## Guide de déploiement du BYOD sans fil pour FlexConnect

#### Table des matières

Introduction Conditions préalables Exigences Composants utilisés **Topologie** Enregistrement des périphériques et approvisionnement des demandeurs Portail d'enregistrement des actifs Portail d'auto-inscription Authentification et provisionnement Provisionnement pour iOS (iPhone/iPad/iPod) Mise en service pour Android Auto-enregistrement BYOD sans fil double SSID Auto-enregistrement BYOD sans fil SSID unique Configuration des fonctionnalités Configuration d'un réseau local sans fil (WLAN) Configuration du point d'accès FlexConnect **Configuration ISE** Expérience utilisateur - Provisionnement d'iOS SSID double SSID unique Expérience utilisateur - Mise en service Android SSID double Portail Mes périphériques **Référence - Certificats** Informations connexes

#### Introduction

Les appareils mobiles sont de plus en plus puissants et populaires auprès des consommateurs. Des millions de ces appareils sont vendus aux consommateurs grâce au Wi-Fi haut débit, ce qui permet aux utilisateurs de communiquer et de collaborer. Les consommateurs sont désormais habitués à l'amélioration de la productivité apportée par ces appareils mobiles dans leur vie et cherchent à apporter leur expérience personnelle dans l'espace de travail. Cela crée les besoins fonctionnels d'une solution BYOD (Bring Your Own Device) sur le lieu de travail.

Ce document présente le déploiement de la solution BYOD dans les filiales. Un employé se

connecte à un identifiant SSID (Service Set Identifier) d'entreprise avec son nouvel iPad et est redirigé vers un portail d'auto-inscription. Cisco Identity Services Engine (ISE) authentifie l'utilisateur par rapport à Active Directory (AD) de l'entreprise et télécharge un certificat avec une adresse MAC et un nom d'utilisateur iPad intégrés sur l'iPad, ainsi qu'un profil demandeur qui impose l'utilisation du protocole EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) comme méthode de connectivité dot1x. En fonction de la stratégie d'autorisation d'ISE, l'utilisateur peut alors se connecter à l'aide de dot1x et accéder aux ressources appropriées.

Les fonctionnalités ISE des versions du logiciel du contrôleur LAN sans fil Cisco antérieures à la version 7.2.10.0 ne prenaient pas en charge les clients de commutation locaux qui s'associaient via des points d'accès FlexConnect. La version 7.2.10.0 prend en charge ces fonctionnalités ISE pour les points d'accès FlexConnect pour la commutation locale et les clients authentifiés de manière centralisée. En outre, la version 7.2.10.0 intégrée à ISE 1.1.1 fournit (sans s'y limiter) les fonctionnalités suivantes de la solution BYOD pour les réseaux sans fil :

- Profilage et posture des périphériques
- Enregistrement des périphériques et approvisionnement du demandeur
- Intégration d'appareils personnels (mise en service d'appareils iOS ou Android)

**Remarque** : bien que pris en charge, les autres périphériques, tels que les ordinateurs portables et les stations de travail sans fil PC ou Mac, ne sont pas inclus dans ce guide.

## Conditions préalables

#### Exigences

Aucune exigence spécifique n'est associée à ce document.

#### Composants utilisés

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

- Commutateurs Cisco Catalyst
- Contrôleurs LAN sans fil (WLAN) Cisco
- Logiciel Cisco WLAN Controller (WLC) versions 7.2.110.0 et ultérieures
- AP 802.11n en mode FlexConnect
- Logiciel Cisco ISE versions 1.1.1 et ultérieures
- Windows 2008 AD avec autorité de certification (CA)
- Serveur DHCP
- Serveur DNS (Domain Name System)
- Protocole NTP (Network Time Protocol)
- Ordinateur portable client sans fil, smartphone et tablettes (Apple iOS, Android, Windows et Mac)

**Remarque** : reportez-vous aux <u>Notes de version relatives aux contrôleurs LAN sans fil Cisco</u> <u>et aux points d'accès légers Cisco pour la version 7.2.110.0</u> pour obtenir des informations importantes sur cette version du logiciel. Connectez-vous au site Cisco.com pour obtenir les dernières notes de version avant de charger et de tester le logiciel.

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. If your network is live, make sure that you understand the potential impact of any command.

#### Topologie

Une configuration minimale du réseau, comme illustré dans ce schéma, est nécessaire pour implémenter et tester correctement ces fonctionnalités :



Pour cette simulation, vous avez besoin d'un réseau avec un point d'accès FlexConnect, un site local/distant avec DHCP local, DNS, le WLC et ISE. Le point d'accès FlexConnect est connecté à une agrégation afin de tester la commutation locale avec plusieurs VLAN.

# Enregistrement des périphériques et approvisionnement des demandeurs

Un périphérique doit être enregistré pour que son demandeur natif puisse être configuré pour l'authentification dot1x. En fonction de la stratégie d'authentification appropriée, l'utilisateur est redirigé vers la page Invité et authentifié par les informations d'identification de l'employé. L'utilisateur voit la page d'enregistrement du périphérique, qui lui demande des informations sur le périphérique. Le processus de mise en service des périphériques commence alors. Si le système d'exploitation n'est pas pris en charge pour le provisionnement, l'utilisateur est redirigé vers le portail d'enregistrement des ressources afin de marquer ce périphérique pour l'accès MAC Authentication Bypass (MAB). Si le système d'exploitation est pris en charge, le processus d'inscription démarre et configure le demandeur natif du périphérique pour l'authentification dot1x.

## Portail d'enregistrement des actifs

Le portail Asset Registration Portal est l'élément de la plate-forme ISE qui permet aux employés d'initier l'intégration des terminaux via un processus d'authentification et d'enregistrement.

Les administrateurs peuvent supprimer des ressources de la page Identités des points de terminaison. Chaque employé peut modifier, supprimer et mettre sur liste noire les ressources qu'il a enregistrées. Les points d'extrémité sur liste noire sont affectés à un groupe d'identité sur liste noire et une stratégie d'autorisation est créée afin d'empêcher l'accès au réseau par les points d'extrémité sur liste noire.

## Portail d'auto-inscription

Dans le flux Central Web Authentication (CWA), les employés sont redirigés vers un portail qui leur permet d'entrer leurs informations d'identification, de s'authentifier et de saisir les détails de l'actif particulier qu'ils souhaitent enregistrer. Ce portail, appelé portail d'approvisionnement en libre-service, est similaire au portail d'enregistrement des périphériques. Il permet aux employés d'entrer l'adresse MAC ainsi qu'une description significative du terminal.

#### Authentification et provisionnement

Une fois que les employés ont sélectionné le portail d'auto-inscription, ils sont invités à fournir un ensemble d'informations d'identification valides afin de passer à la phase de mise en service. Une fois l'authentification réussie, le point de terminaison peut être mis en service dans la base de données des points de terminaison et un certificat est généré pour le point de terminaison. Un lien sur la page permet à l'employé de télécharger l'Assistant Pilote de demandeur (SPW).

**Remarque** : reportez-vous à l'article Cisco <u>FlexConnect Feature Matrix</u> afin d'afficher la dernière matrice de fonctionnalités FlexConnect pour le BYOD.

## Provisionnement pour iOS (iPhone/iPad/iPod)

Pour la configuration EAP-TLS, ISE suit le processus d'inscription Apple Over-the-Air (OTA) :

- Une fois l'authentification réussie, le moteur d'évaluation évalue les stratégies d'approvisionnement du client, ce qui génère un profil de demandeur.
- Si le profil demandeur est défini pour le paramètre EAP-TLS, le processus OTA détermine si l'ISE utilise la signature automatique ou la signature d'une autorité de certification inconnue. Si l'une des conditions est remplie, l'utilisateur est invité à télécharger le certificat d'ISE ou d'AC avant que le processus d'inscription puisse commencer.
- Pour les autres méthodes EAP, ISE envoie le profil final lors d'une authentification réussie.

## Mise en service pour Android

Pour des raisons de sécurité, l'agent Android doit être téléchargé depuis le site Android Marketplace et ne peut pas être mis en service depuis ISE. Cisco télécharge une version candidate de l'assistant sur le marché Android via le compte de l'éditeur du marché Android.

Voici le processus de mise en service d'Android :

- 1. Cisco utilise le kit de développement logiciel (SDK) afin de créer le package Android avec une extension .apk.
- 2. Cisco télécharge un package sur le marché Android.
- 3. L'utilisateur configure la stratégie dans le provisionnement du client avec les paramètres appropriés.
- 4. Après l'enregistrement du périphérique, l'utilisateur final est redirigé vers le service d'approvisionnement du client lorsque l'authentification dot1x échoue.
- 5. La page du portail d'approvisionnement fournit un bouton qui redirige l'utilisateur vers le portail Android Marketplace où il peut télécharger le SPW.
- 6. Le SPW Cisco est lancé et effectue le provisionnement du demandeur : SPW découvre l'ISE et télécharge le profil depuis ISE.SPW crée une paire certificat/clé pour EAP-TLS.SPW effectue un appel de requête proxy SCEP (Simple Certificate Enrollment Protocol) vers ISE et obtient le certificat.SPW applique les profils sans fil.SPW déclenche une nouvelle authentification si les profils sont correctement appliqués.Le SPW se ferme.

