

# Configuration du BYOD ISE avec SSID simple et double dans ISE 3.3

## Table des matières

---

[Introduction](#)

[Fond](#)

[Conditions préalables](#)

[Composant utilisé](#)

[Qu'est-ce que le BYOD avec SSID unique et SSID double sur ISE ?](#)

[SSID unique BYOD](#)

[BYOD à double SSID](#)

[Configuration WLC](#)

[Créer un WLAN pour CWA](#)

[Configuration des serveurs RADIUS](#)

[Configuration des serveurs AAA](#)

[Configuration des stratégies de sécurité pour le WLAN](#)

[Configurer une liste de contrôle d'accès pré-authentification](#)

[Configurer le profil de stratégie](#)

[Appliquer les balises et déployer](#)

[Configurer un SSID ouvert/non sécurisé](#)

[Configuration ISE](#)

[Conditions préalables](#)

[Certificats](#)

[Configuration DNS](#)

[Configuration du périphérique réseau ISE](#)

[Créer un portail BYOD](#)

[Télécharger la dernière version de Cisco IOS®](#)

[Créer un profil de terminal](#)

[Modèle de certificat](#)

[Mappage d'un profil de point de terminaison au portail d'approvisionnement client](#)

[Configuration des ensembles de stratégies ISE pour le BYOD avec un seul SSID](#)

[Configuration des ensembles de stratégies ISE pour le BYOD à double SSID](#)

[Dépannage](#)

[Extrait de journal](#)

[Journaux invités](#)

[Journaux Ise-Psc](#)

[Téléchargement du profil de terminal](#)

---

## Introduction

Le document décrit comment configurer et dépanner les problèmes liés au BYOD sur ISE.

## Fond

Le BYOD est une fonctionnalité qui permet à l'utilisateur d'intégrer ses appareils personnels sur ISE afin de pouvoir utiliser les ressources réseau de l'environnement. Il aide également l'administrateur réseau à empêcher l'utilisateur d'accéder à la ressource critique à partir des périphériques personnels.

Contrairement au flux invité, où le périphérique est authentifié avec la page Invité à l'aide du magasin interne ou d'Active Directory sur ISE. Le BYOD permet à l'administrateur réseau d'installer un profil de point de terminaison sur le point de terminaison pour choisir le type de méthode EAP. Dans des scénarios comme EAP-TLS, le certificat client est signé par l'ISE lui-même pour créer une confiance entre le point d'extrémité et l'ISE.

## Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- contrôleur WLC
- Connaissances de base sur ISE

## Composant utilisé

Les périphériques utilisés ne sont pas limités à une version particulière du flux BYOD :

- Contrôleur sans fil Catalyst 9800-CL (17.12.3)
- Machine virtuelle ISE (3.3)

## Qu'est-ce que le BYOD avec SSID unique et SSID double sur ISE ?

### SSID unique BYOD

Dans une configuration BYOD à SSID unique, les utilisateurs connectent leurs périphériques personnels directement au réseau sans fil de l'entreprise. Le processus d'intégration se déroule sur le même SSID, où ISE facilite l'enregistrement, le provisionnement et l'application des politiques des périphériques. Cette approche simplifie l'expérience utilisateur, mais nécessite une intégration sécurisée et des méthodes d'authentification appropriées pour garantir la sécurité du réseau.

### BYOD à double SSID

Dans une configuration BYOD à double SSID, deux SSID distincts sont utilisés : une pour l'intégration (accès non sécurisé ou restreint) et une autre pour l'accès au réseau d'entreprise. Les utilisateurs se connectent d'abord au SSID d'intégration, effectuent l'enregistrement et le provisionnement des périphériques via ISE, puis basculent vers le SSID d'entreprise sécurisé pour accéder au réseau. Cela permet d'obtenir une couche de sécurité supplémentaire en séparant le trafic d'intégration du trafic de production.

## Configuration WLC

### Créer un WLAN pour CWA

1. Accédez à Configuration > Tags & Profiles > WLANs.
2. Cliquez sur Add pour créer un nouveau WLAN.
  - Définissez un nom WLAN et un SSID (par exemple, BYOD-WiFi).
  - Activez le WLAN.

#### Add WLAN

General Security Advanced

Profile Name\*

SSID\*

WLAN ID\*

Status ENABLED

Broadcast SSID ENABLED

Radio Policy ⓘ

[Show slot configuration](#)

6 GHz  
Status ENABLED  ⓘ  
✖ WPA3 Enabled  
✔ Dot11ax Enabled

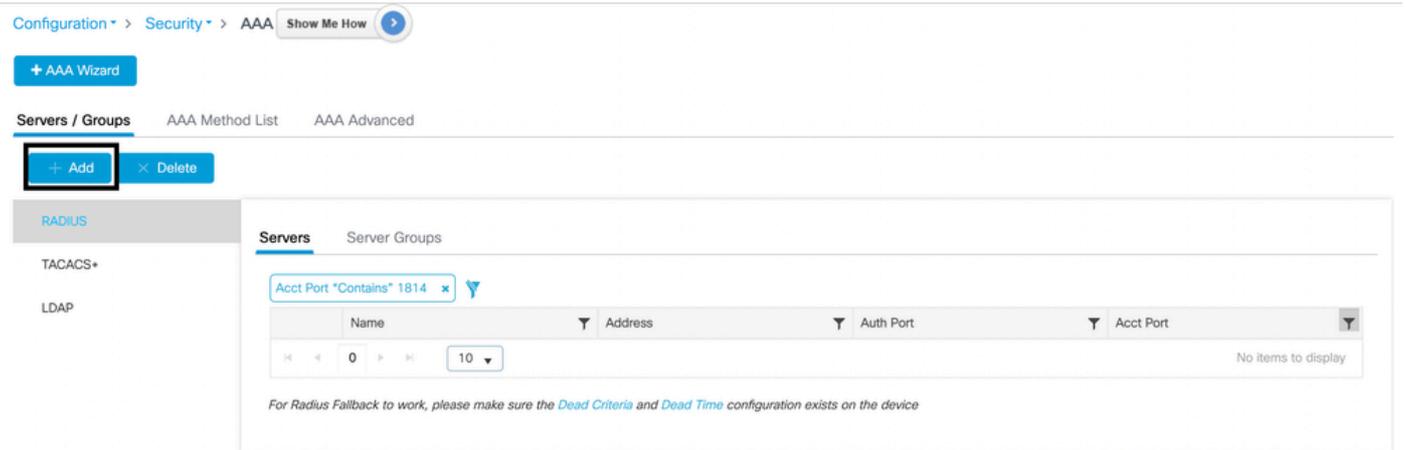
5 GHz  
Status ENABLED

2.4 GHz  
Status ENABLED

802.11b/g Policy

### Configuration des serveurs RADIUS

## 1. Accédez à Configuration > Security > AAA > RADIUS > Servers.



## 2. Cliquez sur Add pour configurer ISE en tant que serveur RADIUS :

- Adresse IP du serveur : Adresse IP d'ISE.
- Secret partagé : Associez les secrets partagés configurés sur ISE.

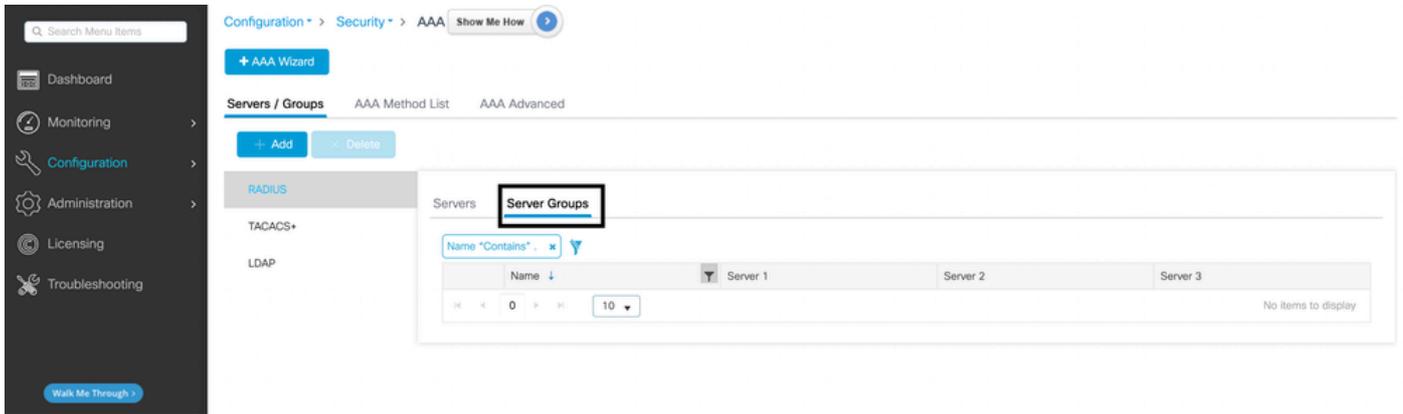
The 'Create AAA Radius Server' dialog is shown. It contains the following fields and options:

- Name\*: BYOD
- Server Address\*: 10.x.x.x (highlighted with a black box)
- PAC Key:
- Key Type: Clear Text
- Key\*: ..... (highlighted with a black box)
- Confirm Key\*: .....
- Auth Port: 1812
- Acct Port: 1813
- Server Timeout (seconds): 1-1000
- Retry Count: 0-100
- Support for CoA:  ENABLED
- CoA Server Key Type: Clear Text
- CoA Server Key: .....
- Confirm CoA Server Key: .....
- Automate Tester:

Buttons: Cancel, Apply to Device

## Configuration des serveurs AAA

### 1. Accédez à Configuration > Security > AAA > Servers/Groups.



2. Attribuez le serveur RADIUS à un groupe de serveurs nouveau ou existant.

### Create AAA Radius Server Group

Name\* **BYOD**

Group Type RADIUS

MAC-Delimiter none

MAC-Filtering none

Dead-Time (mins) 5

Load Balance  DISABLED

Source Interface VLAN ID 1

Available Servers

Assigned Servers **BYOD**

Cancel [Apply to Device](#)

## Configuration des stratégies de sécurité pour le WLAN

1. Accédez à Configuration > Tags & Profiles > WLANs. Modifiez le WLAN créé précédemment.
2. Sous l'onglet Security > Layer 2 :
  - Activer WPA+WPA2
  - Définissez AES(CCMP128) sous Cryptage WPA2
  - Gestion des clés d'authentification 802.1X

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

**Layer2** Layer3 AAA

WPA + WPA2  WPA2 + WPA3  WPA3  Static WEP  None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy  WPA2 Policy   
 GTK Randomize  OSEN Policy

WPA2 Encryption

AES(CCMP128)  CCMP256   
 GCMP128  GCMP256

Protected Management Frame

PMF

Fast Transition

Status   
 Over the DS   
 Reassociation Timeout \*

Auth Key Mgmt

802.1X <input checked="" type="checkbox"/>	PSK <input type="checkbox"/>
Easy-PSK <input type="checkbox"/>	CCKM ⚠ <input type="checkbox"/>
FT + 802.1X <input type="checkbox"/>	FT + PSK <input type="checkbox"/>
802.1X-SHA256 <input type="checkbox"/>	PSK-SHA256 <input type="checkbox"/>

MPSK Configuration

↶ Cancel

📁 Update & Apply to Device

3. Sous l'onglet Security > Layer 3, sélectionnez global dans la liste déroulante pour Web Auth Parameter Map.

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy



[Show Advanced Settings >>>](#)

Web Auth Parameter Map

global



Authentication List

Select a value



*For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device*

Cancel



Update & Apply to Device

## Configurer une liste de contrôle d'accès pré-authentification

Créez une liste de contrôle d'accès pour autoriser Utiliser les actions de redirection :

- Trafic DNS.
- HTTP/HTTPS vers le portail ISE.
- Tous les services back-end requis.

Pour ce faire :

1. Accédez à Configuration > Security > ACLs > Access Control Lists.
2. Créez une nouvelle liste de contrôle d'accès avec des règles pour autoriser le trafic nécessaire.

