Configuration du BYOD sans fil SSID unique sous Windows et ISE

Table des matières

Introduction

Ce document décrit comment configurer Bring Your Own Device sur Cisco Identity Services Engine pour les ordinateurs Windows à l'aide d'un SSID unique et d'un SSID double.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco Identity Services Engine (ISE) version 3.0
- Configuration de Cisco WLC
- Utilisation du BYOD (Bring Your Own Device)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE version 3.0
- Windows 10
- WLC et AP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Théorie

Dans le cas du BYOD avec SSID unique, un seul SSID est utilisé pour l'intégration des périphériques et l'accès complet aux périphériques enregistrés. Tout d'abord, l'utilisateur se connecte au SSID en utilisant le nom d'utilisateur et le mot de passe (MSCHAPv2). Une fois l'authentification réussie sur ISE, l'utilisateur est redirigé vers le portail BYOD. Une fois l'enregistrement du périphérique terminé, le client final télécharge l'assistant NSA (Native Supplicant Assistant) à partir d'ISE . NSA est installé sur le client final et télécharge le profil et le certificat depuis ISE. La NSA configure le demandeur sans fil et le client installe le certificat. Le point de terminaison effectue une autre authentification sur le même SSID en utilisant le certificat téléchargé à l'aide d'EAP-TLS. ISE vérifie la nouvelle demande du client, la méthode EAP et l'enregistrement du périphérique, et donne un accès complet au périphérique.

Étapes du BYOD avec SSID unique Windows

- Authentification EAP-MSCHAPv2 initiale
- Redirection vers le portail BYOD
- Enregistrement des périphériques
- Téléchargement NSA
- Téléchargement du profil
- Téléchargement du certificat
- authentification EAP-TLS

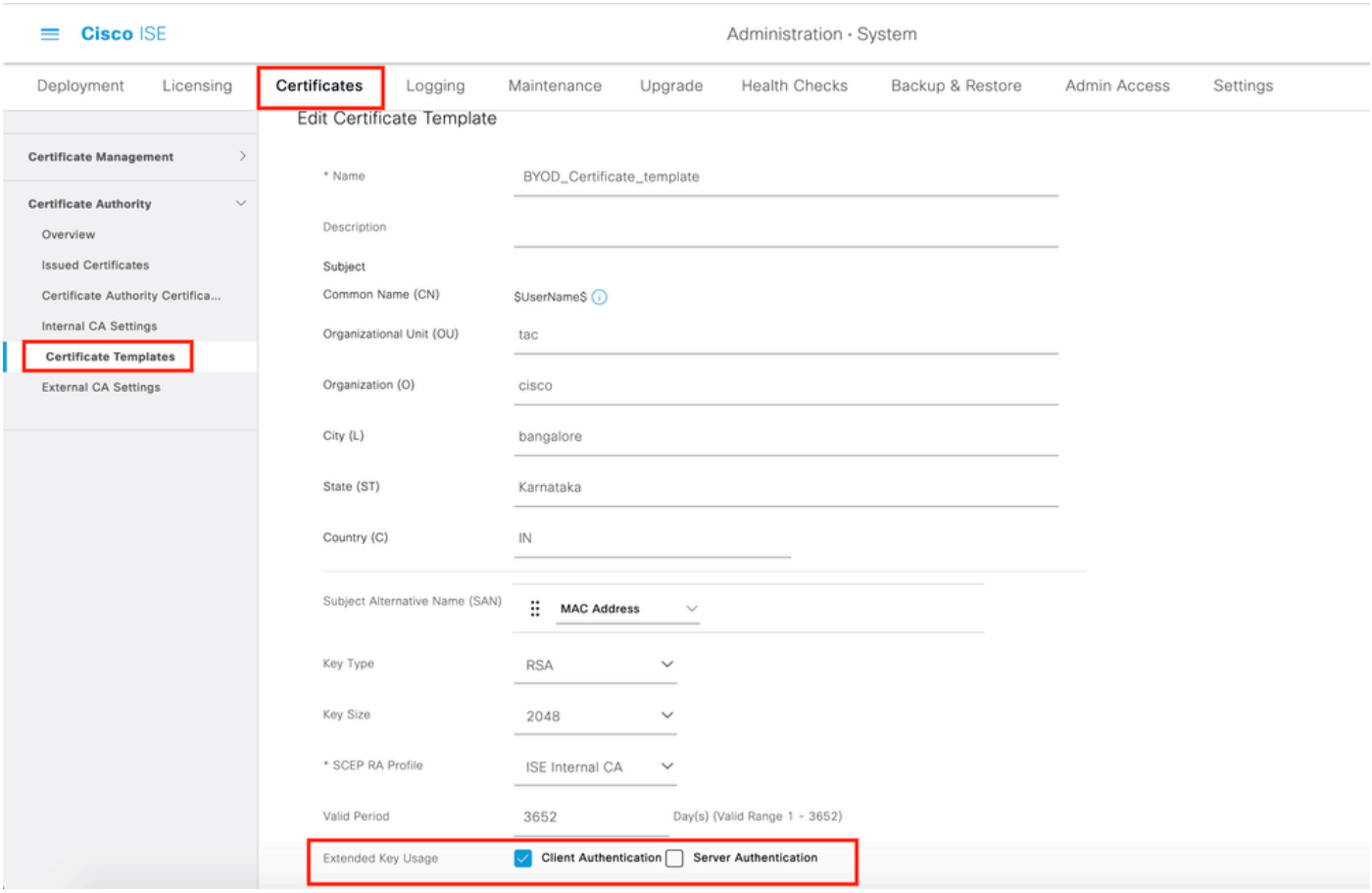
Configurer

Configuration ISE

Étape 1 : ajout d’un périphérique réseau sur ISE et configuration de RADIUS et d’une clé partagée

Accédez à ISE > Administration > Network Devices > Add Network Device.

Étape 2. Créer un modèle de certificat pour les utilisateurs BYOD Le modèle doit avoir une utilisation améliorée de la clé d'authentification client. Vous pouvez utiliser le modèle EAP_Certificate_Template par défaut.

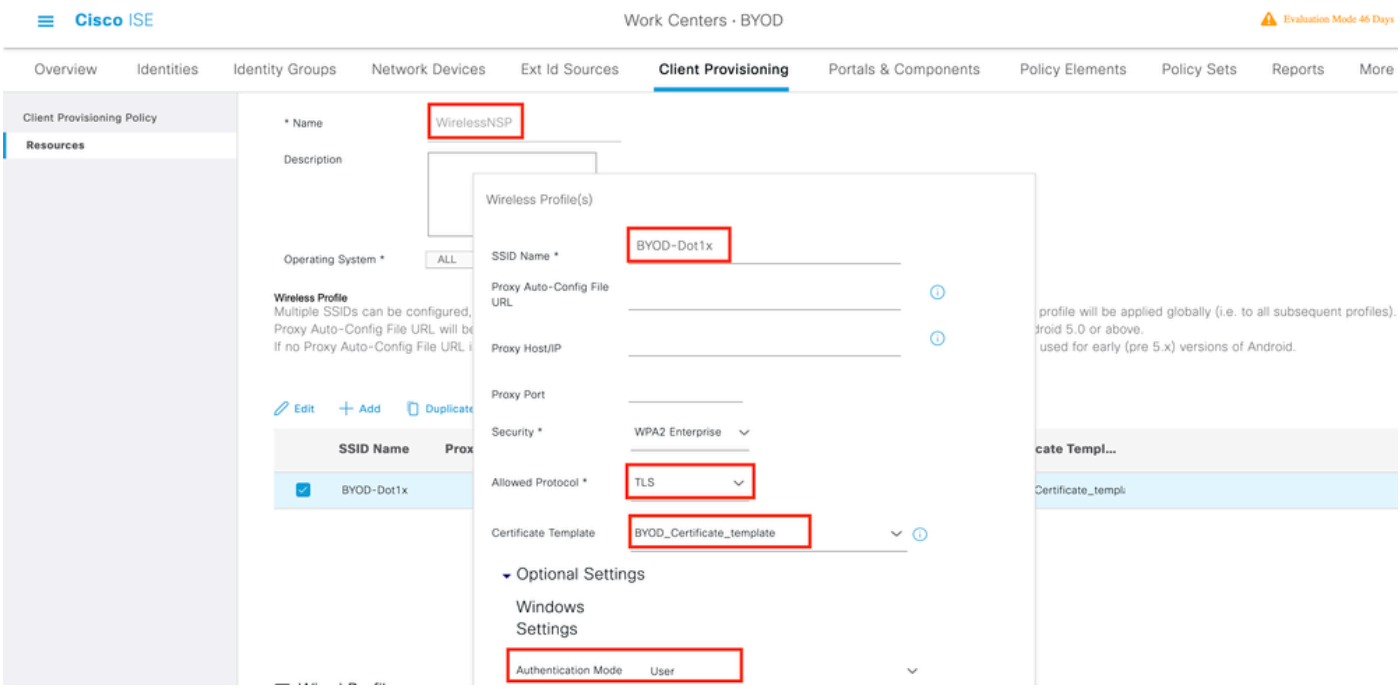


Étape 3 : création d'un profil de demandeur natif pour un profil sans fil

Accédez à ISE > Work Centers > BYOD > Client Provisioning. Cliquez sur Add et choisissez Native Supplicant Profile (NSP) dans la liste déroulante.

