

BYOD sans fil avec Identity Services Engine

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Topologie](#)

[Conventions](#)

[Présentation du contrôleur LAN sans fil RADIUS NAC et CoA](#)

[Flux de fonctionnalités RADIUS NAC et CoA du contrôleur LAN sans fil](#)

[Présentation du profilage ISE](#)

[Créer des utilisateurs d'identité internes](#)

[Ajouter un contrôleur LAN sans fil à ISE](#)

[Configurer ISE pour l'authentification sans fil](#)

[Contrôleur LAN sans fil Bootstrap](#)

[Connexion d'un WLC à un réseau](#)

[Ajouter des serveurs d'authentification \(ISE\) au WLC](#)

[Créer une interface dynamique d'employé WLC](#)

[Créer une interface dynamique WLC Guest](#)

[Ajouter un WLAN 802.1x](#)

[Tester les interfaces dynamiques WLC](#)

[Authentification sans fil pour iOS \(iPhone/iPad\)](#)

[Ajouter une ACL de redirection de position au WLC](#)

[Activer les sondes de profilage sur ISE](#)

[Activer les stratégies de profil ISE pour les périphériques](#)

[Profil d'autorisation ISE pour redirection de découverte de position](#)

[Créer un profil d'autorisation ISE pour l'employé](#)

[Créer un profil d'autorisation ISE pour le sous-traitant](#)

[Politique d'autorisation pour la position/le profilage des périphériques](#)

[Tester la politique de correction de posture](#)

[Politique d'autorisation pour accès différencié](#)

[Test de CoA pour l'accès différencié](#)

[WLAN invité WLC](#)

[Test du WLAN invité et du portail invité](#)

[Accès invité parrainé sans fil ISE](#)

[Invité Sponsorisant](#)

[Test de l'accès au portail invité](#)

[Configuration du certificat](#)

[Intégration à Windows 2008 Active Directory](#)

[Ajouter des groupes Active Directory](#)

[Ajouter une séquence source d'identité](#)

[Accès invité parrainé sans fil ISE avec fonction AD intégrée](#)

[Configuration de la fonctionnalité SPAN sur le commutateur](#)

[Référence : Authentification sans fil pour Apple MAC OS X](#)

[Référence : Authentification sans fil pour Microsoft Windows XP](#)

[Référence : Authentification sans fil pour Microsoft Windows 7](#)

[Informations connexes](#)

Introduction

Cisco Identity Services Engine (ISE) est le serveur de politiques de nouvelle génération de Cisco qui fournit une infrastructure d'authentification et d'autorisation à la solution Cisco TrustSec. Il fournit également deux autres services essentiels :

- Le premier service consiste à fournir un moyen de profiler automatiquement le type de périphérique de point d'extrémité en fonction des attributs que Cisco ISE reçoit de diverses sources d'informations. Ce service (appelé Profiler) offre des fonctions équivalentes à celles que Cisco offrait précédemment avec l'appliance Cisco NAC Profiler.
- Un autre service important fourni par Cisco ISE consiste à analyser la conformité des terminaux, par exemple, l'installation du logiciel AV/AS et la validité de son fichier de définition (appelé Posture). Auparavant, Cisco n'offrait cette fonction de posture exacte qu'avec l'appareil Cisco NAC.

Cisco ISE offre un niveau de fonctionnalité équivalent et est intégré aux mécanismes d'authentification 802.1X.

Cisco ISE intégré aux contrôleurs LAN sans fil (WLC) peut fournir des mécanismes de profilage des appareils mobiles tels que les iDevices d'Apple (iPhone, iPad et iPod), les smartphones Android et autres. Pour les utilisateurs 802.1X, Cisco ISE peut fournir le même niveau de services tels que le profilage et l'analyse de position. Les services invités sur Cisco ISE peuvent également être intégrés au WLC Cisco en redirigeant les demandes d'authentification Web vers Cisco ISE pour authentification.

Ce document présente la solution sans fil pour le BYOD (Bring Your Own Device), comme la fourniture d'un accès différencié basé sur les terminaux connus et la politique de l'utilisateur. Ce document ne fournit pas la solution complète du BYOD, mais sert à démontrer un cas d'utilisation simple de l'accès dynamique. D'autres exemples de configuration incluent l'utilisation du portail de parrainage ISE, où un utilisateur privilégié peut parrainer un invité pour provisionner l'accès invité sans fil.

Conditions préalables

Exigences

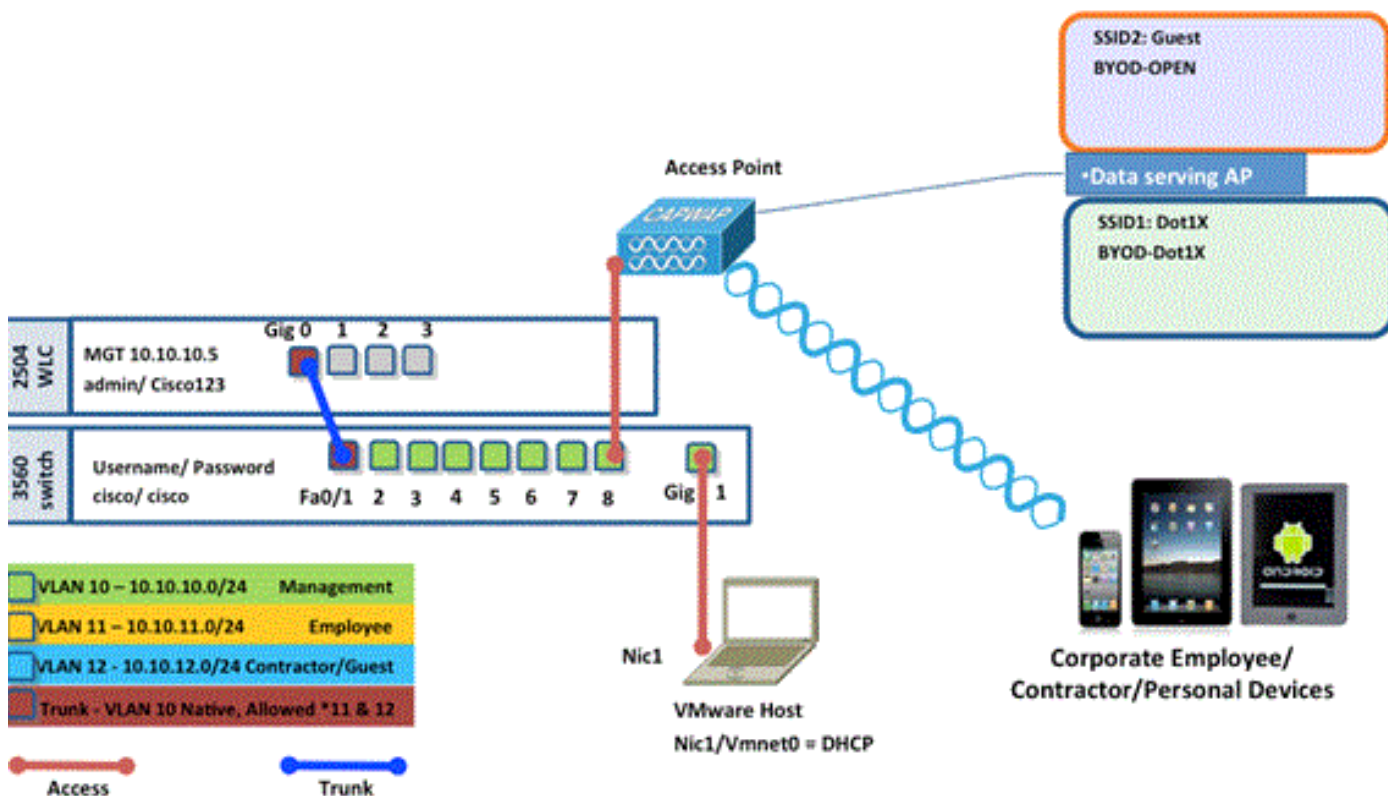
Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

- Contrôleur LAN sans fil Cisco 2504 ou 2106 avec la version logicielle 7.2.103
- Catalyst 3560 - 8 ports
- WLC 2504
- Identity Services Engine 1.0MR (version image du serveur VMware)
- Windows 2008 Server (image VMware) - 512 Mo, disque de 20 GoActive DirectoryDNSDHCPServices de certificats

Topologie



Name	IP Address	Credential
Vmware Host	10.10.10.2	(Machine used to host the ISE 1.0 MR vmware server files)
Identity Service Engine	10.10.10.70	admin/ default1A
Active Directory/ DNS/ DHCP/ CA Server	10.10.10.10	(Machine used to host Active Directory/ DNS/ DHCP/ CA Server)

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Présentation du contrôleur LAN sans fil RADIUS NAC et CoA

Ce paramètre permet au WLC de rechercher les paires AV de redirection d'URL provenant du serveur RADIUS ISE. Ceci est uniquement sur un WLAN qui est lié à une interface avec le paramètre RADIUS NAC activé. Lorsque la paire AV Cisco pour la redirection d'URL est reçue, le

client passe à l'état POSTURE_REQD. C'est fondamentalement la même chose que l'état WEBAUTH_REQD en interne dans le contrôleur.

Lorsque le serveur ISE RADIUS considère que le client est conforme à la position, il émet une ReAuth CoA. L'ID de session est utilisé pour l'associer. Avec ce nouveau AuthC (re-Auth), il n'envoie pas les paires AV de redirection d'URL. Comme il n'y a pas de paires AV de redirection d'URL, le WLC sait que le client ne nécessite plus de posture.

Si le paramètre RADIUS NAC n'est pas activé, le WLC ignore les VSA de redirection d'URL.

CoA-ReAuth : cette option est activée avec le paramètre RFC 3576. La fonctionnalité ReAuth a été ajoutée aux commandes CoA existantes qui étaient auparavant prises en charge.

Le paramètre RADIUS NAC s'exclut mutuellement de cette fonctionnalité, bien qu'il soit requis pour que la CoA fonctionne.

Pre-Posture ACL : lorsqu'un client est à l'état POSTURE_REQ, le comportement par défaut du WLC est de bloquer tout le trafic sauf DHCP/DNS. La liste de contrôle d'accès Pre-Posture (appelée dans la paire AV url-redirect-acl) est appliquée au client et ce qui est autorisé dans cette liste de contrôle d'accès est ce que le client peut atteindre.

Pre-Auth ACL vs. VLAN Override : un VLAN de quarantaine ou AuthC différent du VLAN d'accès n'est pas pris en charge dans 7.0MR1. Si vous définissez un VLAN à partir du serveur Policy Server, il s'agira du VLAN pour toute la session. Aucune modification VLAN n'est nécessaire après la première authentification.

[Flux de fonctionnalités RADIUS NAC et CoA du contrôleur LAN sans fil](#)

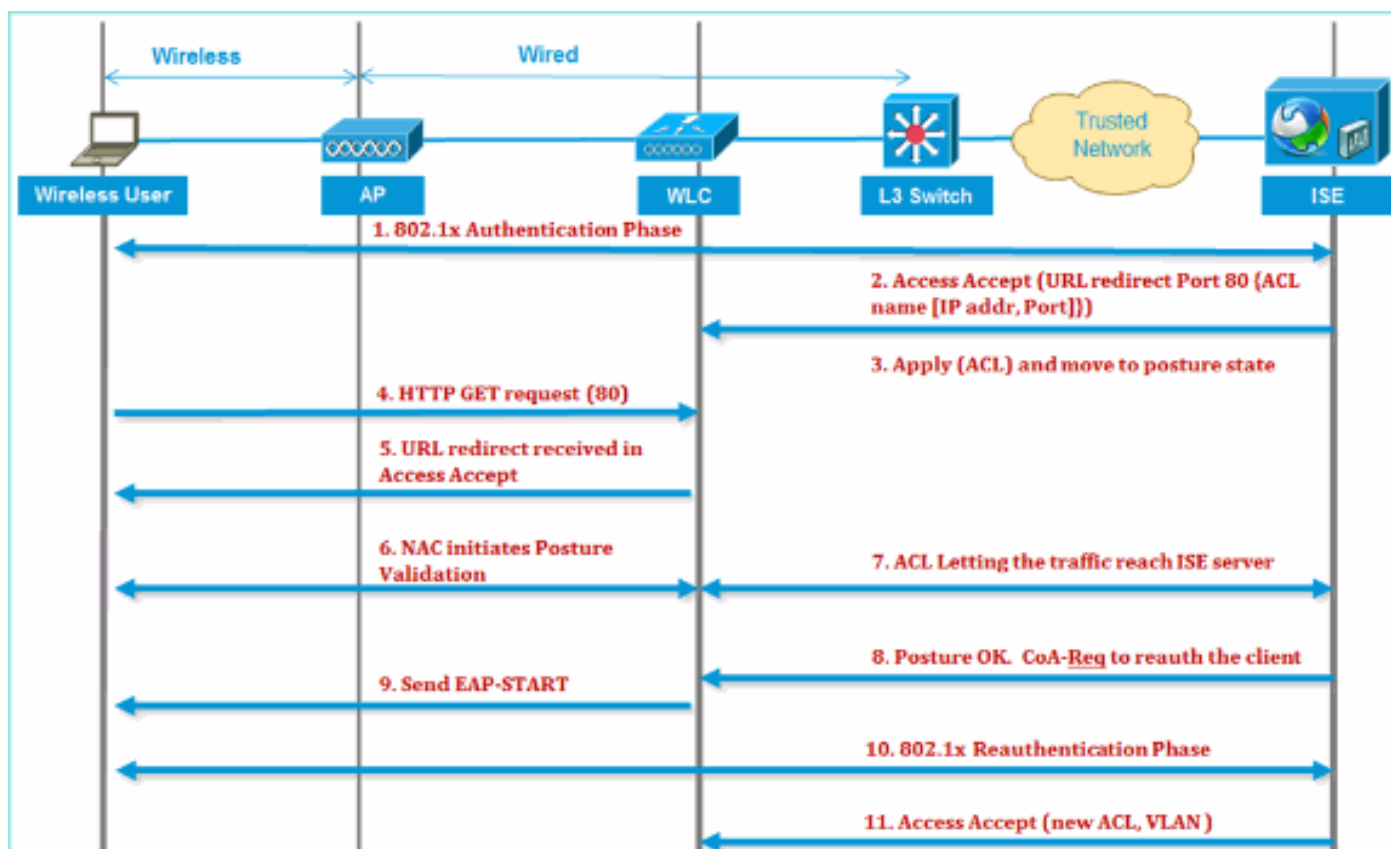
La [figure](#) ci-dessous fournit des détails sur l'échange de messages lorsque le client est authentifié auprès du serveur principal et la validation de la position NAC.

1. Le client s'authentifie avec l'authentification dot1x.
2. RADIUS Access Accept transporte l'URL redirigée pour le port 80 et les ACL de pré-auth qui inclut l'autorisation des adresses IP et des ports, ou le VLAN de quarantaine.
3. Le client sera redirigé vers l'URL fournie dans l'acceptation d'accès, et placé dans un nouvel état jusqu'à ce que la validation de la position soit effectuée. Le client dans cet état parle au serveur ISE et se valide par rapport aux stratégies configurées sur le serveur NAC ISE.
4. L'agent NAC sur le client lance la validation de position (trafic vers le port 80) : l'agent envoie une requête de détection HTTP au port 80, que le contrôleur redirige vers l'URL fournie dans access accept. L'ISE sait que le client tente d'atteindre et répond directement au client. De cette façon, le client apprend l'adresse IP du serveur ISE et, à partir de maintenant, le client parle directement avec le serveur ISE.
5. Le WLC autorise ce trafic car la liste de contrôle d'accès est configurée pour autoriser ce trafic. En cas de remplacement du VLAN, le trafic est ponté de manière à atteindre le serveur ISE.
6. Une fois que le client ISE a terminé l'évaluation, une demande de CoA RADIUS avec le service Reauth est envoyée au WLC. Ceci lance la ré-authentification du client (en envoyant EAP-START). Une fois la réauthentification réussie, l'ISE envoie l'acceptation d'accès avec

une nouvelle liste de contrôle d'accès (le cas échéant) et aucune redirection d'URL, ou VLAN d'accès.

7. WLC prend en charge CoA-Req et Disconnect-Req conformément à la RFC 3576. Le WLC doit prendre en charge CoA-Req pour le service de ré-authentification, conformément à la RFC 5176.
8. Au lieu de listes de contrôle d'accès téléchargeables, des listes de contrôle d'accès préconfigurées sont utilisées sur le WLC. Le serveur ISE envoie simplement le nom de la liste de contrôle d'accès, qui est déjà configurée dans le contrôleur.
9. Cette conception devrait fonctionner pour les cas VLAN et ACL. Dans le cas d'une substitution de VLAN, nous redirigeons simplement le port 80 qui est redirigé et autorise (le pont) le reste du trafic sur le VLAN de quarantaine. Pour la liste de contrôle d'accès, la liste de contrôle d'accès de pré-authentification reçue dans access accept est appliquée.

Cette figure fournit une représentation visuelle de ce flux de fonctions :



Présentation du profilage ISE

Le service Cisco ISE profiler vous permet de découvrir, de localiser et de déterminer les fonctionnalités de tous les terminaux connectés à votre réseau, quel que soit leur type de périphérique, afin de garantir et de maintenir un accès approprié au réseau de votre entreprise. Il collecte principalement un attribut ou un ensemble d'attributs de tous les terminaux de votre réseau et les classe en fonction de leurs profils.

Le profileur se compose des composants suivants :

- Le capteur contient plusieurs sondes. Les sondes capturent des paquets réseau en interrogeant des dispositifs d'accès réseau et transmettent les attributs et leurs valeurs d'attribut qui sont collectés à partir des points d'extrémité à l'analyseur.

- Un analyseur évalue les terminaux à l'aide des stratégies configurées et des groupes d'identités pour faire correspondre les attributs et leurs valeurs d'attribut collectées, ce qui classe les terminaux au groupe spécifié et stocke les terminaux avec le profil correspondant dans la base de données Cisco ISE.

Pour la détection des appareils mobiles, il est recommandé d'utiliser une combinaison de ces sondes pour identifier correctement les appareils :

- RADIUS (Calling-Station-ID) : fournit l'adresse MAC (OUI)
- DHCP (host-name) : nom d'hôte - le nom d'hôte par défaut peut inclure le type de périphérique ; par exemple : jsmith-ipad
- DNS (reverse IP lookup) : FQDN - le nom d'hôte par défaut peut inclure le type de périphérique
- HTTP (User-Agent) : détails sur un type d'appareil mobile spécifique

Dans cet exemple d'iPad, le profileur capture les informations du navigateur Web à partir de l'attribut User-Agent, ainsi que d'autres attributs HTTP à partir des messages de demande, et les ajoute à la liste des attributs de point d'extrémité.



Is the MAC Address
from Apple?



Does the Hostname
contain "iPad"?



Is the Safari Browser
on an iPad?



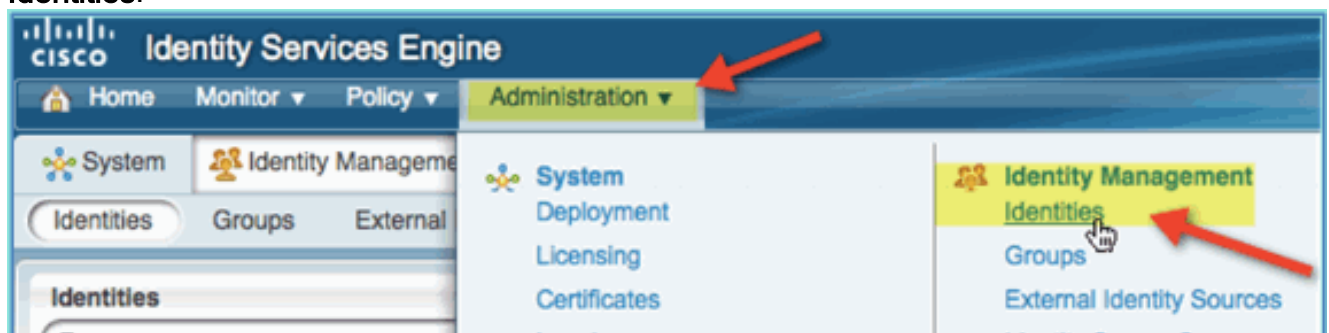
I am
certain it
is an iPad!

MS Active Directory (AD) n'est pas requis pour une simple démonstration de faisabilité. ISE peut être utilisé comme seul magasin d'identités, ce qui inclut un accès différencié des utilisateurs pour l'accès et un contrôle granulaire des politiques.

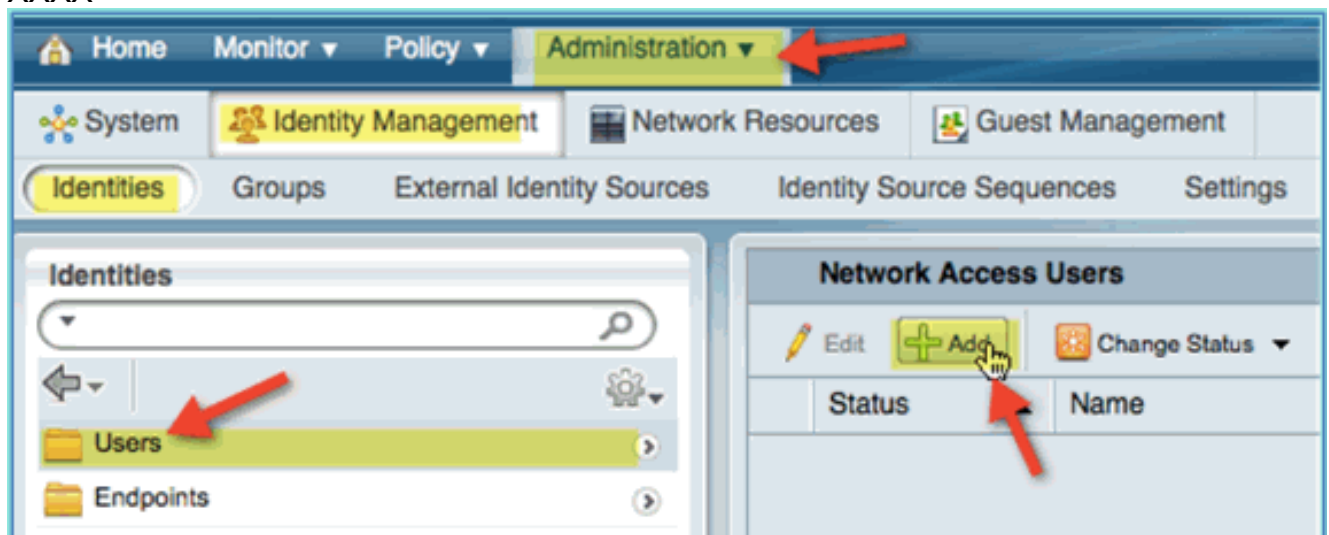
Dans la version 1.0 d'ISE, l'intégration AD permet à l'ISE d'utiliser des groupes AD dans les politiques d'autorisation. Si le magasin d'utilisateurs interne ISE est utilisé (pas d'intégration Active Directory), les groupes ne peuvent pas être utilisés dans les stratégies en association avec les groupes d'identités de périphériques (bogue identifié à résoudre dans ISE 1.1). Par conséquent, seuls les utilisateurs individuels peuvent être différenciés, tels que les employés ou les sous-traitants, lorsqu'ils sont utilisés en plus des groupes d'identités de périphériques.

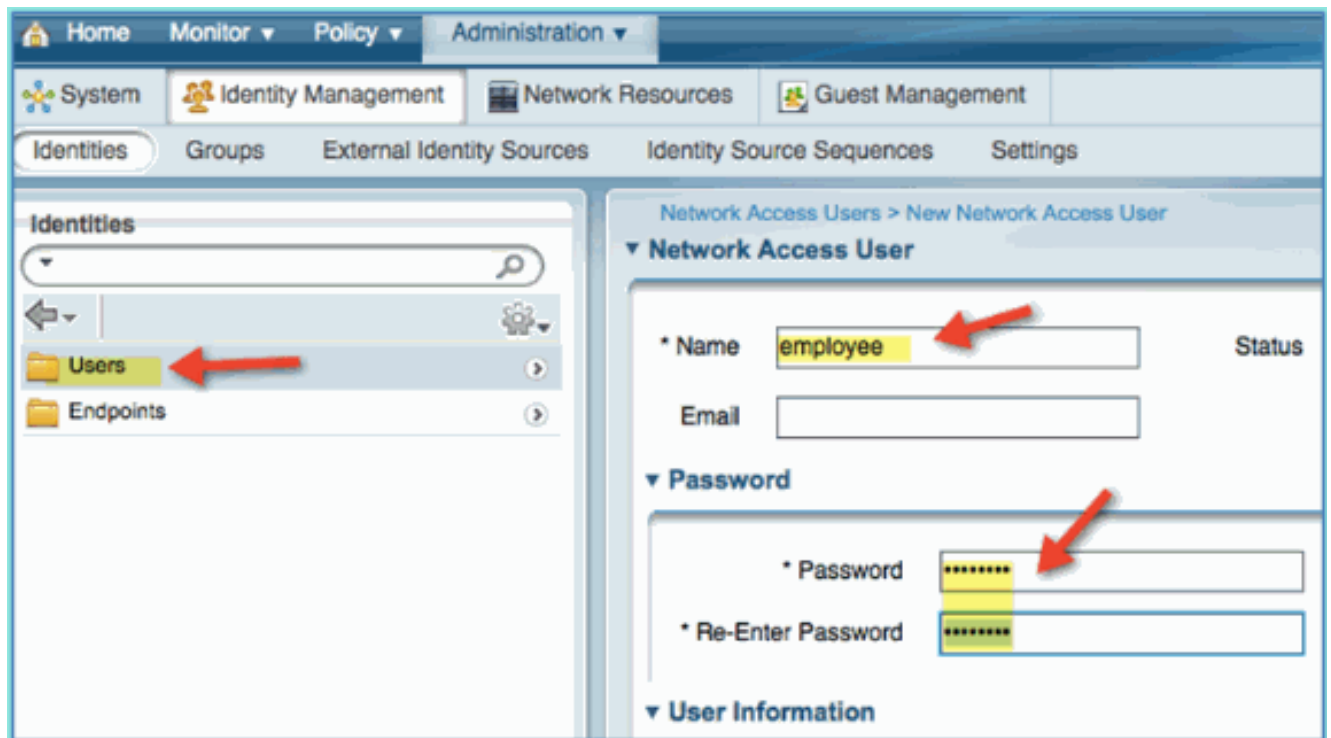
Procédez comme suit :

1. Ouvrez une fenêtre de navigateur à l'adresse <https://ISEip>.
2. Accédez à **Administration > Identity Management > Identities**.

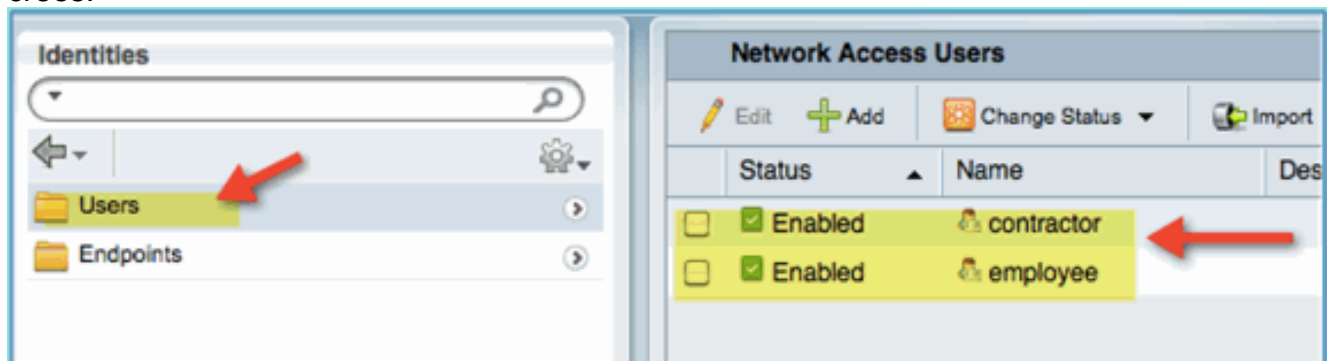


3. Sélectionnez **Users**, puis cliquez sur **Add** (Network Access User). Entrez ces valeurs utilisateur et affectez-les au groupe Employé :
Nom : employé
Mot de passe : XXXX





4. Cliquez sur Submit. Nom : entrepreneur Mot de passe : XXXX
5. Vérifiez que les deux comptes sont créés.



[Ajouter un contrôleur LAN sans fil à ISE](#)

Tout périphérique qui lance des requêtes RADIUS vers l'ISE doit avoir une définition dans ISE. Ces périphériques réseau sont définis en fonction de leur adresse IP. Les définitions de périphériques réseau ISE peuvent spécifier des plages d'adresses IP, ce qui permet à la définition de représenter plusieurs périphériques réels.

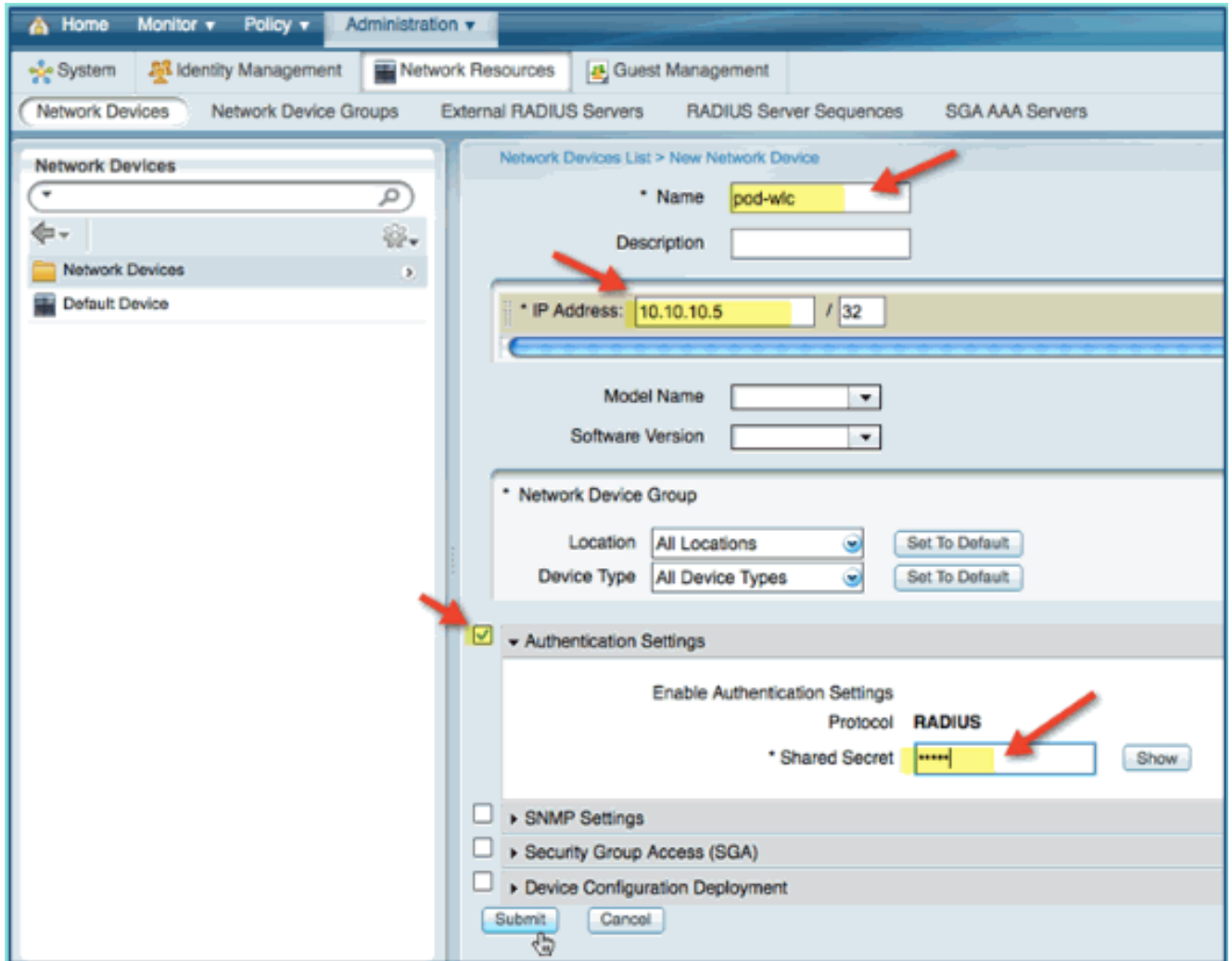
Au-delà de ce qui est requis pour la communication RADIUS, les définitions de périphériques réseau ISE contiennent des paramètres pour d'autres communications ISE/périphériques, telles que SNMP et SSH.

Un autre aspect important de la définition des périphériques réseau est le regroupement approprié des périphériques afin que ce regroupement puisse être exploité dans la politique d'accès réseau.

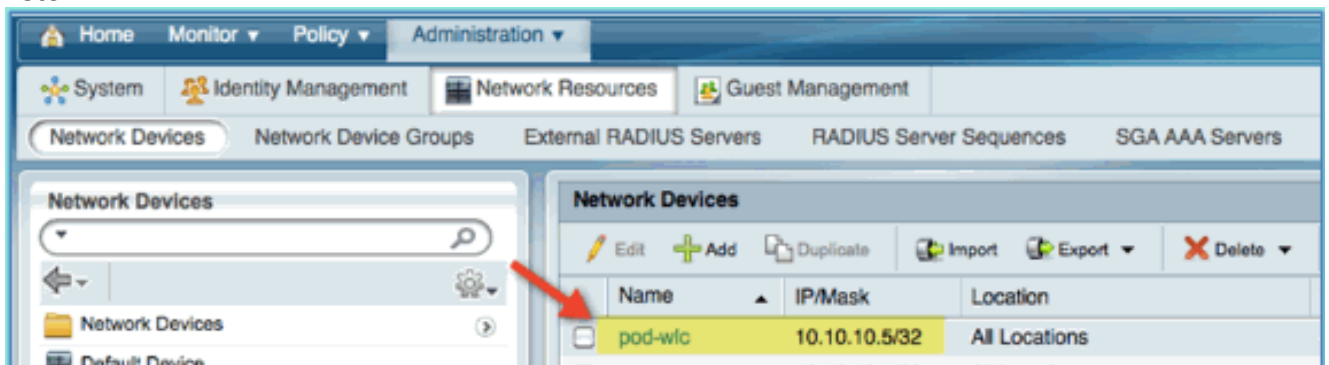
Dans cet exercice, vous allez configurer les définitions de périphériques nécessaires à vos travaux pratiques.

Procédez comme suit :

1. Dans ISE, accédez à **Administration > Network Resources > Network Devices**.



2. Dans Périphériques réseau, cliquez sur **Ajouter**. Entrez l'adresse IP, vérifiez le masque et le paramètre d'authentification, puis entrez « cisco » pour le secret partagé.
3. Enregistrez l'entrée WLC et confirmez le contrôleur dans la liste.

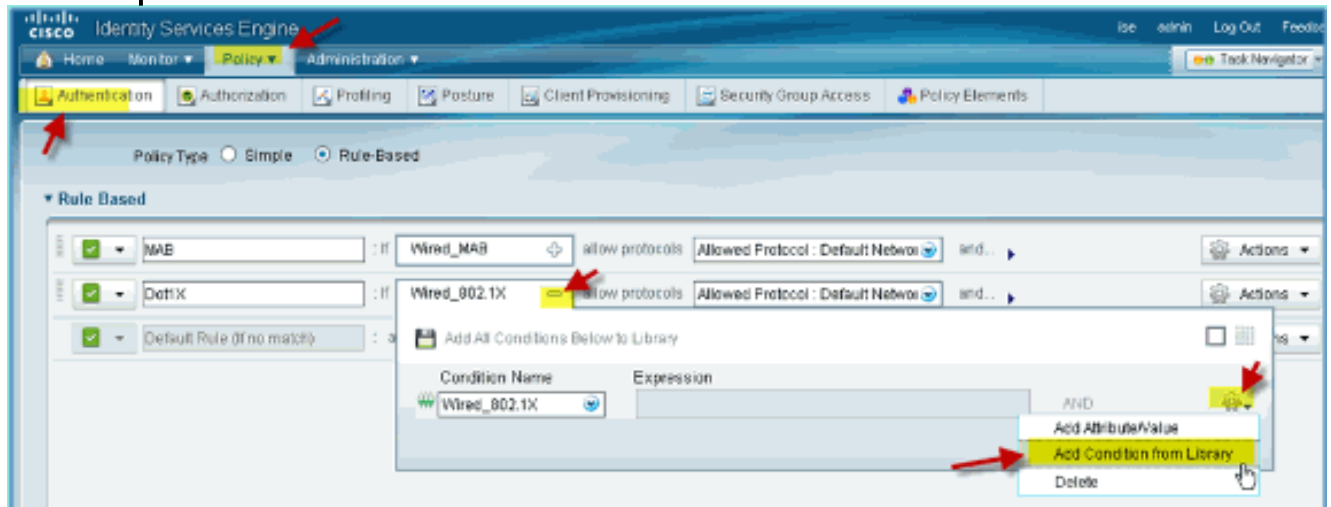


[Configurer ISE pour l'authentification sans fil](#)

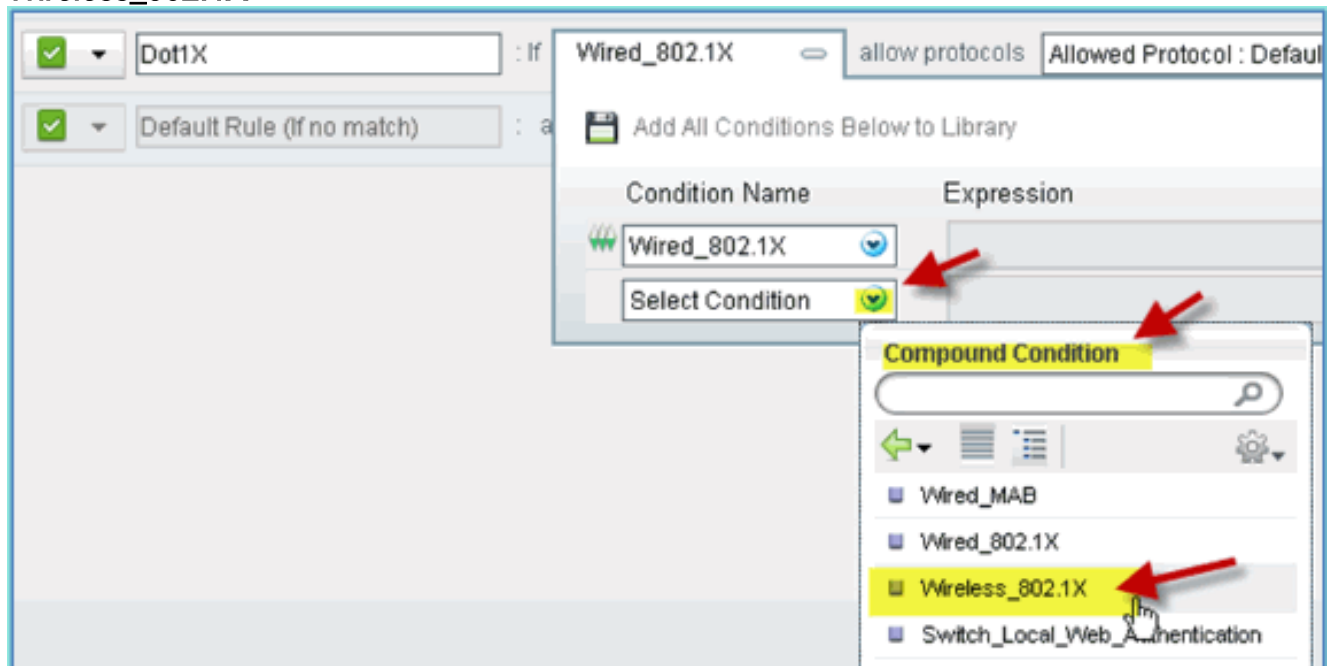
ISE doit être configuré pour authentifier les clients sans fil 802.1x et utiliser Active Directory comme magasin d'identités.

Procédez comme suit :

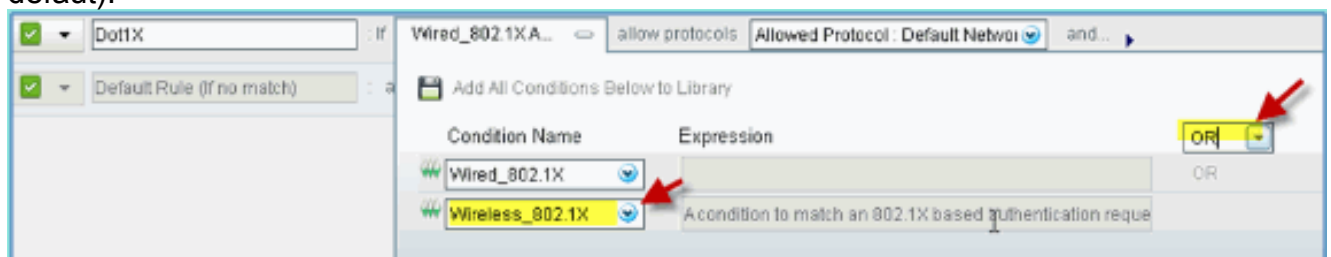
1. Dans ISE, accédez à **Policy > Authentication**.
2. Cliquez pour développer Dot1x > Wired_802.1X (-).
3. Cliquez sur l'icône d'engrenage pour **ajouter une condition à partir de la bibliothèque**.

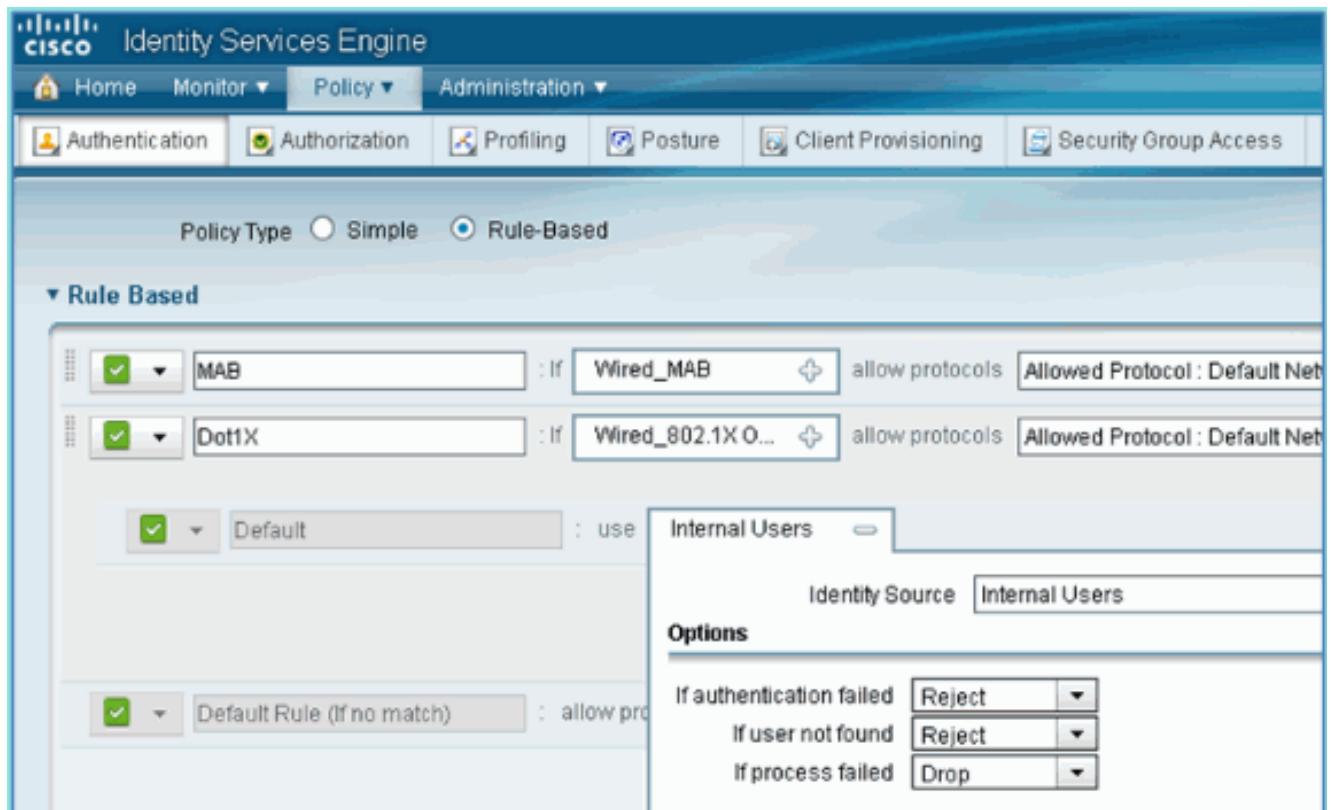


4. Dans la liste déroulante de sélection de condition, choisissez **Compound Condition > Wireless_802.1X**.



5. Définissez la condition Express sur **OR**.
6. Développez l'option after allow protocols et acceptez la valeur par défaut Internal Users (Utilisateurs internes) (par défaut).





7. Laissez tout le reste par défaut. Cliquez sur **Save** pour terminer les étapes.

Contrôleur LAN sans fil Bootstrap

Connexion d'un WLC à un réseau

Un guide de déploiement du contrôleur LAN sans fil Cisco 2500 est également disponible sur le site [Cisco 2500 Series Wireless Controller Deployment Guide](#).

Configuration du contrôleur à l'aide de l'assistant de démarrage

```
(Cisco Controller)
Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
ISE-Podx Enter Administrative User Name (24 characters max): admin
Enter Administrative Password
(3 to 24 characters): Cisco123
Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
```

Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes

Enable 802.11a Network [YES][no]: yes

Enable 802.11g Network [YES][no]: yes

Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no

Configure the ntp system time now? [YES][no]: yes

Enter the date in MM/DD/YY format: mm/dd/yy

Enter the time in HH:MM:SS format: hh:mm:ss

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes

Configuration saved!

