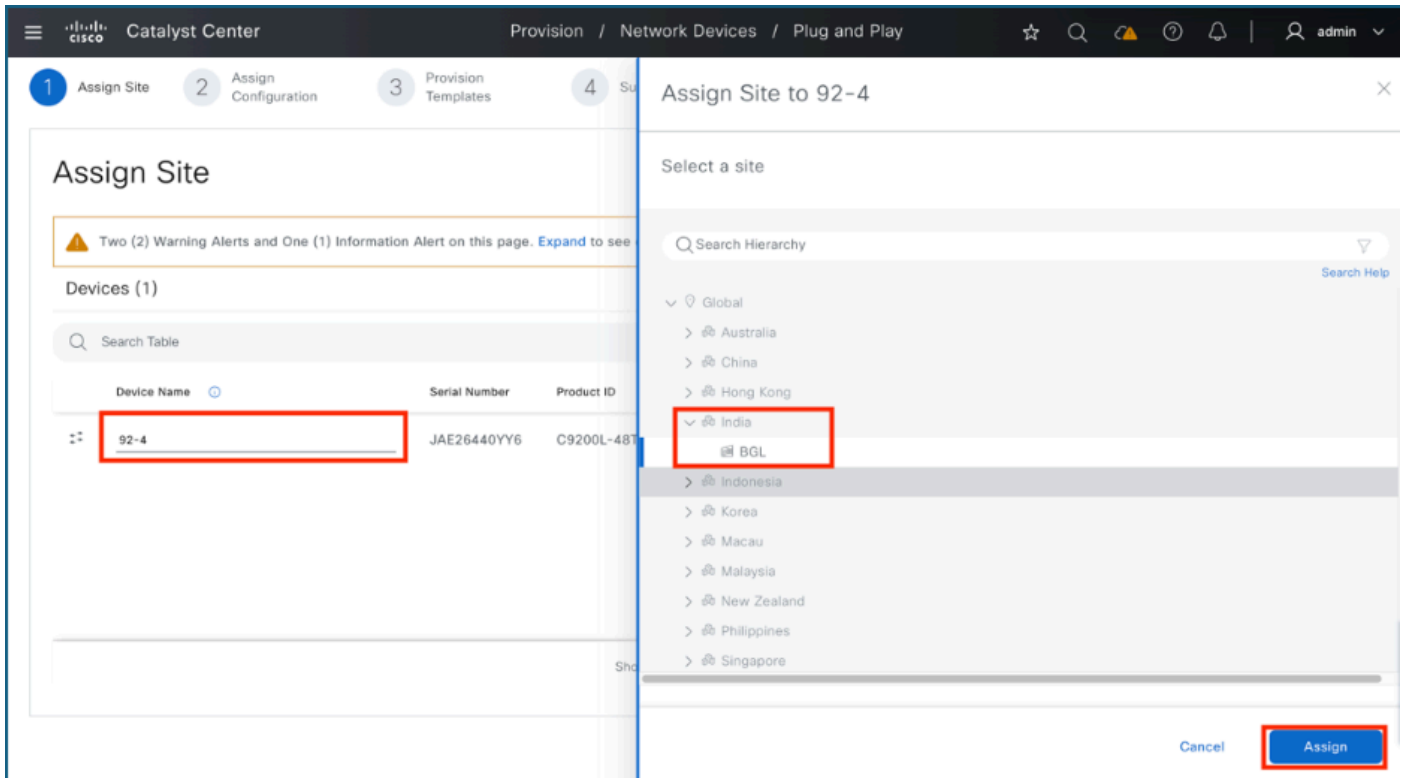
1 Selected Actions Add Devices As of: Jan 5, 2026 9:04 PM Refresh

#	Name	Serial Number	Product ID	Last Contact	State	Onboarding Progress	IP Address	MAC Address
1		JAE26440YY6	C9200L-48T-4G	Jan 05, 2026 9:04:07 PM	Unclaimed	Device is ready to be claimed.	10.127.212.254	NA

Actions menu: Claim, Edit, Reset, Delete, Authorize

9. Attribuez un nom au commutateur et affectez-le à un site

- Name the Device : saisissez le nom souhaité pour le commutateur dans le champ Device Name.
- Lancer l'affectation : cliquez sur le bouton Affecter.
- Sélectionnez l'emplacement : choisissez le site ou le bâtiment approprié, cliquez à nouveau sur Attribuer, puis cliquez sur Suivant pour continuer.



10. Affecter un modèle Jour-0

- Sélectionnez le modèle : cliquez sur le modèle qui a été automatiquement sélectionné en regard de l'option Modèle.
- Vérifier les détails : vérifiez soigneusement les détails de configuration du modèle affecté.
- Continuer : après avoir confirmé l'affectation du modèle, cliquez sur Suivant.

