

Configuration du BYOD sans fil SSID unique sous Windows et ISE

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Théorie](#)

[Configurer](#)

[Configuration ISE](#)

[Configuration WLC](#)

[Vérifier](#)

[Vérification du flux d'authentification](#)

[Consultez le portail Mes périphériques](#)

[Dépannage](#)

[Informations générales](#)

[Analyse du journal de travail](#)

[Journaux ISE](#)

[Journaux client \(journaux spw\)](#)

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.

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Edit Certificate Template

Certificate Management

Certificate Authority

- Overview
- Issued Certificates
- Certificate Authority Certifica...
- Internal CA Settings
- Certificate Templates**
- External CA Settings

* Name: BYOD_Certificate_template

Description:

Subject:

Common Name (CN): \$UserName\$ ⓘ

Organizational Unit (OU): tac

Organization (O): cisco

City (L): bangalore

State (ST): Karnataka

Country (C): IN

Subject Alternative Name (SAN):

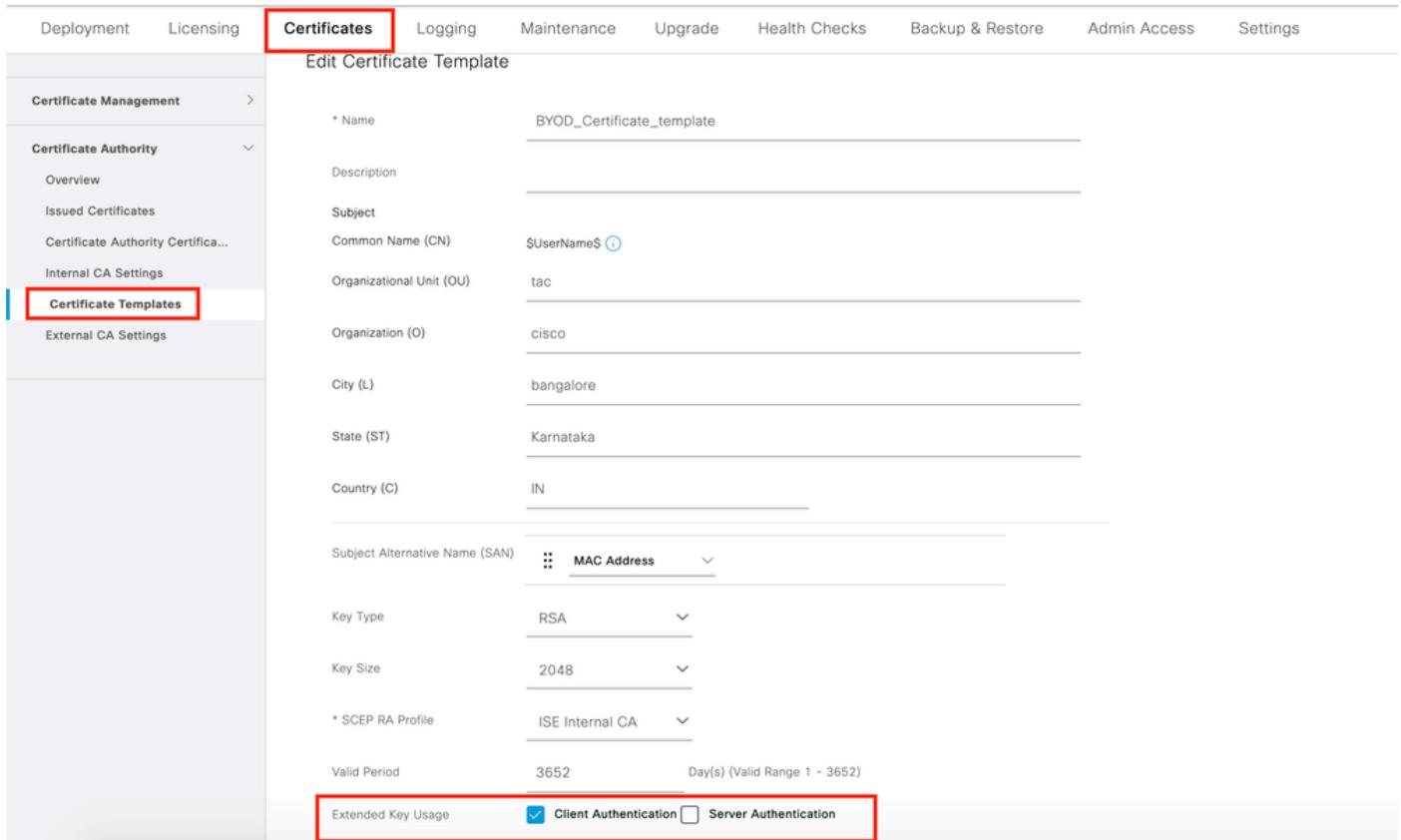
Key Type: RSA

Key Size: 2048

* SCEP RA Profile: ISE Internal CA

Valid Period: 3652 Day(s) (Valid Range 1 - 3652)

Extended Key Usage: Client Authentication Server Authentication



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 Suplicant 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.

Overview	Identities	Identity Groups	Network Devices	Ext Id Sources	Client Provisioning	Portals & Components	Policy Elements	Policy Sets	Reports	More																								
Client Provisioning Policy Resources <table border="1"> <tr> <td>* Name</td> <td>WirelessNSP</td> </tr> <tr> <td>Description</td> <td></td> </tr> <tr> <td>Operating System *</td> <td>ALL</td> </tr> <tr> <td colspan="2"> Wireless Profile Multiple SSIDs can be configured, Proxy Auto-Config File URL will be used if no Proxy Auto-Config File URL is specified. </td> </tr> <tr> <td>SSID Name *</td> <td>BYOD-Dot1x</td> </tr> <tr> <td>Proxy Auto-Config File URL</td> <td></td> </tr> <tr> <td>Proxy Host/IP</td> <td></td> </tr> <tr> <td>Proxy Port</td> <td></td> </tr> <tr> <td>Security *</td> <td>WPA2 Enterprise</td> </tr> <tr> <td>Allowed Protocol *</td> <td>TLS</td> </tr> <tr> <td>Certificate Template</td> <td>BYOD_Certificate_template</td> </tr> <tr> <td colspan="2"> Optional Settings Windows Settings Authentication Mode User </td> </tr> </table>											* Name	WirelessNSP	Description		Operating System *	ALL	Wireless Profile Multiple SSIDs can be configured, Proxy Auto-Config File URL will be used if no Proxy Auto-Config File URL is specified.		SSID Name *	BYOD-Dot1x	Proxy Auto-Config File URL		Proxy Host/IP		Proxy Port		Security *	WPA2 Enterprise	Allowed Protocol *	TLS	Certificate Template	BYOD_Certificate_template	Optional Settings Windows Settings Authentication Mode User	
* Name	WirelessNSP																																	