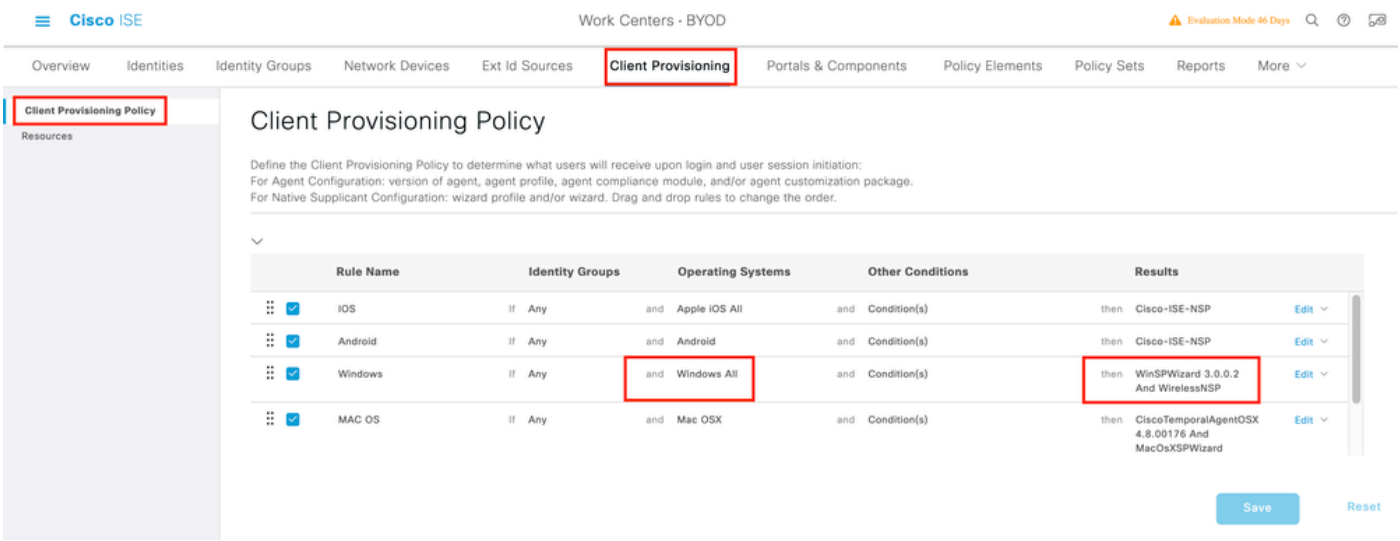
Ici, le nom SSID doit être le même que celui que vous avez utilisé pour vous connecter avant d'effectuer un seul BYOD SSID. Sélectionnez le protocole TLS. Choisissez Certificate template comme créé à l'étape précédente ou vous pouvez utiliser le EAP_Certificate_Template par défaut.

Sous Optional settings, sélectionnez user ou User and Machine authentication selon vos besoins. Dans cet exemple, il est configuré en tant qu'authentification utilisateur. Conservez les autres paramètres par défaut.



Étape 4 : création d'une stratégie de configuration client pour le périphérique Windows

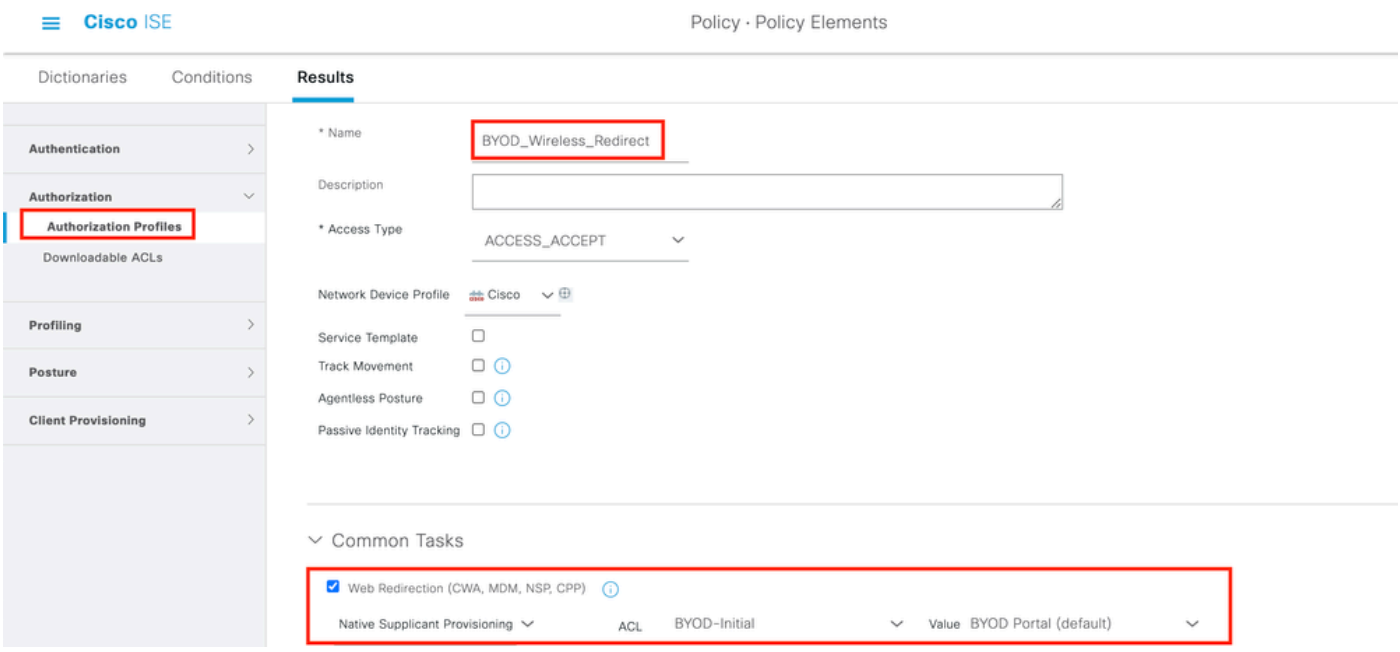
Accédez à ISE > Work Centers > BYOD > Client Provisioning > Client Provisioning Policy. Sélectionnez le système d'exploitation Windows ALL. Sélectionnez WinSPWizard 3.0.0.2 et NSP créés à l'étape précédente.



Étape 5. Créer un profil d'autorisation pour les périphériques non enregistrés comme périphériques BYOD

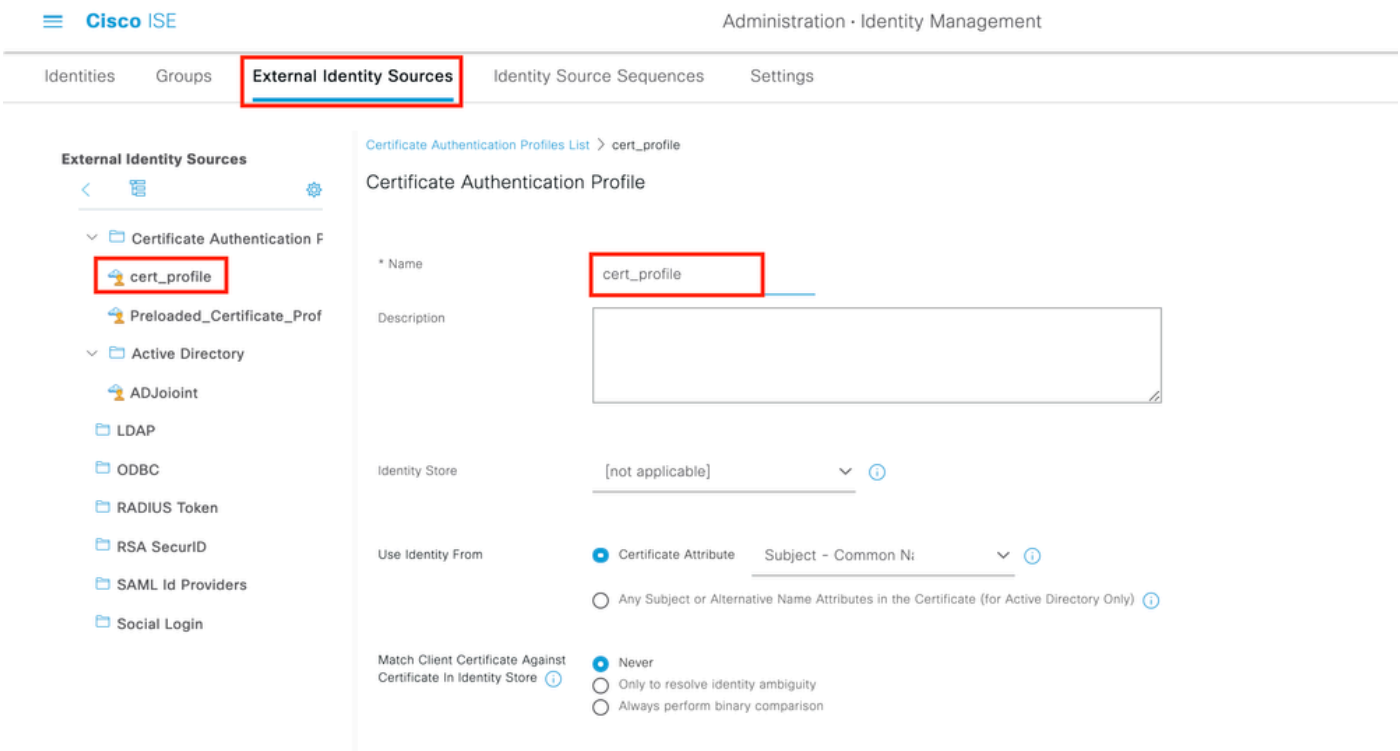
Accédez à ISE > Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add.

Sous Common Task, sélectionnez Native Supplicant Provisioning. Définissez un nom de liste de contrôle d'accès de redirection créé sur le WLC et sélectionnez le portail BYOD. Ici, le portail par défaut est utilisé. Vous pouvez créer un portail BYOD personnalisé. Accédez à ISE > Work Centers > BYOD > Portals and components et cliquez sur Add.

