# Configuration du BYOD sans fil SSID unique sous Windows et ISE

## Contenu

Introduction Conditions préalables **Conditions requises Components Used** Théorie Configuration Configuration ISE Configuration WLC Vérification Vérification du flux d'authentification Vérifier le portail Mes périphériques Dépannage Informations générales Analyse du journal de travail Journaux ISE Journaux client (journaux spw)

## Introduction

Ce document décrit comment configurer le BYOD (Bring Your Own Device) sur Cisco Identity Services Engine (ISE) pour Windows Machine à l'aide d'un SSID unique et d'un SSID double.

## Conditions préalables

### **Conditions requises**

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco ISE version 3.0
- Configuration de Cisco WLC
- Fonctionnement du BYOD

### **Components Used**

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

Étapes SSID unique pour le BYOD de Windows -

- Authentification EAP-MSCHAPv2 initiale
- Redirection vers le portail BYOD
- Enregistrement de périphérique
- téléchargement NSA
- Téléchargement du profil
- Téléchargement du certificat
- Authentification EAP-TLS

## Configuration

### **Configuration ISE**

Étape 1. Ajoutez le périphérique réseau sur ISE et configurez RADIUS et la clé partagée.

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

Étape 2. Créez un modèle de certificat pour les utilisateurs BYOD. Le modèle doit avoir l'authentification client Utilisation améliorée de la clé. Vous pouvez utiliser EAP\_Certificate\_Template par défaut.

Cisco ISE		Administration · System
Deployment Licensing	Certificates Logging	Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings
	Edit Certificate Template	
Certificate Management	* Name	BYOD_Certificate_template
Certificate Authority $\sim$		
Overview	Description	
Issued Certificates	Subject	
Certificate Authority Certifica	Common Name (CN)	\$UserName\$ 🕕
Internal CA Settings	Organizational Unit (OU)	tac
Certificate Templates		
External CA Settings	Organization (O)	cisco
	City (L)	bangalore
	State (ST)	Karnataka
	Country (C)	IN
	Subject Alternative Name (SAN)	MAC Address
	Кеу Туре	RSA V
	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. Créez un profil de demandeur natif pour un profil sans fil.

Accédez à ISE > Work Centers > BYOD > Client Provisioning. Cliquez sur Ajouter et choisissez Profil de demandeur natif (NSP) dans la liste déroulante.

Ici, le nom SSID doit être identique à celui que vous avez connecté avant d'effectuer un seul BYOD SSID. Sélectionnez le protocole TLS. Choisissez le modèle de certificat tel que créé à l'étape précédente ou utilisez le modèle EAP\_Certificate\_Template par défaut .

Sous Paramètres facultatifs, sélectionnez l'authentification utilisateur ou utilisateur et machine selon vos besoins. Dans cet exemple, il est configuré en tant qu'authentification utilisateur. Laissez les autres paramètres par défaut.

E Cisco ISE			Work Centers · BYOD			A Evaluation Mode 46 Days
Overview Identities Identity	y Groups Network Devices	Ext Id Sources	Client Provisioning	Portals & Components	Policy Elements	Policy Sets Reports More
Client Provisioning Policy	* Name Wireles:	sNSP				
Resources	Description					
		Wireless Profile(s)				
	Operating System * ALL	SSID Name *	BYOD-Dot1x			
V N	Wireless Profile Multiple SSIDs can be configured, Prove Auto-Config File LIPL will be	Proxy Auto-Config File URL		0	profile will be appl	lied globally (i.e. to all subsequent profiles)
н	f no Proxy Auto-Config File URL i	Praxy Host/iP			used for early (pre	e 5.x) versions of Android.
6	🖉 Edit 🕂 Add 📋 Duplicate	Proxy Port				
	SSID Name Prox	Security *	WPA2 Enterprise V		cate Templ	
	BYOD-Dot1x	Allowed Protocol *	TLS 🗸		Certificate_templi	
		Certificate Template	BYOD_Certificate_template	~ 🛈		
		<ul> <li>Optional Setti</li> </ul>	ngs			
		Windows Settings				
		Authentication Mode	> User	~		

Étape 4. Créer une stratégie d'approvisionnement client pour le périphérique Windows.

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

≡ Cisco	ISE			Work	Centers - BYOD				A Evaluation Mode 4	6 Days		9
Overview	Identities	Identity Groups	Network Devices	Ext Id Sources	Client Provisioning	Portals & Components	Policy Elements	Policy Sets	Reports M	More $\sim$		
Client Provisionin Resources	ng Policy	Client Define the Cli For Agent Co For Native Su	Provisioning Policy to on nfiguration: version of ager pplicant Configuration: wiz	Policy determine what users will nt, agent profile, agent cor ard profile and/or wizerd.	receive upon login and use mpliance module, and/or at Drag and drop rules to cha	r session initiation: gent customization package. nge the order.						
		~										
			Rule Name	Identity Group	s Operating Sys	tems Other Cor	nditions	R	esults			
		8 🖂	IOS	If Any	and Apple iOS All	and Condition(s	)	then C	isco-ISE-NSP	Ed	<b>x</b> ~	
		# 🗹	Android	If Any	and Android	and Condition(s	)	then C	isco-ISE-NSP	Ed	<b>k</b> ~	
		II 🗹	Windows	If Any	and Windows All	and Condition(s	)	then W	VinSPWizard 3.0.0.2 nd WirelessNSP	Ed	it ~	
		II 🗹	MAC OS	If Any	and Mac OSX	and Condition(s	)	then C 4. M	iscoTemporalAgentOSX .8.00176 And lacOsXSPWizard	Ed	<b>k</b> ~	
									Sav	re		Reset

Étape 5. Créez un **profil d'autorisation** pour les périphériques non enregistrés en tant que périphériques BYOD.

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

Sous **Tâche commune**, sélectionnez **Approvisionnement du demandeur natif**. Définissez un nom de liste de contrôle d'accès Redirect 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**.