### Edit ACL

ACL Name\*  ACL Type

**Rules**

Sequence\*  Action

Source Type

Destination Type

Protocol

Log  DSCP

	Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/>	10	deny	ISE-IP-Address		any		ip	None	None	None	Disabled
<input type="checkbox"/>	20	deny	any		ISE-IP-Address		ip	None	None	None	Disabled
<input type="checkbox"/>	30	deny	any		any		udp	None	eq domain	None	Disabled
<input type="checkbox"/>	40	deny	any		any		udp	eq domain	None	None	Disabled
<input type="checkbox"/>	50	permit	any		any		tcp	None	eq www	None	Disabled

1 - 5 of 5 items

## Configurer le profil de stratégie

1. Accédez à Configuration > Tags & Profiles > Policy. Vous pouvez créer ou utiliser la stratégie par défaut

Configuration > Tags & Profiles > Policy

Description "Contains" default

Admin Status	Associated Policy Tags	Policy Profile Name	Description
<input type="checkbox"/>	<input checked="" type="checkbox"/>	default-policy-profile	default policy profile

1 - 1 of 1 items

2. Attribuez le VLAN approprié sous Access Policies

### Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

**WLAN Local Profiling**

Global State of Device Classification **Disabled** ⓘ

Local Subscriber Policy Name  ⓘ

**VLAN**

VLAN/VLAN Group  ⓘ

Multicast VLAN

**WLAN ACL**

IPv4 ACL  ⓘ

IPv6 ACL  ⓘ

**URL Filters** ⓘ

Pre Auth  ⓘ

Post Auth  ⓘ

3. Activez également Allow AAA Override et l'état NAC sous Advanced de la stratégie.

## Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General Access Policies QOS and AVC Mobility **Advanced**

### WLAN Timeout

Session Timeout (sec)  ⓘ

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

### DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

### AAA Policy

Allow AAA Override

NAC State

Policy Name  ⓘ

Accounting List  ⓘ

Fabric Profile   ⓘ

Link-Local Bridging

mDNS Service Policy  ⓘ  
[Clear](#)

Hotspot Server  ⓘ

### User Defined (Private) Network

Status

Drop Unicast

### DNS Layer Security

DNS Layer Security Parameter Map  ⓘ  
[Clear](#)

Flex DHCP Option for DNS  **ENABLED**

Flex DNS Traffic Redirect  **IGNORE**

### WLAN Flex Policy

VLAN Central Switching

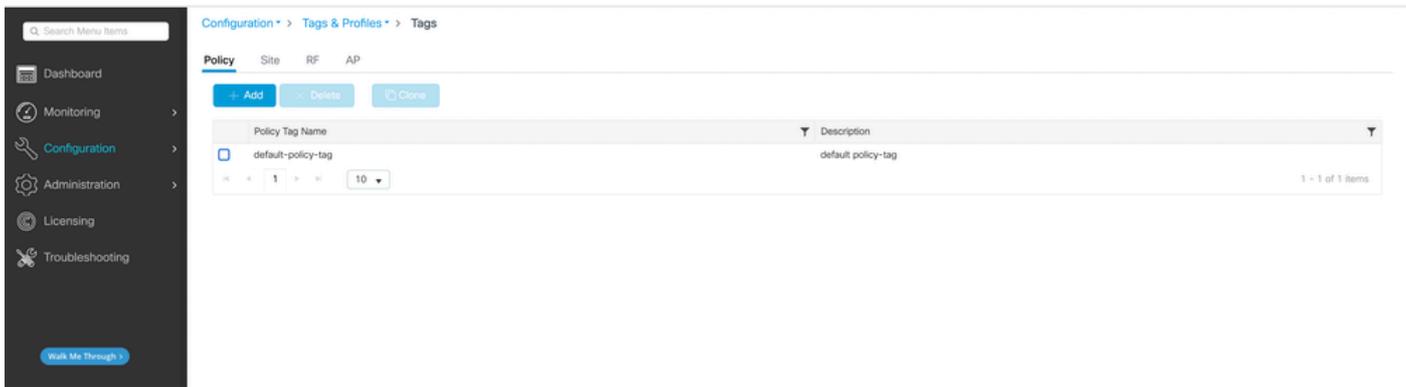
Split MAC ACL  ⓘ

Cancel

Update & Apply to Device

## Appliquer les balises et déployer

- Accédez à Configuration > Tags & Profiles > Tags.
- Créez ou modifiez une balise pour inclure le WLAN et le profil de stratégie.
- Attribuez la balise aux points d'accès.



## Configurer un SSID ouvert/non sécurisé

Le SSID ouvert est créé uniquement lorsque vous décidez d'avoir une configuration BYOD à double SSID sur votre environnement.

1. Accédez à Configuration > Tags & Profiles > WLANs. Cliquez sur le bouton Add.
2. Entrez un nom SSID dans l'onglet General et activez le bouton WLAN.

### Add WLAN

General Security Advanced

Profile Name\* BYOD-Open

SSID\* BYOD-Open

WLAN ID\* 10

Status **ENABLED**

Broadcast SSID **ENABLED**

Radio Policy ⓘ

Show slot configuration

6 GHz  
Status **ENABLED**  ⓘ  
✖ WPA3 Enabled  
✔ Dot11ax Enabled

5 GHz  
Status **ENABLED**

2.4 GHz  
Status **ENABLED**

802.11b/g Policy 802.11b/g ▼

Cancel Apply to Device

3. Cliquez sur l'onglet Sécurité de la même fenêtre. Sélectionnez la case d'option None et activez le filtrage Mac.

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. The 'Layer2' section is highlighted with a black border. In this section, the 'None' radio button is selected, and the 'MAC Filtering' checkbox is checked. Other options like 'WPA + WPA2', 'WPA2 + WPA3', 'WPA3', and 'Static WEP' are unselected. Below the Layer2 section, there are fields for 'Authorization List\*' (set to 'default'), 'OWE Transition Mode' (checked), 'Transition Mode WLAN ID\*' (set to '0-4096'), and 'Lobby Admin Access' (unchecked). A 'Fast Transition' section is also visible, containing 'Status' (set to 'Disabled'), 'Over the DS' (unchecked), and 'Reassociation Timeout \*' (set to '20'). At the bottom of the window, there are 'Cancel' and 'Apply to Device' buttons.

4. Dans la couche 3, sous Sécurité, sélectionnez le paramètre global de la carte de paramètres d'authentification Web. Si un autre profil d'authentification Web est configuré sur le WLC, vous pouvez également le mapper ici :

## Add WLAN



General **Security** Advanced

Layer2 **Layer3** AAA

[Show Advanced Settings >>>](#)

Web Policy

Web Auth Parameter Map

global



Authentication List

Select a value



*For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device*

Cancel

Apply to Device

## Configuration ISE

### Conditions préalables

- S'assurer que Cisco ISE est installé et sous licence pour la fonctionnalité BYOD.
- Ajoutez votre WLC à ISE en tant que périphérique réseau avec le secret partagé RADIUS.

### Certificats

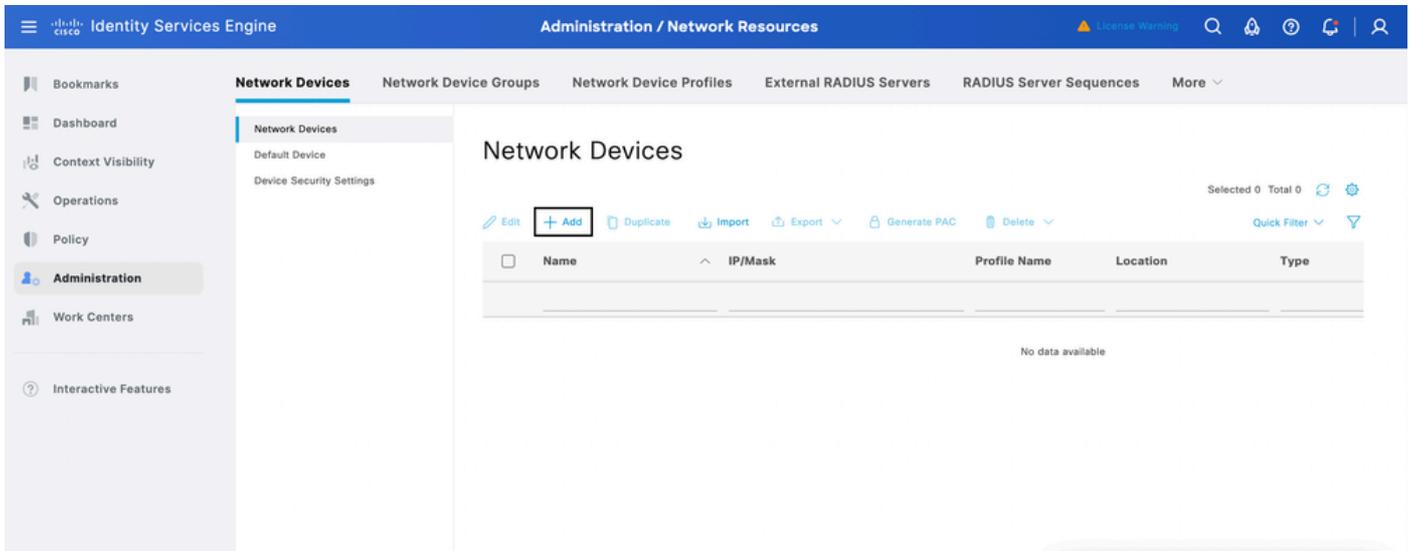
- Installez un certificat de serveur valide sur ISE pour éviter les avertissements de sécurité du navigateur.
- Assurez-vous que le certificat est approuvé par les terminaux (signé par une autorité de certification connue ou une autorité de certification interne avec une racine approuvée).

### Configuration DNS

- Assurez-vous que DNS résout le nom d'hôte ISE pour le portail BYOD.

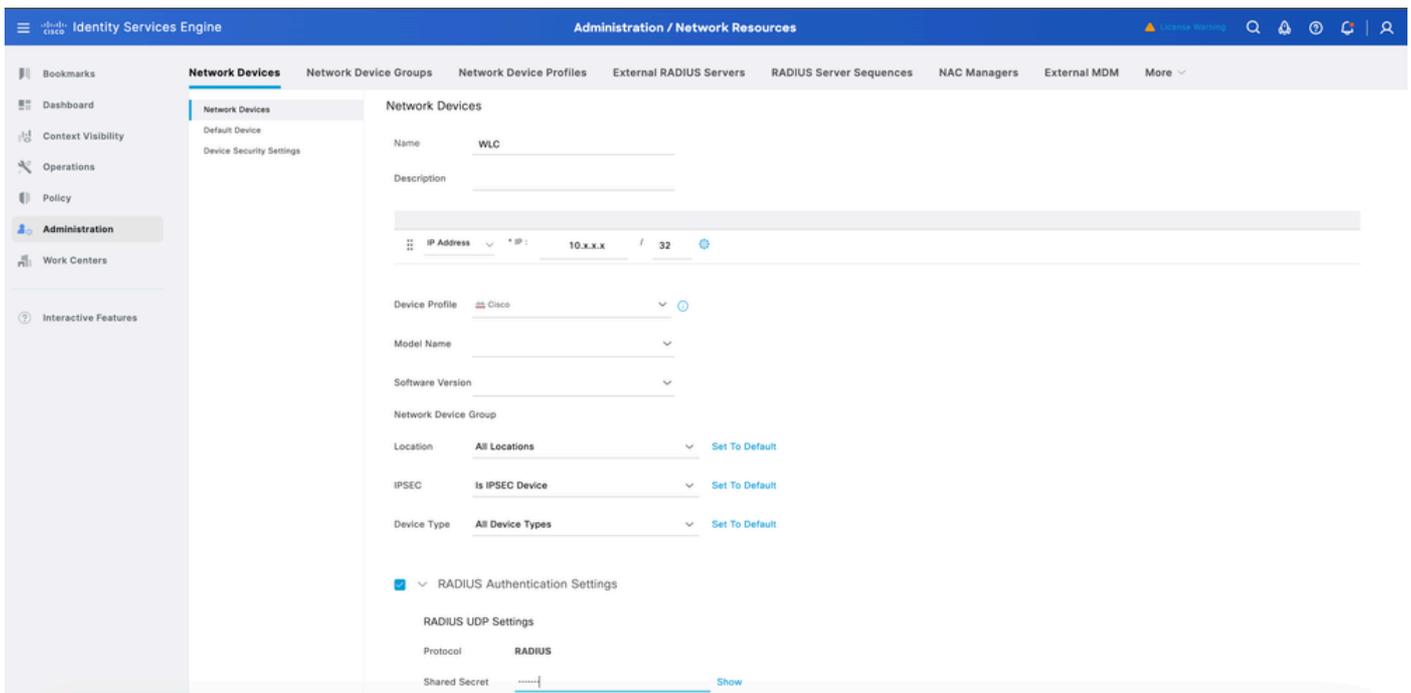
# Configuration du périphérique réseau ISE