Catalyst Center Provision / Network Devices / Plug and Play

Assign Site 2 Assign Configuration 3 Provision Templates 4 Summary

Assign Configuration

Devices (1) Clear Configuration

Search Table

Device Name	Serial Number	Product ID	Assigned Site	Configuration	Actions
92-4	JAE26440YY6	C9200L-48T-4G	Global/India/BGL	Image: Assign Template: 9200-onboarding temp...ing	...

Showing 1 of 1

Cancel Back Next

Catalyst Center Provision / Network Devices / Plug and Play

Assign Site 2 Assign Configuration 3 Provision Templates 4 Summary

Assign Configuration

Devices (1) Configuration for device name: 92-4

Search Table

Device Name	Serial Number	Product ID
92-4	JAE26440YY6	C9200L-48T-4G

Serial Number: JAE26440YY6 Product ID: C9200L-48T-4G

IP Address: 10.127.212.253 Device Family: Switches and Hubs

Assigned Site: Global/India/BGL Device Series: Cisco Catalyst 9200 Series Switches

Device Name: 92-4 Device Type: Cisco Catalyst 9200L Switch Stack

Template

Select a Template (Optional)

9200-onboarding template (Switching) ✕

Ex: Template Name (Profile Type)

Copy running configuration to startup configuration

Template: 9200-onboarding template

Project: Onboarding Configuration

Created: Jan 04, 2026 11:44:04 AM

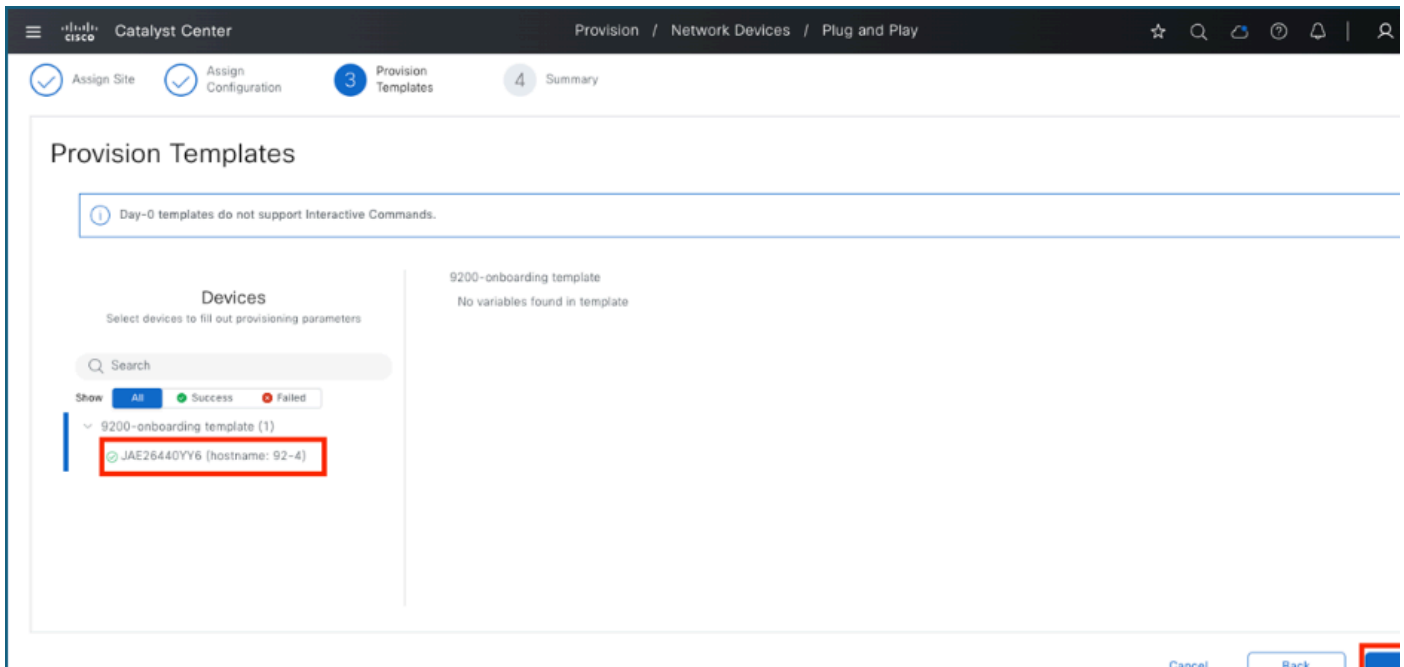
Updated: Jan 04, 2026 12:16:51 PM

Cancel Save

11. Modèles de provisionnement

- Select Device : sous la section template, cliquez sur le périphérique spécifique que vous configurez.