Description																																		
Operating System *	ALL																																	
Wireless Profile Multiple SSIDs can be configured, Proxy Auto-Config File URL will be used if no Proxy Auto-Config File URL is specified.																																		
SSID Name *	BYOD-Dot1x																																	
Proxy Auto-Config File URL																																		
Proxy Host/IP																																		
Proxy Port																																		
Security *	WPA2 Enterprise																																	
Allowed Protocol *	TLS																																	
Certificate Template	BYOD_Certificate_template																																	
Optional Settings Windows Settings Authentication Mode User																																		

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.

Overview	Identities	Identity Groups	Network Devices	Ext Id Sources	Client Provisioning	Portals & Components	Policy Elements	Policy Sets	Reports	More																									
Client Provisioning Policy Resources <p>Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation: For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package. For Native Suplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.</p> <table border="1"> <thead> <tr> <th>Rule Name</th> <th>Identity Groups</th> <th>Operating Systems</th> <th>Other Conditions</th> <th>Results</th> </tr> </thead> <tbody> <tr> <td>IOS</td> <td>If Any</td> <td>and Apple iOS All</td> <td>and Condition(s)</td> <td>then Cisco-ISE-NSP</td> </tr> <tr> <td>Android</td> <td>If Any</td> <td>and Android</td> <td>and Condition(s)</td> <td>then Cisco-ISE-NSP</td> </tr> <tr> <td>Windows</td> <td>If Any</td> <td>and Windows All</td> <td>and Condition(s)</td> <td>then WinSPWizard 3.0.0.2 And WirelessNSP</td> </tr> <tr> <td>MAC OS</td> <td>If Any</td> <td>and Mac OSX</td> <td>and Condition(s)</td> <td>then CiscoTemporNIAgentOSX 4.8.00176 And MacOsXSPWizard</td> </tr> </tbody> </table>											Rule Name	Identity Groups	Operating Systems	Other Conditions	Results	IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP	Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP	Windows	If Any	and Windows All	and Condition(s)	then WinSPWizard 3.0.0.2 And WirelessNSP	MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporNIAgentOSX 4.8.00176 And MacOsXSPWizard
Rule Name	Identity Groups	Operating Systems	Other Conditions	Results																															
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP																															
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP																															
Windows	If Any	and Windows All	and Condition(s)	then WinSPWizard 3.0.0.2 And WirelessNSP																															
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporNIAgentOSX 4.8.00176 And MacOsXSPWizard																															