1. Connectez-vous à l'interface utilisateur Web ISE.
2. Accédez à Administration > Network Resources > Network Devices.



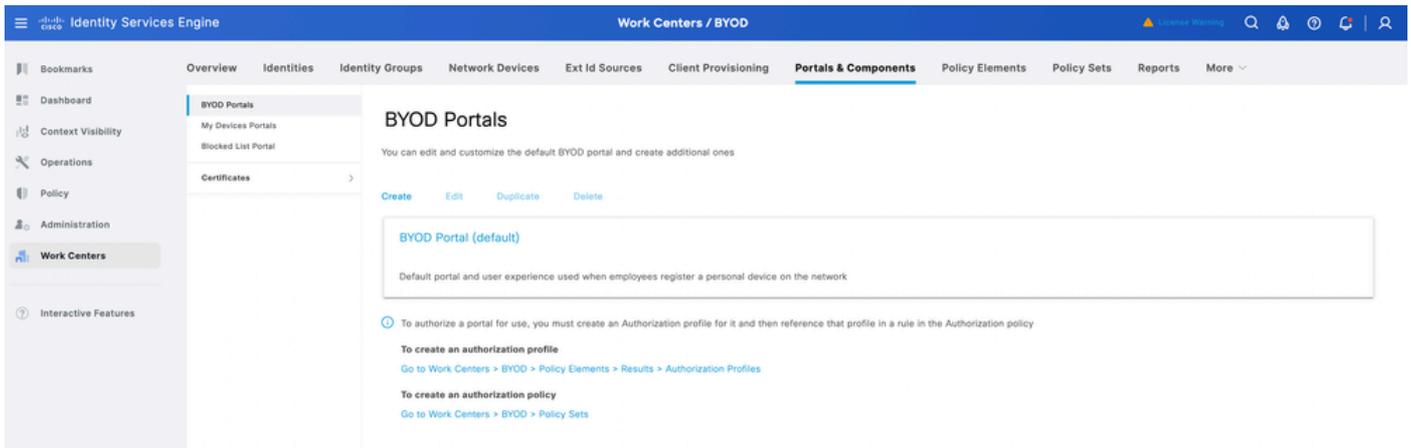
3. Ajoutez votre WLC en tant que périphérique réseau :

- Name : Entrez un nom pour le WLC.
- Adresse IP: Saisissez l'adresse IP de gestion WLC.
- Secret partagé RADIUS : Entrez le même secret partagé que celui configuré sur le WLC.
- Cliquez sur Submit.



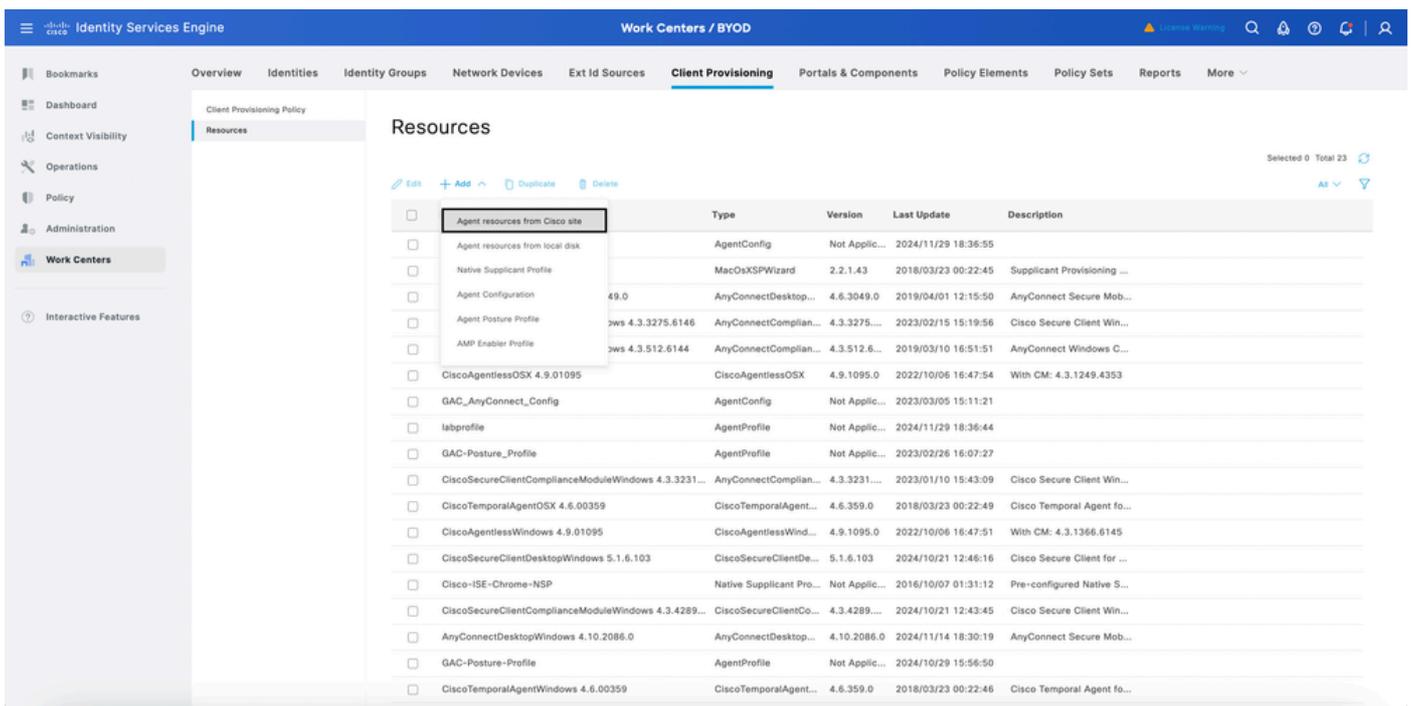
## Créer un portail BYOD

1. Accédez à Work Centers > BYOD > Settings > Portals & Components > BYOD Portals.
2. Cliquez sur Add pour créer un portail BYOD ou vous pouvez utiliser le portail par défaut existant sur ISE.



## Télécharger la dernière version de Cisco IOS®

1. Accédez à Work Centers > BYOD > Client provisioning > Resources.
2. Cliquez sur le bouton Add et sélectionnez agent resources from the Cisco site.



3. Dans la liste des logiciels, sélectionnez la dernière version de Cisco IOS à télécharger.



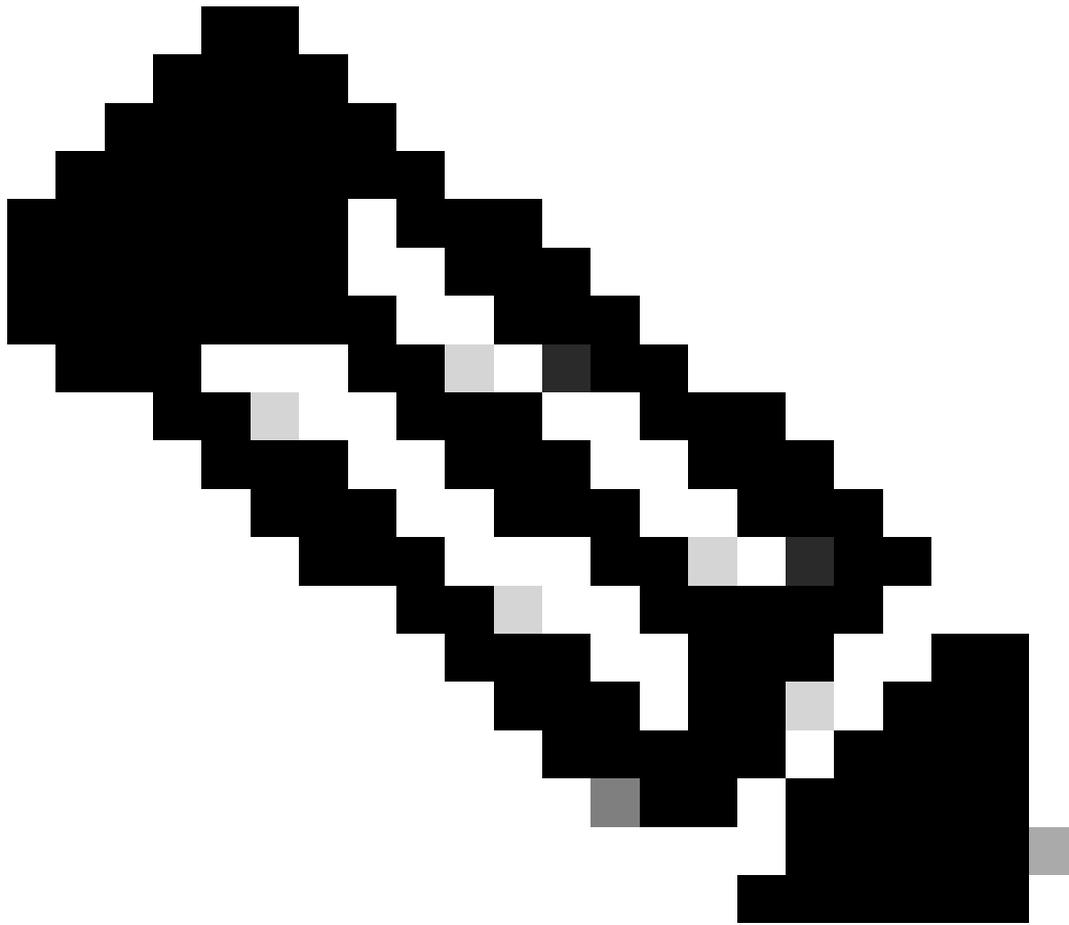
## Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	MacOsXSPWizard 2.7.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
<input type="checkbox"/>	MacOsXSPWizard 3.1.0.1	Supplicant Provisioning Wizard for MAC OSX Version 3.1.0.1
<input type="checkbox"/>	MacOsXSPWizard 3.1.0.2	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
<input type="checkbox"/>	MacOsXSPWizard 3.2.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
<input type="checkbox"/>	MacOsXSPWizard 3.4.0.0	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
<input type="checkbox"/>	WinSPWizard 3.0.0.2	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)
<input checked="" type="checkbox"/>	WinSPWizard 3.0.0.3	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)

For Agent software, please download from <http://cisco.com/go/ciscosecureclient>. Use the "Agent resource from local disk" add option, to import into ISE

Cancel

Save

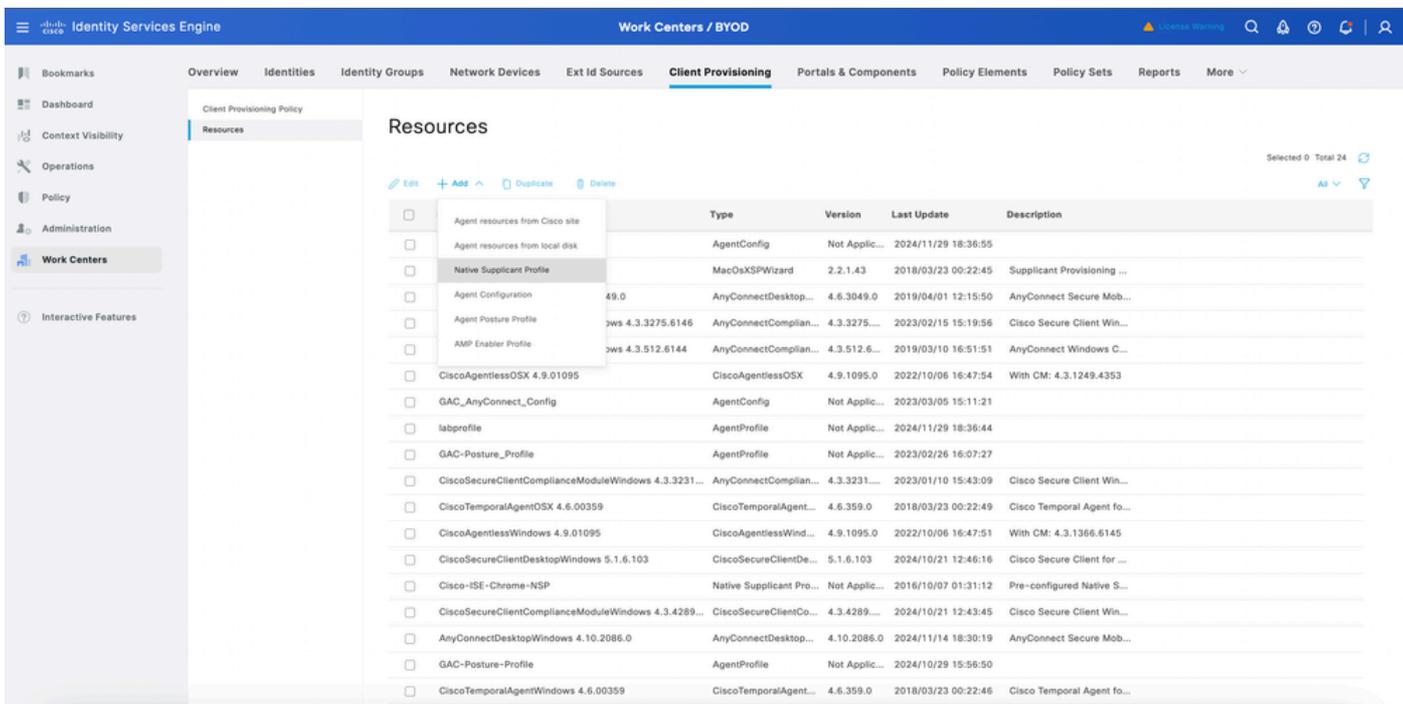


Remarque : Le logiciel Cisco IOS est téléchargé sur ISE pour les terminaux Windows et MacOS. Pour Apple iPhone IOS, il utilise un supplicatant natif pour provisionner l'appareil et Pour appareil Android, vous avez Network setup assistant qui doit être téléchargé à partir de Play Store.