- Identifier les variables : recherchez les valeurs de variable requises associées au modèle.
- Saisissez des valeurs : si des variables sont obligatoires, saisissez les valeurs nécessaires.
- Continuer : cliquez sur Suivant pour passer à l'étape suivante.



12. Résumé

- Vérifier la configuration : sur la page Résumé, vérifiez les paramètres de configuration préparés par Catalyst Center.
- Preview Details : cliquez sur Preview Configuration pour afficher les modifications en attente.
- Verify Sections : développez chaque section pour examiner les détails de configuration spécifiques.
- Finalize : une fois que vous avez vérifié les paramètres, cliquez sur Claim pour continuer.

Catalyst Center Provision / Network Devices / Plug and Play

Assign Site Assign Configuration Provision Templates **4 Summary**

Summary

Devices (1)

Search Table

Device Name	Serial Number	Product ID	Assigned Site	Configuration	Device Configuration
92-4	JAE26440YY6	C9200L-48T-4G	Global/India/BGL	Image: No image selected Template: 9200-onboarding temp...ing)	Preview Configuration

Showing 1 of 1

Cancel Back **Claim**

Catalyst Center Provision / Network Devices / Plug and Play

Assign Site Assign Configuration Provision Templates **4 Summary**

Summary

Devices (1)

Search Table

Device Name	Serial Number	Product ID
92-4	JAE26440YY6	C9200L-48T-4G

Showing 1 of 1

CLI User Password *****

Enable Password *****

NETCONF Port 830

SNMPV2C Read Community *****

> Device Details

> Image Details

> Template CLI Preview

Running configuration will be copied to startup configuration.

[Export](#) [Copy](#)

```
1 !
2 ip domain-name cisco.com
3 !
4 interface Gig1/0/4
5 switchport mode access
6 switchport access vlan 302
7 !
```

> Network Settings

> Day-0 CLI Configuration Preview

13. Suivre l'avancement des demandes

Vous êtes redirigé vers la page Plug and Play pour suivre la progression du périphérique.

- État de surveillance : observez l'état du périphérique au fur et à mesure du processus de demande.
- Confirmation de la fin : lorsque l'état est mis à jour vers Provisioned, le commutateur a été correctement revendiqué et intégré dans l'inventaire Catalyst Center.

The screenshot shows the Catalyst Center interface for Network Plug and Play. The 'Device Status' bar indicates 1 All, 0 Unclaimed, 0 Error, and 0 Provisioned. The 'Devices (1)' section shows a table with one device in the 'Onboarding' state, with the 'Onboarding Progress' column showing 'Executing Workflow'.

#	Device Name	Serial Number	Product ID	Last Contact	State	Onboarding Progress	IP Address	MAC Address
1	92-4	JAE26440YY6	C9200L-48T-4G	Jan 05, 2026 11:27:06 PM	Onboarding	Executing Workflow	10.127.212.253	NA

The screenshot shows the Catalyst Center interface after the device has been provisioned. The 'Device Status' bar now indicates 1 All, 0 Unclaimed, 0 Error, and 1 Provisioned. The 'Devices (1)' section shows the same device in the 'Provisioned' state, with the 'Onboarding Progress' column showing 'Provisioned'.

#	Device Name	Serial Number	Product ID	Last Contact	State	Onboarding Progress	IP Address	MAC Address
1	92-4	JAE26440YY6	C9200L-48T-4G	Jan 05, 2026 11:27:14 PM	Provisioned	Provisioned	10.127.212.253	NA

Vérification

- Accédez au menu Provisionner : ouvrez l'onglet Provisionner de la page principale.
- Voir le stock : sélectionnez l'option Stock.
- Verify Status : vérifiez la liste pour vous assurer que les commutateurs ont été correctement

provisionnés.

The screenshot displays the Cisco Catalyst Center interface for device inventory. A table lists three devices:

Tags	Device Name	IP Address	Vendor	Reachability	EoX Status	Manageability	Compliance
	92-2.cisco.com	10.127.212.49	Cisco	Reachable	Not Scanned	Managed Missing Enable Password	Compliant
	92-4.cisco.com	10.127.212.253	Cisco	Reachable	Not Scanned	Managed Netconf Connection Failure	Compliant
	CAT9200-1	10.127.212.47	Cisco	Unreachable	Not Scanned	Managed Device Unreachable	Compliant

Importation en masse de périphériques dans l'inventaire Plug-and-Play de Catalyst Center

Pour rationaliser les déploiements de grands réseaux, Catalyst Center prend en charge une méthode d'importation en masse pour les périphériques de transfert à l'avance. Ce processus implique le téléchargement d'identifiants de périphériques tels que les PID, les numéros de série et les données facultatives de site ou de modèle, ce qui permet au système d'intégrer automatiquement les périphériques dès qu'ils sont mis sous tension et connectés.