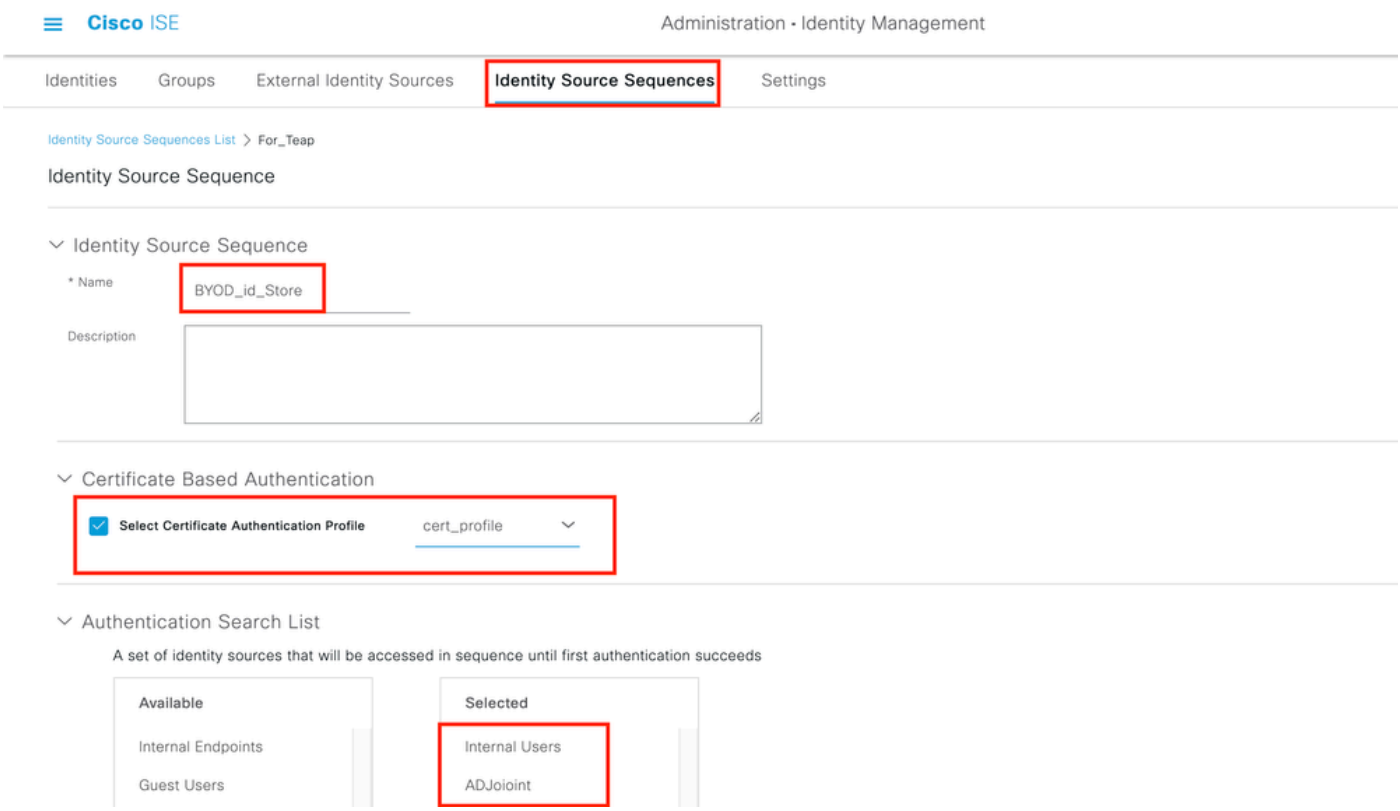


Étape 6. Créer un profil de certificat.

Accédez à ISE > Administration > External Identity Sources > Certificate Profile. Créez ici un nouveau profil de certificat ou utilisez le profil de certificat par défaut.



Étape 7. Créez une séquence source d'identité et sélectionnez le profil de certificat créé à l'étape précédente ou utilisez le profil de certificat par défaut. Ceci est nécessaire lorsque les utilisateurs exécutent EAP-TLS après l'enregistrement BYOD pour obtenir un accès complet.



Étape 8. Création d'un ensemble de stratégies, d'une stratégie d'authentification et d'une stratégie d'autorisation.

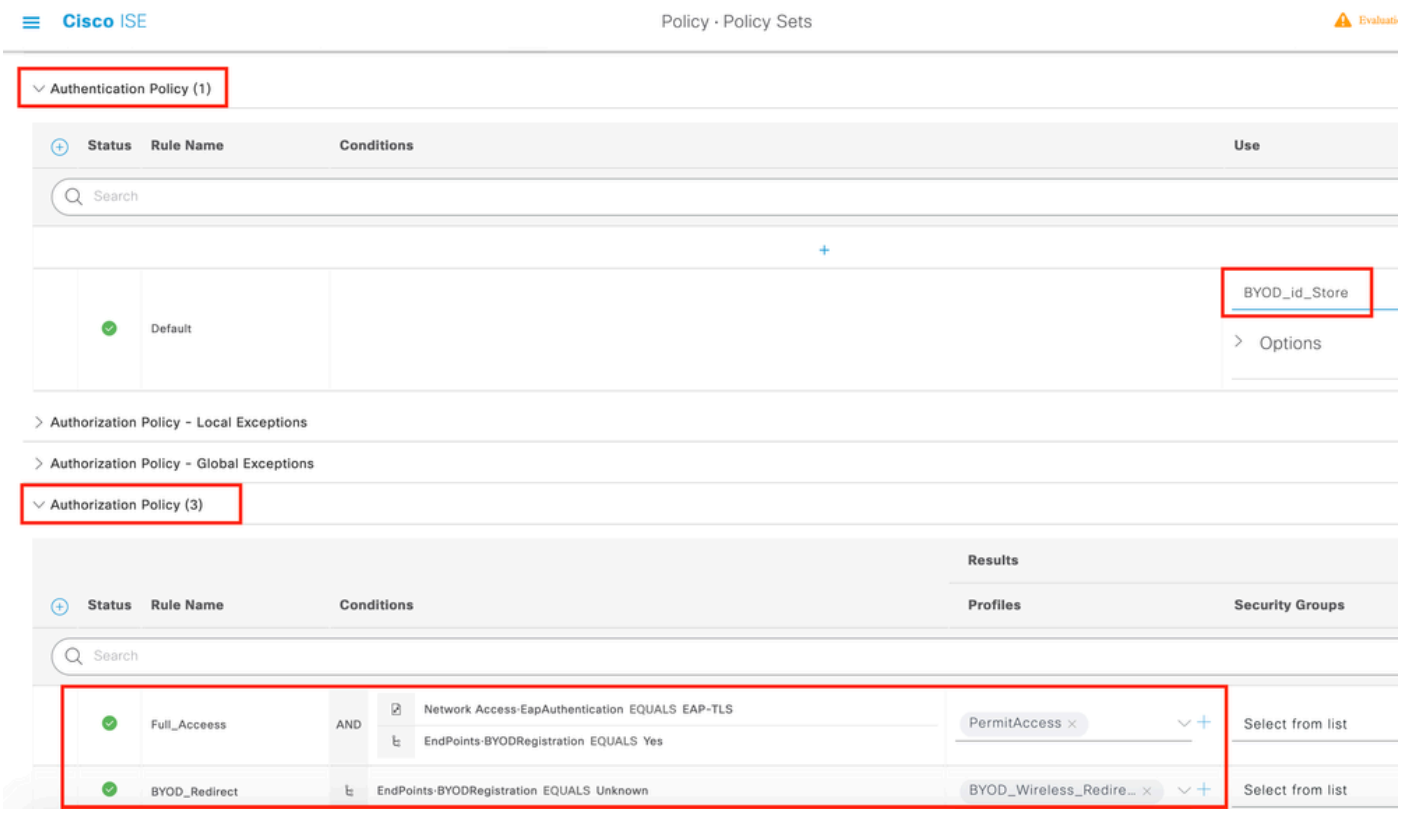
Accédez à ISE > Policy > Policy Sets. Créez un ensemble de stratégies et enregistrez-le.

Créez une stratégie d'authentification et sélectionnez la séquence source d'identité créée à l'étape précédente.

Créer une stratégie d'autorisation. Vous devez créer deux stratégies.

1. Pour les périphériques qui ne sont pas enregistrés BYOD, indiquez le profil de redirection créé à l'étape 5.

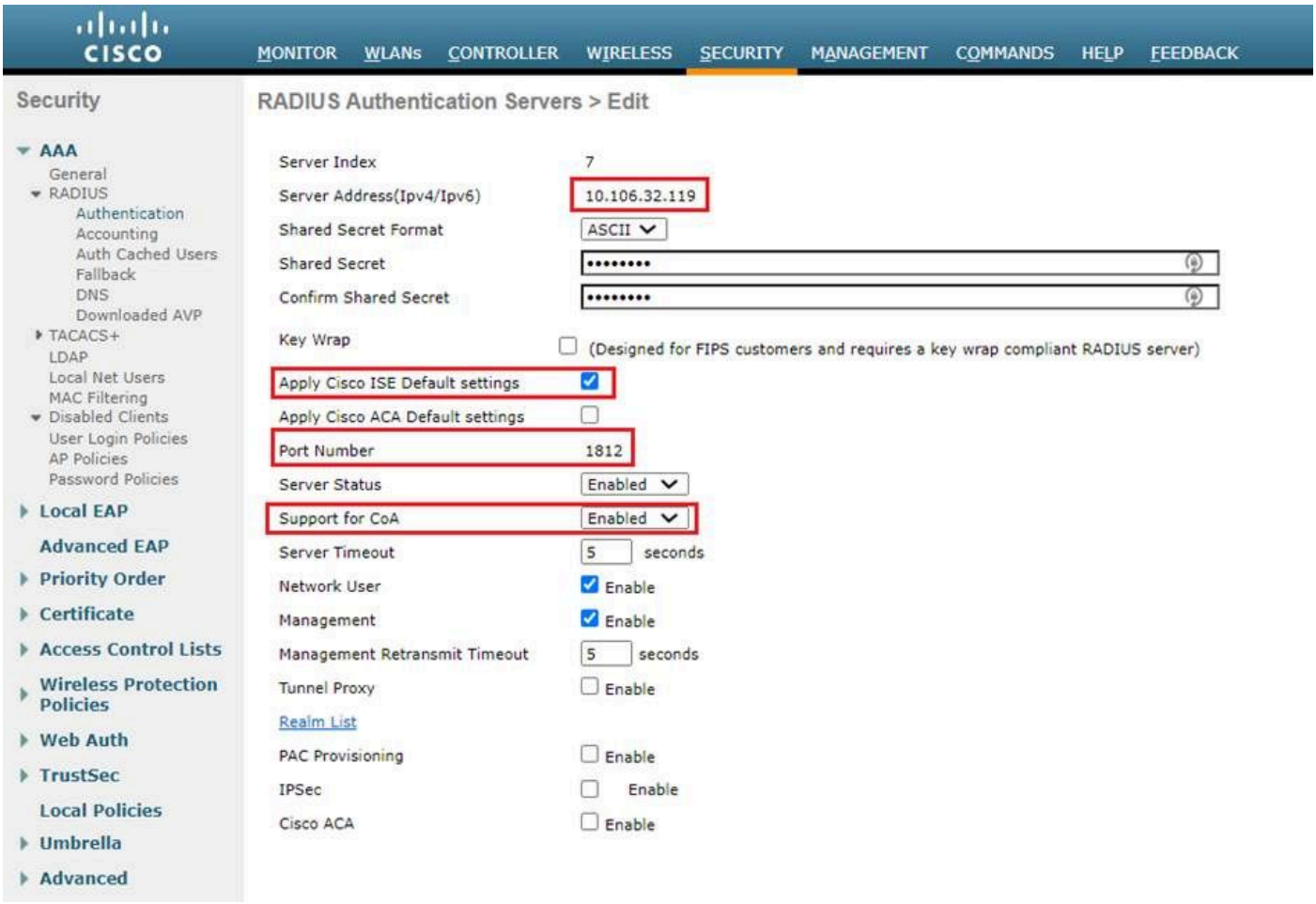
2. Pour les périphériques enregistrés BYOD et exécutant EAP-TLS, donnez un accès complet à ces périphériques.