## Auto-enregistrement BYOD sans fil double SSID

Voici le processus d'auto-enregistrement du BYOD sans fil avec double SSID :

- 1. L'utilisateur s'associe au SSID Invité.
- 2. L'utilisateur ouvre un navigateur et est redirigé vers le portail invité ISE CWA.
- 3. L'utilisateur saisit un nom d'utilisateur et un mot de passe d'employé dans le portail invité.
- 4. ISE authentifie l'utilisateur et, en fonction du fait qu'il s'agit d'un employé et non d'un invité, le redirige vers la page d'accueil Enregistrement des périphériques de l'employé.
- 5. L'adresse MAC est préremplie dans la page d'accueil Enregistrement du périphérique pour l'ID de périphérique. L'utilisateur saisit une description et accepte la politique d'utilisation acceptable (AUP) si nécessaire.
- 6. L'utilisateur sélectionne Accept et commence à télécharger et à installer le SPW.
- 7. Le demandeur de l'appareil de cet utilisateur est mis en service avec tous les certificats.
- La CoA se produit, et le périphérique se réassocie au SSID d'entreprise (CORP) et s'authentifie avec EAP-TLS (ou une autre méthode d'autorisation utilisée pour ce demandeur).

## Auto-enregistrement BYOD sans fil SSID unique

Dans ce scénario, il y a un seul SSID pour l'accès d'entreprise (CORP) qui prend en charge à la fois le protocole PEAP (Protected Extensible Authentication Protocol) et EAP-TLS. Il n'y a pas de SSID invité.

Il s'agit du processus d'auto-enregistrement BYOD sans fil SSID unique :

1. L'utilisateur s'associe à CORP.

- 2. L'utilisateur saisit un nom d'utilisateur et un mot de passe d'employé dans le demandeur pour l'authentification PEAP.
- 3. L'ISE authentifie l'utilisateur et, sur la base de la méthode PEAP, fournit une politique d'autorisation d'acceptation avec redirection vers la page d'invité Enregistrement des périphériques des employés.
- 4. L'utilisateur ouvre un navigateur et est redirigé vers la page d'accueil Enregistrement des périphériques des employés.
- 5. L'adresse MAC est préremplie dans la page d'accueil Enregistrement du périphérique pour l'ID de périphérique. L'utilisateur saisit une description et accepte le protocole AUP.
- 6. L'utilisateur sélectionne Accept et commence à télécharger et à installer le SPW.
- 7. Le demandeur de l'appareil de cet utilisateur est mis en service avec tous les certificats.
- 8. CoA se produit et le périphérique se réassocie au SSID CORP et s'authentifie avec EAP-TLS.

#### Configuration des fonctionnalités

Complétez ces étapes afin de commencer la configuration :

1. Pour ce guide, assurez-vous que la version du WLC est 7.2.110.0 ou ultérieure.



2. Accédez à Security > RADIUS > Authentication, et ajoutez le serveur RADIUS au WLC.

ll cisco	MONITOR	WLANS (	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP [	EEOBACK
Security	RADIUS	Authentica	tion Serve	rs					
AAA     General     RADIUS     Authentication     Accounting     Fallback     TACACS+     LDAP	Call Stat Use AES MAC De Network User	Son ID Type I Key Wrap Simiter Managemen	System M (Designed Hyphen Server t Index	AC Address 1 for FIPS custome	ers and require	es a key wrap com	oliant RADIUS se Nec	rver) Admin 1	Status
Local Net Users MAC Filtering			1	10.10.10.60	1812	D	isabled	Enabled	
Disabled Clients User Login Policies									

3. Ajoutez l'ISE 1.1.1 au WLC :

Saisissez un secret partagé.Définissez Support for RFC 3576 sur Enabled.

MONITOR WLANS O	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBAC
RADIUS Authentica	tion Servers	s > Edit					
All of the Sector							
Server Index		1					
Server Address		10.10.10.60					
Shared Secret Format		ASCII :					
Shared Secret							
Confirm Shared Secret							
Key Wrap		(Designed fo	r FIPS custome	ers and requires a k	key wrap complia	nt RADIU	S server)
Port Number		1812					
Server Status		Enabled :					
Support for RFC 3576		Enabled :	0				
Server Timeout		2 second	is				
Network User		S Enable					
Management		S Enable					
IPSec		Enable					

4. Ajoutez le même serveur ISE qu'un serveur de comptabilité RADIUS.

MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANA	
RADIUS Accounti	ng Servers >	Edit			
Server Index	1				
Server Address	10.1	0.10.60			
Shared Secret Format	ASC	* II			
Shared Secret	•••				
Confirm Shared Secre	et				
Port Number	1813	1813			
Server Status	Ena	bled 0			
Server Timeout	2	seconds			
Network User	🗹 E	nable			
IPSec		Enable			

 Créez une liste de contrôle d'accès de pré-authentification WLC à utiliser dans la stratégie ISE ultérieurement. Naviguez jusqu'à WLC > Security > Access Control Lists > FlexConnect ACLss, et créez une nouvelle ACL FlexConnect nommée ACL-REDIRECT (dans cet exemple).

cisco		<u>W</u> LANs		WIF
Security	FlexConr	nect Aco	cess Control Li	ists
<ul> <li>AAA</li> <li>Local EAP</li> <li>Priority Order</li> <li>Certificate</li> </ul>	Acl Name	ECT		
Access Control Lists     Access Control Lists     CPU Access Control Lists     FlexConnect ACLs     Wireless Protection     Policies				

6. Dans les règles de liste de contrôle d'accès, autorisez tout le trafic vers/depuis l'ISE et autorisez le trafic client pendant le provisionnement du demandeur.

Pour la première règle (séquence 1) :

Définissez Source sur **Any**.Définissez IP (adresse ISE)/ Netmask **255.255.255.255**.Définir l'action sur **Autoriser**.

Access Control List	ts > Rules > Edit		
Sequence	1		
Source	Any :		
		IP Address	Netmask
Destination	IP Address ‡	10.10.10.60	255.255.255.255
Protocol	Any		
DSCP	Any ÷		
Direction	Any :		
Action	Permit ‡		

Pour la deuxième règle (séquence 2), définissez l'adresse IP source (adresse ISE)/ masque 255.255.255 sur **Any** et l'action sur **Permit**.

Gene	ral									
Access	s List Name	ACL-RED	IR	ECT						
Seq	Action	Source IP/Mask	:	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCF	,
1	Permit	0.0.0.0 0.0.0.0	/	10.10.10.60 255.255.255.255	/	Any	Any	Any	Any	
2	Permit	10.10.10.60 255.255.255.255	/	0.0.0.0	1	Any	Any	Any	Any	

7. Créez un nouveau groupe FlexConnect nommé Flex1 (dans cet exemple) :

Accédez à **FlexConnect Group > WebPolicies** tab.Dans le champ ACL WebPolicy, cliquez sur **Add**, et sélectionnez **ACL-REDIRECT** ou l'ACL FlexConnect créée précédemment.Confirmez qu'il renseigne le champ **Listes de contrôle d'accès WebPolicy**.

uluili. cisco	MONITOR WLANS CONTROLLER WERELESS SECURITY MANAGEMENT COMMANDS HELP	Sage Configuration   Bing   Logout   Befine EEEDBACK
Wireless	FlexConnect Groups > Edit 'Flex1'	< Back Apply
Access Points     All APs     Radios     OPD 114-00	General Local Authentication Image Upgrade VLAN-ACL mapping WLAN-ACL ma	pping WebPolicies
802.11b/g/h Global Configuration	WebPolicies	
Mesh RF Profiles FlexConnect Groups	Metroley ACL ACLIEDIRECT	
HerConnect ACCS > 802.11a/n > 802.11b/g/n	ACL-REDIRECT	
▶ Media Stream		

8. Cliquez sur Apply et sur Save Configuration.

#### Configuration d'un réseau local sans fil (WLAN)

Complétez ces étapes afin de configurer le WLAN :

1. Créez un SSID WLAN ouvert pour l'exemple de double SSID :

Entrez un nom WLAN : **DemoCWA** (dans cet exemple).Sélectionnez l'option **Enabled** pour Status.

WLANs > E	dit 'Demo	CWA'	
General	Security	QoS	Advanced
Profile Na	me	DemoC	WA
Туре		WLAN	
SSID		DemoC	WA
Status		F Enat	bled
Security I	Policies	MAC F (Modifica	iltering ations done under se
Radio Pol	icy	All	
Interface Group(G)	/Interface	manag	ement 💌
Multicast	Vlan Feature	Enab	led
Broadcas	t SSID	₩ Enab	led

2. Accédez à l'onglet Security > Layer 2 et définissez ces attributs :

Sécurité de couche 2 : **aucune**Filtrage MAC : **activé** (case cochée)Transition rapide : **Désactivé** (case non cochée)

_ANs > E	dit 'Demo	CWA'			
General	Security	QoS	Advanced		
Layer 2	Layer 3	AAAS	ervers		
Layer 2 Security MAC Filtering					
Fast Tran	Mé	C Filterin	9 <mark>2</mark> 🔽		
Fast Tran Fast Transi	M#	AC Filterin	¶ 2g		

3. Accédez à l'onglet AAA Servers, et définissez ces attributs :

Serveurs d'authentification et de compte : activéServeur 1 : <adresse IP ISE>

eneral Se	curity	QoS Advanced
Layer 2 L	ayer 3	AAA Servers
Select AAA sen	vers belo	ow to override use of default servers on this WLAN
Badless Commen		
Radius Servers Radius Serve	er Overw	rite interface Enabled
Radius Servers Radius Serve	er Overw	rite interface Enabled Authentication Servers Accounting Servers Servers Enabled
Radius Servers Radius Serve Server 1	er Overw	rite interface Enabled  Authentication Servers Accounting Servers  Enabled  IP:10.10.10.60, Port:1812  IP:10.10.10.60, Port:1812
Radius Servers Radius Serve Server 1 Server 2	er Overw	rite interface Enabled           Authentication Servers         Accounting Servers           Image: Servers         Image: Servers

4. Faites défiler l'onglet **AAA Servers**. Sous Ordre de priorité d'authentification pour l'utilisateur d'authentification Web, assurez-vous que **RADIUS** est utilisé pour l'authentification et que les autres ne sont pas utilisés.