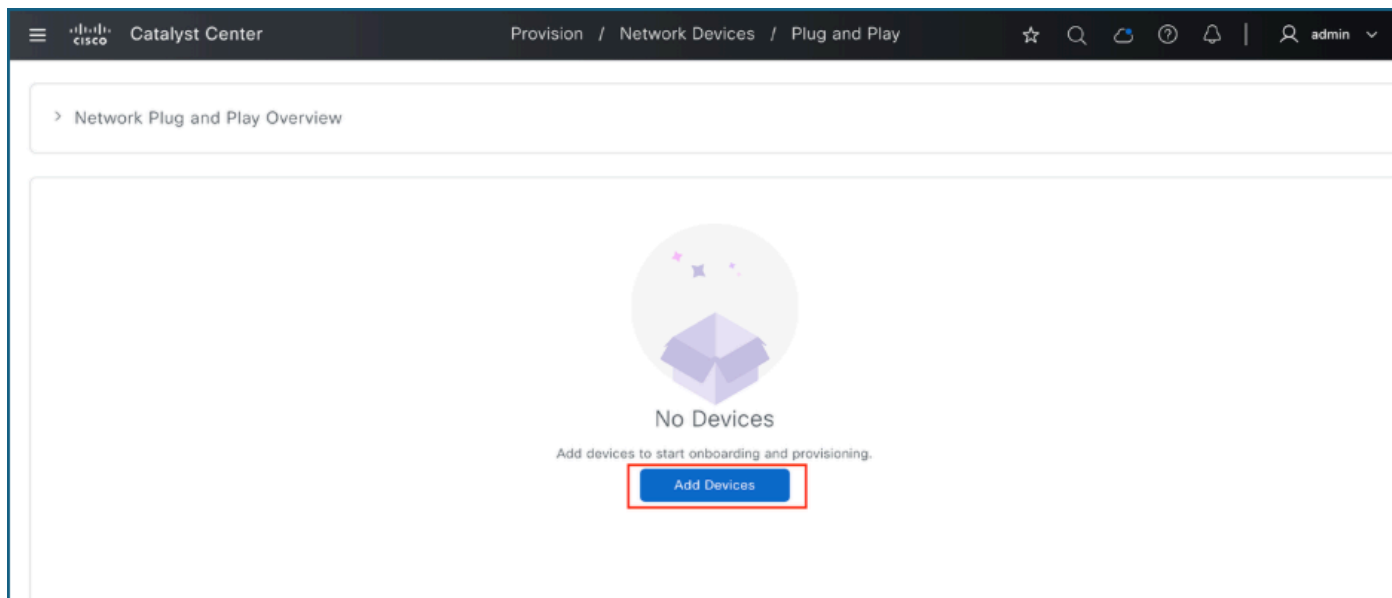
1. Conditions préalables

Pour assurer la réussite de l'importation en vrac, les exigences suivantes doivent être respectées :