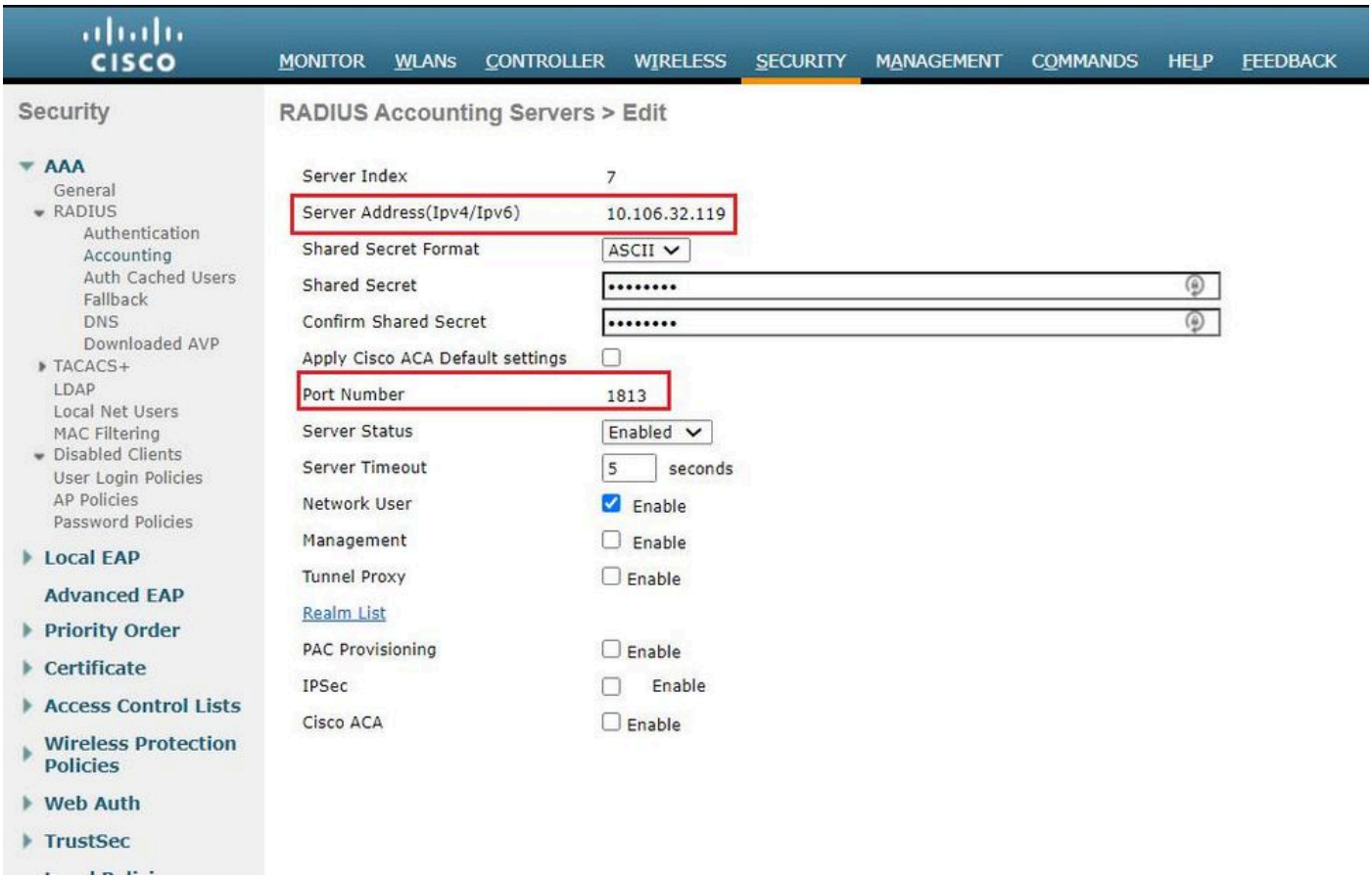
Configuration WLC

Étape 1 : configuration du serveur Radius sur le WLC

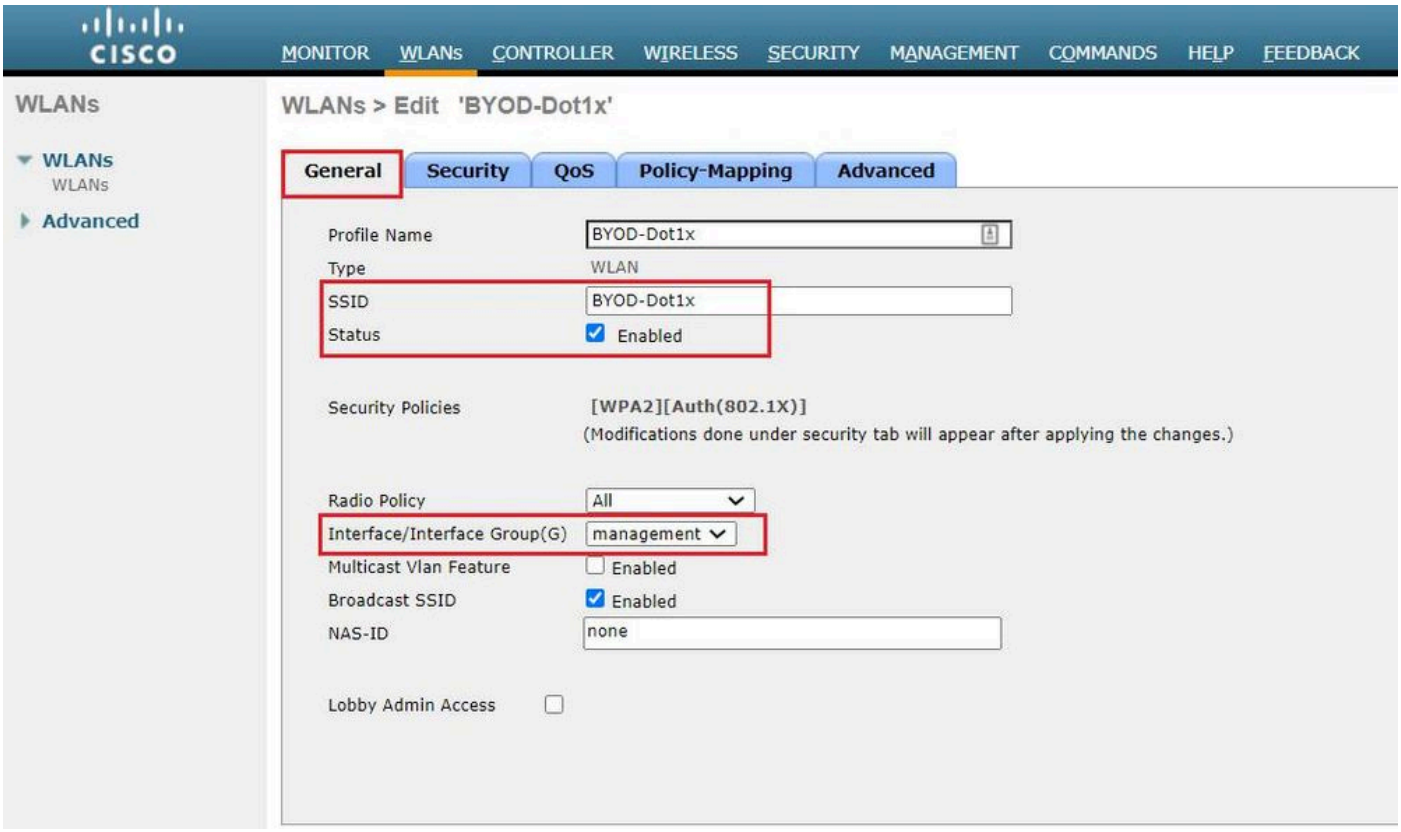
Accédez à Security > AAA > Radius > Authentication.



Accédez à Security > AAA > Radius > Accounting.



Étape 2 : configuration d’un SSID Dot1x



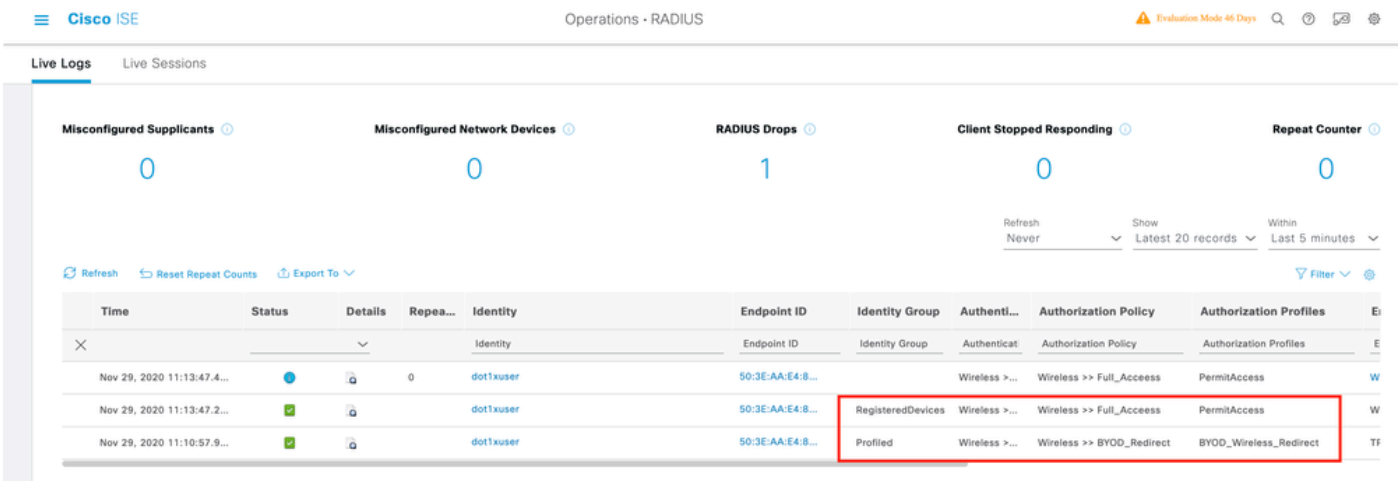
Étape 3 : configuration de la liste de contrôle d’accès Redirect pour fournir un accès limité au périphérique.

- Autoriser le trafic UDP vers DHCP et DNS (DHCP est autorisé par défaut).
- Communication avec ISE.
- Refuser tout autre trafic.