Resetting system with new configuration...

Restarting system.

Configuration du commutateur voisin

Le contrôleur est connecté au port Ethernet du commutateur voisin (Fast Ethernet 1). Le port du commutateur voisin est configuré en tant qu'agrégation 802.1Q et autorise tous les VLAN sur l'agrégation. Le VLAN 10 natif permet de connecter l'interface de gestion du WLC.

La configuration du port de commutation 802.1Q est la suivante :

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

[Ajouter des serveurs d'authentification \(ISE\) au WLC](#)

L'ISE doit être ajouté au WLC afin d'activer la norme 802.1X et la fonctionnalité CoA pour les terminaux sans fil.

Procédez comme suit :

1. Ouvrez un navigateur, puis connectez-vous au WLC pod (en utilisant le protocole HTTP sécurisé) > <https://wlc>.
2. Accédez à **Security > Authentication > New**.

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

RADIUS Authentication Servers > New

Server Index (Priority)	1
Server IP Address	10.10.10.70
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

- Entrez les valeurs suivantes : Adresse IP du serveur : 10.10.10.70 (vérifier l'affectation) Secret partagé : cisco Prise en charge de RFC 3576 (CoA) : activé (par défaut) Tout le reste : par défaut
- Cliquez sur **Apply** pour continuer.
- Sélectionnez **RADIUS Accounting > add NEW**.

CISCO

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT C

Security RADIUS Accounting Servers > New

Server Index (Priority)	2
Server IP Address	10.10.10.70
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Port Number	1813
Server Status	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

- Entrez les valeurs suivantes : Adresse IP du serveur : 10.10.10.70 Secret partagé : cisco Tout le reste : par défaut
- Cliquez sur **Apply**, puis enregistrez la configuration pour le WLC.

Créer une interface dynamique d'employé WLC

Complétez ces étapes afin d'ajouter une nouvelle interface dynamique pour le WLC et le mapper au VLAN Employé :

1. À partir de WLC, naviguez vers **Controller > Interfaces**. Cliquez ensuite sur **New**.



2. À partir de WLC, naviguez vers **Controller > Interfaces**. Saisissez les informations suivantes :
Nom de l'interface : Employé
ID de VLAN :

11



3. Saisissez les informations suivantes pour l'interface Employé :
Numéro de port : 1
Identificateur VLAN : 11
Adresse IP : 10.10.11.5
Masque réseau : 255.255.255.0
Passerelle : 10.10.11.1
DHCP : 10.10.10.10

Configuration

Quarantine

Quarantine Vlan Id

Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

DHCP Information

Primary DHCP Server

Secondary DHCP Server

4. Vérifiez que la nouvelle interface dynamique d'employé est créée.

CISCO

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMUNITY

Controller

General

Inventory

Interfaces

Interface Groups

Multicast

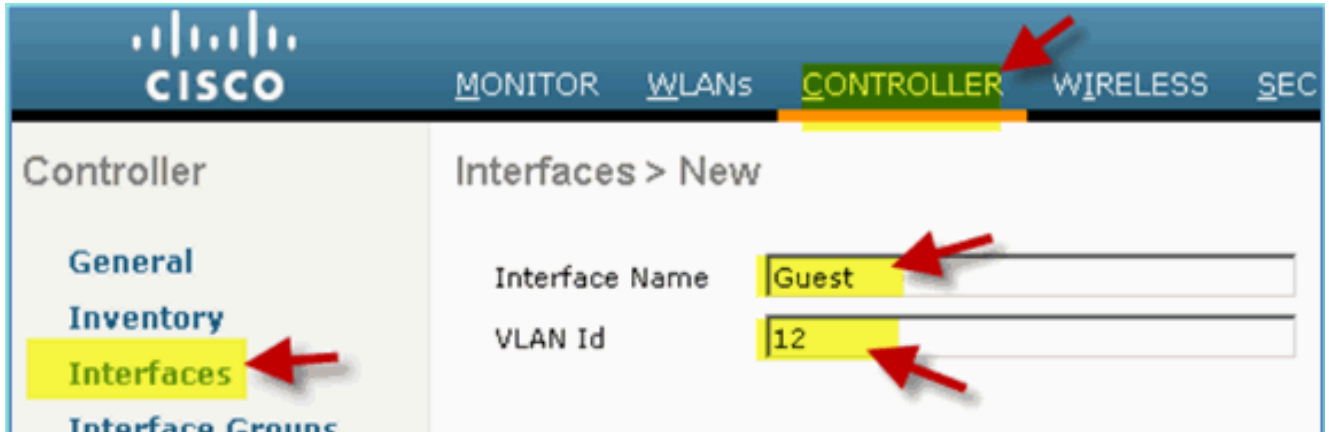
Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type
employee	11	10.10.11.5	Dynamic
management	untagged	10.10.10.5	Static
virtual	N/A	1.1.1.1	Static

Créer une interface dynamique WLC Guest

Complétez ces étapes afin d'ajouter une nouvelle interface dynamique pour le WLC et de le mapper au VLAN invité :

1. À partir de WLC, naviguez vers **Controller > Interfaces**. Cliquez ensuite sur **New**.
2. À partir de WLC, naviguez vers **Controller > Interfaces**. Saisissez les informations suivantes :
:Nom de l'interface : Guest
ID de VLAN : 12



3. Saisissez les informations suivantes pour l'interface Invité :
Numéro de port : 1
Identificateur VLAN : 12
Adresse IP : 10.10.12.5
Masque réseau : 255.255.255.0
Passerelle : 10.10.12.1
DHCP : 10.10.10.10

Configuration

Quarantine
Quarantine Vlan Id

Physical Information

Port Number
Backup Port
Active Port
Enable Dynamic AP Management

Interface Address

VLAN Identifier
IP Address
Netmask
Gateway

DHCP Information

Primary DHCP Server
Secondary DHCP Server

Access Control List

ACL Name

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

4. Vérifiez que l'interface invité a été ajoutée.

Interface Name	VLAN Identifier	IP Address	Interface Type
employee	11	10.10.11.5	Dynamic
guest	12	10.10.12.5	Dynamic
management	untagged	10.10.10.5	Static
virtual	N/A	1.1.1.1	Static

Ajouter un WLAN 802.1x

À partir du bootstrap initial du WLC, un WLAN par défaut a peut-être été créé. Si c'est le cas, modifiez-le ou créez un nouveau WLAN pour prendre en charge l'authentification 802.1X sans fil, comme indiqué dans le guide.

Procédez comme suit :

1. À partir du WLC, accédez à **WLAN > Create New**.



2. Pour le WLAN, saisissez les informations suivantes : Nom du profil : pod1x SSID : pod1x identique



3. Dans l'onglet WLAN settings > General, procédez comme suit : Politique radio : TousInterface/groupe : gestion Tout le reste : par défaut

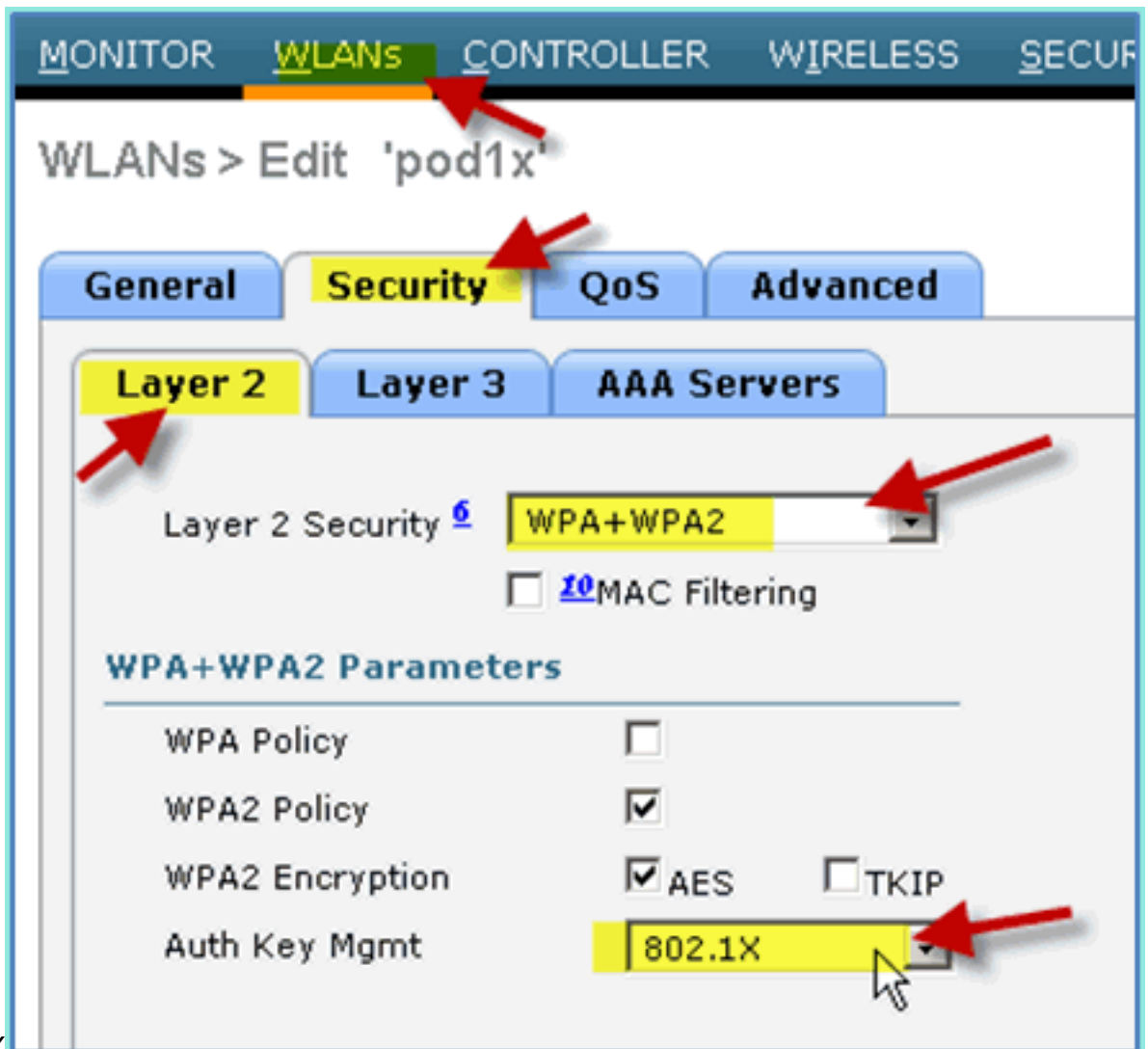
MONITOR WLANS CONTROLLER WIRELESS SECURITY

WLANs > Edit 'pod1x'

General Security QoS Advanced

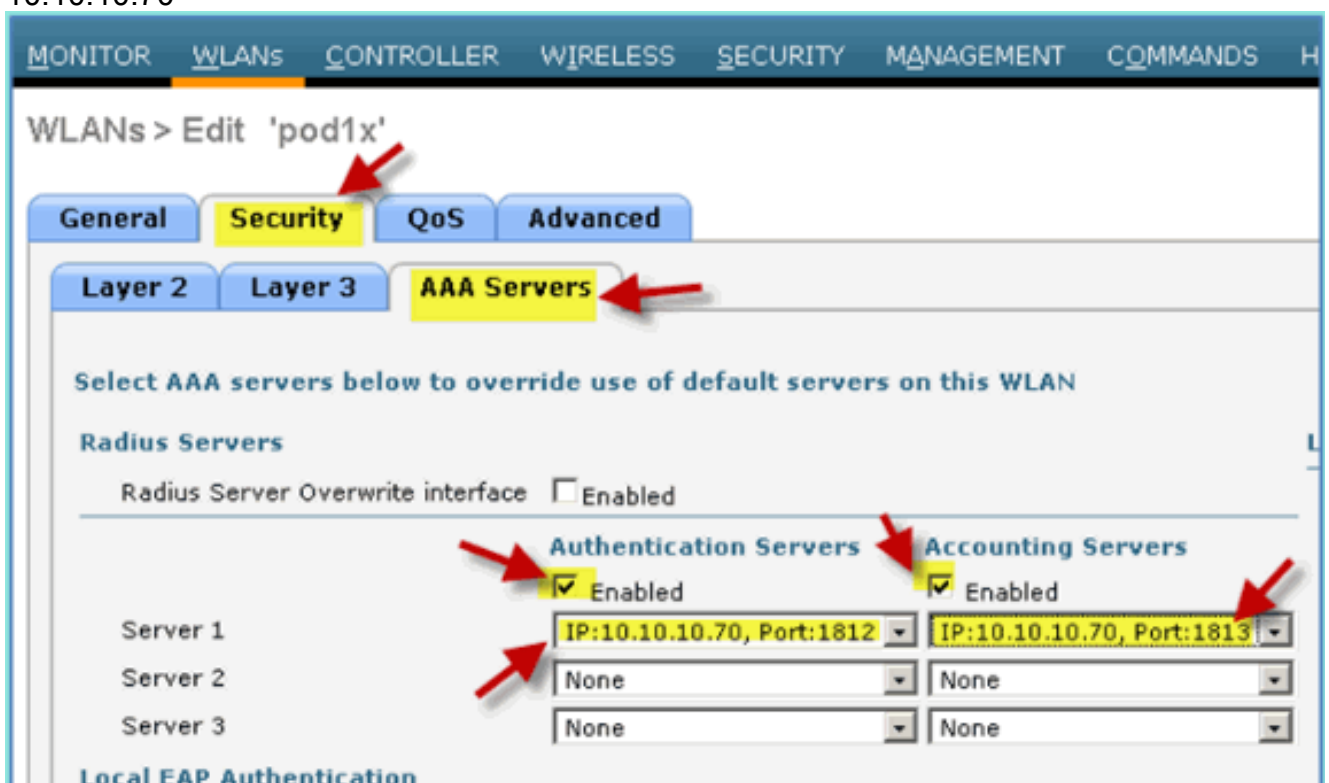
Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab w
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

4. Dans l'onglet WLAN > Security > Layer 2, définissez les paramètres suivants : sécurité de couche 2:WPA+WPA2Politique/Cryptage WPA2 : activé/AESGestion des clés d'authentification :



802.1X

5. Dans l'onglet WLAN > Security > AAA Servers, définissez les paramètres suivants : Interface de remplacement du serveur radio : désactivée Serveurs d'authentification/de comptabilité : activés Serveur 1 : 10.10.10.70



6. Dans l'onglet WLAN > Advanced, définissez les paramètres suivants : Autoriser le remplacement AAA : activé État NAC : Rayon NAC (sélectionné)

The screenshot shows the 'WLANs > Edit 'pod1x'' configuration page. The 'Advanced' tab is selected and highlighted in yellow. A red arrow points to the 'Advanced' tab. In the 'Advanced' section, the 'Allow AAA Override' checkbox is checked and highlighted in yellow, with another red arrow pointing to it. The 'NAC State' dropdown menu is also highlighted in yellow, with a red arrow pointing to it, and it is set to 'Radius NAC'. Other visible settings include 'Coverage Hole Detection' (checked), 'Enable Session Timeout' (checked, 1800 secs), 'Aironet IE' (checked), 'Diagnostic Channel' (unchecked), 'IPv6 Enable' (unchecked), 'Override Interface ACL' (None), 'P2P Blocking Action' (Disabled), 'Client Exclusion' (checked, 60 secs), 'Maximum Allowed Clients' (0), and 'Static IP Tunneling' (unchecked). The right-hand side of the page shows sections for 'DHCP', 'Management Frame Protection (MFP)', 'DTIM Period (in beacon intervals)', and 'NAC'.

7. Revenez à l'onglet WLAN > General > Enable WLAN (Case à cocher).

WLANs > Edit 'pod1x'

General Security QoS Advanced

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Tester les interfaces dynamiques WLC

Vous devez vérifier rapidement si les interfaces des employés et des invités sont valides. Utilisez n'importe quel périphérique à associer au WLAN, puis modifiez l'affectation de l'interface WLAN.

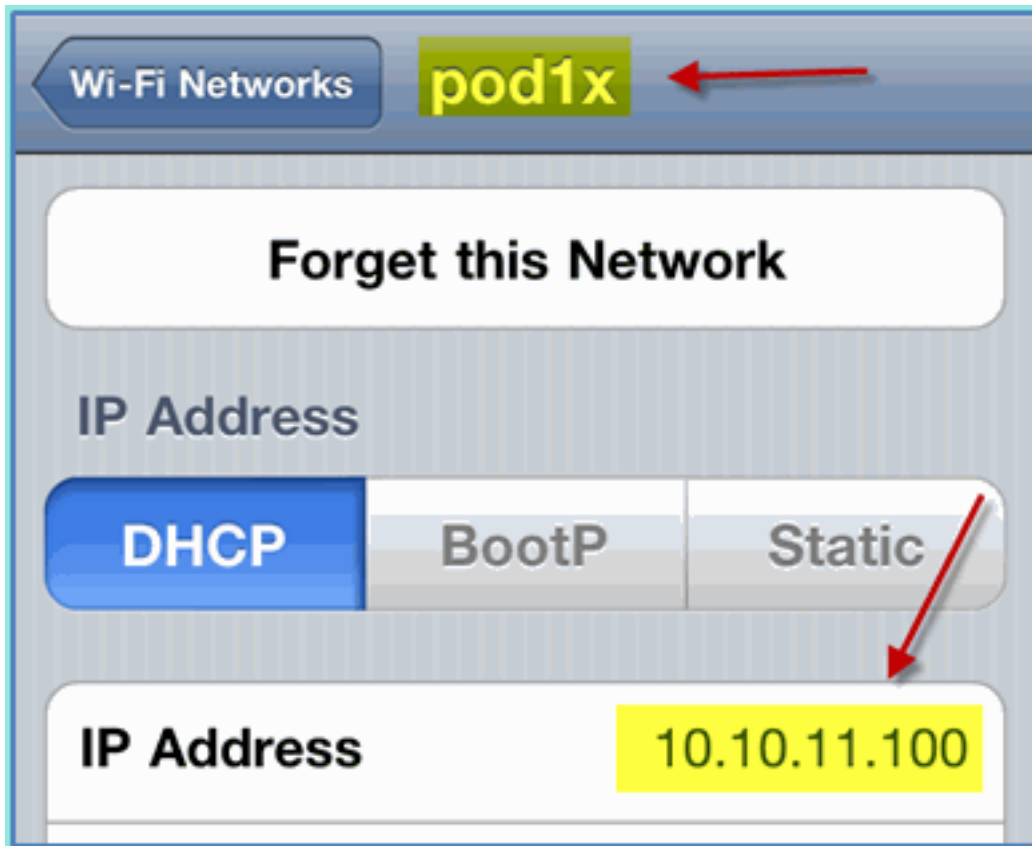
1. À partir du WLC, naviguez vers **WLAN > WLANs**. Cliquez pour modifier votre SSID sécurisé créé dans l'exercice précédent.
2. Remplacez Interface/Interface Group par **Employee**, puis cliquez sur **Apply**.

The screenshot displays the Cisco WLAN configuration interface. At the top, the Cisco logo is on the left, and navigation tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, and SECURITY are on the right. The 'WLANs' tab is selected. On the left sidebar, a tree view shows 'WLANs' and 'Advanced' folders, with 'WLANs' selected. The main content area is titled 'WLANs > Edit 'pod1x''. Below this title are four tabs: General, Security, QoS, and Advanced. The 'General' tab is active. The configuration details are as follows:

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security to
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	guest
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Red arrows point to the 'WLANs' tab in the top navigation, the 'WLANs' folder in the sidebar, the 'General' tab, and the 'management' option in the dropdown menu for 'Interface/Interface Group(G)'. A mouse cursor is hovering over the 'employee' option in the dropdown menu.

3. S'il est configuré correctement, un périphérique reçoit une adresse IP du VLAN employé (10.10.11.0/24). Cet exemple montre un périphérique iOS qui obtient une nouvelle adresse



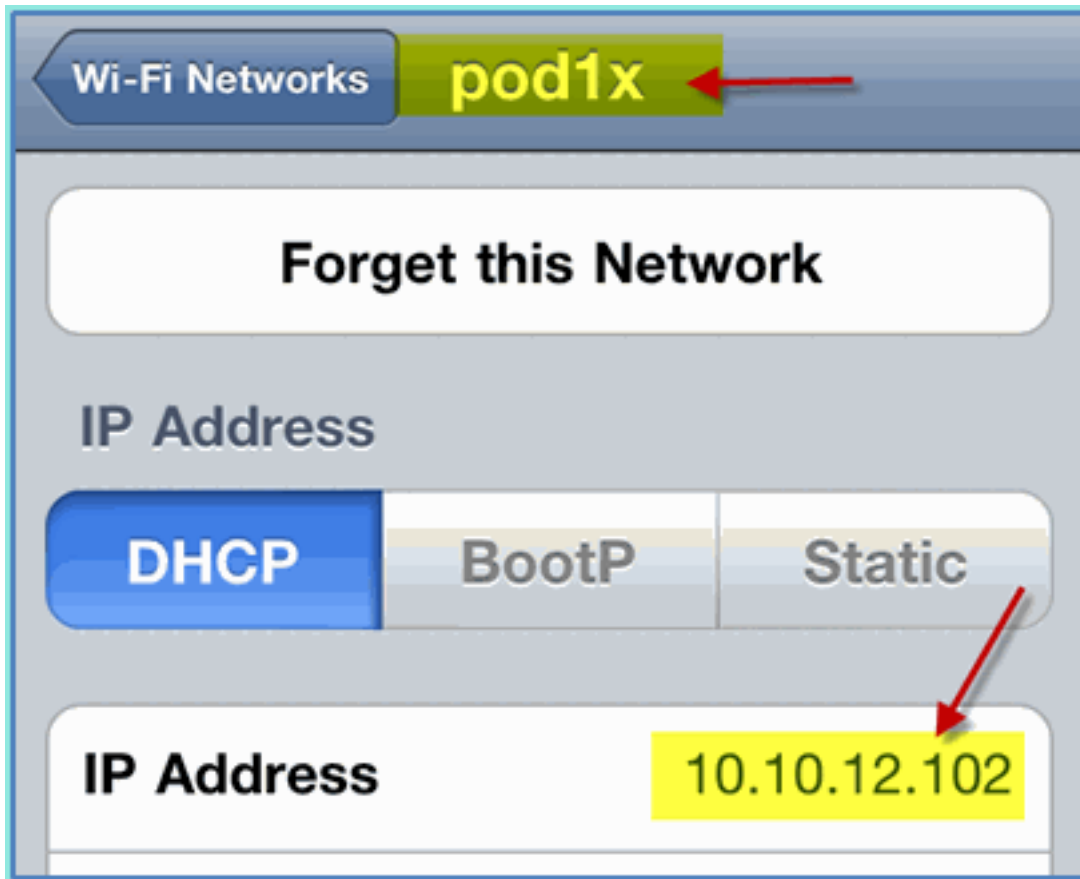
IP.

4. Une fois l'interface précédente confirmée, changez l'affectation de l'interface WLAN en **Guest**, puis cliquez sur **Apply**.

The screenshot displays the Cisco WLAN configuration page. At the top, the navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The main content area is titled 'WLANs > Edit 'pod1x''. Below this, there are four tabs: 'General', 'Security', 'QoS', and 'Advanced'. The 'General' tab is active, showing the following configuration details:

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under se
Radio Policy	All
Interface/Interface Group(G)	quest
Multicast Vlan Feature	quest
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

5. S'il est configuré correctement, un périphérique reçoit une adresse IP du VLAN invité (10.10.12.0/24). Cet exemple montre un périphérique iOS qui obtient une nouvelle adresse



IP.

6. **IMPORTANT** : redéfinissez l'affectation d'interface sur la gestion d'origine.
7. Cliquez sur **Apply** et enregistrez la configuration pour le WLC.

[Authentification sans fil pour iOS \(iPhone/iPad\)](#)

Associez au WLC via un SSID authentifié un utilisateur INTERNE (ou un utilisateur AD intégré) à l'aide d'un appareil iOS tel qu'un iPhone, iPad ou iPod. Ignorez ces étapes si elles ne s'appliquent pas.

1. Sur l'appareil iOS, accédez aux paramètres WLAN. Activez WIFI, puis sélectionnez le SSID 802.1X créé dans la section précédente.
2. Fournissez ces informations afin de vous connecter :
Nom d'utilisateur : employé (interne - Employé) ou entrepreneur (interne - Entrepreneur)
Mot de passe :



XXXX

3. Cliquez pour accepter le certificat



ISE.

4. Vérifiez que le périphérique iOS obtient une adresse IP de l'interface de gestion



(VLAN10).

5. Sur le WLC > Monitor > Clients, vérifiez les informations de point de terminaison, y compris l'utilisation, l'état et le type EAP.

The screenshot displays the Cisco ISE Monitor interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The left sidebar shows a menu with 'Monitor' selected, and sub-items like 'Summary', 'Access Points', 'Cisco CleanAir', 'Statistics', 'CDP', 'Rogues', 'Clients', and 'Multicast'. The main content area is titled 'Clients > Detail' and is divided into two sections: 'Client Properties' and 'Security Information'.

Client Properties

MAC Address	5c:59:48:40:82:8d
IP Address	10.10.10.102
Client Type	Regular
User Name	aduser
Port Number	1
Interface	management
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RUN
AAA Override ACL Name	none



6. De même, les informations client peuvent être fournies par la page ISE > Monitor > Authentication.

CISCO Identity Services Engine

Home Monitor Policy Administration

Authentications Alarms Reports Troubleshoot

Add or Remove Columns Refresh

Time	Status	Details	Username	Endpoint ID	Network Device	Authorization Profiles	Ident
Jul 13,11 04:39:36.573 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	
Jul 13,11 04:38:46.285 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	

7. Cliquez sur l'icône **Details** afin d'effectuer une hiérarchisation vers le bas jusqu'à la session pour obtenir des informations détaillées sur la session.



Showing Page 1 of 1

First Prev

AAA Protocol > RADIUS Authentication Detail

RADIUS Audit Session ID : 0a0a0a050000000d4e1e2a45

AAA session ID : ise/99967658/11

Date : July 13, 2011

Generated on July 13, 2011 4:41:11 PM PDT

Authentication Summary

Logged At: July 13, 2011 4:39:36.573 PM

RADIUS Status: Authentication succeeded

NAS Failure:

Username: aduser

MAC/IP Address: 5C:59:48:40:82:8D

Network Device: WLC : 10.10.10.5 :

Allowed Protocol: Default Network Access

Identity Store: AD1

Authorization Profiles: PermitAccess

SGA Security Group:

Authentication Protocol : PEAP(EAP-MSCHAPv2)

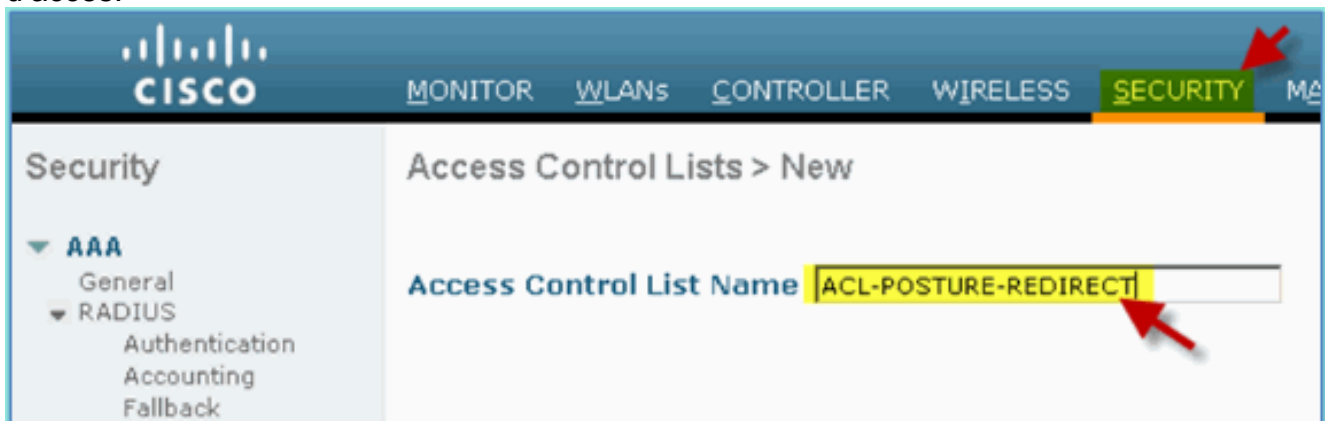
[Ajouter une ACL de redirection de position au WLC](#)

La liste de contrôle d'accès de redirection de position est configurée sur le WLC, où ISE utilisera pour restreindre la position du client. Efficacement et au minimum, la liste de contrôle d'accès autorise le trafic entre ISE. Des règles facultatives peuvent être ajoutées à cette liste de contrôle d'accès si nécessaire.

1. Accédez à **WLC > Security > Access Control Lists > Access Control Lists**. Cliquez sur **New**.



2. Entrez un nom (ACL-POSTURE-REDIRECT) pour la liste de contrôle d'accès.



3. Cliquez sur **Add New Rule** pour la nouvelle liste de contrôle d'accès. Définissez les valeurs suivantes sur la séquence de liste de contrôle d'accès #1. Cliquez sur **Apply** lorsque vous avez terminé. Source : Tout Destination : adresse IP 10.10.10.70, 255.255.255.255 Protocole : Tout Action : Autoriser

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Access Control Lists > Rules > Edit

Sequence:

Source:

Destination: IP Address: Netmask:

Protocol:

DSCP:

Direction:

Action:

4. La séquence de confirmation a été ajoutée.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any	0

5. Cliquez sur **Ajouter une nouvelle règle**. Définissez les valeurs suivantes sur la séquence de liste de contrôle d'accès #2. Cliquez sur **Apply** lorsque vous avez terminé. Source : adresse IP 10.10.10.70, 255.255.255.255 Destination : Tout Protocole : Tout Action : Autoriser

Sequence:

Source: IP Address: Netmask:

Destination:

Protocol:

DSCP:

Direction:

Action:

6. La séquence de confirmation a été ajoutée.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
<u>1</u>	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
		0.0.0.0	255.255.255.255					
<u>2</u>	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
		255.255.255.255	0.0.0.0					

7. Définissez les valeurs suivantes sur la séquence de liste de contrôle d'accès #3. Cliquez sur **Apply** lorsque vous avez terminé. Source : Tout Destination : Tout Protocole : UDP Port source : DNS Port de destination : Tout Action :

Sequence: 3

Source: Any

Destination: Any

Protocol: UDP

Source Port: DNS

Destination Port: Any

DSCP: Any

Direction: Any

Action: Permit

Autoriser

8. La séquence de confirmation a été ajoutée.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
<u>1</u>	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
		0.0.0.0	255.255.255.255					
<u>2</u>	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
		255.255.255.255	0.0.0.0					
<u>3</u>	Permit	0.0.0.0 /	0.0.0.0 /	UDP	DNS	Any	Any	Any
		0.0.0.0	0.0.0.0					

9. Cliquez sur **Ajouter une nouvelle règle**. Définissez les valeurs suivantes sur la séquence de

liste de contrôle d'accès #4. Cliquez sur **Apply** lorsque vous avez terminé. Source : ToutDestination : ToutProtocole : UDPPort source : ToutPort de destination : DNSAction : Autoriser

The screenshot shows a configuration form for a firewall rule. The fields and their values are as follows:

- Sequence:** 4
- Source:** Any
- Destination:** Any
- Protocol:** UDP
- Source Port:** Any
- Destination Port:** DNS
- DSCP:** Any
- Direction:** Any
- Action:** Permit

10. La séquence de confirmation a été ajoutée.

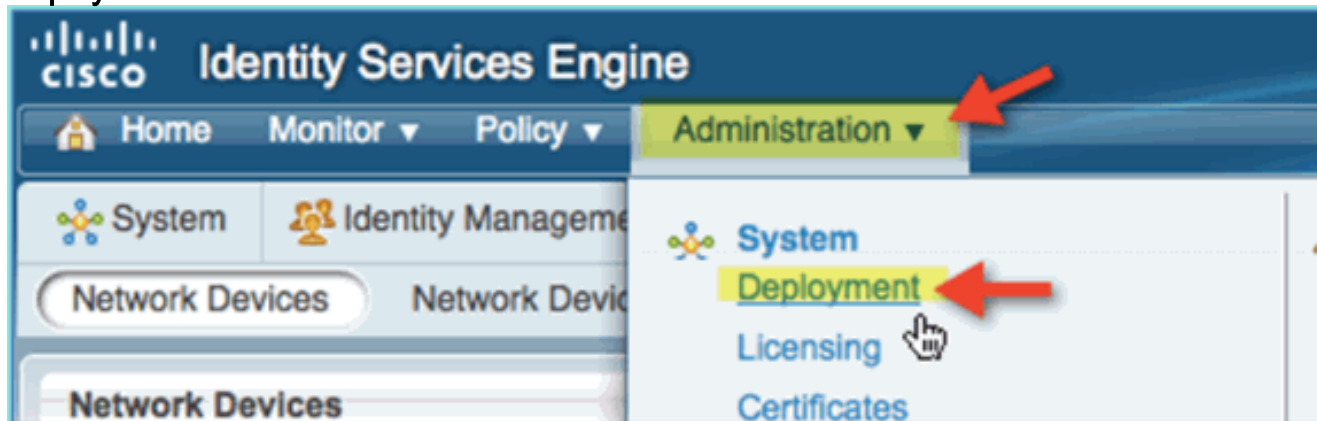
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
2	Permit	0.0.0.0 /	255.255.255.255 /	Any	Any	Any	Any	Any
3	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
3	Permit	255.255.255.255 /	0.0.0.0 /	UDP	DNS	Any	Any	Any
4	Permit	0.0.0.0 /	0.0.0.0 /	UDP	Any	DNS	Any	Any
		0.0.0.0 /	0.0.0.0 /					

11. Enregistrez la configuration actuelle du WLC.

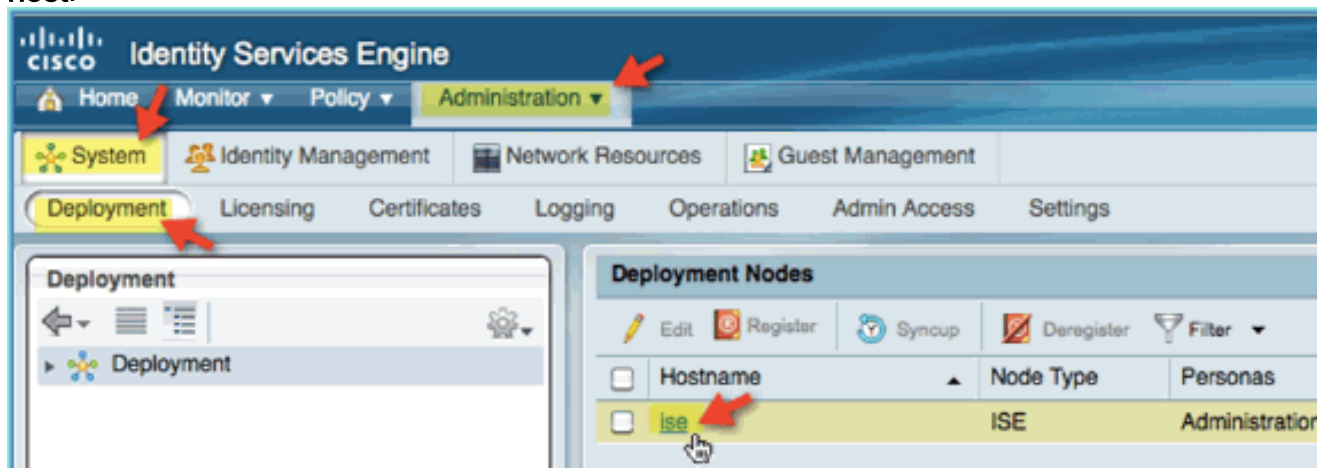
Activer les sondes de profilage sur ISE

L'ISE doit être configuré en tant qu'analyseur pour profiler efficacement les terminaux. Par défaut, ces options sont désactivées. Cette section explique comment configurer ISE pour qu'il soit utilisé comme sonde.

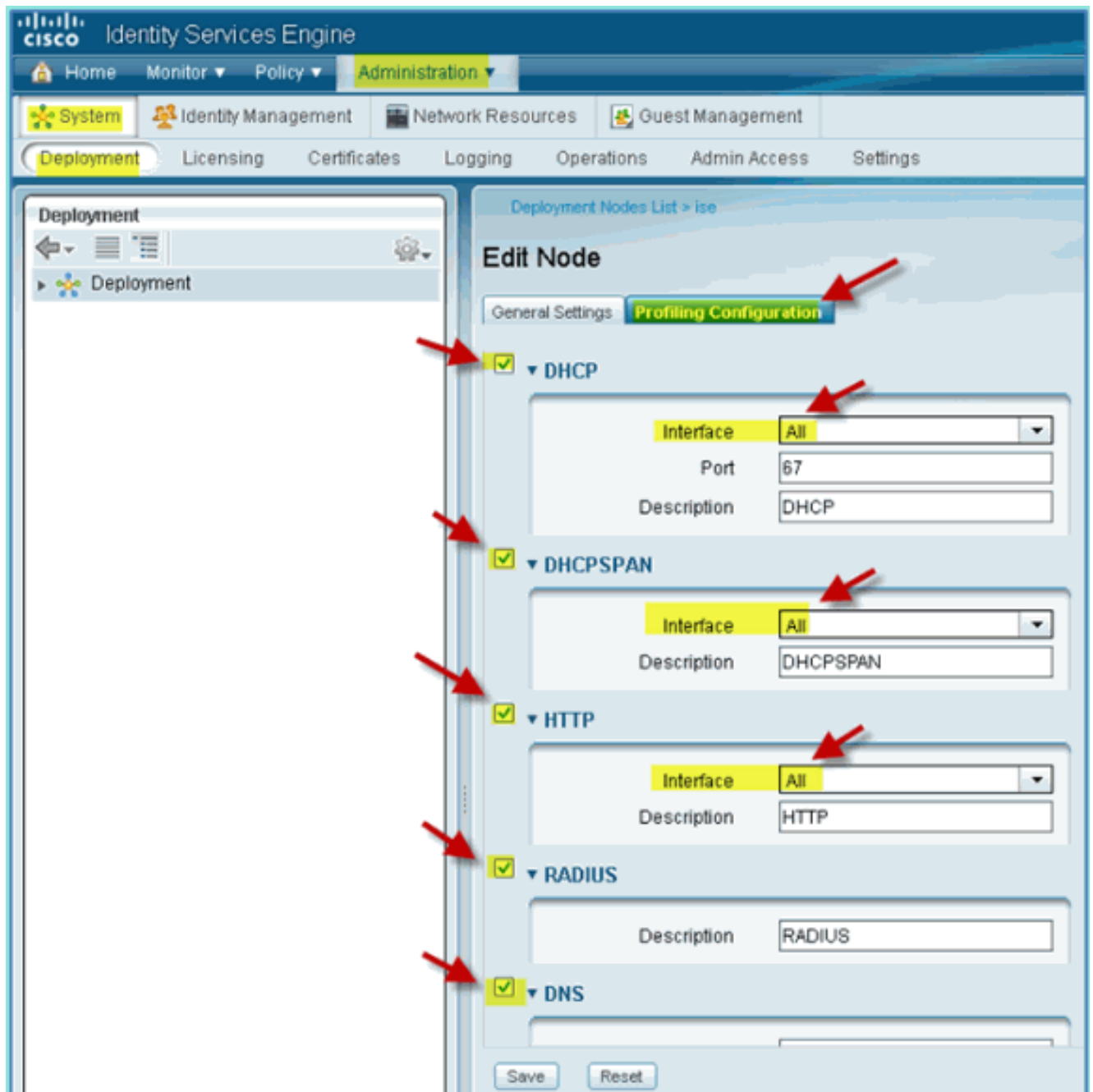
1. Dans Gestion ISE, accédez à **Administration > System > Deployment**.



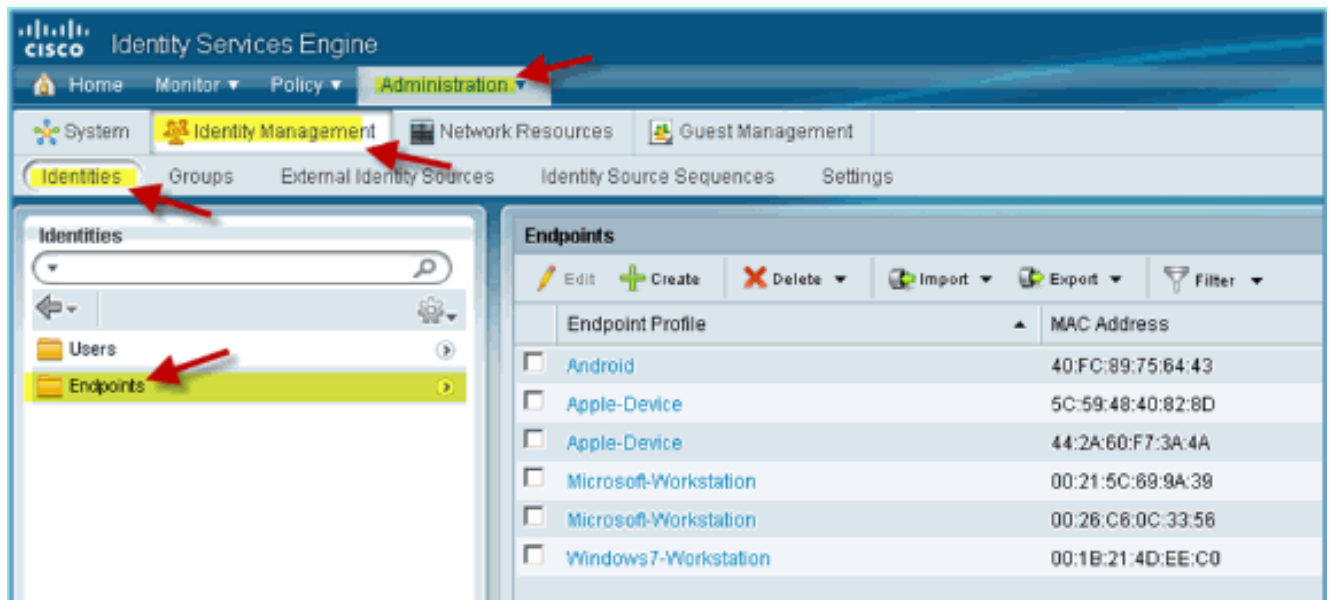
2. Sélectionnez ISE. Cliquez sur **Edit ISE host**.



3. Sur la page Edit Node, sélectionnez Profiling Configuration et configurez les éléments suivants :
DHCP : activé, tout (ou par défaut)
DHCPSPAN : Activé, Tous (ou par défaut)
HTTP : activé, tout (ou par défaut)
RADIUS : activé, S/ODNS : activé,
S/O



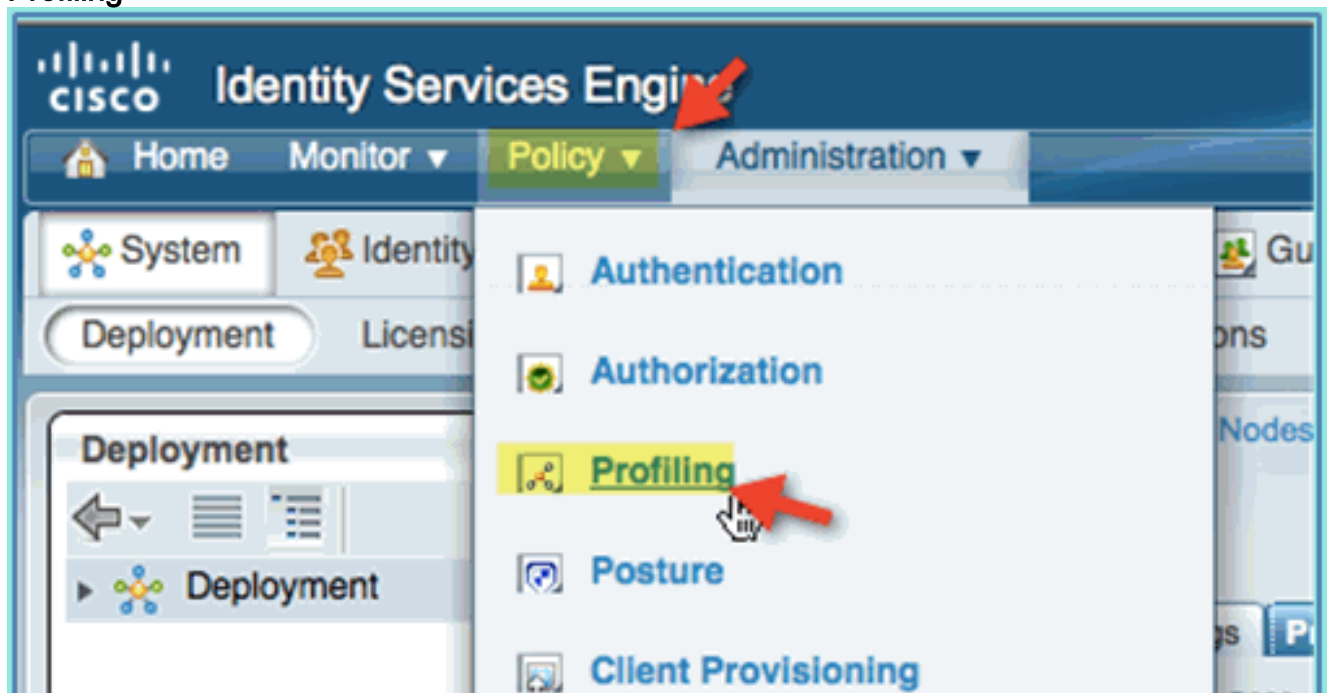
4. Réassocier les périphériques (iPhone/iPad/Droids/Mac, etc.).
5. Confirmez les identités des terminaux ISE. Accédez à **Administration > Identity Management > Identities**. Cliquez sur Endpoints pour afficher la liste des éléments profilés. **Remarque** : le profilage initial provient de sondes RADIUS.