Authentication prior web-auth user	rity order for	-	
Not Used LOCAL LDAP	> <	Order Used For Authentic	Up Down

5. Accédez à l'onglet Avancé, et définissez ces attributs :

Allow AAA Override	F Enabled	0.002
Coverage Hole Detection	P Enabled	DHCP Server Coversid
Enable Secolor Timeout	gr (1800 Session Timesut (sess)	DHCP Adds. Assignment T Annuire
Aironat IE	\$P Brakind	Nanaparent Frame Postsching (NFF
Diagnostic Channel	["Evabled	
Override Interface ACL	Post None R Post None R	1879 Class Protection . Optional
F2F Blocking Action	Constrained in	BTIM Period (in kearon intervals)
Clarit Exclusion	C'Evabled	
Maximum Allowed Clients	F	802.33.wh (3 - 298) [3 802.333/ph (3 - 299) [3
Static IP Tunneling 🛤	C Enabled	NAC
wi-Fi Direct Clients Policy	Doabled R	NAC State Radius NAC 💌
Recimum Allowed Cleanty Fer AT Radio	[200	Card Balancing and Band Veloci

Autoriser le remplacement AAA : activéÉtat NAC : Radius NAC

**Remarque** : le contrôle d'admission réseau (NAC) RADIUS n'est pas pris en charge lorsque le point d'accès FlexConnect est en mode déconnecté. Ainsi, si le point d'accès FlexConnect est en mode autonome et perd la connexion au WLC, tous les clients sont déconnectés et le SSID n'est plus annoncé.

6. Faites défiler la page vers le bas dans l'onglet Avancé et définissez Commutation locale FlexConnect sur **Activé**.



7. Cliquez sur Apply et sur Save Configuration.



8. Créez un SSID WLAN 802.1X nommé **Demo1x** (dans cet exemple) pour les scénarios SSID simple et double.

WLANs > Edit 'Demo	1x'
General Security	QoS Advanced
Profile Name	Demoix
Туре	WLAN
SSID	Demo1x
Status	Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under secu
Radio Policy	All
Interface/Interface Group(G)	management 💌
Multicast Vlan Feature	Enabled
Broadcast SSID	Enabled

9. Accédez à l'onglet Security > Layer 2 et définissez ces attributs :

Sécurité de couche 2 : **WPA+WPA2**Transition rapide : **Désactivé** (case non cochée)Gestion des clés d'authentification : 802.IX : **Activer** 

eneral	Security	QoS	Advanced
Layer 2	Layer 3	AAA Se	rvers
1	Carrier 6 1	WDA+WDA2	
Layer 2	Security ~ []	AC Filtering	
Fast Trans	sition		
East Transit	ion E		
Over the DS			
ALEL OLE P.	-		
Peacenciatio	on Timeout 20		
Reassociatio	on Timeout 20		
Reassociatio	on Timeout 20 2 Parameter	rs	
Reassociatio WPA+WPA WPA Pol	on Timeout 20 2 Parameter licy	rs	
WPA+WPA WPA Pol	on Timeout 20 2 Parameter licy	ns	
Reassociati WPA+WPA WPA Pol WPA2 Po	on Timeout 20 2 Parameter licy olicy	2010 2010 2010 2010 2010 2010 2010 2010	
Reassociati WPA+WPA WPA Pol WPA2 Pol WPA2 Er	on Timeout 20 2 Parameter licy olicy ncryption	rs F F AES	□ткі
Reassociation WPA+WPA WPA Pol WPA2 Pol WPA2 En Authentica	on Timeout 20 2 Parameter licy olicy ncryption ation Key Ma	rs F AES nagement	Гткі
Reassociation WPA+WPA WPA Pol WPA2 Pol WPA2 En Authentica 802.1X	on Timeout 20 2 Parameter licy olicy ncryption ation Key Ma	rs	Гткі
Reassociation WPA+WPA WPA Pol WPA2 Pol WPA2 En Authentica 802.1X CCKM	on Timeout 20 2 Parameter licy olicy ncryption ation Key Ma	rs	⊏ткі

10. Accédez à l'onglet Avancé, et définissez ces attributs :

Autoriser le remplacement AAA : activéÉtat NAC : Radius NAC

Now AAA Override	F Enabled	Best P
Coverage Hole Detection	P Enabled	DHCP Server Coverride
Inable Session Timesult	gr [1900	
inunat II	W English	DHCP ABP. Assignment [ Required
Sagnutic Channel	Created	Management Frame Protection (NFP)
Iverride Interface ACL	Put fars 2 Put fars 2	MPR Claud Rodention . Collected .
OF Blocking Action	Disabled R	DTIN Period (in beauty internals)
Sant Exclusion	Render In	and a second for the second second second
	Timeout Value (secs)	802.33m/h (3 - 299) [3
Sants	9	882.135/ph (1 - 298) [1
and in the second second	Chuthe	NAC

11. Faites défiler vers le bas dans l'onglet **Advanced**, et définissez FlexConnect Local Switching sur **Enabled**.

FlexConnect	
FlexConnect Local Switching <sup>2</sup>	☑ Enabled
Rectanged and had	· P susses

12. Cliquez sur Apply et sur Save Configuration.



13. Vérifiez que les deux nouveaux WLAN ont été créés.

MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
WLANs								Entries 1 - 5 of 2
Current Fi	lter: Nor	ne [Change	Filter] [Clear	Filter]	1	Create New	• G	0
	ID Туре	Profile Na	me		VLAN SSID		Admin Status	Security Policies
E 1	WLAS	85×			LEH .		Disable	6 [WPA2[[Auth(952.14]]
C 2	WLAN						Enabled	[#PA2][Auth(PS2)]
□ <u>2</u>	WLAN	Demo1x		C	Demo1x		Enabled	[WPA2][Auth(802.1X)]
□ <u>4</u>	WLAN	DemoCWA		C	DemoCWA		Enabled	MAC Filtering
E 1	WLAS	fig-r			les .		Creatile	d Web-Auth

#### Configuration du point d'accès FlexConnect

Complétez ces étapes afin de configurer le point d'accès FlexConnect :

1. Accédez à WLC > Wireless, et cliquez sur le point d'accès FlexConnect cible.

MONITOR	<u>W</u> LANs		WIRELESS
All APs			
Current Fil	ter		None
Number o	f APs		2
AP Name		AP	Model
Site-B-Flex		AI	R-LAP1262N-A-K

2. Cliquez sur l'onglet FlexConnect.



3. Activez la prise en charge VLAN (case cochée), définissez l'ID du VLAN natif, puis cliquez sur VLAN Mappings.

VLAN Support	2	
Native VLAN ID	1	VLAN Mappings
FlexConnect Group Name	Not Cont	figured 😡

4. Définissez l'ID de VLAN sur **21** (dans cet exemple) pour le SSID pour la commutation locale.

	<u>W</u> LANs		WIRELESS	SECURITY
All APs	> Site-B-	FlexAP > VLA	N Mapping	s
AP Nam	e	Site-B-FlexAP		
Base Ra	dio MAC	e8:04:62:0a:68:80	D	
WLAN Id	SSID			VLAN ID
3	Demo1x			21
4	DemoCW/	4		21
				- AND CONTRACT PAGE

5. Cliquez sur Apply et sur Save Configuration.

#### **Configuration ISE**

Complétez ces étapes afin de configurer l'ISE :

1. Connectez-vous au serveur ISE : <https://ise>.

	Identity Services Engine
© 2012 Class Systems, Jrc. Class, Class Systems and Class Systems Ing efficience in the U.S and certain other countries.	p are registered trademarks of Caso Systems, Disc. and/or its

2. Accédez à Administration > Identity Management > External Identity Sources.



3. Cliquez sur Active Directory.



4. Dans l'onglet Connexion :

Ajoutez le nom de domaine de **corp.rf-demo.com** (dans cet exemple) et remplacez le nom du magasin d'identités par défaut par **AD1**.Cliquez sur **Save Configuration**.Cliquez sur **Joindre**, et fournissez le nom d'utilisateur et le mot de passe du compte Administrateur AD requis pour joindre.L'état doit être vert. Enable **Connected to :** (case cochée).