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 Suplicant 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.

The screenshot shows the 'Results' tab selected in the 'Authorization Profiles' section. The profile is named 'BYOD_Wireless_Redirect'. The 'Access Type' is set to 'ACCESS_ACCEPT'. Under 'Network Device Profile', 'Cisco' is selected. In the 'Common Tasks' section, the 'Web Redirection (CWA, MDM, NSP, CPP)' checkbox is checked, and the 'Value' dropdown is set to 'BYOD Portal (default)'. A red box highlights the 'Web Redirection' checkbox and the 'Value' dropdown.

Étape 6. Créez 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.

The screenshot shows the 'External Identity Sources' tab selected in the 'Administration · Identity Management' interface. On the left, under 'External Identity Sources', 'Certificate Authentication F' is expanded, showing 'cert_profile' selected. On the right, the 'Certificate Authentication Profile' configuration page is displayed. The 'Name' field is set to 'cert_profile'. The 'Identity Store' dropdown is set to '[not applicable]'. Under 'Use Identity From', the 'Certificate Attribute' radio button is selected, with 'Subject - Common Name' chosen. Under 'Match Client Certificate Against Certificate In Identity Store', the 'Never' radio button is selected. A red box highlights the 'cert_profile' name in the 'Name' field.

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.

[Identities](#) [Groups](#) [External Identity Sources](#) [Identity Source Sequences](#) [Settings](#)[Identity Source Sequences List > For_Teap](#)

Identity Source Sequence

Identity Source Sequence

* Name

BYOD_id_Store

Description

Certificate Based Authentication

 Select Certificate Authentication Profile

cert_profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available

Internal Endpoints

Guest Users

Selected

Internal Users

ADJoinoint

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.

Authentication Policy (1)

Status	Rule Name	Conditions	Use
<input type="checkbox"/>	Default		<input type="checkbox"/> BYOD_id_Store Options

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

Results			Profiles	Security Groups
Status	Rule Name	Conditions		
<input type="checkbox"/>	Full_Access	AND <input type="checkbox"/> Network Access-EapAuthentication EQUALS EAP-TLS <input type="checkbox"/> EndPoints-BYODRegistration EQUALS Yes	PermitAccess	<input type="checkbox"/> Select from list
<input type="checkbox"/>	BYOD_Redirect	<input type="checkbox"/> EndPoints-BYODRegistration EQUALS Unknown	BYOD_Wireless_Redire...	<input type="checkbox"/> Select from list

Configuration WLC

Étape 1 : configuration du serveur Radius sur le WLC

Accédez à Security > AAA > Radius > Authentication.

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Auth Cached Users
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
 - Advanced EAP
 - Priority Order
 - Certificate
 - Access Control Lists
 - Wireless Protection Policies
 - Web Auth
 - TrustSec
 - Local Policies
 - Umbrella
 - Advanced

RADIUS Authentication Servers > Edit

Server Index	7
Server Address(Ipv4/Ipv6)	10.106.32.119
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Apply Cisco ISE Default settings	<input checked="" type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Port Number	1812
Server Status	Enabled
Support for CoA	Enabled
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
Realm List	
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Accédez à Security > AAA > Radius > Accounting.