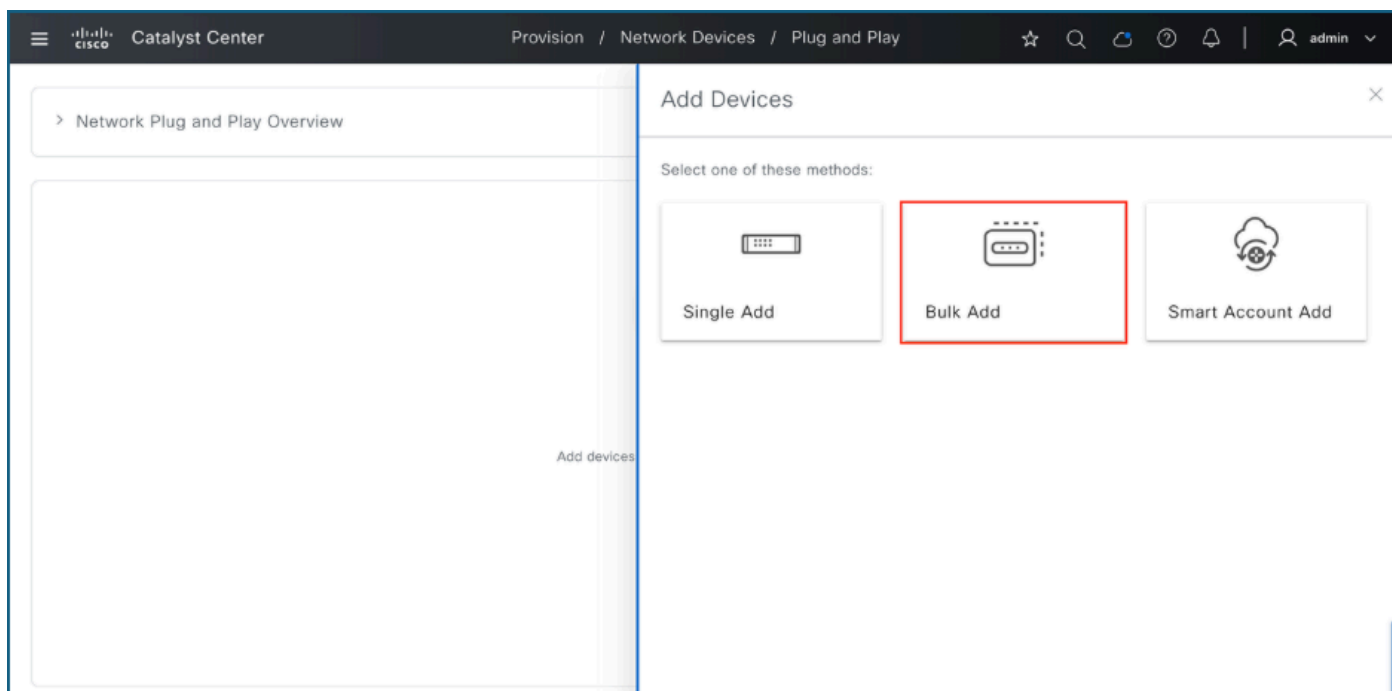
- L'instance de Catalyst Center doit être accessible et opérationnelle.
- Le matériel doit être officiellement pris en charge par le service Cisco Plug and Play.
- Les numéros de série et les PID des périphériques doivent être accessibles.
- Les hiérarchies de sites cibles doivent être préconfigurées dans l'environnement Catalyst Center.

2. Procédure d'importation en vrac

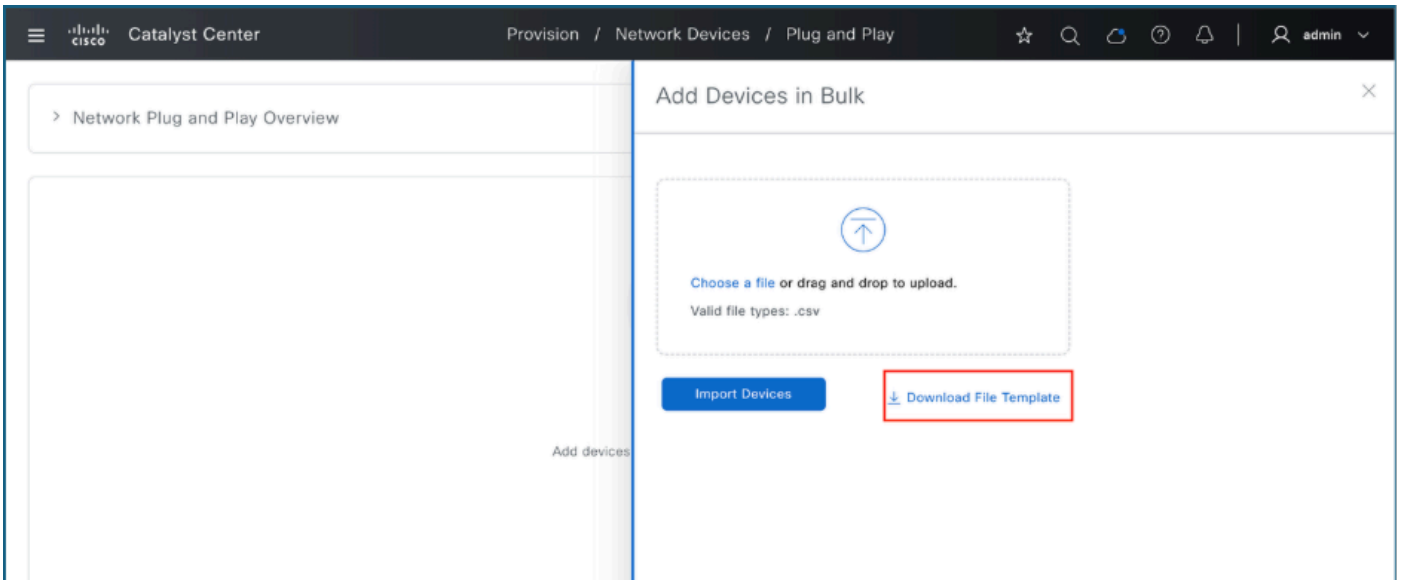
1. Connectez-vous à Catalyst Center
2. Accédez à Provisionner > Plug and Play
3. Cliquez sur Add Devices