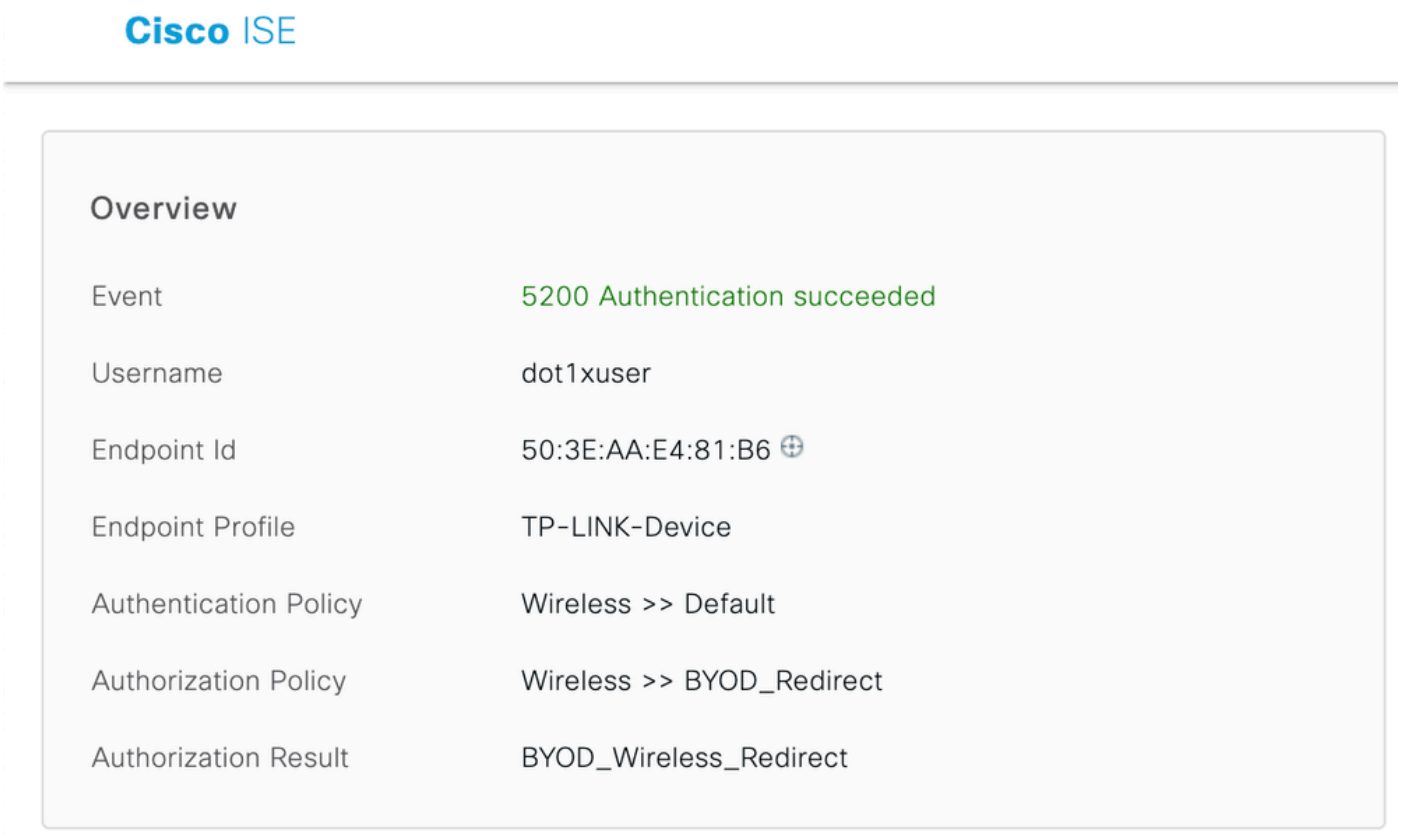
Name : BYOD-Initial (OU tout autre nom que vous avez attribué manuellement à la liste de contrôle d'accès dans le profil d'autorisation)

Vérifier

Vérification du flux d'authentification



1. Lors de la première connexion, l'utilisateur effectue l'authentification PEAP à l'aide d'un nom d'utilisateur et d'un mot de passe. Sur ISE, l'utilisateur accède à la règle de redirection BYOD-Redirect.

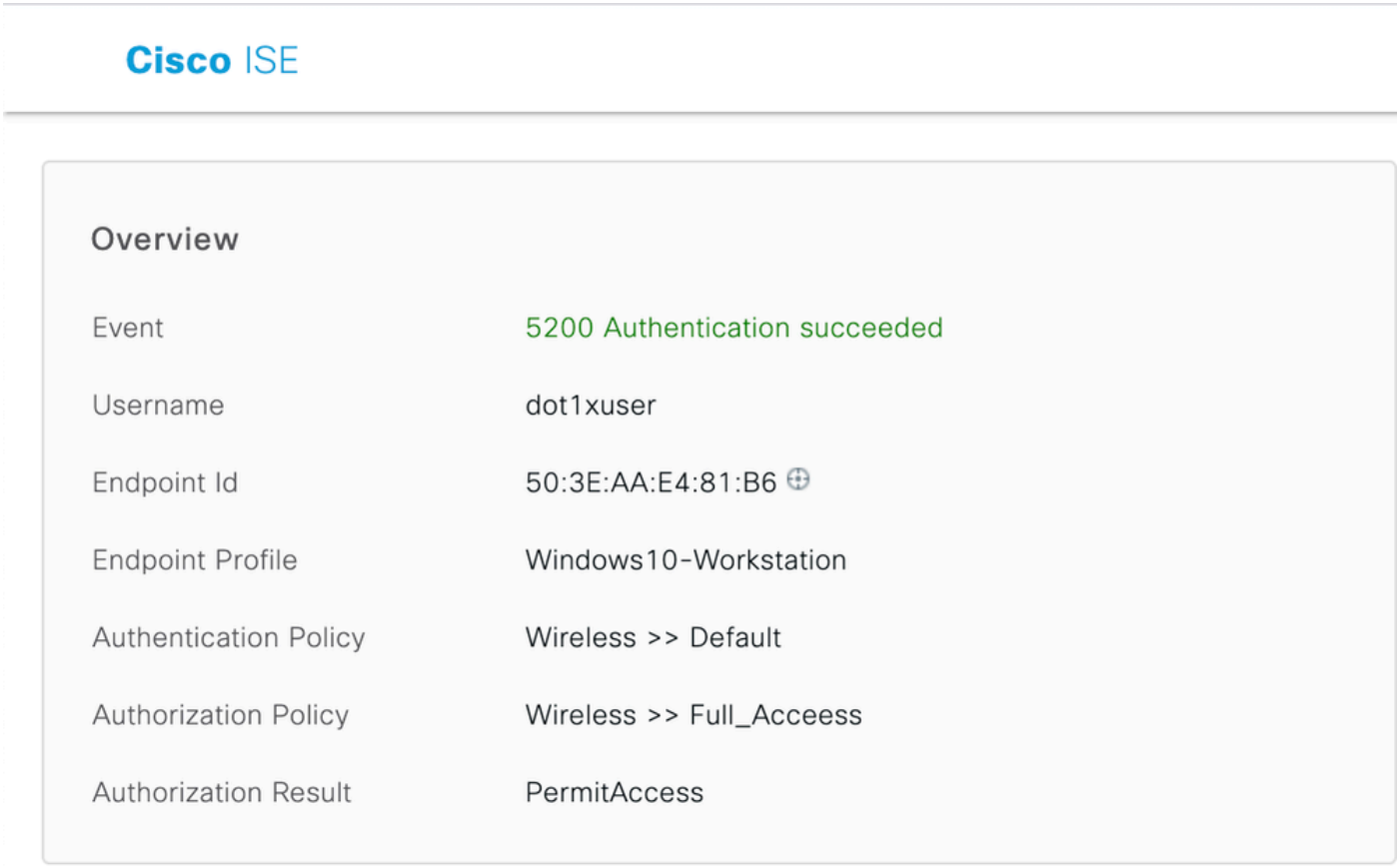


Cisco ISE

Authentication Details

Source Timestamp	2020-11-29 11:10:57.955
Received Timestamp	2020-11-29 11:10:57.955
Policy Server	isee30-primary
Event	5200 Authentication succeeded
Username	dot1xuser
User Type	User
Endpoint Id	50:3E:AA:E4:81:B6
Calling Station Id	50-3e-aa-e4-81-b6
Endpoint Profile	TP-LINK-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	0a6a21b20000009a5fc3d3ad
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	WLC1

2. Une fois l'enregistrement BYOD terminé, l'utilisateur est ajouté au périphérique enregistré et exécute maintenant EAP-TLS et obtient un accès complet.

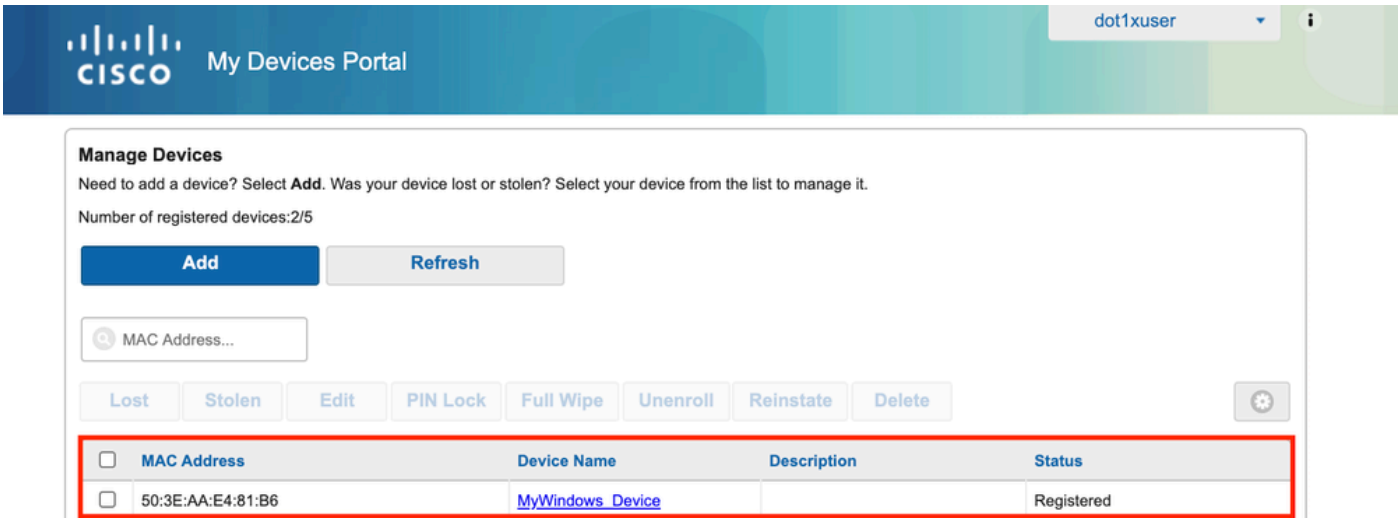


Consultez le portail Mes périphériques

Accédez au portail MyDevices et connectez-vous avec les informations d'identification. Vous pouvez voir le nom du périphérique et l'état d'enregistrement.