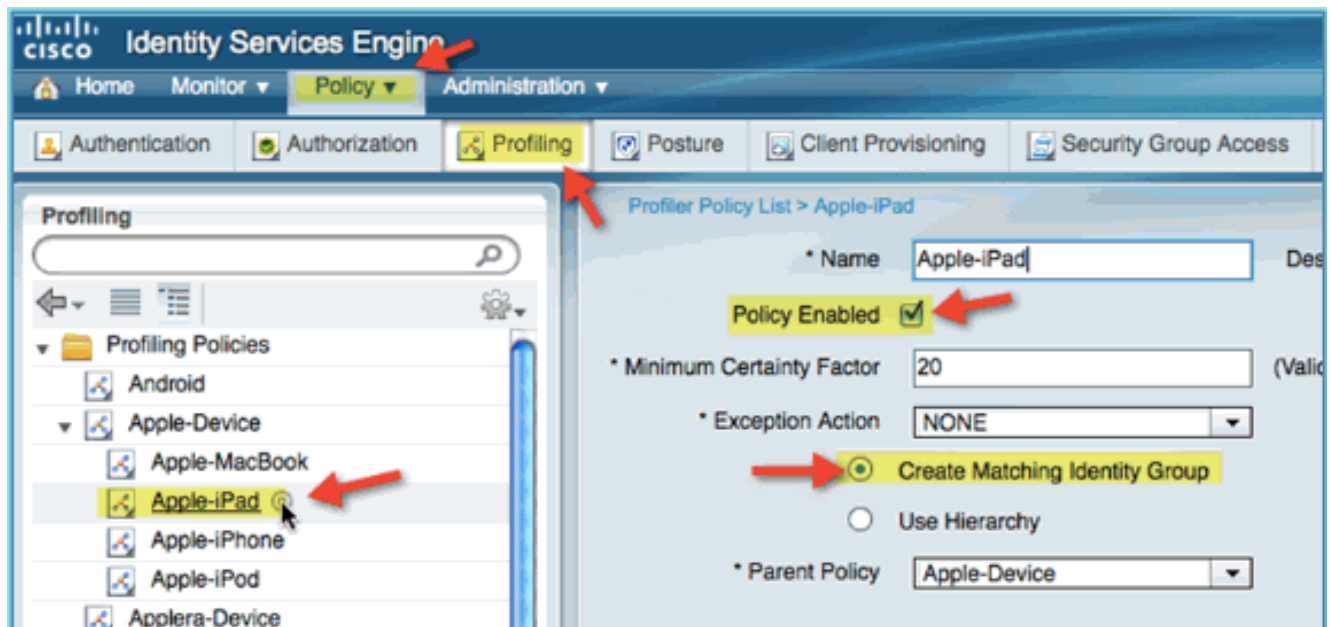
Activer les stratégies de profil ISE pour les périphériques

Dès sa livraison, ISE fournit une bibliothèque de différents profils de terminaux. Complétez ces étapes afin d'activer les profils pour les périphériques :

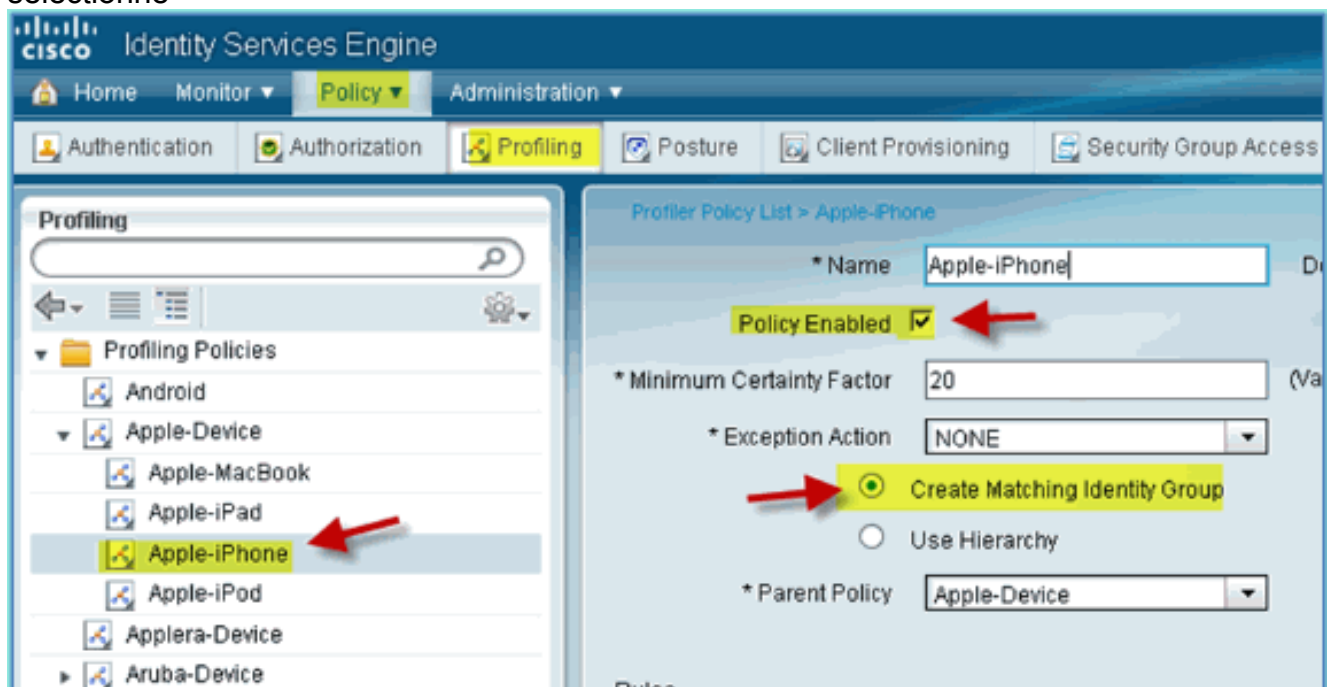
1. Dans ISE, accédez à **Policy > Profiling**.



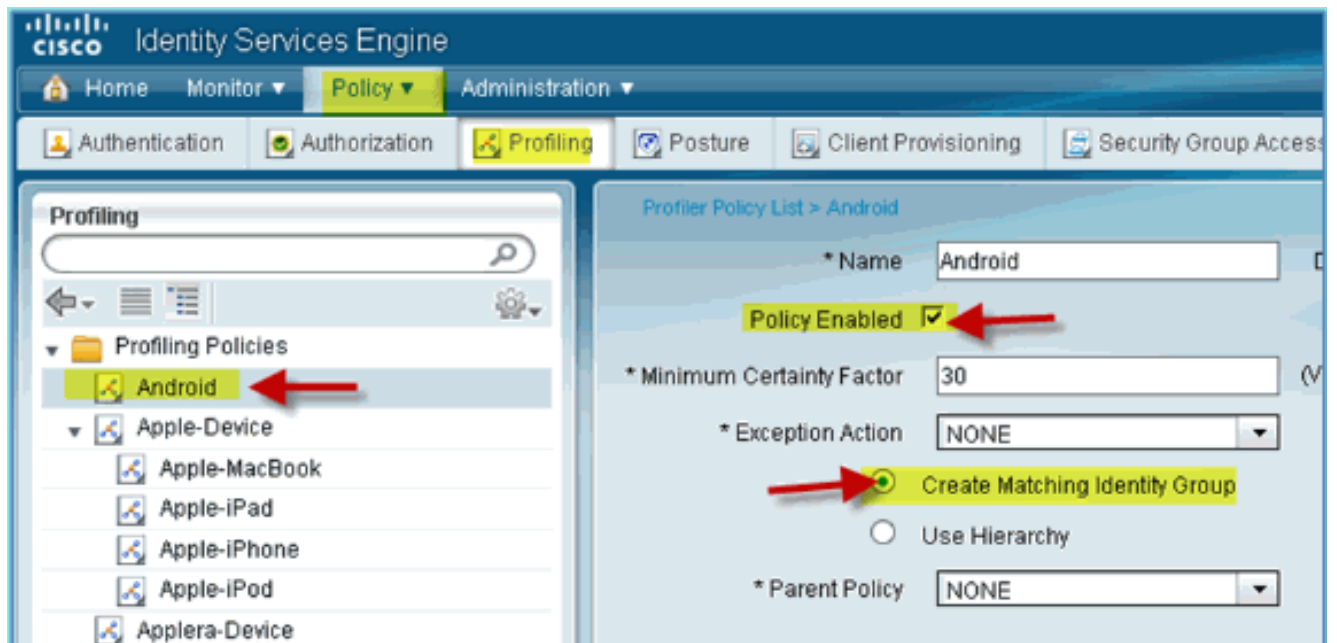
2. Dans le volet de gauche, développez **Stratégies de profilage**.
3. Cliquez sur **Apple Device > Apple iPad**, et définissez les paramètres suivants :
Stratégie activée : activée
Créer un groupe d'identités correspondant : sélectionné



4. Cliquez sur **Apple Device > Apple iPhone**, définissez les paramètres suivants : Stratégie activée : activée
Créer un groupe d'identités correspondant : sélectionné



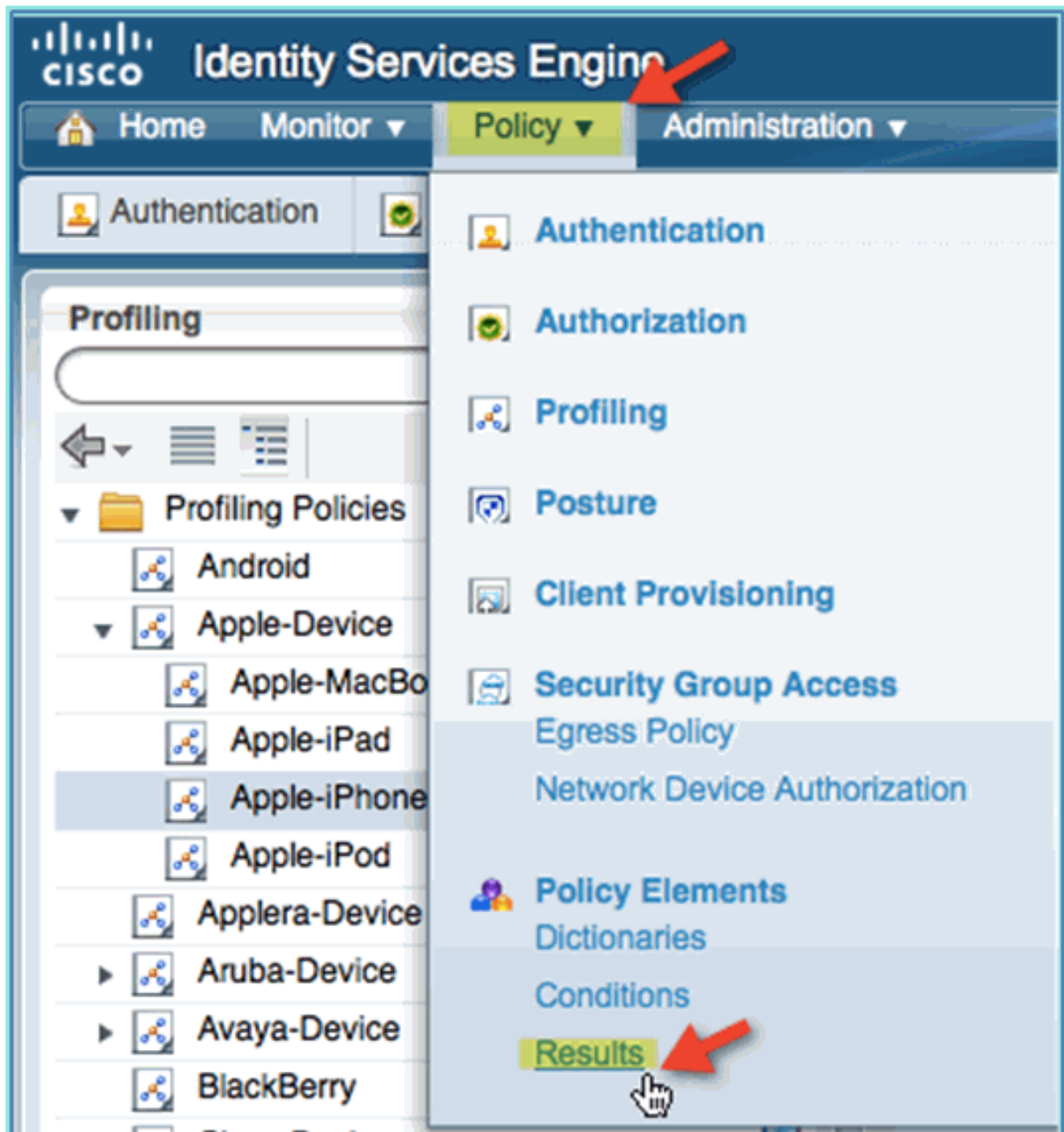
5. Cliquez sur **Android**, définissez les paramètres suivants : Stratégie activée : activée
Créer un groupe d'identités correspondant : sélectionné



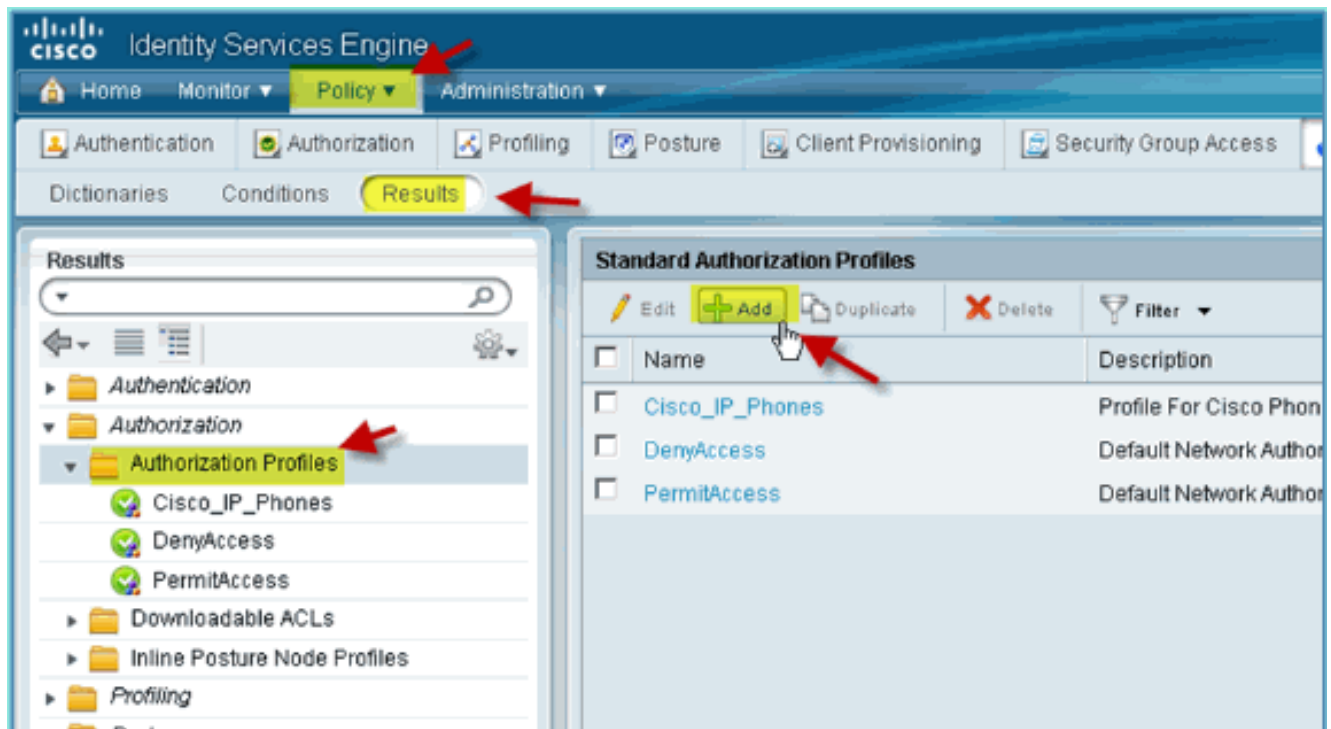
[Profil d'autorisation ISE pour redirection de découverte de position](#)

Complétez ces étapes afin de configurer une politique d'autorisation. La redirection permet de rediriger les nouveaux périphériques vers ISE pour une détection et un profilage corrects :

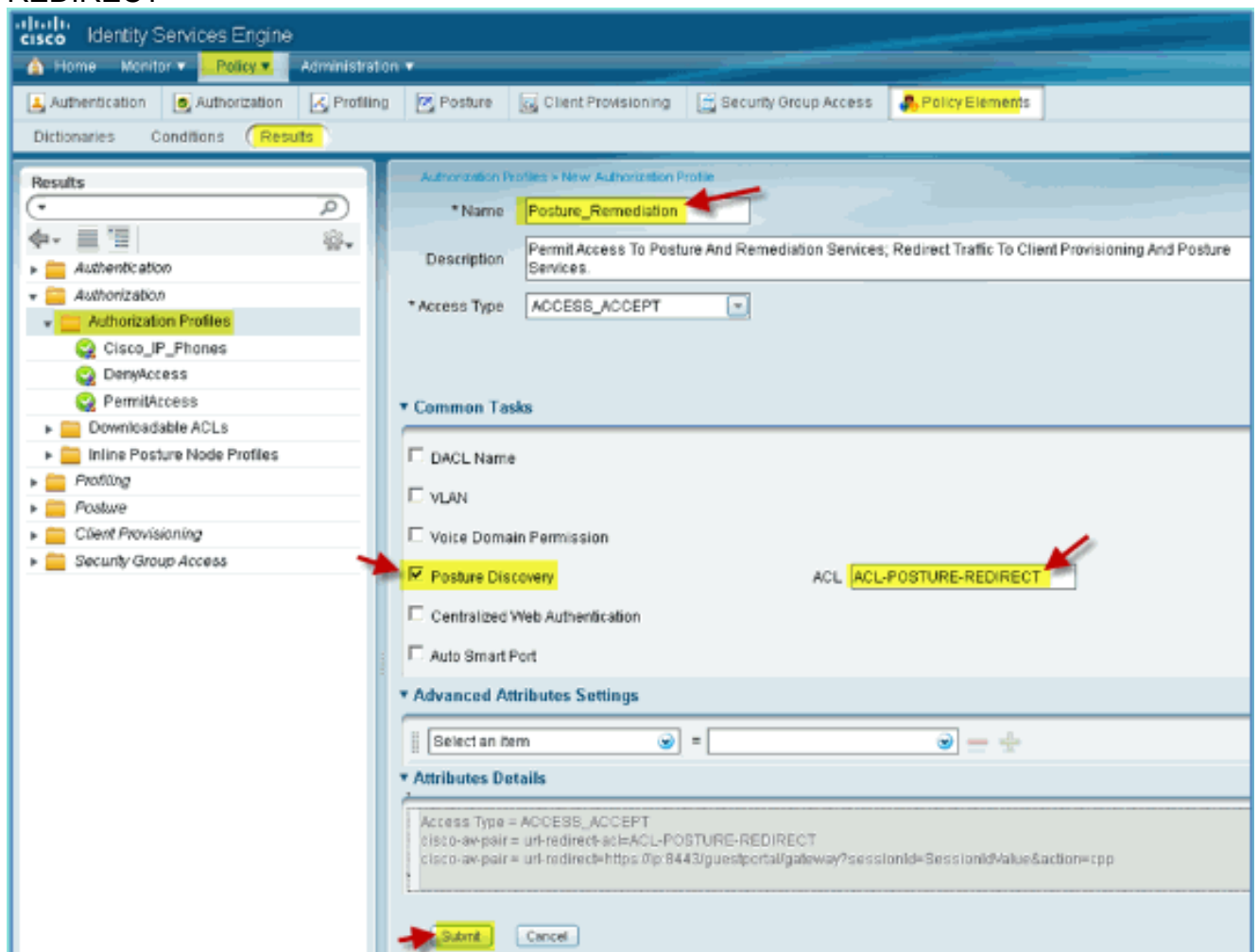
1. Dans ISE, accédez à **Policy > Policy Elements > Results**.



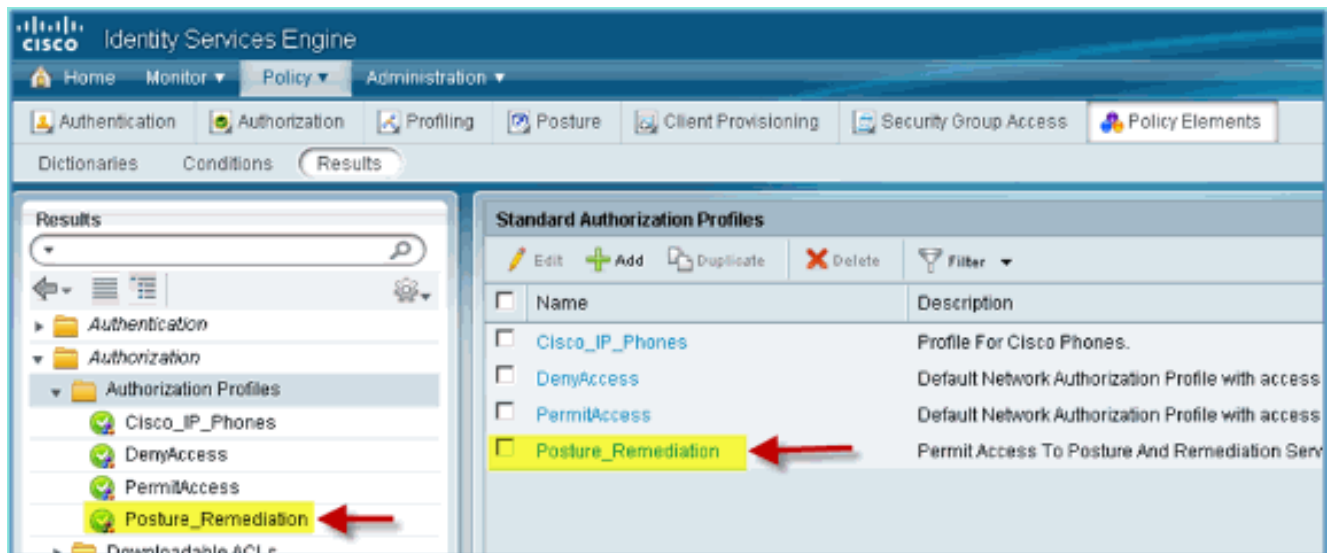
2. Développez **Autorisation**. Cliquez sur **Profils d'autorisation** (volet gauche), puis sur **Ajouter**.



3. Créez le profil d'autorisation avec les éléments suivants :
 - Nom : Posture_RemediationType
 - d'accès : Access_Accept
 - Outils courants : Détection de position, activée
 - Détection de position, ACL ACL-POSTURE-REDIRECT



4. Cliquez sur **Submit** pour terminer cette tâche.
5. Vérifiez que le nouveau profil d'autorisation est ajouté.

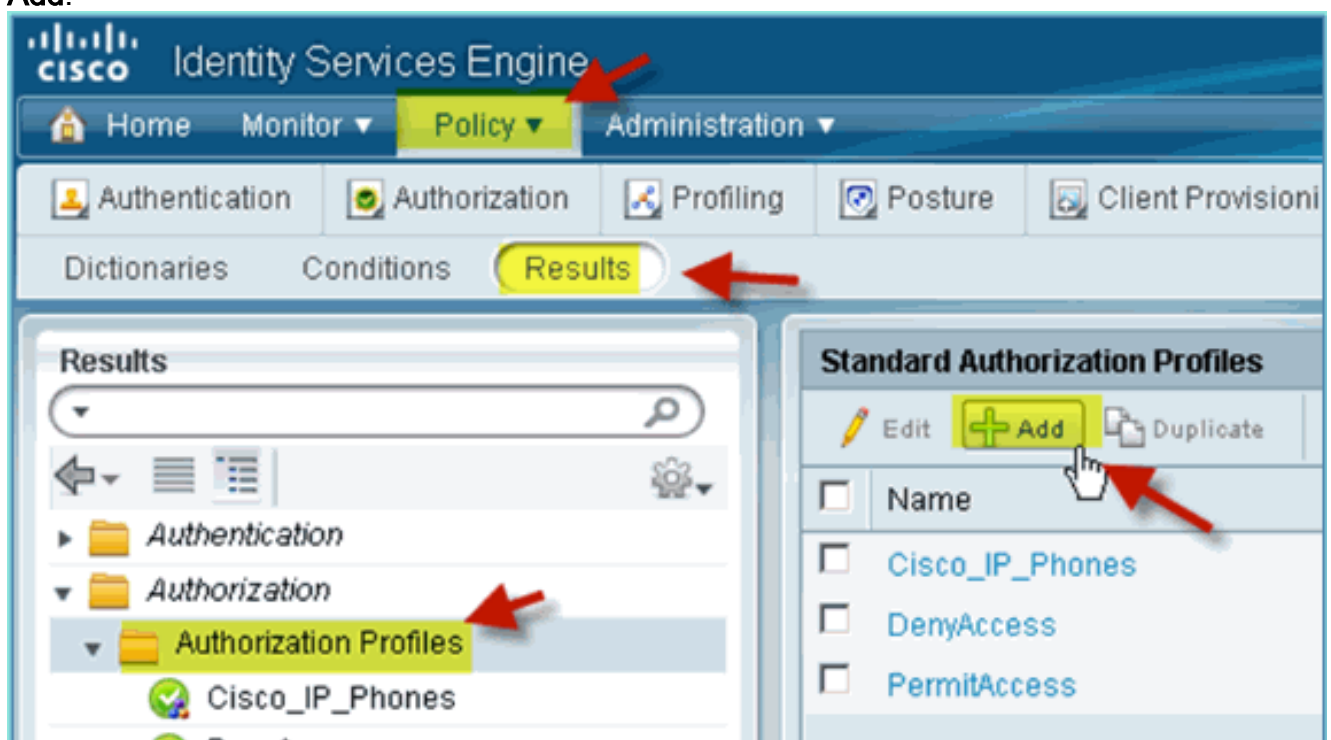


Créer un profil d'autorisation ISE pour l'employé

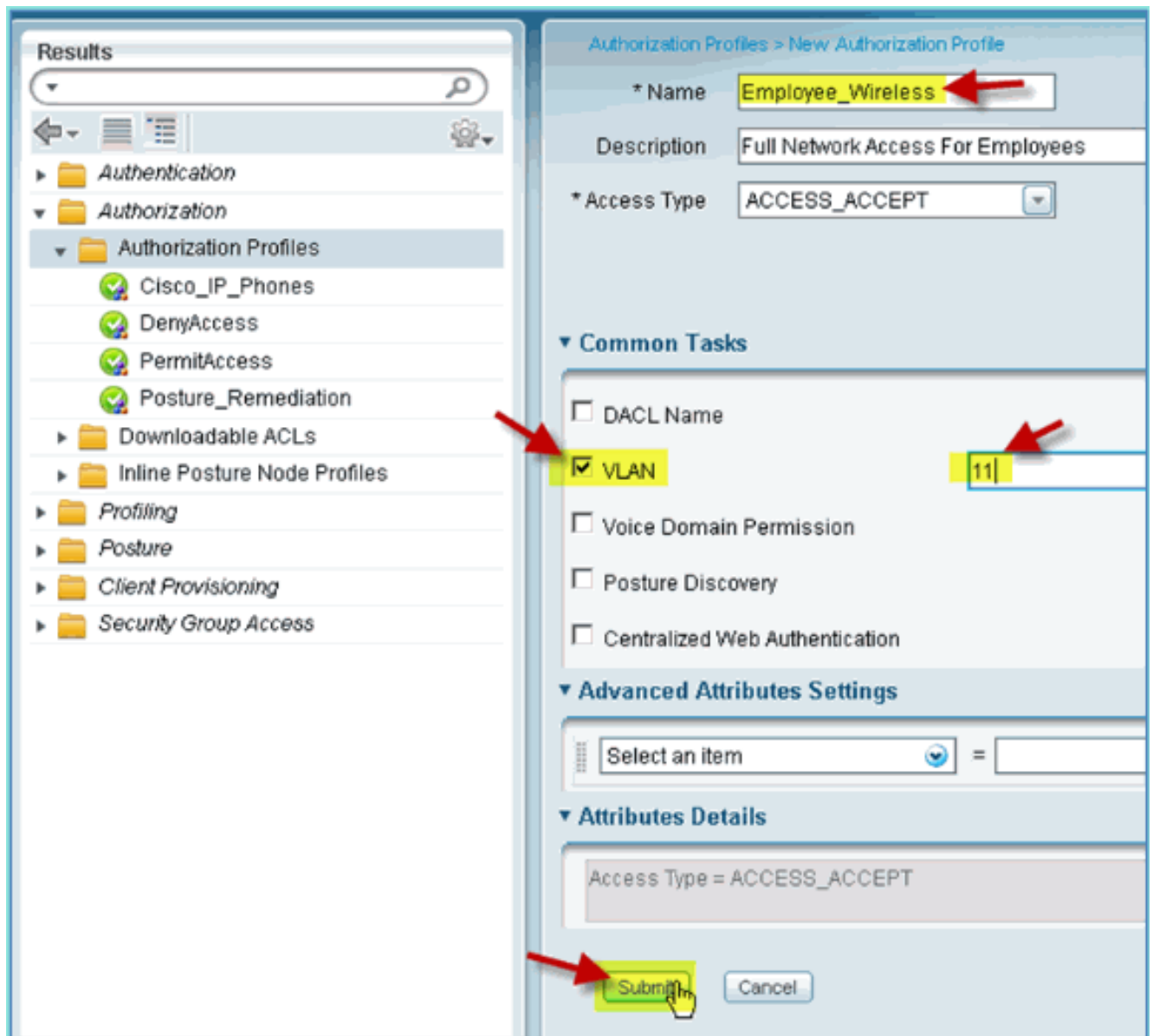
L'ajout d'un profil d'autorisation pour un employé permet à ISE d'autoriser et d'autoriser l'accès avec les attributs affectés. Le VLAN 11 employé est attribué dans ce cas.

Procédez comme suit :

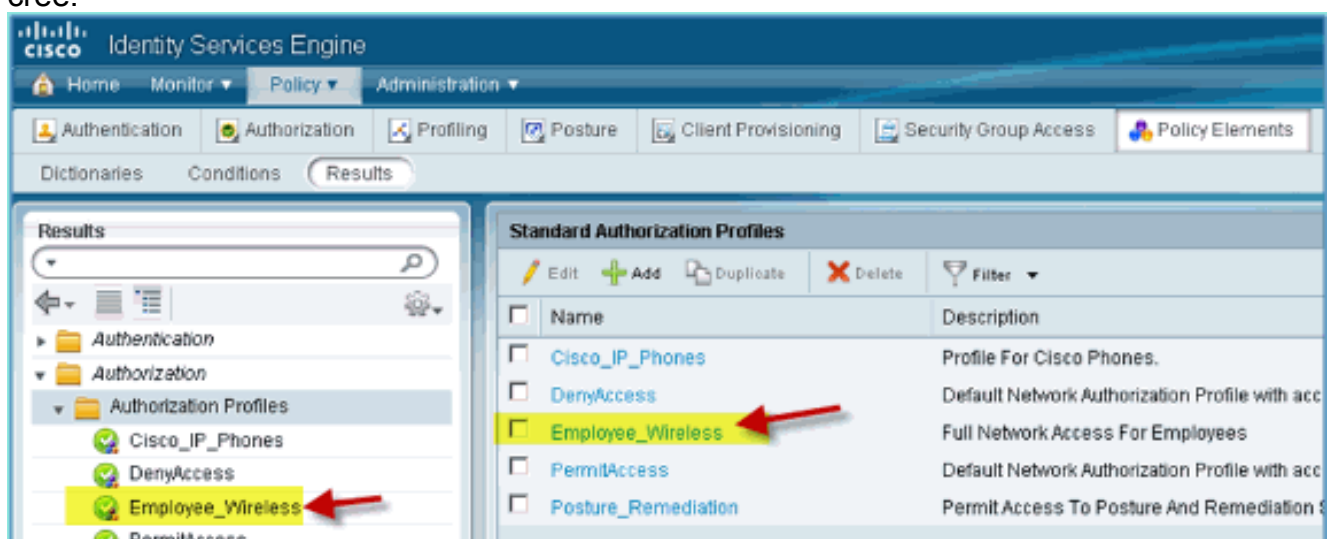
1. Dans ISE, accédez à **Policy > Results**. Développez **Authorization**, puis cliquez sur **Authorization Profiles** et cliquez sur **Add**.



2. Saisissez les informations suivantes pour le profil d'autorisation Employé : Nom : Employee_WirelessTâches courantes :VLAN, activéVLAN, sous-valeur 11
3. Cliquez sur **Submit** pour terminer cette tâche.



4. Vérifiez que le nouveau profil d'autorisation d'employé a été créé.

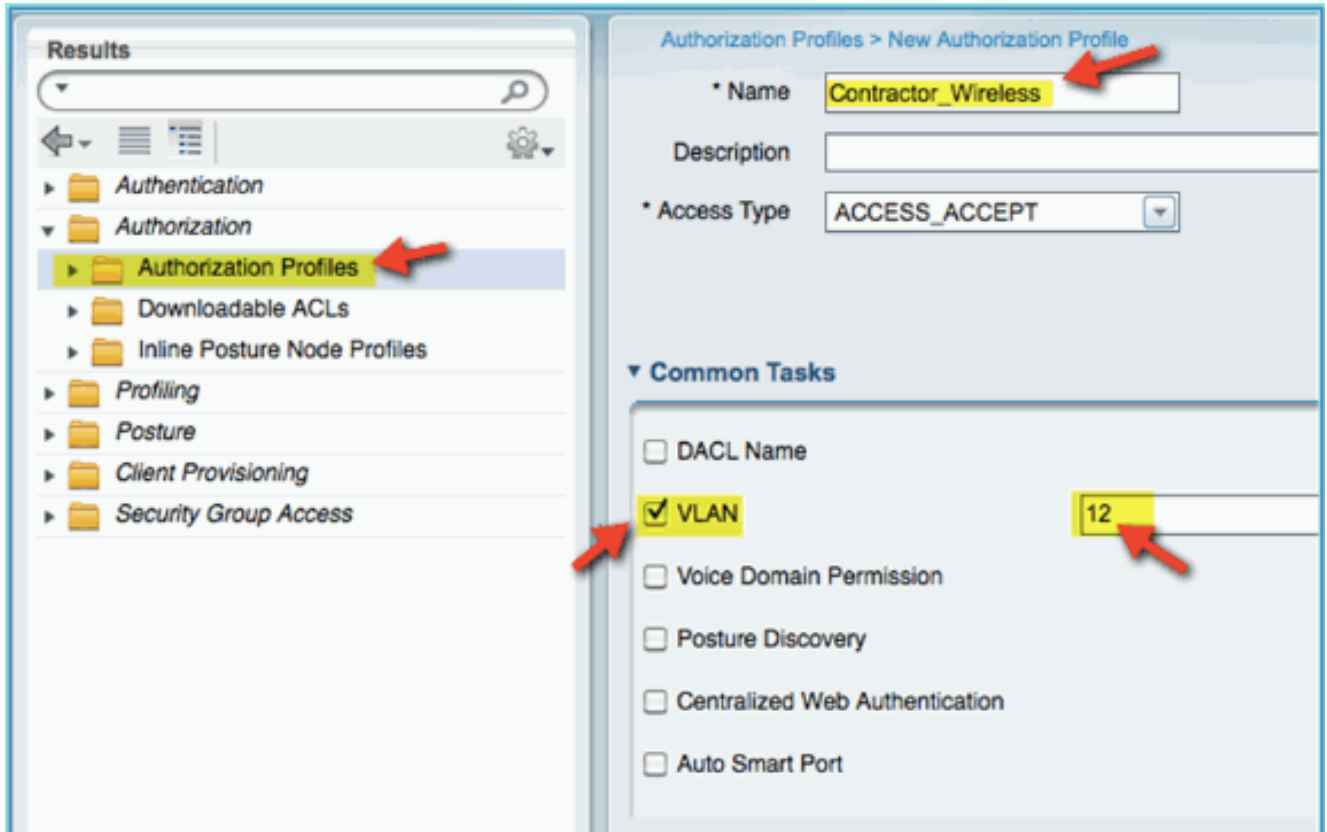


Créer un profil d'autorisation ISE pour le sous-traitant

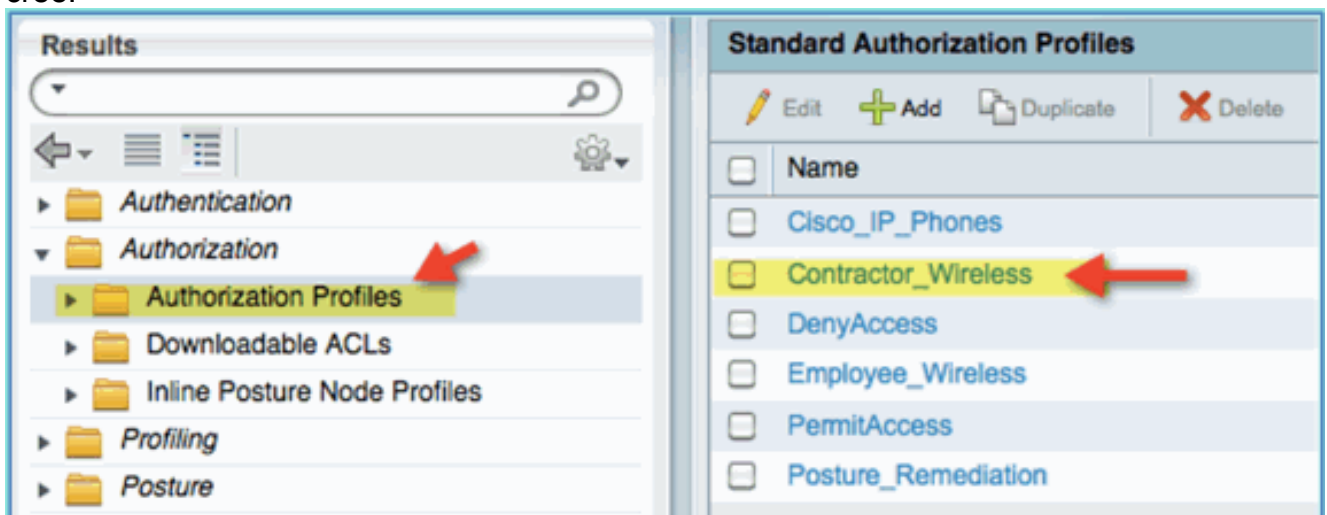
L'ajout d'un profil d'autorisation pour un sous-traitant permet à ISE d'autoriser et d'autoriser l'accès avec les attributs affectés. Le VLAN 12 du sous-traitant est attribué dans ce cas.

Procédez comme suit :

1. Dans ISE, accédez à **Policy > Results**. Développez **Authorization**, puis cliquez sur **Authorization Profiles** et cliquez sur **Add**.
2. Saisissez les informations suivantes pour le profil d'autorisation Employé : Nom : Employee_Wireless Tâches courantes : VLAN, activé VLAN, sous-valeur 12



3. Cliquez sur **Submit** pour terminer cette tâche.
4. Vérifiez que le profil d'autorisation du fournisseur a été créé.



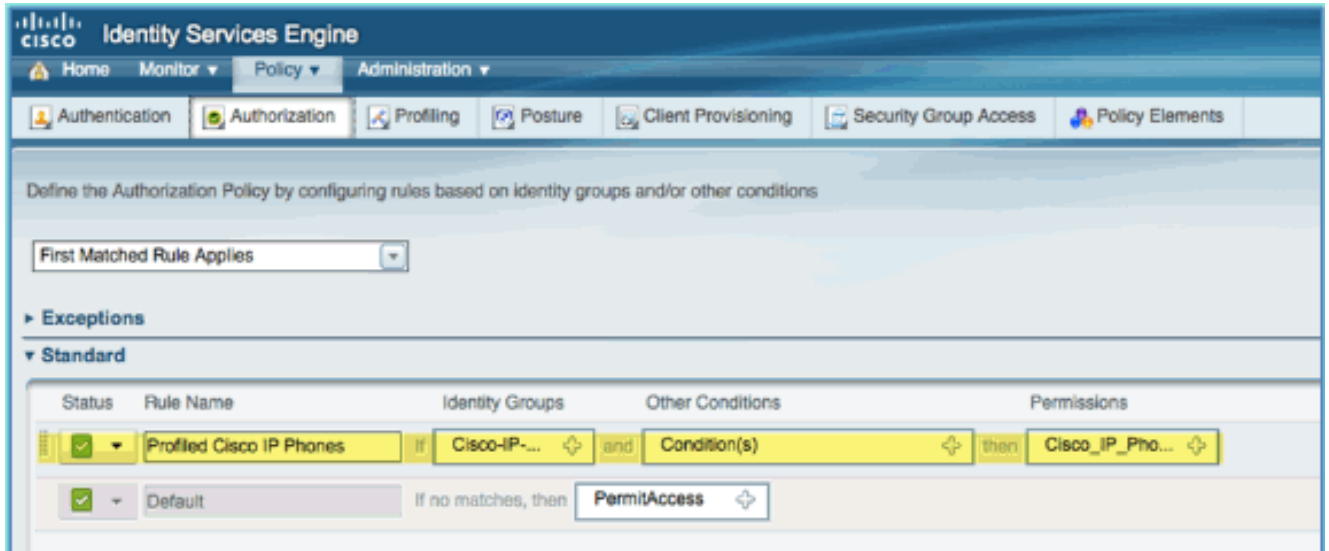
Politique d'autorisation pour la position/le profilage des périphériques

Si peu d'informations sont disponibles sur un nouveau périphérique lorsqu'il arrive sur le réseau,

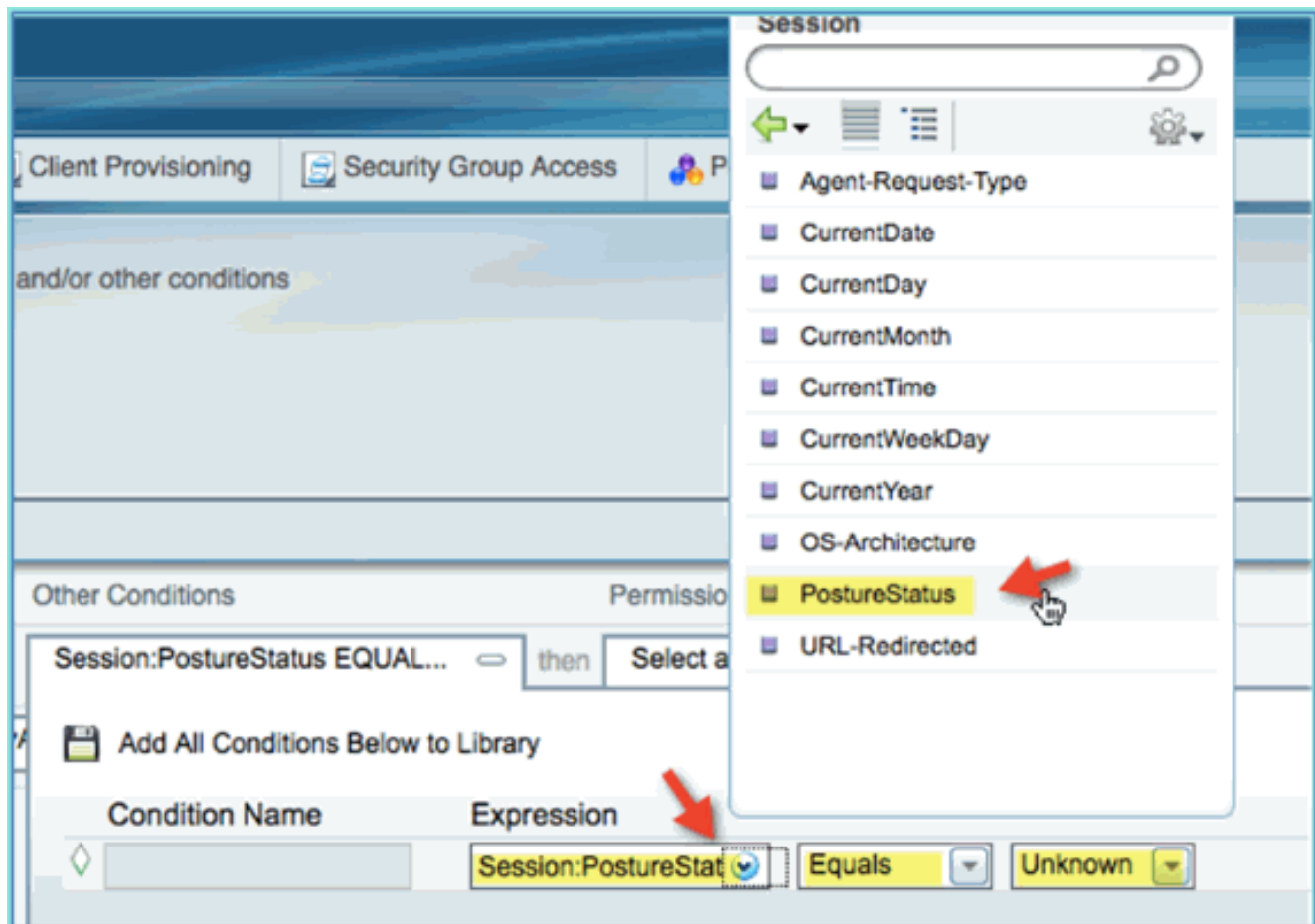
un administrateur crée la stratégie appropriée pour permettre l'identification des points d'extrémité inconnus avant d'autoriser l'accès. Dans cet exercice, la stratégie d'autorisation sera créée de sorte qu'un nouveau périphérique sera redirigé vers ISE pour l'évaluation de la position (pour les périphériques mobiles sans agent, seul le profilage est pertinent) ; les terminaux seront redirigés vers le portail captif ISE et identifiés.