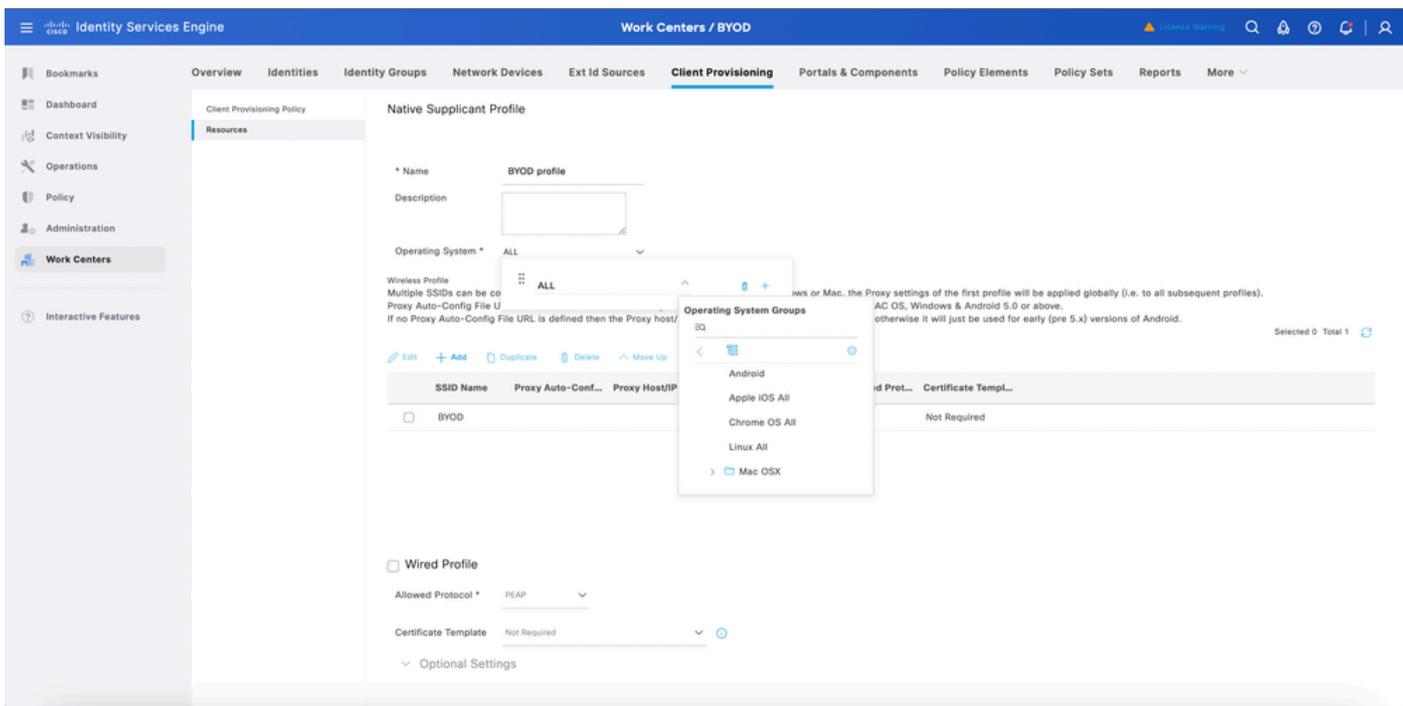
---

## Créer un profil de terminal

1. Accédez à Work Centers > BYOD > Client provisioning > Resources.
2. Cliquez sur Add, sélectionnez Native supplicatant profile dans le menu déroulant.



3. Dans la liste déroulante Operating system (Système d'exploitation), sélectionnez le système d'exploitation requis que vous souhaitez intégrer au périphérique ou définissez-le sur ALL (TOUS) pour intégrer tous les terminaux de votre environnement :



4. Cliquez sur Add dans la page pour créer le profil de point de terminaison afin de configurer la norme 802.1X pour le point de terminaison :

## Wireless Profile(s)

SSID Name \*

Proxy Auto-Config File URL  ⓘ

Proxy Host/IP  ⓘ

Proxy Port

Security \*  ▼

Allowed Protocol \*  ▼

Certificate Template  ▼ ⓘ

### Optional Settings

#### Windows Settings

Authentication Mode  ▼

Automatically use logon name and password (and domain if any)

Enable fast reconnect

Enable quarantine checks

Disconnect if server does not present cryptobinding TLV

Do not prompt user to authorize new servers or trusted certification authorities

Connect even if the network is not broadcasting its name (SSID)

#### iOS Settings

Enable if target network is hidden

#### Android Settings

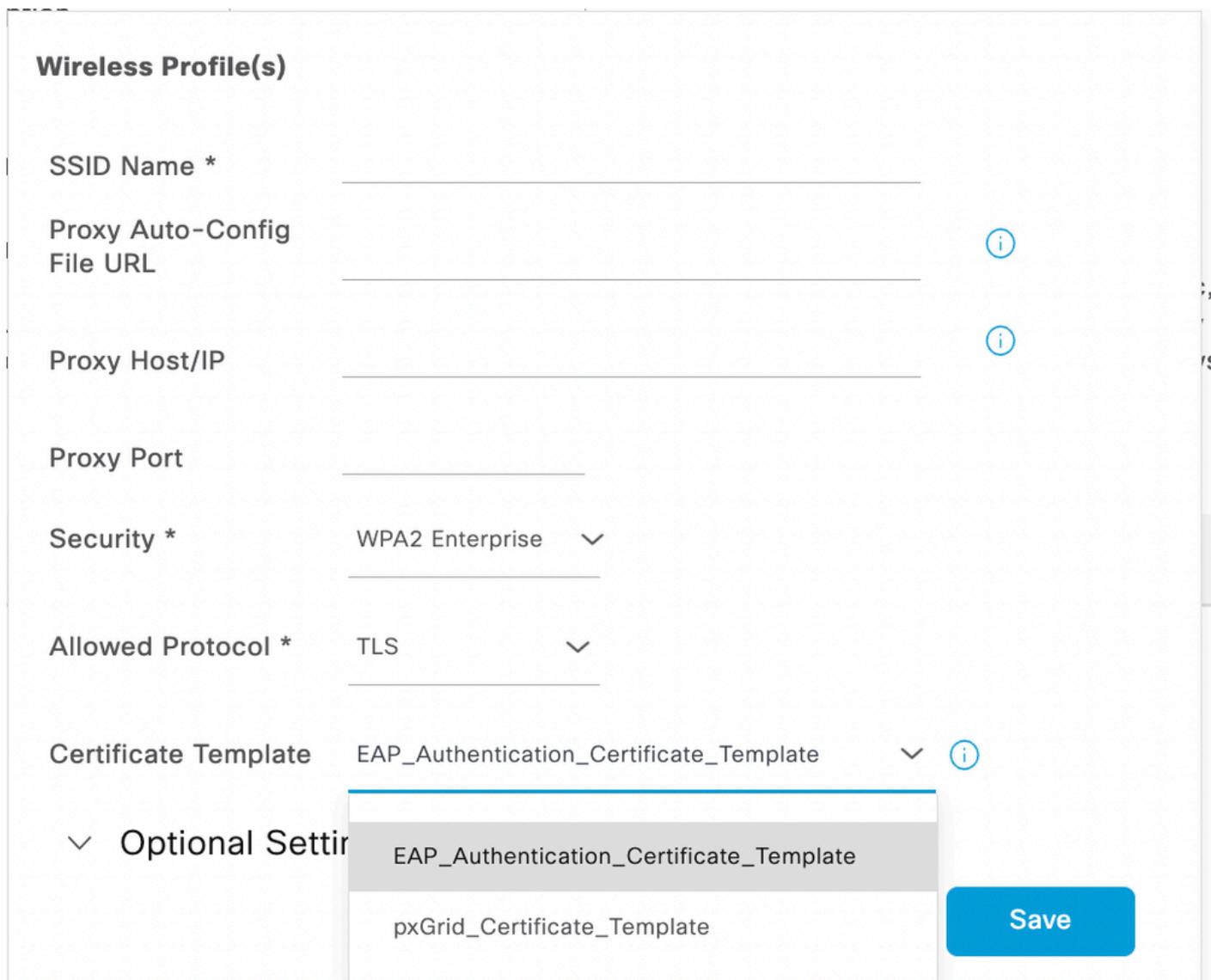
Certificate Enrollment Protocol: ⓘ

En fonction de vos besoins, configurez le profil de point de terminaison pour le point de terminaison dans votre environnement. Le profil de terminaux nous permet de configurer EAP-PEAP, EAP-TLS.

5. Cliquez sur Enregistrer, puis sur Soumettre sur le profil de point de terminaison.

## Modèle de certificat

Le profil de point de terminaison est préconfiguré pour exécuter EAP-TLS. Un modèle de certificat doit être ajouté au profil. Par défaut, ISE a deux modèles prédéfinis qui peuvent être choisis dans la liste déroulante.



**Wireless Profile(s)**

SSID Name \*

Proxy Auto-Config File URL ⓘ

Proxy Host/IP ⓘ

Proxy Port

Security \* WPA2 Enterprise ▾

Allowed Protocol \* TLS ▾

Certificate Template EAP\_Authentication\_Certificate\_Template ▾ ⓘ

Optional Settings

- EAP\_Authentication\_Certificate\_Template
- pxGrid\_Certificate\_Template

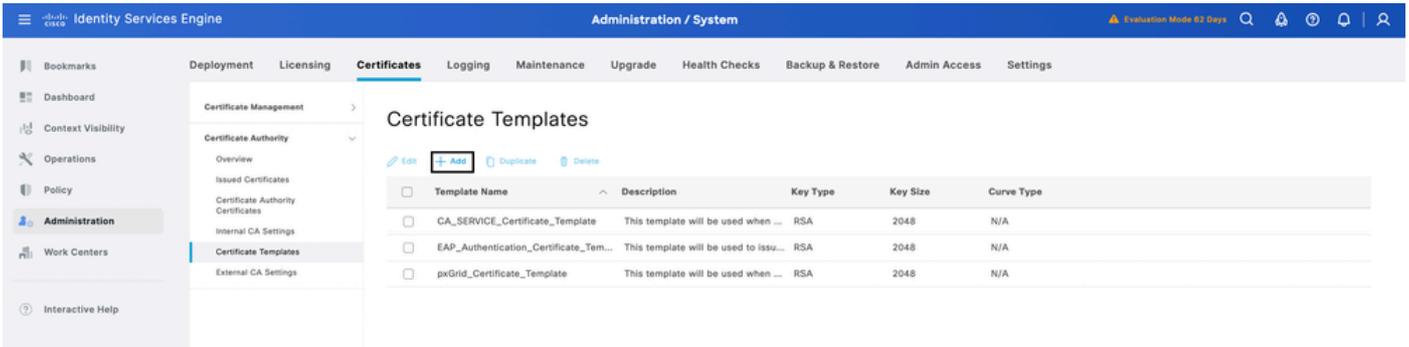
Save

Pour créer un nouveau modèle de certificat, procédez comme suit :