4. Cliquez sur Bulk Add



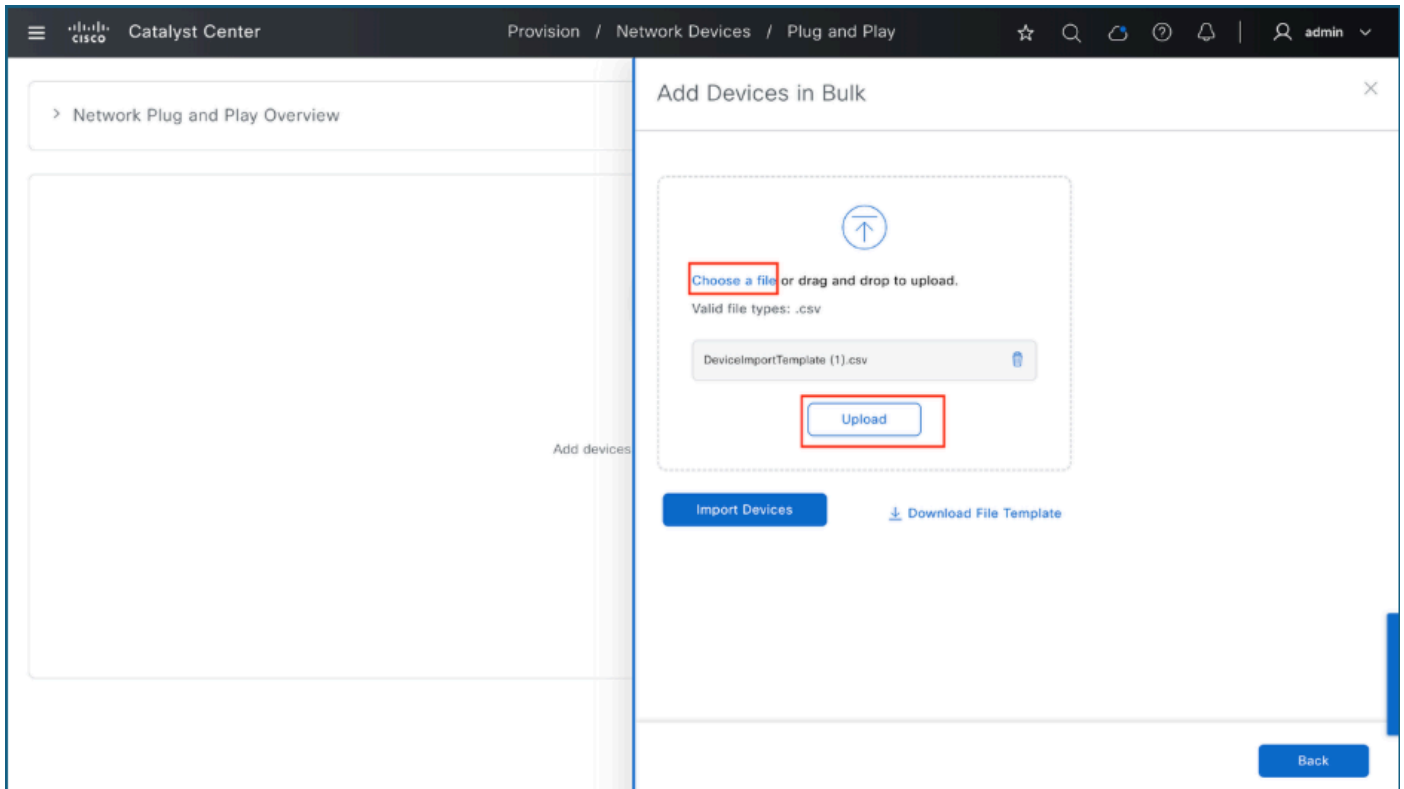
5. Cliquez sur Download File Template pour télécharger l'exemple de fichier CSV