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Auth Cached Users
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
 - Advanced EAP
 - Priority Order
 - Certificate
 - Access Control Lists
 - Wireless Protection Policies
 - Web Auth
 - TrustSec
 - Local Policies
 - Umbrella
 - Advanced

RADIUS Accounting Servers > Edit

Server Index	7
Server Address(Ipv4/Ipv6)	10.106.32.119
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Apply Cisco ACA Default settings	<input type="checkbox"/>
Port Number	1813
Server Status	Enabled
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable
Tunnel Proxy	<input type="checkbox"/> Enable
Realm List	
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Étape 2 : configuration d'un SSID Dot1x

WLANS > Edit 'BYOD-Dot1x'

General **Security** **QoS** **Policy-Mapping** **Advanced**

Profile Name	BYOD-Dot1x
Type	WLAN
SSID	BYOD-Dot1x
Status	<input checked="" type="checkbox"/> Enabled

Security Policies: [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All
Interface/Interface Group(G): management

Multicast Vlan Feature: Enabled
Broadcast SSID: Enabled
NAS-ID: none

Lobby Admin Access:

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)

Access Control Lists > Edit

General

Access List Name	BYOD-Initial
Deny Counters	0

Access Control Lists

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	Any	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	10.106.32.119 / 255.255.255.255	Any	Any	Any	Any	Any	0
3	Permit	10.106.32.119 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
4	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

Vérifier

Vérification du flux d'authentification

The screenshot shows the Cisco ISE Operations - RADIUS dashboard. At the top, there are five summary metrics: Misconfigured Suplicants (0), Misconfigured Network Devices (0), RADIUS Drops (1), Client Stopped Responding (0), and Repeat Counter (0). Below these are refresh and reset buttons, and dropdown filters for 'Show' (Never, Latest 20 records, Within Last 5 minutes) and 'Filter'.

The main area displays a table of live logs. The columns include Time, Status, Details, Repea..., Identity, Endpoint ID, Identity Group, Authenti..., Authorization Policy, Authorization Profiles, and a timestamp column. Three log entries are listed:

Time	Status	Details	Repea...	Identity	Endpoint ID	Identity Group	Authenti...	Authorization Policy	Authorization Profiles	Timestamp
Nov 29, 2020 11:13:47.4...	Success	dot1xuser	0	dot1xuser	50:3E:AA:E4:8...	Wireless >...	Wireless >> Full_Access	PermitAccess	W	Nov 29, 2020 11:13:47.4...
Nov 29, 2020 11:13:47.2...	Success	dot1xuser	0	dot1xuser	50:3E:AA:E4:8...	RegisteredDevices	Wireless >...	Wireless >> Full_Access	PermitAccess	W
Nov 29, 2020 11:10:57.9...	Success	dot1xuser	0	dot1xuser	50:3E:AA:E4:8...	Profiled	Wireless >...	Wireless >> BYOD_Redirect	BYOD_Wireless_Redirect	TF

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

Overview

Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Endpoint Profile	TP-LINK-Device
Authentication Policy	Wireless >> Default
Authorization Policy	Wireless >> BYOD_Redirect
Authorization Result	BYOD_Wireless_Redirect

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.

Overview

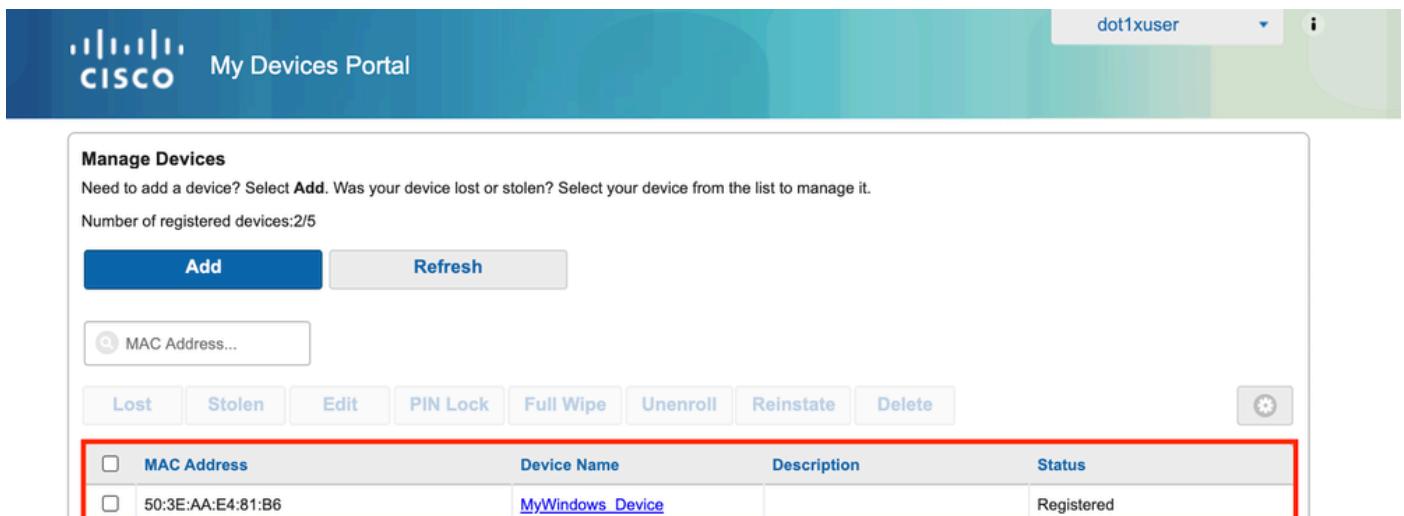
Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6 
Endpoint Profile	Windows10-Workstation
Authentication Policy	Wireless >> Default
Authorization Policy	Wireless >> Full_Acceess
Authorization Result	PermitAccess