		Policy · Policy Elements
Dictionaries 0	Conditions	Results
Authentication	>	* Name BYOD_Wireless_Redirect
Authorization	~	Description
Authorization Profile	s	* Access Type ACCESS_ACCEPT ~
		Network Device Profile 🏥 Cisco 🗸 🕀
Profiling	>	Service Template
Posture	>	Track Movement
Client Provisioning	>	Agentiess Posture
		✓ Common Tasks
		Web Redirection (CWA, MDM, NSP, CPP)
		Native Supplicant Provisioning V ACL BYOD-Initial V Value BYOD Portal (default) V

Étape 6. Créez un profil de certificat.

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

E Cisco ISE	Administration · Identity Management
Identities Groups External Iden	ity Sources Identity Source Sequences Settings
External Identity Sources  C  C  C  C  C  C  C  C  C  C  C  C  C	Certificate Authentication Profiles List > cert_profile Certificate Authentication Profile * Name Cert_profile Description
	Identity Store [not applicable]
C RADIUS Token	
SAML Id Providers	Use Identity From Certificate Attribute Subject - Common N:
Social Login	Match Client Certificate Against <ul> <li>Never</li> <li>Only to resolve identity ambiguity</li> <li>Always perform binary comparison</li> </ul>

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

≡ 0	isco ISE		Ac	dministration - Identity Management				
Identiti	es Groups	External Identity Sources	Identity Source Sequer	nces Settings				
Identity Identit	dentity Source Sequences List > For_Teap Identity Source Sequence							
∨ Ide * Nar Desc	V Identity Source Sequence       * Name     BYOD_id_Store       Description							
	✓ Certificate Based Authentication          ✓ Select Certificate Authentication Profile							
∨ Ai	<ul> <li>Authentication Search List</li> <li>A set of identity sources that will be accessed in sequence until first authentication succeeds</li> </ul>							
	Available	Se	lected					
	Internal Endpoi	nts Int	ernal Users					
	Guest Users	A	DJoioint					

Étape 8. Créez un jeu de stratégies, une stratégie d'authentification et une stratégie d'autorisation.

Accédez à ISE > Policy > Policy Sets. Créez un jeu de stratégies et enregistrez.

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

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

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

2. Périphériques enregistrés pour le BYOD et faisant EAP-TLS. Accorder un accès complet à ces périphériques.

≡ c	E Cisco ISE Policy · Policy Sets					
∨ Auti	henticatio	n Policy (1)				
(+)	Status	Rule Name	Cor	ditions		Use
0	) Search					
				+		
						BYOD_id_Store
	•	Default				> Options
> Auti	horization	Policy - Local Exceptions				
> Auti	horization	Policy - Global Exceptions	•			
∨ Auti	horization	Policy (3)				
					Results	
Ð	Status	Rule Name	Cor	ditions	Profiles	Security Groups
0	) Search					
	0	Full_Acceess	AND	Network Access-EapAuthentication EQUALS EAP-TLS	PermitAccess × · · · +	Select from list
_				EndPoints-BYODRegistration EQUALS Yes		
	0	BYOD_Redirect	F	EndPoints-BYODRegistration EQUALS Unknown	BYOD_Wireless_Redire $\times$ $\sim$ +	Select from list

## **Configuration WLC**

Étape 1. Configurez Radius Server sur WLC.

#### Accédez à Security > AAA > Radius > Authentication.

cisco	MONITOR WLANS	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Security	RADIUS Authenti	cation Serve	rs > Edit					
<ul> <li>▼ AAA         General         <ul> <li>RADIUS                 Authentication                 Accounting                 Auth Cached Users                 Fallback                 DNS                 Downloaded AVP</li> </ul> </li> </ul>	Server Index Server Address(Ipv4 Shared Secret Forma Shared Secret Confirm Shared Secr	l/Ipv6) at ret	7 10.106.32.11 ASCII ~	9				(p) (p)
TACACS+ LDAP	Key Wrap	C	Oesigned fo	r FIPS custome	ers and requires a k	ey wrap complian	nt RADIU	S server)
Local Net Users	Apply Cisco ISE Defa	ault settings						
<ul> <li>Disabled Clients</li> </ul>	Apply Cisco ACA Def	ault settings						
User Login Policies	Port Number		1812					
Password Policies	Server Status		Enabled V	1				
Local EAP	Support for CoA		Enabled 🗸	1				
Advanced EAP	Server Timeout		5 secon	nds				
Priority Order	Network User		Z Enable					
Certificate	Management		Z Enable					
Access Control Lists	Management Retran	smit Timeout	5 secon	ds				
Wireless Protection	Tunnel Proxy		Enable					
Policies	Realm List							
Web Auth	PAC Provisioning		Enable					
TrustSec	IDSec		Enable					
Local Policies	Cines ACA							
▶ Umbrella	CISCO ACA							
5								

Advanced

## Accédez à Sécurité > AAA > Rayon > Comptabilité.

iliilii cisco	Monitor <u>w</u> lans <u>c</u> ontroll	er W <u>i</u> reless	<u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
Security	RADIUS Accounting Server	s > Edit					
<ul> <li>▼ AAA</li> <li>General</li> <li>▼ RADIUS</li> </ul>	Server Index Server Address(Ipv4/Ipv6)	7					
Authentication Accounting Auth Cached Users Fallback DNS	Shared Secret Format Shared Secret Confirm Shared Secret	ASCII ~				٩	
<ul> <li>TACACS+ LDAP Local Net Users MAC Filtering</li> <li>Disabled Clients User Login Policies AP Policies Password Policies</li> </ul>	Apply Cisco ACA Default settings Port Number Server Status Server Timeout Network User	1813 Enabled ✓ 5 seconds ✓ Enable					
<ul> <li>Local EAP</li> <li>Advanced EAP</li> <li>Priority Order</li> </ul>	Management Tunnel Proxy <u>Realm List</u>	Enable     Enable					
<ul> <li>Certificate</li> <li>Access Control Lists</li> <li>Wireless Protection Policies</li> </ul>	PAC Provisioning IPSec Cisco ACA	Enable     Enable     Enable     Enable					
<ul><li>Web Auth</li><li>TrustSec</li></ul>							