Connection	Advanced Settin	gs	Groups	At	tributes		
		* Don	nain Name	corp.rf-d	emo.com		
	* Id	entity S	tore Name	AD1			
an er men enden	marks asland a	a lala a		and an a	la nada la laina	d there a law	
ne or more nodes connection. 약 Join 약 Leave	may be selected fo	ion -	or Leave ope	rations. I	f a node is joine	ed then a lea	we operation is
one or more nodes connection. 9 Join 9 Leave	may be selected fo	ion +	or Leave ope	ole	fa node is joine Status	ed then a lea	we operation is

5. Effectuer un test de connexion de base à AD avec un utilisateur de domaine actuel.

oonneedon.			
👷 Join 🛛 👷 Leave	👷 Test Connection 👻		
ISE Node	Basic Test		
✓ ise11-mnr Detailed Test			
Test Connection * User Name: paul * Password:	×		

6. Si la connexion à Active Directory réussit, une boîte de dialogue confirme que le mot de passe est correct.



7. Naviguez jusqu'à Administration > Identity Management > External Identity Sources :

Cliquez sur **Certificate Authentication Profile**.Cliquez sur **Add** pour un nouveau profil d'authentification de certificat (CAP).

cisco Identity Service	s Engine		
🛕 Home Operations 🔻	Policy 🔻 Administr	ation 🔻	
🔆 System 🦉 Identity M	lanagement 🔛 Net	twork Resources	🛃 Web Portal Manage
Identities Groups Extern	nal Identity Sources	Identity Source Seq	uences Settings
External Identity Sources		Certificate Aut	hentication Profile
<b>∲•</b>	ŵ.	I co ala	
Certificate Authentication Profi	ie 💿	Coic Mr. Add	
Active Directory		Name V	4
CDAP LDAP	۲		
RADIUS Token	۲		
RSA SecurID			

8. Entrez le nom **CertAuth** (dans cet exemple) pour le CAP ; pour l'attribut Principal Username X509, sélectionnez **Common Name**, puis cliquez sur **Submit**.

Certificate Authentication Profiles List > New	Certificate Authentication Profile	
Certificate Authentication Pr	ofile	
* Name	CertAuth	
Description		
Principal Username X509 Attribute	Common Name	*
Perform Binary Certificate Compo LDAP/AD Instance Name	arison with Certificate retrieved fro	om LDAP or Active Directory
Submit Cancel		

9. Vérifiez que le nouveau CAP est ajouté.

cisco Identity Services Engine	
🍐 Home Operations 🔻 Policy 🔻 Admini	stration 🔻
🔆 System 🦉 Identity Management 📰 I	Network Resources 🛛 🛃 Web Portal Management
Identities Groups External Identity Sources	Identity Source Sequences Settings
External Identity Sources	Certificate Authentication Profile
<b>♦•</b>	
Certificate Authentication Profile	
2 Active Directory	Name
🚞 LDAP 💿	Certie an
RADIUS Token ()	
🚞 RSA SecurID 💿	

10. Accédez à Administration > Identity Management > Identity Source Sequences, et cliquez sur Add .

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 🖉	Administration 🔻
🔆 System 🏾 👰 Identity Management	Network Resources 🛛 🛃 Web Portal Management
Identities Groups External Identity Sour	rces Identity Source Sequences Settings
Identity Source Sequence	
Name	Description
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal
MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Po
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal

11. Attribuez à la séquence le nom **TestSequence** (dans cet exemple).

cisco Id	entity Services Engine
💧 Home	Operations   Policy   Administration
🔆 System	Veb Portal Mana
Identities (	Groups External Identity Sources Identity Source Sequences Settings
Identity Source Seq Identity Sou Identity Sou	uences List > New Identity Source Sequence rce Sequence urce Sequence
* Name	TestSequence
Description	
<ul> <li>Certificate</li> </ul>	e Based Authentication

12. Faites défiler jusqu'à Certificate Based Authentication :

Enable Select Certificate Authentication Profile (case cochée). Sélectionnez CertAuth (ou un autre profil CAP créé précédemment).

<ul> <li>Certificate Based Authentication</li> </ul>	
Select Certificate Authentication Profile	CertAuth 💌
<ul> <li>Authentication Search List</li> </ul>	

13. Faites défiler jusqu'à Authentication Search List :

Déplacer AD1 de Disponible à Sélectionné.Cliquez sur le bouton Haut afin de déplacer AD1 vers la priorité supérieure.

▼ Authentication Search List			
A set of identity sources that will be accessed in sequence until first authentication succeeds			
Available		Selected	_
	*	Internal Users Internal Endpoints	
	>> *		V V

14. Cliquez sur Submit afin d'enregistrer.

Advanced Search List Settings Select the action to be performed if a selected identity store cannot be accessed for authentication
<ul> <li>Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"</li> <li>Treat as if the user was not found and proceed to the next store in the sequence</li> </ul>
Submit

15. Vérifiez que la nouvelle séquence source d'identité est ajoutée.

cisco Identity Services Engine	all'all'a	
🛕 Home Operations 🔹 Policy 💌 Administrat	tion 🔹	
🔆 System 🛛 🖉 Identity Management 🖉 Netv	work Resources 🚯 Web Portal Management	
Identities Groups External Identity Sources	dentity Source Sequences Settings	
Identity Source Sequence		
Edit - Add L Duplicate X Delete		
Name .	Description	Identity Stores
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users
TestSequence		CertAuth, Internal Users, Internal Endpoints

16. Utilisez AD afin d'authentifier le portail Mes périphériques. Accédez à ISE > Administration
 > Identity Management > Identity Source Sequence, et modifiez
 MyDevices\_Portal\_Sequence.

🔆 System 🏾 👰 Identity Management	Network Resources 🛛 🛃 Web
Identities Groups External Identity Source	Identity Source Sequences
dentity Source Sequence	
/Edit 🕂 Add 🖓 Duplicate 🗙 Delete	
/Edit 🛖Add 🖓Duplicate 🗙Delete	Description
/ Edit + Add Duplicate XDelete	Description     A Built-in Identity Sequence
Edit + Add Duplicate XDelete     Name     Guest_Portal_Sequence     MyDevices_Portal_Sequence	Description     A Built-in Identity Sequence     A Built-in Identity Sequence
Edit + Add Duplicate XDelete     Name     Guest_Portal_Sequence     MyDevices_Portal_Sequence     Sponsor_Portal_Sequence	Description     A Built-in Identity Sequence     A Built-in Identity Sequence     A built-in Identity Sequence

17. Ajoutez **AD1** à la liste Sélectionné et cliquez sur le bouton Haut afin de déplacer AD1 vers la priorité supérieure.



18. Cliquez sur Save.



19. Vérifiez que la séquence de magasin d'identités pour MyDevices\_Portal\_Sequence contient **AD1**.



20. Répétez les étapes 16 à 19 afin d'ajouter AD1 pour Guest\_Portal\_Sequence, et cliquez sur **Save**.



21. Vérifiez que Guest\_Portal\_Sequence contient AD1.

	Name	Description	Identity Stores
Ð	Guest_Portal_Sequence	A Built-in Identity Sequence For The Guest Portal	Internal Users, AD1
100			

22. Afin d'ajouter le WLC au périphérique d'accès réseau (WLC), naviguez à Administration > Ressources réseau > Périphériques réseau, et cliquez sur Add.

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 💌 Adminis	tration 🔻
Network Devices Network Device Groups Exte	mal RADIUS Servers RADIUS Server Sequences Network Devices
v     v    v	/ Edit Add Duplicate Import

23. Ajoutez le nom du WLC, l'adresse IP, le masque de sous-réseau, etc.

Network Devices List > New Net	twork Device		
Network Devices			
* Name Description	WLC		
* IP Address:	10.10.10.5 / 32		
Model Name Software Version	×		
* Network Device Group			
Location	All Locations 📀 Set To Default		
Device Type	All Device Types 📀 Set To Default		

24. Faites défiler jusqu'à Authentication Settings, puis saisissez Shared Secret. Cela doit correspondre au secret partagé du WLC RADIUS.

•	▼ Authentication Settings		
	Enable Authentication Settings Protocol	RADIUS	
	* Shared Secret	•••••	Show
	Enable KeyWrap		
	<ul> <li>Key Encryption Key</li> </ul>		Show
	<ul> <li>Message Authenticator Code Key</li> </ul>		Show
	Key Input Format	ASCII HEXADECIM	AL
	SNMP Settings		
	SGA Attributes		
Sub	mit Cancel		

- 25. Cliquez sur Submit.
- 26. Accédez à ISE > Policy > Policy Elements > Results.

cisco Identity Service	es Engine
🛕 Home Operations 🔻	Policy  Administration
System      Identity I     Network Devices     Network Devices	<ul> <li>Authentication</li> <li>Authorization</li> <li>Profiling</li> <li>Posture</li> <li>Client Provisioning</li> <li>Security Group Access</li> </ul>
Network Devices	Network Device Authorization
	Policy Elements Dictionaries Conditions Results

27. Développez **Results** and **Authorization**, cliquez sur **Authorization Profiles**, puis cliquez sur **Add** pour un nouveau profil.

cisco Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 Admin	istration 🔻
🛃 Authentication 💿 Authorization 🔀 P	Profiling 🕐 Posture 😡 Client Provisioning
Dictionaries Conditions Results	
Results	Standard Authorization Profiles
P	/ Edit Add C Duplicate X Delete
Authentication	Name V
* 🧰 Authorization	Blackist_Access
🔻 🧱 Authorization Profiles	
Garage Blacklist_Access	DenvAccess

28. Donnez à ce profil les valeurs suivantes :

Nom : CWA

Authorization Profiles > Authorization	New Authorization Profile Profile
* Name	CWA
Description	
* Access Type	ACCESS_ACCEPT +

Activer l'authentification Web (case cochée) :

Authentification Web : **centralisée**ACL : **ACL-REDIRECT** (Cela doit correspondre au nom de l'ACL de pré-auth du WLC.)Redirection : **par défaut** 

<ul> <li>Common Tasks</li> </ul>							
DACL Name							
ULAN VLAN							
Voice Domain Permissio	n						
Web Authentication	Centralized	*	ACL	ACL-REDIRECT	Redirect	Default	•

29. Cliquez sur Submit, et confirmez que le profil d'autorisation CWA a été ajouté.



30. Cliquez sur Add afin de créer un nouveau profil d'autorisation.



- 31. Donnez à ce profil les valeurs suivantes :
  - Nom : Provisionnement

Authorization Profiles > Authorization	New Authorization Profile Profile
* Name	Provision
Description	
* Access Type	ACCESS_ACCEPT 🔹

Activer l'authentification Web (case cochée) :

Valeur d'authentification Web : Approvisionnement du demandeur



ACL : ACL-REDIRECT (Cela doit correspondre au nom de l'ACL de pré-auth du WLC.)