Vous pouvez créer une URL pour le portail MyDevices.

Accédez à ISE > Work Centers > BYOD > Portal and Components > My Devices Portal > Login Settings, puis saisissez l'URL complète.



Dépannage

Informations générales

Pour le processus BYOD, ces composants ISE doivent être activés lors du débogage sur les noeuds PSN.

scep - messages du journal scep. Fichiers journaux cibles guest.log et ise-psc.log.

client-webapp - composant responsable des messages d'infrastructure. Fichier journal cible - ise-psc.log

portal-web-action : composant responsable du traitement de la stratégie de provisionnement du client. Fichier journal cible - guest.log.

portal - tous les événements liés au portail. Fichier journal cible - guest.log

portal-session-manager -Fichiers journaux cibles - Messages de débogage relatifs à la session du portail - gues.log

ca-service- messages ca-service -Fichiers journaux cibles -caservice.log et caservice-misc.log

ca-service-cert - messages de certificat ca-service - fichiers journaux cibles - caservice.log et caservice-misc.log

admin-ca- ca-service messages admin -Target log files ise-psc.log, caservice.log et casrvice-misc.log

certprovisioningportal - messages du portail d'approvisionnement de certificats - Fichiers journaux cibles ise-psc.log

nsf- Messages associés à NSF -Fichiers journaux cibles ise-psc.log

nsf-session - Messages relatifs au cache de session - Fichiers journaux cibles ise-psc.log

runtime-AAA - Tous les événements d'exécution. Fichier journal cible - prrt-server.log .

Pour les journaux côté client :

Recherchez %temp%\spwProfileLog.txt (ex : C:\Users\<username>\AppData\Local\Temp\spwProfileLog.txt)

Analyse du journal de travail

Journaux ISE

Accès initial - Accepter avec ACL de redirection et URL de redirection pour le portail BYOD.

Port-server.log

```
Radius,2020-12-02 05:43:52,395,DEBUG,0x7f433e6b8700,cntx=0008590803,sesn=isee30-primary/392215758/699,C
```

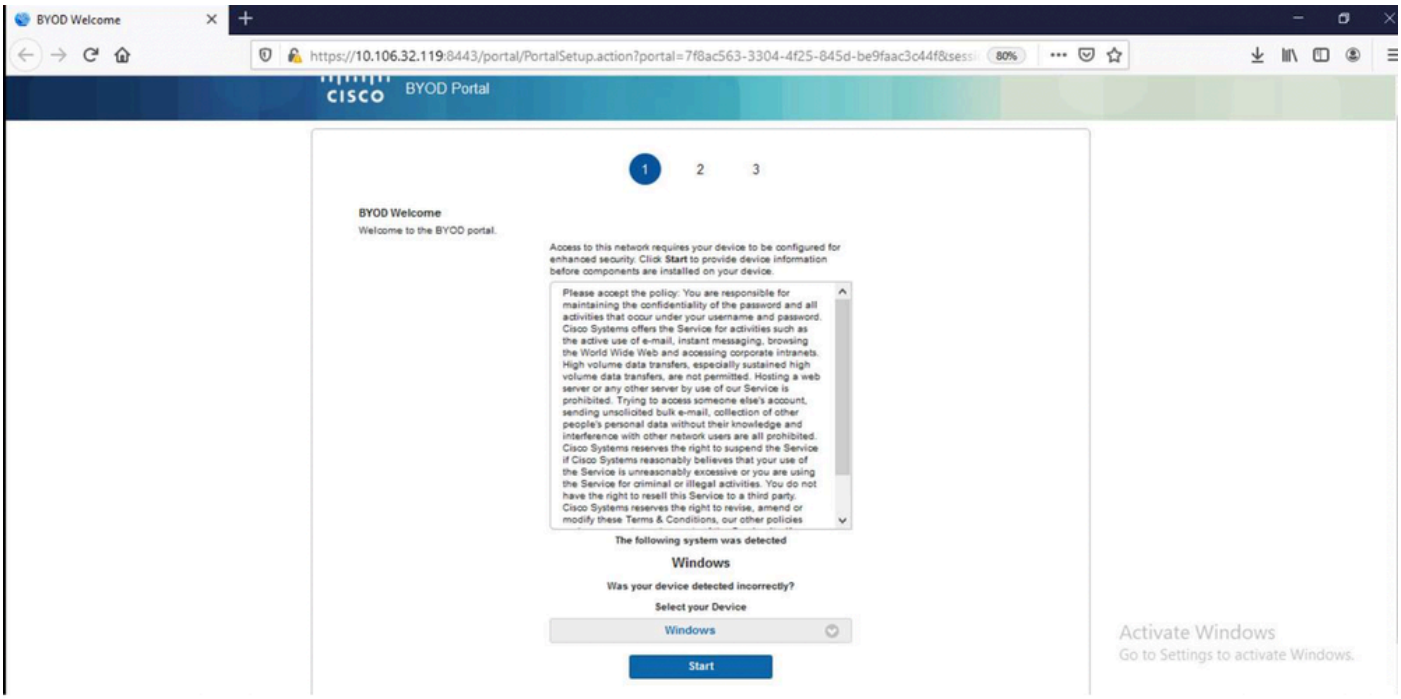
```
[1] User-Name - value: [dot1xuser]

[25] Class - value: [****]

[79] EAP-Message - value: [ñ

[80] Message-Authenticator - value: [.2{wëbÙ¨ÅþO5‹Z]

[26] cisco-av-pair - value: [url-redirect-acl=BYOD-Initial]

[26] cisco-av-pair - value: [url-redirect=https://10.106.32.119:8443/portal/gateway?sessionId=0a6a

[26] MS-MPPE-Send-Key - value: [****]

[26] MS-MPPE-Recv-Key - value: [****] ,RADIUSHandler.cpp:2216
```

Lorsqu'un utilisateur final tente de naviguer vers un site Web et a été redirigé par WLC vers l'URL de redirection ISE.

Invité.log

```
2020-12-02 05:43:58,339 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-5][] com.cisco.ise.portal.Gatewa

redirect=www.msftconnecttest.com/redirect

client_mac=null

daysToExpiry=null

ap_mac=null

switch_url=null

wlan=null

action=nsp

sessionId=0a6a21b20000009f5fc770c7

portal=7f8ac563-3304-4f25-845d-be9faac3c44f

isExpired=null

token=53a2119de6893df6c6fca25c8d6bd061


2020-12-02 05:43:58,339 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-5][] cisco.ise.portalwebaction.u


2020-12-02 05:43:58,339 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-5][] cisco.ise.portalwebaction.u


2020-12-02 05:43:58,344 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-5][] cisco.ise.portal.util.Porta
```

```
2020-12-02 05:43:58,344 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-5][] cisco.ise.portal.util.Porta
2020-12-02 05:43:58,344 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-5][] com.cisco.ise.portal.Gatewa

2020-12-02 05:43:58,355 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.c

2020-12-02 05:43:58,356 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a

2020-12-02 05:43:58,356 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a

2020-12-02 05:43:58,360 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a
2020-12-02 05:43:58,360 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a

2020-12-02 05:43:58,360 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager

2020-12-02 05:43:58,361 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager
2020-12-02 05:43:58,361 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager
2020-12-02 05:43:58,361 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager
2020-12-02 05:43:58,361 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager
2020-12-02 05:43:58,361 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager

2020-12-02 05:43:58,362 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager
2020-12-02 05:43:58,365 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager

2020-12-02 05:43:58,366 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.c
2020-12-02 05:40:35,611 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-6][] com.cisco.ise.portalSession
2020-12-02 05:40:35,611 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-6][] cisco.ise.portalwebaction.c
```



Cliquez sur Start sur la page BYOD Welcome.

```
020-12-02 05:44:01,926 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.ac
```

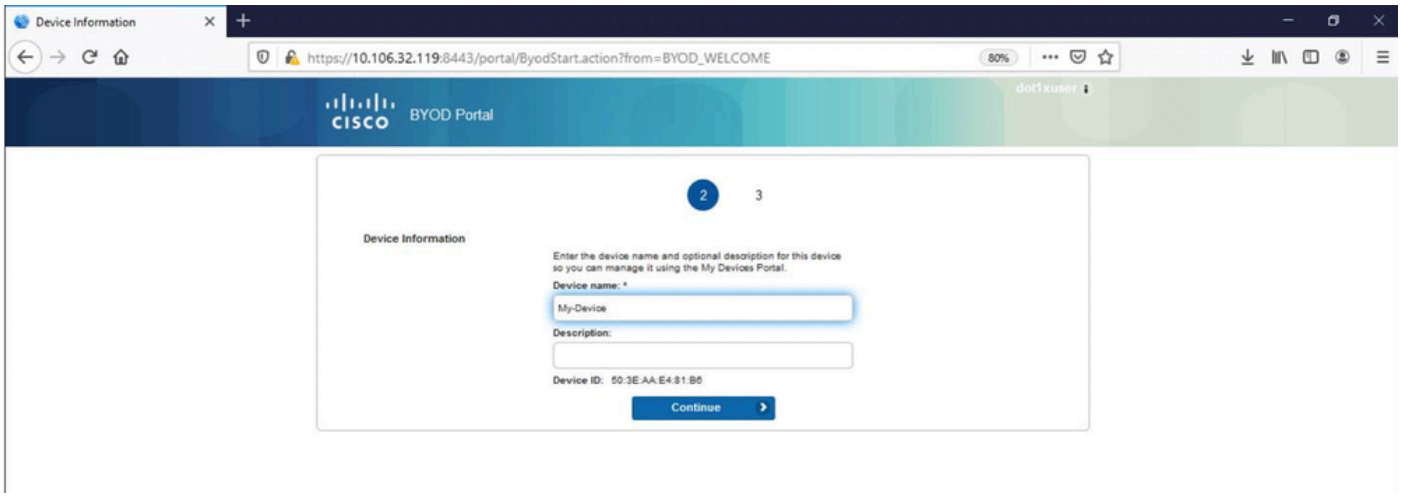
```
2020-12-02 05:44:01,926 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.c
```

À ce stade, ISE évalue si les fichiers/ressources nécessaires au BYOD sont présents ou non et se met à l'état BYOD INIT.

```
2020-12-02 05:44:01,936 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] guestaccess.flowmanager.ste
```

```
2020-12-02 05:44:01,936 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] guestaccess.flowmanager.ste
2020-12-02 05:44:01,936 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager
2020-12-02 05:44:01,936 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager
```