## Étape 2. Configurez un SSID Dot1x.

cisco	<u>M</u> onitor <u>W</u> lans <u>C</u> ontroi	oller w <u>i</u> reless <u>s</u> ecurity m <u>a</u> nagement c <u>o</u> mmands he <u>l</u> p <u>f</u> eedback
WLANs	WLANs > Edit 'BYOD-Do	ot1x'
WLANS	General Security Qo	oS Policy-Mapping Advanced
Advanced	Profile Name	BYOD-Dot1x
	Type	BYOD-Dot1x
	Status	Z Enabled
	Radio Policy	(Modifications done under security tab will appear after applying the changes.)
	Interface/Interface Group(G)	management 🗸
	Multicast Vlan Feature	Enabled
	Broadcast SSID	Z Enabled
	NAS-ID	none
	Lobby Admin Access	

	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK						
WLANs	WLANs > Edit 'BYOD-Dot1x'						
VLANS	General Security QoS Policy-Mapping Advanced						
Advanced	Layer 2 Layer 3 AAA Servers						
	Layer 2 Security  WPA2+WPA3						
	Security Type Enterprise 🗸						
	MAC Filtering <sup>2</sup>						
	WPA2+WPA3 Parameters						
	Policy WPA2 UWPA3 Encryption Cipher Compass Compass						
	Fast Transition						
	Fast Transition Adaptive 🗸						
	Over the DS						
	Reassociation Timeout 20 Seconds						
	Protected Management Frame						
	Authentication Key Management 19						
	802 1X-SHA1						
CISCO	Monitor <u>w</u> lans <u>c</u> ontroller w <u>i</u> reless <u>s</u> ecurity m <u>a</u> nagement c <u>o</u> mmands he <u>l</u> p <u>f</u> eedback						
WLANs	WLANs > Edit 'BYOD-Dot1x'						
WLANS WLANS	WLANs > Edit 'BYOD-Dot1x' General Security QoS Policy-Mapping Advanced						
WLANS WLANS WLANS Advanced	WLANs > Edit 'BYOD-Dot1x' General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers						
WLANS WLANS Advanced	WLANs > Edit 'BYOD-Dot1x'         General       Security       QoS       Policy-Mapping       Advanced         Layer 2       Layer 3       AAA Servers         Select AAA servers below to override use of default servers on this WLAN         RADIUS Servers         RADIUS Server Overwrite interface       Enabled         Apply Cisco ISE Default Settings       Enabled         Server 1       IP:10.106.32.119, Port:1812         Server 2       None       None         Server 3       None       None						
WLANS WLANS Advanced	WLANs > Edit 'BYOD-Dot1x'         General Security QoS Policy-Mapping Advanced         Layer 2 Layer 3 AAA Servers         Select AAA servers below to override use of default servers on this WLAN         RADIUS Servers         RADIUS Server Overwrite interface Enabled         Apply Cisco ISE Default Settings Enabled         Authentication Servers Accounting Servers         Enabled         Server 1         IP:10.106.32.119, Port:1812 V         Server 2         None         Server 3         None         Server 4         None         Server 4						
WLANS WLANS Advanced	WLANs > Edit 'BYOD-Dot1x'         General       Security       Qos       Policy-Mapping       Advanced         Layer 2       Layer 3       AAA Servers         Select AAA servers below to override use of default servers on this WLAN         RADIUS Servers         RADIUS Server Overwrite interface       Enabled         Apply Cisco ISE Default Settings       Enabled         Authentication Servers       Accounting Servers         Enabled       Enabled         Server 1       IP:10.106.32.119, Port:1812         Server 3       None         Server 4       None         Server 5       None         Server 5       None						
WLANS WLANS Advanced	WLANs > Edit 'BYOD-Dot1x'         General       Security       QoS       Policy-Mapping       Advanced         Layer 2       Layer 3       AAA Servers         Select AAA servers below to override use of default servers on this WLAN         RADIUS Servers         RADIUS Server Overwrite interface       Enabled         Apply Cisco ISE Default Settings       Enabled         Authentication Servers       EAP Parameters         Enabled       Enabled         Server 1       IP:10.106.32.119, Port:1812          Server 2       None         Server 3       None         Server 4       None         Server 5       None         Server 6       None         Server 6       None         Server 6       None						

uluili. cisco	MONITOR WLANS CONTROLLER W	ireless security management commai	NDS HELP FEEDBACK
CISCO WLANS * WLANS WLANS • Advanced	MONITOR WLANS CONTROLLER W/ WLANS > Edit 'BYOD-Dot1x' General Security QoS Po Allow AAA Override Coverage Hole Detection Enable Session Timeout Aironet IE Diagnostic Channel 18 Override Interface ACL Layer2 Acl URL ACL P2P Blocking Action Client Exclusion 2 Maximum Allowed Clients 2 Static IP Tunneling 11	IRELESS SECURITY MANAGEMENT COMMAN	DHCP         DHCP Server         DHCP Addr. Assignment         DHCP Addr. Assignment         Required         Management Frame Protection (MFP)         MFP Client Protection 4         Optional ▼         DTIM Period (in beacon intervals)         802.11a/n (1 - 255)         1         NAC         NAC State         ISE NAC ▼         Load Balancing and Band Select
	Wi-Fi Direct Clients Policy Maximum Allowed Clients Per AP Radio Clear HotSpot Configuration	Disabled V 200 Enabled	Client Load Balancing

Étape 3. Configurez la liste de contrôle d'accès Redirect pour fournir un accès limité pour le provisionnement du 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 élément que vous avez appelé manuellement la liste de contrôle d'accès dans le profil d'autorisation)

cisco	MONIT	for <u>w</u> i	LANS (	CONTROLLE	R WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK					
ecurity	Acce	ss Cont	trol Lis	ts > Edit											
AAA Local EAP	Gene	ral													
Advanced EAP	Access	List Name	Name BYOD-Initial		al										
Priority Order	Deny 0	Deny Counters 0													
Certificate	Seq	Seg Action Source IP/Ma		e IP/Mask	Destination IP/Mask			Protocol Sou	Source Port Dest Port	DSCP	Direction	Number of Hits			
Access Control Lists	1	Permit	0.0.0.0	)	/ 0.0.0.0	0.0.0.0	/ 0.0.0	).0	UDP	Any	Any	Any	Any	0	
CPU Access Control Lists	2	Permit	0.0.0.0	)	/ 0.0.0.0	10.106.3	2.119 / 255.	255.255.255	Any	Any	Any	Any	Any	0	
FlexConnect ACLs	3	Permit	10.106	.32.119	/ 255.255.255.2	255 0.0.0.0	/ 0.0.0	0.0	Any	Any	Any	Any	Any	0	
URL ACLS	4	Deny	0.0.0.0	)	/ 0.0.0.0	0.0.0	/ 0.0.0	0.0	Алу	Any	Any	Any	Any	0	
Wireless Protection Policies															
Web Auth															
TrustSec															
Local Policies															
Umbrella															
Advanced															