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.



The screenshot shows the Cisco My Devices Portal interface. At the top, there's a navigation bar with the Cisco logo and a dropdown menu set to "dot1xuser". Below the header, a search bar contains "My Devices Portal". The main area is titled "Manage Devices" and includes a sub-instruction: "Need to add a device? Select Add. Was your device lost or stolen? Select your device from the list to manage it." It displays "Number of registered devices: 2/5". There are two buttons: "Add" (blue) and "Refresh". A search input field has "MAC Address..." placeholder text. Below are several status buttons: "Lost", "Stolen", "Edit", "PIN Lock", "Full Wipe", "Unenroll", "Reinstate", and "Delete". A gear icon is also present. A table lists the registered devices:

MAC Address	Device Name	Description	Status
50:3E:AA:E4:81:B6	MyWindows_Device		Registered

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

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.co

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

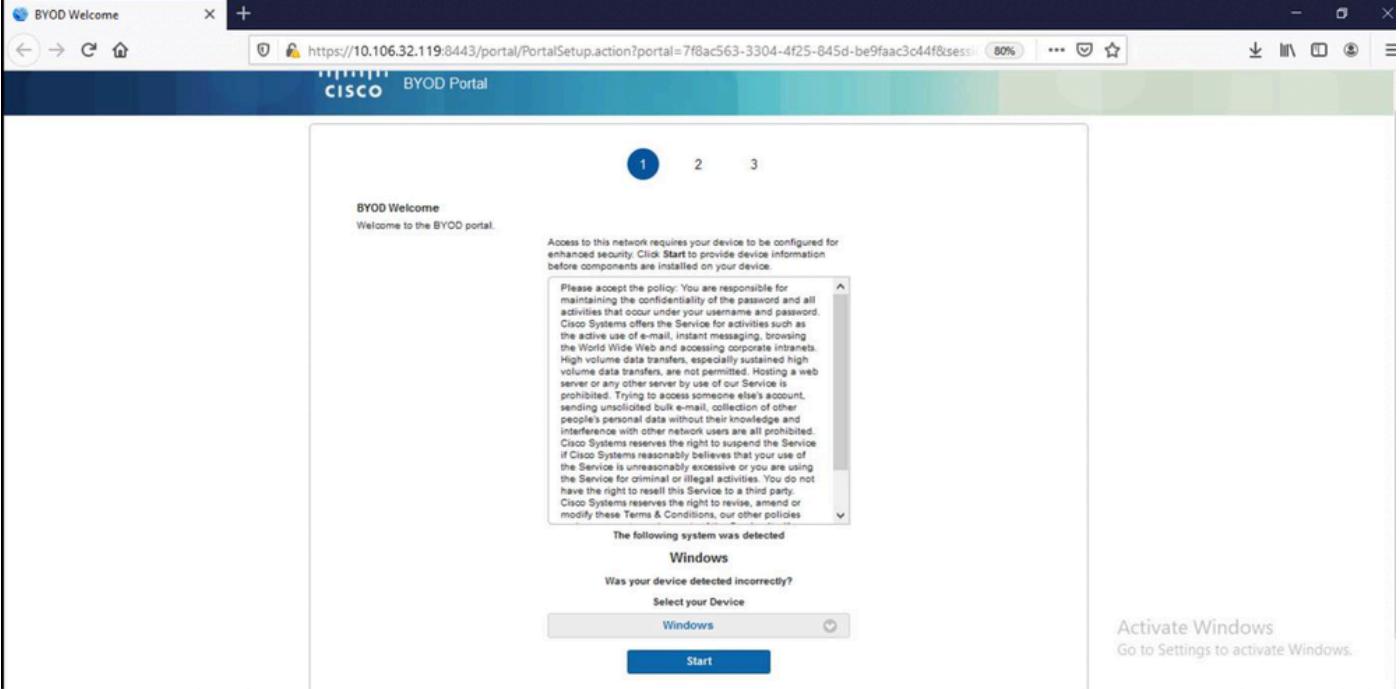
2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a
2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a

