BYOD inalámbrico con Identity Services Engine

Contenido

Introducción

Cisco Identity Services Engine (ISE) es el servidor de políticas de última generación de Cisco que proporciona infraestructura de autenticación y autorización a la solución Cisco TrustSec. También proporciona otros dos servicios esenciales:

- El primer servicio consiste en proporcionar una forma de crear perfiles de tipo de dispositivo de terminal automáticamente en función de los atributos que Cisco ISE recibe de diversas fuentes de información. Este servicio (denominado Profiler) proporciona funciones equivalentes a las que Cisco ha ofrecido anteriormente con el dispositivo Cisco NAC Profiler.
- Otro servicio importante que proporciona Cisco ISE es analizar la conformidad de los terminales; por ejemplo, la instalación del software AV/AS y su validez de archivo de definición (conocida como estado). Cisco ha proporcionado anteriormente esta función de estado exacto solo con el dispositivo Cisco NAC.

Cisco ISE proporciona un nivel de funcionalidad equivalente y se integra con los mecanismos de autenticación 802.1X.

Cisco ISE integrado con controladores de LAN inalámbrica (WLC) puede proporcionar mecanismos de definición de perfiles de dispositivos móviles como iDevices de Apple (iPhone, iPad y iPod), smartphones basados en Android y otros. Para los usuarios de 802.1X, Cisco ISE puede proporcionar el mismo nivel de servicios, como la definición de perfiles y el análisis de estado. Los servicios para invitados de Cisco ISE también se pueden integrar con el WLC de Cisco redirigiendo las solicitudes de autenticación web a Cisco ISE para su autenticación.

Este documento presenta la solución inalámbrica para la iniciativa "Traiga su propio dispositivo" (BYOD), como proporcionar acceso diferenciado basado en terminales conocidos y en la política del usuario. Este documento no proporciona la solución completa de BYOD, pero sirve para demostrar un sencillo caso práctico de acceso dinámico. Otros ejemplos de configuración incluyen el uso del portal de patrocinadores de ISE, donde un usuario con privilegios puede patrocinar a un invitado para proporcionar acceso inalámbrico a invitados.

Prerequisites

Requirements

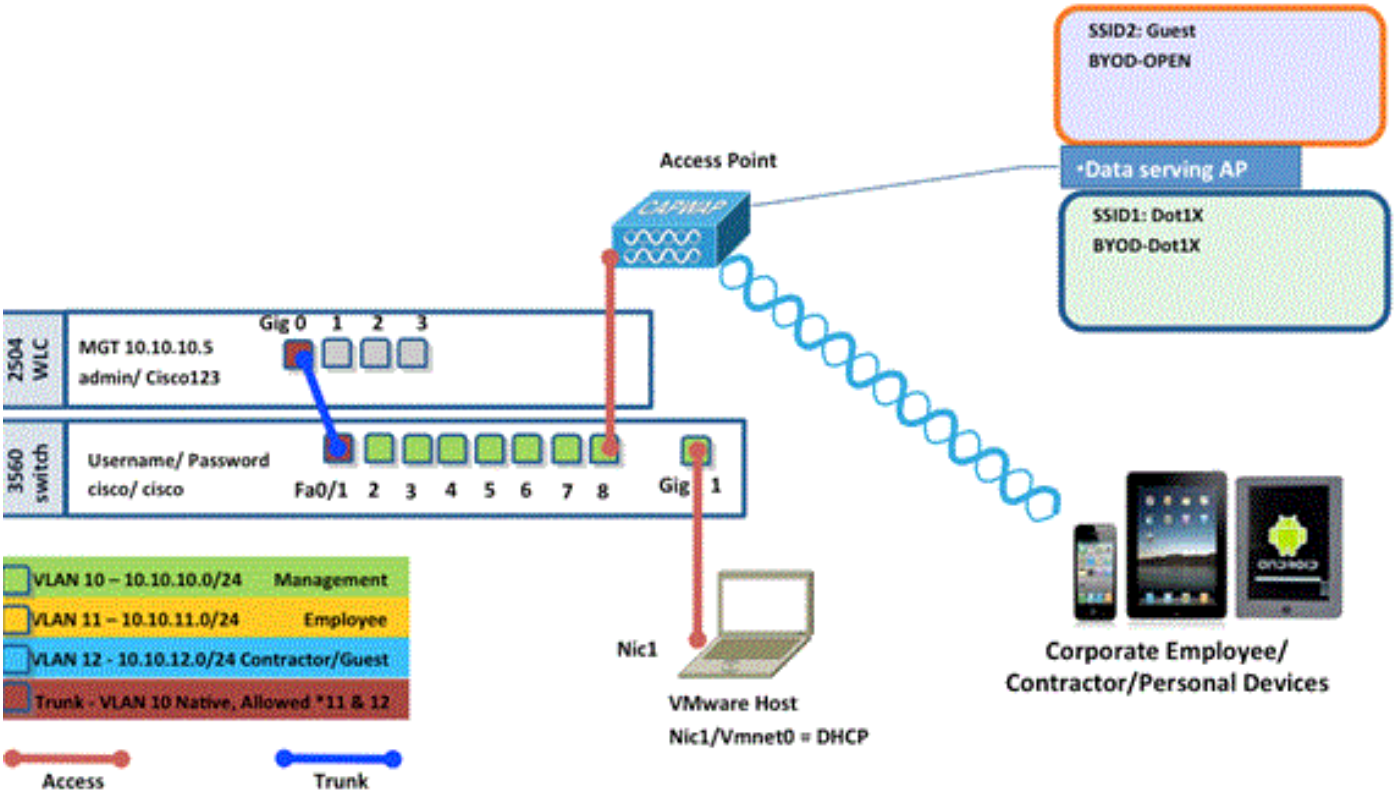
No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Wireless LAN Controller 2504 o 2106 con versión de software 7.2.103
- Catalyst 3560: 8 puertos
- WLC 2504
- Identity Services Engine 1.0MR (versión de imagen de servidor VMware)
- Windows 2008 Server (imagen de VMware): 512 MB, disco de 20 GBDirectorio activoDNSDHCPServicios de certificados

Topología



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)*

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Descripción general de RADIUS NAC y CoA del controlador de LAN inalámbrica

Esta configuración permite que el WLC busque los pares AV-Pairs de redirección URL que

provienen del servidor RADIUS de ISE. Esto es sólo en una WLAN que está ligada a una interfaz con el parámetro RADIUS NAC habilitado. Cuando se recibe el par AV de Cisco para la redirección URL, el cliente se pone en el estado POSTURE_REQD. Básicamente, esto es lo mismo que el estado WEBAUTH_REQD internamente en el controlador.

Cuando el servidor RADIUS de ISE considera que el cliente cumple con la condición, emite una ReAuth de CoA. Session_ID se utiliza para vincularlo entre sí. Con esta nueva AuthC (re-Auth) no envía los pares AV de URL-Redirect. Debido a que no hay URL Redirect AV-Pairs, el WLC sabe que el cliente ya no requiere Posture.

Si la configuración RADIUS NAC no está habilitada, el WLC ignora el VSA de redirección de URL.

CoA-ReAuth: Esto se habilita con la configuración RFC 3576. La capacidad ReAuth se agregó a los comandos CoA existentes que se admitían anteriormente.

El parámetro RADIUS NAC se excluye mutuamente de esta capacidad, aunque es necesario para que funcione el CoA.

ACL Pre-Postura: Cuando un cliente está en el estado POSTURE_REQ, el comportamiento predeterminado del WLC es bloquear todo el tráfico excepto DHCP/DNS. La ACL Pre-Postura (a la que se le llama en el par AV de url-redirect-acl) se aplica al cliente, y lo que se permite en esa ACL es lo que el cliente puede alcanzar.

ACL Pre-Auth vs. Anulación de VLAN: 7.0MR1 no admite una cuarentena o una VLAN de autenticación diferente de la VLAN de acceso. Si configura una VLAN desde el Policy Server, será la VLAN para toda la sesión. No se necesitan cambios de VLAN después de la primera autenticación.

Flujo de funciones de RADIUS NAC y CoA del controlador de LAN inalámbrica

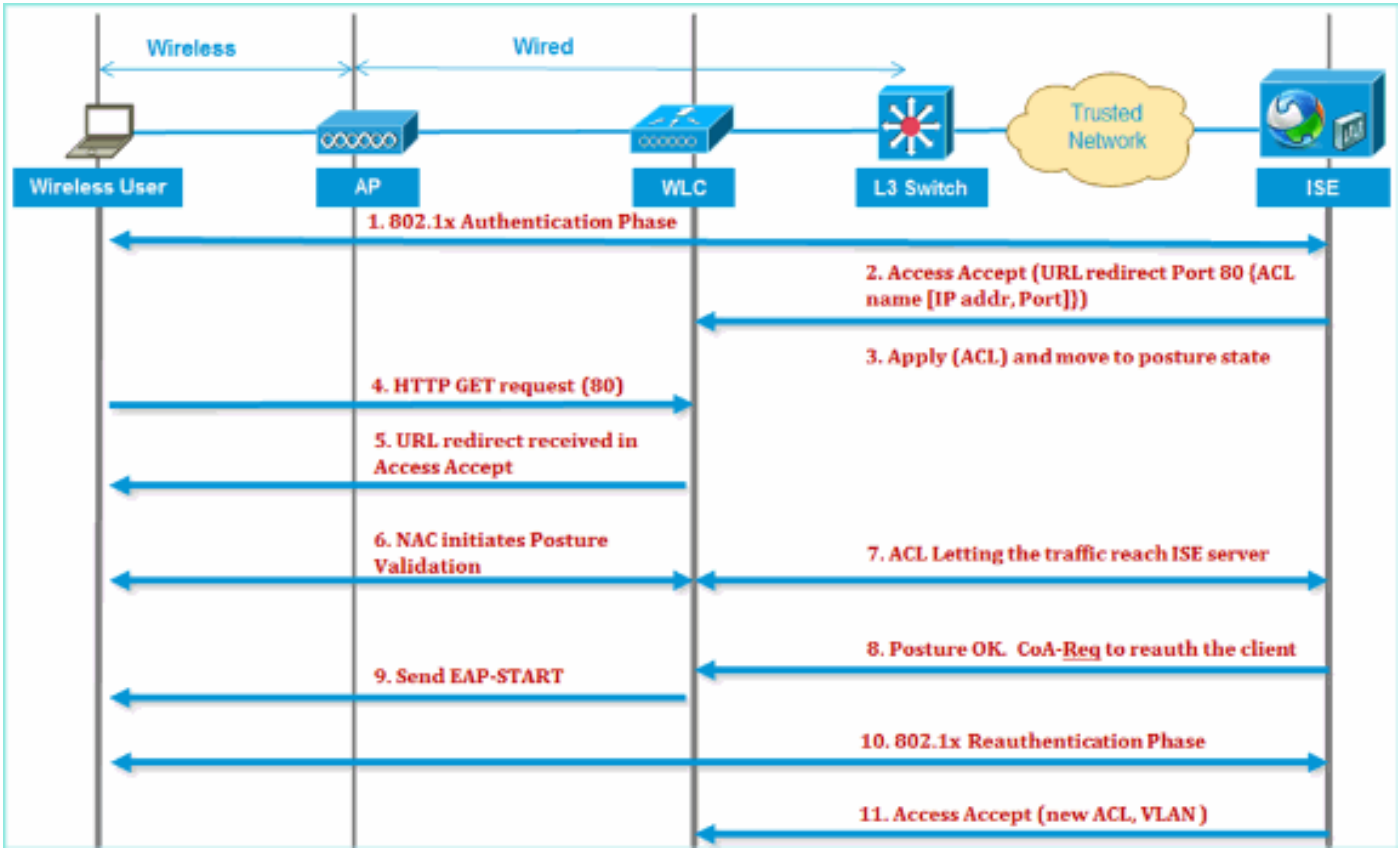
La siguiente figura proporciona detalles del intercambio de mensajes cuando el cliente se autentica en el servidor backend y la validación de estado de NAC.

1. El cliente autentica mediante la autenticación dot1x.
2. RADIUS Access Accept transporta la URL redirigida para el puerto 80 y las ACL previas a la autenticación que incluyen permitir direcciones IP y puertos, o poner en cuarentena VLAN.
3. El cliente será redirigido a la URL proporcionada en access accept, y se pondrá en un nuevo estado hasta que se realice la validación de estado. El cliente en este estado se comunica con el servidor ISE y se valida con las políticas configuradas en el servidor ISE NAC.
4. El agente NAC del cliente inicia la validación de estado (tráfico al puerto 80): el agente envía una solicitud de detección HTTP al puerto 80, que el controlador redirige a la URL proporcionada en la aceptación de acceso. El ISE sabe que el cliente está intentando ponerse en contacto con él y responde directamente. De esta manera, el cliente aprende acerca de la IP del servidor ISE y, a partir de ahora, el cliente habla directamente con el servidor ISE.
5. El WLC permite este tráfico porque la ACL está configurada para permitir este tráfico. En caso de anulación de VLAN, el tráfico se puentea de modo que llegue al servidor ISE.
6. Una vez que el cliente de ISE completa la evaluación, se envía una petición de CoA de RADIUS con el servicio de reautenticación al WLC. Esto inicia la reautenticación del cliente

(mediante el envío de EAP-START). Una vez que la reautenticación se realiza correctamente, ISE envía la aceptación de acceso con una nueva ACL (si la hay) y sin redirección de URL ni acceso a VLAN.

7. WLC tiene soporte para CoA-Req y Disconnect-Req según RFC 3576. El WLC necesita soportar CoA-Req para el servicio de reautenticación, según RFC 5176.
8. En lugar de las ACL descargables, las ACL preconfiguradas se utilizan en el WLC. El servidor ISE envía simplemente el nombre de ACL, que ya está configurado en el controlador.
9. Este diseño debería funcionar para los casos de VLAN y ACL. En caso de anulación de VLAN, simplemente redirigimos el puerto 80 y permite el resto (bridge) del tráfico en la VLAN de cuarentena. Para la ACL, se aplica la ACL previa a la autenticación recibida en la aceptación de acceso.

Esta figura proporciona una representación visual de este flujo de funciones:



Descripción general de ISE Profiling

El servicio Cisco ISE Profiler proporciona la funcionalidad necesaria para detectar, localizar y determinar las capacidades de todos los terminales conectados de la red, independientemente del tipo de dispositivo, con el fin de garantizar y mantener un acceso adecuado a la red de la empresa. Recopila principalmente un atributo o un conjunto de atributos de todos los terminales de la red y los clasifica según sus perfiles.

El generador de perfiles consta de los siguientes componentes:

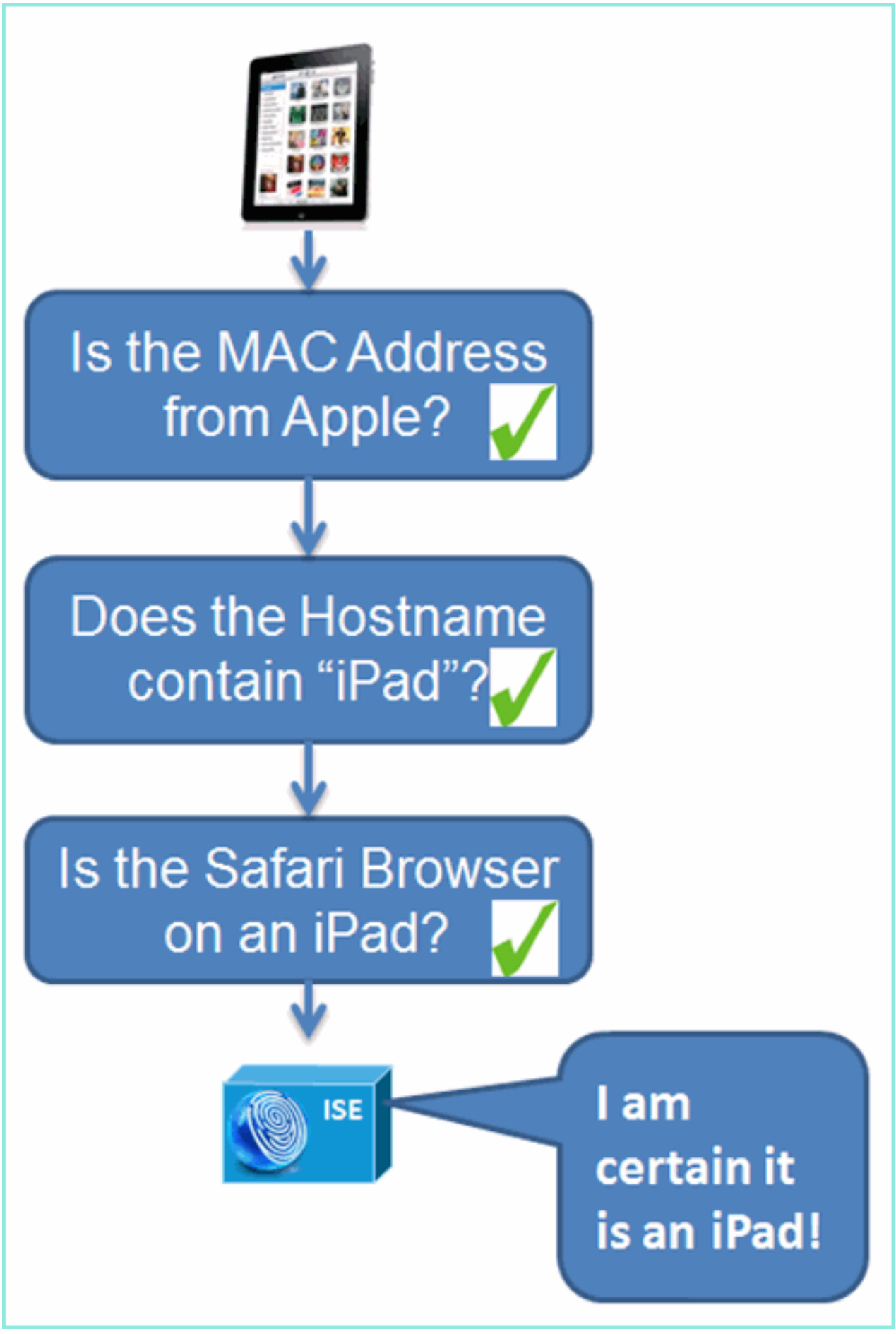
- El sensor contiene una serie de sondas. Los sondeos capturan paquetes de red consultando a los dispositivos de acceso a la red y reenvían los atributos y sus valores de atributo que se recopilan de los terminales al analizador.