Common Tasks		
DACL Name		
VLAN		
Voice Domain Permission		
G Web Authentication	Supplicant Provisioning	ACL ACL-REDIRECT
C Auto Smart Bort		

32. Cliquez sur **Submit**, et confirmez que le profil d'autorisation Provisionnement a été ajouté.



33. Faites défiler vers le bas dans Résultats, développez **Approvisionnement client**, et cliquez sur **Ressources**.



34. Sélectionnez Profil du demandeur natif.



35. Attribuez au profil le nom WirelessSP (dans cet exemple).

Native Supplicant Profil	e
* Name	WirelessSP
Description	

36. Entrez les valeurs suivantes :

Type de connexion : **sans fil**SSID : **Demo1x** (cette valeur provient de la configuration WLAN WLC 802.1x)Protocole autorisé : **TLS**Taille de la clé : **1024** 

Operating System	ALL 💠		
Connection Type	Wired		
	Vireless		
		*SSID	Demoix
		Security	WPA2 Enterprise 🔹
* Allowed Protocol	PEAP		v
Optional Settings	TLS PEAP	ę	2
Submit Cancel			

- 37. Cliquez sur Submit.
- 38. Cliquez sur Save.

* Allowed Protocol	TLS	•
* Key Size	1024	
Save Reset		

39. Vérifiez que le nouveau profil a été ajouté.

Resources						
/ Edit Add - Duplicate	XDelete					
Name	Туре					
Wireless	NativeSPProfile					

40. Accédez à Policy > Client Provisioning.



41. Saisissez les valeurs suivantes pour la règle de mise en service des périphériques iOS :

Nom de la règle : iOSGroupes d'identités : Tous

Rule Name	Ide	ntity Groups	5	Operating Syste	ms	0	ther Conditions
IOS	If A	ny 💠	and	Choose a	-	and	Condition(s)
				Choose an	Operat	ting S	ystem 👷 🕂
	Rule Name	Rule Name Ide	Rule Name Identity Groups	Rule Name Identity Groups IOS If Any I and	Rule Name     Identity Groups     Operating System       IOS     If     Any     and       Choose a     Choose a	Rule Name     Identity Groups     Operating Systems       IOS     If     Any     and     Choose a       Ichoose an Operation     Ichoose an Operation	Rule Name     Identity Groups     Operating Systems     O       IOS     If     Any     and     Choose a     and       Choose an Operating System     Image: Choose a     Image: Choose a     Image: Choose a     Image: Choose a

Systèmes d'exploitation : Mac iOS All

Operating System Grou	ups
	Q
<b>◆•</b> ■ '≡	ŵ
Android	
Mac OSX	
Mac iOS All	
🚞 Windows All 🖼	۲

Résultats : WirelessSP (il s'agit du profil de demandeur natif créé précédemment)

ther Conditions	Results
	then Result 🕀 🥎

Accédez à Results > Wizard Profile (liste déroulante) > WirelessSP.



WizardProfile	
	R
<b>◆</b> • ■ '≣	ŵ
Clear Selection	
Wireless	

42. Vérifiez que le profil de mise en service iOS a été ajouté.

			Rule Name	I	identity Gr	roups		Operating System	ns		Other Conditions		Results	
1	¥.	٠	105	If [	Any	$\diamond$	and	Mac IOS All	$\diamond$	and	Condition(s)	\$ then	WrelessSP	$\diamond$

43. Sur le côté droit de la première règle, localisez la liste déroulante Actions et sélectionnez **Dupliquer ci-dessous** (ou ci-dessus).



44. Remplacez le nom de la nouvelle règle par Android.



45. Remplacez les systèmes d'exploitation par Android.



- 46. Laissez les autres valeurs inchangées.
- 47. Cliquez sur Save (Enregistrer) (écran inférieur gauche).



48. Accédez à ISE > Policy > Authentication.



49. Modifiez la condition pour inclure Wireless\_MAB et développez Wired\_MAB.



50. Cliquez sur la liste déroulante Nom de la condition.



51. Sélectionnez Dictionaries > Compound Condition.



52. Sélectionnez Wireless\_MAB.



53. Àdroite de la règle, sélectionnez la flèche à développer.

: If Wireless_MAB I allow protocols Allowed Protocol : Default Netwo and	5
--	---

54. Sélectionnez ces valeurs dans la liste déroulante :

Source d'identité : **TestSequence** (valeur créée précédemment)Si l'authentification a échoué : **Reject**Si utilisateur introuvable : **Continuer**Si le processus a échoué : **Abandonner** 

use	TestSequence 🗢
	Identity Source TestSequence
	Options
	If authentication failed Reject
History	If user not found Continue
	If process failed Drop 🔹

55. Accédez à la règle Dot1X, et modifiez ces valeurs :



Con	npound Condition
	(م
4	· 🔳 📜 🙀 🍇
	Wired_MAB
	Wireless_MAB
	Wired_802.1X
ш.	Wireless_802.1X Jhn
	Switch_Local_Web_Authentication
	WLC_Web_Authentication
:If :all	Wired_802.1X allo Wired_802.1X allo Add All Conditions Below t Condition Name Wireless_802.1X O

Condition : Sans fil\_802.1X

Source d'identité : TestSequence

Identity Source TestSequence	se for authe
Options	Identity Source List
If authentication failed Reject	
If user not found Reject *	[م]
If process failed Drop 🔹	<b>♦•</b>
Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS	Internal Endpoints
it is not possible to continue processing when authentication fails a	Internal Users
If continue option is selected in these cases, requests will be reject	Guest_Portal_Sequence
	Sponsor_Portal_Sequence
	MyDevices_Portal_Sequence
	TestSequence
Internal Users 👄	CertAuth
	DenyAccess

56. Cliquez sur **Save**.



57. Accédez à ISE > Policy > Authorization.



58. Les règles par défaut (telles que Liste noire par défaut, Profil et Par défaut) sont déjà configurées à partir de l'installation ; les deux premières peuvent être ignorées ; la règle par défaut sera modifiée ultérieurement.

rst M	fatched R	ule Applies +			
Exc	eptions (	0)			
Star	ndard				
	Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
		Black List Default	f Blacklist	then	Blacklist_Access
	-	Deallard Gross 10 Diseased	Cisco-ID-Diseas	then	Care ID Dhone

59. Àdroite de la deuxième règle (téléphones IP Cisco avec profil), cliquez sur la flèche vers le bas en regard de Edit, puis sélectionnez **Insert New Rule Below**.



Un nouveau numéro de règle standard est ajouté.

	Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
1		Black List Default	f Blackist	then Blackist_Access
		Profiled Osco IP Phones	Cisco-IP-Phone	then Osco_IP_Phones
12	- 1	Standard Rule 1	f Any $\Diamond$ and Condition(s) $\Diamond$	then AuthZ Profil 💠
		Default	If no matches, then PermitAccess	

60. Remplacez le nom de la règle Standard Rule # par **OpenCWA**. Cette règle lance le processus d'enregistrement sur le WLAN ouvert (SSID double) pour les utilisateurs qui viennent sur le réseau invité afin d'avoir des périphériques provisionnés.



61. Cliquez sur le signe plus (+) pour Condition(s), puis cliquez sur **Sélectionner une condition** existante dans la bibliothèque.

Cisco-IP-Phone		then Cisco_IP_Phone
f Any 💠 an	d Select Condition	Select Existing Condition from Library (2) or Create

62. Sélectionnez Compound Conditions > Wireless\_MAB.

٩
🔶 🗐 🗐 🛞 -
Wired_802.1X
Wired_MA8
Wireless_802.1X
Wireless_MAB
Catalyst_Switch_cocal_Web_Authentica
WLC_Web_Authentication

63. Dans le profil AuthZ, cliquez sur le signe plus (+), puis sélectionnez Standard.
|                | Profiles              |               |
|----------------|-----------------------|---------------|
|                |                       | P             |
| licy Elements  | <b>∲-</b> ■ '≣        | \$\$ <b>.</b> |
|                | 🚞 Inline Posture Node | ۲             |
|                | 🚞 Security Group      | ۲             |
|                | Standard 🔓            | ۲             |
| rmissions      |                       |               |
| icklist_Access |                       |               |
| co_IP_Phones   |                       |               |
| AuthZ Profil 🗢 |                       |               |
| Select an item | ◎                     |               |
|                |                       |               |

64. Sélectionnez le CWA standard (il s'agit du profil d'autorisation créé précédemment).



65. Vérifiez que la règle est ajoutée avec les conditions et l'autorisation correctes.



66. Cliquez sur Done (Terminé) (à droite de la règle).



67. Àdroite de la même règle, cliquez sur la flèche vers le bas en regard de Modifier, puis

sélectionnez Insérer une nouvelle règle ci-dessous.