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.co
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.co



Cliquez sur Start sur la page BYOD Welcome.

2020-12-02 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.co

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.step

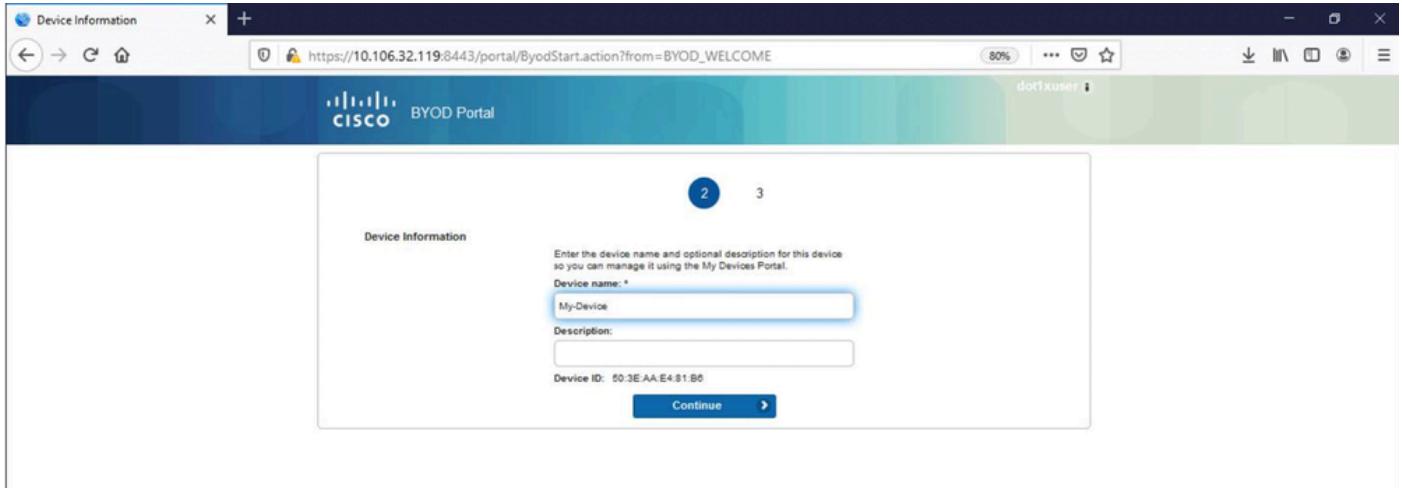
2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] guestaccess.flowmanager.step