- Un analizador evalúa los terminales utilizando las políticas configuradas y los grupos de identidad para hacer coincidir los atributos y sus valores de atributo recopilados, lo que clasifica los terminales en el grupo especificado y almacena los terminales con el perfil coincidente en la base de datos de Cisco ISE.

Para la detección de dispositivos móviles, se recomienda utilizar una combinación de estas sondas para la identificación correcta del dispositivo:

- RADIUS (ID de la estación de llamada): proporciona la dirección MAC (OUI)
- DHCP (nombre de host): nombre de host; el nombre de host predeterminado puede incluir el tipo de dispositivo; por ejemplo: jsmith-ipad
- DNS (búsqueda de IP inversa): FQDN; el nombre de host predeterminado puede incluir el tipo de dispositivo
- HTTP (agente de usuario): detalles sobre un tipo de dispositivo móvil específico

En este ejemplo de un iPad, el generador de perfiles captura la información del navegador web del atributo User-Agent, así como otros atributos HTTP de los mensajes de solicitud, y los agrega a la lista de atributos de punto final.



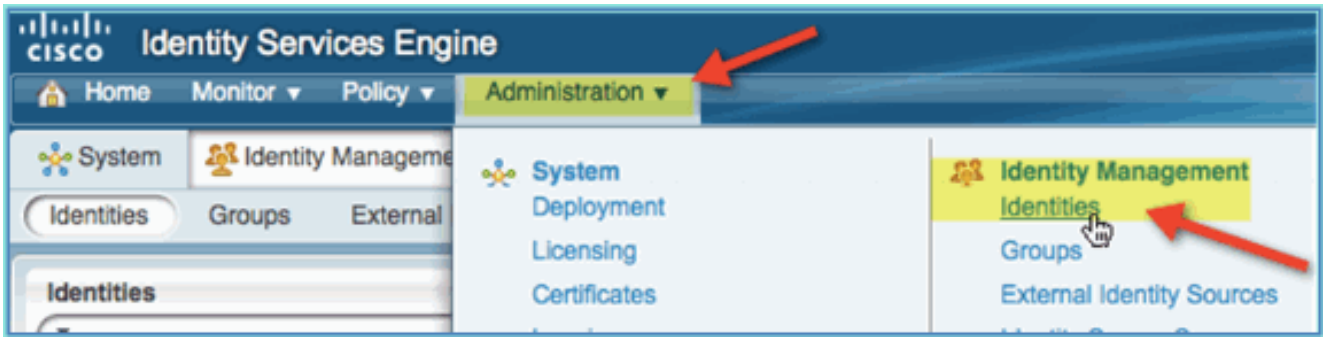
[Crear usuarios de identidad interna]

MS Active Directory (AD) no es necesario para una prueba de concepto sencilla. ISE se puede utilizar como único almacén de identidades, lo que incluye la diferenciación del acceso de los usuarios para el control granular de políticas y el acceso.

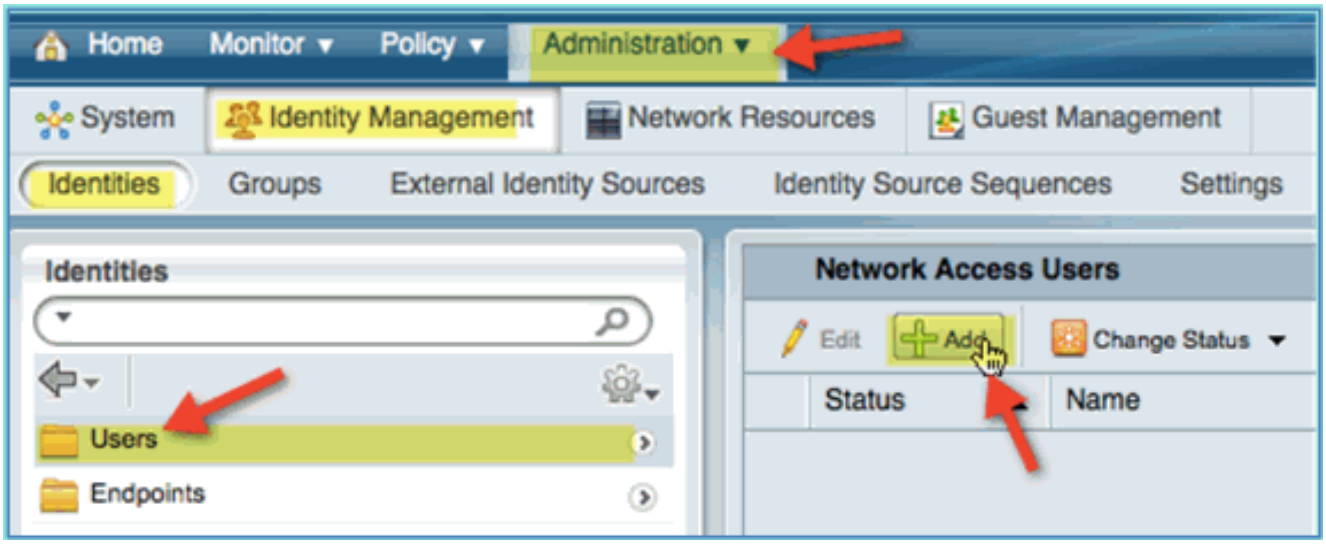
Con el lanzamiento de ISE 1.0, mediante la integración de AD, ISE puede utilizar grupos de AD en las políticas de autorización. Si se utiliza el almacén interno de usuarios de ISE (sin integración de AD), no se pueden usar grupos en políticas junto con grupos de identidad de dispositivos (el error identificado se resolverá en ISE 1.1). Por lo tanto, solo se pueden diferenciar los usuarios individuales, como los empleados o contratistas, cuando se utilizan además de los grupos de identidad de dispositivos.

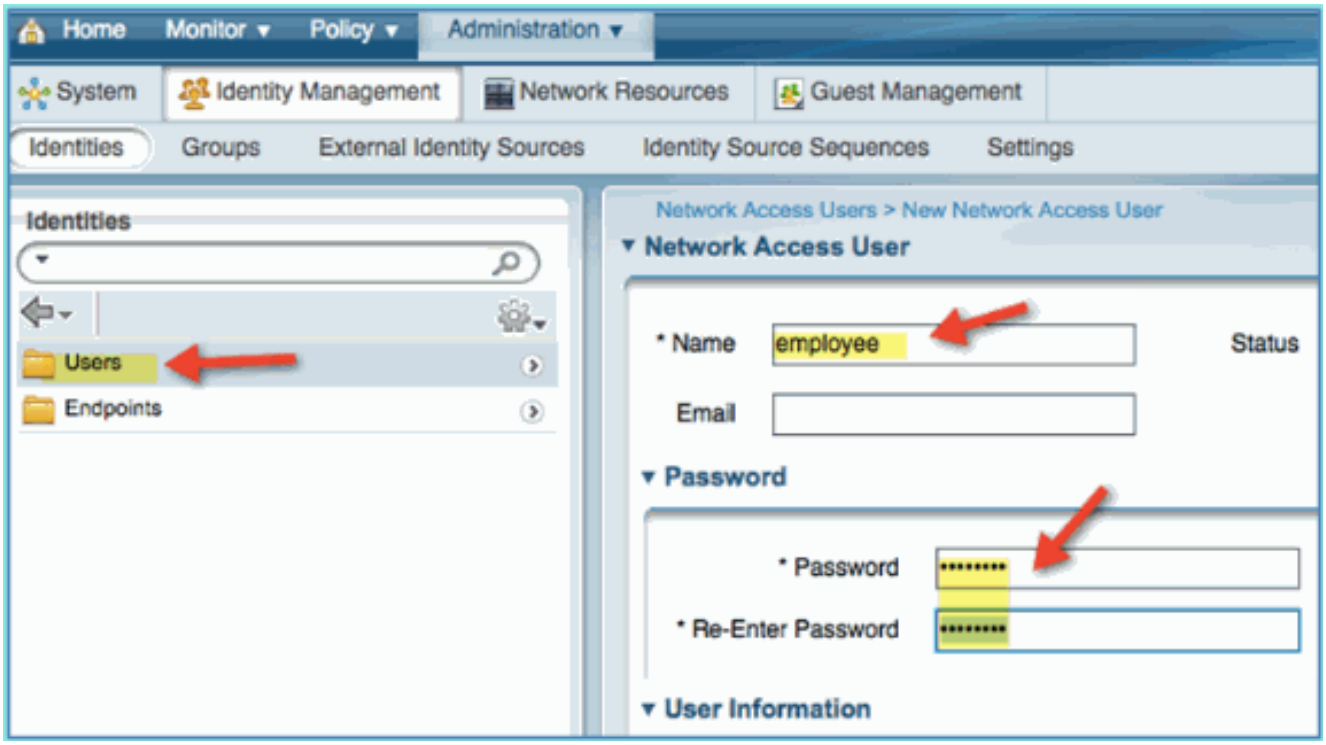
Complete estos pasos:

1. Abra una ventana del navegador a la dirección https://ISEip.
2. Vaya a **Administration > Identity Management > Identities**.

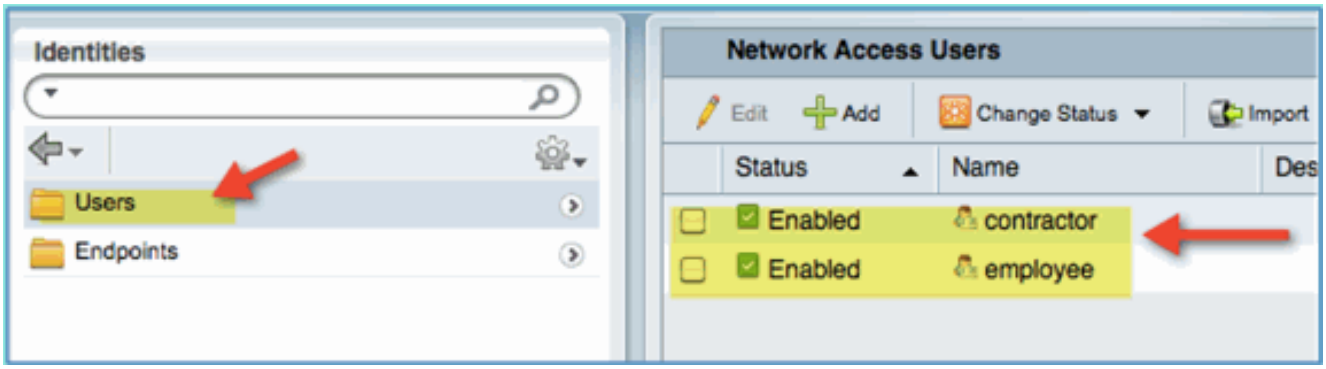


3. Seleccione **Users** y, a continuación, haga clic en **Add** (Network Access User). Introduzca estos valores de usuario y asígnelos al grupo Empleado:Nombre: empleadoContraseña: XXXX





4. Haga clic en Submit (Enviar).Nombre: contratistaContraseña: XXXX
5. Confirme que se han creado ambas cuentas.



Adición de un controlador de LAN inalámbrica a ISE

Cualquier dispositivo que inicie solicitudes RADIUS a ISE debe tener una definición en ISE. Estos dispositivos de red se definen en función de su dirección IP. Las definiciones de dispositivos de red de ISE pueden especificar intervalos de direcciones IP, lo que permite que la definición represente varios dispositivos reales.

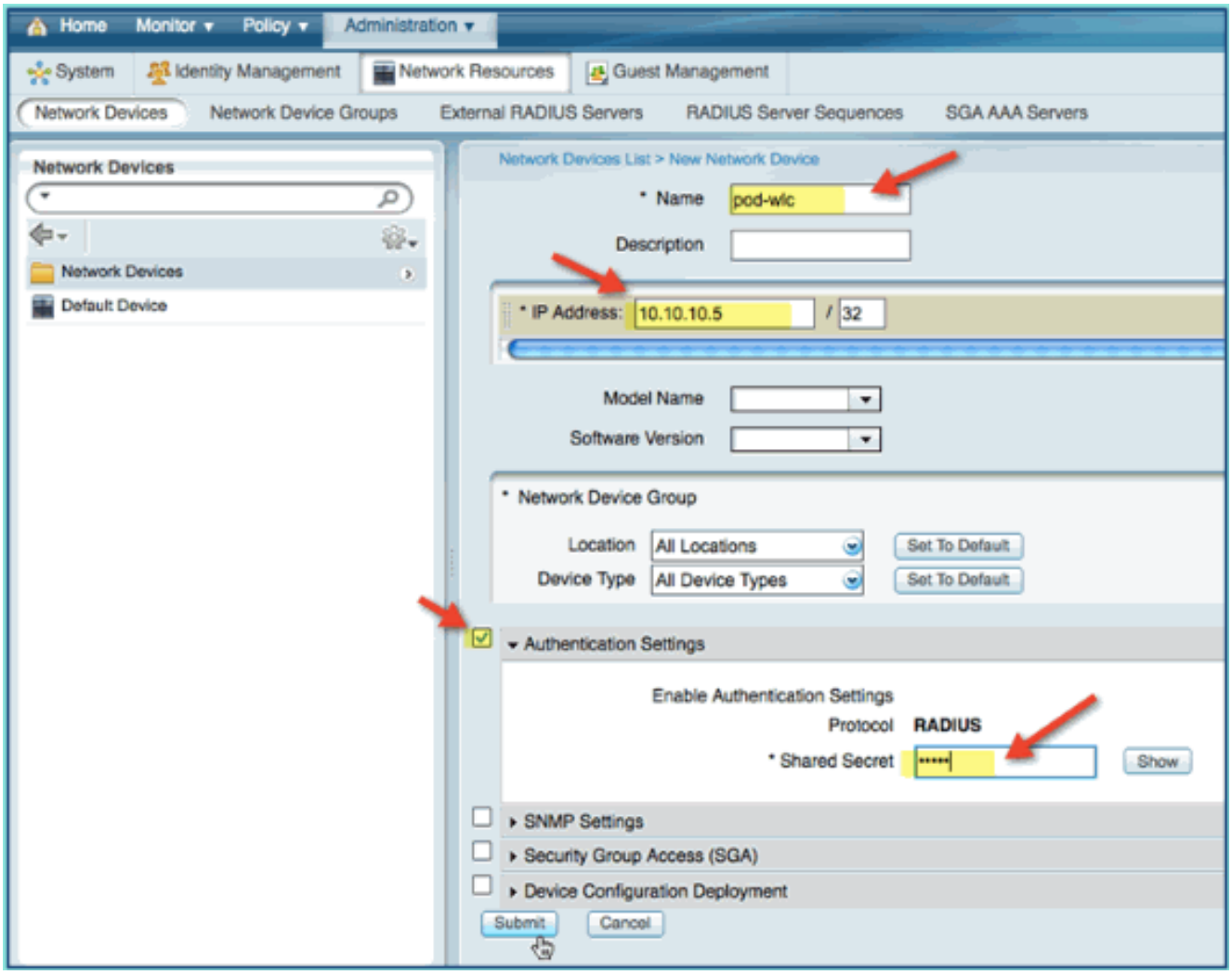
Más allá de lo necesario para la comunicación RADIUS, las definiciones de dispositivos de red ISE contienen ajustes para otras comunicaciones ISE/dispositivos, como SNMP y SSH.