68. Remplacez le nom de la règle Standard Rule # par **PEAPrule** (dans cet exemple). Cette règle s'applique au protocole PEAP (également utilisé pour un seul scénario SSID) pour vérifier que l'authentification 802.1X sans TLS (Transport Layer Security) et que le provisionnement du demandeur réseau est initié avec le profil d'autorisation de provisionnement créé précédemment.

DpenCWA	if Wireless_MAB	then CWA	
💉 🛃 🔹 Standard Rule 1	Any 💠 and Condition(s)	then Auth2 Profil	

69. Remplacez la condition par Wireless\_802.1X.

Condition(s)	- then AuthZ Profil 4	
n 💾 Add All Conditions Below	v to Library	
Condition Name	Expression	
Wireless_802.1X	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port	ŵ <b>.</b>

70. Cliquez sur l'icône d'engrenage sur le côté droit de la condition, et sélectionnez **Ajouter un attribut/une valeur**. Il s'agit d'une condition « et » et non d'une condition « ou ».



71. Localisez et sélectionnez Network Access.

1 (10) LOA		Dictionaries
		(م
		🔶 🗐 🗄 🚳 -
os and other conditions)		
		-
	then	· · · · · · · · · · · · · · · · · · ·
	then	
	then	
Condition(s)	-	2 mar
tAccess		
Condition Name	Expression	
Wireless_802.1X 📀	Radius:Service-Type E	Network Access
◊	Select Attribute	

72. Sélectionnez AuthenticationMethod, et entrez les valeurs suivantes :



AuthenticationMethod : égal à

Network Access:Au🛇	<b>•</b>
	Equals Not Equals

Sélectionnez MSCHAPV2.



Ceci est un exemple de la règle ; assurez-vous de confirmer que la condition est un AND.

and	Condition(s)	🗢 then 🛛 AuthZ Profil 💠		
-				
	Condition Name	Expression	AND	
	Wireless_802.1X 📀	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port		ŵ.
	♦	Network Access:Au Equals * MSCHAPV2 *	0	<b>⊜</b> .

73. Dans Profil AuthZ, sélectionnez **Standard > Provisionner** (il s'agit du profil d'autorisation créé précédemment).

then	AuthZ Profil	Done
	Select an item 📀 — 🕂	

Standard	ž
	و م
<b>⟨</b> ] = :	<b>₩</b> •
Servision (h)	

74. Cliquez sur Done.



75. Àdroite de la règle PEAP, cliquez sur la flèche vers le bas en regard de Edit, puis sélectionnez **Insert New Rule Below**.



76. Modifiez le nom de la règle en remplaçant Standard Rule # par **AllowRule** (dans cet exemple). Cette règle sera utilisée afin d'autoriser l'accès aux périphériques enregistrés avec des certificats installés.



77. Sous Condition(s), sélectionnez Conditions composées.

	Dictionaries	
		R
	<b>∢-</b> ≡ '≡	\@+
ant Dravisioning	Simple Conditions	۲
	Compound Conditions	R.
	Time and Date Conditions	50
Condition(s)		
Add All Conditions E		
Condition Name		

78. Sélectionnez Wireless\_802.1X.



79. Ajoutez un attribut AND.

Wireless_802.1X	then	
Add All Conditions Belo	w to Library	
Condition Name	Expression	
Wireless_802.1X 📀	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port	<u>B</u> -

80. Cliquez sur l'icône d'engrenage sur le côté droit de la condition, et sélectionnez **Ajouter un attribut/une valeur**.



81. Localisez et sélectionnez Radius.

			Dictionaries	
			<b>*</b>	
Client Provisioning 🔄 Secur	ity Group Access	s 🥐	and the second s	1
			Caco-dettre	
		these	Cause of McDille	
		then	anace 🗧	
		then	🛄 EndPointe	
			🔛 duest	
etwork Access:AuthenticationMe	thod	then	🛄 Adentity-Group	
Wireless 8021X Network Acce	66:A		Internal.ter	
·			Moreault 🔛	
Condition Name	Expression		Sectored Access	AND V
			🧰 Radius	
Wireless_802.1X 📀	Radius:Service	-Type E	Section 1	20-
٥	Select Attri	bute 🤇		o

82. Sélectionnez Calling-Station-ID-[31].



83. Sélectionnez Égal.

Radius:Service-Type EQUALS	6 Framed AND Ra	dius:NAS-Port	
Radius:Calling-Statio	Founds 0		٥
	Not Equals		

84. Accédez à CERTIFICATE, puis cliquez sur la flèche droite.

Standard
<b>∲-</b> ■ 1≣
and the other process
CHAR CHAR
😋 Caco JP JPares
Cambractivit2
Carry-Rocass
Q Discovery
Carl Englishment (1)
PermitAccess
😋 Provision 💟

85. Sélectionnez Autre nom du sujet.



86. Pour le profil AuthZ, sélectionnez Standard.

	Profiles		
		R	
	<b>◆-</b> ■ '=	\$÷-	
v Elements	🔛 Jahn Posture Node		
	🛄 fiscally linup		
	Standard	R	
_IP_Phones		0	
sion	-		
AuthZ Profil 🗢			
Select an item	4		

87. Sélectionnez Autoriser l'accès.



88. Cliquez sur Done.



Voici un exemple de la règle :

Ĩ	OperCHA	/ Wesley, Mill	the second	CHR
1	Riha	F Intelesc, 802 55 VIC Nativoli Access Authenticator/Rethod 802/8L5 MICHAPU2 )		Provision
1	AllowRule	Wireless_802.1X Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name	then	PermitAccess

89. Recherchez la règle Default afin de modifier PermitAccess en DenyAccess.



90. Cliquez sur **Edit** afin de modifier la règle par défaut.



91. Accédez au profil AuthZ existant de PermitAccess.



92. Sélectionnez Standard.



93. Sélectionnez RefuserAccès.

Standard	
<b>∲• </b> ■ `≡	
Content of the conten	
Caso, JP , Phones	() () 
Carbonary .	

94. Vérifiez que la règle par défaut a la valeur DenyAccess si aucune correspondance n'est trouvée.

100000000				
ø	2	Default	DenyAccess	÷

95. Cliquez sur Done.



Il s'agit d'un exemple des principales règles requises pour ce test ; elles s'appliquent à un seul SSID ou à deux SSID.

OpenCWA	Wireless_MAB	then CWA
PEAPrule	(Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 )	then Provision
AllowRule	(Wireless_802.1X AND Radus:Caling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name )	then PermitAccess
Default	fino matches, then DenyAccess	

96. Cliquez sur Save.



97. Accédez à ISE > Administration > System > Certificates afin de configurer le serveur ISE avec un profil SCEP.



98. Dans Opérations de certificat, cliquez sur Profils CA SCEP.



99. Cliquez sur Add.



100. Entrez les valeurs suivantes pour ce profil :

Nom : **mySCEP** (dans cet exemple)URL : **https://***<ca-server***/CertSrv/mscep/** (Vérifiez la configuration de votre serveur AC pour obtenir l'adresse correcte.)

EP Certificat	e Authority	
* Name	mySCEP	
Description		
* URL	https://10.10.10.10/certsrv/mscep/	Test Connectivity

101. Cliquez sur Test Connectivity afin de tester la connectivité de la connexion SCEP.



102. Cette réponse indique que la connectivité du serveur a réussi.



103. Cliquez sur Submit.



104. Le serveur répond que le profil AC a été créé avec succès.



105. Vérifiez que le profil d'autorité de certification SCEP est ajouté.

SCEP CA Profiles			
/Edt +Add XDelete		Show All	- % +
Name Name	Description	URL	CA Cert Name
MySCEP		https://10.10.10/certsrv/mscep	RFDemo-MSCE

### Expérience utilisateur - Provisionnement d'iOS

#### SSID double

Cette section couvre le double SSID et décrit comment se connecter à l'invité à provisionner et comment se connecter à un WLAN 802.1x.

Complétez ces étapes afin de provisionner iOS dans le scénario de double SSID :

1. Sur l'appareil iOS, accédez à **Réseaux Wi-Fi**, et sélectionnez **DemoCWA** (WLAN ouvert configuré sur WLC).



2. Ouvrez le navigateur Safari sur l'appareil iOS et visitez une URL accessible (par exemple, un serveur Web interne/externe). L'ISE vous redirige vers le portail. Cliquez sur **Continue**.



3. Vous êtes redirigé vers le portail invité pour vous connecter.



4. Connectez-vous avec un compte d'utilisateur et un mot de passe AD. Installez le profil AC lorsque vous y êtes invité.



5. Cliquez sur Installer le certificat approuvé du serveur AC.



6. Cliquez sur **Terminé** une fois le profil complètement installé.



7. Revenez au navigateur et cliquez sur **Register**. Notez l'ID de périphérique qui contient l'adresse MAC du périphérique.