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.co

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



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

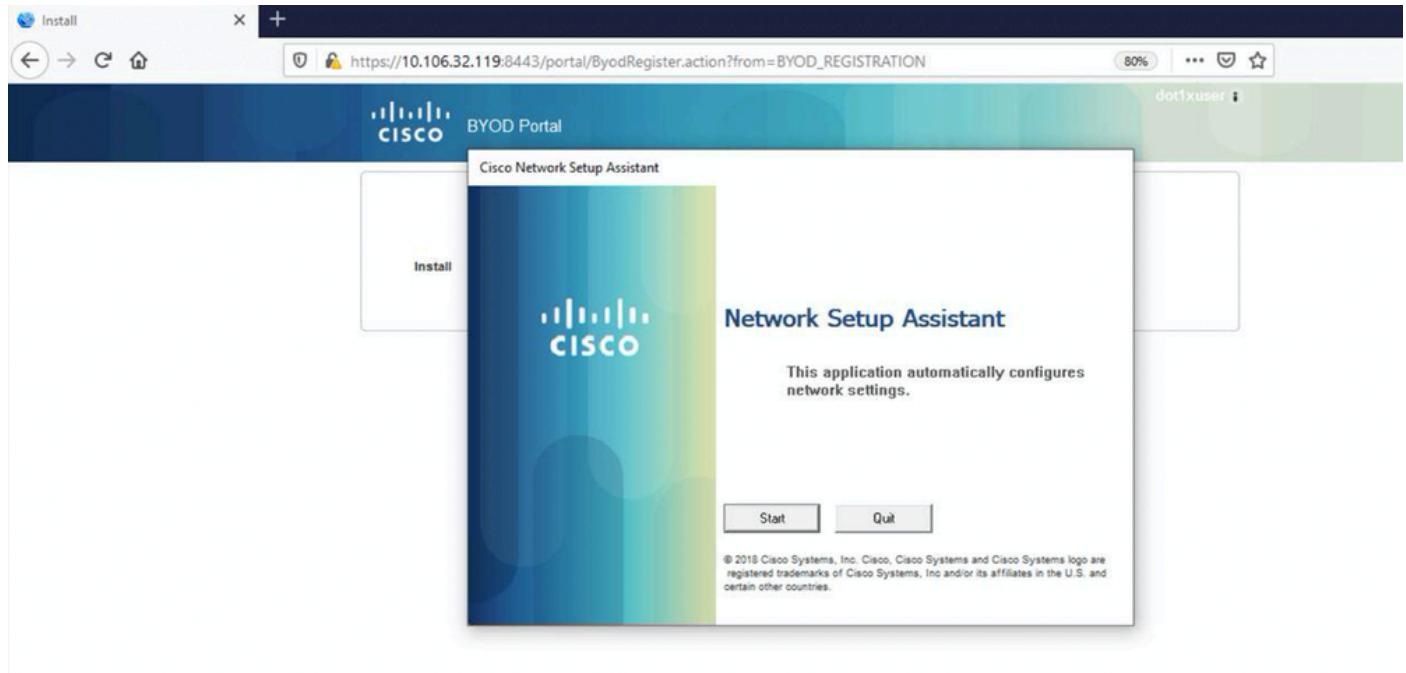
isSameDeviceRegistered = false

```
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.co
```

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

```
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

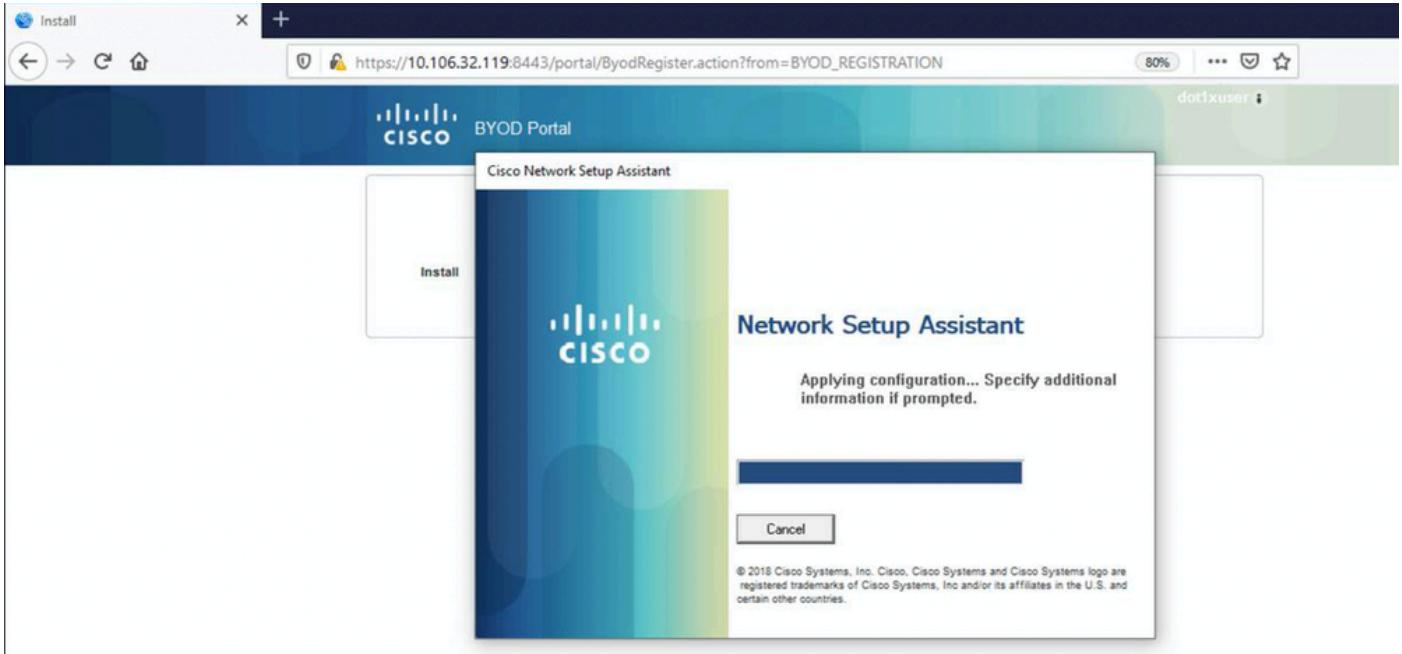
false

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.ScepUtil
```

```
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.PkiMessage
```

```
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.PkiMessage
```

```
2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessage
```

```
2020-12-02 05:45:11,334 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessage
```