Otro aspecto importante de la definición de dispositivos de red es la agrupación adecuada de dispositivos para que esta agrupación pueda aprovecharse en la política de acceso a la red.

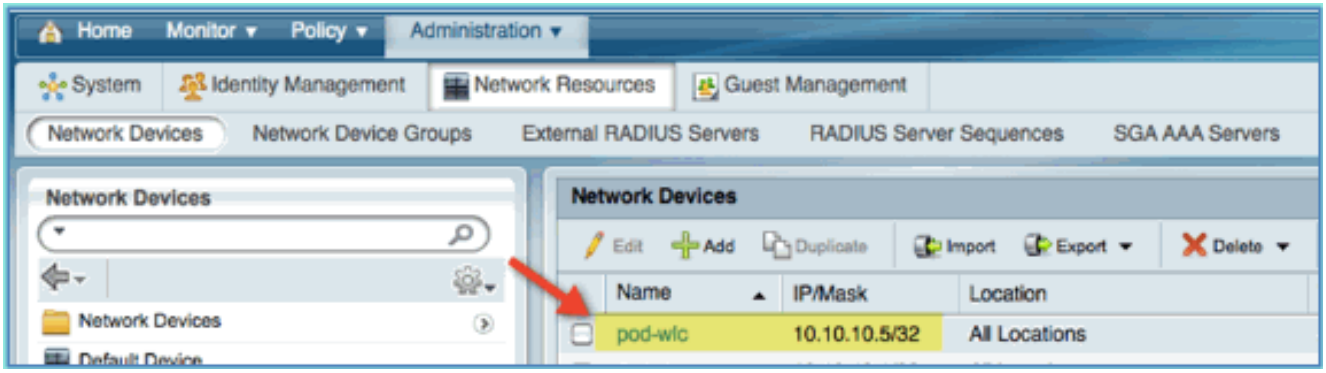
En este ejercicio, se configuran las definiciones de dispositivos requeridas para su laboratorio.

Complete estos pasos:

1. En ISE, vaya a **Administration > Network Resources > Network Devices**.



2. En Dispositivos de red, haga clic en **Agregar**. Introduzca la dirección IP, la máscara compruebe la configuración de autenticación y, a continuación, introduzca 'cisco' para el secreto compartido.
3. Guarde la entrada del WLC, y confirme el controlador en la lista.



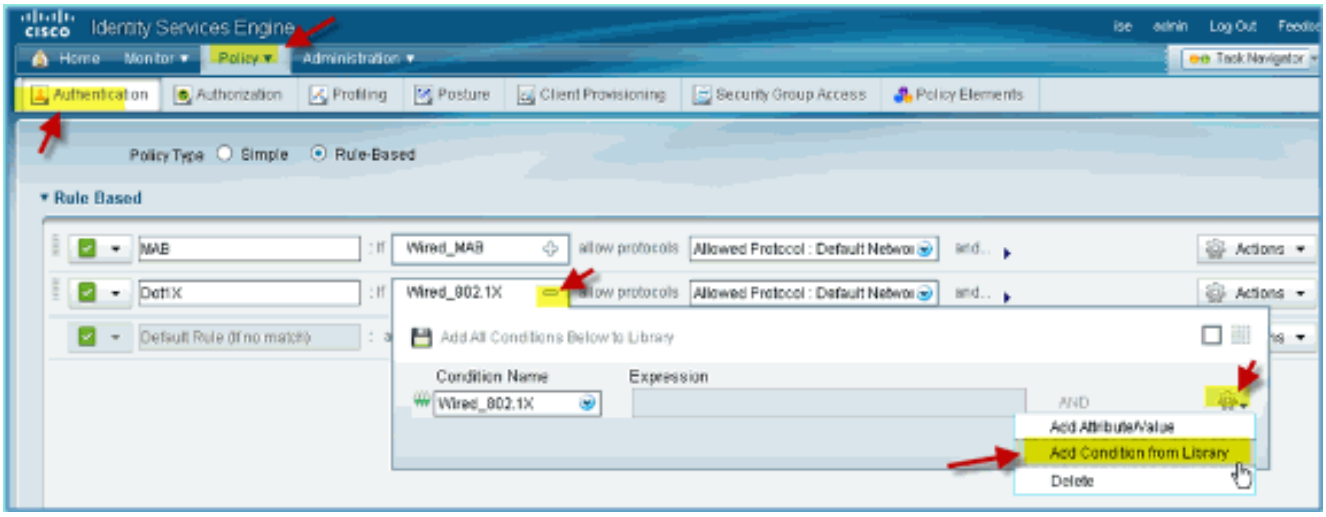
Configuración de ISE para la autenticación inalámbrica

ISE debe configurarse para autenticar clientes inalámbricos 802.1x y para utilizar Active Directory como almacén de identidades.

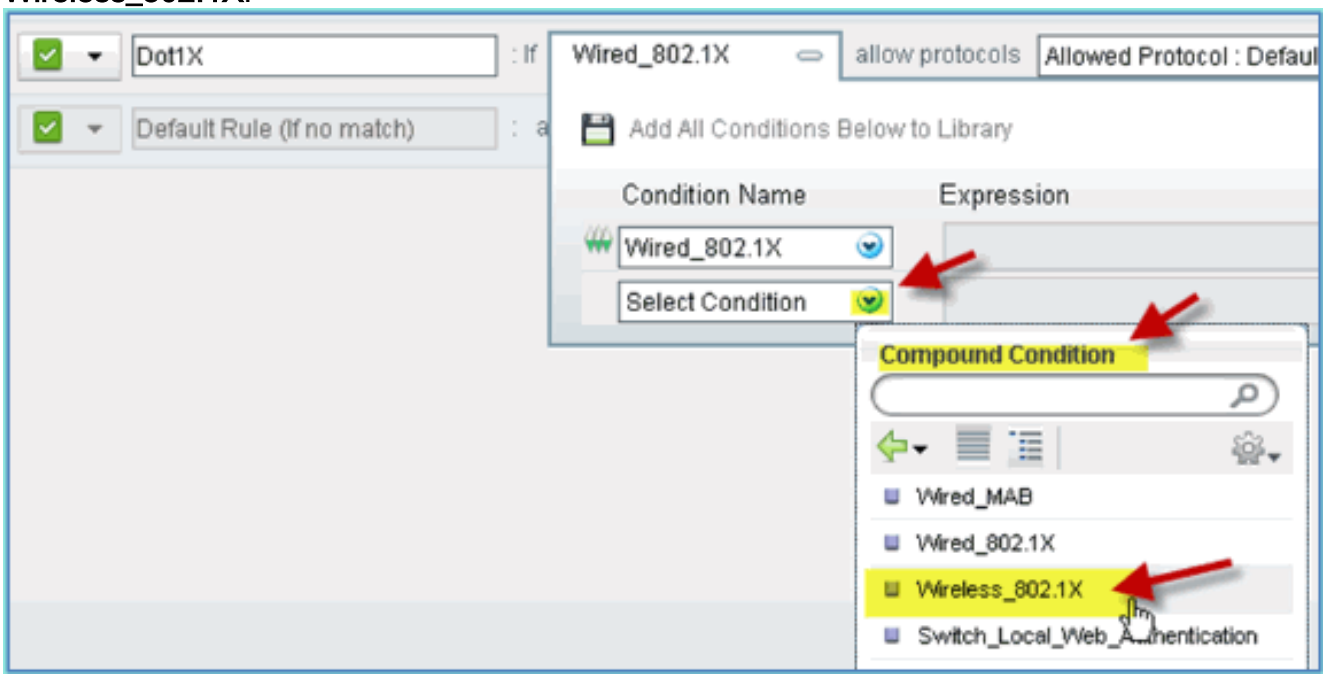
Complete estos pasos:

1. En ISE, vaya a **Policy > Authentication**.
2. Haga clic para expandir Punto1x > Con cables_802.1X (-).

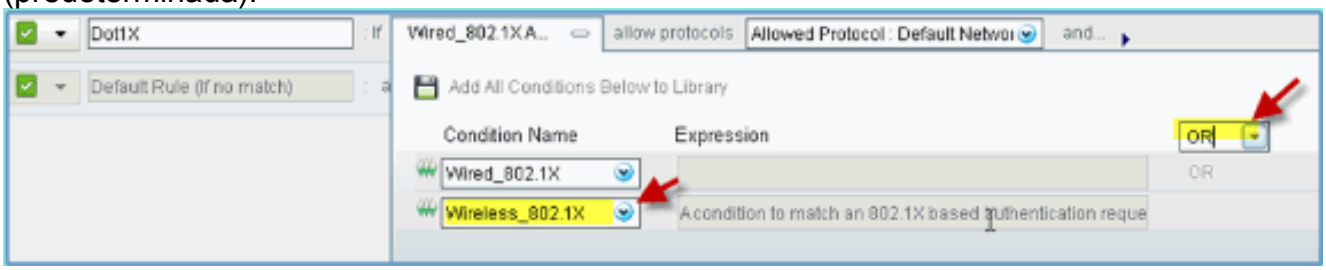
3. Haga clic en el icono del engranaje para **Agregar condición desde la biblioteca**.

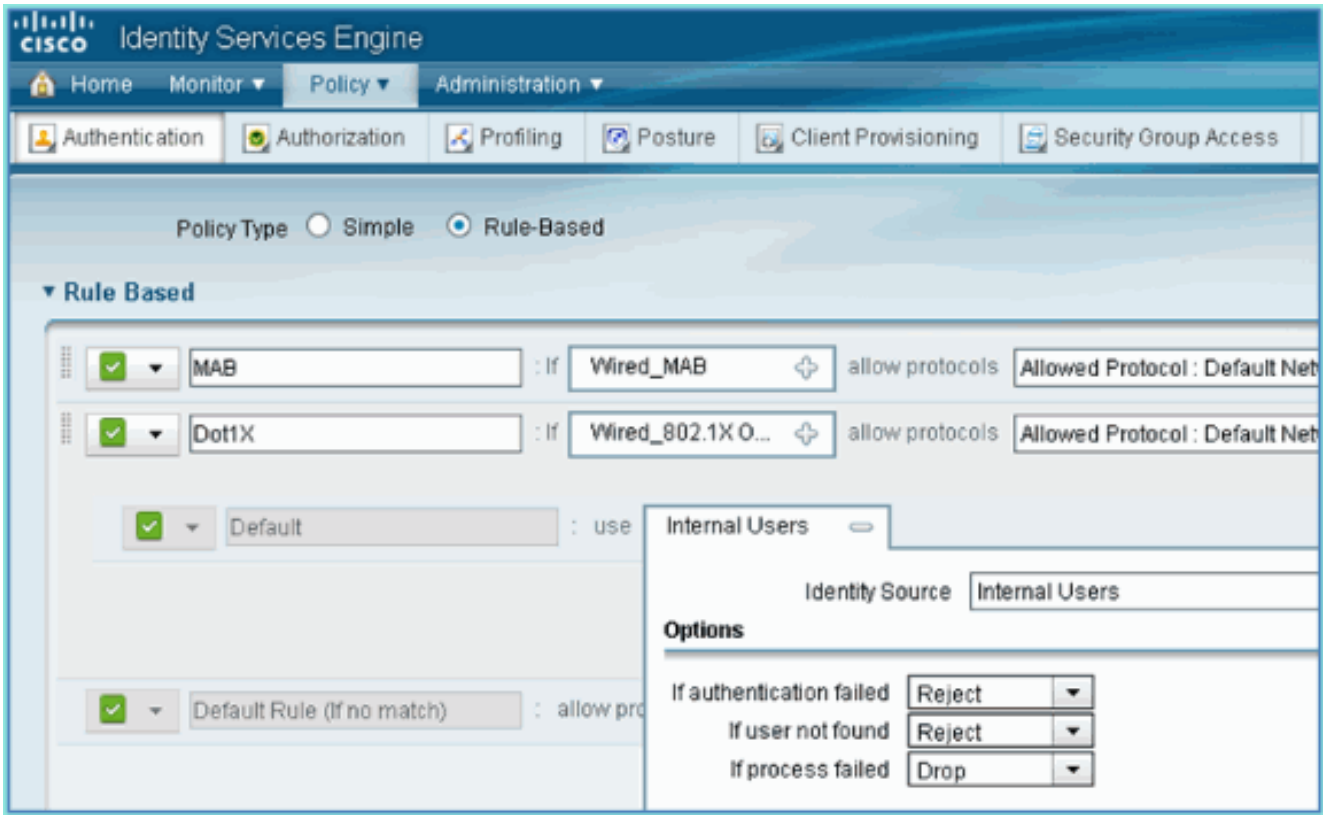


4. En el menú desplegable de selección de condiciones, elija **Condición compuesta > Wireless_802.1X**.



5. Establezca la condición Express en **OR**.
6. Expanda la opción después de permitir protocolos y acepte la opción predeterminada Usuarios internos (predeterminada).





7. Deje todo lo demás en modo predeterminado. Haga clic en **Guardar** para completar los pasos.

Controlador de LAN inalámbrica Bootstrap

Conexión del WLC a una red

La guía de implementación de Cisco 2500 Wireless LAN Controller también está disponible en la Guía de implementación de Cisco 2500 Series Wireless Controller.

Configurar el controlador mediante el Asistente para inicio

```
(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.
```

Configuración del switch vecino

El controlador está conectado al puerto Ethernet del switch vecino (Fast Ethernet 1). El puerto del switch vecino se configura como un trunk 802.1Q y permite todas las VLAN en el trunk. La VLAN 10 nativa permite que se conecte la interfaz de administración del WLC.

La configuración del puerto del switch 802.1Q es la siguiente:

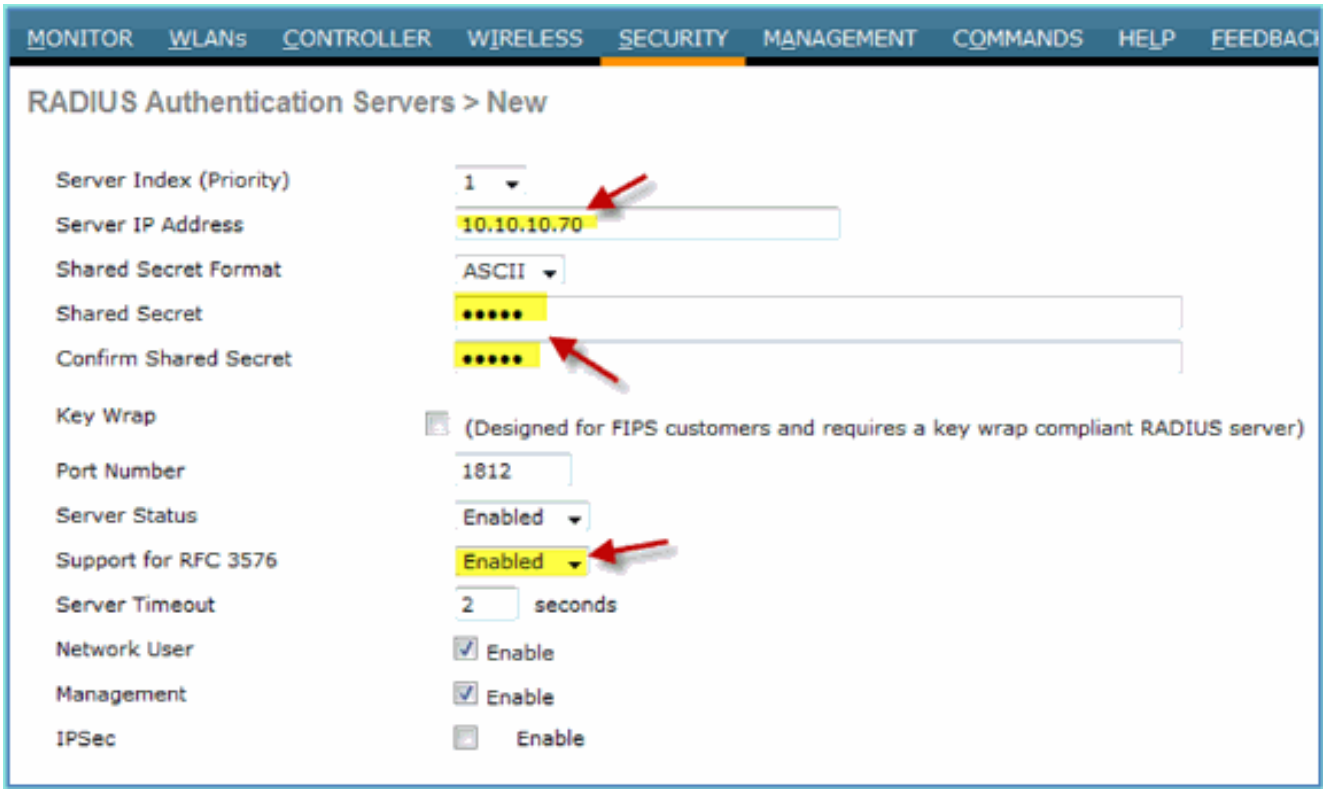
```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

Agregar servidores de autenticación (ISE) al WLC

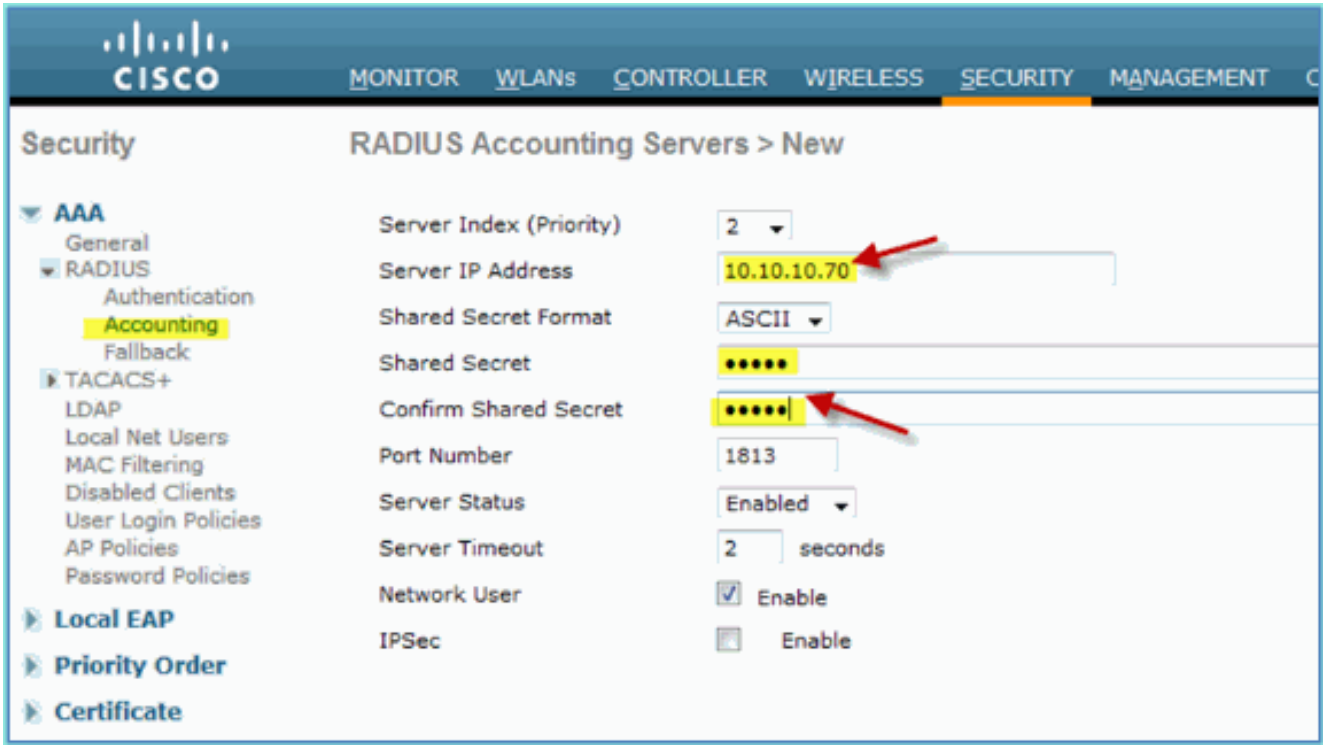
Es necesario agregar ISE al WLC para habilitar 802.1X y la función CoA para los terminales inalámbricos.

Complete estos pasos:

1. Abra un navegador, luego conéctese al POD WLC (usando HTTP seguro) > https://wlc.
2. Vaya a **Seguridad > Autenticación >**
   Nuevo.



3. Introduzca estos valores:Dirección IP del servidor: 10.10.10.70 (comprobar asignación)Secreto compartido: CiscoCompatibilidad con RFC 3576 (CoA): habilitado (predeterminado)Todo lo demás: Predeterminado
4. Haga clic en **Apply** para continuar.
5. Seleccione **RADIUS Accounting > add NEW**.

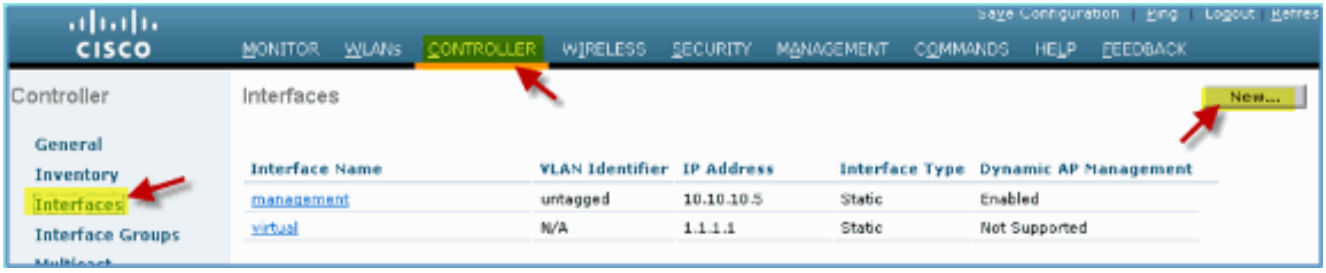


6. Introduzca estos valores:Dirección IP del servidor: 10.10.10.70Secreto compartido: CiscoTodo lo demás: Predeterminado
7. Haga clic en **Aplicar**, después guarde la configuración para el WLC.

Crear interfaz dinámica de empleado de WLC

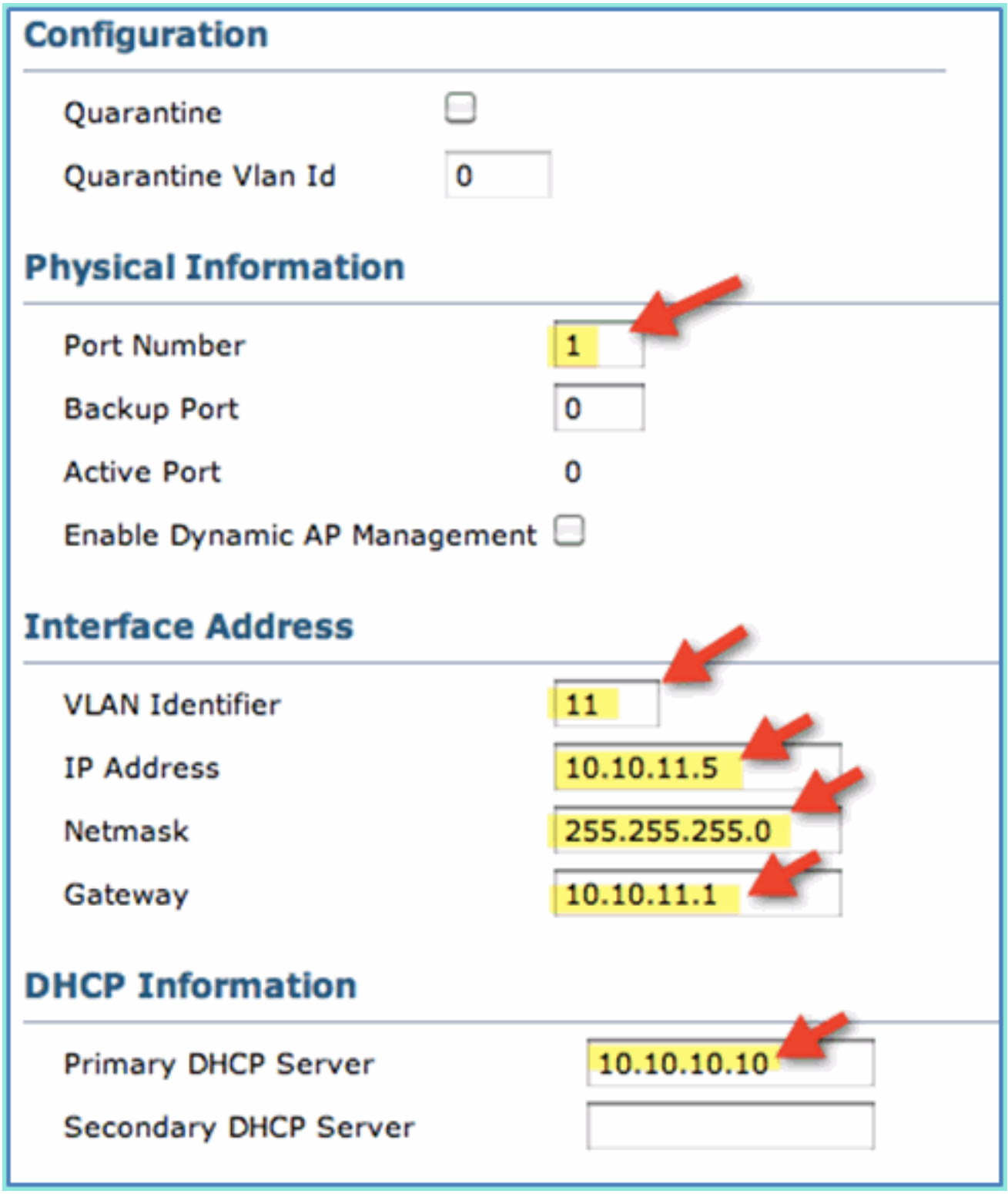
Complete estos pasos para agregar una nueva interfaz dinámica para el WLC y asignarla a la VLAN del empleado:

1. Desde el WLC, navegue hasta **Controlador > Interfaces**. A continuación, haga clic en **Nuevo**.



2. Desde el WLC, navegue hasta **Controlador > Interfaces**. Introduzca lo siguiente:Nombre de interfaz: EmpleadoID de VLAN:
   11

3. Introduzca lo siguiente para la interfaz de empleado:Número de puerto: 1Identificador de VLAN: 11Dirección IP: 10.10.11.5Máscara de red: 255.255.255.0Gateway: 10.10.11.1DHCP: 10.10.10.10

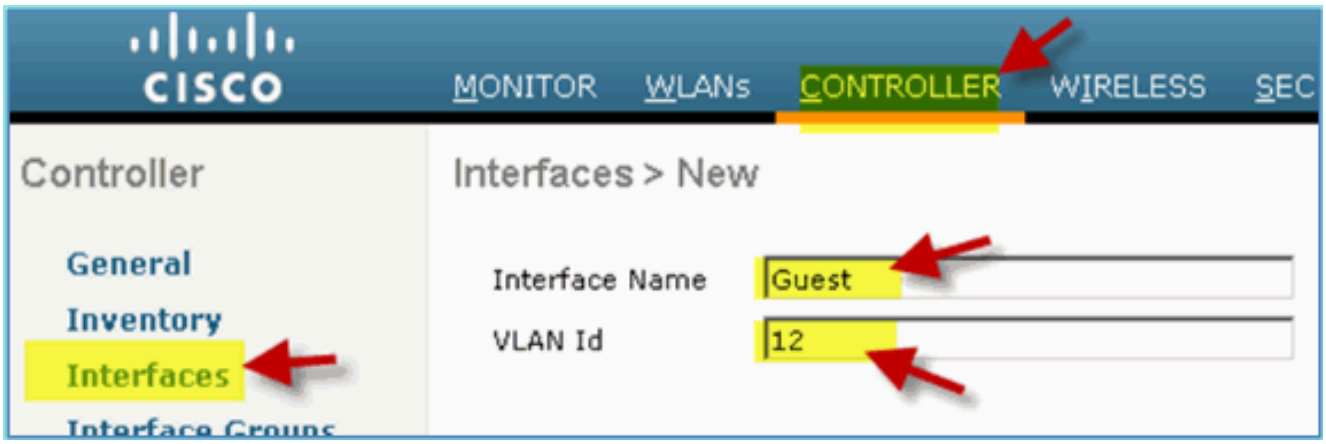


4. Confirme que se ha creado la nueva interfaz dinámica de empleado.

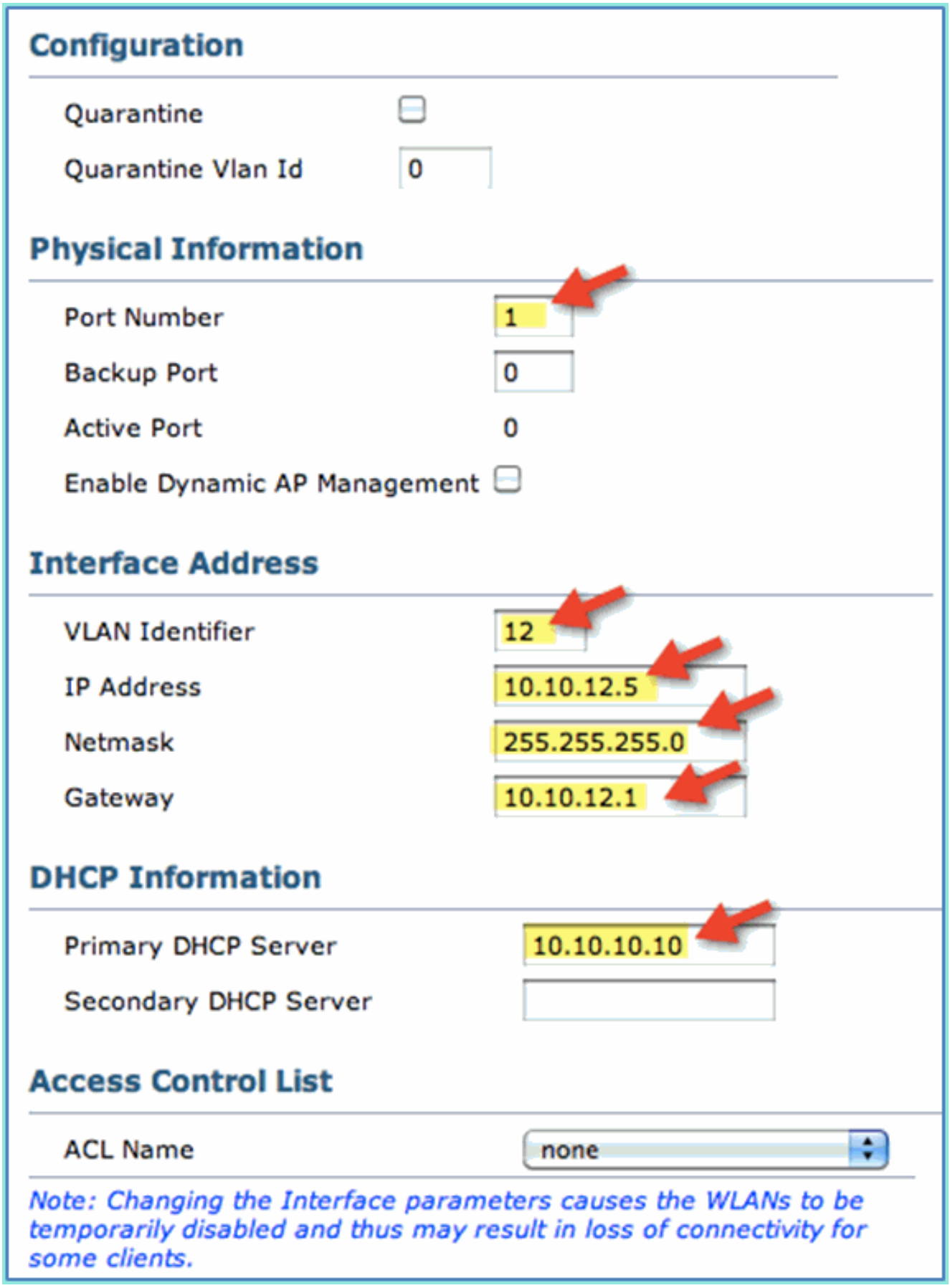
Crear interfaz dinámica de invitado WLC

Complete estos pasos para agregar una nueva interfaz dinámica para el WLC y lo mapee a la VLAN de invitado:

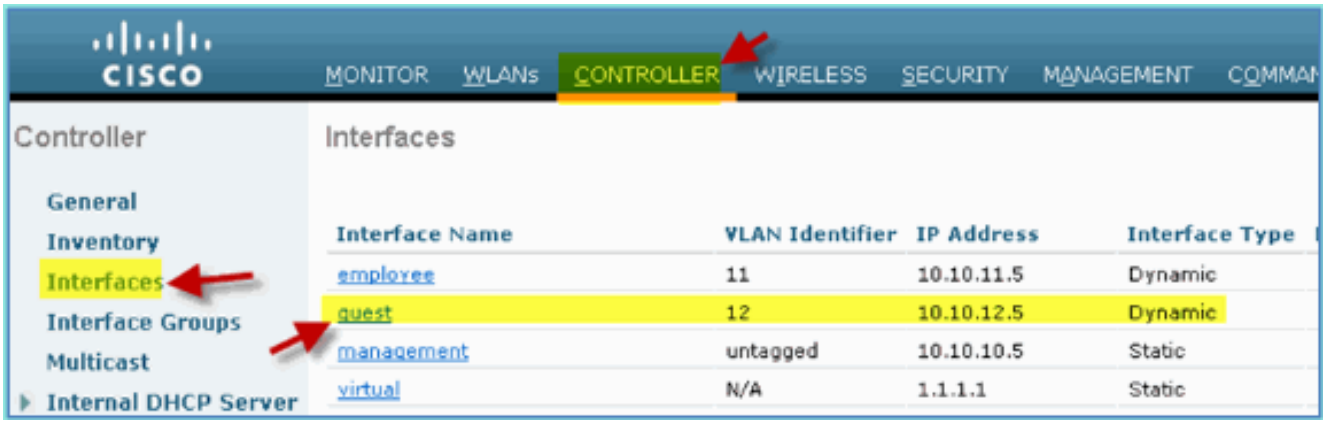
1. Desde el WLC, navegue hasta **Controlador > Interfaces**. A continuación, haga clic en **Nuevo**.
2. Desde el WLC, navegue hasta **Controlador > Interfaces**. Introduzca lo siguiente:Nombre de interfaz: InvitadoID de VLAN:
   12



3. Introduzca estos datos para la interfaz de invitado:Número de puerto: 1Identificador de VLAN: 12Dirección IP: 10.10.12.5Máscara de red: 255.255.255.0Gateway: 10.10.12.1DHCP: 10.10.10.10



4. Confirme que se ha agregado la interfaz de invitado.



Agregar WLAN 802.1x

Desde el bootstrap inicial del WLC, pudo haber habido una WLAN predeterminada creada. Si es así, modifíquela o cree una nueva WLAN para admitir la autenticación inalámbrica 802.1X tal y como se indica en la guía.

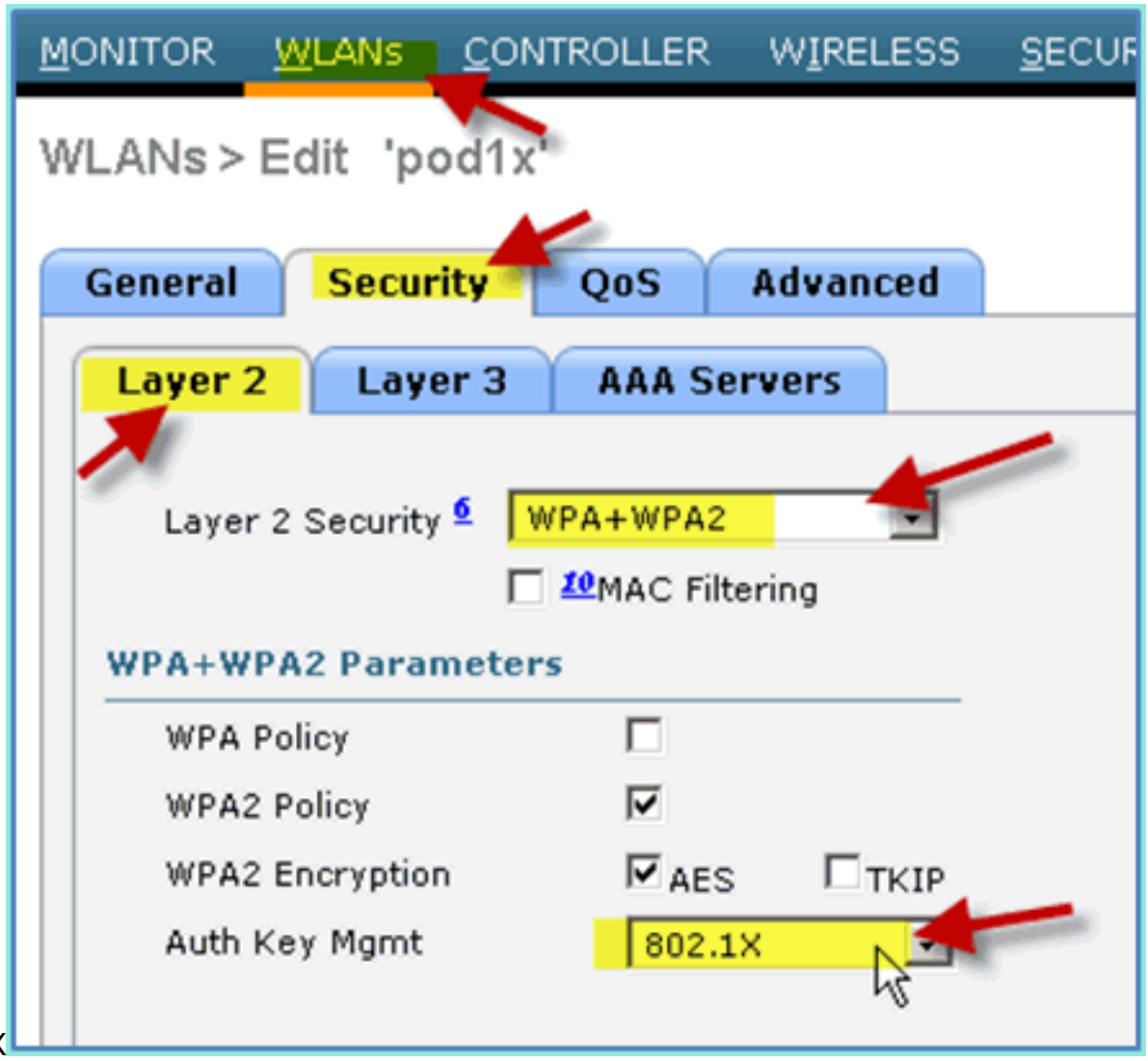
Complete estos pasos:

1. Desde WLC, navegue hasta **WLAN > Create New**.

2. Para la WLAN, introduzca lo siguiente:Nombre del perfil: pod1xSSID: Mismo

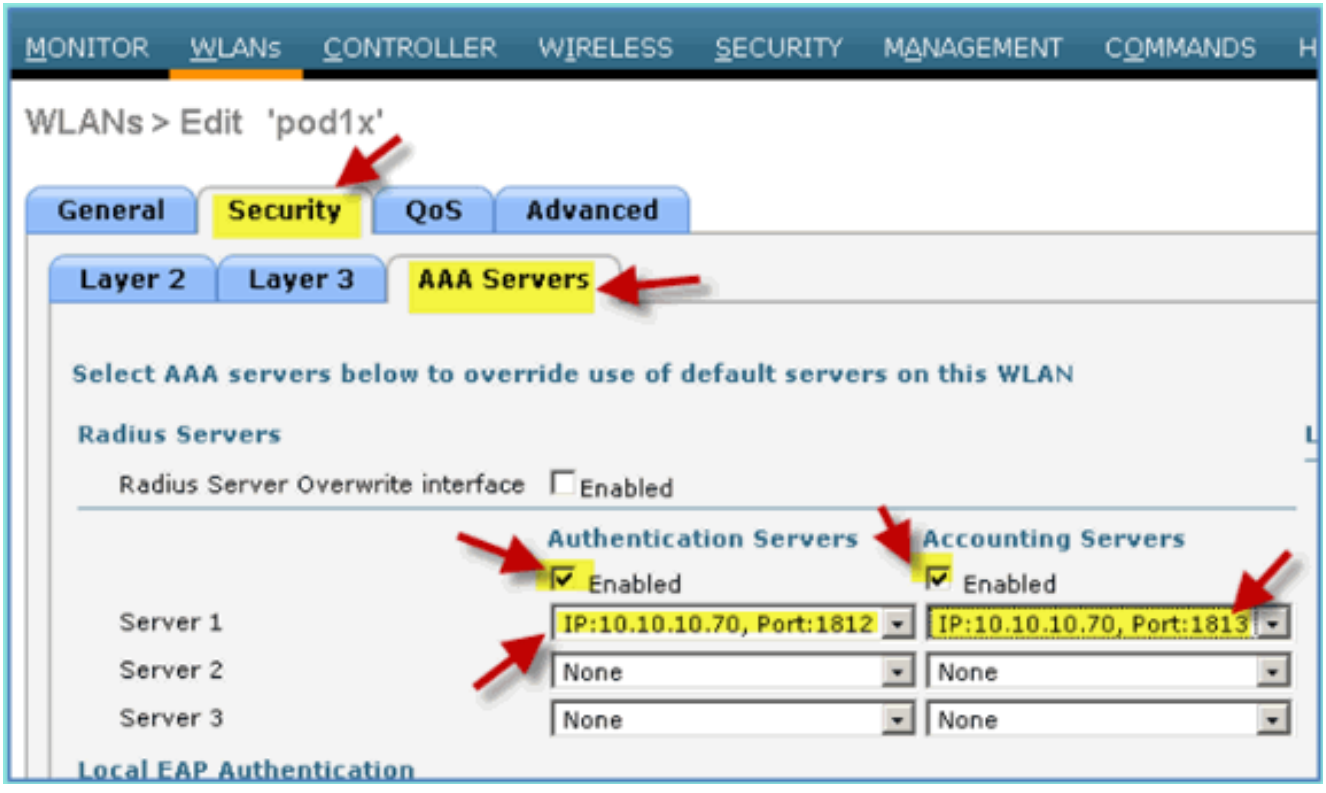
3. Para la ficha WLAN settings > General (Parámetros de WLAN > General), utilice lo siguiente:Política de radio: todosInterfaz/Grupo: gestiónTodo lo demás: por defecto

4. Para la ficha WLAN > Security > Layer 2 (WLAN > Seguridad > Capa 2), establezca lo siguiente:Seguridad de capa 2:WPA+WPA2Política/cifrado WPA2: habilitado/AESGestión de claves de autenticación:

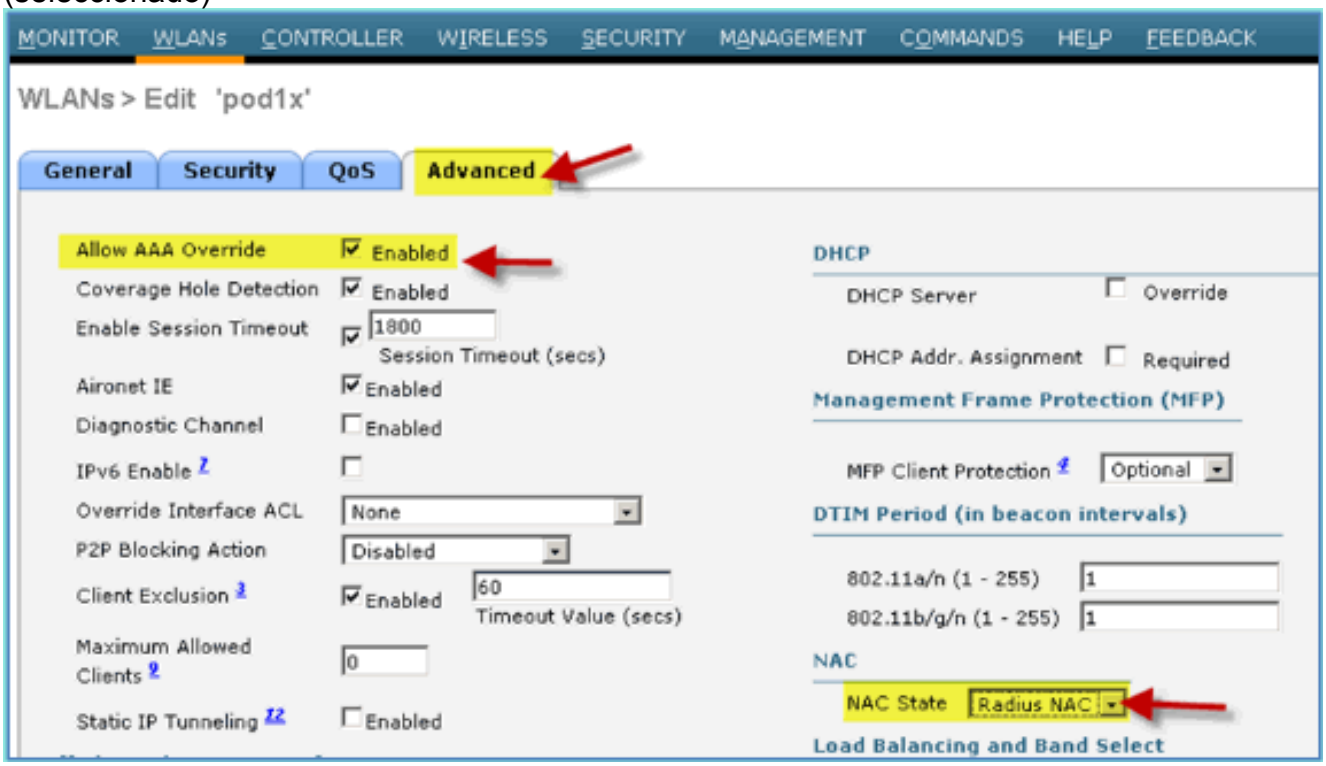


802.1X

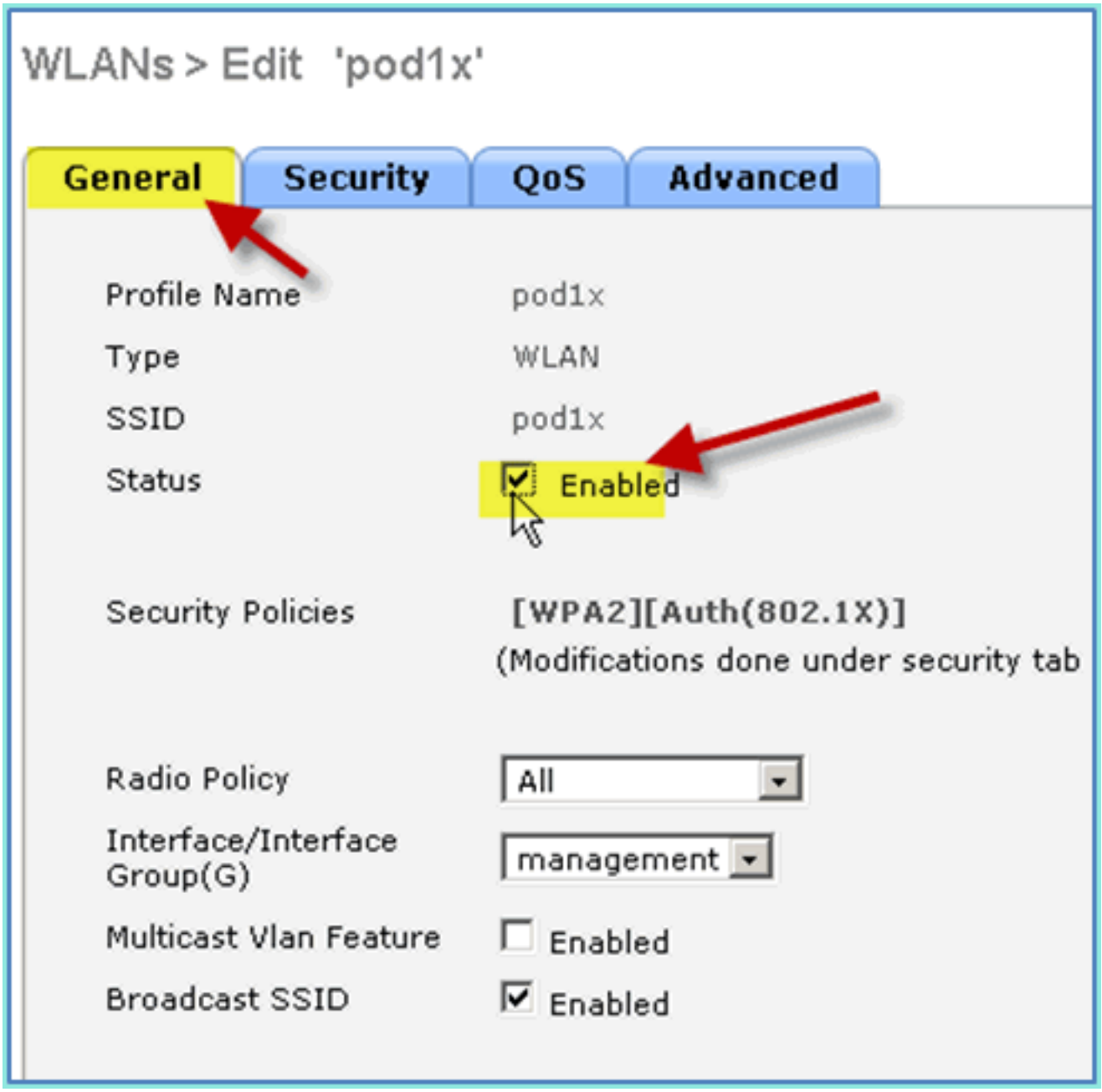
5. Para la ficha WLAN > Security > AAA Servers, configure lo siguiente:Interfaz de sobrescritura del servidor de radio: deshabilitadaServidores de autenticación/cuentas: HabilitadosServidor 1:
10.10.10.70



6. En la ficha WLAN > Advanced (WLAN > Avanzado), defina las siguientes opciones:Permitir Sustitución de AAA: ActivadoEstado de NAC: Radius NAC (seleccionado)



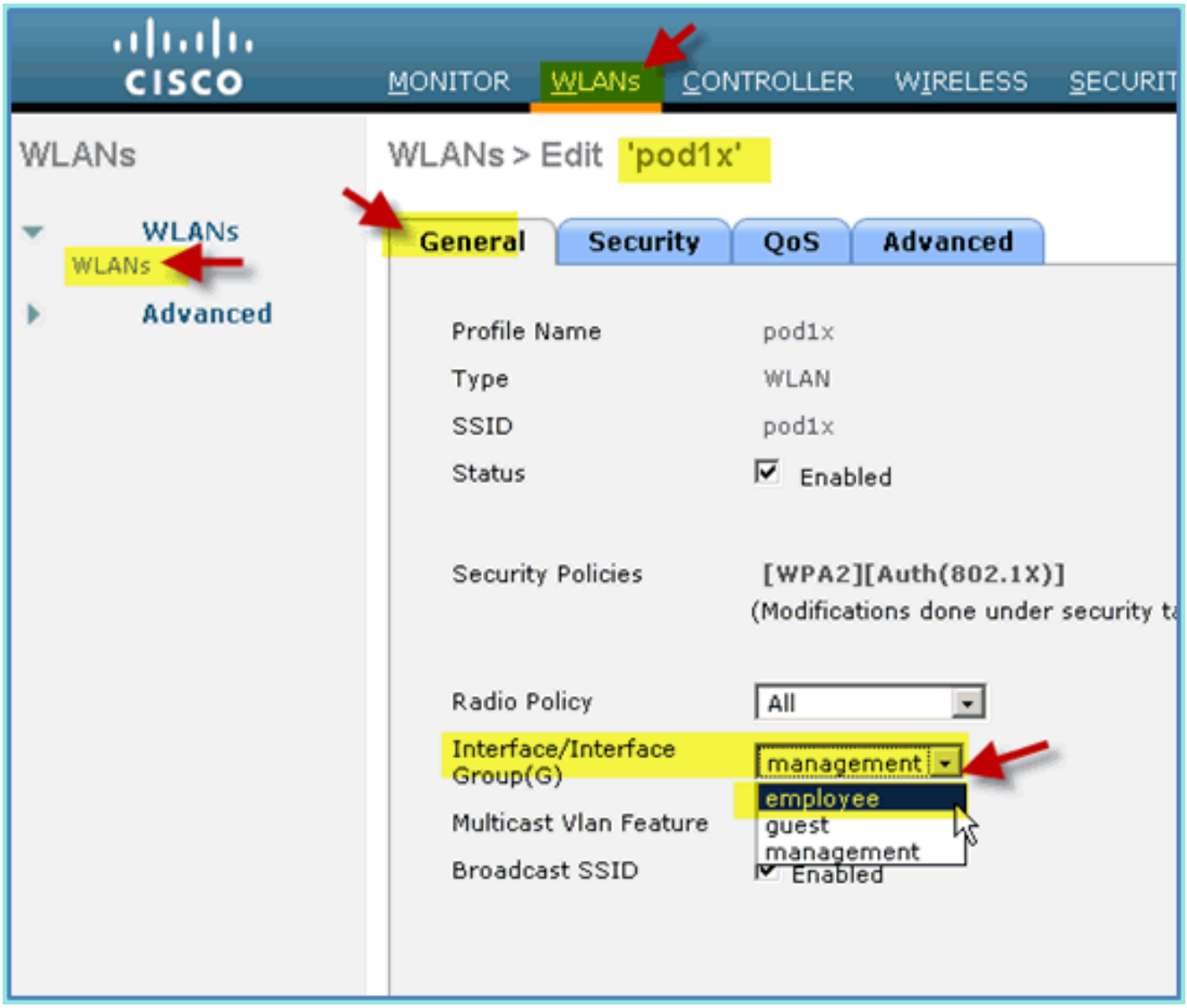