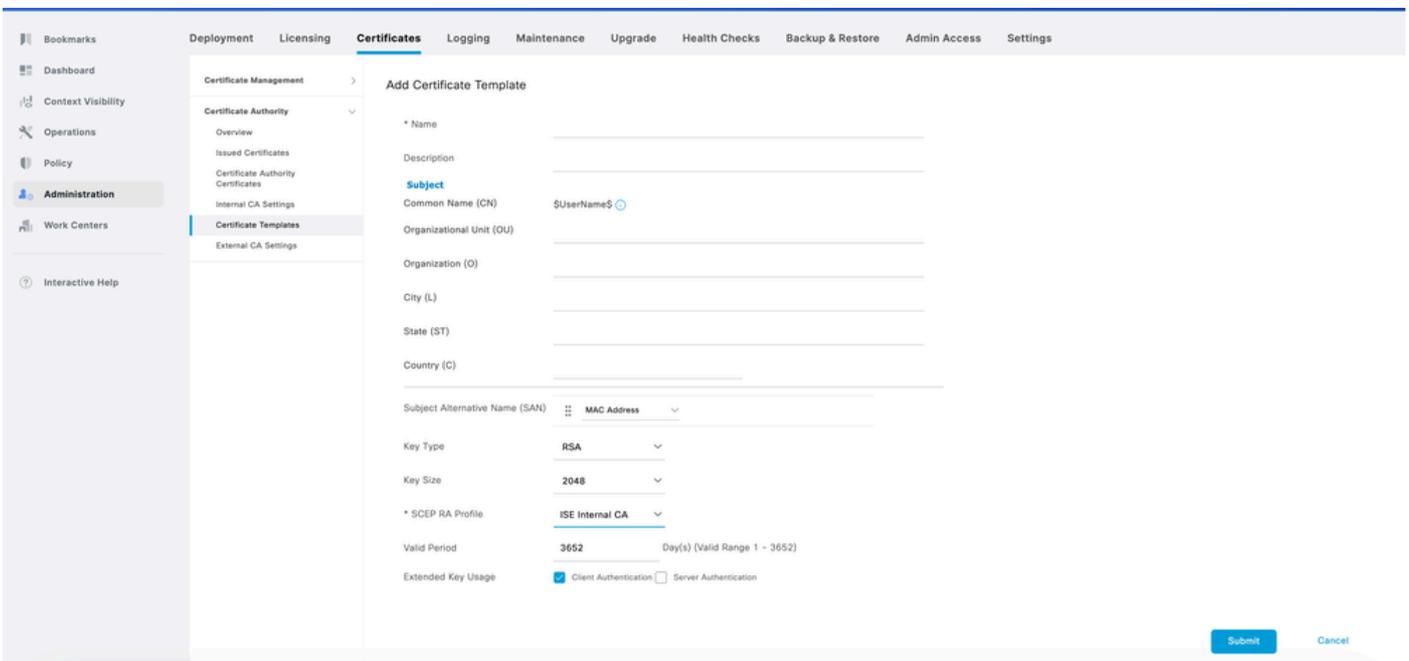
1. Accédez à Administration > System > Certificates > Certificate Authority > Certificate

## Templates.

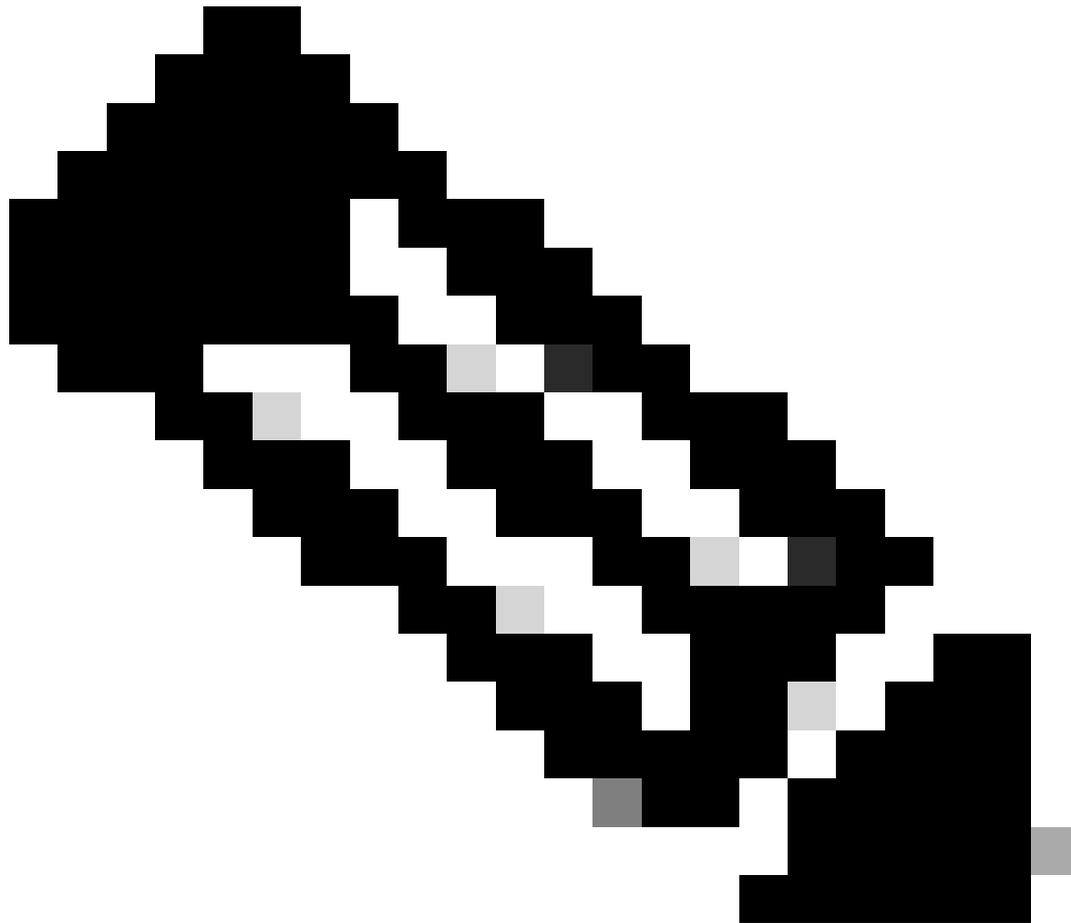
2. Cliquez sur le bouton Ajouter de la page.



3. Renseignez les détails adaptés aux besoins spécifiques de votre organisation.



4. Cliquez sur Soumettre pour enregistrer les modifications.

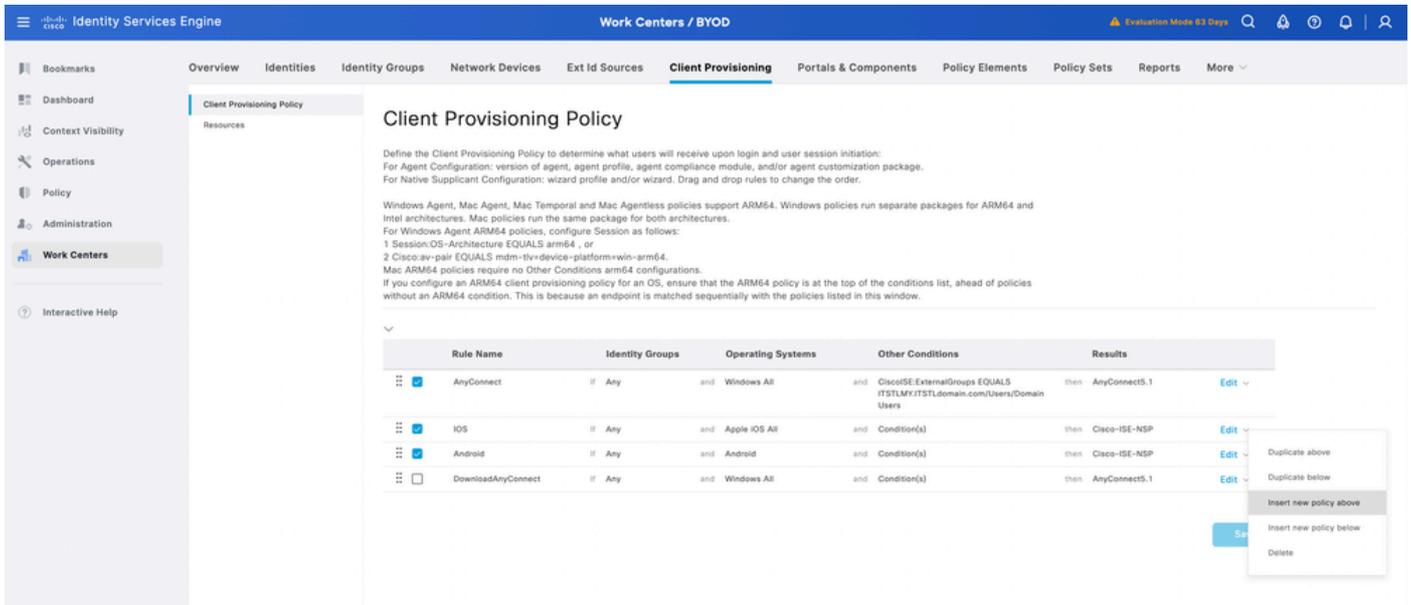


Remarque : Le modèle de certificat peut être utile dans un scénario où vous avez différents domaines et où vous segmentez l'utilisateur en ajoutant une valeur différente dans l'unité d'organisation du certificat.

---

## Mappage d'un profil de point de terminaison au portail d'approvisionnement client

1. Accédez à Work Centers > BYOD > Client provisioning > Client provisioning Policy.
2. Cliquez sur **v** on des règles pour créer une nouvelle règle d'approvisionnement de client.