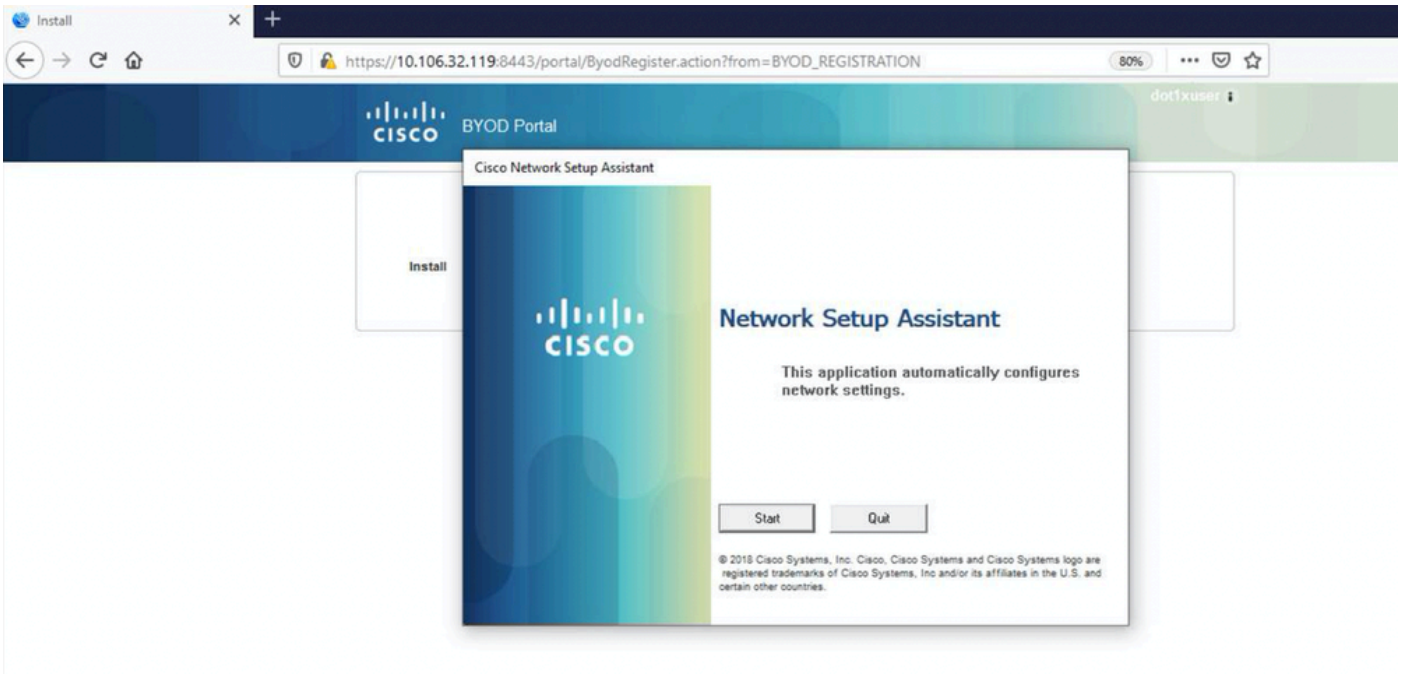
```
2020-12-02 05:44:01,950 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.c
2020-12-02 05:44:01,950 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.c
```



Entrez le nom du périphérique et cliquez sur register.

```
2020-12-02 05:44:14,682 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.a

Request Parameters:
from=BYOD_REGISTRATION
token=PZBMFBHX3FBPXT8QF98U717ILNOTD68D
device.name=My-Device
device.description=

2020-12-02 05:44:14,682 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portal.actions.By

2020-12-02 05:44:14,682 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.a
2020-12-02 05:44:14,682 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.a

2020-12-02 05:44:14,683 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cpm.guestaccess.apiservices
username= dot1xuser
idGroupID= aa13bb40-8bff-11e6-996c-525400b48521
authStoreGUID= 9273fe30-8c01-11e6-996c-525400b48521
nadAddress= 10.106.33.178
isSameDeviceRegistered = false
```

```
2020-12-02 05:44:14,900 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cpm.guestaccess.flowmanager

2020-12-02 05:44:14,902 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.c

2020-12-02 05:44:01,954 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.c

2020-12-02 05:44:14,969 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.client.provision
```



À présent, lorsque l'utilisateur clique sur Démarrer sur la NSA, un fichier nommé spwProfile.xml est temporairement créé sur le client qui copie le contenu de Cisco-ISE-NSP.xml téléchargé sur le port TCP 8905.

Invité.log

```
2020-12-02 05:45:03,275 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet
2020-12-02 05:45:03,275 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet

2020-12-02 05:45:03,308 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet
2020-12-02 05:45:03,308 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet
```

WirelessNSP

2.0

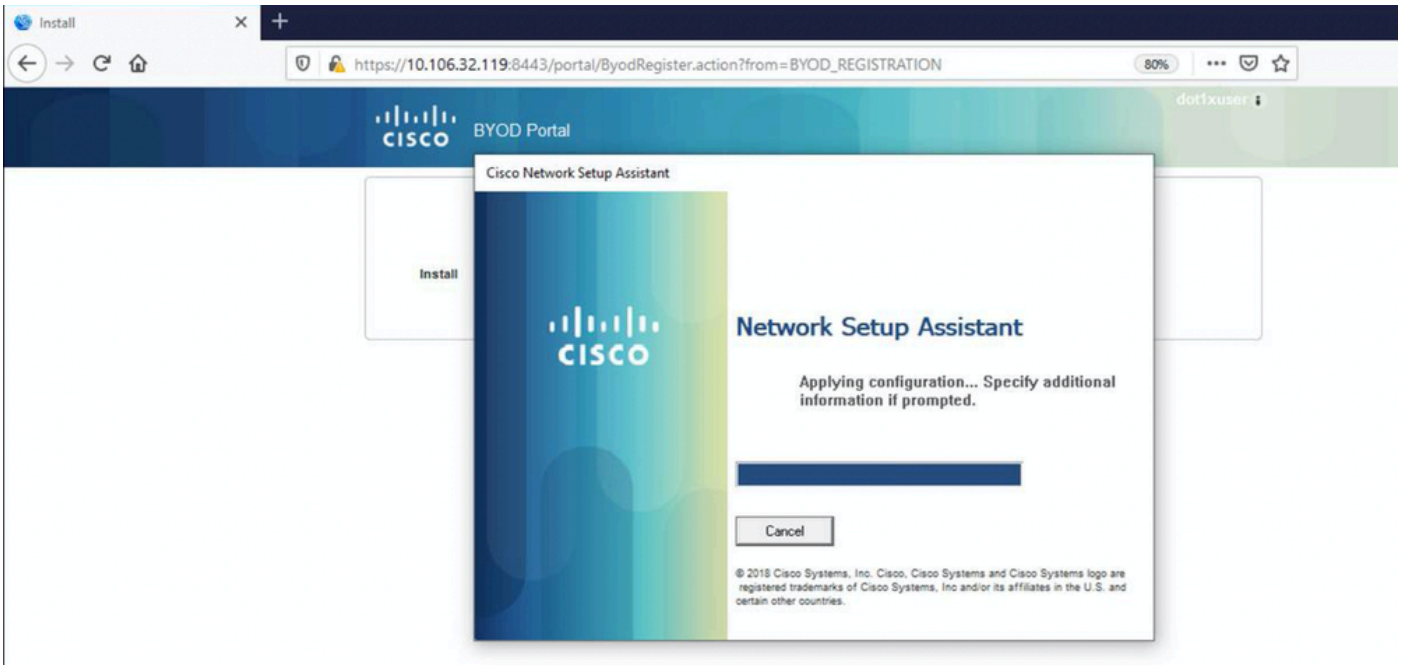
ALL

wireless

BYOD-Dot1x

```
            WPA2

             TLS

             false

           e2c32ce0-313d-11eb-b19e-e60300a810d5

---output omitted---

2020-12-02 05:45:03,310 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet
```

Après avoir lu le contenu du fichier spwProfile.xml, NSA configure le profil réseau et génère un CSR, puis l'envoie à l'ISE pour obtenir un certificat à l'aide du client PKI d'URL



ise-psc.log

```
2020-12-02 05:45:11,298 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.cpm.provisioning.cert

2020-12-02 05:45:11,331 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.cpm.provisioning.cert

2020-12-02 05:45:11,331 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.cpm.provisioning.cert

2020-12-02 05:45:11,331 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.cpm.scep.util.ScepUti
2020-12-02 05:45:11,331 INFO   [https-jsse-nio-10.106.32.119-8443-exec-1][] com.cisco.cpm.scep.ScepCert
2020-12-02 05:45:11,332 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessag
2020-12-02 05:45:11,332 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkcsPkiEn
2020-12-02 05:45:11,333 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessag
2020-12-02 05:45:11,333 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessag
2020-12-02 05:45:11,334 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessag
```

ca-service.log

```
2020-12-02 05:45:11,379 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
version      [0]
```

```
subject      [C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser]
---output omitted---
2020-12-02 05:45:11,379 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
2020-12-02 05:45:11,379 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
```

caservice-misc.log

```
2020-12-02 05:45:11,380 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
2020-12-02 05:45:11,380 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
```

caservice.log

```
2020-12-02 05:45:11,380 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e

2020-12-02 05:45:11,380 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
    1: 50-3E-AA-E4-81-B6

2020-12-02 05:45:11,380 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
2020-12-02 05:45:11,380 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e

2020-12-02 05:45:11,395 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
2020-12-02 05:45:11,395 INFO   [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
class [com.cisco.cpm.caservice.CaResultHolder] [1472377777]: result: [CA_OK]
subject      [CN=dot1xuser, OU=tac, O=cisco, L=bangalore, ST=Karnataka, C=IN]
version      [3]
serial       [0x518fa73a-4c654df2-82ffdb02-6080de8d]
validity     [after [2020-12-01T05:45:11+0000] before [2030-11-27T07:35:10+0000]]
keyUsages    [ digitalSignature nonRepudiation keyEncipherment ]
```