7. Vuelva a la ficha WLAN > General > Enable WLAN (Activar WLAN) (casilla de verificación).



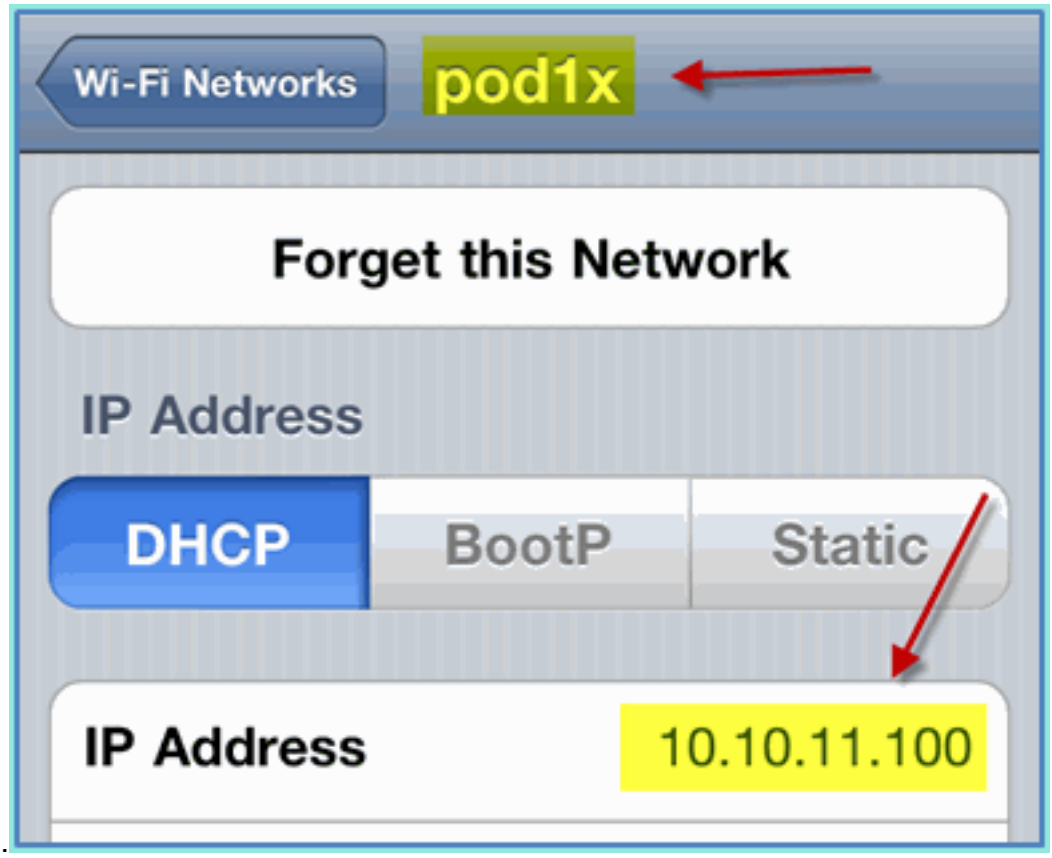
Probar interfaces dinámicas de WLC

Debe realizar una comprobación rápida de las interfaces válidas de empleado e invitado. Utilice cualquier dispositivo para asociarse a la WLAN y, a continuación, cambie la asignación de la interfaz WLAN.

1. Desde WLC, navegue hasta **WLAN > WLANs**. Haga clic aquí para editar el SSID seguro creado en el ejercicio anterior.
2. Cambie la interfaz/grupo de interfaz a **Empleado** y haga clic en **Aplicar**.

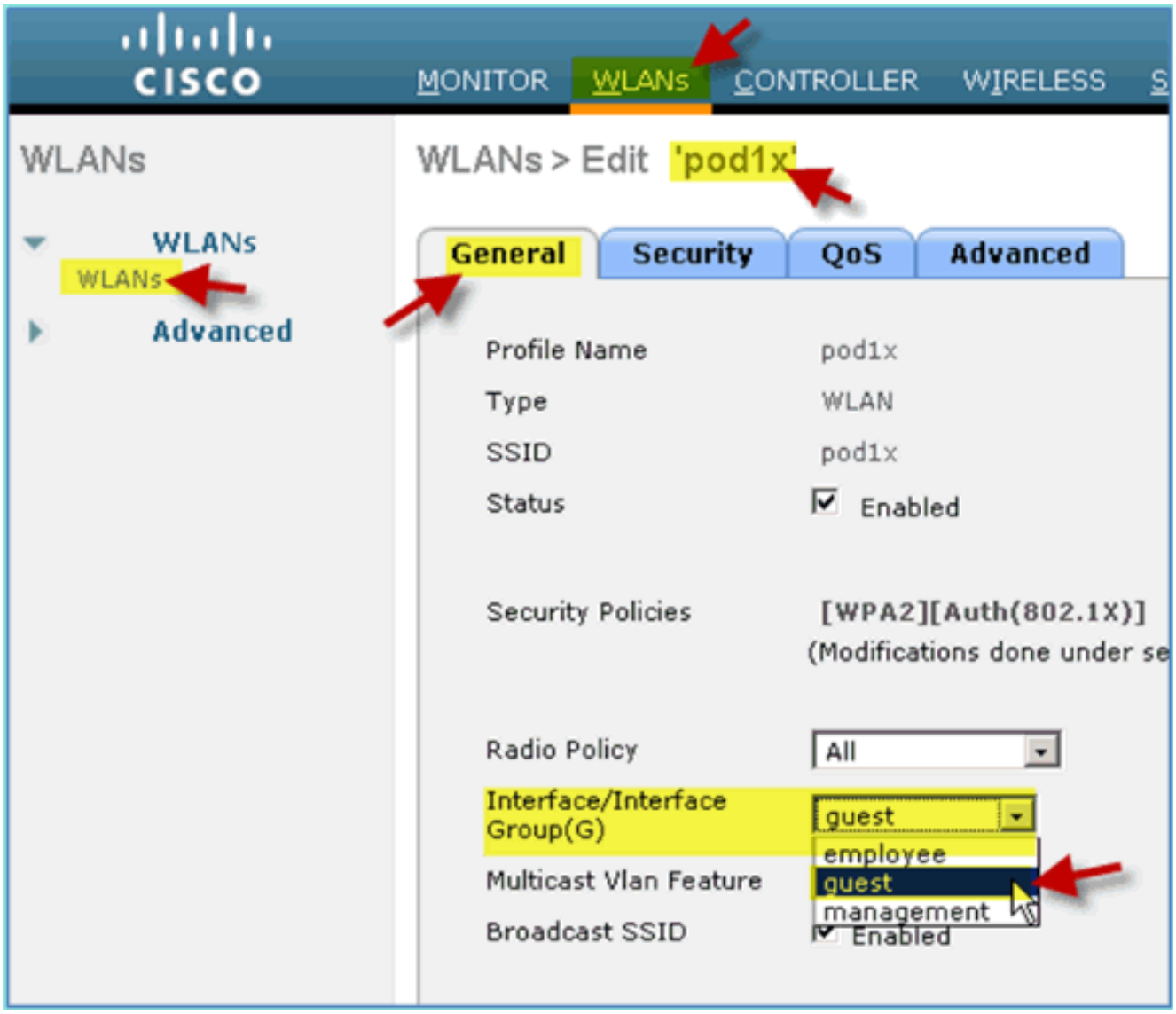


3. Si se configura correctamente, un dispositivo recibe una dirección IP de la VLAN del empleado (10.10.11.0/24). Este ejemplo muestra un dispositivo iOS que obtiene una nueva

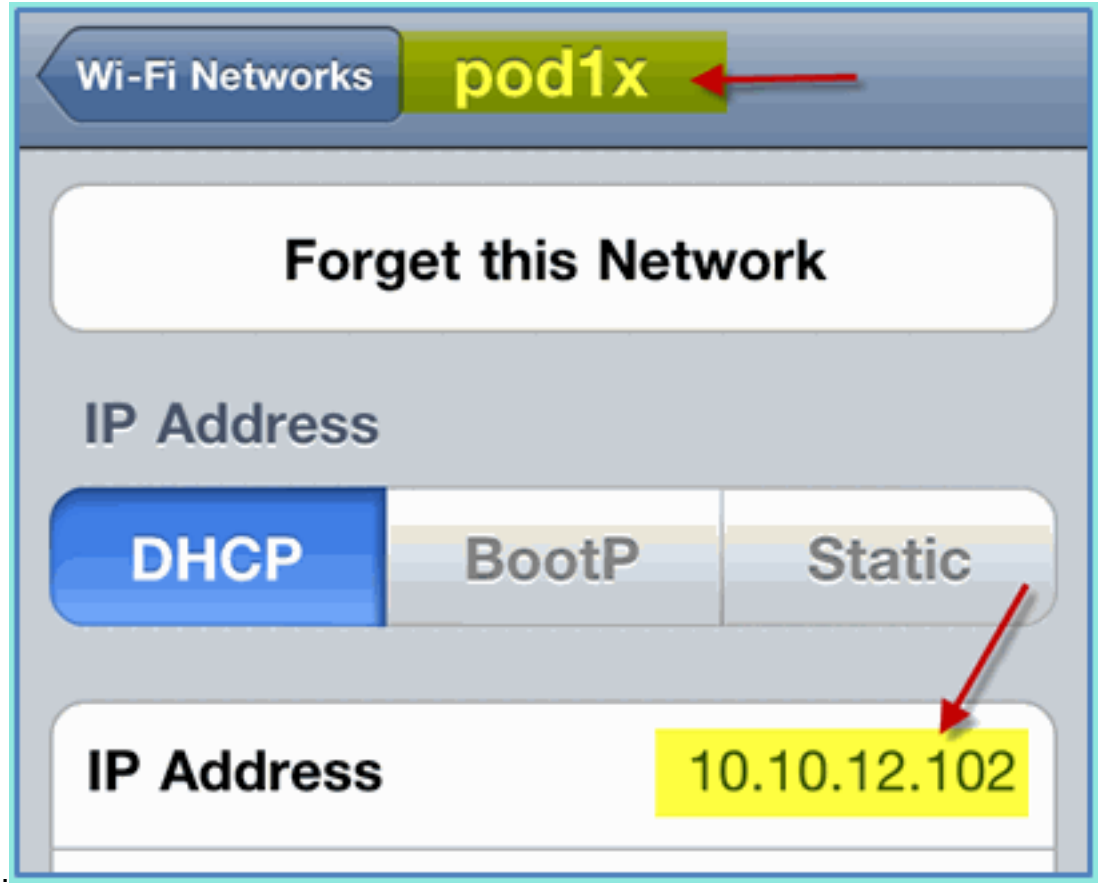


dirección IP.

4. Una vez confirmada la interfaz anterior, cambie la asignación de la interfaz WLAN a **Guest** y haga clic en
Apply.



5. Si se configura correctamente, un dispositivo recibe una dirección IP de la VLAN de invitado (10.10.12.0/24). Este ejemplo muestra un dispositivo iOS que obtiene una nueva dirección

IP. 

6. **IMPORTANTE:** Vuelva a cambiar la asignación de interfaz a la administración original.
7. Haga clic en **Aplicar** y guarde la configuración para el WLC.

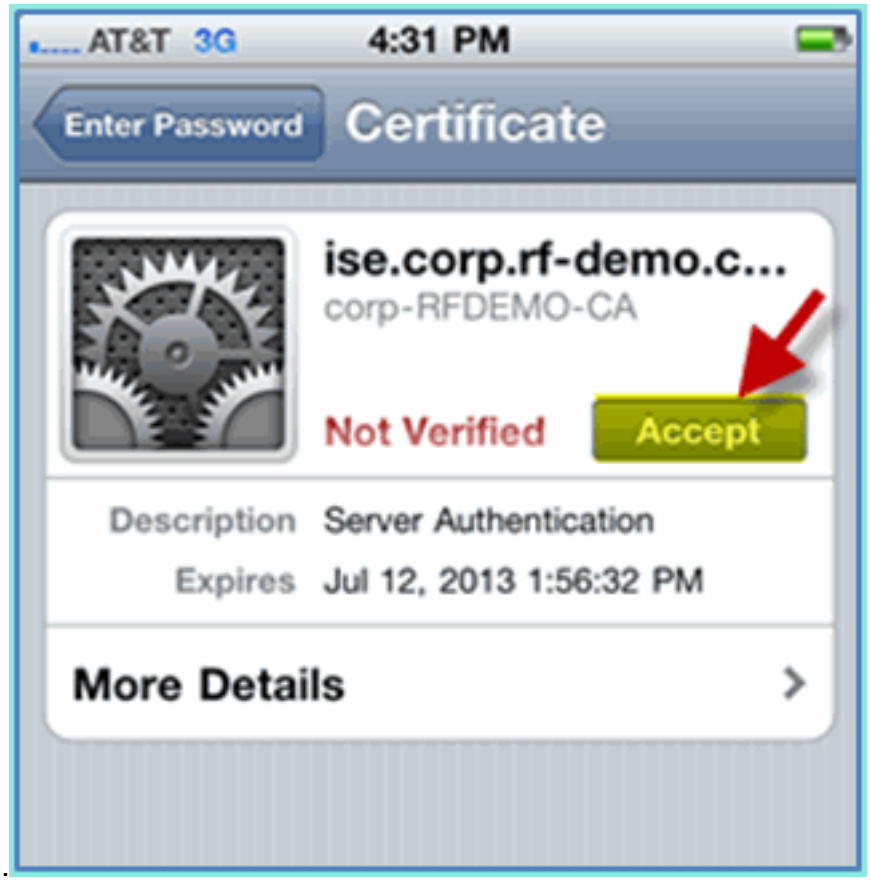
Autenticación inalámbrica para iOS (iPhone/iPad)

Asociarse al WLC a través de un SSID autenticado a un usuario INTERNO (o integrado, usuario AD) usando un dispositivo iOS como un iPhone, iPad o iPod. Omita estos pasos si no es aplicable.

1. En el dispositivo con iOS, vaya a la configuración de WLAN. Active WIFI y, a continuación, seleccione el SSID 802.1X activado creado en la sección anterior.
2. Proporcione esta información para conectarse:Nombre de usuario: empleado (interno - empleado) o contratista (interno - contratista)Contraseña:

XXXX

3. Haga clic para aceptar el certificado de