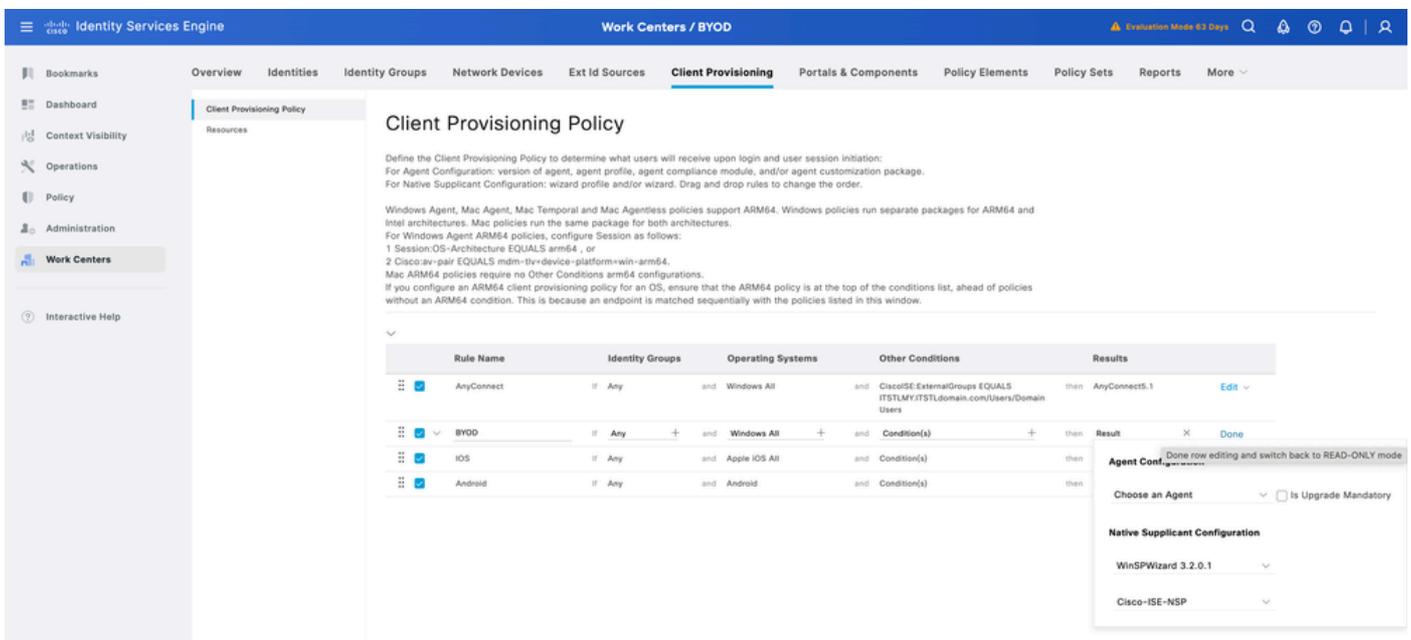


3. Publiez la création de la nouvelle règle sur la page

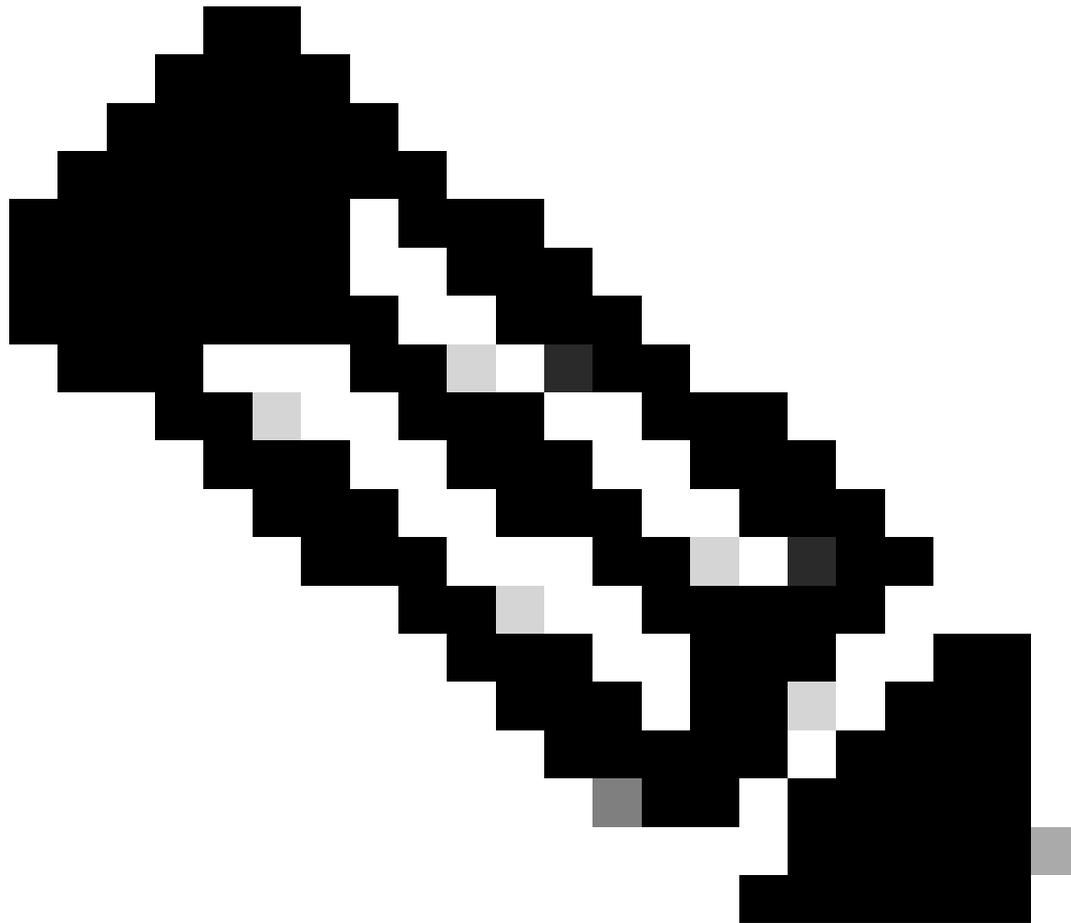
4. Ajoutez le groupe d'identités si vous souhaitez restreindre l'accès de certains utilisateurs au portail BYOD

5. Ajoutez le système d'exploitation auquel vous souhaitez accéder au portail BYOD

6. Mappez la version de Cisco IOS à partir de la liste déroulante et sélectionnez également le profil de point de terminaison que vous avez créé à partir du résultat



7. Cliquez sur Terminé, puis sur le bouton Enregistrer.



Remarque : Cette stratégie a un impact sur l'approvisionnement du client de posture et sur l'approvisionnement BYOD, où la section Configuration de l'agent détermine l'agent de posture et le module de conformité appliqués pour les vérifications de posture, tandis que la section Configuration du demandeur natif gère les paramètres des flux d'approvisionnement BYOD

---

## Configuration des ensembles de stratégies ISE pour le BYOD avec un seul SSID

1. Accédez à Policy > Policy Set et créez une stratégie pour le flux BYOD sur ISE :

Policy Sets Reset [Reset Policy Set Hit Counts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<span style="color: green;">●</span>	BYOD		Wireless_802.1X	Default Network Access	0		
<span style="color: green;">●</span>	Default	Default policy set		Default Network Access	0		

Reset [Save](#)

2. Ensuite, accédez à Administration > Gestion des identités > Sources d'identité externes > Profil d'authentification de certificat. Cliquez sur le bouton Add pour créer le profil de certificat :

Identity Services Engine Administration / Identity Management

External Identity Sources

- Certificate Authentic...
- Active Directory
- CiscoISE
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login
- REST

Certificate Authentication Profile

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

Name	Description
Preloaded_Certificate_Profile	Precreated Certificate Authorization Profile.

Identity Services Engine Administration / Identity Management

External Identity Sources

Certificate Authentication Profiles List > New Certificate Authentication Profile

Certificate Authentication Profile

\* Name: BYOD

Description:

Identity Store: [not applicable]

Use Identity From:  Certificate Attribute **Subject - Common Nar**

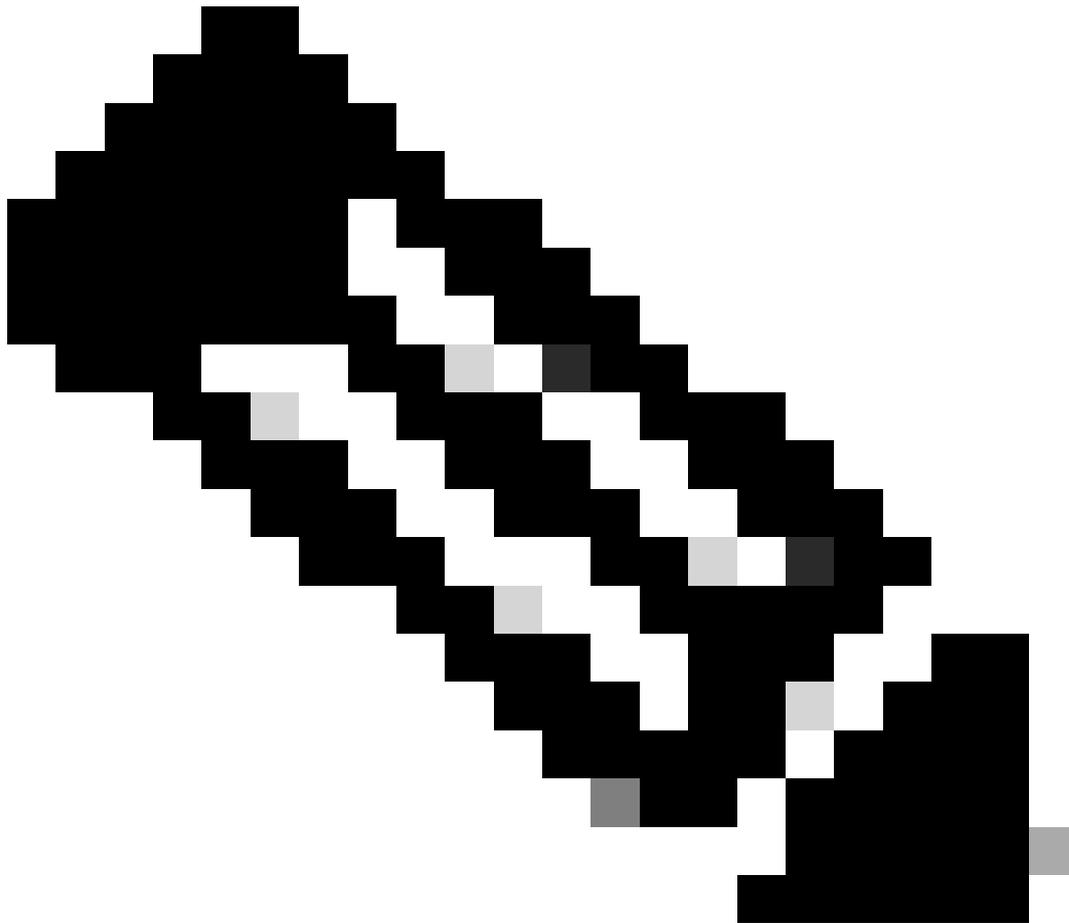
Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store:  Never

Only to resolve identity ambiguity

Always perform binary comparison

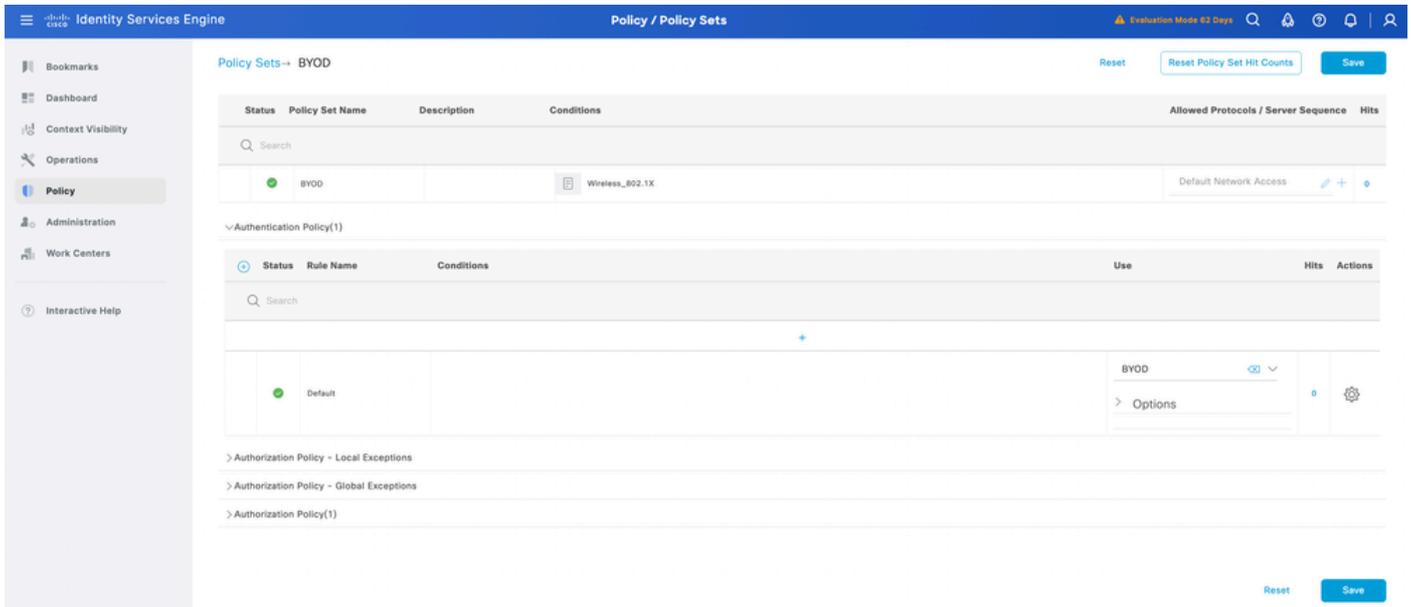
[Submit](#) [Cancel](#)



Remarque : Dans le magasin d'identités, vous pouvez toujours sélectionner votre Active Directory qui a été intégré à ISE pour effectuer une recherche d'utilisateur à partir du certificat pour plus de sécurité.