8. Cliquez sur Install afin d'installer le profil vérifié.



9. Cliquez sur Installer maintenant.



10. Une fois le processus terminé, le profil WirelessSP confirme que le profil est installé. Cliquez sur **Done**.

Profile Installed Done					
J. J	WirelessSP Cisco				
	<b>Verified</b>				
Description	ISE Profile desc	1			
Signed	ise11-mnr.corp.rf-demo.com				
Received	Mar 24, 2012				
Contains	Certificate SCEP enrollment request Wi-Fi Network				
More Details >					

11. Accédez à **Réseaux Wi-Fi**, et changez le réseau en **Demo1x**. Votre périphérique est maintenant connecté et utilise TLS.

Settings Wi-Fi Netv	vorks				
Wi-Fi					
Choose a Network					
bibo	ú 🕈 🧕				
✓ Demo1x	و ج 🔒				
DemoCWA 🔶					
Netherstorm	4 🕈 🙆				

12. Sur l'ISE, accédez à **Operations > Authentications**. Les événements montrent le processus par lequel le périphérique est connecté au réseau invité ouvert, passe par le processus d'enregistrement avec l'approvisionnement du demandeur et est autorisé à autoriser l'accès après l'enregistrement.

A Home Operations	Pol	icy 🔹	Administration •	Alarms 🛒 Report	ts 🔪 Trouble	shoot			040 T
Live Authentications									
🚔 Add or Remove Columns 🕶	😵 Ref	resh					Refresh Every 3 secon	ds • Stow	Latest 20 records * within L
Time	Status	Detais	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:27:57.052 AM			paul	E8:05:80:97:09-41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:27:21.714 AM			68:06:88:97:09:41	68:05:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:27:20.438 AM	2				WLC				Dynamic Authorization succeeded
Mar 25,12 12:26:56.187 AM	1		paul	E0:06:00:97:09:41	WLC	CWA	Any,Profiled.Apple-Pad	Pending	

13. Accédez à ISE > Administration > Identity Management > **Groups > Endpoint Identity Groups > RegisteredDevices**. L'adresse MAC a été ajoutée à la base de données.

<ul> <li>Admin</li> <li>Admin</li> <li>Admin</li> <li>Admin</li> <li>System</li> <li>Admin</li> <li>Admin</li> </ul>	inistration 🔻
Identities Groups External Identity Sources          Identities Groups         Identity Groups         Image: State of the sta	Identity Source Sequences Settings     Endpoint Group Lit > RegisteredDevices   Endpoint Group     * Name RegisteredDevices   Description Asset Registered Endpoints Identity Group   Parent Group   Save Reset   • Endpoints   Identity Group Endpoints   MAC Address   • Es:06:38:97:09:41

#### SSID unique

Cette section couvre le SSID unique et décrit comment se connecter directement à un WLAN 802.1x, fournir un nom d'utilisateur/mot de passe AD pour l'authentification PEAP, fournir un accès via un compte invité et se reconnecter avec TLS.

Complétez ces étapes afin de provisionner iOS dans le scénario SSID unique :

1. Si vous utilisez le même périphérique iOS, supprimez le terminal des périphériques enregistrés.

Endpoint Group List > RegisteredDevices Endpoint Group					
* Name	RegisteredDevices				
Description	Asset Registered Endpoint				
Parent Group					
Save Reset					
<ul> <li>Endpoints</li> </ul>					
Identity Group	) Endpoints				
	×Remove *				
MAC Addre	Remove Selected				
E8:06:88:9	Remove All				

2. Sur l'appareil iOS, accédez à **Paramètres > Généraux > Profils**. Supprimer les profils installés dans cet exemple.



3. Cliquez sur **Remove** afin de supprimer les profils précédents.





- 4. Connectez-vous directement à la norme 802.1x avec le périphérique existant (effacé) ou avec un nouveau périphérique iOS.
- 5. Connectez-vous à **Dot1x**, entrez un nom d'utilisateur et un mot de passe, puis cliquez sur **Joindre**.

Enter the password for "Demo1x" Cancel Enter Password Join					
Username paul					
Password ••••••3					
Mode Automatic >					

- 6. Répétez les étapes 90 et suivantes à partir de la section <u>Configuration ISE</u> jusqu'à ce que les profils appropriés soient complètement installés.
- 7. Accédez à ISE > Operations > Authentications afin de surveiller le processus. Cet exemple montre le client qui est connecté directement au WLAN 802.1X lors de son provisionnement, de sa déconnexion et de sa reconnexion au même WLAN à l'aide de TLS.

Live Authentications									
🚔 Add or Remove Columns 💌	🔂 Raf	resh					Refresh Every	3 seconds *	Show Latest 20 records
Time •	Status	Detais	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:40:03:593 AM		ò	paul	E8.06.88.97.09.41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:39:53.353 AM	2	ò	E8:06:88:97:09:41	E8:06:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.867 AM	2	à	paul	E8:06:08:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

8. Accédez à WLC > Monitor > [Client MAC]. Dans les détails du client, notez que le client est à l'état EXÉCUTÉ, que sa commutation de données est définie sur local et que l'authentification est centralisée. Ceci est vrai pour les clients qui se connectent au point d'accès FlexConnect.

Live AL	thentications									
add o	r Remove Columns +	🔂 Reh	resh					Refresh Every	3 seconds *	Show Latest 20 records
Time		Status	Detais	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12	12:40:03.593 AM	2	ò	paul	E8.06.88.97.09.41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12	12:39:53.353 AM	2	ò	E8:05:88:97:09:41	E8:06:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12	12:39:08.867 AM		à	paul	E8:06:88:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

## Expérience utilisateur - Mise en service Android

#### SSID double

Cette section couvre le double SSID et décrit comment se connecter à l'invité à provisionner et comment se connecter à un WLAN 802.1x.

Le processus de connexion de l'appareil Android est très similaire à celui d'un appareil iOS (SSID simple ou double). Cependant, une différence importante est que l'appareil Android a besoin d'accéder à Internet pour accéder à Google Marketplace (maintenant Google Play) et télécharger l'agent demandeur.

Complétez ces étapes afin de provisionner un appareil Android (comme le Samsung Galaxy dans cet exemple) dans le scénario de double SSID :

1. Sur l'appareil Android, utilisez le Wi-Fi afin de vous connecter à **DemoCWA**, et ouvrez le WLAN invité.



2. Acceptez tout certificat afin de vous connecter à ISE.



3. Saisissez un nom d'utilisateur et un mot de passe sur le portail invité pour vous connecter.



4. Cliquez sur **Register**. L'appareil tente d'accéder à Internet afin d'accéder à Google

Marketplace. Ajoutez des règles supplémentaires à la liste de contrôle d'accès de préauthentification (telle que ACL-REDIRECT) dans le contrôleur afin d'autoriser l'accès à Internet.



5. Google répertorie Cisco Network Setup comme une application Android. Cliquez sur Install.



6. Connectez-vous à Google et cliquez sur INSTALL.



7. Click OK.



8. Sur l'appareil Android, recherchez l'application Cisco SPW installée et ouvrez-la.



- 9. Assurez-vous que vous êtes toujours connecté au portail invité depuis votre appareil Android.
- 10. Cliquez sur Start afin de démarrer l'assistant de configuration Wi-Fi.



11. Le SPW Cisco commence à installer les certificats.



12. Lorsque vous y êtes invité, définissez un mot de passe pour le stockage des informations d'identification.



13. Le SPW Cisco renvoie un nom de certificat, qui contient la clé utilisateur et le certificat utilisateur. Cliquez sur OK afin de confirmer.

Certificate name							
Certificate name:							
paul	paul						
Package contains One user key One user certificate							
OK Cancel							
Cancal							

14. Cisco SPW continue et demande un autre nom de certificat, qui contient le certificat CA. Entrez le nom **iseca** (dans cet exemple), puis cliquez sur **OK** pour continuer.

Certificate name						
Certificate name: iseca Package contains One CA certificate						
OK Cancel						
paul is installed.						
Can	cel					

15. L'appareil Android est maintenant connecté.



# Portail Mes périphériques

Le portail Mes périphériques permet aux utilisateurs de mettre sur liste noire les périphériques précédemment enregistrés en cas de perte ou de vol d'un périphérique. Il permet également aux utilisateurs de se réinscrire si nécessaire.

Complétez ces étapes afin de mettre un périphérique sur liste noire :

1. Pour vous connecter au portail Mes périphériques, ouvrez un navigateur, connectez-vous à https://ise-server:8443/mydevices (notez le numéro de port 8443) et connectez-vous avec un compte Active Directory.

CISCO My Devices Portal		
	Username Password	Paul

2. Localisez le périphérique sous Device ID, et cliquez sur **Lost?** afin de lancer la liste noire d'un périphérique.

Add a	New Device	To add a device, p (optional); then cli	lease enter the Device ID (MAC Address) and a description ck submit to add the device.	
Your De	* Desc Desc	ription		•
State	Device ID	Description	Action	
	EB:06:88:97:09:41		Edit   Logi2   🚆	

3. Lorsque l'ISE affiche un avertissement, cliquez sur Yes afin de continuer.



4. ISE confirme que le périphérique est marqué comme perdu.



5. Toute tentative de connexion au réseau avec le périphérique précédemment enregistré est désormais bloquée, même si un certificat valide est installé. Voici un exemple de périphérique sur liste noire dont l'authentification échoue :

Live Authentications										
🙀 Add or Remove Columns +	😵 Raf	resh					Refresh Eve	ery 3 seconds *	Show Latest 20 records	*
Time •	Status	Detals	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event	
Mar 25,12 12:49:07.851 AM	•	ò	paul	E8:06:88:97:09:41	WLC	Blacklist_Access	Blacklet		Authentication falled	
Mar 25,12 12:40:59.057 AM	•	ò	E8:06:08:97:09:41	EB-06-88-97-09-41	WLC	Blacklist_Access	Blacklet		Authentication falled	
Mar 25 12 12-40-54 197 AM		-	and	000000000000	WEC	Blackfet Access	Blacklet		Authentication falled	

6. Un administrateur peut accéder à ISE > Administration > Identity Management > **Groups**, cliquer sur **Endpoint Identity Groups** > **Blacklist** et voir que le périphérique est sur liste noire.