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]

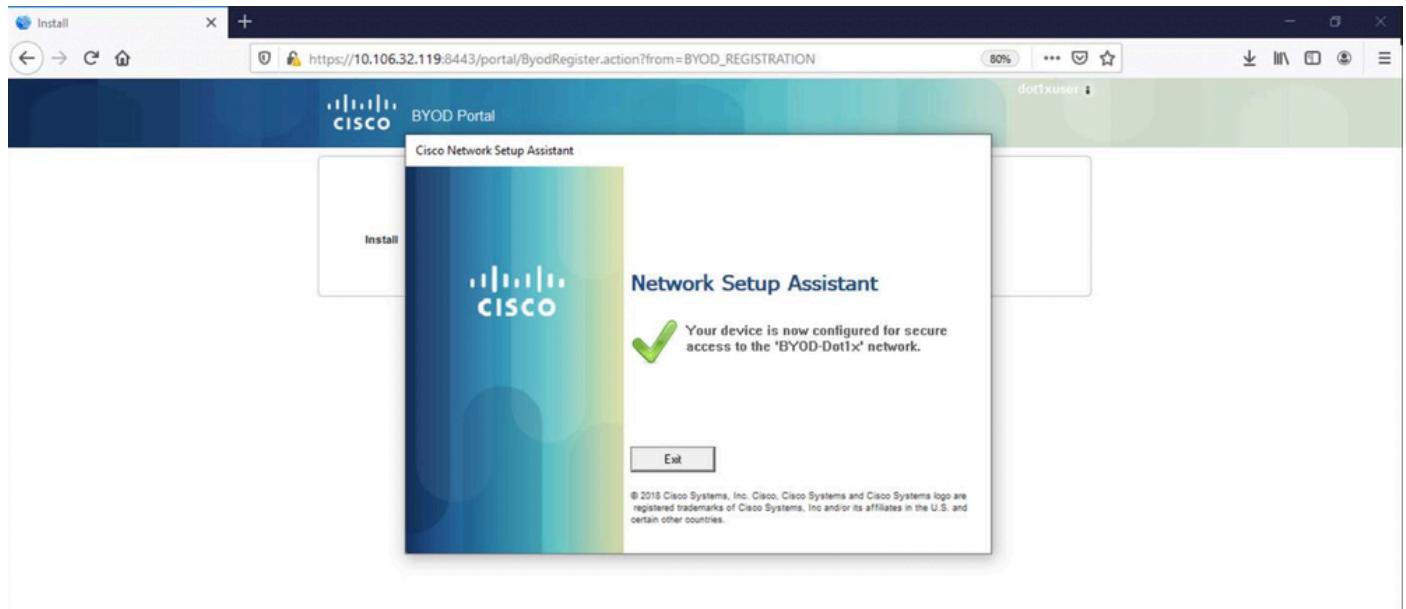
ise-psc.log

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.cert

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.cert

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: [ÙØyÉöžö|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.anhsinh.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\AppData  
[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 successfully 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.