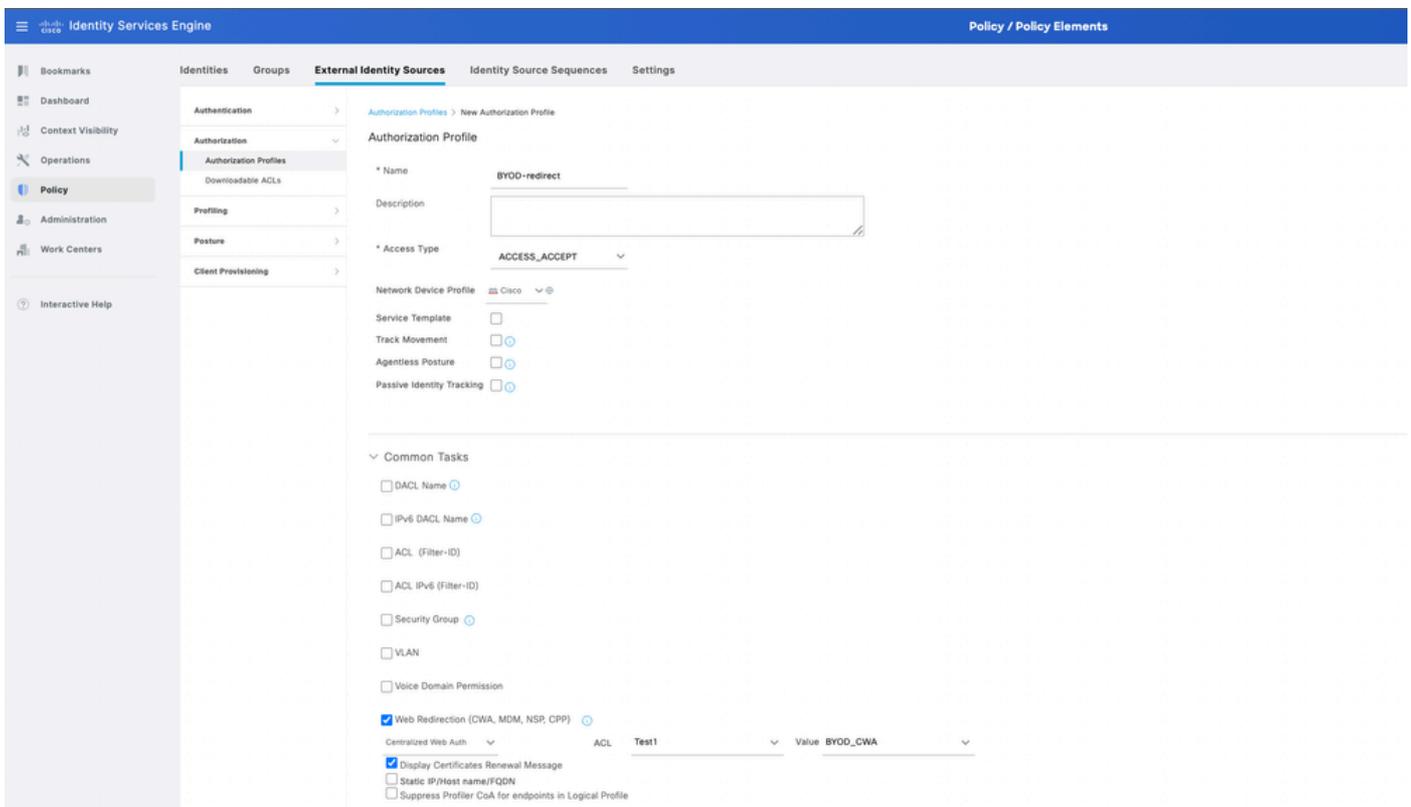
---

3. Cliquez sur Soumettre pour enregistrer la configuration. Ensuite, mappez le profil de certificat à la stratégie définie pour le BYOD :

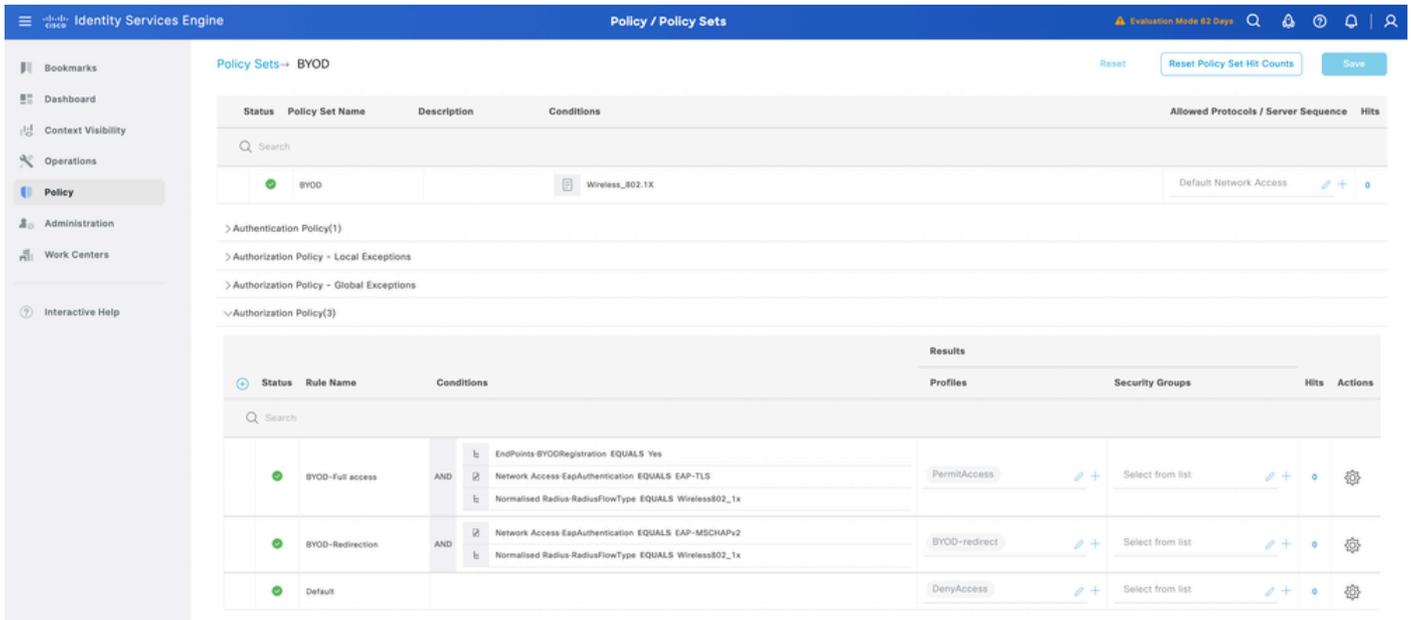


4. Configurez le profil d'autorisation pour la redirection BYOD et l'accès complet après le flux BYOD. Allez à Policy > Policy Elements > Results > Authorization > Authorization Profiles (politique > éléments de politique > résultats > autorisation > profils d'autorisation).

5. Cliquez sur Ajouter et créez un profil d'autorisation. Vérifiez la redirection Web (CWA, MDM, NSP, CPP) et mappez la page du portail BYOD. Ajoutez également le nom de la liste de contrôle d'accès de redirection du WLC au profil. Pour le profil d'accès complet, configurez un accès autorisé avec le VLAN d'entreprise correspondant dans le profil.



6. Mappez le profil d'autorisation à la règle d'autorisation. La règle EndPoints·BYODegistration doit avoir la valeur yes pour l'accès complet au BYOD afin que l'utilisateur puisse accéder au réseau après le flux BYOD.



## Configuration des ensembles de stratégies ISE pour le BYOD à double SSID

Dans la configuration BYOD à double SSID, le jeu de deux stratégies est configuré sur ISE. Le premier ensemble de politiques concerne le SSID ouvert/non sécurisé, où la configuration de l'ensemble de politiques redirige l'utilisateur vers la page BYOD lors de la connexion au SSID ouvert/non sécurisé

1. Accédez à Policy > Policy Set et créez une politique pour le flux BYOD sur ISE.
2. Créez un ensemble de stratégies pour le SSID ouvert/non sécurisé et le SSID d'entreprise qui authentifie l'utilisateur BYOD enregistré sur ISE.

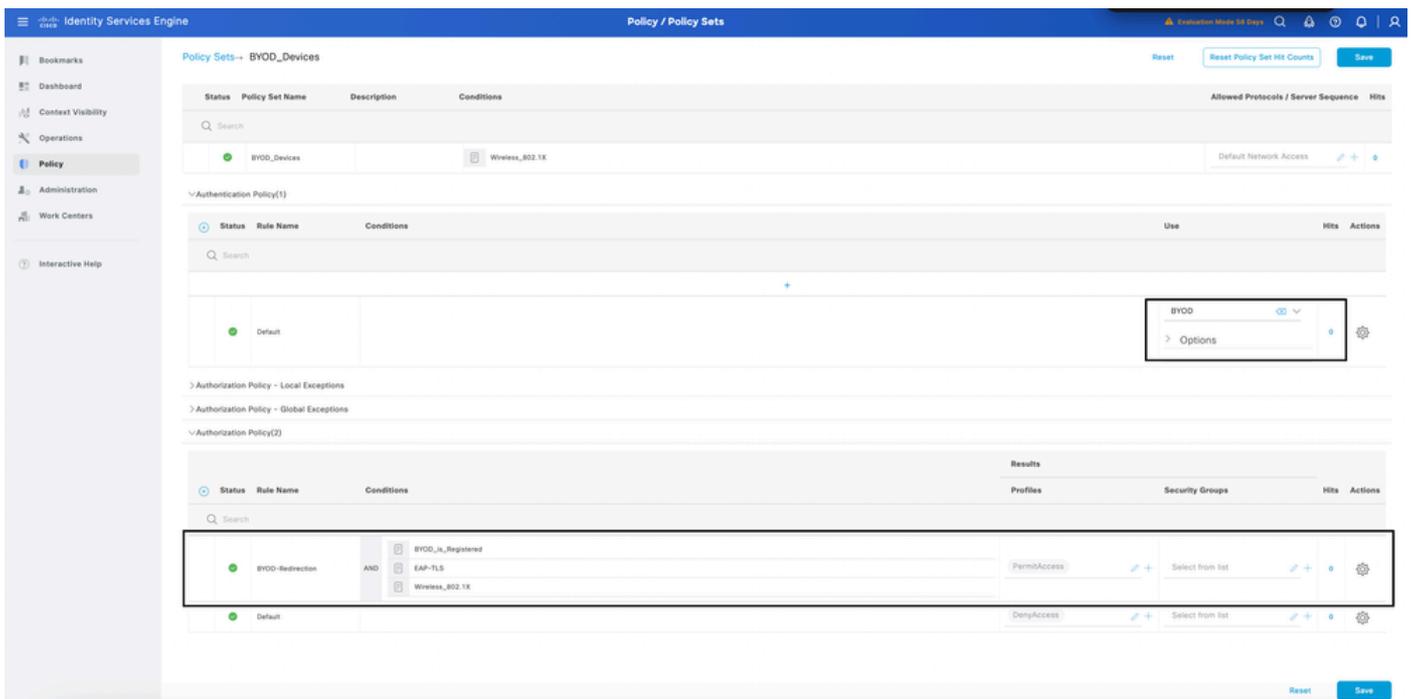


3. Dans le jeu de stratégies d'intégration, sélectionnez Continuer sous les options. Pour la stratégie d'autorisation, créez une condition et mappez le profil d'autorisation de redirection. Les mêmes étapes sont impliquées dans la création du profil d'autorisation, que l'on peut trouver au point 4.



4. Dans l'ensemble de stratégies enregistrées pour le BYOD, configurez la stratégie d'authentification avec le profil de certificat identique à celui trouvé.

dans Configurer les ensembles de stratégies ISE pour le BYOD avec un seul SSID au point 2. Créez également une condition pour la stratégie d'autorisation et mappez le profil d'accès complet à la stratégie.



## Journalisation

À partir du journal en direct d'ISE, l'authentification de l'utilisateur réussira et sera redirigée vers la page du portail BYOD. Une fois le flux BYOD terminé, l'utilisateur doit pouvoir accéder au réseau

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authorization Policy	Authoriz...	IP Address	Network De...	Devi...
Feb 24, 2025 12:30:18.1...	<span style="color: blue;">●</span>		0	test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD	PermitAcc...	10.127.196.2...		TenGig...
Feb 24, 2025 12:06:43.0...	<span style="color: green;">■</span>			test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD_redirect	BYOD_Re...	10.127.196.2...	BYOD-Switch	TenGig...
Feb 24, 2025 12:06:37.9...	<span style="color: green;">■</span>			test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD_redirect	BYOD_Re...	10.127.196.2...	BYOD-Switch	TenGig...