Procédez comme suit :

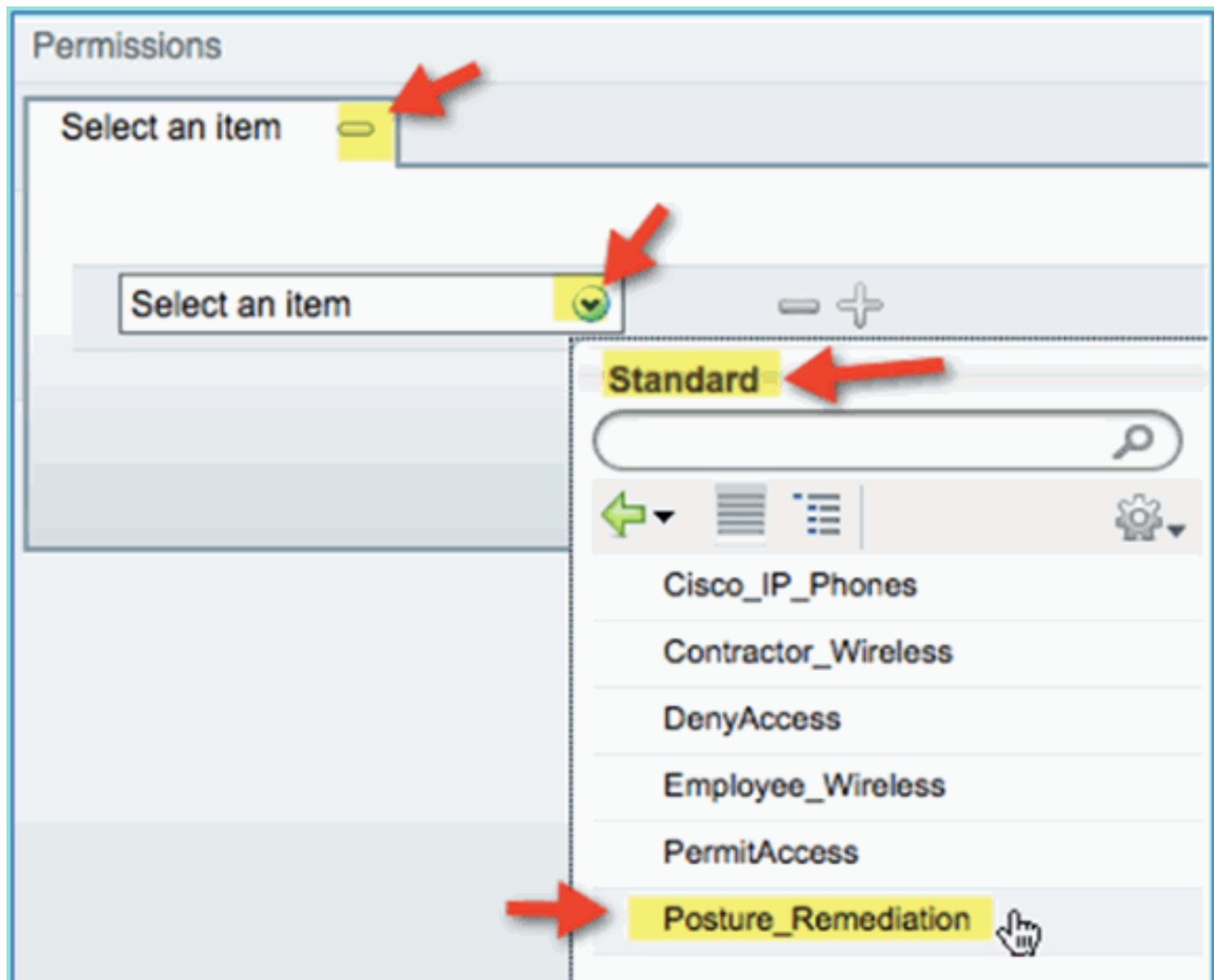
1. Dans ISE, accédez à **Policy > Authorization.**



2. Il existe une stratégie pour les téléphones IP Cisco avec profil. C'est prêt à l'emploi. Modifiez-le en tant que stratégie de posture.
3. Entrez les valeurs suivantes pour cette stratégie :
Nom de la règle : Posture_RemediationGroupes d'identités : TousAutres conditions > Créer nouveau : (Avancé) Session > ÉtatPositionÉtatPosture > Est égal à : Inconnu



4. Définissez les paramètres suivants pour les autorisations :Autorisations > Standard :
Posture_Remediation



5. Cliquez sur **Save**. Remarque : vous pouvez également créer des éléments de stratégie personnalisés pour faciliter leur utilisation.

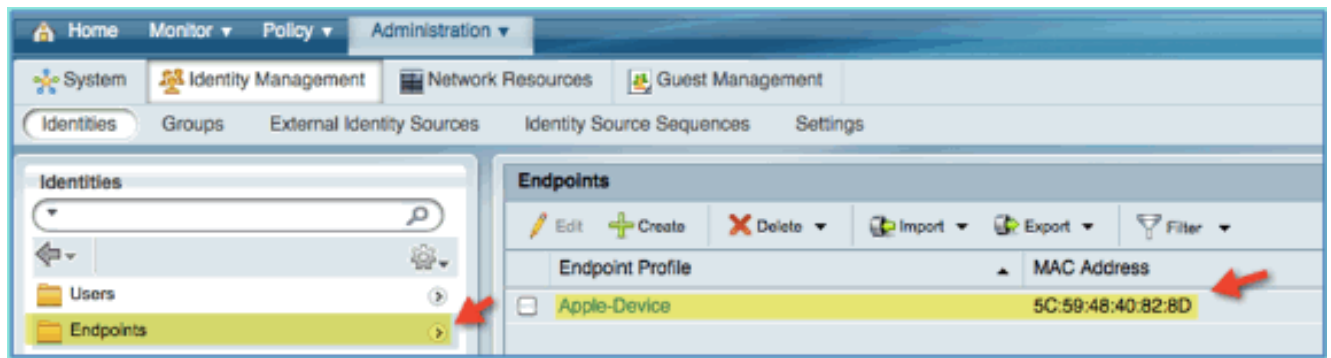
[Tester la politique de correction de posture](#)

Il est possible d'effectuer une démonstration simple pour montrer qu'ISE établit correctement le profil d'un nouveau périphérique en fonction de la politique de posture.

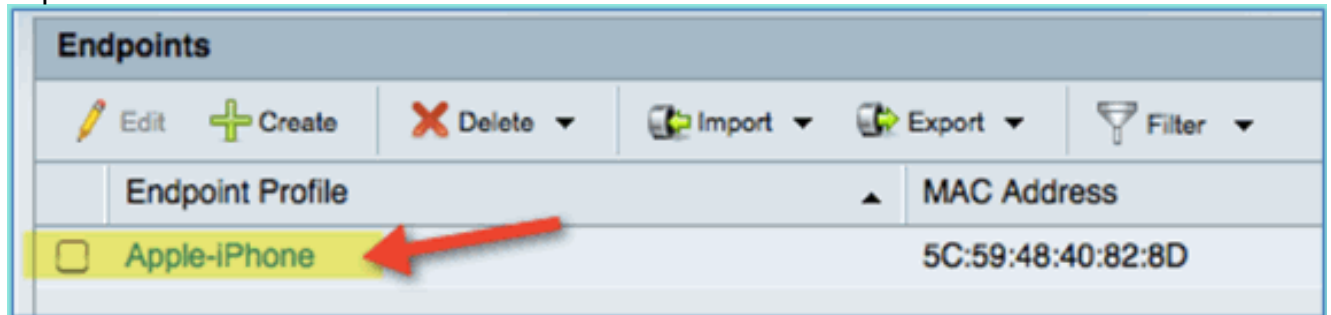
1. Dans ISE, accédez à **Administration > Identity Management > Identities**.



2. Cliquez sur **Terminaux**. Associez et connectez un périphérique (un iPhone dans cet exemple).



3. Actualisez la liste Endpoints. Observez les informations fournies.
4. À partir du périphérique d'extrémité, accédez à :URL : http://www (ou 10.10.10.10)Le périphérique est redirigé. Acceptez toute invite de certificats.
5. Une fois le périphérique mobile complètement redirigé, actualisez à nouveau la liste des terminaux à partir d'ISE. Observez ce qui a changé. Le terminal précédent (par exemple, Apple-Device) aurait dû être remplacé par « Apple-iPhone », etc. La raison en est que la sonde HTTP obtient efficacement des informations d'agent utilisateur, dans le cadre du processus de redirection vers le portail captif.

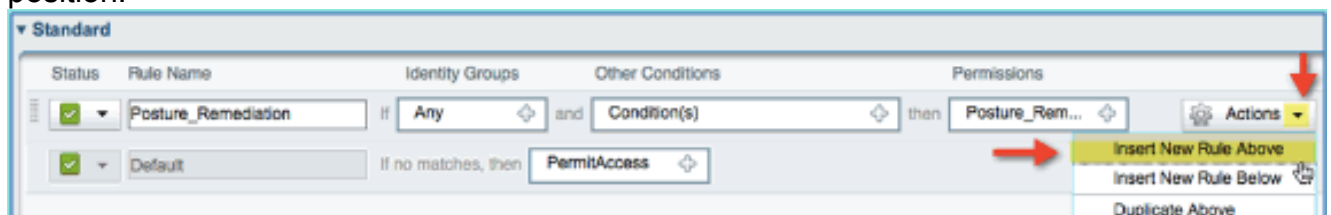


Politique d'autorisation pour accès différencié

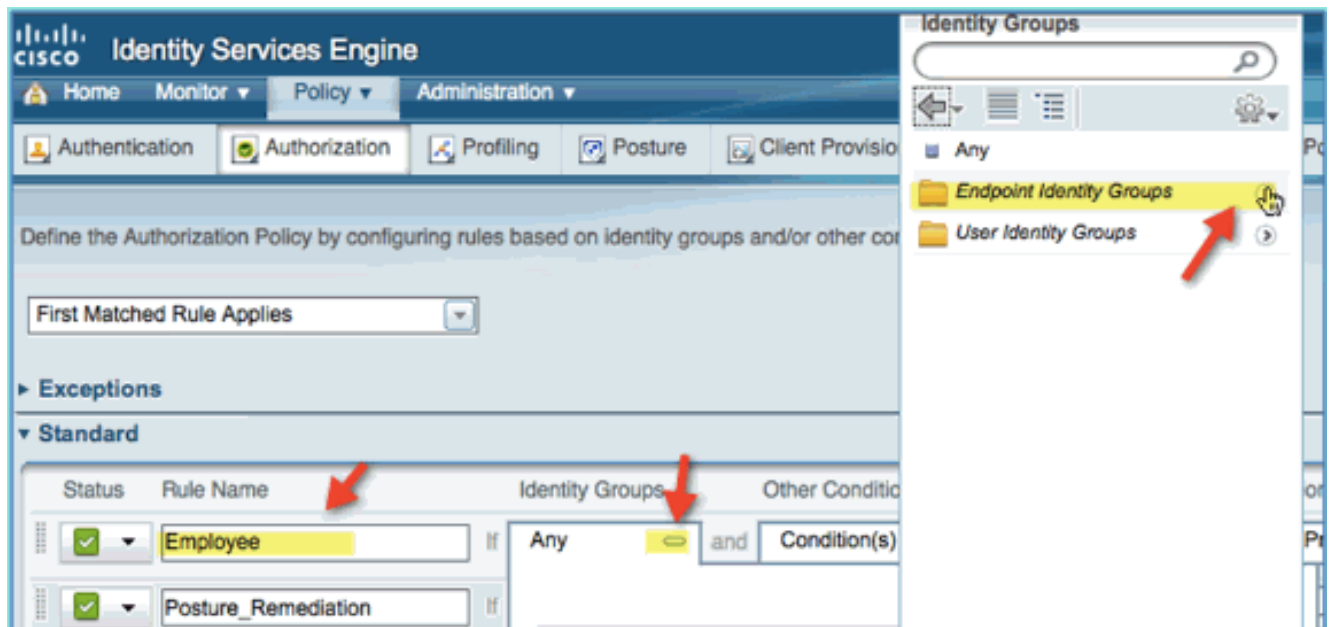
Après avoir testé avec succès l'autorisation de position, continuez à élaborer des politiques pour prendre en charge l'accès différencié pour l'employé et l'entrepreneur avec des périphériques connus et différentes affectations de VLAN spécifiques au rôle d'utilisateur (dans ce scénario, Employé et entrepreneur).

Procédez comme suit :

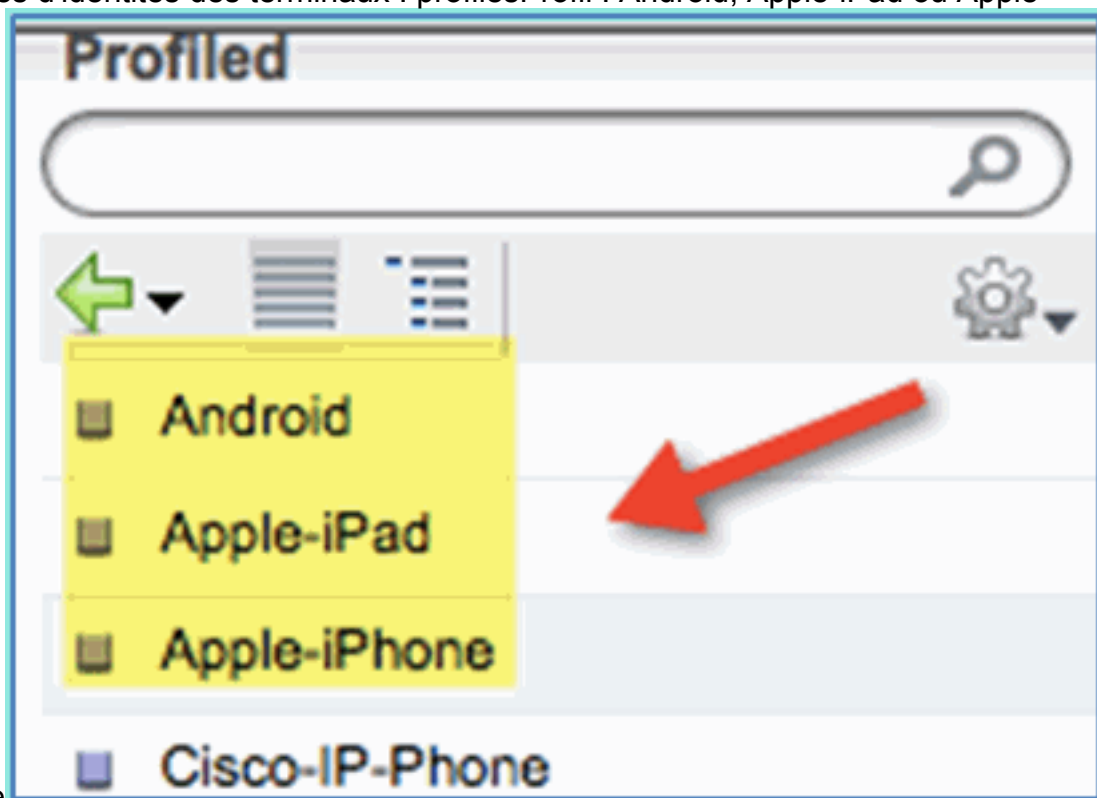
1. Accédez à ISE > Policy > Authorization.
2. Ajoutez/insérez une nouvelle règle au-dessus de la politique/ligne de correction de position.



3. Entrez les valeurs suivantes pour cette stratégie :Nom de la règle : EmployéGroupes d'identités (développer) : Groupes d'identités des terminaux

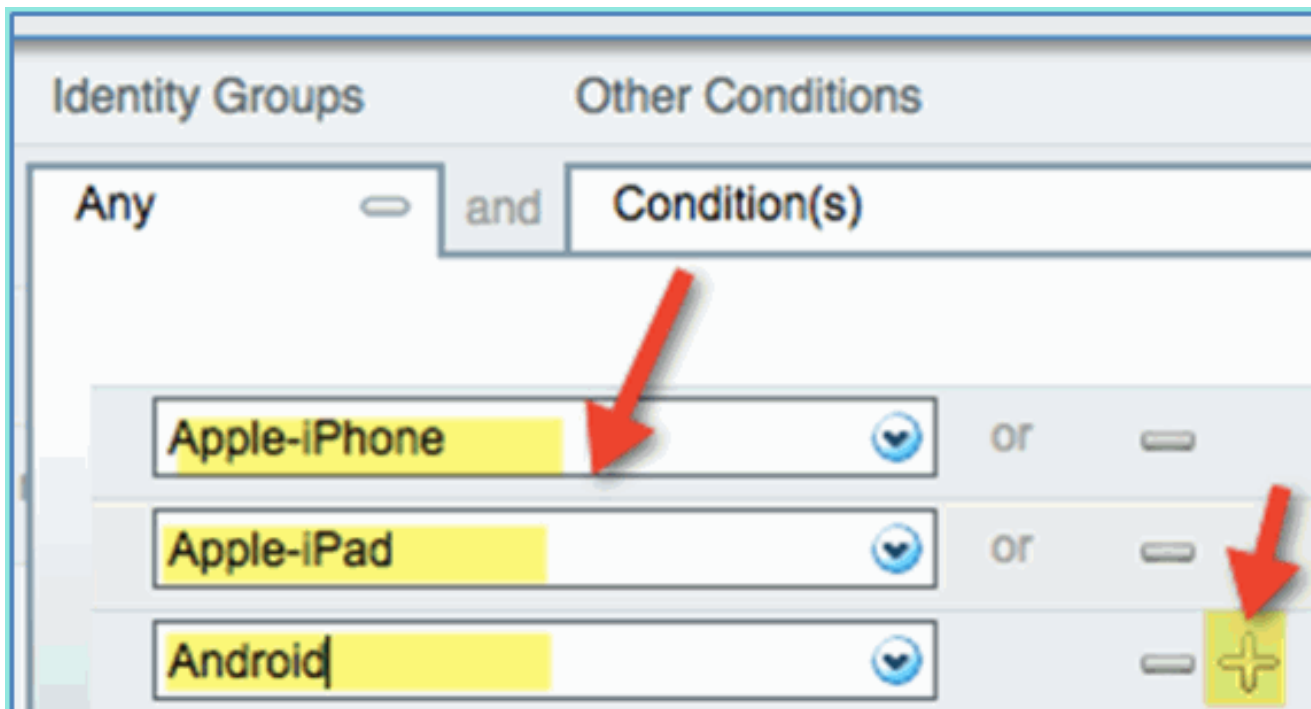


Groupes d'identités des terminaux : profilés Profil : Android, Apple-iPad ou Apple-

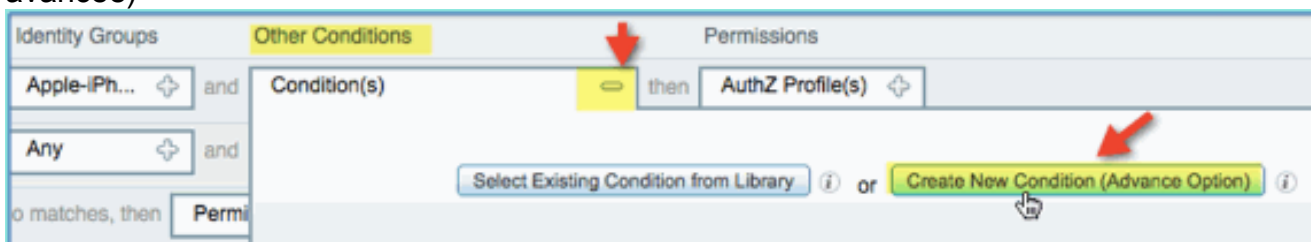


iPhone

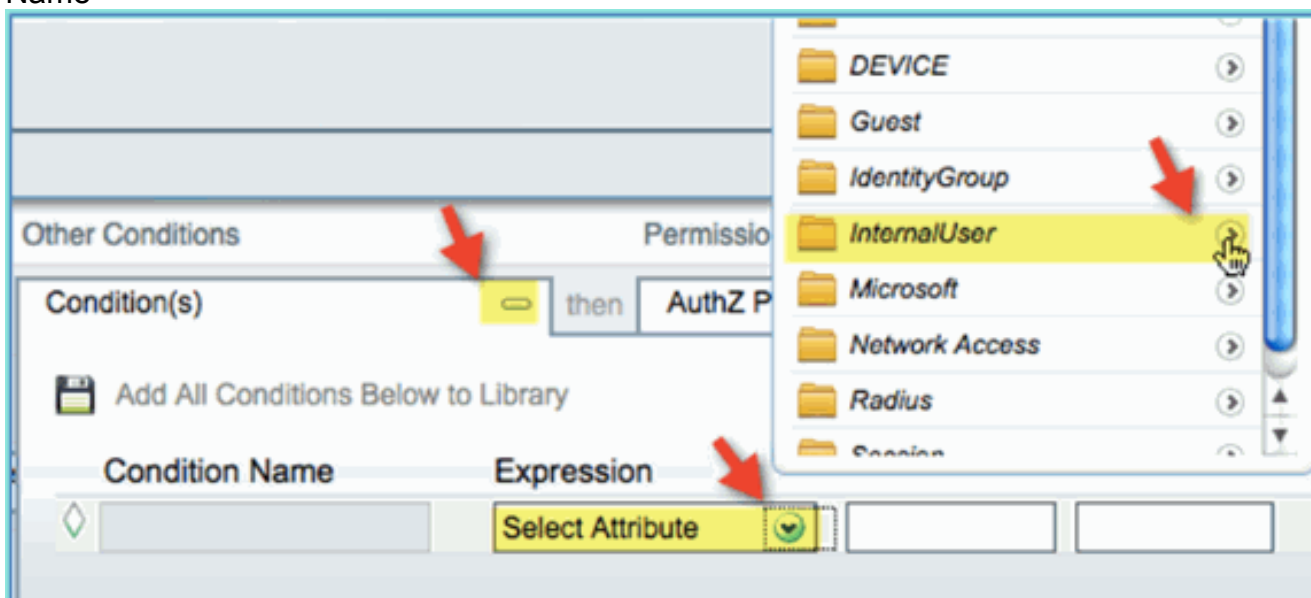
4. Afin de spécifier des types de périphériques supplémentaires, cliquez sur le + et ajoutez d'autres périphériques (si nécessaire) : Groupes d'identités des terminaux : profilés Profil : Android, Apple-iPad ou Apple-iPhone



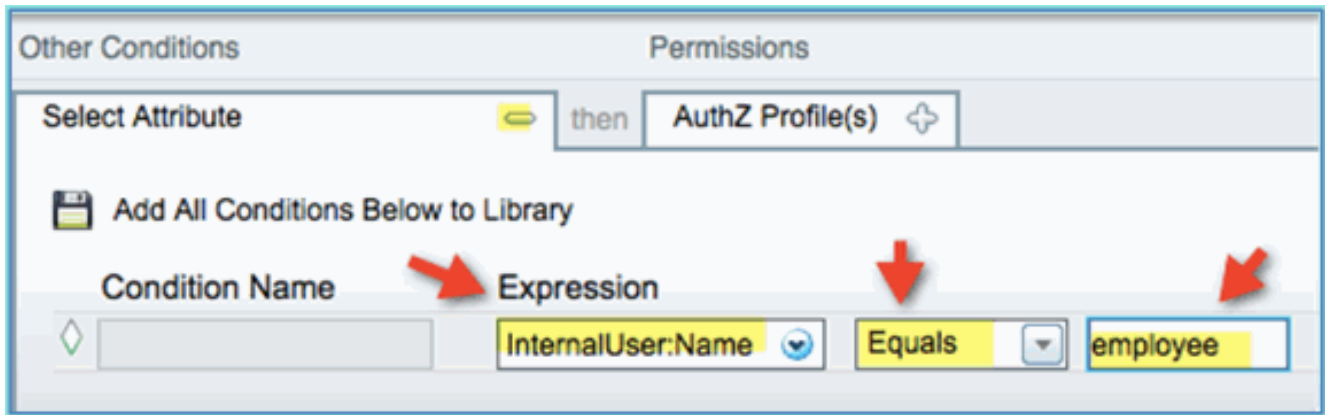
5. Spécifiez les valeurs d'autorisation suivantes pour cette stratégie :Autres conditions (développer) : Créer une nouvelle condition (option avancée)



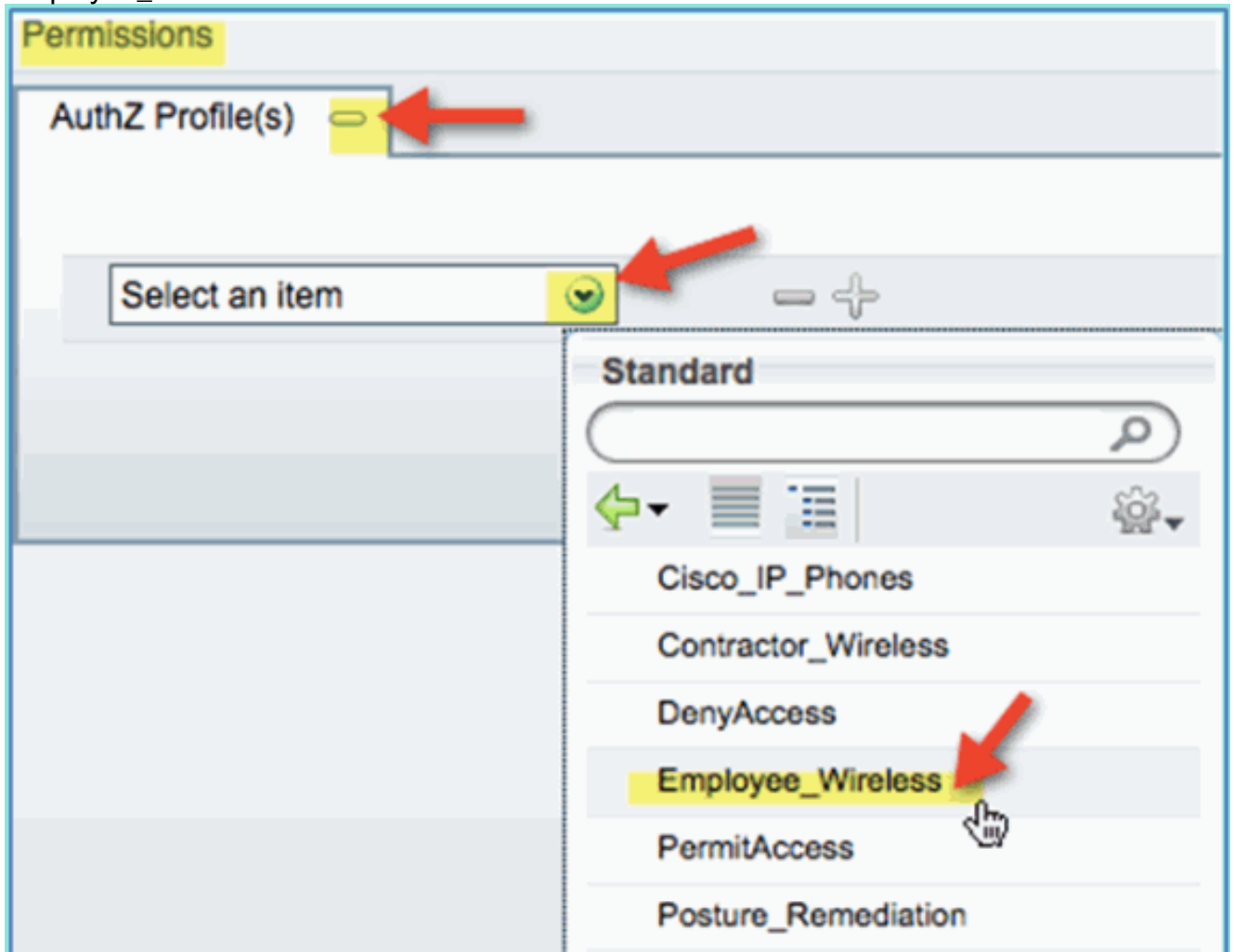
Condition > Expression (de la liste) : InternalUser > Name



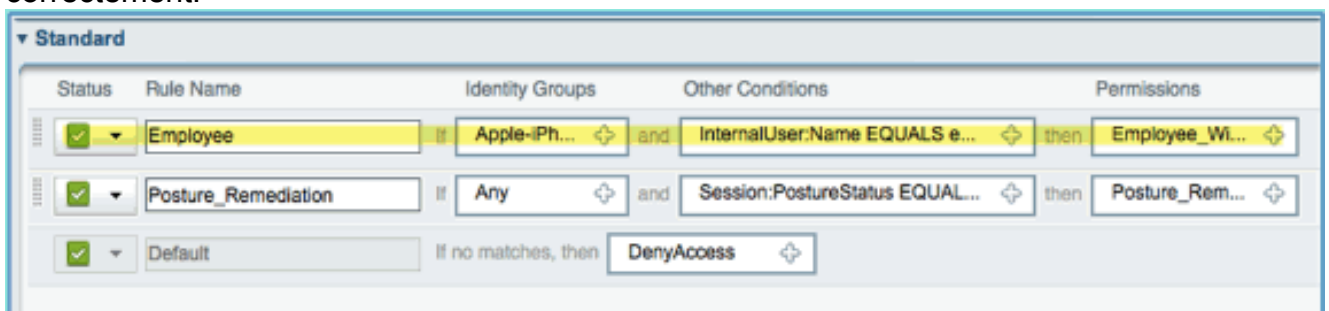
InternalUser > Nom : employé



6. Ajouter une condition pour la session de posture Conforme :Autorisations > Profils > Standard :
Employee_Wireless

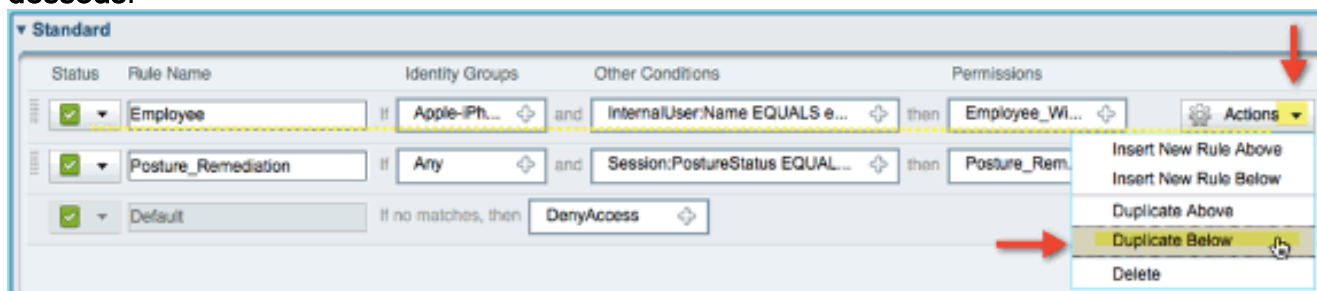


7. Cliquez sur **Save**. Vérifiez que la stratégie a été ajoutée correctement.

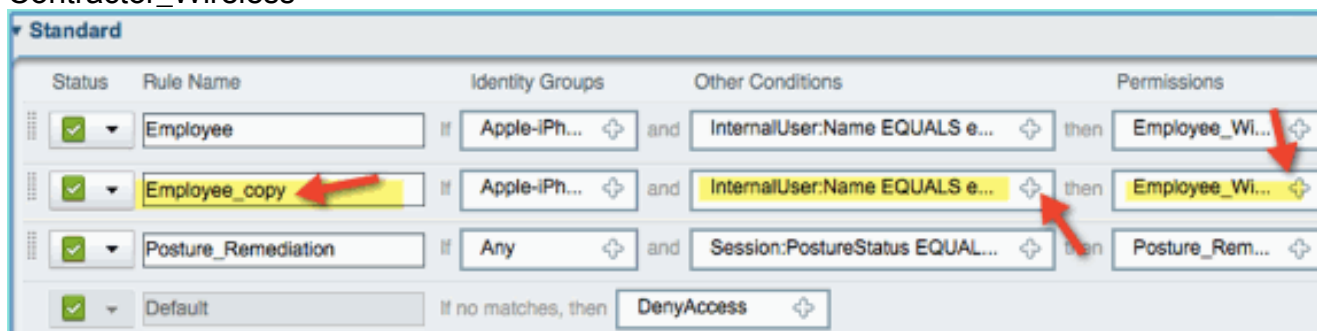


8. Poursuivez en ajoutant la politique de l'entrepreneur. Dans ce document, la stratégie

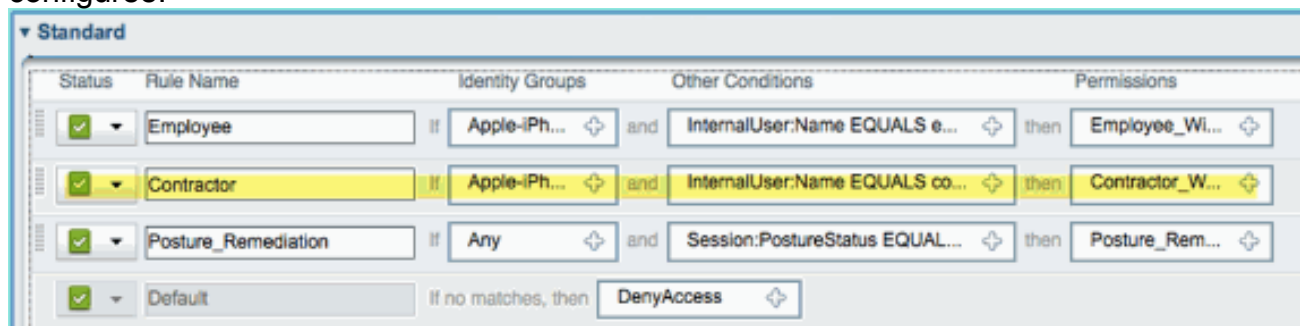
précédente est dupliquée afin d'accélérer le processus (ou, vous pouvez configurer manuellement les bonnes pratiques). Dans la politique Employé > Actions, cliquez sur **Dupliquer ci-dessous**.



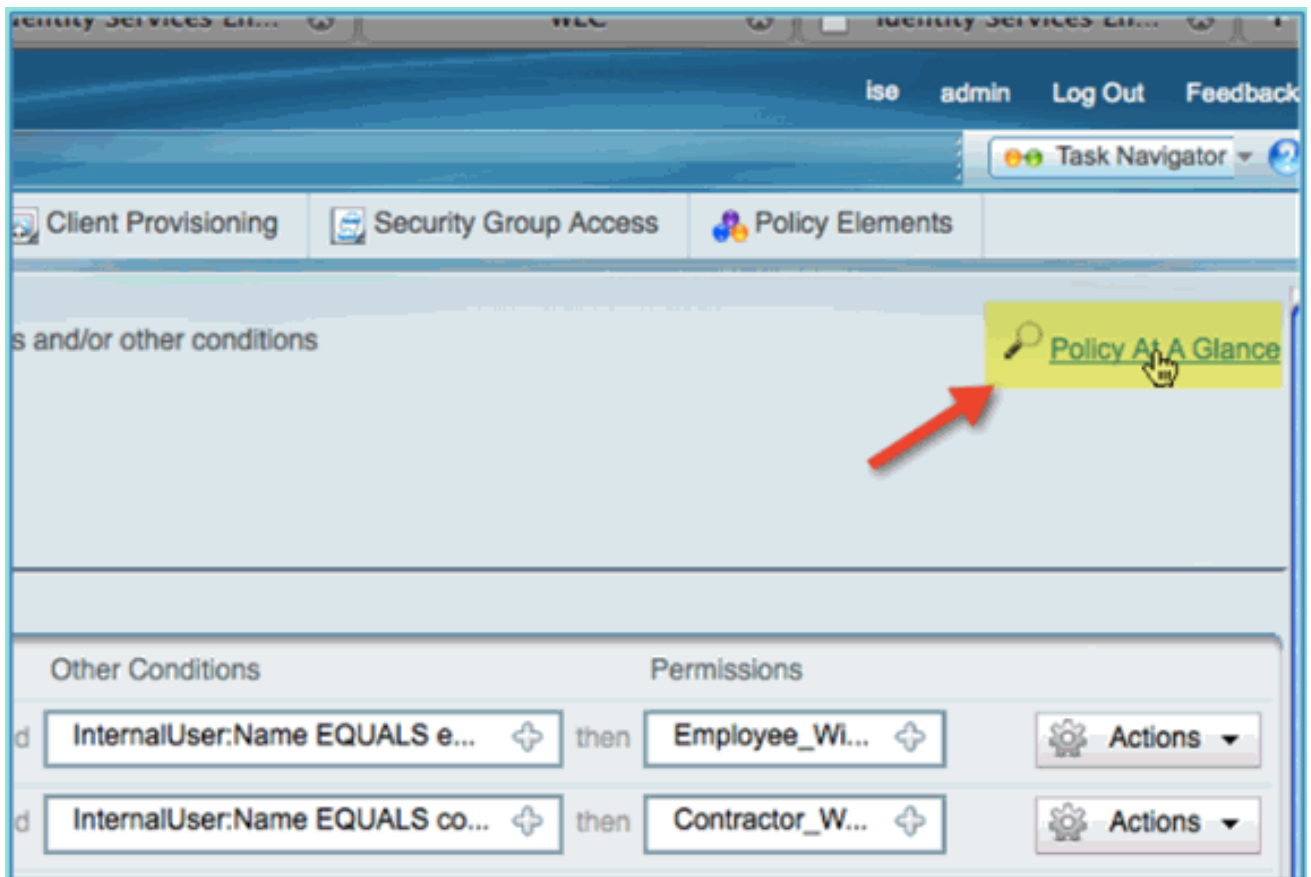
- Modifiez les champs suivants pour cette stratégie (copie dupliquée) : Nom de la règle : EntrepreneurAutres conditions > Utilisateur interne > Nom : entrepreneurAutorisations : Contractor_Wireless



- Cliquez sur **Save**. Vérifiez que la copie dupliquée précédente (ou la nouvelle stratégie) est correctement configurée.



- Pour afficher un aperçu des stratégies, cliquez sur **Policy-at-a-Glance (Aperçu de la stratégie)**.



La vue Policy at A Glance fournit un résumé consolidé et des politiques faciles à voir.

Authorization Policy At A Glance				
First Matched Rule Applies				
Exceptions				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
No data available				
Standard				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
<input checked="" type="checkbox"/> Enabled	Employee	Android OR Apple-iPad OR Apple-iphone	InternalUser:Name EQUALS employee	Employee_Wireless
<input checked="" type="checkbox"/> Enabled	Contractor	Android OR Apple-iPad OR Apple-iphone	InternalUser:Name EQUALS contractor	Contractor_Wireless
<input checked="" type="checkbox"/> Enabled	Posture_Remediation	Any	Session:PostureStatus EQUALS Unknown	Posture_Remediation
<input checked="" type="checkbox"/> Enabled	Default	Any		DenyAccess

Test de CoA pour l'accès différencié

Une fois les profils d'autorisation et les politiques préparés pour différencier l'accès, il est temps de les tester. Avec un seul WLAN sécurisé, un employé se verra attribuer le VLAN employé et un sous-traitant sera affecté au VLAN sous-traitant. Un iPhone/iPad Apple est utilisé dans les exemples suivants.

Procédez comme suit :

1. Connectez-vous au réseau local sans fil sécurisé (POD1x) avec l'appareil mobile et utilisez les informations d'identification suivantes :
 Nom d'utilisateur : employee
 Mot de passe : XXXXX



2. Cliquez sur **Joindre**. Vérifiez que le VLAN 11 (VLAN employé) est attribué à l'employé.



3. Cliquez sur **Oublier ce réseau**. Confirmez en cliquant sur



Oublier.

4. Accédez au WLC et supprimez les connexions client existantes (si la même chose a été utilisée dans les étapes précédentes). Accédez à **Monitor > Clients > MAC address**, puis cliquez sur **Remove**.

Monitor

Clients

Summary

Current Filter

▶ Access Points

▶ Cisco CleanAir

▶ Statistics

▶ CDP

▶ Rogues

Clients

Multicast

Client MAC Addr

[44:2a:60:f7:3a:4a](#)

[5c:59:48:40:82:8d](#)

Status	Auth	Port	WGB
--------	------	------	-----

Associated	Yes	1	No
------------	-----	---	----

Associated	No	1	
------------	----	---	--

LinkTest

Disable

Remove

802.11aTSM

802.11b/gTSM

5. Une autre façon sûre d'effacer les sessions client précédentes est de désactiver/activer le WLAN. Accédez à **WLC > WLANs > WLAN**, puis cliquez sur le WLAN à modifier. Décochez la case **Activé > Appliquer** (pour désactiver). Cochez la case **Enabled > Apply** (pour réactiver).



6. Revenez à l'appareil mobile. Reconnectez-vous au même WLAN avec les informations d'identification suivantes :
Nom d'utilisateur : entrepreneur
Mot de passe :

Enter the password for "pod1x"

Cancel **Enter Password**

Username contractor ←

Password ●●●●●●●● | ←

Mode Automatic >

1 2 3 4 5 6 7 8 9 0

XXXX

7. Cliquez sur **Joindre**. Vérifiez que le VLAN 12 (VLAN entrepreneur/invité) est attribué à l'utilisateur du sous-



traitant.

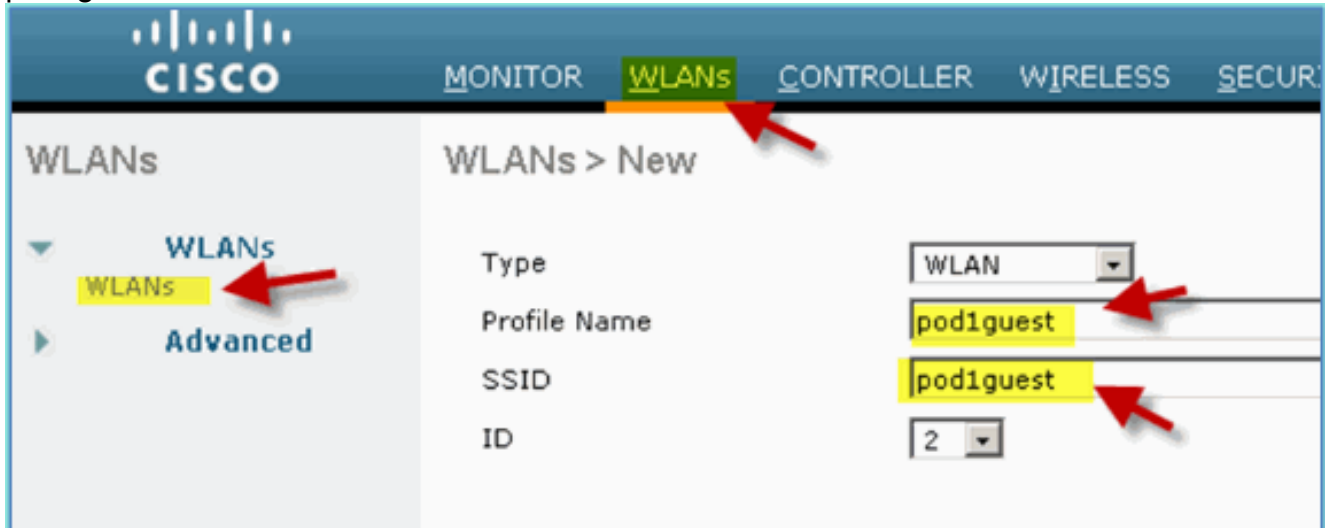
8. Vous pouvez consulter la vue du journal en temps réel d'ISE dans **ISE > Surveillance > Autorisations**. Vous devriez voir des utilisateurs individuels (employé, sous-traitant) obtenir des profils d'autorisation différenciés (Employee_Wireless vs Contractor_Wireless) dans différents VLAN.

Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Aug 02,11 03:40:18.331 PM	✓		employee	5C:59:48:40:82:80		wic		Employee_Wireless
Aug 02,11 03:36:33.663 PM	✓		contractor	5C:59:48:40:82:80		wic		Contractor_Wireless

[WLAN invité WLC](#)

Complétez ces étapes afin d'ajouter un WLAN invité pour permettre aux invités d'accéder au portail des invités du sponsor ISE :

1. À partir du WLC, naviguez vers **WLANs > WLANs > Add New**.
2. Saisissez les informations suivantes pour le nouveau WLAN invité :
Nom du profil :
pod1guestSSID :
pod1guest



3. Cliquez sur **Apply**.
4. Sous l'onglet WLAN invité > General, saisissez les informations suivantes :
État :
Désactivé
Interface/groupe d'interfaces :
Invité

MONITOR **WLANs** CONTROLLER WIRELESS SECUR

WLANs > Edit 'pod1guest'

General Security QoS Advanced

Profile Name pod1guest

Type WLAN

SSID pod1guest

Status Enabled

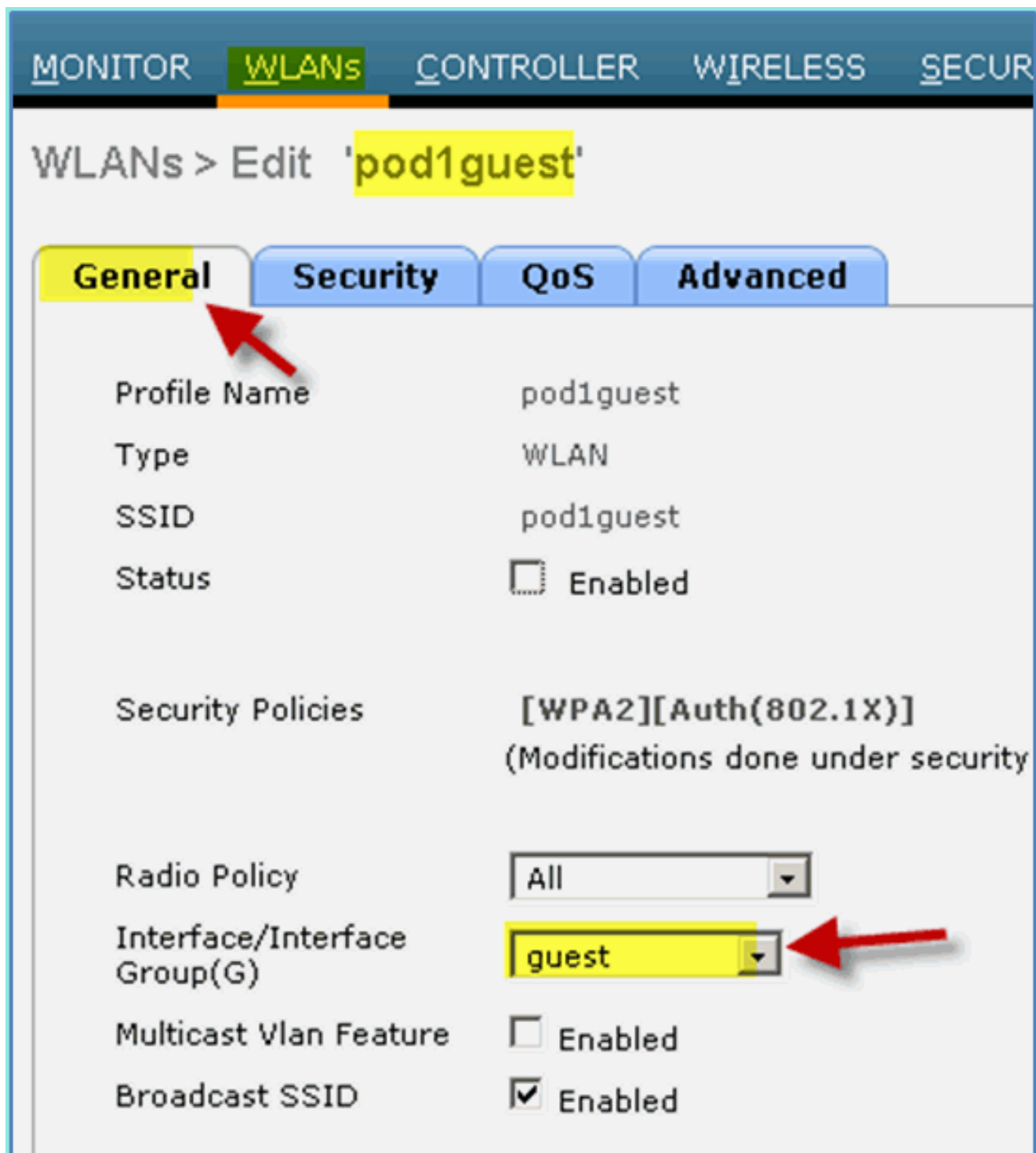
Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security)

Radio Policy All

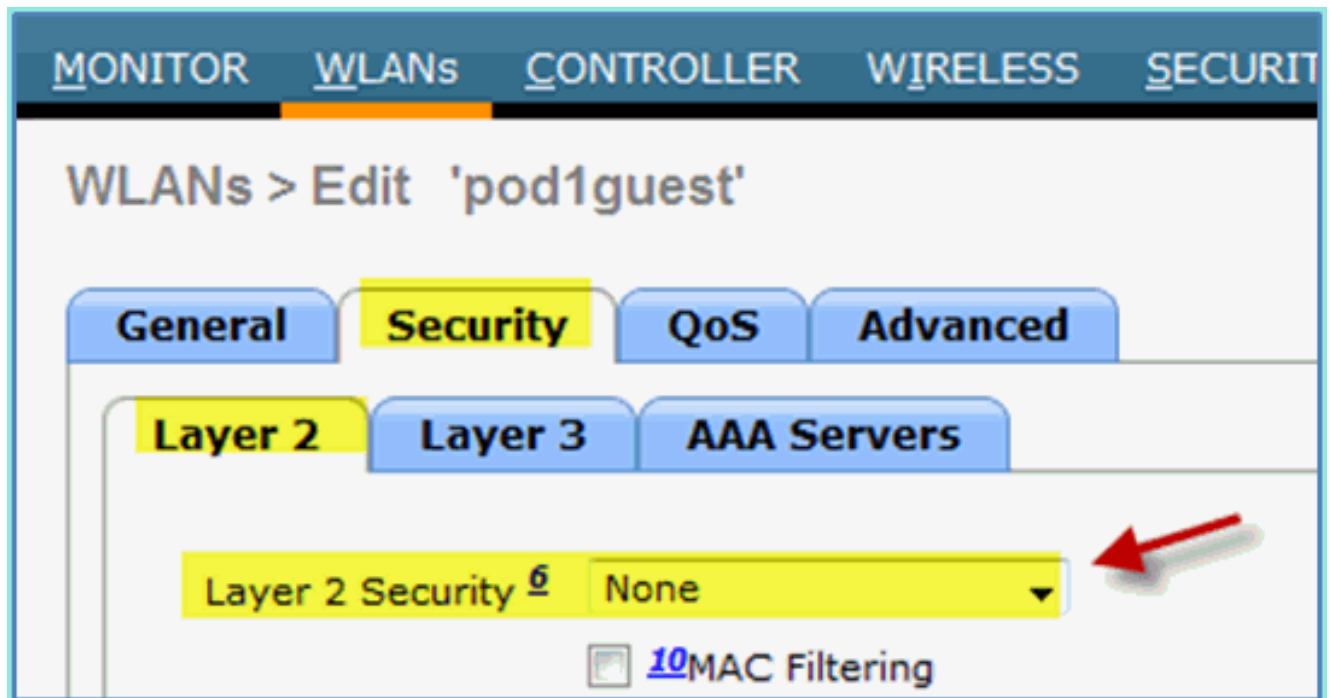
Interface/Interface Group(G) **guest**

Multicast Vlan Feature Enabled

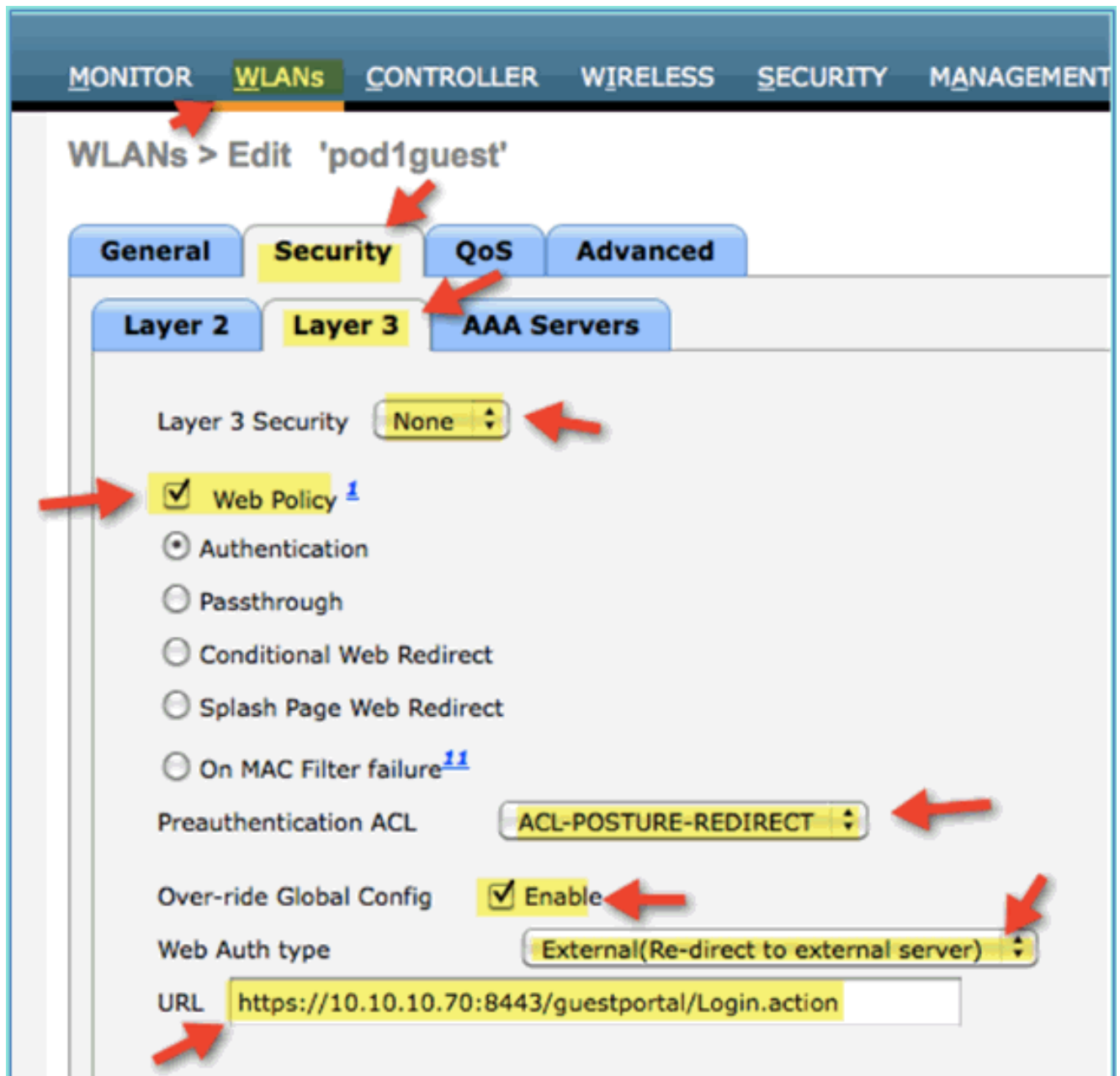
Broadcast SSID Enabled



5. Accédez à WLAN invité > Security > Layer2 et saisissez les informations suivantes : Sécurité de couche 2 : aucune



6. Accédez à l'onglet **WLAN** invité > **Security** > **Layer3** et entrez les éléments suivants : Sécurité de couche 3 : aucune
Stratégie Web : activée
Sous-valeur de stratégie Web : authentification
ACL de pré-authentification : ACL-POSTURE-REDIRECT
Type d'authentification Web : Externe (redirection vers un serveur externe)
URL : <https://10.10.10.70:8443/guestportal/Login.action>



7. Cliquez sur **Apply**.

8. Veillez à enregistrer la configuration WLC.

Test du WLAN invité et du portail invité

Vous pouvez maintenant tester la configuration du réseau local sans fil invité. Il doit rediriger les invités vers le portail des invités ISE.

Procédez comme suit :

1. À partir d'un appareil iOS tel qu'un iPhone, accédez à **Réseaux Wi-Fi > Activer**. Sélectionnez ensuite le réseau invité

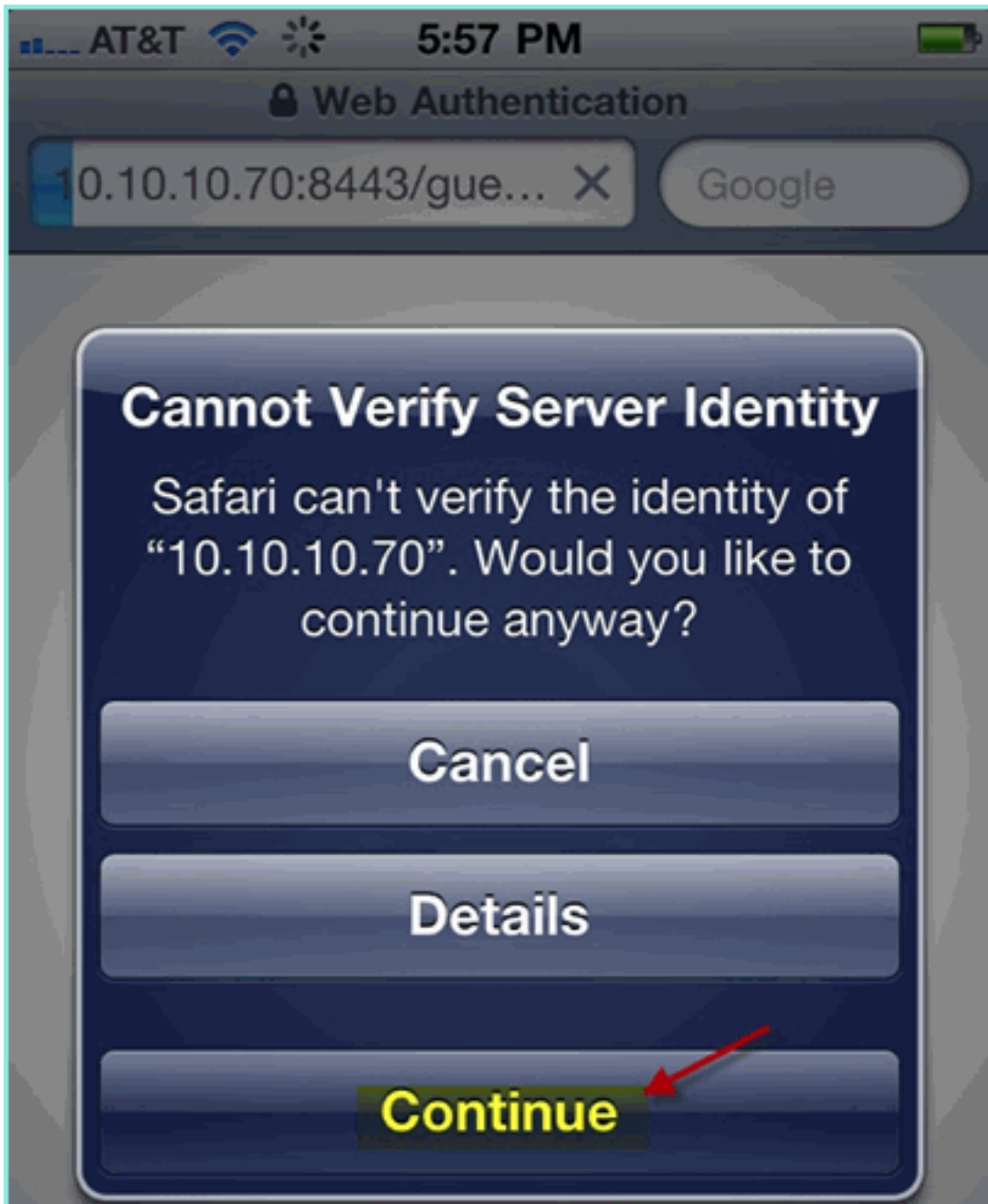


POD.

2. Votre périphérique iOS doit afficher une adresse IP valide du VLAN invité (10.10.12.0/24).



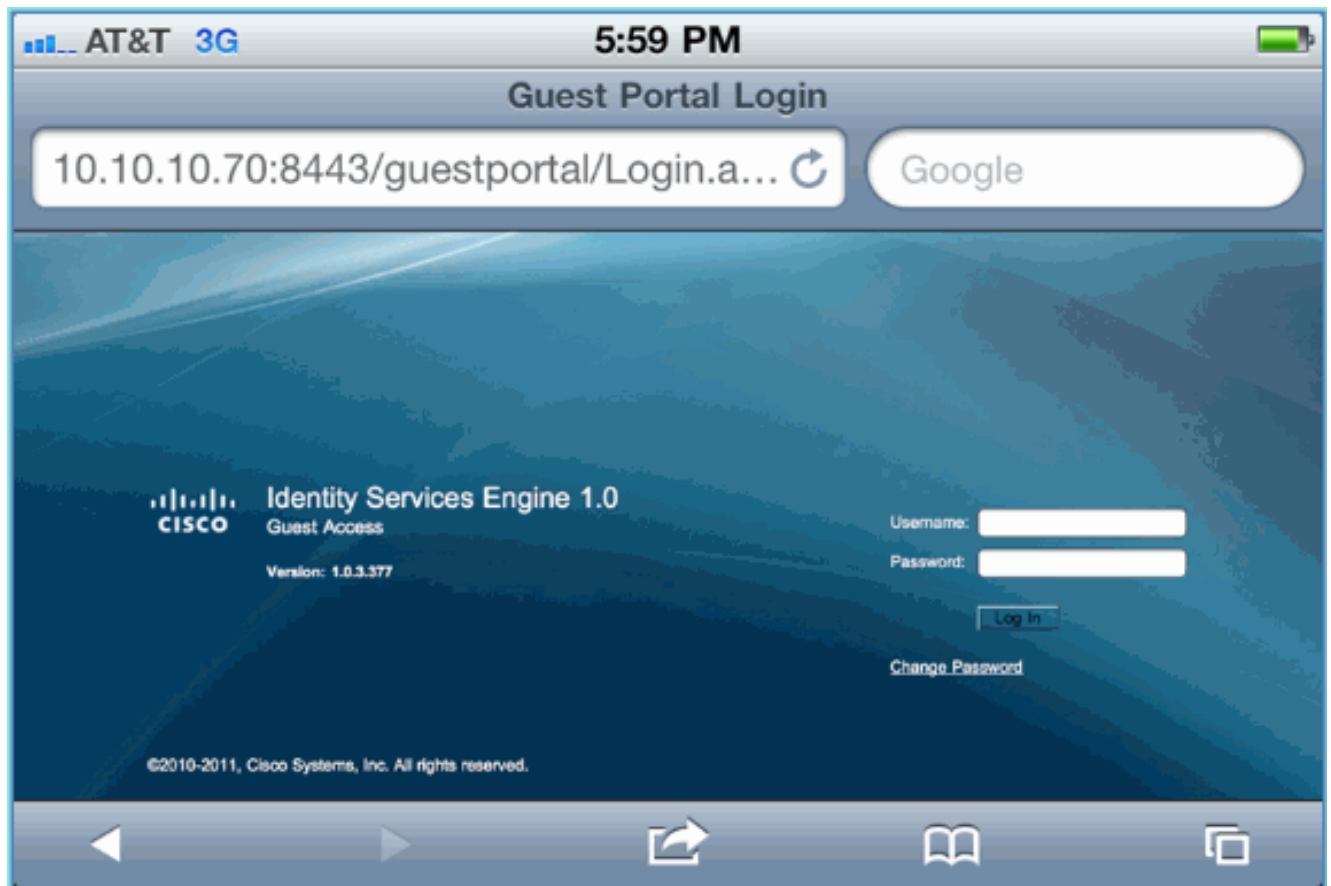
3. Ouvrez le navigateur Safari et connectez-vous à :URL : <http://10.10.10.10> Une redirection d'authentification Web apparaît.
4. Cliquez sur **Continue** jusqu'à ce que vous arriviez à la page ISE Guest



Portal.

L'exempl

e de capture d'écran suivant montre l'appareil iOS sur une connexion Guest Portal. Cela confirme que la configuration correcte du WLAN et du portail invité ISE est active.

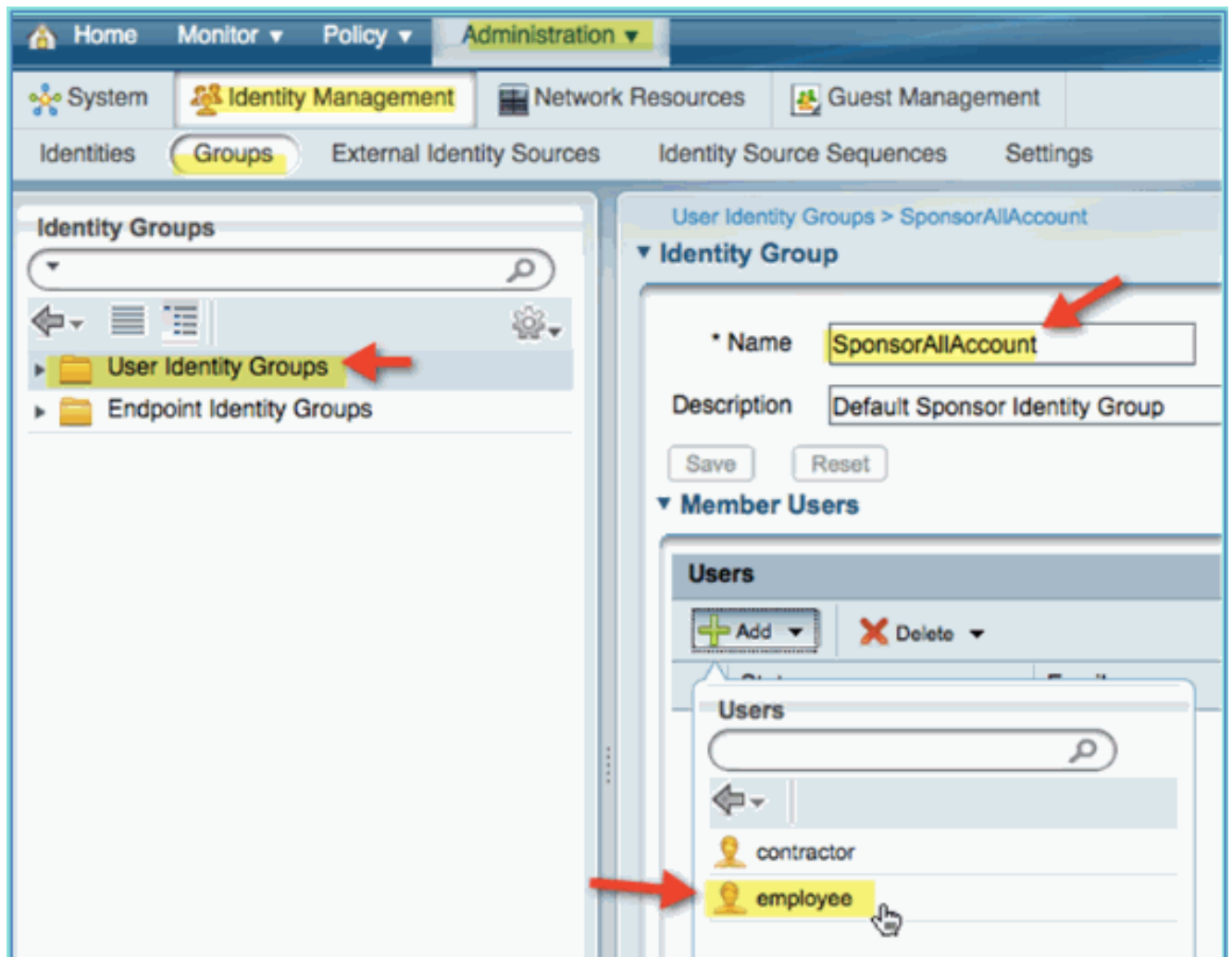


[Accès invité parrainé sans fil ISE](#)

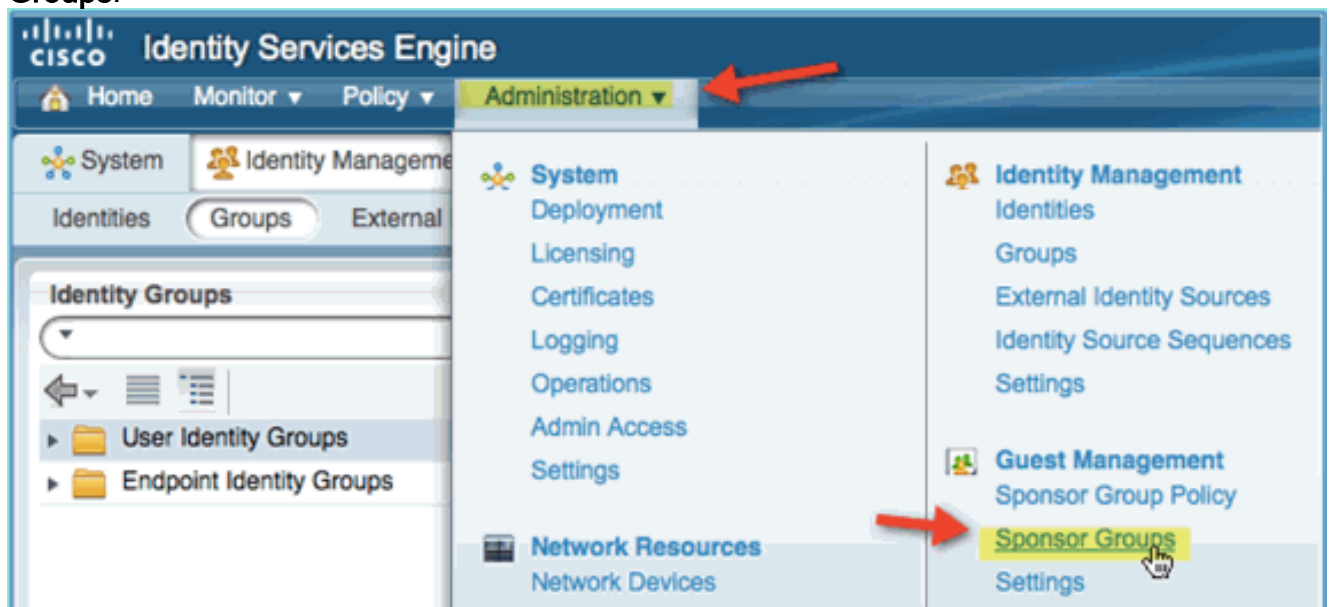
ISE peut être configuré pour autoriser le parrainage d'invités. Dans ce cas, vous allez configurer des stratégies d'invité ISE pour autoriser les utilisateurs internes ou de domaine AD (s'ils sont intégrés) à parrainer l'accès invité. Vous configurerez également ISE pour permettre aux sponsors d'afficher le mot de passe invité (facultatif), ce qui est utile pour ces travaux pratiques.

Procédez comme suit :

1. Ajoutez l'utilisateur employé au groupe `CompteTousSponsor`. Pour ce faire, vous pouvez accéder directement au groupe ou modifier l'utilisateur et attribuer un groupe. Pour cet exemple, accédez à **Administration > Identity Management > Groups > User Identity Groups**. Cliquez ensuite sur **SponsorAllAccount** et ajoutez l'utilisateur employé.



2. Accédez à **Administration > Guest Management > Sponsor Groups**.



3. Cliquez sur **Modifier**, puis choisissez **SponsorAllAccounts**.





CISCO Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy **Sponsor Groups** Settings

Guest Sponsor Groups

 Edit  Add  Delete  Filter

<input type="checkbox"/>	Sponsor Group Name	Description
<input checked="" type="checkbox"/>	SponsorAllAccounts	Default SponsorGroup
<input type="checkbox"/>	SponsorGroupGrpAccounts	Default SponsorGroup

4. Sélectionnez les niveaux d'autorisation et définissez les paramètres suivants :Afficher le mot de passe invité :
Oui

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb trail is "Sponsor Group List > SponsorAllAccounts". The "Authorization Levels" tab is selected and highlighted in green. A red arrow points to this tab. Below the tabs, a list of authorization settings is shown. The "View Guest Password" setting is highlighted in yellow, with a red arrow pointing to its "Yes" value. Other settings include "Allow Login", "Create Accounts", "Create Bulk Accounts", "Create Random Accounts", "Import CSV", "Send Email", "Send SMS", "Allow Printing Guest Details", "View/Edit Accounts", and "Suspend/Reinstate Accounts". At the bottom, there are "Save" and "Reset" buttons.

Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	No
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)

5. Cliquez sur **Save** afin de terminer cette tâche.

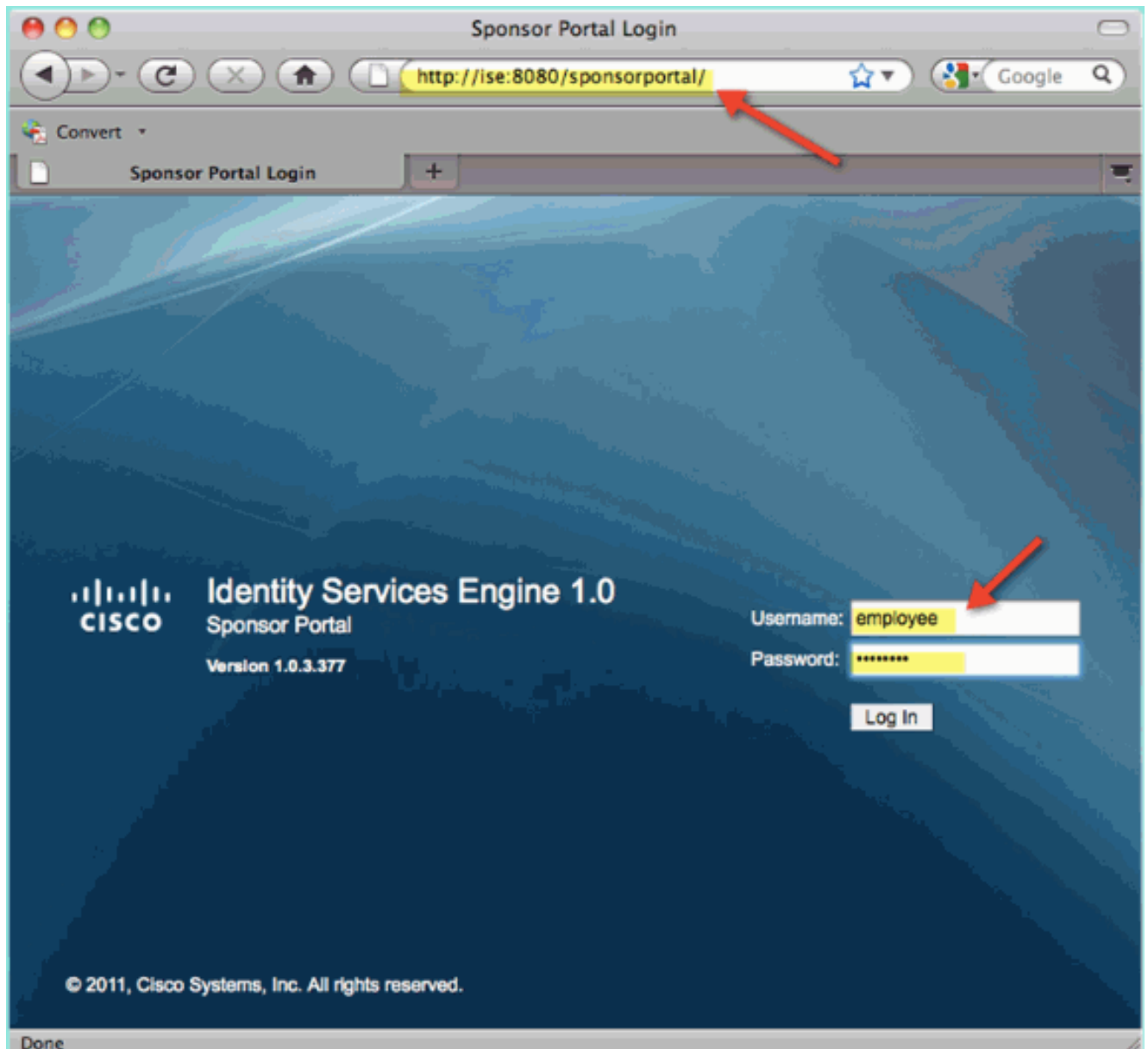
Invité Sponsorisant

Vous avez précédemment configuré la stratégie et les groupes d'invités appropriés pour permettre aux utilisateurs du domaine AD de parrainer des invités temporaires. Ensuite, vous accédez au portail des sponsors et créez un accès invité temporaire.

Procédez comme suit :

1. À partir d'un navigateur, accédez à l'une des URL suivantes : <http://<ip>:8080/sponsor-portal/> ou <https://<ip>:8443/sponsor-portal/>. Connectez-vous ensuite à l'aide des commandes suivantes : Nom d'utilisateur : aduser (Active Directory), employee (Internal

User)Mot de passe :
XXXX



2. Sur la page Sponsor, cliquez sur **Create Single Guest User Account**.

CISCO Sponsor Portal

▼ Sponsor

- Home
- Settings Customization

▼ Account Management

- View Guest Accounts
- Create Multiple Accounts

Sponsor Portal: Getting Started

- [View All Guest User Accounts](#)
- [Create Single Guest User Account](#)**
- [Create Multiple Guest User Accounts](#)

3. Pour un invité temporaire, ajoutez ce qui suit :
- Prénom : obligatoire (par exemple, Sam)
 - Nom : Obligatoire (par exemple, Jones)
 - Rôle du groupe : Invité
 - Profil horaire : DefaultOneHour
 - Fuseau horaire : Tout/Par défaut

Sponsor Portal

Account Management > [View All Guest Accounts](#) > Create Guest Account

Create Guest Account

First Name:

Last Name:

Email Address:

Phone Number:

Company:

Optional Data 1:

Optional Data 2:

Optional Data 3:

Optional Data 4:

Optional Data 5:

Group Role:

Time Profile:

Timezone:

⚙ = Required fields

4. Cliquez sur Submit.
5. Un compte invité est créé en fonction de votre entrée précédente. Notez que le mot de passe est visible (à partir de l'exercice précédent) par opposition au hachage ***.
6. Laissez cette fenêtre ouverte et affichez le nom d'utilisateur et le mot de passe de l'invité. Vous les utiliserez pour tester la connexion au portail invité (suivant).



Successfully Created Guest Account **siam0002**

Username: **siam0002** ←
Password: **5_5g6d7Kx** ←
First Name: Sam ←
Last Name: iAm
Email Address:
Phone Number:
Company:
Status: AWAITING INITIAL LOGIN
Suspended: false
Optional Data 1:
Optional Data 2:
Optional Data 3:
Optional Data 4:
Optional Data 5:
Group Role: Guest
Time Profile: DefaultOneHour

Timezone: EST
Account Start Date: 2011-07-15 13:56:04 EST
Account Expiration Date: 2011-07-15 14:56:04 EST

Email

Print

Create Another Account

View All Accounts

Test de l'accès au portail invité

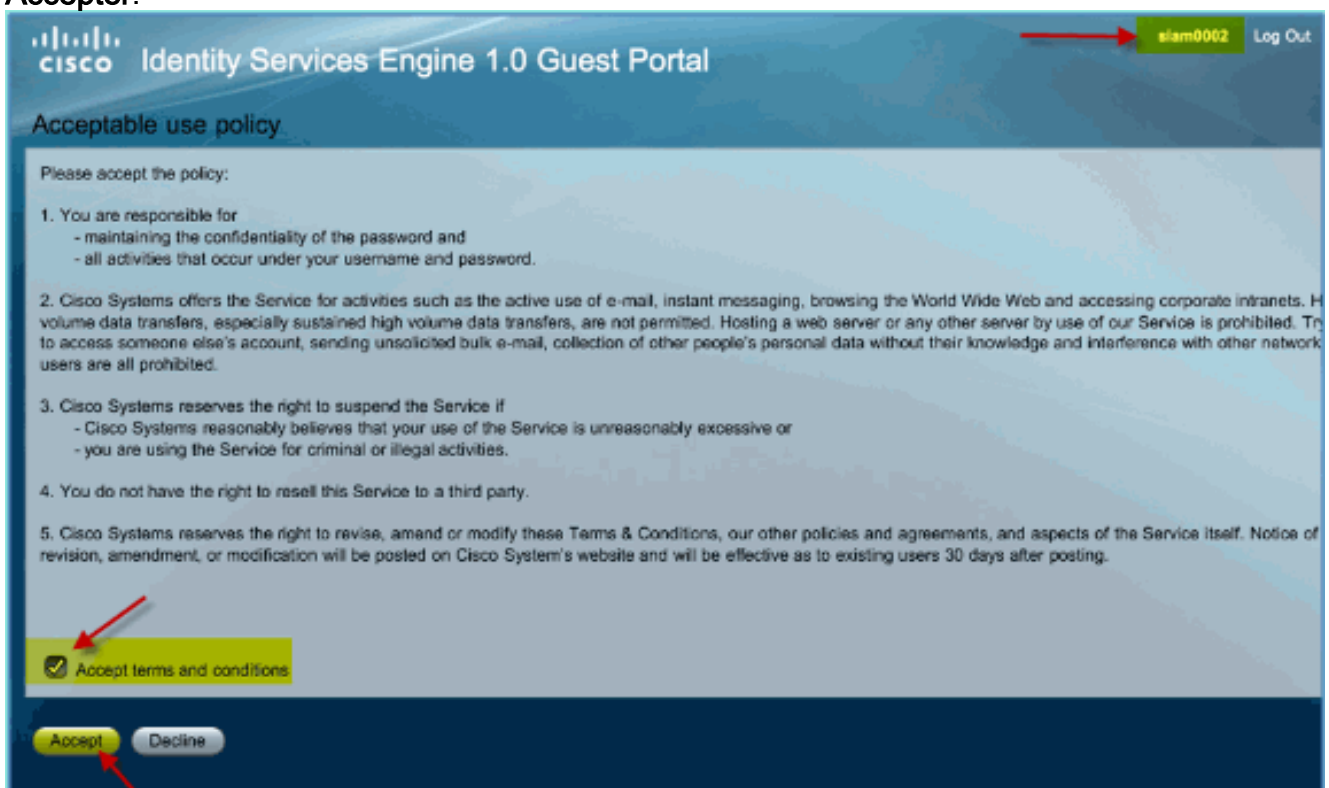
Avec le nouveau compte invité créé par un utilisateur/sponsor AD, il est temps de tester le portail et l'accès invité.

Procédez comme suit :

1. Sur un périphérique préféré (dans ce cas un iOS/iPad Apple), connectez-vous au SSID du Pod Guest et vérifiez l'adresse IP/la connectivité.
2. Utilisez le navigateur et essayez d'accéder à <http://www.Vous> êtes redirigé vers la page Connexion au portail invité.



3. Connectez-vous à l'aide du compte invité créé dans l'exercice précédent. En cas de succès, la page Politique d'utilisation acceptable s'affiche.
4. Cochez **Accepter les conditions générales**, puis cliquez sur **Accepter**.



L'URL d'origine est terminée et le point de terminaison est autorisé à accéder en tant qu'invité.

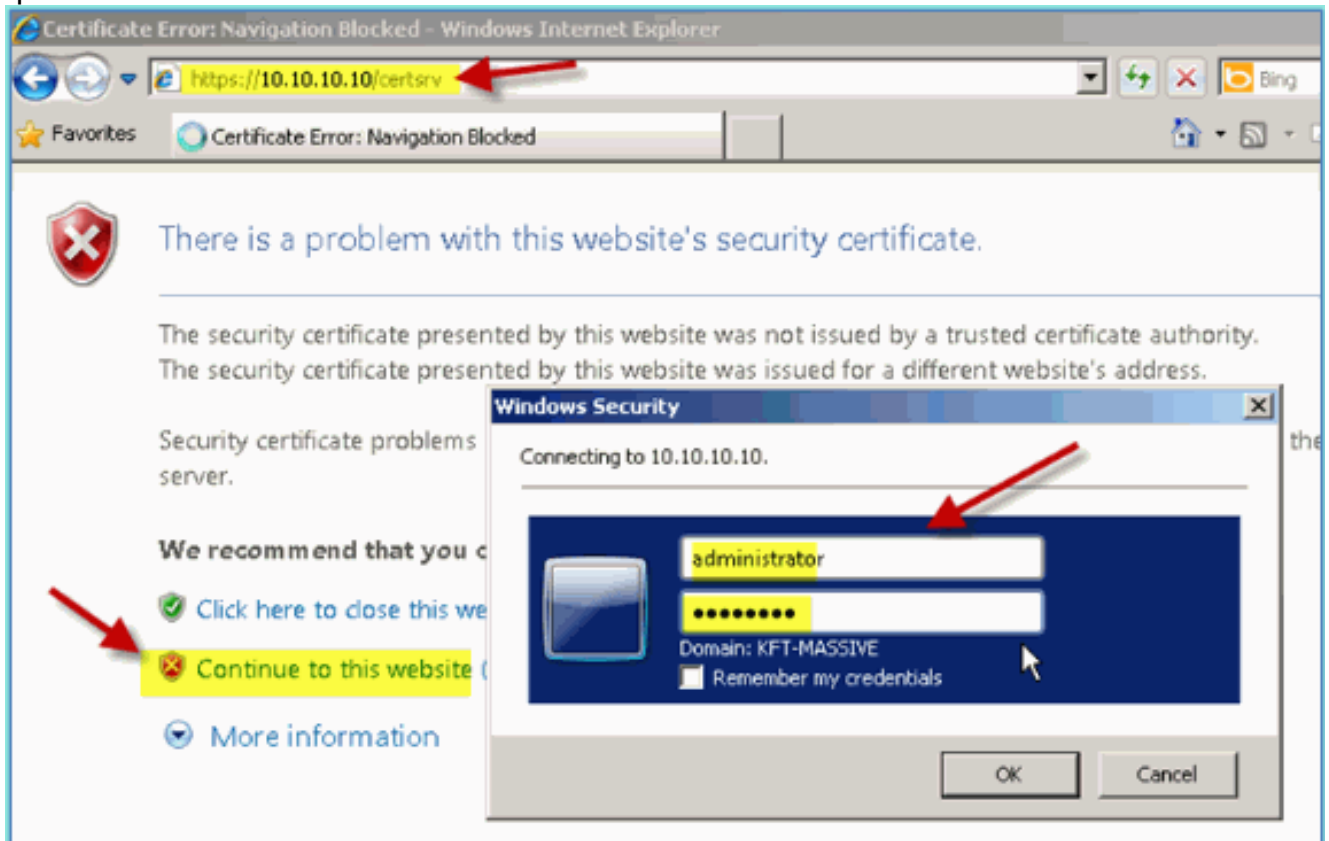
Configuration du certificat

Afin de sécuriser les communications avec ISE, déterminez si la communication est liée à l'authentification ou à la gestion ISE. Par exemple, pour la configuration à l'aide de l'interface utilisateur Web ISE, les certificats X.509 et les chaînes de certificats de confiance doivent être configurés pour activer le chiffrement asymétrique.

Procédez comme suit :

1. À partir de votre ordinateur connecté par câble, ouvrez une fenêtre de navigateur vers <https://AD/certsrv>. **Remarque** : utilisez le protocole HTTP sécurisé. **Remarque** : utilisez Mozilla Firefox ou MS Internet Explorer pour accéder à ISE.

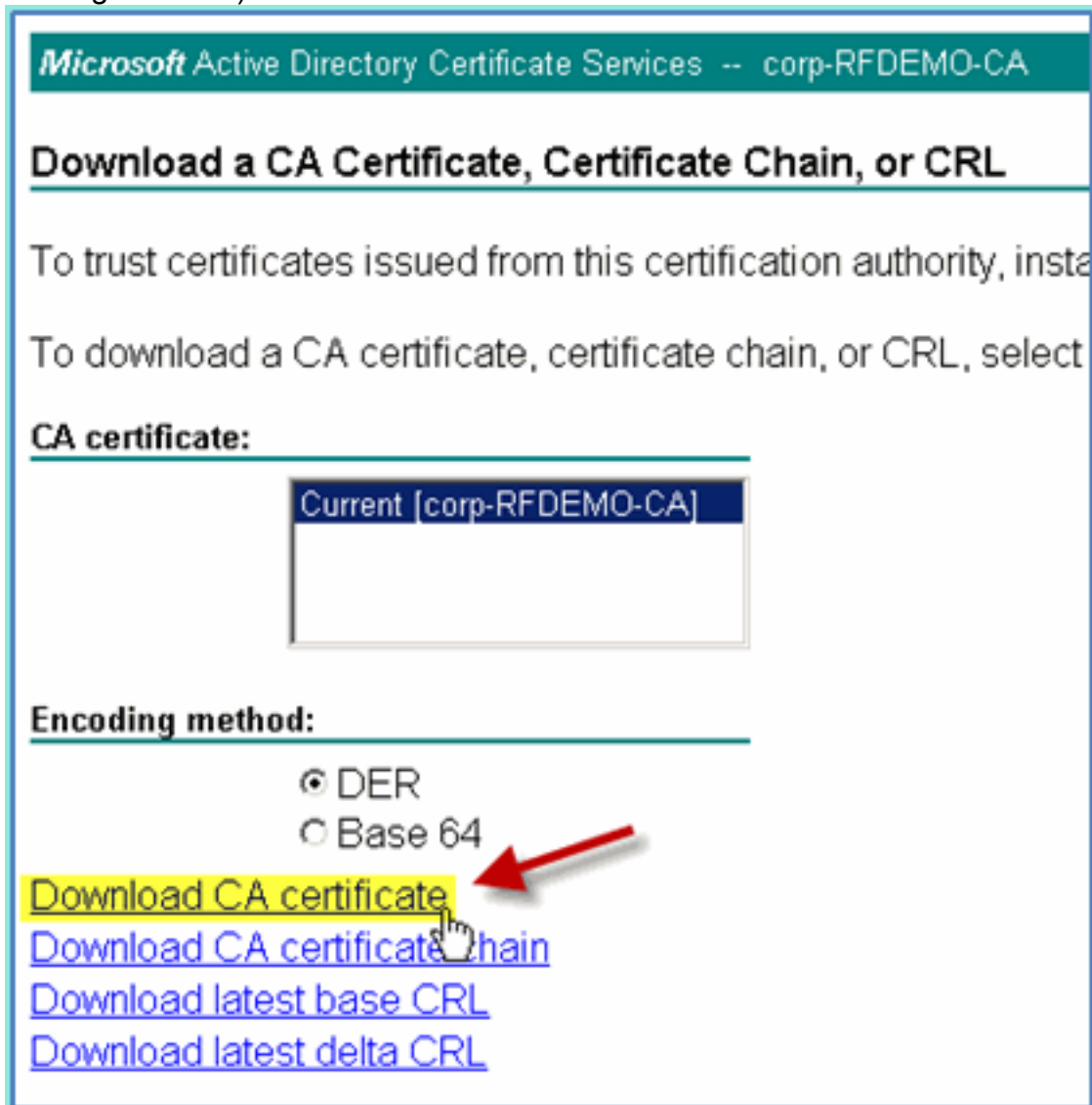
2. Connectez-vous en tant qu'administrateur/Cisco123.