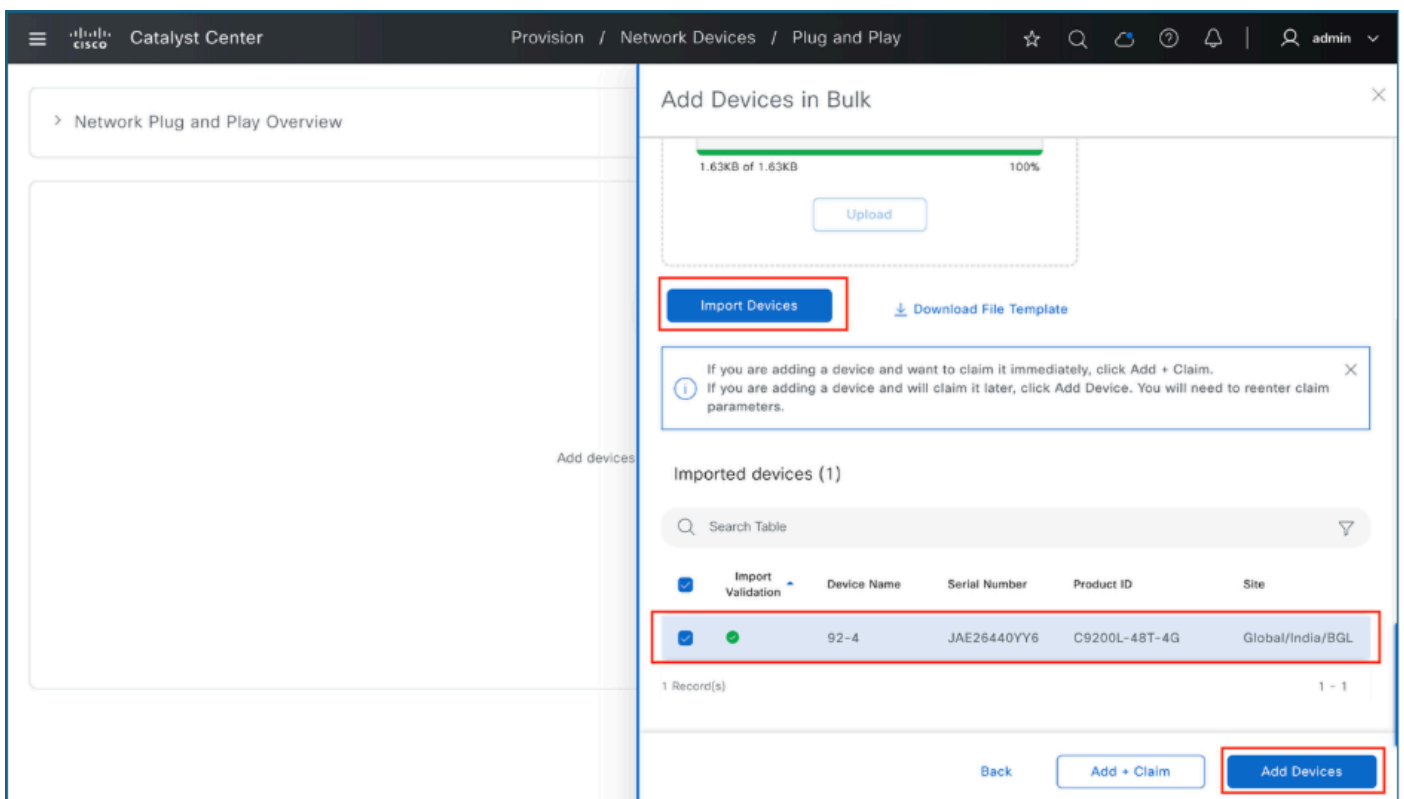
6. Remplissez le fichier CSV avec les détails de périphérique requis.

	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 recommended. 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>/<floor name>										
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 Access (Leave blank for A (Leave blank for Access Points)						
18											
19	JAE26440YY6	C9200L-48T-4G	92-4	Global/India/BGL							
20											

7. Téléchargez le fichier CSV terminé.



8. Importez les périphériques à partir du fichier CSV et ajoutez-les à l'inventaire Plug and Play



9. Les périphériques apparaissent dans l'inventaire comme Non contactés.

The screenshot shows the Catalyst Center interface for Network Plug and Play. The top navigation bar includes the Cisco logo, 'Catalyst Center', and the path 'Provision / Network Devices / Plug and Play'. The main content area is titled 'Network Plug and Play Overview'. Below this, there are filters for 'Device Status' (All (1), Unclaimed (1), Error (0), Provisioned (0)) and 'Devices (1)'. A search bar is present. The table below shows one device with the following details:

#	Device Name	Serial Number	Product ID	Last Contact	State	Onboarding Progress	IP Address	MAC Address	Source
1	92-4	JAE26440YY6	C9200L-48T-4G	Not Contacted	Unclaimed	Device is ready to be claimed.	NA	NA	User