## Vérification

Vérification du flux d'authentification

E Cisco ISE		Operations - RADIUS				A Evaluatio	n Mode 46 Days	Q 0	P	ø
Live Logs Live Sessions										
Misconfigured Supplicants 🔘	Misconfigured Ne	twork Devices 🕕 RA	DIUS Drops 🕕		Client Stoppe	d Responding 🕕		Repeat C	ounter	
0	(	)	1			0		(	C	
🖉 Refresh 🕁 Reset Repeat Counts 🖒 Export To 🗸					Refres	n Show Latest 20	records 🗸	Within Last 5 mi	inutes ter 🗸 - {	<u>~</u>
Time Status D	etails Repea I	Identity	Endpoint ID	Identity Group	Authenti	Authorization Policy	Authorizatio	n Profiles		E
×	~	Identity	Endpoint ID	Identity Group	Authenticat	Authorization Policy	Authorization	Profiles		ε
Nov 29, 2020 11:13:47.4 0	0 0	dot1xuser	50:3E:AA:E4:8		Wireless >	Wireless >> Full_Acceess	PermitAccess			w
Nov 29, 2020 11:13:47.2 🗹		dot1xuser	50:3E:AA:E4:8	RegisteredDevices	Wireless >	Wireless >> Full_Acceess	PermitAccess			w
Nov 29, 2020 11:10:57.9		dot1xuser	50:3E:AA:E4:8	Profiled	Wireless >	Wireless >> BYOD_Redirect	BYOD_Wireles	s_Redirect		ΤF
									_	

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	

## 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	0a6a21b2000009a5fc3d3ad
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	WLC1

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

## Cisco ISE

#### 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

## Cisco ISE

#### Authentication Details

Source Timestamp	2020-11-29 11:13:47.246
Received Timestamp	2020-11-29 11:13:47.246
Policy Server	isee30-primary
Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Calling Station Id	50-3e-aa-e4-81-b6
Endpoint Profile	Windows10-Workstation
Endpoint Profile Identity Group	Windows10-Workstation RegisteredDevices
Endpoint Profile Identity Group Audit Session Id	Windows10-Workstation RegisteredDevices 0a6a21b20000009a5fc3d3ad
Endpoint Profile Identity Group Audit Session Id Authentication Method	Windows10-Workstation RegisteredDevices 0a6a21b20000009a5fc3d3ad dot1x
Endpoint Profile Identity Group Audit Session Id Authentication Method Authentication Protocol	Windows10-Workstation RegisteredDevices 0a6a21b20000009a5fc3d3ad dot1x EAP-TLS
Endpoint Profile Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type	Windows10-Workstation RegisteredDevices 0a6a21b20000009a5fc3d3ad dot1x EAP-TLS Framed

#### Vérifier 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.

My Devices Portal				
1300				
anago Devices				
arrage Devices aed to add a device? Select Add. Was your de	vice lost or stolen? Select your device	e from the list to manage it.		
umber of registered devices:2/5		-		
Add	Refresh			
MAC Address				
Lost Stolen Edit F	IN Lock Full Wipe Uner	nroll Reinstate Delete		
MAC Address	Device Name	Description	Status	

## Dépannage

#### Informations générales

Pour le processus BYOD, ces composants ISE doivent être activés dans le débogage sur les noeuds PSN -

scep - messages du journal scep. Fichier journal cible guest.log et ise-psc.log.

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

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

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

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

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

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

admin-ca- ca-service messages admin -ise-psc.log des fichiers journaux cibles, caservice.log et casrvice-misc.log

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

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

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

runtime-AAA - Tous les événements Runtime. Fichier journal cible - prrt-server.log.

Pour les journaux côté client :

#### Rechercher %temp%\spwProfileLog.txt (ex : C:\Users\<nom d'utilisateur>\AppData\Local\Temp\spwProfileLog.txt)

#### Analyse du journal de travail

#### Journaux ISE

Initial Access-Accepcept avec liste de contrôle d'accès redirigée et URL de redirection pour le portail BYOD.

#### Prrt-server.log-

Radius,2020-12-02 05:43:52,395,DEBUG,0x7f433e6b8700,cntx=0008590803,sesn=isee30primary/392215758/699,CPMSessionID=0a6a21b2000009f5fc770c7,user=dot1xuser,CallingStationID=50-3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=254 Length=459 [1] User-Name value: [dot1xuser] [25] Class - value: [\*\*\*\*] [79] EAP-Message - value: [ñ [80] Message-Authenticator - value: [.2{wëbÙ<sup>\*\*</sup>Åp05<Z] [26] cisco-av-pair - value: [url-redirect-acl=BY0D-Initial] [26] cisco-av-pair - value: [urlredirect=https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009f5fc770c7&portal=7f8 ac563-3304-4f25-845d-be9faac3c44f&action=nsp&token=53a2119de6893df6c6fca25c8d6bd061] [26] MS-MPPE-Send-Key - value: [\*\*\*\*] [26] MS-MPPE-Recv-Key - value: [\*\*\*\*] ,RADIUSHandler.cpp:2216 Lorsqu'un utilisateur final essaie de naviguer sur un site Web et a été redirigé par le WLC vers l'URL de redirection ISE.