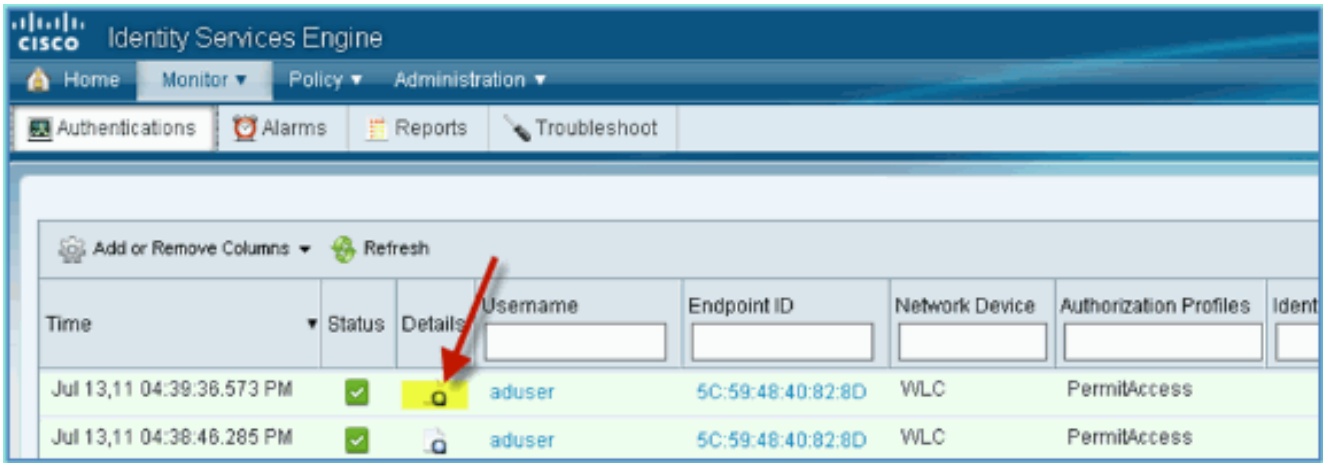
ISE. 

4. Confirme que el dispositivo con iOS está obteniendo una dirección IP de la interfaz de

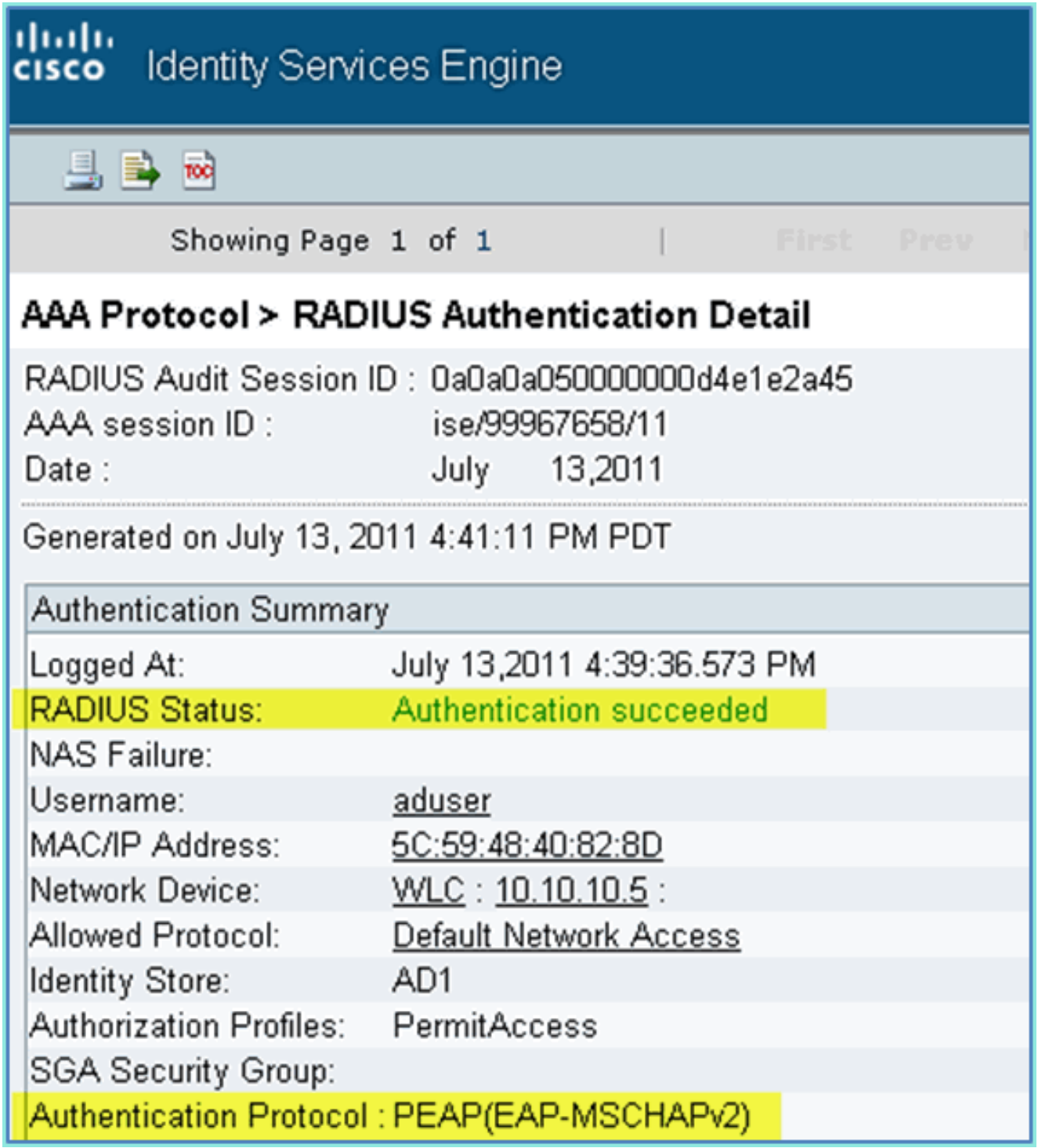
administración (VLAN10).

5. En el WLC > Monitor > Clients, verifique la información del punto final incluyendo el uso, el estado y el tipo
   EAP.

6. Del mismo modo, la información del cliente se puede proporcionar en la página ISE > Monitor > Authentication.



7. Haga clic en el icono **Details** para acceder a la sesión y obtener información detallada de la misma.



Agregar ACL de redirección de posición al WLC

La ACL de redirección de postura se configura en el WLC, donde ISE la utilizará para restringir el estado del cliente. De forma eficaz y como mínimo, la ACL permite el tráfico entre ISE. Si es necesario, se pueden agregar reglas opcionales en esta ACL.

1. Navegue hasta **WLC > Security > Access Control Lists > Access Control Lists**. Haga clic en **New**.

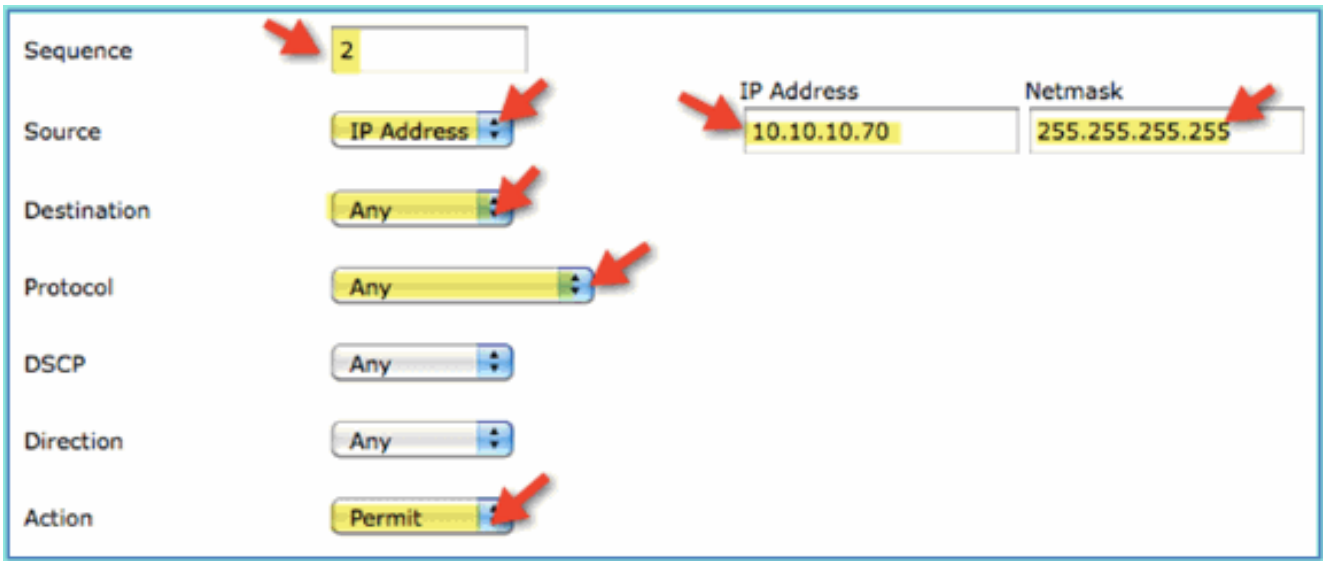
2. Proporcione un nombre (ACL-POSTURE-REDIRECT) para la ACL.

3. Haga clic en **Add New Rule** para la nueva ACL. Establezca los siguientes valores en la secuencia de ACL #1. Haga clic en **Apply** cuando termine.Fuente: AnyDestino: dirección IP 10.10.10.70, 255.255.255.255Protocolo: cualquieraAcción:
Permitir

4. Se ha agregado la secuencia de confirmación.

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

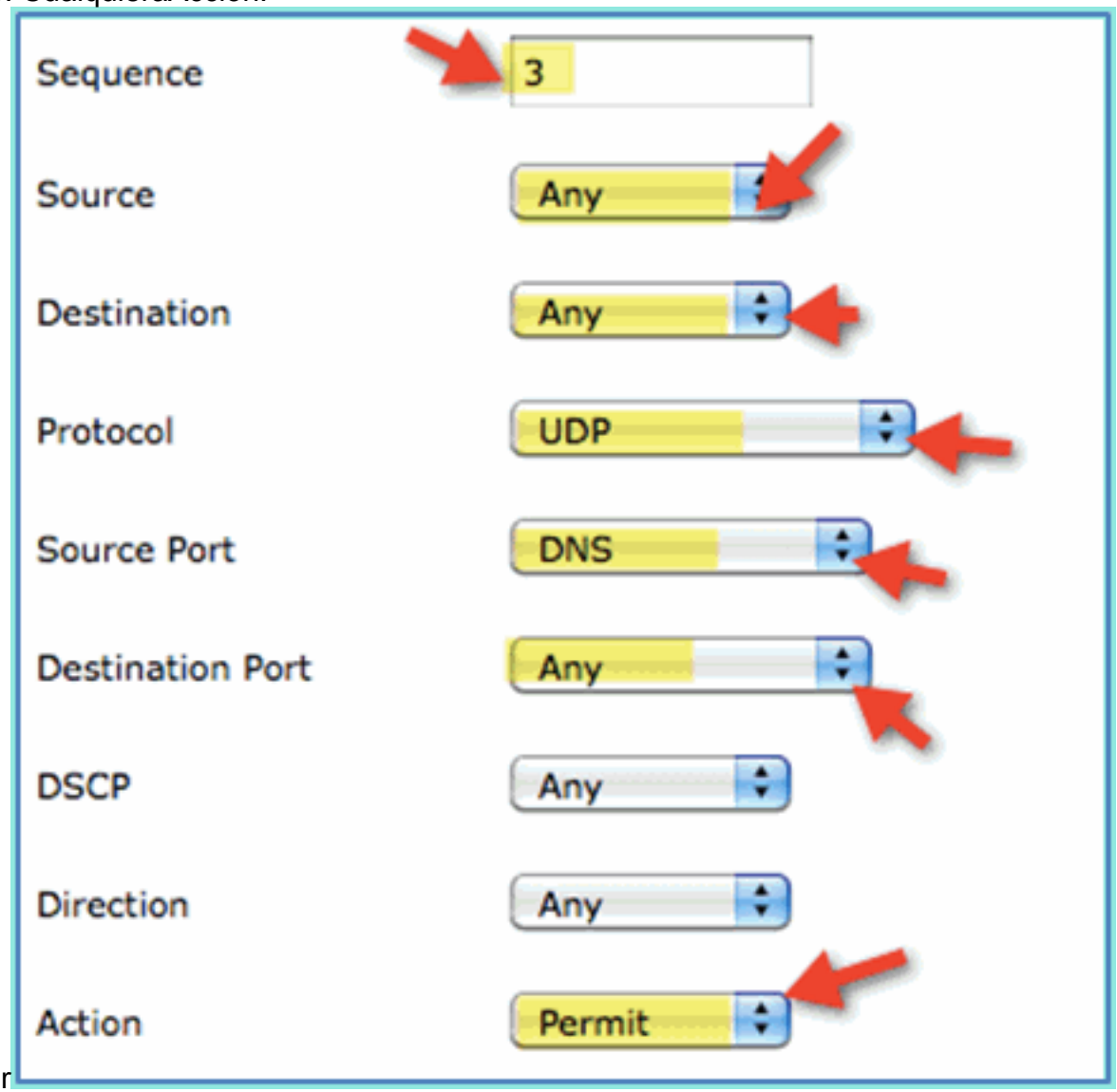
5. Haga clic en **Agregar nueva regla**. Establezca los siguientes valores en la secuencia de ACL #2. Haga clic en **Apply** cuando termine.Fuente: dirección IP 10.10.10.70, 255.255.255.255Destino: CualquieraProtocolo: cualquieraAcción: Permitir



6. Se ha agregado la secuencia de confirmación.

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