10. Une fois que le périphérique a contacté Catalyst Center, il est prêt à être réclamé.

The screenshot shows the Catalyst Center interface for Network Plug and Play. The top navigation bar includes the Cisco logo, 'Catalyst Center', and the path 'Provision / Network Devices / Plug and Play'. The main content area is titled 'Network Plug and Play Overview'. Below this, there are filters for 'Device Status' (All (1), Unclaimed (1), Error (0), Provisioned (0)) and 'Devices (1)'. A search bar is present. The table below shows one device with the following details:

#	Device Name	Serial Number	Product ID	Last Contact	State	Onboarding Progress	IP Address	MAC Address
1	92-4	JAE26440YY6	C9200L-48T-4G	Jan 06, 2026 5:57:31 PM	Unclaimed	Device is ready to be claimed.	10.127.212.253	NA

Dépannage

Si le commutateur n'apparaît pas sur la page Plug and Play de Catalyst Center, voici les étapes à suivre pour identifier et résoudre le problème.

1. Validation de la connectivité PnP

Ces commandes valident la connectivité Plug-and-Play à Catalyst Center.

1.1. Accessibilité ICMP

Vérifiez la connectivité ICMP en envoyant une requête ping à l'adresse IP de l'interface d'entreprise ou à l'adresse IP virtuelle (VIP) de Catalyst Center. Assurez-vous que Catalyst Center est accessible 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. Validation HTTP HELLO

Plug and Play (PnP) échoue si Catalyst Center ne répond pas aux demandes de validation HELLO. Pour vérifier la connectivité, exécutez cette commande à partir d'un terminal de périphérique ou d'une invite de commande : `curl -v http://<Catalyst Center IP>/pnp/HELLO`

Confirmez la réception d'une réponse « HELLO ».

```
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. Récupération de certificat HTTPS

La fonctionnalité Plug and Play échoue si le certificat du serveur Catalyst Center ne peut pas être récupéré manuellement via HTTPS. Pour le vérifier, utilisez cette commande : `copy https://<catc-ip-address>/ca/pem mypem2`

Vérifiez que le transfert de fichiers s'effectue sans erreurs.

```
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. État du profil PnP

Si un commutateur n'apparaît pas sur la page PnP de Catalyst Center, examinez la connectivité HTTP PnP en exécutant la commande `show pnp profile`

- Vérifiez que Plug-and-Play utilise l'URL active correcte.
- Vérifiez que « Failed Counters » dans les statistiques HTTP est 0. Une valeur supérieure à 0 indique des problèmes d'accessibilité entre le commutateur et Catalyst Center. Cette image illustre un scénario impliquant des problèmes d'accessibilité.

```
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-Procl, Last-Name=[PnP-Discovery-Procl
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#
```

Cet exemple illustre un scénario sans problème d'accessibilité.

```

PnP-T1-Discovery: Active-Name=[PnP-Discovery-Proc], Last-Name=[-]
Active-URL=[http://catcl.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=48881114
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://catcl.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=48881570
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. Validation DHCP

Ces commandes permettent de valider la configuration et la connectivité DHCP.

2.1. Vérification de l'attribution des adresses IP DHCP

Exécutez la commande : `show ip interface brief`, pour vérifier que l'interface SVI du VLAN Plug and Play a reçu une adresse IP du serveur DHCP.

```

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. Confirmer le serveur de location

Exécutez la commande `show dhcp lease` pour vérifier les informations du serveur de bail DHCP.

```
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-V1302
  Client-ID hex dump: 636973636F2D343436342E336362312E
                       326266372D566C333032
  Hostname: Switch
```

2.3. Valider l'option 43 à l'aide des journaux de débogage

Pour valider l'option 43, activez le débogage DHCP avec la commande `debug dhcp detail`. Après avoir activé le débogage, exécutez un `shutdown` et `no shutdown` sur l'interface pour redémarrer le processus DHCP. Dans les journaux, localisez la section « DHCP : Analyse : Option spécifique au constructeur 43 : ». Copiez la chaîne hexadécimale comme indiqué dans cette section, convertissez-la en texte à l'aide d'un convertisseur hexadécimal-ASCII approprié, et vérifiez que la chaîne résultante pointe correctement vers Catalyst Center.

```

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: 3541314E3B42323B48343B4931302E3132372E3231322E34333B4A38303B
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: DHCP: 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

```

Meilleures pratiques

- Assurez-vous que le commutateur est dans son état par défaut. S'il a déjà été provisionné, utilisez la commande `npa service reset` pour le réinitialiser.
- Évitez d'interrompre le processus Plug and Play via la console.
- Vérifiez les certificats et la résolution DNS avant le déploiement.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.