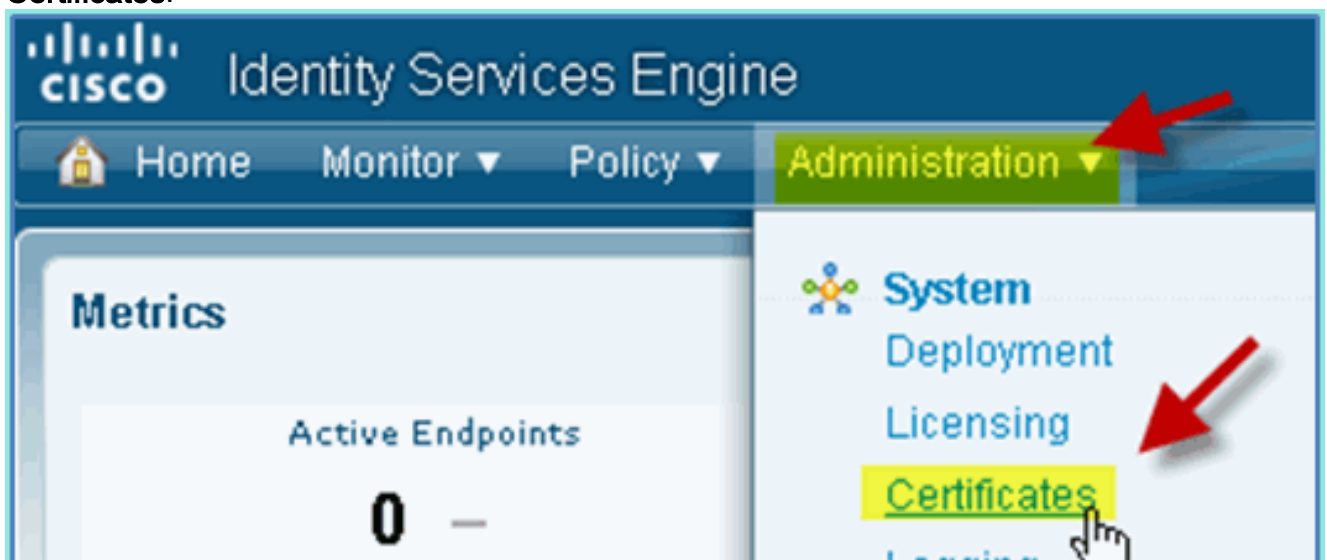
3. Cliquez sur **Download a CA certificate, certificate chain ou CRL**.



4. Cliquez sur **Download CA certificate** et enregistrez-le (notez l'emplacement d'enregistrement).

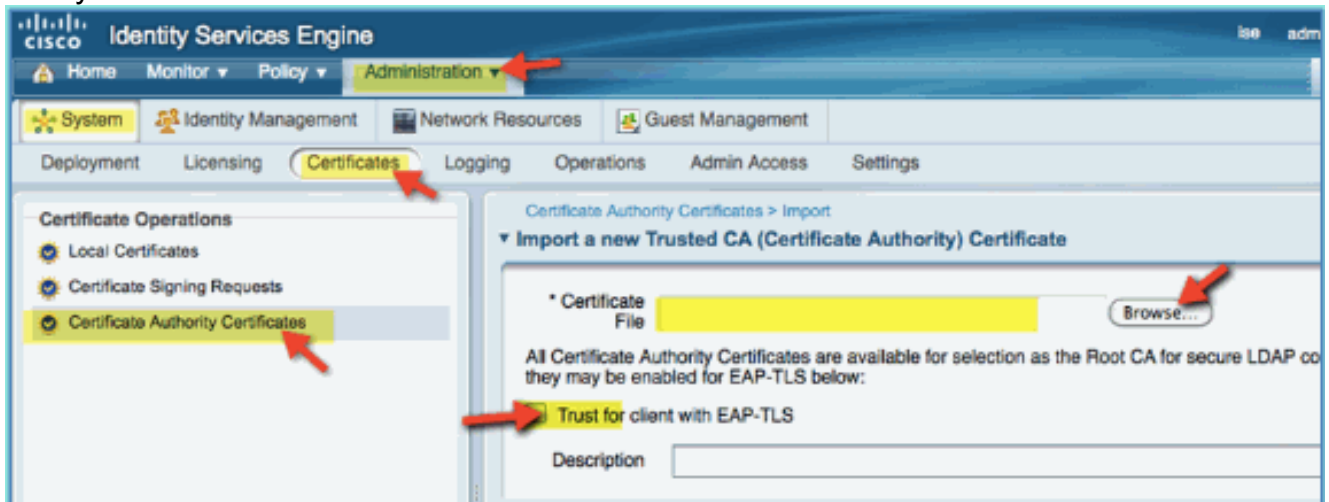


5. Ouvrez une fenêtre de navigateur sur <https://<Pod-ISE>>.
6. Accédez à **Administration > System > Certificates > Certificates Authority Certificates**.

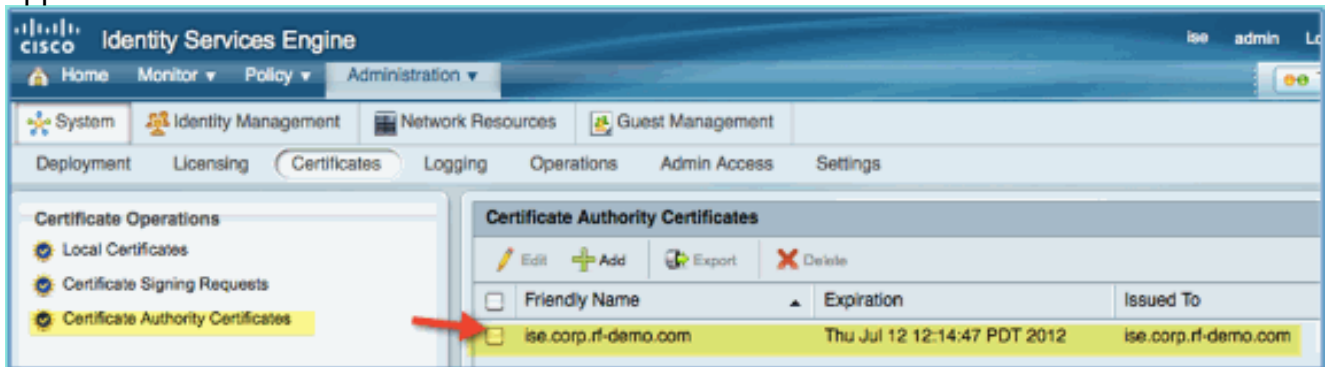


7. Sélectionnez l'opération **Certificats de l'autorité de certification** et accédez au certificat CA téléchargé précédemment.

8. Sélectionnez **Trust for client with EAP-TLS**, puis envoyez.

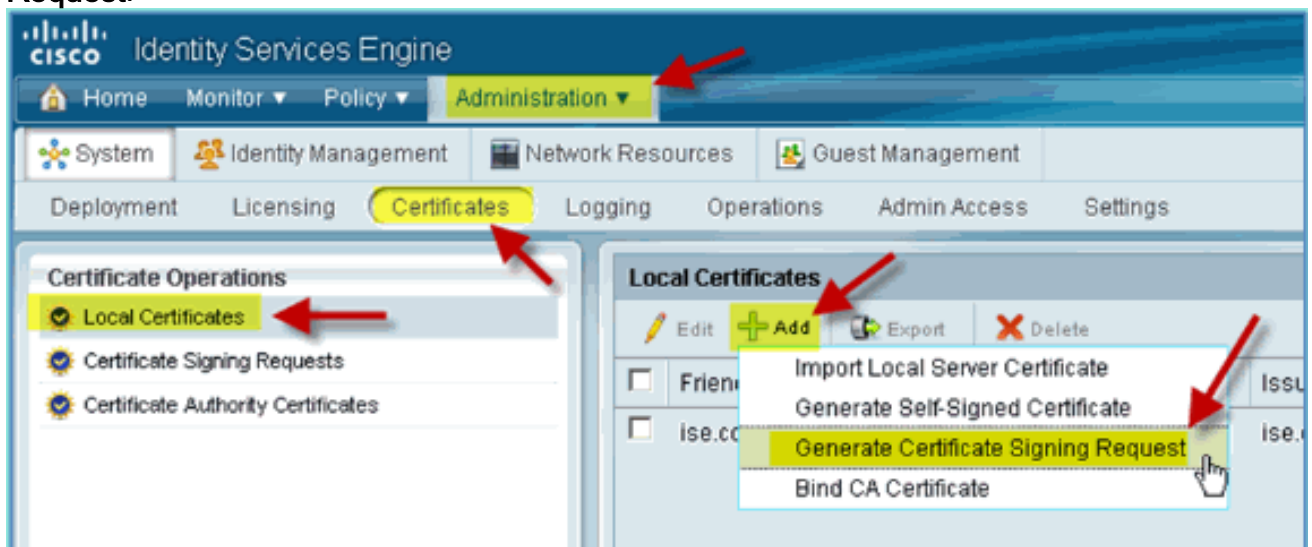


9. Vérifiez que l'autorité de certification a été ajoutée comme autorité de certification racine approuvée.



10. Dans un navigateur, accédez à **Administration > System > Certificates > Certificates Authority**.

11. Cliquez sur **Add**, puis sur **Generate Certificate Signing Request**.



12. Soumettez ces valeurs :Objet du certificat : CN=ise.corp.rf-demo.comLongueur de clé : 2048

Local Certificates > Generate Certificate Signing Request

▼ **Generate Certificate Signing Request**

Certificate

* Certificate Subject

* Key Length

Digest to Sign With SHA1

13. ISE vous demande si le CSR est disponible dans la page CSR. Cliquez sur OK.



14. Sélectionnez le CSR dans la page ISE CSR et cliquez sur **Export**.

15. Enregistrez le fichier à n'importe quel emplacement (par exemple, Téléchargements, etc.)

16. Le fichier sera enregistré en tant que *.pem.

Cisco Identity Services Engine Administration

System Identity Management Network Resources Guest Management

Deployment Licensing **Certificates** Logging Operations Admin Access Settings

Certificate Operations

- Local Certificates
- Certificate Signing Requests**
- Certificate Authority Certificates

Certificate Signing Requests

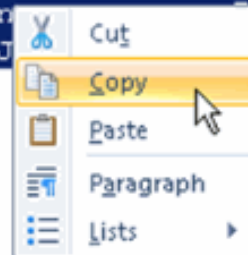
Export Delete

<input checked="" type="checkbox"/>	Friendly Name	Certificate Subject	Key Length
<input checked="" type="checkbox"/>	ise.corp.rf-demo.com	CN=ise.corp.rf-demo.com	2048