#### Guest.log -

```
2020-12-02 05:43:58,339 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][]
com.cisco.ise.portal.Gateway -::- Gateway Params (after update):
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.utils.RadiusSessionUtil -::- sessionId=0a6a21b20000009f5fc770c7 :
token=53a2119de6893df6c6fca25c8d6bd061 2020-12-02 05:43:58,339 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-5][] cisco.ise.portalwebaction.utils.RadiusSessionUtil -::- Session
token successfully validated. 2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-5][] cisco.ise.portal.util.PortalUtils -::- UserAgent : Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0 2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-5][] cisco.ise.portal.util.PortalUtils -::- isMozilla: true 2020-12-02
05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][] com.cisco.ise.portal.Gateway -
::- url: /portal/PortalSetup.action?portal=7f8ac563-3304-4f25-845d-
be9faac3c44f&sessionId=0a6a21b20000009f5fc770c7&action=nsp&redirect=www.msftconnecttest.com%2Fre
direct 2020-12-02 05:43:58,355 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.controller.PortalFlowInterceptor -::- start guest flow interceptor...
2020-12-02 05:43:58,356 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.actions.BasePortalAction -::- Executing action PortalSetup via request
/portal/PortalSetup.action 2020-12-02 05:43:58,356 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7][] cisco.ise.portalwebaction.actions.PortalSetupAction -::- executeAction... 2020-12-02
05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.actions.BasePortalAction -::- Result from action, PortalSetup: success
2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.actions.BasePortalAction -::- Action PortalSetup Complete for request
/portal/PortalSetup.action 2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7][] cpm.guestaccess.flowmanager.processor.PortalFlowProcessor -::- Current flow step:
```