Du point de vue de l'utilisateur, ils sont d'abord redirigés vers la page BYOD et le périphérique approprié doit être sélectionné à partir de la page Web. Pour le test, un périphérique Windows 10 a été utilisé

BYOD Portal
test ⓘ

1
2
3

### BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

**The following system was detected**

**Windows**

**Was your device detected incorrectly?**

**Select your Device**

Windows ▼

Start

Après avoir cliqué sur le bouton Next (Suivant), vous êtes dirigé vers une page où l'utilisateur est invité à saisir le nom du périphérique et sa description

The screenshot shows the 'BYOD Portal' interface. At the top left is the Cisco logo, and at the top right is the text 'test'. The main content area has a blue header with 'BYOD Portal' and a progress indicator showing step 2 of 3. Below the header, the section is titled 'Device Information'. The instructions read: 'Enter the device name and optional description for this device so you can manage it using the My Devices Portal.' There are three input fields: 'Device name: \*' (highlighted with a blue glow), 'Description:', and 'Device ID:'. The 'Device ID' field contains a blacked-out value. At the bottom of the form is a blue 'Continue' button with a right-pointing arrow.

Indiquez que l'utilisateur doit télécharger l'outil Network Assistant pour télécharger le profil de point de terminaison et le certificat EAP TLS pour l'authentification si le profil est configuré pour effectuer l'authentification EAP-TLS

The screenshot shows the 'BYOD Portal' interface at step 3 of the process. The header is the same as in the previous screenshot. The main content area has a blue header with 'BYOD Portal' and a progress indicator showing step 3 of 3. Below the header, the section is titled 'Install'. The instructions read: 'Please wait while we download the Cisco Network Setup Assistant. You will then need to manually run the Setup Assistant and follow the instructions to finish registering this device.'

Exécutez l'application Network Assistant avec des privilèges d'administrateur et cliquez sur le bouton Démarrer pour démarrer le flux d'intégration :



## Network Setup Assistant

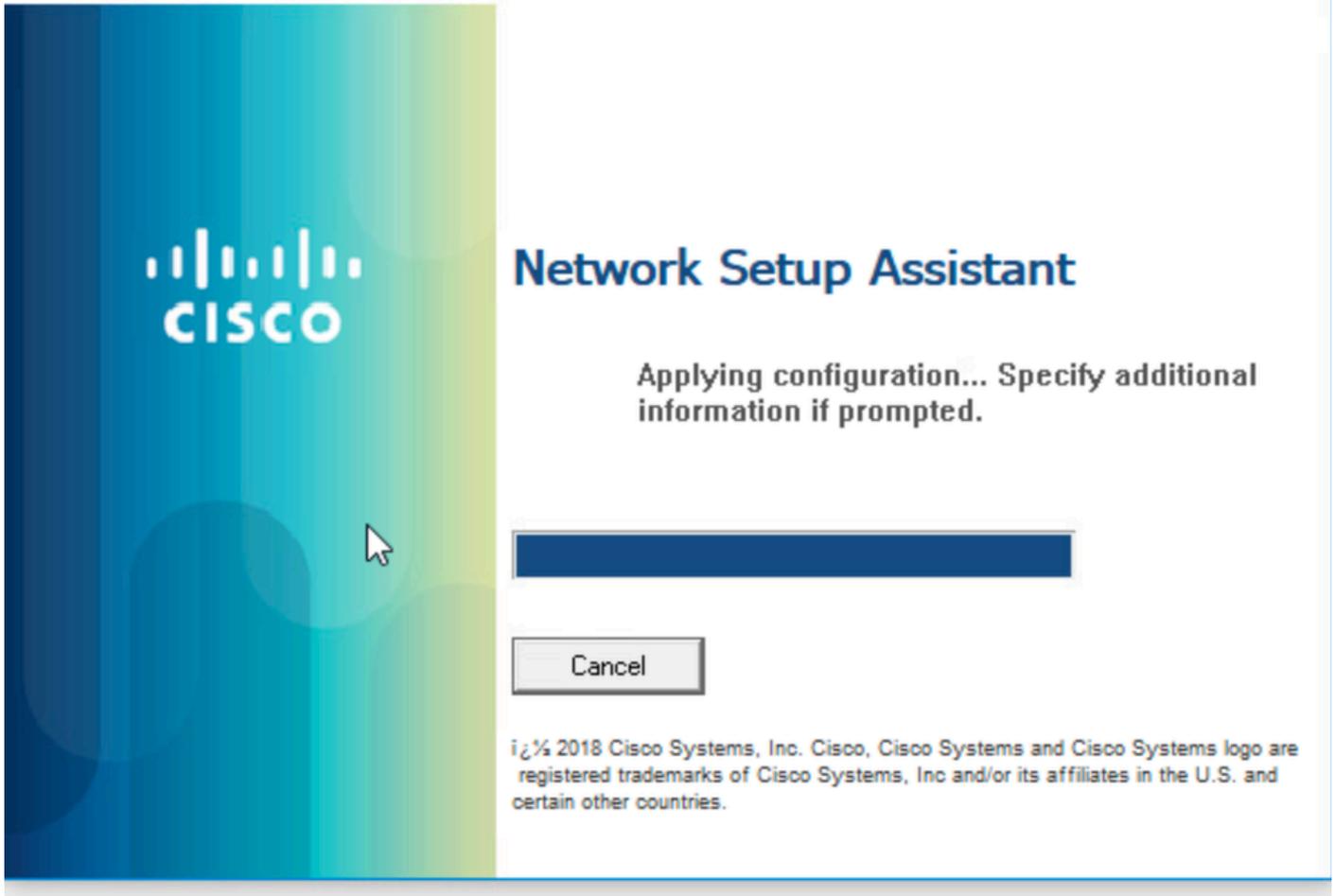


This application automatically configures network settings.

Start

Quit

© 2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.



L'utilisateur a été correctement intégré au réseau avec son périphérique personnel pour accéder aux ressources.

## Dépannage

Pour résoudre le problème du BYOD, activez ce débogage sur ISE

Attributs à définir au niveau de débogage :

- client (guest.log)
- client-webapp (guest.log)
- scep (ise-psc.log)
- ca-service (ise-psc.log)
- admin-ca (ise-psc.log)
- runtime-AAA (prt-server.log)
- nsf (ise-psc.log)
- nsf-session (ise-psc.log)
- profiler (profiler.log)

# Extrait de journal

## Journaux invités

Ces journaux indiquent que l'utilisateur a correctement redirigé la page et téléchargé l'application Network Assistant :

```
2025-02-24 12:06:08,053 INFO [https-jsse-nio-10.127.196.172-8443-exec-4][]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D59CC5:-
chemin de mappage trouvé dans action-forwards, transfert vers : pages/byodWelcome.jsp // Page
d'accueil du BYOD
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5::test:- Taille
de pTranSteps:1
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5::test:-
getNextFlowStep, pTranSteps:[id: d2513b7b-7249-4bc3-a423-0e7d9a0b2500]
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5::test:-
getNextFlowStep, stepTran:d2513b7b-7 249-4bc3-a423-0e7d9a0b2500
2025-02-24 12:06:09,979 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D59CC5:-
chemin de mappage trouvé dans action-forwards, transfert vers : pages/byodRegistration.jsp
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5::test:- Taille
de pTranSteps:1
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5::test:-
getNextFlowStep, pTranSteps:[id: f203b757-9e8a-473e-abdc-879d0cd37491]
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5::test:-
getNextFlowStep, stepTran:f203b75 -9e8a-473e-abdc-879d0cd37491
2025-02-24 12:06:14,647 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D59CC5:-
chemin de mappage trouvé dans action-forwards, transfert vers : pages/byodInstall.jsp
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][]
cisco.cpm.client.provisioning.StreamingServlet -:0000000000000000B30D59CC5:- Session = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][]
cisco.cpm.client.provisioning.StreamingServlet -:0000000000000000B30D59CC5:- portalSessionId
= null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]]
cisco.cpm.client.provisioning.StreamingServlet -:0000000000000000B30D59CC5:-
StreamingServlet URI:/auth/provisioning/download/f6b73ef8-4502-4d50-81aa-
bbb91e8828da/NetworkSetupAssistant.exe // L'application d'assistance réseau a été envoyée au
point d'extrémité
```

## Journaux Ise-Psc

Lorsque l'application est téléchargée sur le terminal, elle lance un flux SCEP pour obtenir le certificat client auprès d'ISE.

```
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- CertStore contient 4 certificat(s) :
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 1. '[issuer=CN=Certificate Services Root CA - iseguest ;
serial=32281512738768960628252532784663302089]'
2025-02-24 12:04:39,808 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 2. '[issuer=CN=Certificate Services Endpoint Sub CA -
iseguest ; serial=131900858749761727853768227590303808637]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 3. '[issuer=CN=Certificate Services Root CA - iseguest ;
serial=68627620160586308685849818775100698224]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 4. '[issuer=CN=Certificate Services Node CA - iseguest ;
serial=72934767698603097153932482227548874953]'
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Sélection du certificat de chiffrement
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Sélection du certificat avec la clé keyEncipherment
keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 1 certificat(s) trouvé(s) avec keyEncipherment keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Utilisation de [issuer=CN=Certificate Services Endpoint
Sub CA - iseguest ; serial=131900858749761727853768227590303808637] pour le chiffrement
des messages
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Sélection du certificat du vérificateur
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Sélection du certificat avec la clé de signature
numériqueUtilisation
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 1 certificat(s) trouvé(s) avec la clé de signature
numériqueUtilisation
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Utilisation de [issuer=CN=Certificate Services Endpoint
Sub CA - iseguest ; serial=131900858749761727853768227590303808637] pour la vérification
des messages
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Sélection du certificat de l'émetteur
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
```

org.jscep.client.CertStoreInspector -::::- Sélection d'un certificat avec basicConstraints  
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler\_Worker-5][[]]  
org.jscep.client.CertStoreInspector -::::- 3 certificat(s) trouvé(s) avec basicConstraints  
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler\_Worker-5][[]]  
org.jscep.client.CertStoreInspector -::::- Utilisation de [issuer=CN=Certificate Services Endpoint  
Sub CA - iseguest ; serial=131900858749761727853768227590303808637] pour l'émetteur  
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler\_Worker-5][[]]  
com.cisco.cpm.scep.PKIServerLoadBalancer -::::- Mesures de performances des serveurs SCEP :  
name[actif/inactif, nombre total de demandes, nombre total de défaillances, nombre de demandes  
en vol, moyenne RTT]  
[http://127.0.0.1:9444/caservice/scep\[actif,96444,1,0,120\]](http://127.0.0.1:9444/caservice/scep[actif,96444,1,0,120])

## Téléchargement du profil de terminal

Une fois le processus SCEP terminé et le terminal installé le certificat, l'application télécharge le profil du terminal pour une authentification ultérieure qui serait effectuée par le périphérique :

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]  
cisco.cpm.client.provisioning.EvaluationServlet -::::- Référent = Windows // Le périphérique  
Windows a été détecté en fonction de la page Web  
24-02-2025 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]  
cisco.cpm.client.provisioning.EvaluationServlet -::::- Session = 0000000000000000B30D59CC5  
24-02-2025 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]  
cisco.cpm.client.provisioning.EvaluationServlet -::::- Session = 0000000000000000B30D59CC5  
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]  
cisco.cpm.client.provisioning.EvaluationServlet -::::- provisionner le profil nsp  
24-02-2025 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]  
cisco.cpm.client.provisioning.StreamingServlet -::::- Session = 0000000000000000B30D59CC5  
24-02-2025 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]  
cisco.cpm.client.provisioning.StreamingServlet -::::- portalSessionId = null  
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]  
cisco.cpm.client.provisioning.StreamingServlet -::::- StreamingServlet  
URI:/auth/provisioning/download/b8ce01e6-b150-4d4e-9698-40e48d5e0197/Cisco-ISE-  
NSP.xml//Le profil NSP est téléchargé sur le point d'extrémité  
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]  
cisco.cpm.client.provisioning.StreamingServlet -::::- Diffusion en continu sur IP: type de fichier :  
NativeSPProfile, nom de fichier : Cisco-ISE-NSP.xml //Application Network Assistant  
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]  
cisco.cpm.client.provisioning.StreamingServlet -::::- BYODStatus:INIT\_PROFILE  
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]  
cisco.cpm.client.provisioning.StreamingServlet -::::- userId a été défini pour tester  
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]]  
cisco.cpm.client.provisioning.StreamingServlet -::::- le type de redirection est : SUCCESS\_PAGE,  
l'URL de redirection est : pour mac :

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.