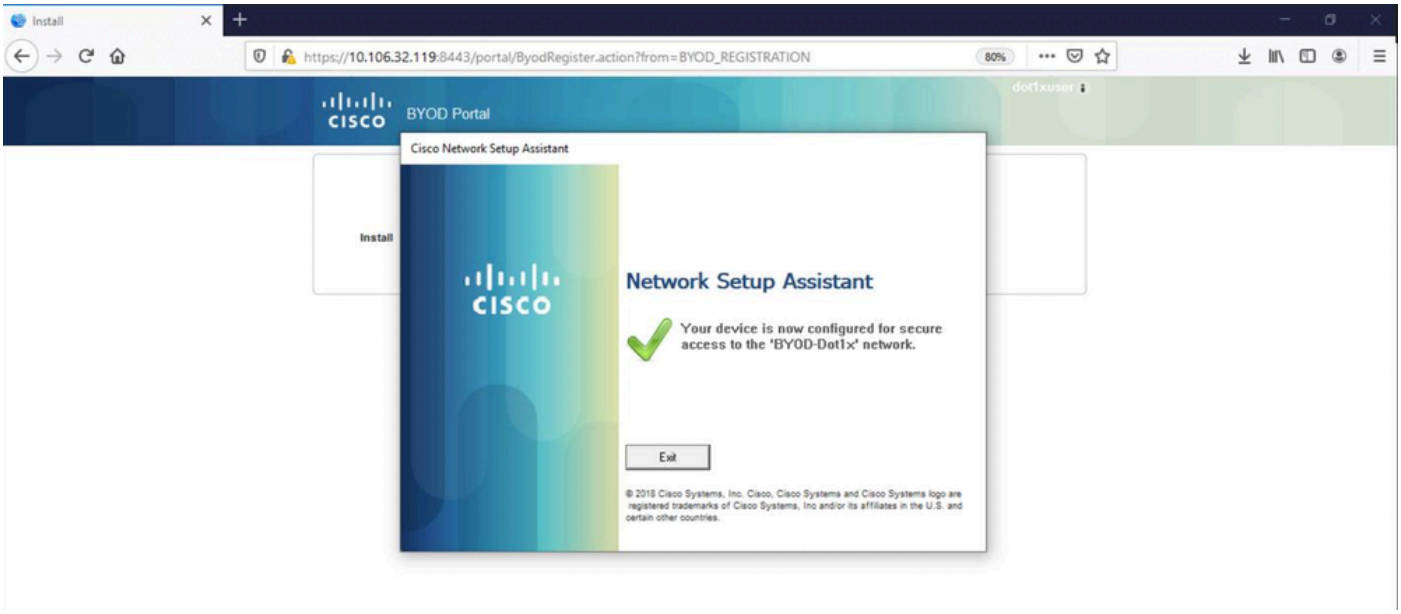
ise-psc.log

```
2020-12-02 05:45:11,407 DEBUG  [AsyncHttpClient-15-9][] org.jscep.message.PkiMessageDecoder -::::- Veri
```

caservice.log

```
2020-12-02 05:45:11,570 DEBUG  [Infra-CAServiceUtil-Thread][] cisco.cpm.caservice.util.CaServiceUtil -:
```

ise-psc.log




```
2020-12-02 05:45:13,381 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.provisioning.cer
2020-12-02 05:45:13,381 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCer
2020-12-02 05:45:13,385 INFO   [https-jsse-nio-10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCer
2020-12-02 05:45:13,596 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.provisioning.cer
```

Après l'installation du certificat, les clients lancent une autre authentification à l'aide d'EAP-TLS et obtiennent un accès complet.

prt-server.log

```
Eap,2020-12-02 05:46:57,175,INFO ,0x7f433e6b8700,cntx=0008591342,sesn=isee30-primary/392215758/701,CPMS
,EapParser.cpp:150
```

```
Radius,2020-12-02 05:46:57,435,DEBUG,0x7f433e3b5700,cntx=0008591362,sesn=isee30-primary/392215758/701,C
     [1] User-Name - value: [dot1xuser]
     [25] Class - value: [****]
     [79] EAP-Message - value: [E
     [80] Message-Authenticator - value: [Ù(ØyËöžö|kÔ,¸}]
    [26] MS-MPPE-Send-Key - value: [****]
    [26] MS-MPPE-Recv-Key - value: [****] ,RADIUSHandler.cpp:2216
```

Journaux client (journaux spw)

Le client lance le téléchargement du profil.

```
[Mon Nov 30 03:34:27 2020] Downloading profile configuration...
[Mon Nov 30 03:34:27 2020] Discovering ISE using default gateway
[Mon Nov 30 03:34:27 2020] Identifying wired and wireless network interfaces, total active interfaces:
[Mon Nov 30 03:34:27 2020] Network interface - mac:50-3E-AA-E4-81-B6, name: Wi-Fi 2, type: unknown
[Mon Nov 30 03:34:27 2020] Identified default gateway: 10.106.33.1
[Mon Nov 30 03:34:27 2020] Identified default gateway: 10.106.33.1, mac address: 50-3E-AA-E4-81-B6
[Mon Nov 30 03:34:27 2020] DiscoverISE - start
[Mon Nov 30 03:34:27 2020] DiscoverISE input parameter : strUrl [http://10.106.33.1/auth/discovery]
[Mon Nov 30 03:34:27 2020] [HTTPConnection] CrackUrl: host = 10.106.33.1, path = /auth/discovery, user =
[Mon Nov 30 03:34:27 2020] [HTTPConnection] HttpSendRequest: header = Accept: */*
 headerLength = 12 data =  dataLength = 0
[Mon Nov 30 03:34:27 2020]  HTTP Response header: [HTTP/1.1 200 OK

Location: https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009c5fc4fb5e&portal=7f8ac563-

[Mon Nov 30 03:34:36 2020] [HTTPConnection] CrackUrl: host = 10.106.32.119, path = /auth/provisioning/d

Mon Nov 30 03:34:36 2020] parsing wireless connection setting
[Mon Nov 30 03:34:36 2020] Certificate template: [keytype:RSA, keysize:2048, subject:OU=tac;O=cisco;L=b
[Mon Nov 30 03:34:36 2020] set ChallengePwd
```

Le client vérifie si le service WLAN est en cours d'exécution.

```
[Mon Nov 30 03:34:36 2020] WirelessProfile::StartWLanSvc - Start
[Mon Nov 30 03:34:36 2020] Wlansvc service is in Auto mode ...
[Mon Nov 30 03:34:36 2020] Wlansvc is running in auto mode...
[Mon Nov 30 03:34:36 2020] WirelessProfile::StartWLanSvc - End

[Mon Nov 30 03:34:36 2020] Wireless interface 1 - Desc: [TP-Link Wireless USB Adapter], Guid: [{65E78DD
[Mon Nov 30 03:34:36 2020] Wireless interface - Mac address: 50-3E-AA-E4-81-B6
[Mon Nov 30 03:34:36 2020] Identifying wired and wireless interfaces...
[Mon Nov 30 03:34:36 2020] Found wireless interface - [ name:Wi-Fi 2, mac address:50-3E-AA-E4-81-B6]
[Mon Nov 30 03:34:36 2020] Wireless interface [Wi-Fi 2] will be configured...
[Mon Nov 30 03:34:37 2020] Host - [ name:DESKTOP-965F94U, mac addresses:50-3E-AA-E4-81-B6]
```

Le client commence à appliquer le profil.

```
[Mon Nov 30 03:34:37 2020] ApplyProfile - Start...
[Mon Nov 30 03:34:37 2020] User Id: dot1xuser, sessionid: 0a6a21b20000009c5fc4fb5e, Mac: 50-3E-AA-E4-81
[Mon Nov 30 03:34:37 2020] number of wireless connections to configure: 1
[Mon Nov 30 03:34:37 2020] starting configuration for SSID : [BYOD-Dot1x]
[Mon Nov 30 03:34:37 2020] applying certificate for ssid [BYOD-Dot1x]
```

Certificat d'installation client.

```
[Mon Nov 30 03:34:37 2020] ApplyCert - Start...
[Mon Nov 30 03:34:37 2020] using ChallengePwd
[Mon Nov 30 03:34:37 2020] creating certificate with subject = dot1xuser and subjectSuffix = OU=tac;O=c
[Mon Nov 30 03:34:38 2020] Self signed certificate
```

```
[Mon Nov 30 03:34:44 2020] Installed [isee30-primary.anshsinh.local, hash: 5b a2 08 1e 17 cb 73 5f  ba
] as rootCA
[Mon Nov 30 03:34:44 2020] Installed CA cert for authMode machineOrUser - Success

Certificate is downloaded . Omitted for brevity -

[Mon Nov 30 03:34:50 2020] creating response file name C:\Users\admin\AppData\Local\Temp\response.cer
[Mon Nov 30 03:34:50 2020] Certificate issued - successfully
[Mon Nov 30 03:34:50 2020] ScepWrapper::InstallCert start
[Mon Nov 30 03:34:50 2020] ScepWrapper::InstallCert: Reading scep response file  [C:\Users\admin\AppDat
[Mon Nov 30 03:34:51 2020] ScepWrapper::InstallCert GetCertHash -- return val 1
[Mon Nov 30 03:34:51 2020] ScepWrapper::InstallCert end
[Mon Nov 30 03:34:51 2020] ApplyCert - End...
[Mon Nov 30 03:34:51 2020] applied user certificate using template id e2c32ce0-313d-11eb-b19e-e60300a81
```

ISE configure le profil sans fil

```
[Mon Nov 30 03:34:51 2020] Configuring wireless profiles...
[Mon Nov 30 03:34:51 2020] Configuring ssid [BYOD-Dot1x]
[Mon Nov 30 03:34:51 2020] WirelessProfile::SetWirelessProfile - Start
[Mon Nov 30 03:34:51 2020] TLS - TrustedRootCA Hash: [ 5b a2 08 1e 17 cb 73 5f  ba 5b 9f a2 2d 3b fc d2
```

Profil

BYOD-Dot1x

BYOD-Dot1x

true

ESS

auto

false

WPA2

AES

true

true

user

13

0

13

true

false

5b a2 08 1e 17 cb 73 5f ba 5b 9f a2 2d 3b fc d2 86 0d a5 9b

false

```
Wireless interface succesfully initiated, continuing to configure SSID
[Mon Nov 30 03:34:51 2020] Currently connected to SSID: [BYOD-Dot1x]

[Mon Nov 30 03:34:51 2020] Wireless profile: [BYOD-Dot1x] configured successfully
[Mon Nov 30 03:34:51 2020] Connect to SSID
[Mon Nov 30 03:34:51 2020] Successfully connected profile: [BYOD-Dot1x]
[Mon Nov 30 03:34:51 2020] WirelessProfile::SetWirelessProfile. - End

[Mon Nov 30 03:35:21 2020] WirelessProfile::IsSingleSSID - Start
[Mon Nov 30 03:35:21 2020] Currently connected to SSID: [BYOD-Dot1x], profile ssid: [BYOD-Dot1x], Singl
[Mon Nov 30 03:35:21 2020] WirelessProfile::IsSingleSSID - End

[Mon Nov 30 03:36:07 2020] Device configured successfully.
```

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.