		S-D/SU-IDSSCabSouel 2020	1-12-02 05:43:58	3,361 DEBUG [nttps-
jsse-nio-10.106.32.119	9-8443-exec-7][]	cpm.questaccess.flowman	ager.step.Step	Executor -::- Getting
next flow step for INI	TT with TranEnum	= PROCEED 2020-12-02 05:4	3:58.361 DEBUG	[https-isse-nio-
10 106 32 119-8//3-02	2c - 71[] com ques	staccess flowmanager ster	StenEvecutor -	$\cdots$ StepTran for
	DROCEED toSton=	PVOD WELCOME 2020 12 02	05.42.50 261 DI	EPIIC [https jago njo
10 106 22 110 0442 and	PROCEED, COSCEP-	BIOD_WELCOME 2020-12-02	05:45:58,501 Dr	LEOG [IICCPS-JSSE-IIIO-
10.106.32.119-8443-exe	ec-/j[j cpm.gues	staccess.llowmanager.step	.StepExecutor -	-::- Find Next
Step=BYOD_WELCOME 2020	0-12-02 05:43:58	3,361 DEBUG [https-jsse-n	110-10.106.32.11	19-8443-exec-7][]
cpm.guestaccess.flowma	anager.step.Step	Executor -::- Step : BYC	D_WELCOME will	be visible! 2020-12-
02 05:43:58,361 DEBUG	[https-jsse-nio	0-10.106.32.119-8443-exec	:-7][]	
cpm.guestaccess.flowma	anager.step.Step	Executor -::- Returning	next step =BYOI	D_WELCOME 2020-12-02
05:43:58,362 DEBUG [ht	ttps-jsse-nio-10	.106.32.119-8443-exec-7]	[]	
cpm.guestaccess.flowma	anager.adaptor.P	PortalUserAdaptorFactory	-::- Looking up	p Guest user with
uniqueSubjectId=5f5592	2a4f67552b855ecc	56160112db42cf7074e 2020	-12-02 05:43:58	8,365 DEBUG [https-
jsse-nio-10.106.32.119	9-8443-exec-7][]			
cpm.guestaccess.flowma	anager.adaptor.P	PortalUserAdaptorFactory	-::- Found Gues	st user 'dot1xuserin
DB using uniqueSubject	tID '5f5592a4f67	'552b855ecc56160112db42cf	7074e'. authSto	preName in
DB=Internal Users, aut	thStoreGUID in D	DB=9273fe30-8c01-11e6-996	c-525400b48521.	. DB ID=bab8f27d-
c44a-48f5-9fe4-5187047	7bffc0 2020-12-0	02 05:43:58,366 DEBUG [ht	tps-jsse-nio-10	0.106.32.119-8443-
exec-7][] cisco.ise.po	ortalwebaction.c	controller.PortalStepCont	roller -::- +++	++ updatePortalState:
PortalSession (e0d457d		a-5cf29e12dacc) current	state is INITIA	ATED and current step
is BYOD WELCOME 2020-1	12 - 02 05 · 40 · 35 6	11 DEBUG [https-isse-nic	-10 106 32 119-	-8443-evec-61[]
com disco iso portalso	nacionManagor Po	rtalSoggion -··- Sotting	t = 100.1000.520.115	$C_{1}$
	11 DEDUC [https	$i_{a}$	1 the portal ses	SSION State to ACTIVE
2020-12-02 03:40:35,61	II DEBUG [IICCPS-	JSSE-1110-10.106.32.119-0	443-exec-6][]	
	L	D + 1 0 + 0 + 1 1		
cisco.ise.portalwebact	tion.controller.	PortalStepController -::	- nextStep: BYC	DD_WELCOME - o ×
cisco.ise.portalwebact ♥ BYOD Welcome × + ← → C ☆ ♥ ♥ ♠	tion.controller. https://10.106.32.119:8443/portal/P	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9	- nextStep: BYC	DD_WELCOME - ♂ × 7☆ ⊻ II\ ⊡ ⊛ ≡
cisco.ise.portalwebact $\bigcirc$ BYOD Welcome × + $(\leftarrow) \rightarrow @ @ @ 0 @ @$	tion.controller.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9	- nextStep: BYC	
cisco.ise.portalwebact	tion.controller.	PortalStepController -::	- nextStep: BYC	DD_WELCOME - ♂ × ₽☆ ⊻ № ⊡ ⊛ ≡
cisco.ise.portalwebact	tion.controller.	PortalStepController -::	- nextStep: BYC	DD_WELCOME -
cisco.ise.portalwebact ● BYOD Welcome × + ← → C û	tion.controller.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9	- nextStep: BYC	DD_WELCOME →
cisco.ise.portalwebact ● BYOD Welcome × + ← → C û	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9	- nextStep: BYC	DD_WELCOME →
cisco.ise.portalwebact ● BYOD Welcome × + ← → C ☆ ⑦ €	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOD portal.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9  1 2 3  Access to this network requires your device to be configured for	- nextStep: BYC	DD_WELCOME →
cisco.ise.portalwebact ● BYOD Welcome × + ← → C ☆ ⑦ €	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOD portal.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9	- nextStep: BYC	DD_WELCOME →
cisco.ise.portalwebact ♥ BYOD Welcome × + ← → C û © €	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOD portal.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9 1 2 3 Access to this network requires your device to be configured for enhanced security. Click Start to provide device information before component are installed on you device. Please accept the policy. You are responsible for maintaining the confidentitity of the password and all	- nextStep: BYC	DD_WELCOME →
cisco.ise.portalwebact ♥ BYOD Welcome × + ← → C û	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOD portal.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9 1 2 3 Access to this network requires your device to be configured for enhanced security. Click Statt to provide device information before component as in Statt to provide device information before component as information or your device to the configured for maintaining the configuration of your devices to the statt advittes that coor under your devices to the advised and all advittes that coor under your devices to the advised and all advittes that coor under your devices to the stattes such as Clicko System offers the Stattes to the stattes such as	- nextStep: BYC	
cisco.ise.portalwebact ♥ BYOD Welcome × + ← → C û © € 1 ♥	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOD portal.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9 1 2 3 Access to this network requires your device to be configured for enhanced security. Click Bart to provide device information to the society of the society of the society of the society the society of the offending that the sponsible for maintaining the confidentiated many and passwork ( the society of the societ	- nextStep: BYC	
cisco.ise.portalwebact ♥ BYOD Welcome × + ← → C û ♥ 0 € 1 ♥ 0 ♥ 0 ♥ 0 ♥ 0 ♥ 0 ♥ 0 ♥ 0 ♥ 0	tion.controller. https://10.106.32.119.8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOD portal.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9 1 2 3 Access to this network requires your device to be configured for entended security. Click Mart to provide device information before components are installed on your device. Please accept the policy. You are responsible for maintaining the confidentially of the passwork and all all shifts that cocur under your device. Network work of the state of the state of the state of the state access of the most by our device. Network work of the state of the state of the state of the state access of the most by our device. Network work of the state of the st	- nextStep: BYC	
cisco.ise.portalwebact ♥ BYOD Welcome × + ← → C ☆ ⑦ € 1 ♥	tion.controller. https://10.106.32.119.8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOD portal.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9 1 2 3 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 access the policy. You are responsible to consolite the policy. You are responsible to activities that occur under your userame and password. Click Start to provide device information before components are installed on your device. Please access the policy. You are responsible to activities the Gas arankers, respecially submitted high over ror any other shore by use of due Services is prohibited. Trying to access someone seles as account, specific personal data without their knowledge and	- nextStep: BYC	
cisco.ise.portalwebact ♥ BYOD Welcome × + ← → ⊂ ☆	tion.controller. https://10.106.32.119.8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOD portal.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9 1 2 3 Access to this network requires your devices to be configured for entrol of the policy of the second second point of the maintaining the confidentiality of the password and all activities that door under your userneme and password. Choo System offer the Service for advivities such as maintaining the confidentiality of the password and all activities that door under your userneme and password. Choo System offer the Service for advivities such as the advive use of e-mail, instant messaging, to storing the Viold Wide Was and accessing corporate interares volume data bandres, are not permitted. Housing a which prohibited that networks are all prohibited. Choo System reserve the use of userval in the Service is prohibited that networks are all prohibited. Choo System reserves the use of userval in the Service to the restored uses are all prohibited.	- nextStep: BYC	
cisco.ise.portalwebact ♥ BYOD Welcome × + ← → ⊂ ☆	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the EYOO portal.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9 1 2 3 Access to this network requires your device to be configured for shore components are installed on your device. Please accept the policy. You are responsible for maintaining the confidentiality of the password and all advited bar to coor under your username and password. Clob Systems offses the Service for activities such as advited bar tanafees, especially sutained high volume data transfers, especially butter high volume data the Word Weard and assessmence else's associations and the transfers butter high volume data transfers, especially sutained high volume data transfers, especially sutained high volume data transfers, especially sutained high volume data transfers, especially ustained high volume data transfers, especially the volume data transfers, especially associative as an all prohibited. For oriminal of the top would by use of the the Service is urmeasonably espective or you are using the	- nextStep: BYC	
cisco.ise.portalwebact ● BYOD Welcome × + ← → C û □ ■	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOO portal.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9 1 2 3 Access to this network requires your device to be configured for source of the policy. You are responsible for maintaining the confidentiality of the password and at advilles that accounter your username and password. The socie of the policy. You are responsible for maintaining the confidentiality of the password and at advilles that another, especially sutained high volume data transfers, especial sutained high volume data transfers, especially sutained high volume data transfers, especially the volume high to service is unreasonably excessive or you are using the Service is unreaso	- nextStep: BYC	
cisco.ise.portalwebact ● BYOD Welcome × + ← → C û © €	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOD portal.	PortalStepController -:: ortalSetup.action?portal=7f8ac563-3304-4f25-845d-bes 1 2 3 Access to this network requires your device to be configured for source component as a installed on your device to component as a installed on your device t	- nextStep: BYC	
cisco.ise.portalwebact ♥ BYOD Welcome × + ← → C û ♥ ♥ ↓ ♥	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOD portal.	<text><text><text><text><text></text></text></text></text></text>	- nextStep: BYC	
cisco.ise.portalwebact ♥ BYOD Welcome × + ← → C û © € □	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOD portal.	Portal StepController - :: otdSetup.action?portal=768ac563-3304-4425-845d-bess totalSetup.action.action?portal=768ac563-3304-4425-845d-bess totalSetup.action.	- nextStep: BYC	
cisco.ise.portalwebact ♥ BYOD Welcome × + ← → C û © € □	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the BYOD portal.	Portal StepController - :: otdSetup.action?portal=78ac563-3304-4425-843d-best totalSetup.action?portal=78ac563-3304-843d-best totalSetup.action?portal=78ac563-3304-843d-best totalSetup.action?portal=78ac563-3304-843d-best totalSetup.action.action?portal=78ac563-3304-843d-best totalSetup.action	- nextStep: BYC	DD_WELCOME
cisco.ise.portalwebact ♥ BYOD Welcome × + ← → C û © € 1 ♥	tion.controller. https://10.106.32.119:8443/portal/P CISCO BYOD Portal BYOD Welcome Welcome to the EYOO portal.	Portal StepController - :: otdSetup.action?portal=78ac563-3304-4425-8436-bes d 2 3 d 3 d	- nextStep: BYC	Activate Windows Go to Settings to activate Windows.