17. Recherchez le fichier CSR et modifiez-le à l'aide de Notepad/Wordpad/TextEdit.

18. Copier le contenu (Sélectionner tout > Copier).

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyTCCAAbECAQAwHzEdMBSGA1UEAxMUaXNlLmNvcnAucmYtZGVtby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXaeWDSqfI64K59dyRLm8JAxan
WYTaAJ68/Ke206ws/K3BFAFJQhndQQ0hYVmGcJLvn03pXtRln/q/HBuglLIItIvbe
86FADPq3kUNb48UHcdR9b5rUs7B8T5E6banZia6eHSXjIzX4f0U7mVOrzALeAPDK
HXU+/y/gleyNL6P8zC4bvi/SZXhZp1OvTQpi+8lh14M5ROChhbPUnB3EGVaIVRiN
wYn8Ojvejbtg//k0CItGARlG2IFbBbgUpkMVhDQqgixp3wrlm3hi9JXgffEI f4BO
sirLrhvMSuSNESnIVWYrRLz5Xt4dMct+bu08xaEYPqgoukYjxsA9gn0bRDMJAgMB
AAGgZTBjBgkqhkiG9w0BCQ4xVjBUMASGA1UdDwQEAWICrDAdBgNVHQ4EFgQU2jmj
715rSw0yVb/vlWAYkK/YBwkWewYDVR0lBAwwCgYIKwYBBQUHAwEwEQYJYIZIAYb4
QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUAA4IBAQBz4YPO9sN7WF2Htg+48300mw9q
gA/MMZsTioEPekcunrm+ZFtlAXajB32uwHHi1lc9Rn93TgOWPFxKEX9E89fz8WDK
J4qsQM7KEYOpQt4bia07188Lm6BBTk9mRhiTBwSF3dx0tlzfgiHc72kjWvxsgg/c
k8a7LHYgkgLRYBnpu15RjQ7wWijArH8cK1OrVT42riz7vK0g0nkWRHF52uiu3AkP
LPKQ72N2XYIXfu0jdgOaJjmsk6T9nLABVYQ6n...KDJTHchcwx6I1k/
V5QYBOjTYHXIPG8/ned9z3M0iZd2sm4XNS2bJ...W1ZuB6drHg9
-----END CERTIFICATE REQUEST-----
```



19. Ouvrez une fenêtre de navigateur sur <https://<Pod-AD>/certsrv>.
20. Cliquez sur **Demander un certificat**.

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Welcome

Use this Web site to request a certificate for your Web browser to communicate with over the Web, sign and encrypt messages.

You can also use this Web site to download a certificate automatically for a pending request.

For more information about Active Directory Certificate Services, click the following link:

Select a task:

[Request a certificate](#)

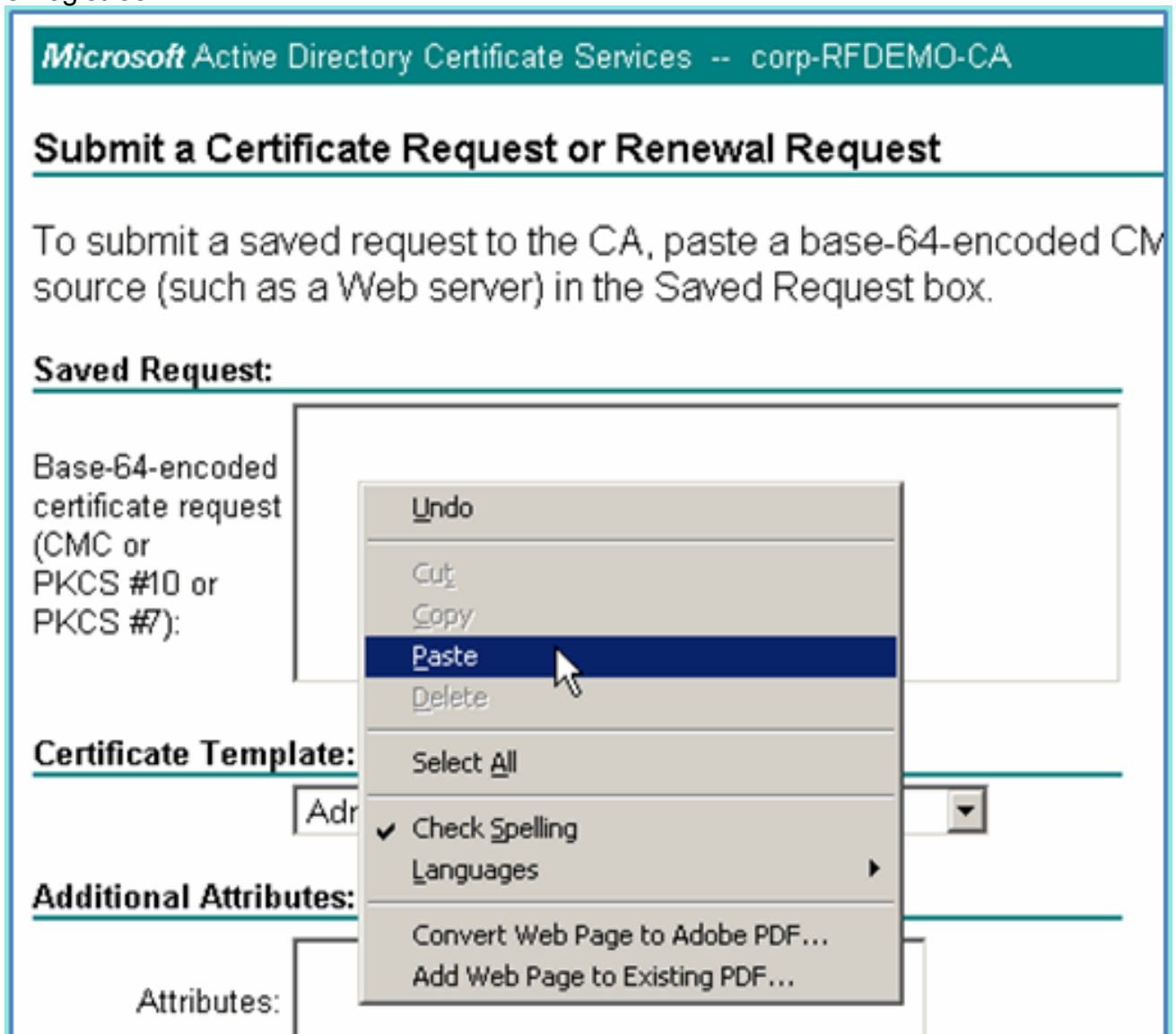
[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

21. Cliquez pour envoyer une **demande de certificat avancée**.



22. Collez le contenu CSR dans le champ Requête enregistrée.



23. Sélectionnez **Web Server** comme modèle de certificat, puis cliquez sur **Submit**.

Microsoft Active Directory Certificat...

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
gA/MMZsTioEPekcunnm+ZFt1AXajB32uwHH11c9
J4qsQM7KEYOpQt4bia071S8Lm6BBTk9mRhiTBwSF
kSa7LHYgkgLRYBnpul5RjQ7wWijArH8cK1OrVT42
LPKQ72N2XYIXfu0jdgogaJjmsk6T9nLABVYQ6nKQx
V5QYBOjTYHXIPG8/ned9z3MOiZd2sm4XNS2bJfO/
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

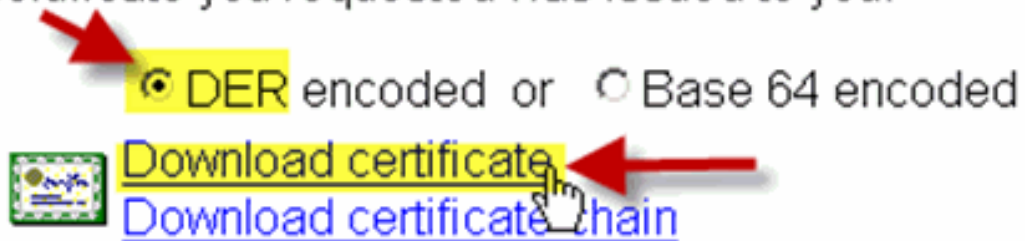
Attributes:

Submit >

24. Sélectionnez **DER encoded**, puis cliquez sur **Download certificate**.

Certificate Issued

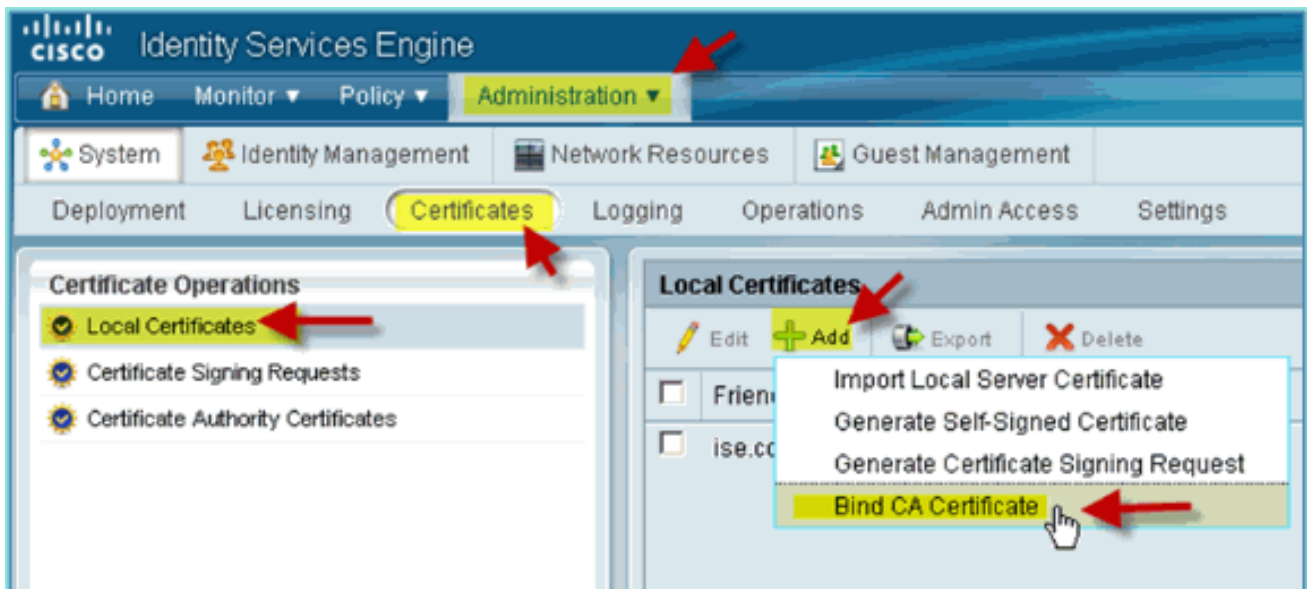
The certificate you requested was issued to you.



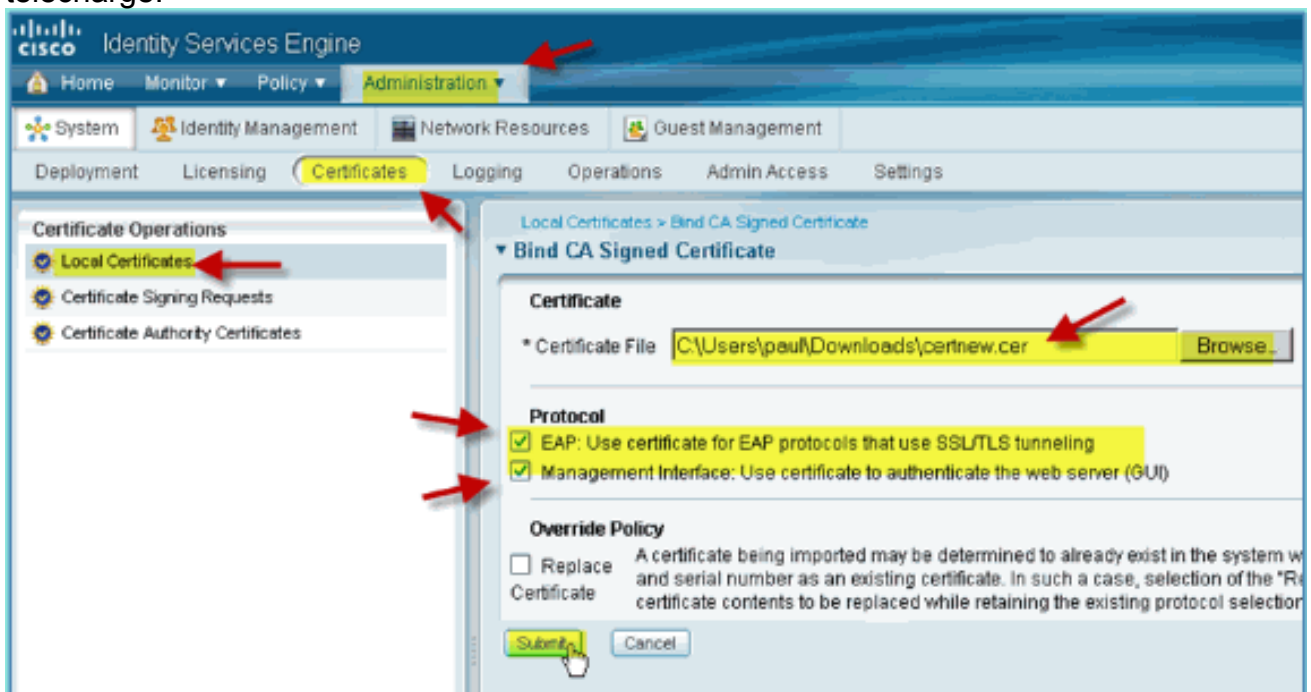
25. Enregistrez le fichier à un emplacement connu (par exemple, Téléchargements)
26. Accédez à **Administration > System > Certificates > Certificates Authority Certificates**.



27. Cliquez sur **Add > Bind CA Certificate**.

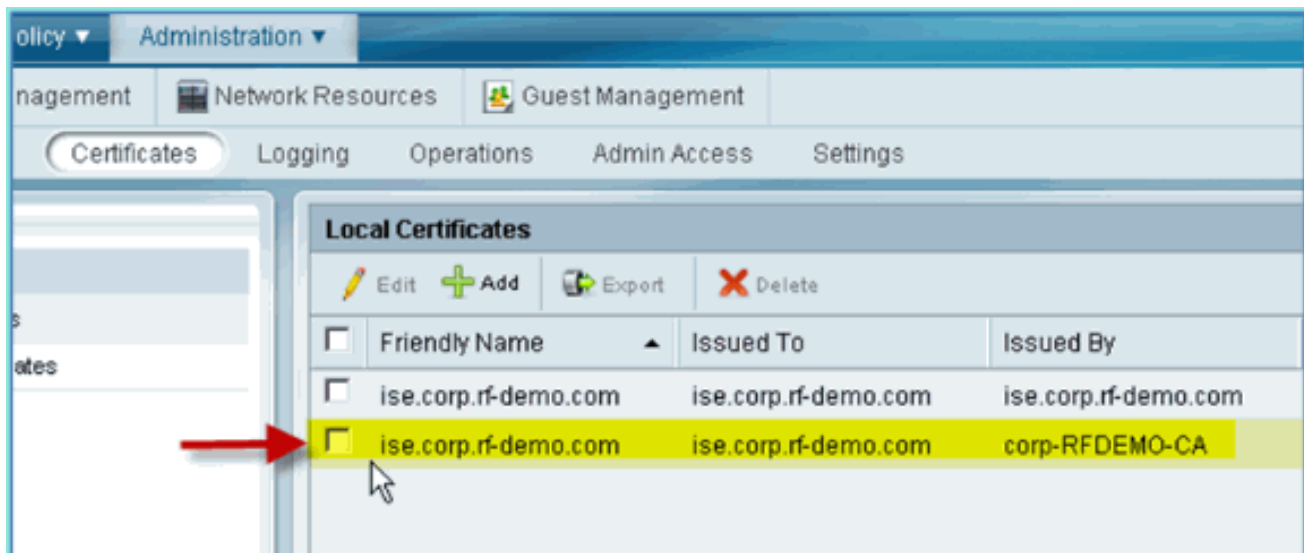


28. Accédez au certificat CA précédemment téléchargé.



29. Sélectionnez **Protocol EAP** et **Management Interface**, puis cliquez sur **Submit**.

30. Vérifiez que l'autorité de certification a été ajoutée comme autorité de certification racine approuvée.

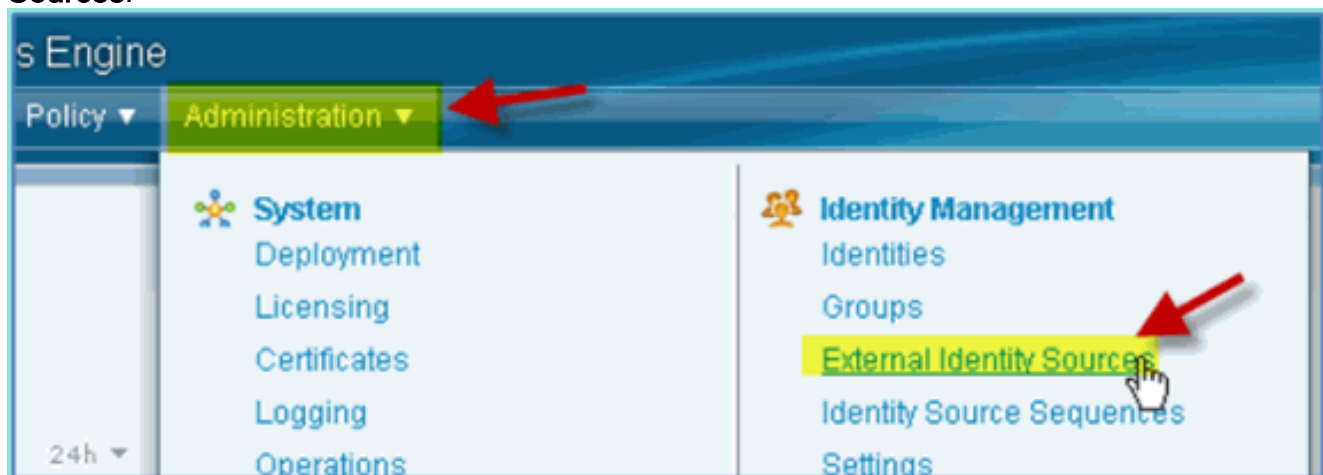


[Intégration à Windows 2008 Active Directory](#)

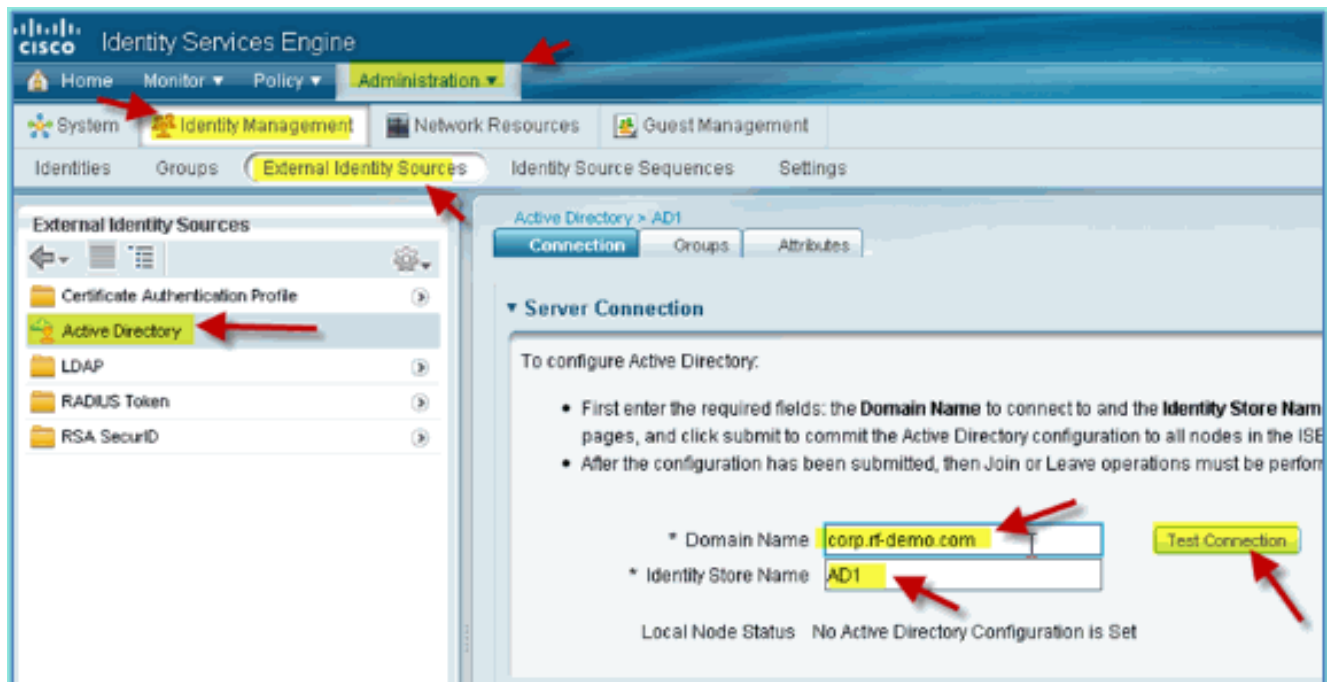
ISE peut communiquer directement avec Active Directory (AD) pour l'authentification utilisateur/machine ou pour la récupération des informations d'autorisation et des attributs utilisateur. Pour communiquer avec AD, ISE doit être « joint » à un domaine AD. Dans cet exercice, vous allez joindre ISE à un domaine AD et vérifier que la communication AD fonctionne correctement.

Procédez comme suit :

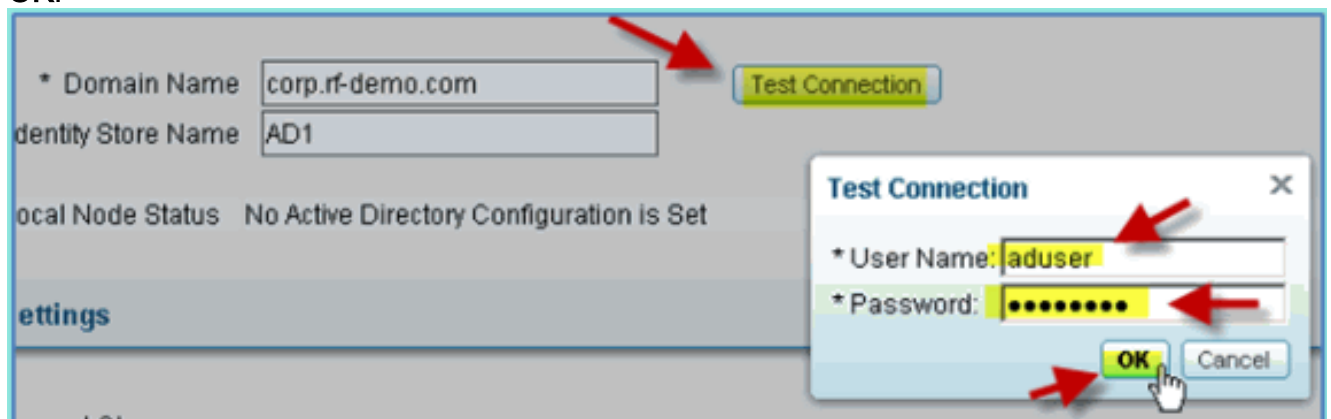
1. Afin de joindre ISE au domaine AD, à partir d'ISE allez à **Administration > Identity Management > External Identity Sources**.



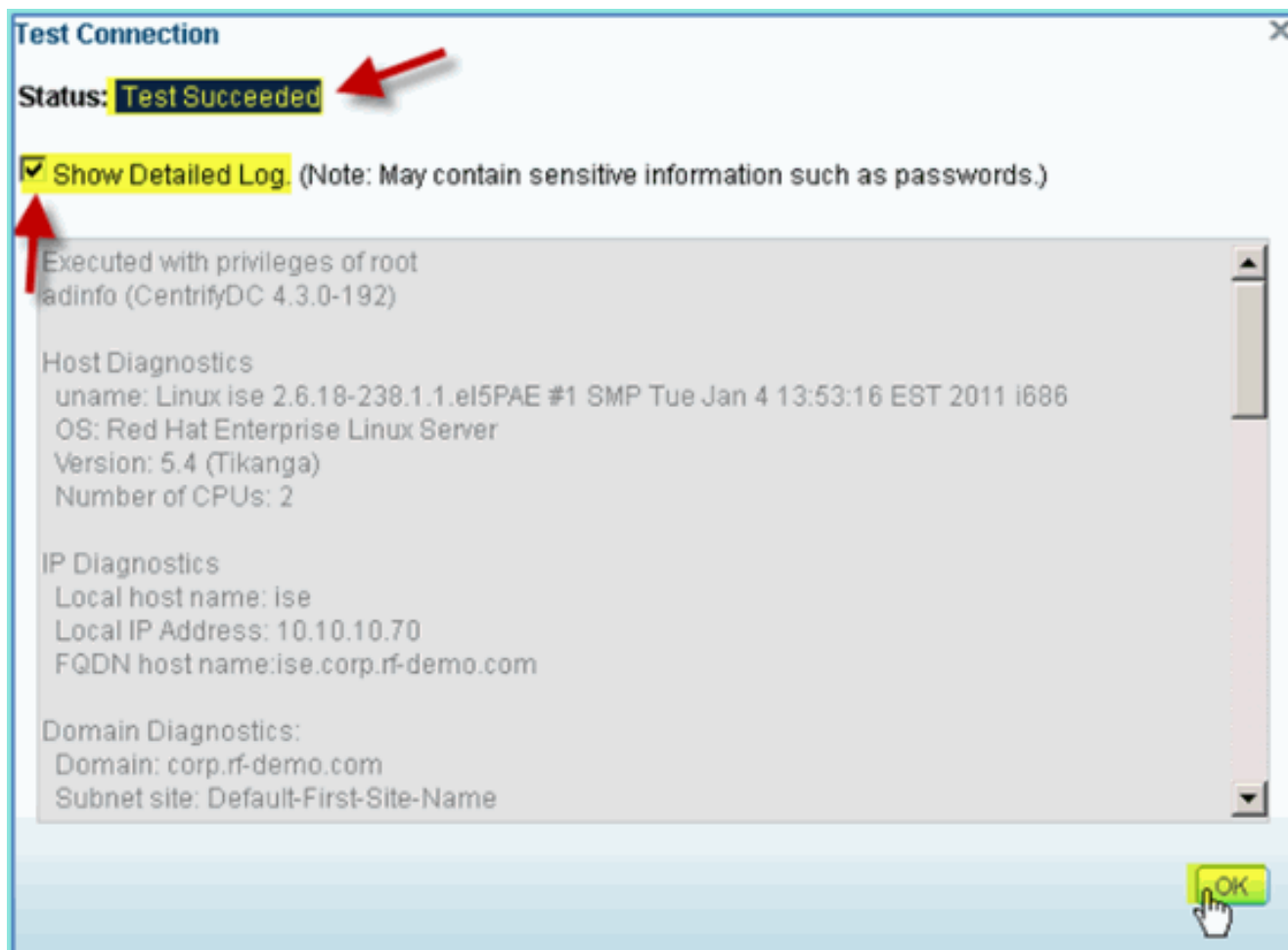
2. Dans le volet gauche (Sources d'identité externes), sélectionnez **Active Directory**.
3. Sur le côté droit, sélectionnez l'onglet **Connection** et saisissez ce qui suit :
 Nom de domaine : corp.rf-demo.com
 Nom du magasin d'identités : AD1



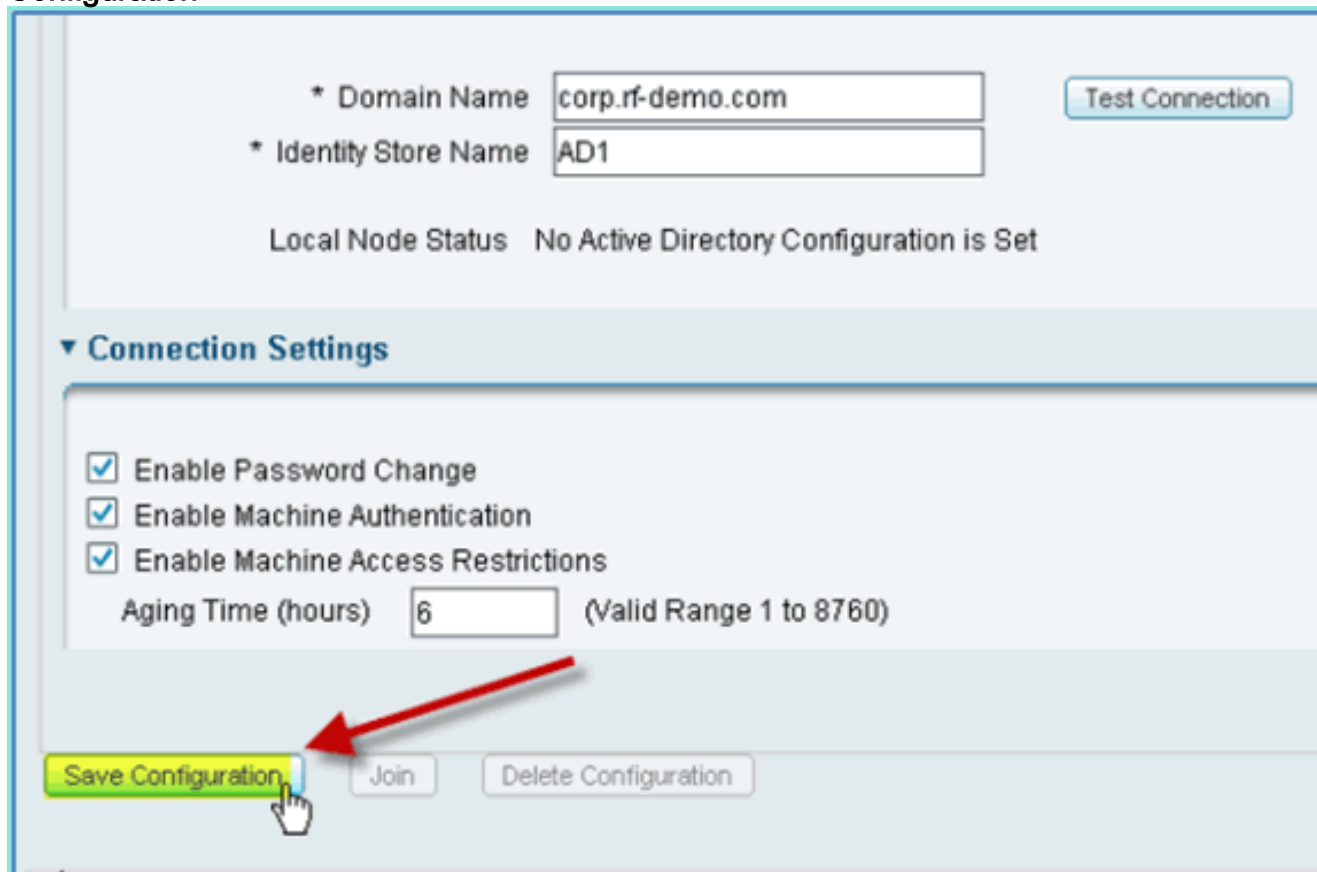
4. Cliquez sur **Tester la connexion**. Saisissez le nom d'utilisateur AD (aduser/Cisco123), puis cliquez sur **OK**.



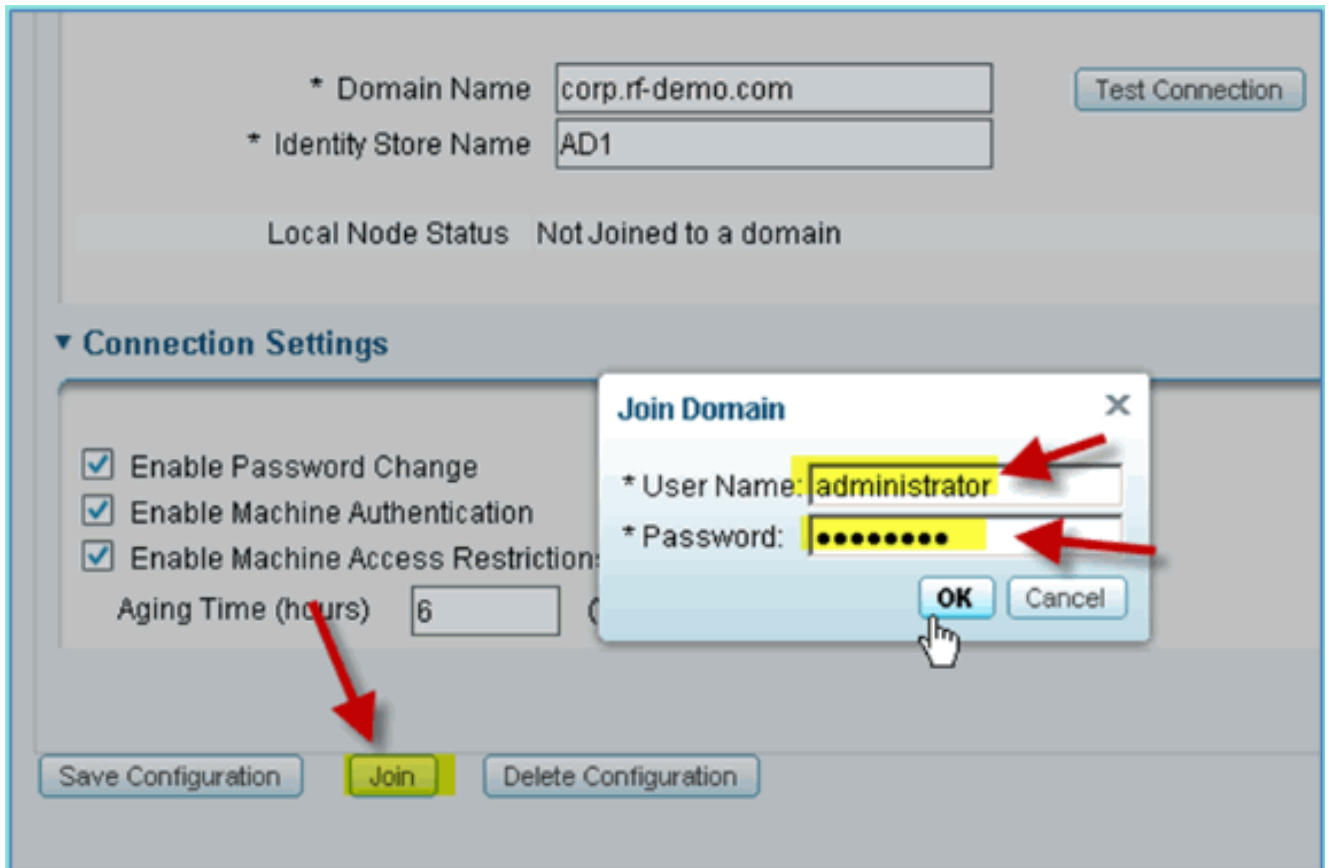
5. Vérifiez que l'état du test indique **Test Succeeded (Test réussi)**.
6. Sélectionnez **Afficher le journal détaillé** et observez les détails utiles pour le dépannage. Cliquez sur **OK** pour continuer.



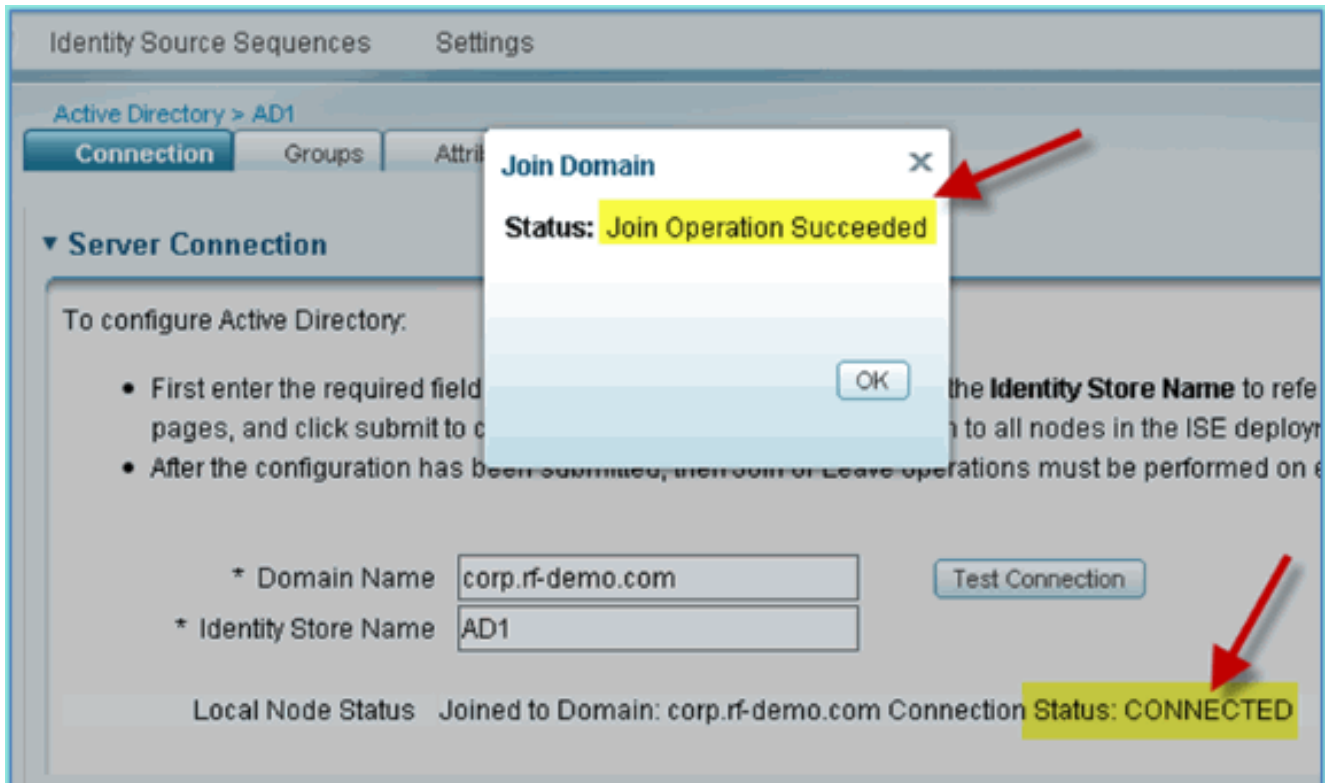
7. Cliquez sur **Save Configuration**.



8. Cliquez sur **Joindre**. Entrez l'utilisateur AD (administrator/Cisco123), puis cliquez sur **OK**.



9. Vérifiez que l'état de l'opération de jointure indique **Réussite**, puis cliquez sur **OK** pour continuer. L'état de la connexion au serveur indique **CONNECTED**. Si cet état change à tout moment, un test de connexion permet de résoudre les problèmes liés aux opérations AD.



[Ajouter des groupes Active Directory](#)

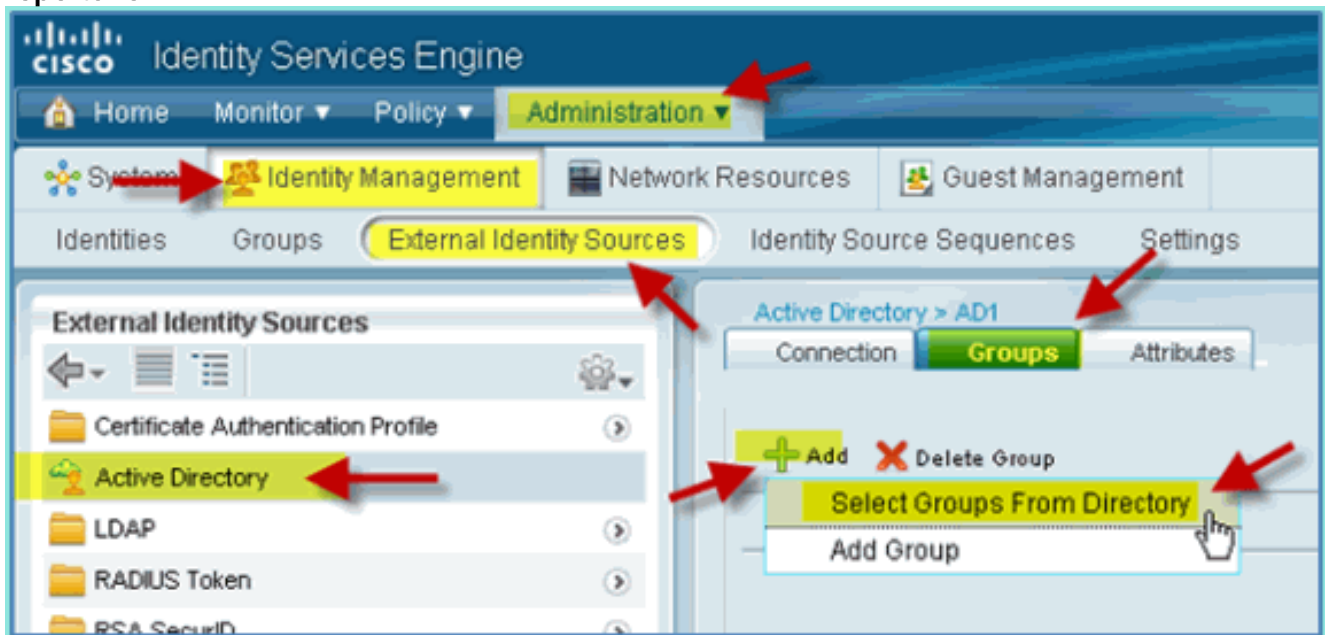
Lorsque des groupes AD sont ajoutés, un contrôle plus granulaire est autorisé sur les politiques

ISE. Par exemple, les groupes AD peuvent être différenciés par des rôles fonctionnels, tels que les groupes Employé ou Entrepreneur, sans que le bogue associé ne se produise dans les exercices ISE 1.0 précédents où les politiques étaient limitées aux utilisateurs.

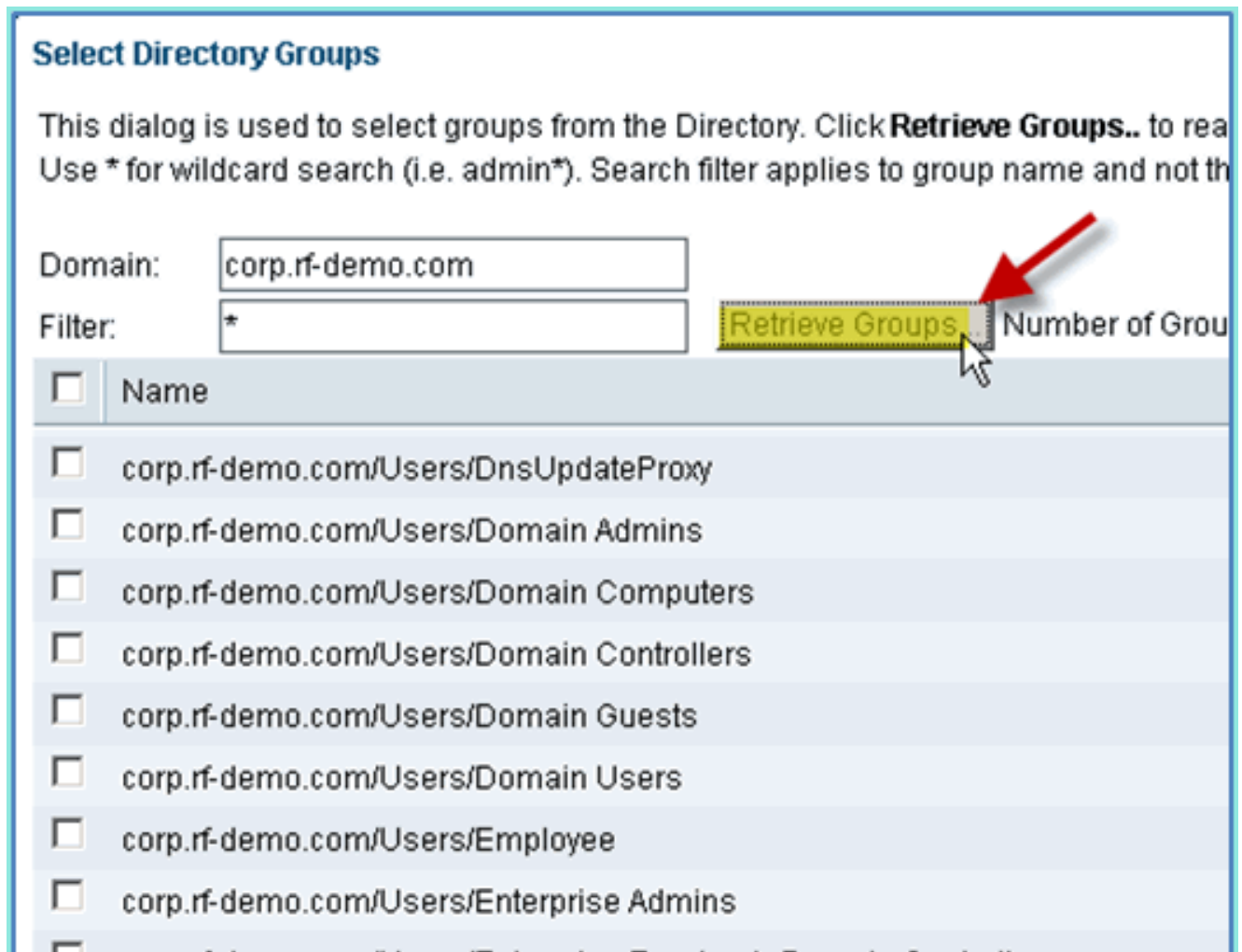
Dans ces travaux pratiques, seuls les utilisateurs du domaine et/ou le groupe Employé sont utilisés.

Procédez comme suit :

1. Dans ISE, accédez à **Administration > Identity Management > External Identity Sources**.
2. Sélectionnez **Active Directory > onglet Groupes**.
3. Cliquez sur **+Ajouter**, puis **sélectionnez Groupes dans le répertoire**.



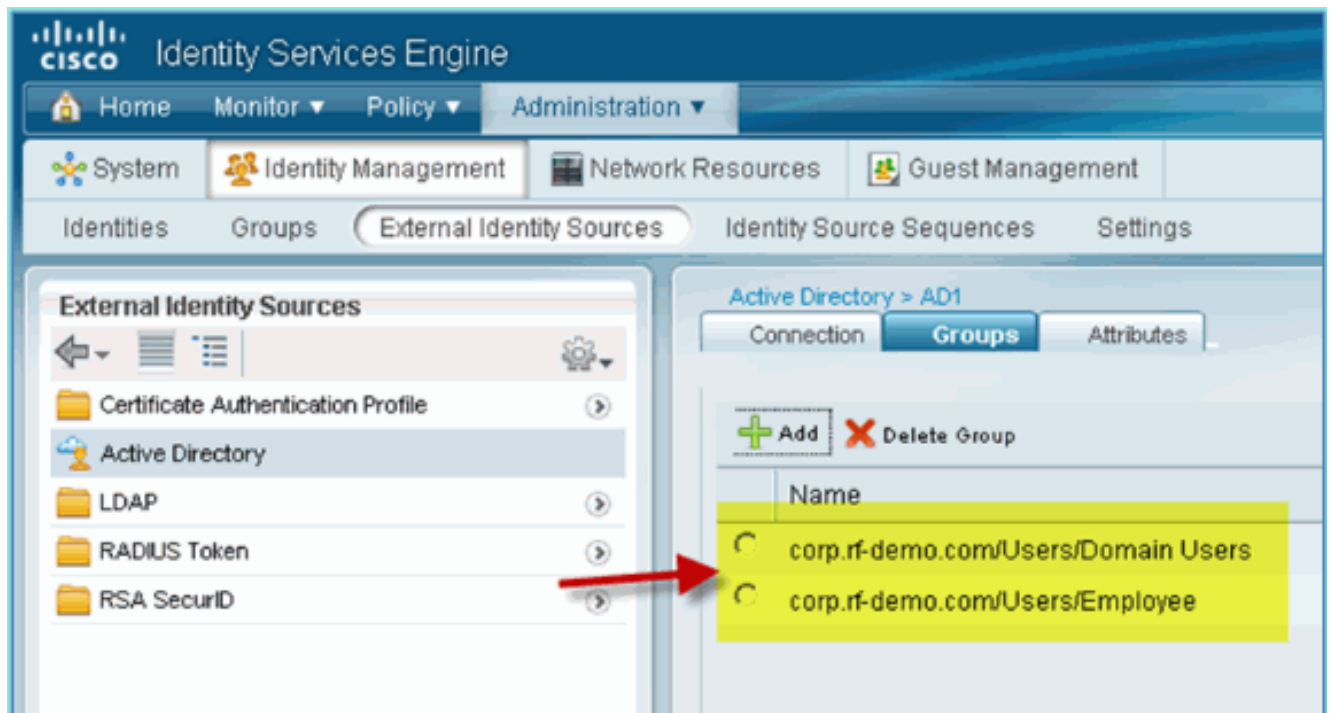
4. Dans la fenêtre de suivi (Sélectionner les groupes de répertoires), acceptez les valeurs par défaut pour le domaine (corp-rf-demo.com) et le filtre (*). Cliquez ensuite sur **Récupérer les groupes**.



5. Cochez les cases correspondant aux groupes **Utilisateurs du domaine** et **Employé**. Cliquez sur **OK** lorsque vous avez terminé.



6. Vérifiez que les groupes ont été ajoutés à la liste.

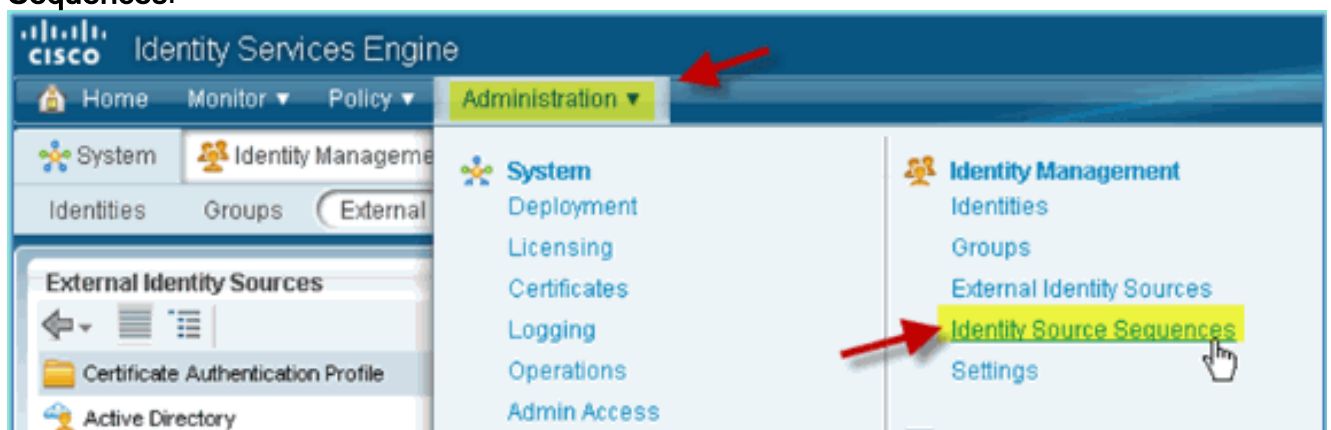


Ajouter une séquence source d'identité

Par défaut, ISE est configuré pour utiliser les utilisateurs internes pour le magasin d'authentification. Si AD est ajouté, un ordre de priorité de séquence peut être créé pour inclure l'AD qu'ISE utilisera pour vérifier l'authentification.

Procédez comme suit :

1. Dans ISE, accédez à **Administration > Identity Management > Identity Source Sequences**.



2. Cliquez sur **+Add** afin d'ajouter une nouvelle séquence.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Monitor', 'Policy', and 'Administration'. Below this, there are tabs for 'System', 'Identity Management', 'Network Resources', and 'Guest Management'. The 'Identity Source Sequences' page is active, showing a table of existing sequences. The 'Add' button is highlighted with a yellow box and a red arrow pointing to it.

Name	Description	Identity Stores
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

3. Entrez le nouveau nom : **AD_Internal**. Ajoutez toutes les sources disponibles au champ Sélectionné. Ensuite, réorganisez selon les besoins de sorte que AD1 soit placé en haut de la liste. Cliquez sur Submit.