Identity Groups	Endpoint Group			
	Name Blacklist     Description Blacklist Identity Group     Save Reset     Tendpoints     Identity Group Endpoints	* Name Blacklist Description Blacklist Identity Group Parent Group Save Reset • Endpoints Identity Group Endpoints		
	Add XRemove +			
	: MAC Address			

Complétez ces étapes afin de réactiver un périphérique sur liste noire :

1. Dans le portail Mes périphériques, cliquez sur Réinstaller pour ce périphérique.



2. Lorsque ISE vous invite à émettre un avertissement, cliquez sur Yes afin de continuer.



3. ISE confirme que le périphérique a été correctement réinstallé. Connectez le périphérique réinstallé au réseau afin de tester que le périphérique sera désormais autorisé.



## **Référence - Certificats**

ISE nécessite non seulement un certificat racine CA valide, mais également un certificat valide signé par l'autorité de certification.

Complétez ces étapes afin d'ajouter, lier et importer un nouveau certificat d'autorité de certification approuvée :

 Accédez à ISE > Administration > System > Certificates, cliquez sur Local Certificates, puis cliquez sur Add.



2. Sélectionnez Générer une demande de signature de certificat (CSR).



3. Entrez l'objet du certificat **CN=***<ISE-SERVER hostname.FQDN>*. Pour les autres champs, vous pouvez utiliser la valeur par défaut ou les valeurs requises par la configuration de votre autorité de certification. Cliquez sur Submit.

Local Certificates > Generate Certificate Signing Request Generate Certificate Signing Request						
Certificate						
* Certificate Subject	CN=ise11-mnr.corp.rf-demo.com					
* Key Length	2048 💌					
* Digest to Sign With	SHA-256 *					
Submit Cancel						

4. ISE vérifie que le CSR a été généré.



5. Afin d'accéder au CSR, cliquez sur les opérations Certificate Signing Requests.



6. Sélectionnez la CSR récemment créée, puis cliquez sur Export.



7. ISE exporte le CSR vers un fichier .pem. Cliquez sur **Save File**, puis sur **OK** afin d'enregistrer le fichier sur l'ordinateur local.



8. Localisez et ouvrez le fichier de certificat ISE à l'aide d'un éditeur de texte.



9. Copiez le contenu entier du certificat.



 Connectez-vous au serveur AC et connectez-vous avec un compte administrateur. Le serveur est une autorité de certification Microsoft 2008 sur https://10.10.10.10/certsrv (dans cet exemple).



11. Cliquez sur Demander un certificat.



12. Cliquez sur Advanced certificate request (requête de certificat avancée).



13. Cliquez sur la deuxième option afin d'envoyer une demande de certificat en utilisant un CMC codé en base 64 ou ... .



14. Collez le contenu du fichier de certificat ISE (.pem) dans le champ Requête enregistrée, assurez-vous que le modèle de certificat est **Web Server**, puis cliquez sur **Submit**.
| Microsoft Certificate Services labsrv.corp.rf-demo.com                        |   |  |  |  |  |
|---|---|--|--|--|--|
| Submit a Certificate Request or Renewal Request                               |   |  |  |  |  |
| To submit a sav<br>Saved Request  | ved request to the CA, paste a base-64-encoded CN box.  |  |  |  |  |
| Saved Request:  |   |  |  |  |  |
| Base-64-encoded<br>certificate request<br>(CMC or<br>PKCS #10 or<br>PKCS #7): | MASGA1UdDwQEAwICrDAdBgNVHQ4EFgQUBJa5qgBc<br>VR01BAwwCgYIKwYBBQUHAwEwEQYJYIZIAYb4QgEB<br>BQUAA4GBAKS+tyTCZiNKcXIygxHTWjepfDqWdoSZ<br>1/t65UI0KQAyBRUp21TpHf+o27eDTVwW83bCmbD1<br>osMN8EmLCVz2RPOTE4aKtkJeSoHF10Y/+vPrb1pM<br>END CERTIFICATE |  |  |  |  |
| Certificate Temp  | late:   |  |  |  |  |
|   | Web Server  |  |  |  |  |
| Additional Attributes:  |   |  |  |  |  |
| Attributes:   |   |  |  |  |  |
|   | Submit >  |  |  |  |  |

15. Cliquez sur Télécharger le certificat.



16. Enregistrez le fichier certnew.cer ; il sera utilisé ultérieurement afin d'établir une liaison avec l'ISE.



17. Dans Certificats ISE, accédez à Certificats locaux, puis cliquez sur Add > Bind CA Certificate.

🛕 Home Operations 🔻 Policy 🔻 Adminis	tration 🔻
🔆 System 🛛 👰 Identity Management 🛛 📷 M	Network Resources 🛛 🛃 Web Portal Management
Deployment Licensing Certificates Logging	g Maintenance Admin Access Settings
Certificate Operations	Local Certificates
Certificate Signing Requests Certificate Authority Certificates SCEP CA Profiles	Friend Import Local Server Certificate Generate Self-Signed Certificate Generate Certificate Signing Request
CCSP Services	Bind CA Certificate

18. Recherchez le certificat qui a été enregistré sur l'ordinateur local à l'étape précédente, activez les protocoles **EAP** et **Management Interface** (les cases sont cochées), puis cliquez sur **Submit**. ISE peut prendre plusieurs minutes ou plus pour redémarrer les services.

Deployment Licensing Certificates Logo	ing Maintenance Admin Access Settings
Deployment Licensing Certificates Logo Certificate Operations © Local Certificates © Certificate Signing Requests © Certificate Authority Certificates © SCEP CA Profiles © OCSP Services	ing   Maintenance   Admin Access   Settings     Local Certificates > Bind CA Signed Certificate   Bind CA Signed Certificate     Dertificate   * Certificate File   C:\Users\Paul Nguyen\Downloads\certnew(4).cer   Browse_     Friendly Name
	Override Policy     Replace Certificate   A certificate being imported may be determined to already exist in the systectificate     Certificate   A certificate being imported may be determined to already exist in the systectificate     Certificate   A certificate being imported may be determined to already exist in the systection of the "Replace Certificate" option will a selections for the certificate.     Cancel   Cancel

19. Revenez à la page de renvoi de l'autorité de certification (https://CA/certsrv/) et cliquez sur Download a CA certificate, certificate chain, or CRL.



20. Cliquez sur **Download CA certificate**.

Microsoft Active Directory Certificate Services - co				
Download a CA Certificate, Certificate Ch				
To trust certificates issued from this certification				
To download a CA certificate, certificate chair				
CA certificate:				
Encoding method:				
© DER © Base 64				
Download CA certificate				

21. Enregistrez le fichier sur l'ordinateur local.

|--|

22. Une fois le serveur ISE en ligne, accédez à **Certificates**, et cliquez sur **Certificate Authority Certificates**.



23. Cliquez sur Import.



24. Recherchez le certificat CA, activez **Trust for client authentication** (la case est cochée), puis cliquez sur **Submit**.

Certificate Authority Certificates > In Import a new Trusted C	n <del>port</del> CA (Certificate Authority) Certificate
* Certificate File Friendly Name	C:\Users\Paul Nguyen\Downloads\certnew.c Browse_
All Certificate Authority Cert authentication below:	ificates are available for selection as the Root CA for secure LDAJ
Enable Validation of	Certificate Extensions (accept only valid certificate)
Description	
Submit Cancel	

25. Vérifiez que le nouveau certificat CA approuvé est ajouté.

😽 System 🦉 Identity Management	Network Resources		🛃 Web Portal Managemer		
Deployment Licensing Certificates	Logging Mainten	iance A	dmin Access	Settings	
Certificate Operations	Certificate	Certificate Authority Certificates			
Certificate Signing Requests	/ Edit		Export	XDelete	
Certificate Authority Certificates	Friend	Friendly Name			
🔹 SCEP CA Profiles	Corp-R	corp-RFDEMO-CA#corp-RFDEMO-CA#00002			
🔅 OCSP Services	ise11-r	ise11-mnr.corp.rf-demo.com#ise11-mnr.corp			

## Informations connexes

- Guide d'installation matérielle de Cisco Identity Services Engine, version 1.0.4
- Contrôleurs de LAN sans fil de la gamme Cisco 2000
- Contrôleurs de réseau LAN fil de la gamme Cisco 4400
- Gamme Cisco Aironet 3500
- Guide de déploiement du contrôleur de filiale sans fil Flex 7500
- Apportez votre propre appareil Authentification unifiée des appareils et expérience d'accès cohérente
- BYOD sans fil avec Identity Services Engine
- <u>Assistance et documentation techniques Cisco Systems</u>

## 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.