#### Cliquez sur Démarrer sur la page d'accueil du BYOD.

020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Executing action ByodStart via request /portal/ByodStart.action 2020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.controller.PortalPreResultListener -:dot1xuser:currentStep: BYOD\_WELCOME

## À ce stade, ISE évalue si les fichiers/ressources nécessaires pour le 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.guest.ByodWelcomeStepExecutor -:dot1xuser:- userAgent=Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0, os=Windows 10 (All), nspStatus=SUCCESS 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dot1xuser:- NSP Downloadalble Resource data=>, resource=DownloadableResourceInfo :WINDOWS\_10\_ALL https://10.106.32.119:8443/auth/provisioning/download/a2b317ee-df5a-4bda-abc3e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b20000009f5fc770c7&os=WINDOWS\_10\_ALL null null https://10.106.32.119:8443/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/ null null https://10.106.32.119:8443/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/NetworkSetupAssistant.exe, coaType=NoCoa 2020-12-02 05:44:01,936 DEBUG [https-jssenio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager.utils.NSPProvAccess -: dot1xuser:-It is a WIN/MAC! 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager.step.StepExecutor -: dot1xuser: - Returning next step =BYOD\_REGISTRATION 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.controller.PortalStepController -:dot1xuser:- ++++ updatePortalState: PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is ACTIVE and current step is BYOD\_REGISTRATION 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.controller.PortalStepController -: dot1xuser:- nextStep: BYOD\_REGISTRATION

Sevice Information	× +	F				- ø ×
(←) → 健 @		0 🔒	https://10.106.32.119:8443/portal/l	ByodStart.action?from=BYOD_WELCOME	80% … 🗟 🟠	± ⊪\ © ≋ ≡
			CISCO BYOD Portal		dot1xuser 1	
				2 3		
			Device Information	Enter the device name and optional description for this device		
				Device name: *		
				My-Device		
				Description:		
				Device ID: 50:3E:AA:E4:81:86		
				Continue		

#### Saisissez 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.actions.BasePortalAction -:dot1xuser:- Executing action ByodRegister
via request /portal/ByodRegister.action 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.ByodRegisterAction -: dot1xuser:- executeAction... 2020-12-02
05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Result from action,
ByodRegister: success 2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -: dot1xuser:- Action ByodRegister Complete
for request /portal/ByodRegister.action 2020-12-02 05:44:14,683 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] cpm.guestaccess.apiservices.mydevices.MyDevicesServiceImpl -
:dot1xuser:- Register Device : 50:3E:AA:E4:81:B6 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.step.StepExecutor -:dot1xuser:-
Returning next step =BYOD_INSTALL 2020-12-02 05:44:14,902 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-1][] cisco.ise.portalwebaction.controller.PortalStepController -: dot1xuser:- ++++
updatePortalState: PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is ACTIVE
and current step is BYOD_INSTALL 2020-12-02 05:44:01,954 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-3][] cisco.ise.portalwebaction.controller.PortalFlowInterceptor -:dot1xuser:- result:
success 2020-12-02 05:44:14,969 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.client.provisioning.StreamingServlet -::- StreamingServlet
URI:/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/NetworkSetupAssistant.exe
```



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

#### Guest.log -

```
2020-12-02 05:45:03,275 DEBUG [portal-http-service15][]
```

```
cisco.cpm.client.provisioning.StreamingServlet -::- StreamingServlet
```

URI:/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-e4ec38ee188c/WirelessNSP.xml 2020-12-02 05:45:03,275 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet -::-Streaming to ip:10.106.33.167 file type: NativeSPProfile file name:WirelessNSP.xml 2020-12-02 05:45:03,308 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet -::-SFW profile :: 2020-12-02 05:45:03,308 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet -::-

Après avoir lu le contenu du **fichier spwProfile.xml**, la NSA configure le profil réseau et génère un CSR, puis l'envoie à l'ISE pour obtenir un certificat à l'aide de l'URL <u>https://10.106.32.119:8443/auth/pkiclient.exe</u>

🎯 Install	× +				
← → ♂ ☆	0 🕰	https://10.106.3	2.119:8443/portal/ByodRegister.a	ction?from=BYOD_REGISTRATION	80% … 🛛 ☆
		uluilu cisco	BYOD Portal		dotixuser :
		Install	Cisco Network Setup Assistant	Network Setup Assistant         Applying configuration Specify additional information if prompted.         Lance         9 2015 Claso Systems. Inc. Claso. Claso Systems and Claso Systems logo a registered trademarks of Claso Systems. Inc and/or its affiliates in the U.S. ar certain other countries.	9

#### 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance] com.cisco.cpm.scep.CertRequestInfo -::::- Found challenge password with cert template ID. Caservice.log -2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance] cisco.cpm.caservice.util.CaServiceUtil -::::- Checking cache for certificate template with ID: e2c32ce0-313d-11eb-b19e-e60300a810d5 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance] com.cisco.cpm.caservice.CertificateAuthority -::::- CA SAN Extensions = GeneralNames: 1: 50-3E-AA-E4-81-B6 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job

com.cisco.cpm.caservice.CertificateAuthority -::::- CA : add SAN extension... 2020-12-02

4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]

2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance] cisco.cpm.scep.util.ScepUtil -:::::- Algorithm OID in CSR: 1.2.840.113549.1.1.1 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance] com.cisco.cpm.scep.CertRequestInfo -:::::- Found challenge password with cert template ID.

#### caservice-misc.log -

2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request] com.cisco.cpm.caservice.CrValidator -:::::- performing certificate request validation: 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 0x67ee11d5 request validation] com.cisco.cpm.caservice.CrValidator -::::- RDN value = dot1xuser 2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request] com.cisco.cpm.caservice.CrValidator -::::- request validation result CA\_OK

#### ca-service.log -