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences List > New Identity Source Sequence

▼ Identity Source Sequence

* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

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

Available	Selected
	AD1 Internal Users Internal Endpoints

▼ Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

Treat as if the user was not found and proceed to the next store in the sequence

4. Vérifiez que la séquence a été ajoutée à la liste.

Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences

Edit Add Duplicates Delete Filter

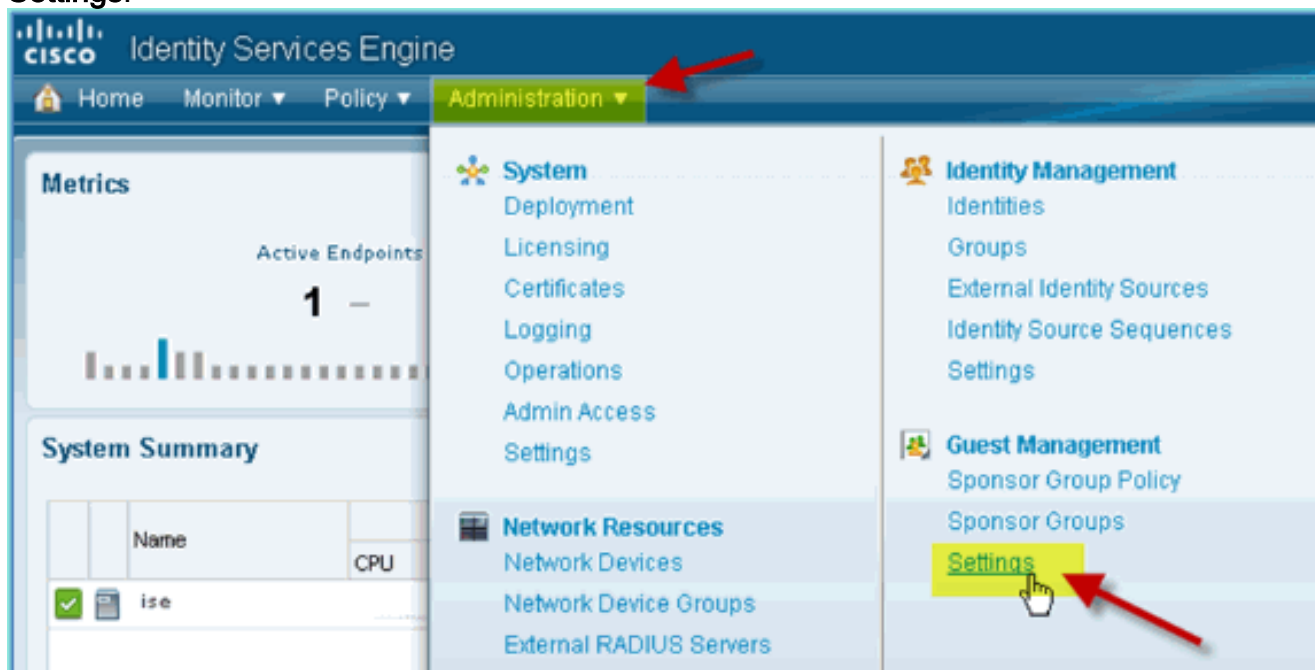
Name	Description	Identity Stores
AD_Internal		AD1, Internal Endpoints, Internal Users
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

Accès invité parrainé sans fil ISE avec fonction AD intégrée

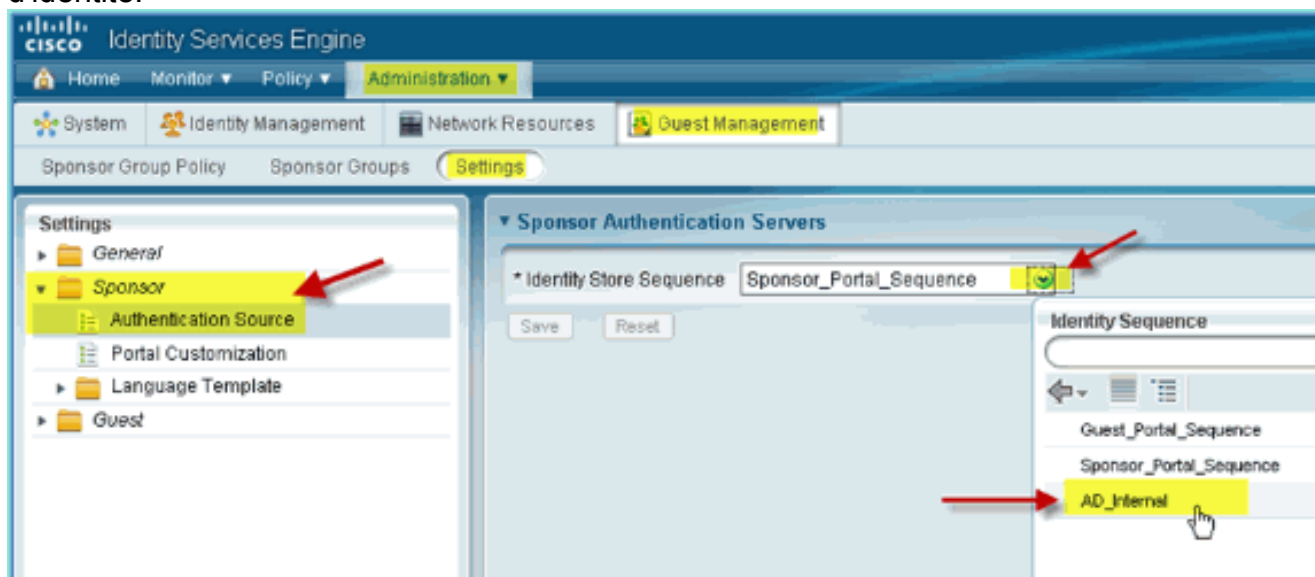
ISE peut être configuré pour autoriser les invités à être parrainés avec des stratégies afin de permettre aux utilisateurs du domaine AD de parrainer l'accès invité.

Procédez comme suit :

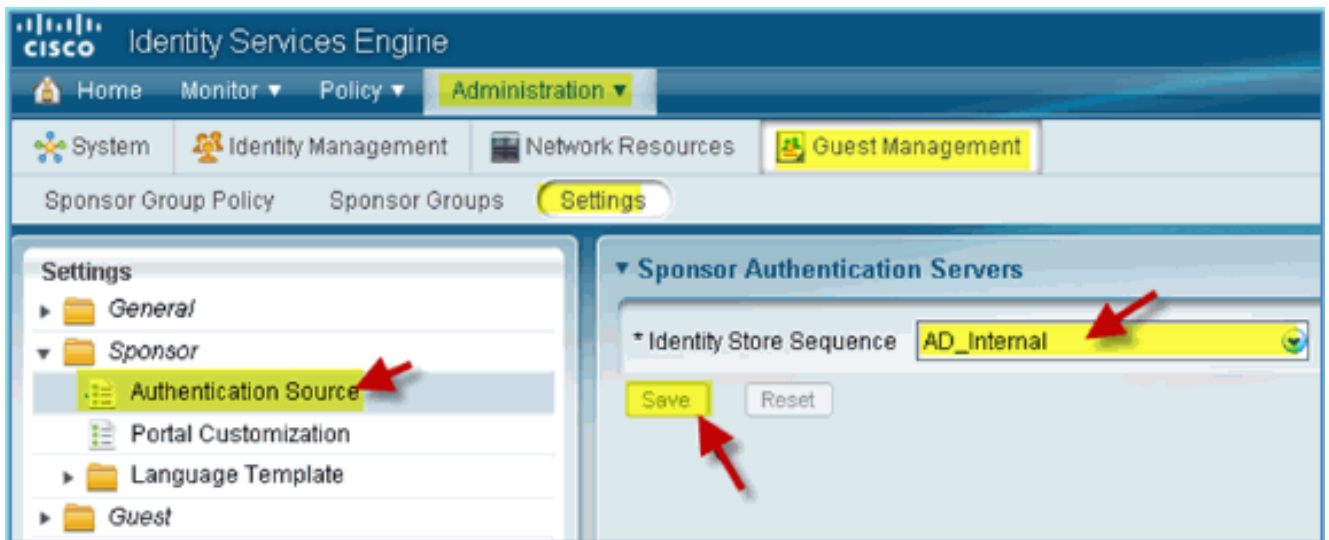
1. Dans ISE, accédez à **Administration > Guest Management > Settings**.



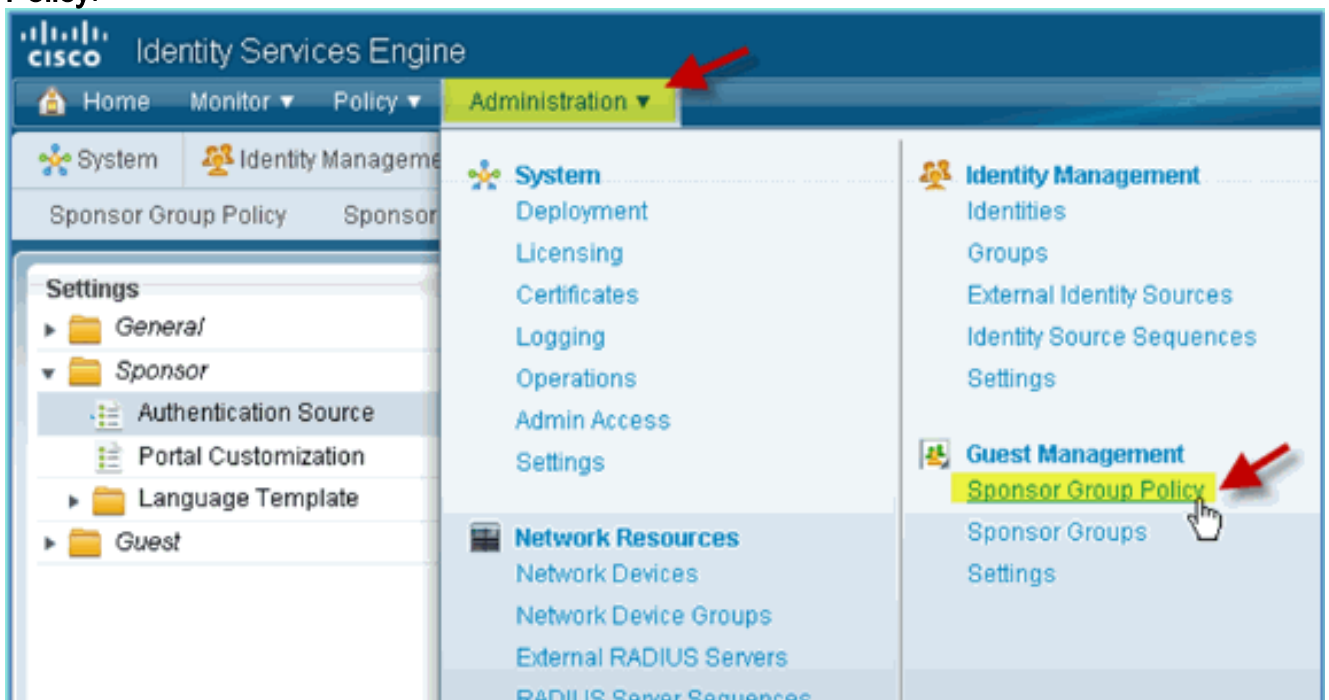
2. Développez **Sponsor**, puis cliquez sur **Authentication Source**. Sélectionnez ensuite **AD_Internal** comme séquence de stockage d'identité.



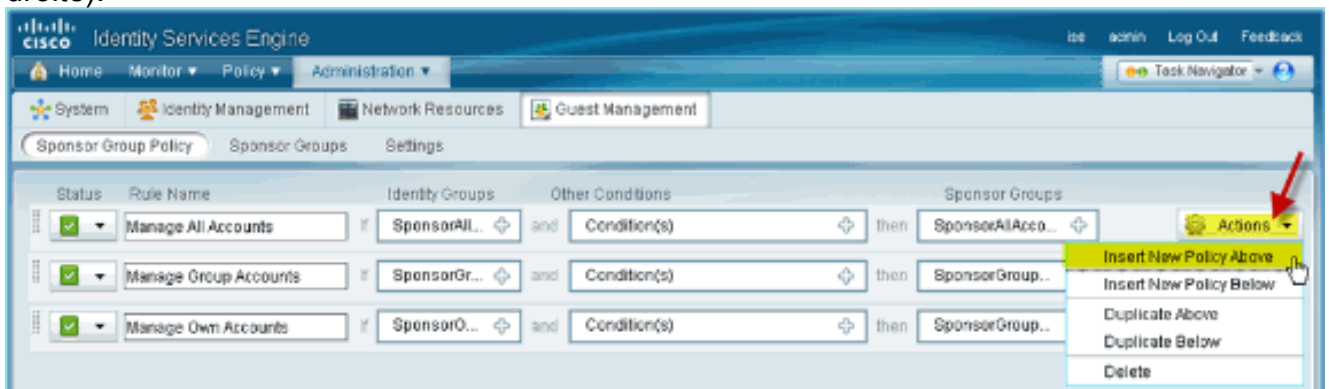
3. Confirmez **AD_Internal** comme séquence de stockage d'identités. Cliquez sur **Save**.



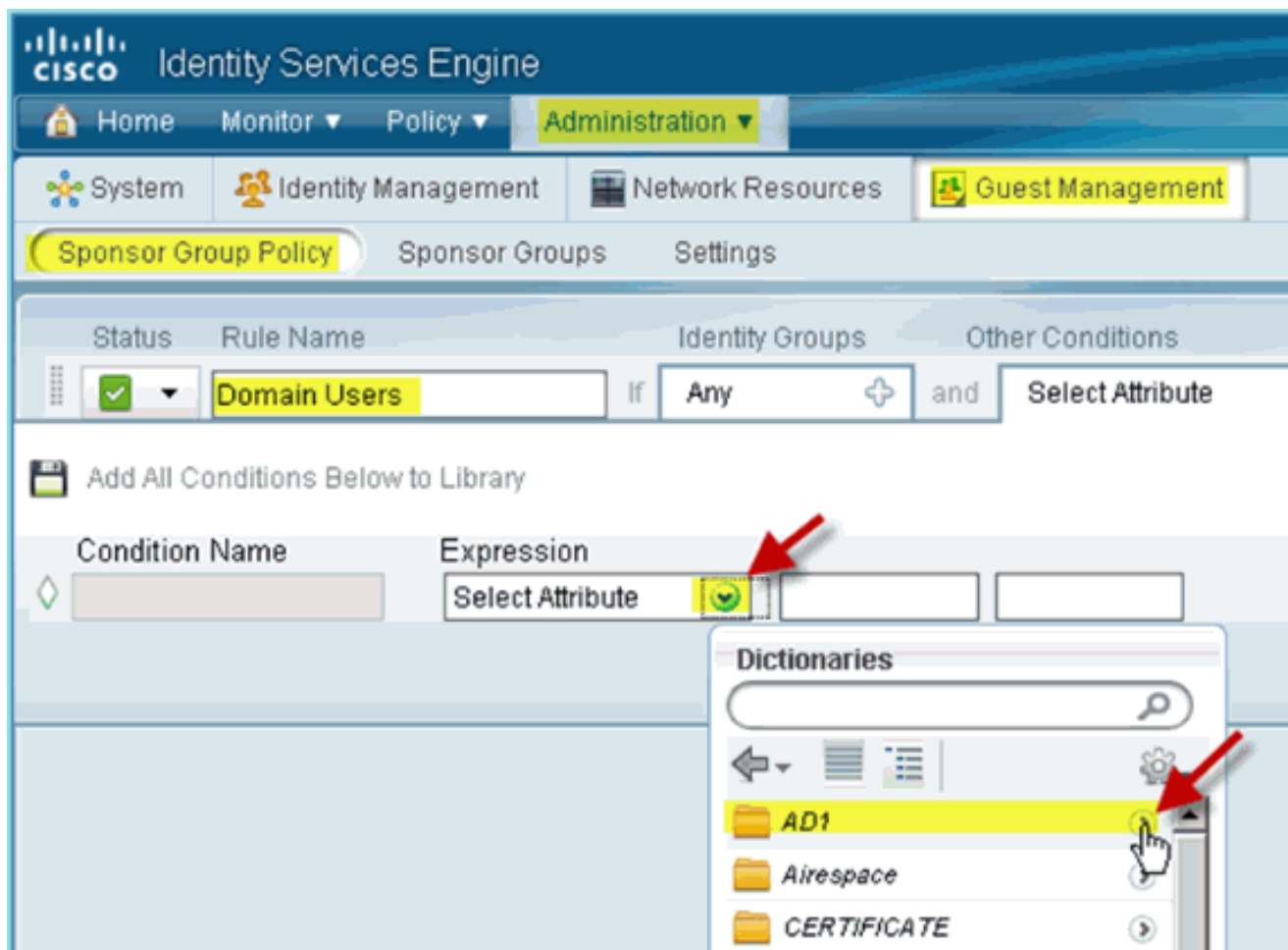
4. Accédez à Administration > Guest Management > Sponsor Group Policy.



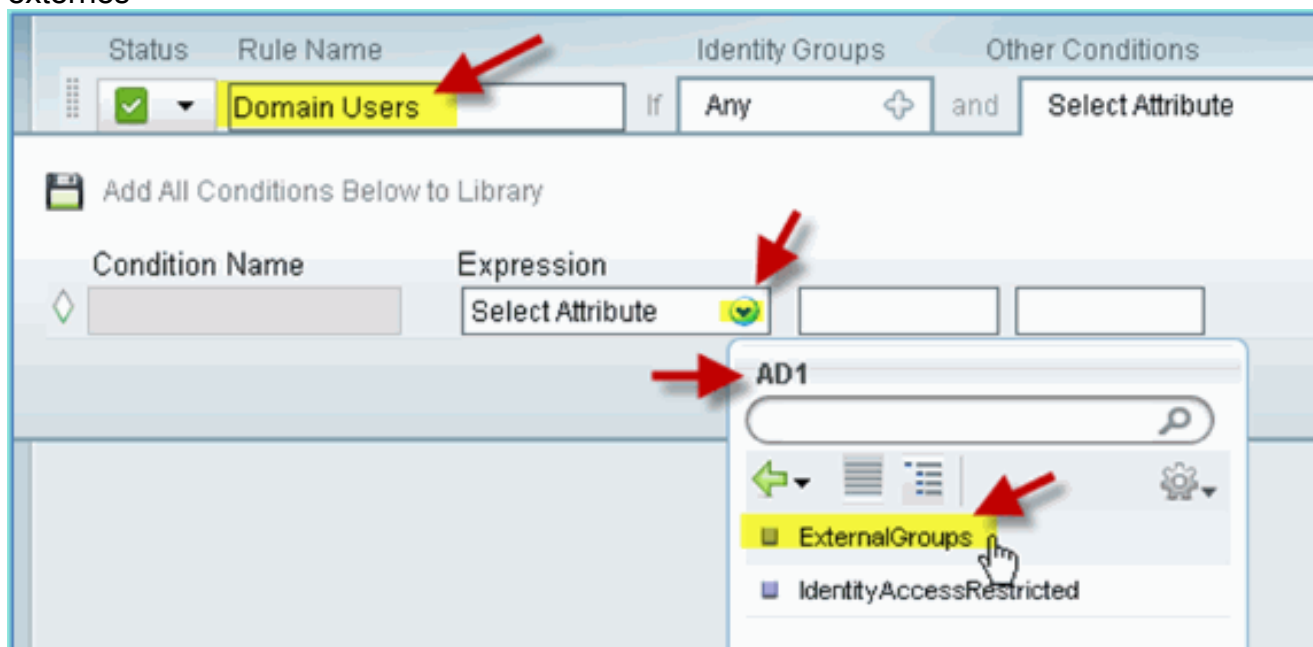
5. Insérer une nouvelle stratégie au-dessus de la première règle (cliquez sur l'icône Actions à droite).



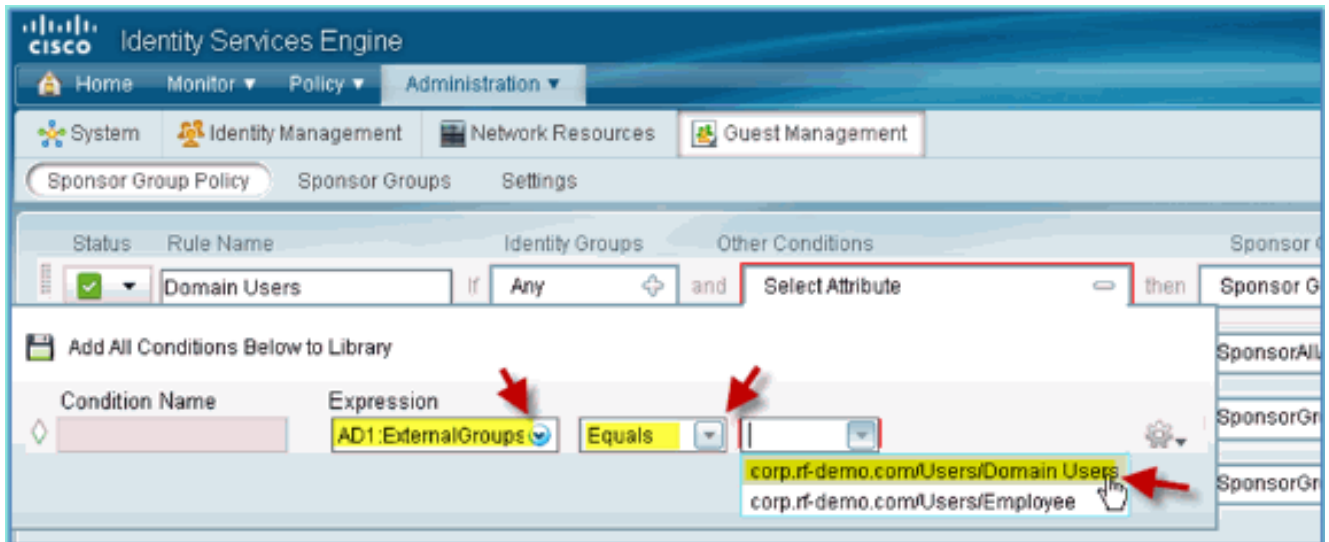
6. Pour la nouvelle stratégie de groupe de sponsor, créez les éléments suivants :
 Nom de la règle : Utilisateurs du domaine
 Groupes d'identités : TousAutres conditions : (Créer nouveau / Avancé) > AD1



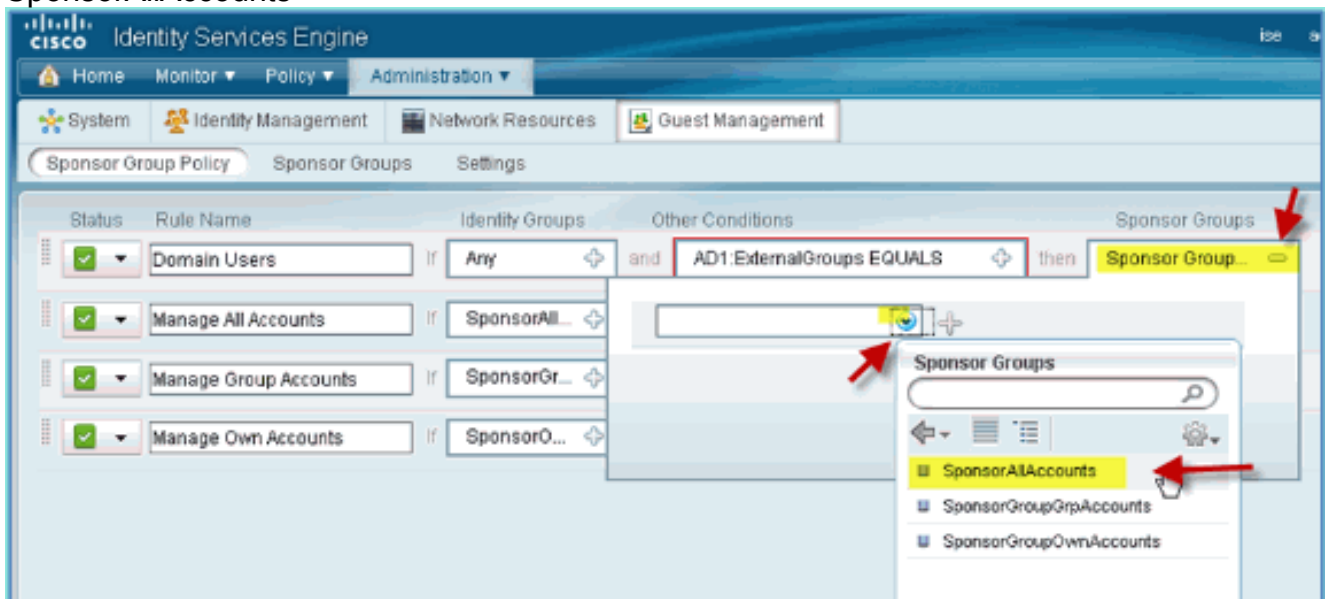
AD1 : groupes
externes



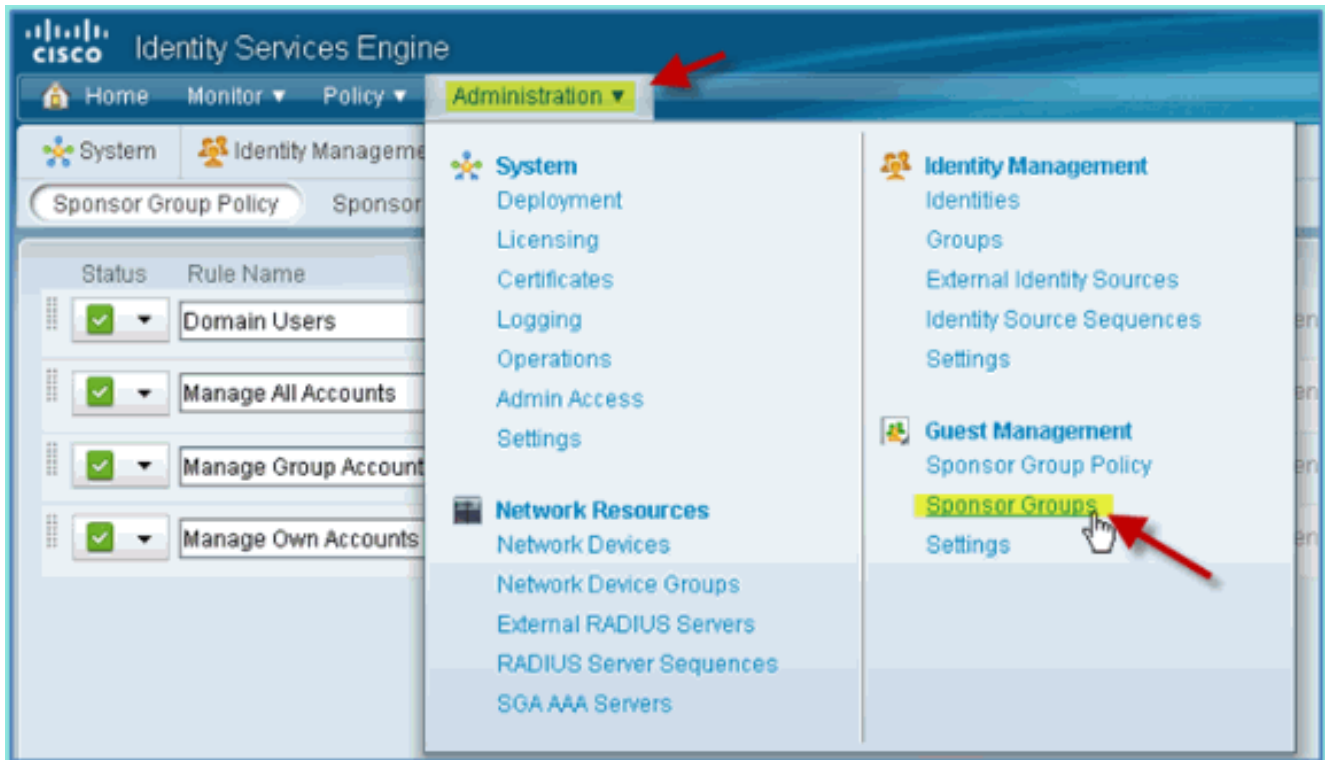
Groupes externes AD1 > Égal à > corp.rf-demo.com/Users/Domain
utilisateurs



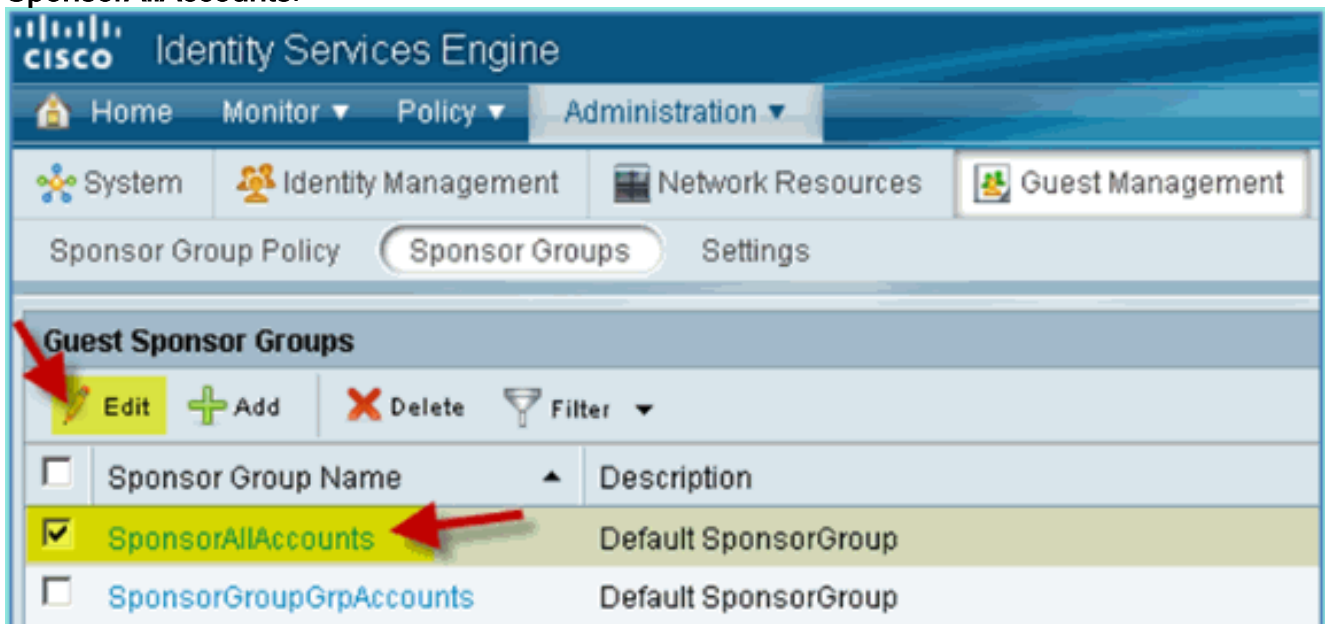
7. Dans Groupes de sponsors, définissez les paramètres suivants : Groupes de sponsors : SponsorAllAccounts



8. Accédez à Administration > Guest Management > Sponsor Groups.



9. Sélectionnez Edition > SponsorAllAccounts.



10. Sélectionnez les niveaux d'autorisation et définissez les paramètres suivants :Afficher le mot de passe invité :
Oui

The screenshot displays the Cisco ISE Administration interface. The breadcrumb path is 'Sponsor Group List > SponsorAllAccounts'. The 'Authorization Levels' tab is active, showing a list of permissions. The 'View Guest Password' setting is highlighted in yellow and has a red arrow pointing to it. The 'Save' and 'Reset' buttons are located at the bottom left of the configuration area.

Setting	Value
Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	No
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)

[Configuration de la fonctionnalité SPAN sur le commutateur](#)

Configurez la fonctionnalité SPAN : l'interface de sonde/gestion ISE est L2 adjacente à l'interface de gestion WLC. Le commutateur peut être configuré pour la fonctionnalité SPAN et d'autres interfaces, telles que les VLAN d'interface employé et invité.

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

[Référence : Authentification sans fil pour Apple MAC OS X](#)

Associez-vous au WLC via un SSID authentifié en tant qu'utilisateur INTERNE (ou utilisateur AD

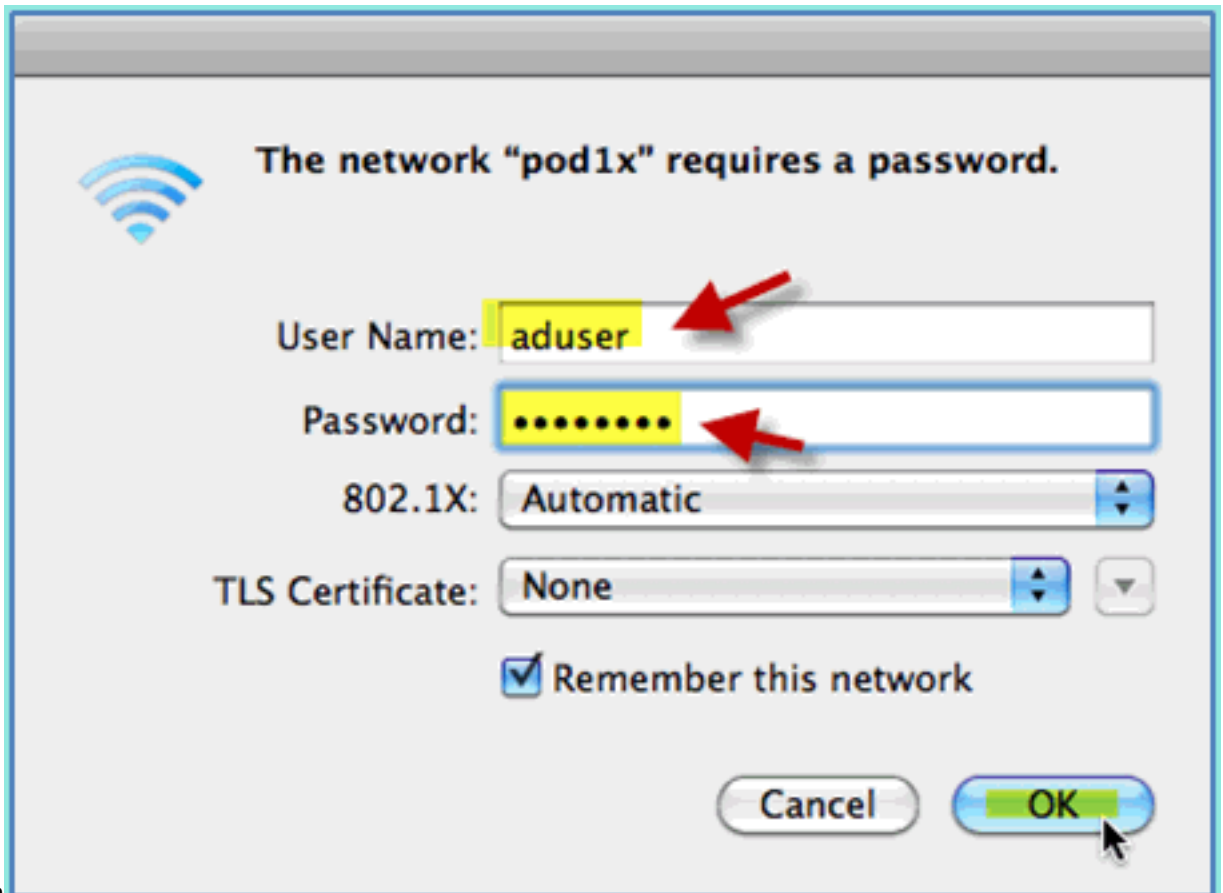
intégré) à l'aide d'un ordinateur portable sans fil Apple Mac OS X. Ignorer si non applicable.

1. Sur un Mac, accédez aux paramètres WLAN. Activez WIFI, puis sélectionnez le SSID POD 802.1X activé et connectez-vous à celui-ci créé dans l'exercice



précédent.

2. Fournissez les informations suivantes pour vous connecter :Nom d'utilisateur : utilisateur (si AD est utilisé), employé (interne - Employé), entrepreneur (interne - Entrepreneur)Mot de passe : XXXX802.1X : AutomatiqueCertificat TLS :

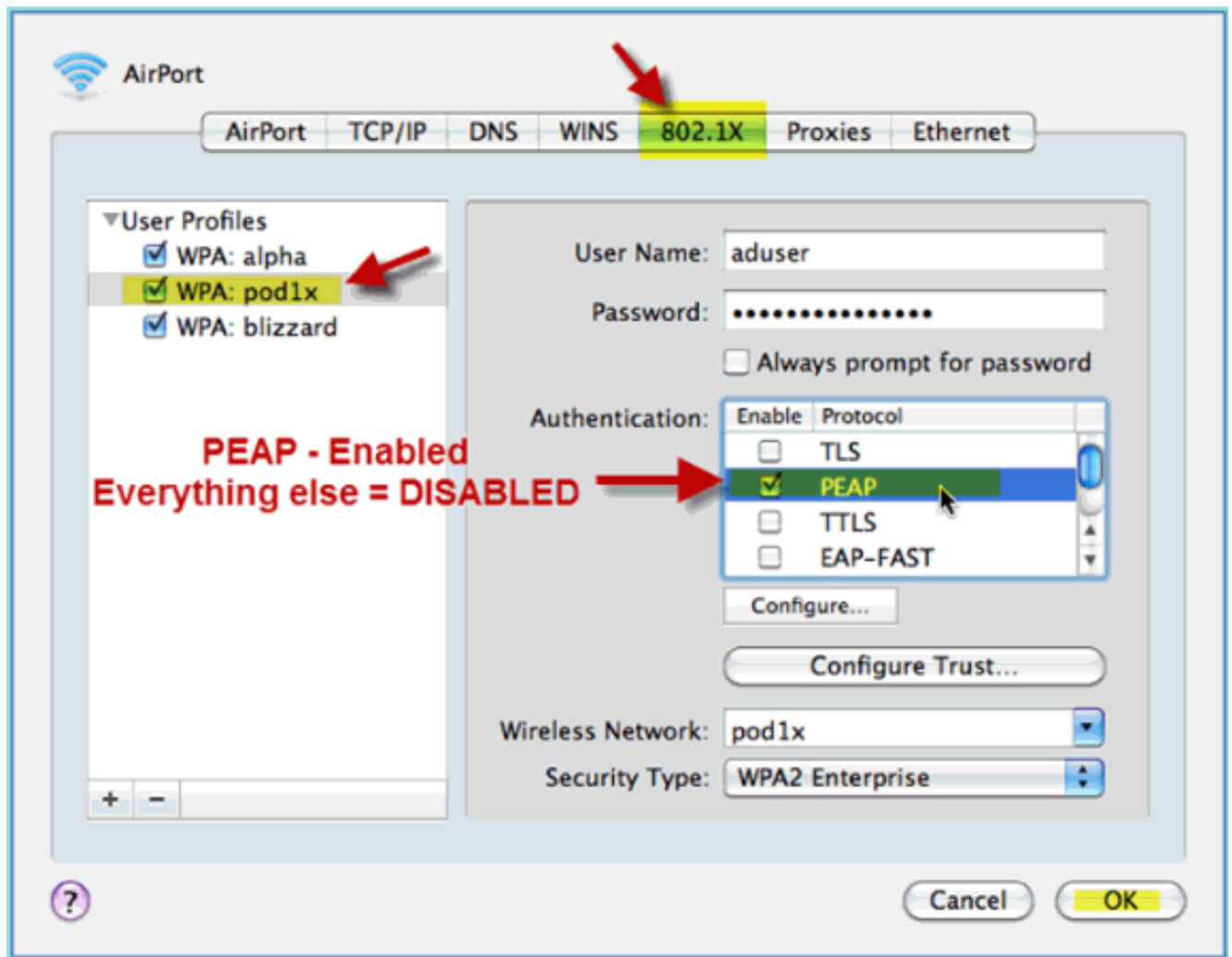


Aucun

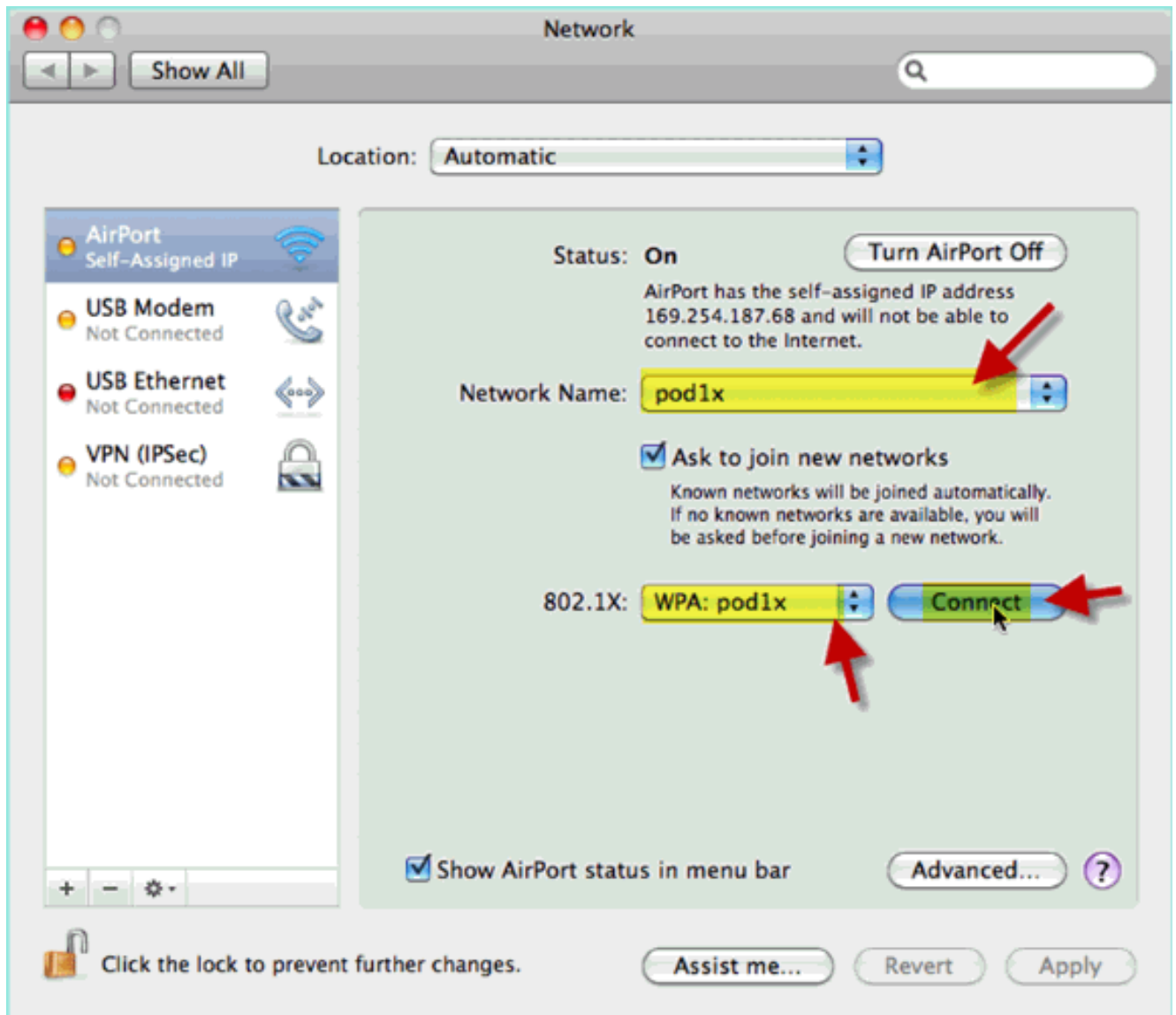
À ce stade, l'ordinateur portable risque de ne pas se connecter. En outre, ISE peut lancer un événement en échec comme suit :

Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain

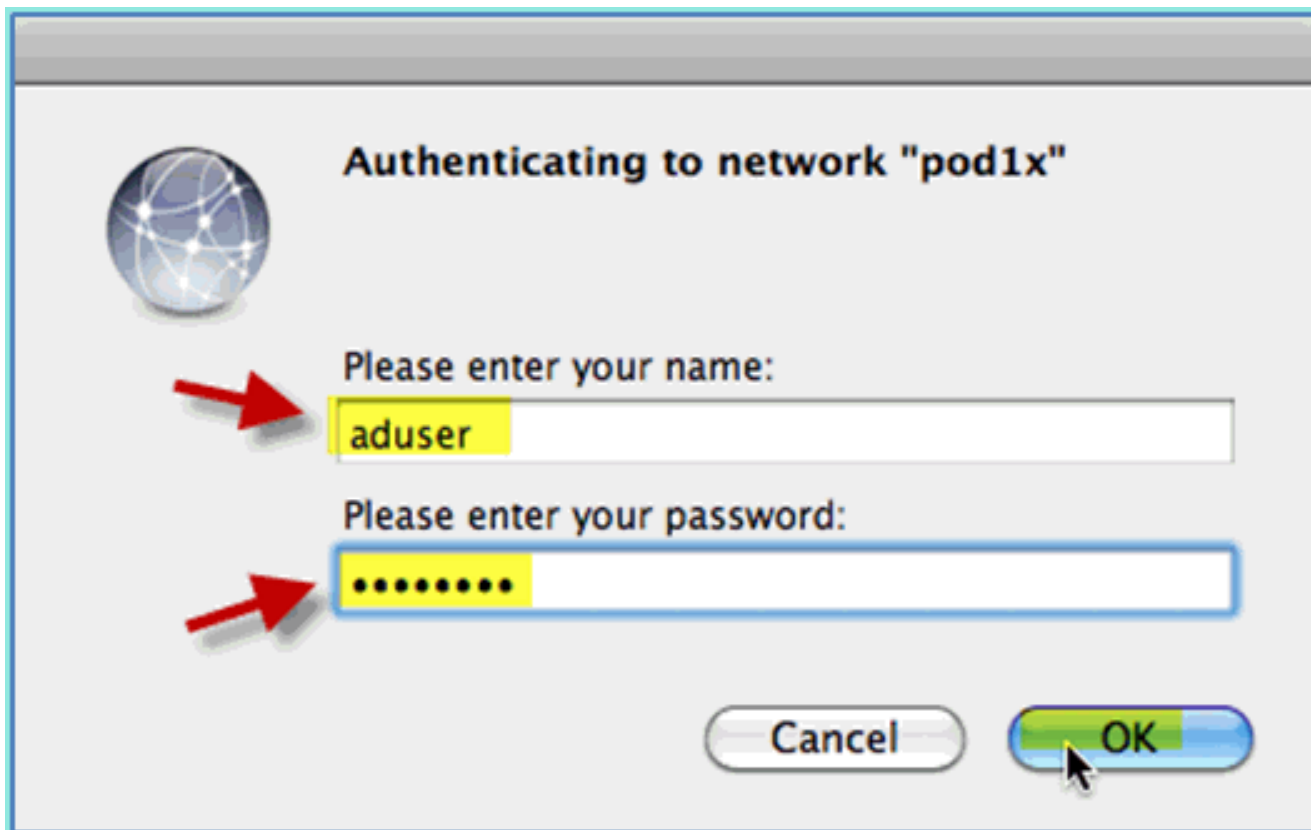
3. Accédez à **Préférences système > Réseau > Aéroport > 802.1X** et définissez le nouveau SSID POD / WPA profile Authentication comme suit :
TLS : désactivé
PEAP : activé
TTLS : désactivé
EAP-FAST : désactivé



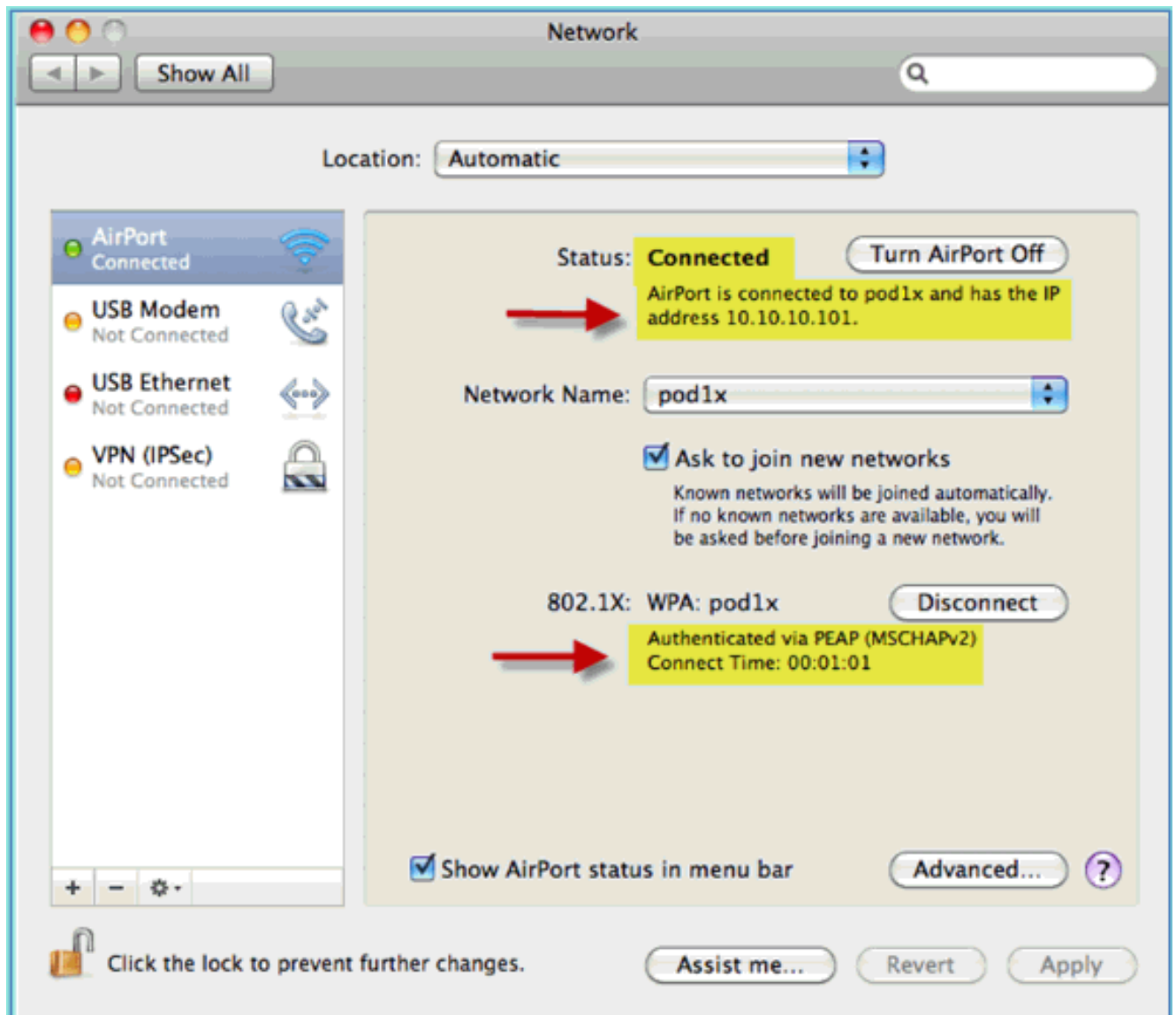
4. Cliquez sur **OK** pour continuer et permettre l'enregistrement du paramètre.
5. Dans l'écran Network (Réseau), sélectionnez le SSID approprié + le profil WPA 802.1X et cliquez sur **Connect**.



6. Le système peut vous demander un nom d'utilisateur et un mot de passe. Entrez l'utilisateur et le mot de passe AD (aduser/XXXX), puis cliquez sur OK.



Le client doit afficher **Connected** via PEAP avec une adresse IP valide.

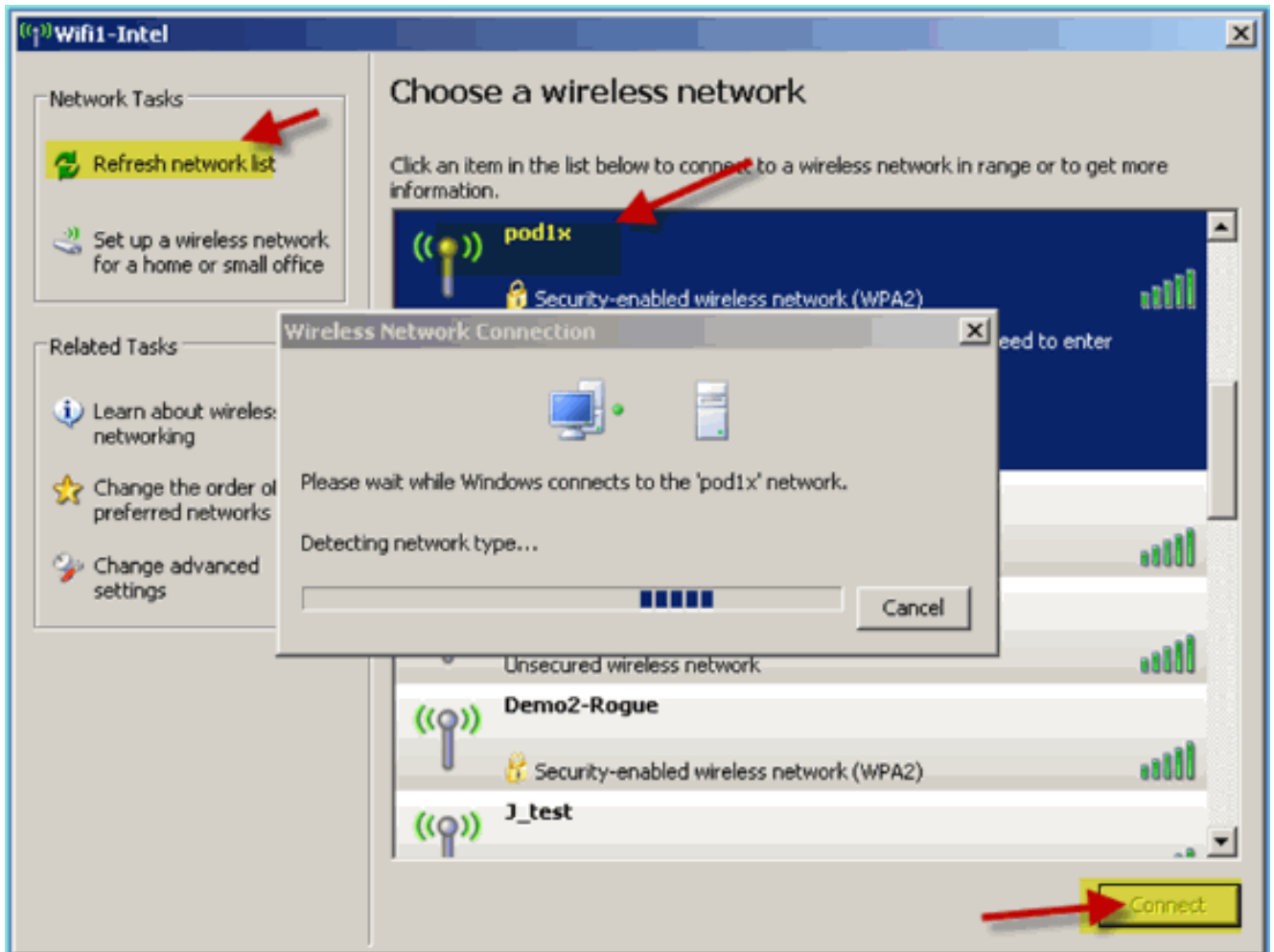


Référence : Authentification sans fil pour Microsoft Windows XP

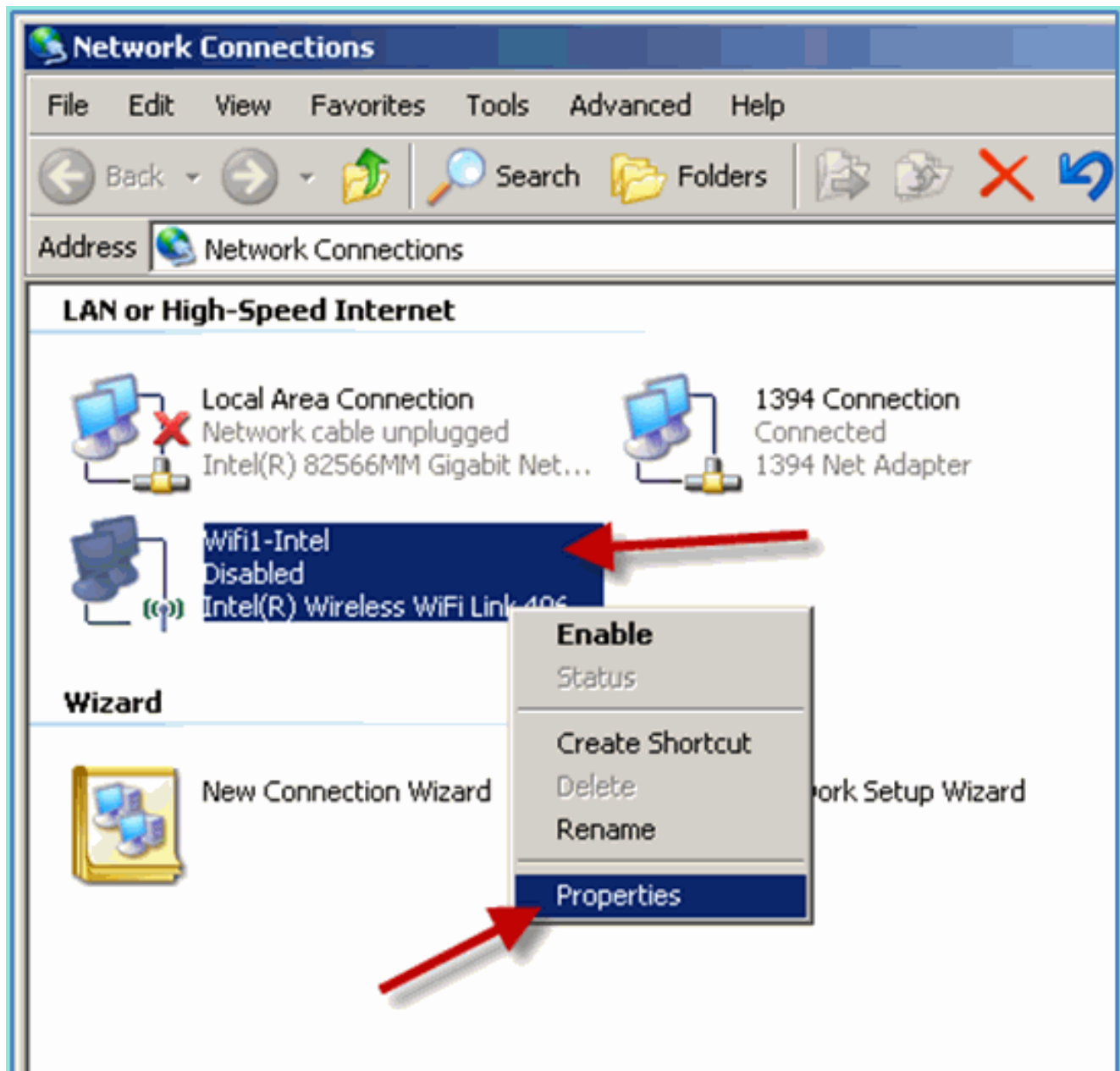
Associer au WLC via un SSID authentifié en tant qu'utilisateur INTERNE (ou utilisateur AD intégré) à l'aide d'un ordinateur portable sans fil Windows XP. Ignorer si non applicable.

Procédez comme suit :

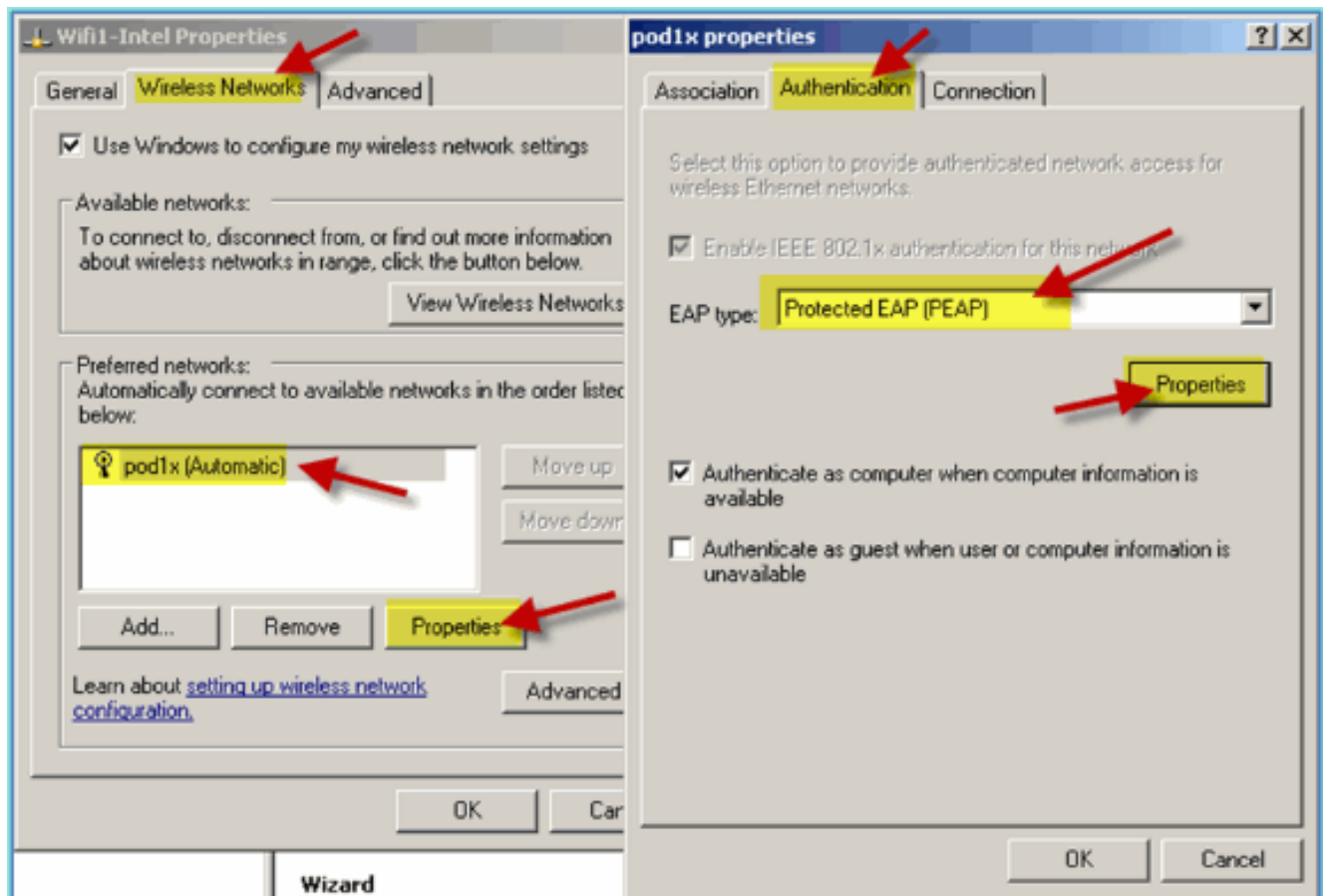
1. Sur l'ordinateur portable, accédez aux paramètres WLAN. Activez le WIFI et connectez-vous au SSID POD 802.1X créé dans l'exercice précédent.



2. Accédez aux propriétés réseau de l'interface WIFI.

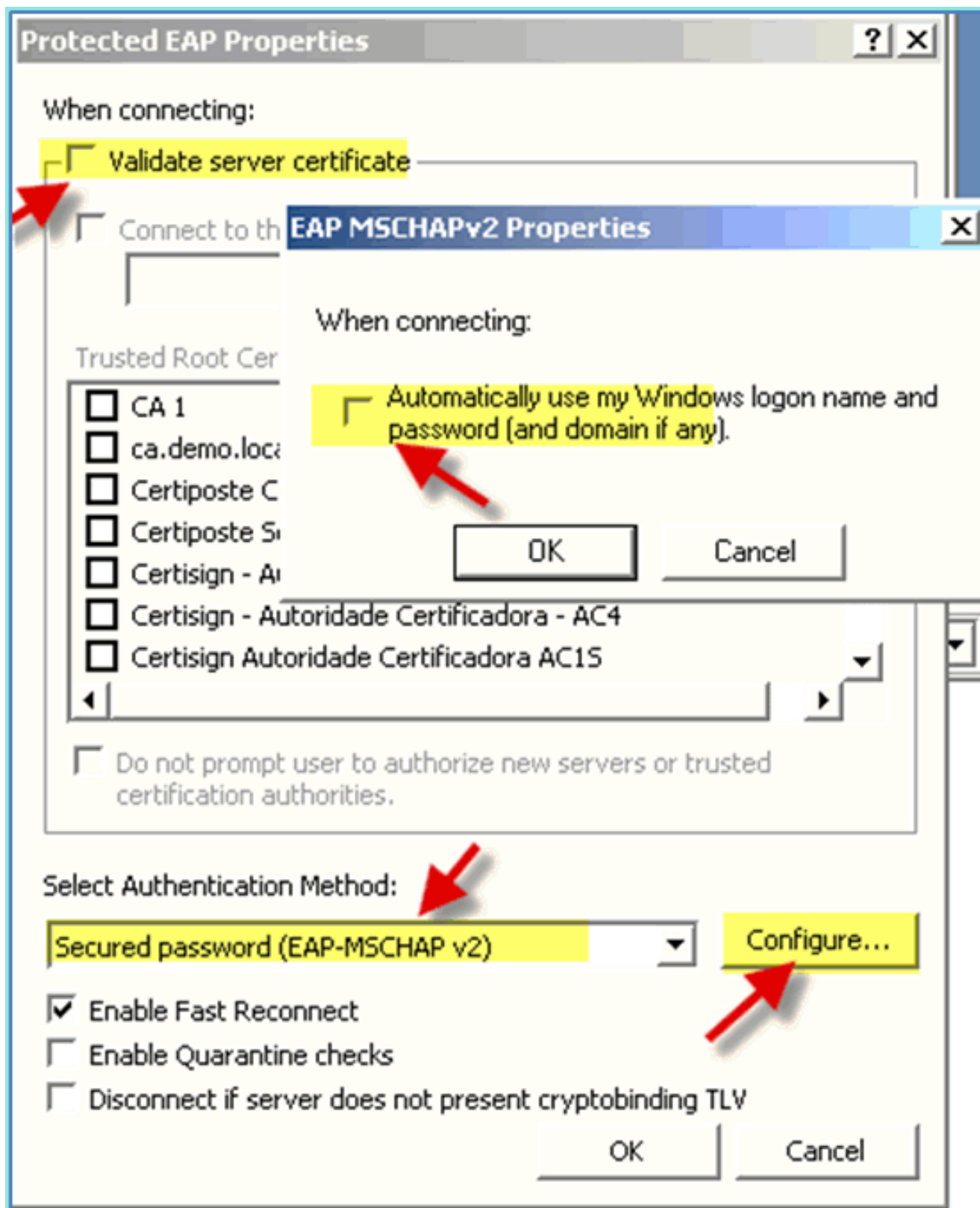


3. Accédez à l'onglet **Wireless Networks**. Sélectionnez le pod SSID network properties > Authentication tab > EAP type = Protected EAP (PEAP).



4. Cliquez sur Propriétés EAP.

5. Définissez les paramètres suivants : Valider le certificat du serveur : Désactivé
Méthode d'authentification : mot de passe sécurisé (EAP-MSCHAP v2)

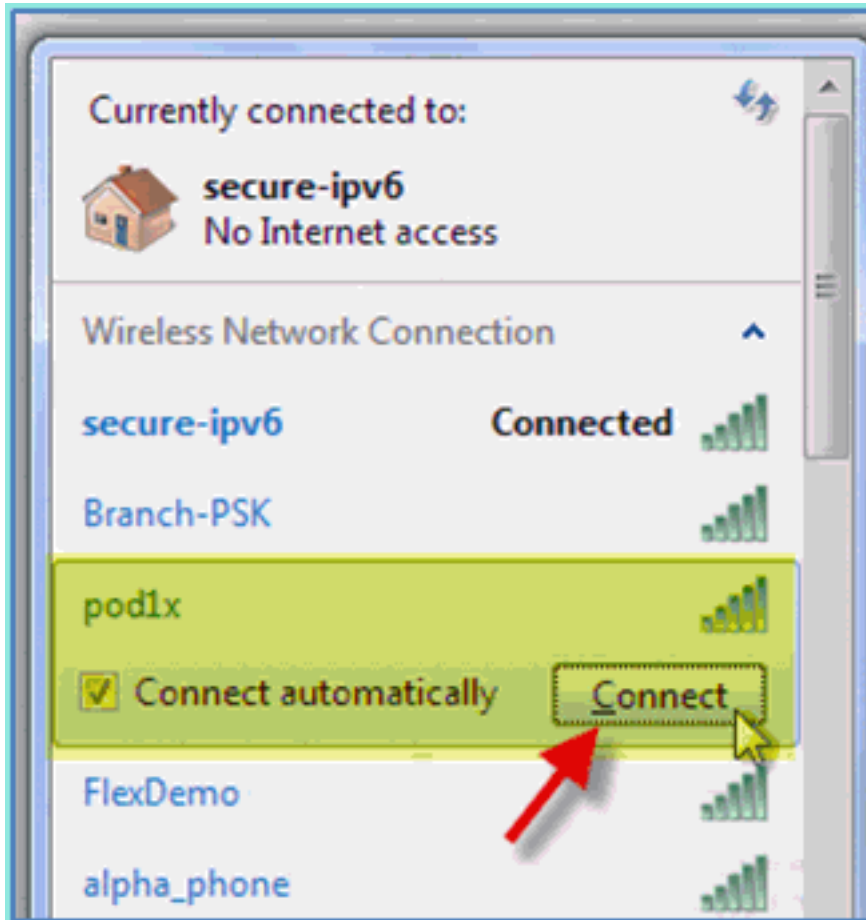


6. Cliquez sur **OK** dans toutes les fenêtres pour terminer cette tâche de configuration.
7. Le client Windows XP demande le nom d'utilisateur et le mot de passe. Dans cet exemple, il s'agit de aduser/XXXX.
8. Confirmez la connectivité réseau, l'adressage IP (v4).

[Référence : Authentification sans fil pour Microsoft Windows 7](#)

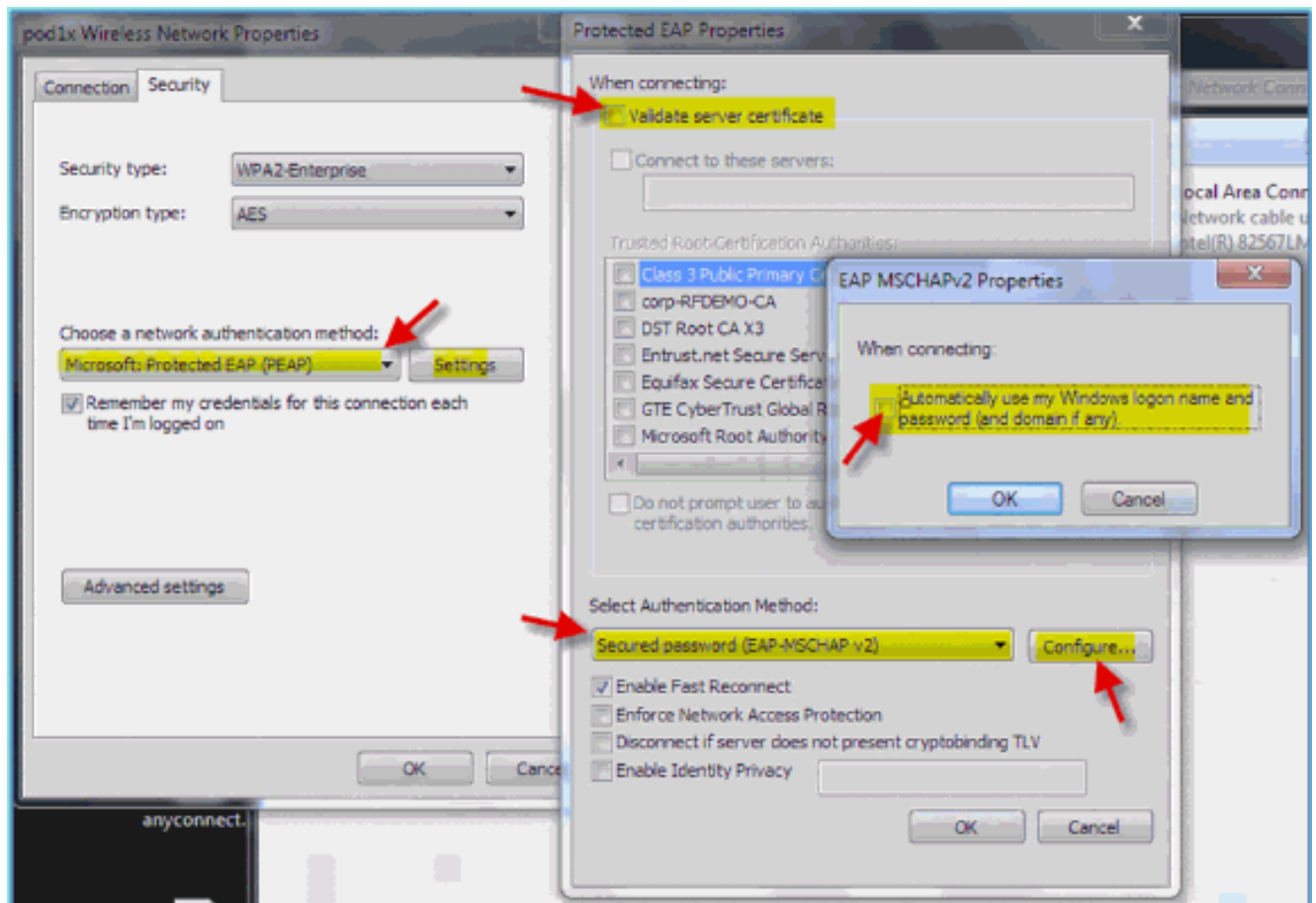
Associer au WLC via un SSID authentifié en tant qu'utilisateur INTERNE (ou utilisateur AD intégré) à l'aide d'un ordinateur portable sans fil Windows 7.

1. Sur l'ordinateur portable, accédez aux paramètres WLAN. Activez le WIFI et connectez-vous au SSID POD 802.1X créé dans l'exercice



précédent.

2. Accédez au Gestionnaire sans fil et modifiez le nouveau profil sans fil POD.
3. Définissez les paramètres suivants :
 - Méthode d'authentification : PEAP
 - Mémoriser mes informations d'identification... : Désactivé
 - Valider le certificat du serveur (paramètre avancé) : Désactivé
 - Méthode d'authentification (paramètres avancés) : EAP-MSCHAP v2
 - Utiliser automatiquement mon ouverture de session Windows... : Désactivé



Informations connexes

- [Assistance et documentation techniques - Cisco Systems](#)

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.