```
2020-12-02 05:45:11,298 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -:::- Found incoming certifcate request for
internal CA. Increasing Cert Request counter. 2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] cisco.cpm.provisioning.cert.CertProvisioningFactory -:::- Key type
is RSA, retrieving ScepCertRequestProcessor for caProfileName=ISE Internal CA 2020-12-02
05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.cpm.provisioning.cert.CertRequestValidator -::::- Session user has been set to = dot1xuser
2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.cpm.scep.util.ScepUtil -:::- Algorithm OID in CSR: 1.2.840.113549.1.1.1 2020-12-02
05:45:11,331 INFO [https-jsse-nio-10.106.32.119-8443-exec-1][]
com.cisco.cpm.scep.ScepCertRequestProcessor -:::- About to forward certificate request
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser with transaction id n@P~N6E to server
http://127.0.0.1:9444/caservice/scep 2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessageEncoder -::::- Encoding message:
org.jscep.message.PkcsReq@5c1649c2[transId=4d22d2e256a247a302e900ffa71c35d75610de67,messageType=
PKCS_REQ, senderNonce=Nonce
[7d9092a9fab204bd7600357e38309ee8], messageData=org.bouncycastle.pkcs.PKCS10CertificationRequest@
4662a5b0] 2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
org.jscep.message.PkcsPkiEnvelopeEncoder -::::- Encrypting session key using key belonging to
[issuer=CN=Certificate Services Endpoint Sub CA - isee30-primary;
serial=162233386180991315074159441535479499152] 2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessageEncoder -::::- Signing message using
key belonging to [issuer=CN=isee30-primary.anshsinh.local;
serial=126990069826611188711089996345828696375] 2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessageEncoder -::::- SignatureAlgorithm
SHA1withRSA 2020-12-02 05:45:11,334 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
org.jscep.message.PkiMessageEncoder -:::- Signing
org.bouncycastle.cms.CMSProcessableByteArray@5aa9dfcc content
```

#### ise-psc.log-

prrt-server.log -

obtiennent un accès complet.

2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Performing doGetCertInitial found Scep certificate processor for txn id n@P~N6E 2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCertRequestProcessor -::::- Polling C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser for certificate request n@P~N6E with id {} 2020-12-02 05:45:13,385 INFO [https-jsse-nio-10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCertRequestProcessor -:::- Certificate request Complete for C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser Trx Idn@P~N6E 2020-12-02 05:45:13,596 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.provisioning.cert.CertProvisioningFactory -:::- BYODStatus:COMPLETE\_OTA\_NSP

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



#### ise-psc.log -

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

#### caservice.log -

2020-12-02 05:45:11,407 DEBUG [AsyncHttpClient-15-9][] org.jscep.message.PkiMessageDecoder - ::::- Verifying message using key belonging to 'CN=Certificate Services Endpoint RA - isee30-primary'

#### ise-psc.log -

05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance] com.cisco.cpm.caservice.CertificateAuthority -::::- CA Cert Template name = BYOD\_Certificate\_template 2020-12-02 05:45:11,395 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance] cisco.cpm.caservice.util.CaServiceUtil -::::- Storing certificate via REST for serial number: 518fa73a4c654df282ffdb026080de8d 2020-12-02 05:45:11,395 INFO [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance] com.cisco.cpm.caservice.CertificateAuthority -:::- issuing Certificate Services Endpoint Certificate: 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 ]

```
Eap,2020-12-02 05:46:57,175,INFO ,0x7f433e6b8700,cntx=0008591342,sesn=isee30-
primary/392215758/701,CPMSessionID=0a6a21b2000009f5fc770c7,CallingStationID=50-3e-aa-e4-81-
b6,EAP: Recv EAP packet, code=Response, identifier=64, type=EAP-TLS, length=166
,EapParser.cpp:150 Radius,2020-12-02
05:46:57,435,DEBUG,0x7f433e3b5700,cntx=0008591362,sesn=isee30-
primary/392215758/701,CPMSessionID=0a6a21b20000009f5fc770c7,user=dot1xuser,CallingStationID=50-
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=5 Length=231 [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 commence à télécharger le 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: 1 [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 = , port = 80, scheme = 3, flags = 0 [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=0a6a21b2000009c5fc4fb5e&portal=7f8ac563-

https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009c5fc4fb5e&portal=7f8ac563-3304-4f25-845d-

be9faac3c44f&action=nsp&token=29354d43962243bcb72193cbf9dc3260&redirect=10.106.33.1/auth/discove
ry [Mon Nov 30 03:34:36 2020] [HTTPConnection] CrackUrl: host = 10.106.32.119, path =
/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-

e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b20000009c5fc4fb5e&os=WINDOWS\_10\_ALL, user = , port = 8443, scheme = 4, flags = 8388608 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=bangalore;ST=Karnataka;C=IN, SAN:MAC] [Mon Nov 30 03:34:36 2020] set ChallengePwd

#### 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: [{65E78DDE-E3F1-4640-906B-15215F986CAA}]... [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: 0a6a21b2000009c5fc4fb5e, Mac: 50-3E-AA-E4-81-B6, profile: WirelessNSP [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 du 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=cisco;L=bangalore;ST=Karnataka;C=IN [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 5b 9f a2 2d 3b fc d2 86 0d a5 9b ] 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\Local\Temp\response.cer]. [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-e60300a810d5 **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 86 0d a5 9b]

#### profil

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], Single SSID [Mon Nov 30 03:35:21 2020]
WirelessProfile::IsSingleSSID - End [Mon Nov 30 03:36:07 2020] Device configured successfully.