7. Establezca los siguientes valores en la secuencia de ACL #3. Haga clic en **Apply** cuando termine.Fuente: AnyDestino: CualquieraProtocolo: UDPPuerto de origen: DNSPuerto de destino: CualquieraAcción:



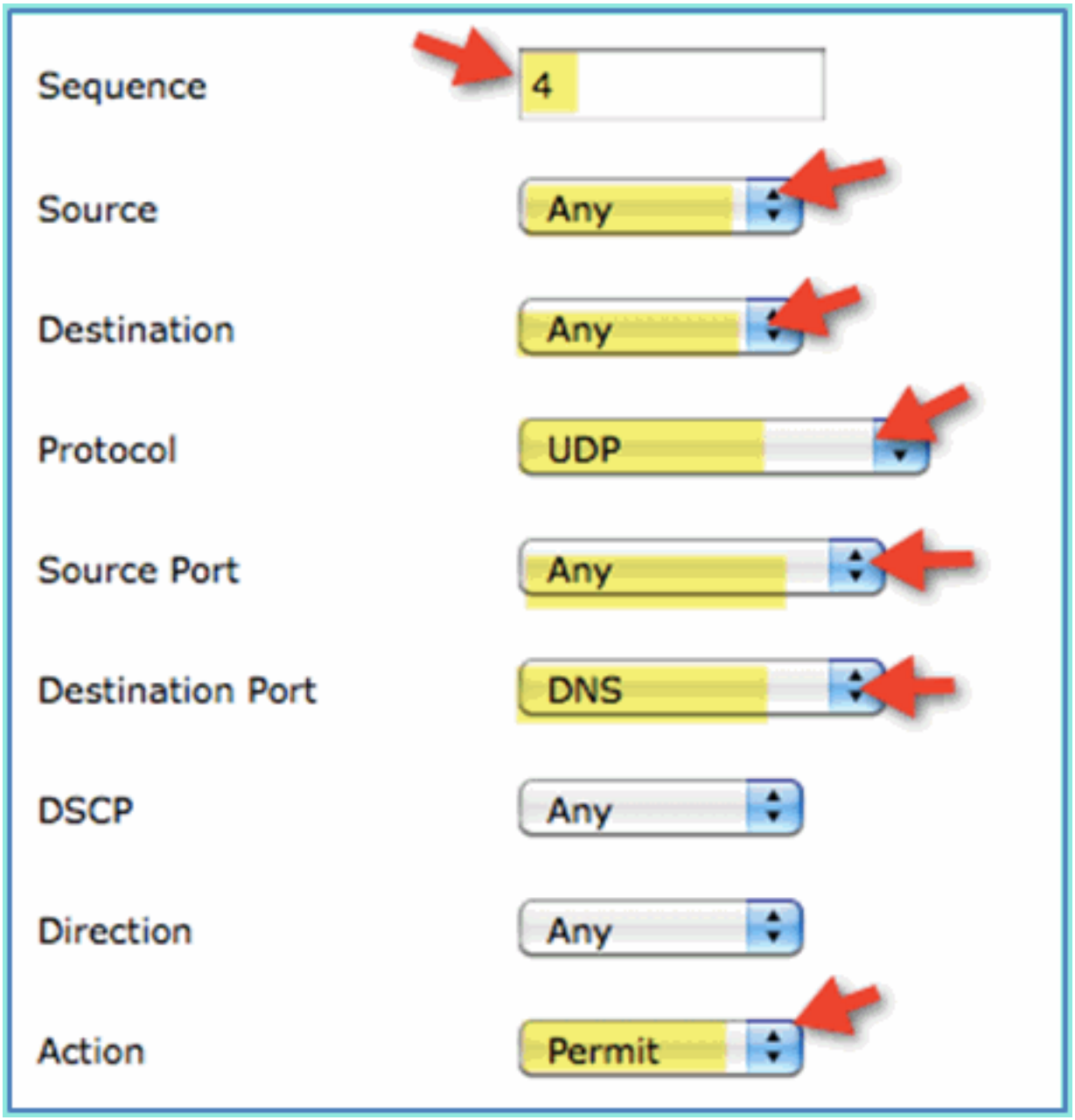
Permitir

8. Se ha agregado la secuencia de confirmación.

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

9. Haga clic en **Agregar nueva regla**. Establezca los siguientes valores en la secuencia de ACL

#4. Haga clic en **Apply** cuando termine.Fuente: AnyDestino: CualquieraProtocolo: UDPPuerto de origen: CualquieraPuerto de destino: DNSAcción: Permitir



10. Se ha agregado la secuencia de confirmación.

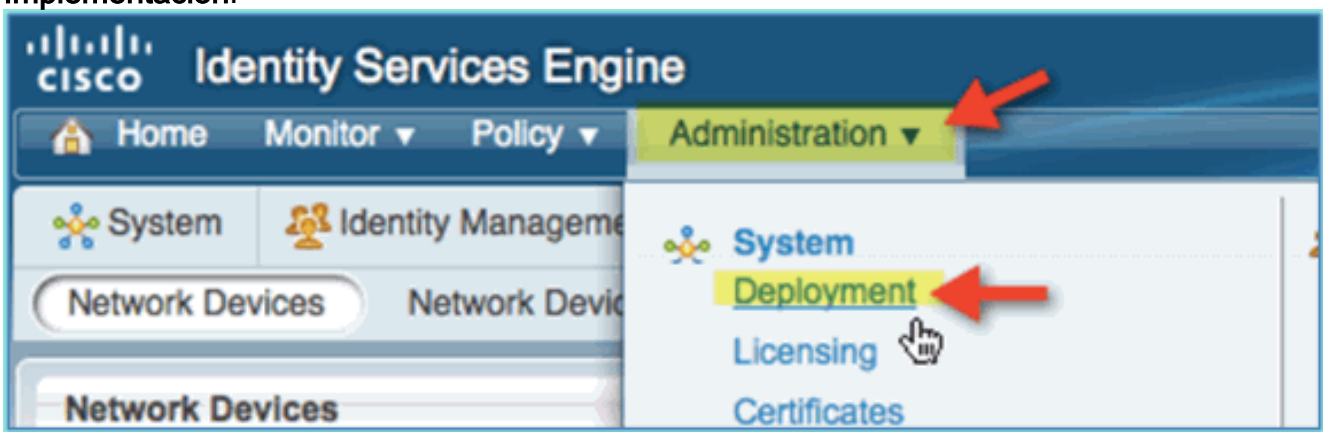
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any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

11. Guarde la configuración actual del WLC.

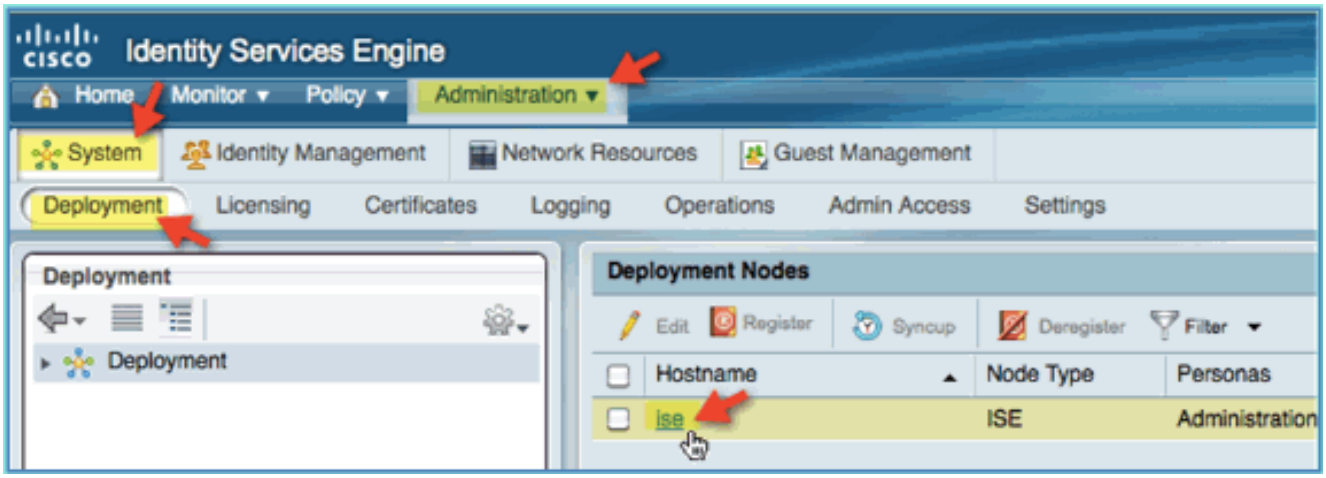
Habilitar sondeos de perfiles en ISE

ISE debe configurarse como sondas para crear perfiles de terminales de forma eficaz. De forma predeterminada, estas opciones están desactivadas. Esta sección muestra cómo configurar ISE para que sean sondeos.

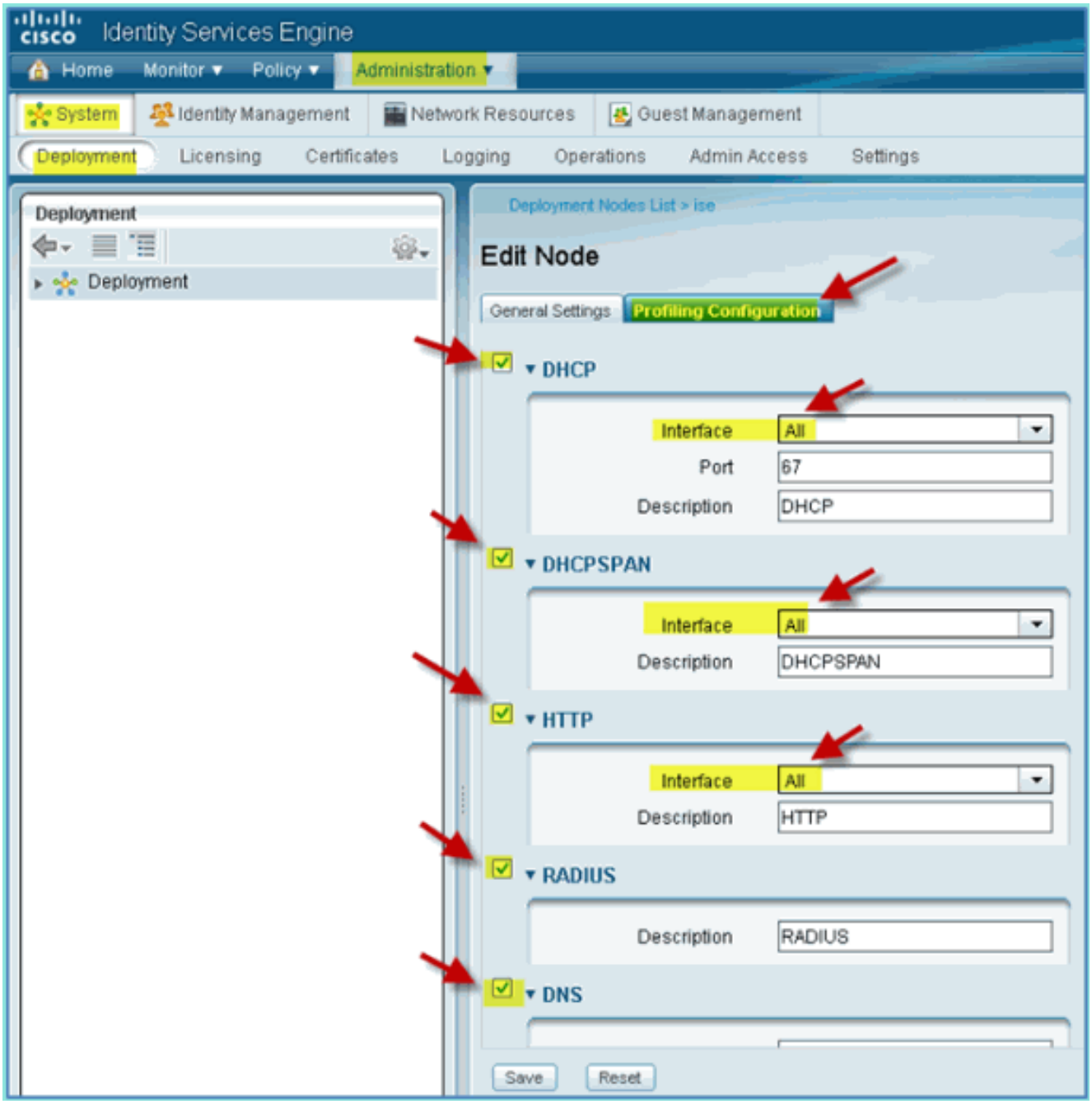
1. Desde Administración de ISE, navegue hasta **Administración > Sistema > Implementación**.



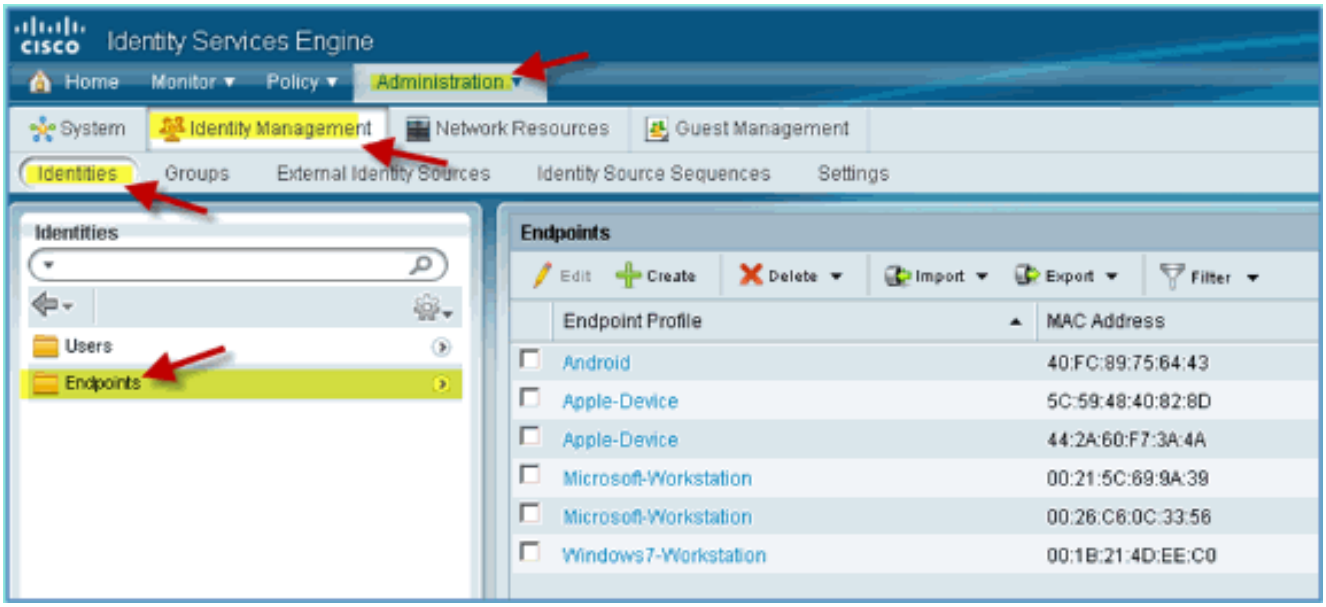
2. Elija **ISE**. Haga clic en **Editar host ISE**.



3. En la página Editar Nodo, seleccione la configuración de definición de perfiles y configure lo siguiente:DHCP: activado, todos (o predeterminado)DHCPSPAN: activado, todos (o predeterminado)HTTP: habilitado, todos (o predeterminado)RADIUS: activado, N/DDNS: activado,
N/D



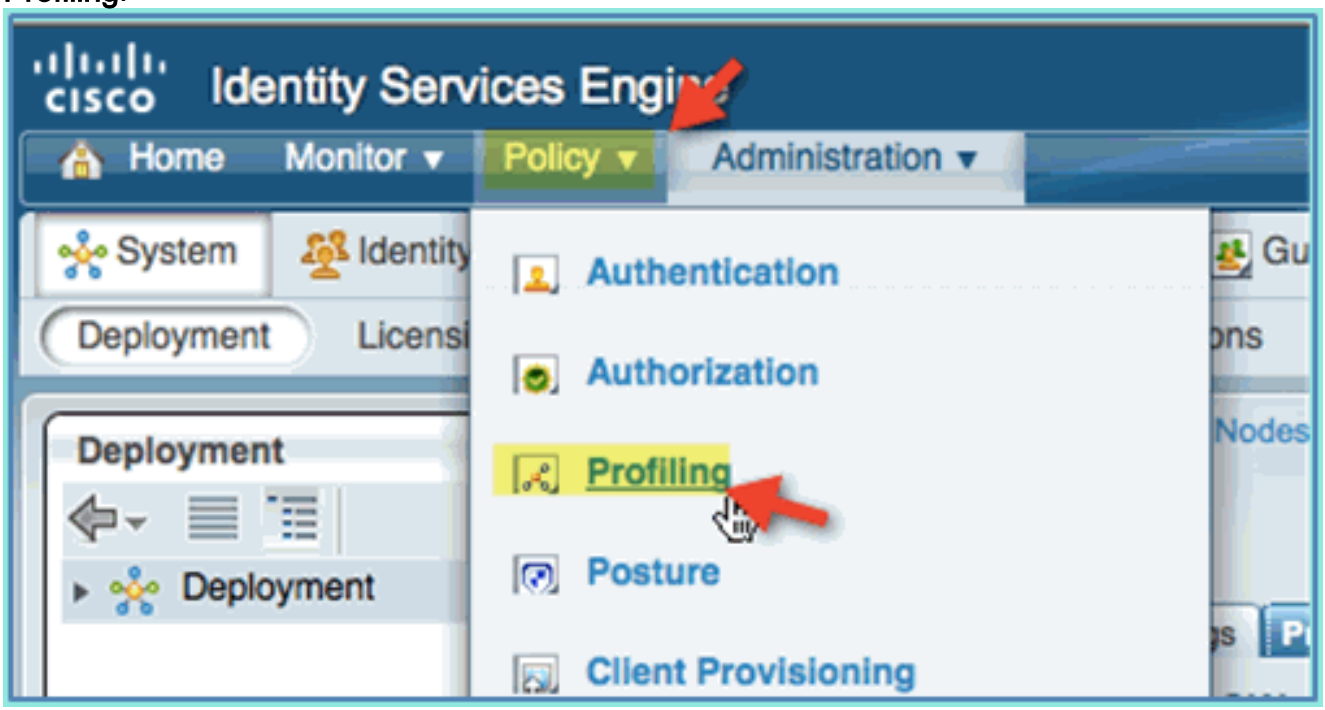
4. Vuelva a asociar los dispositivos (iPhone/iPads/Droids/Mac, etc.).
5. Confirme las identidades de terminales ISE. Vaya a **Administration > Identity Management > Identities**. Haga clic en Terminales para mostrar los perfiles.**Nota:** La definición de perfiles inicial procede de sondas
   RADIUS.



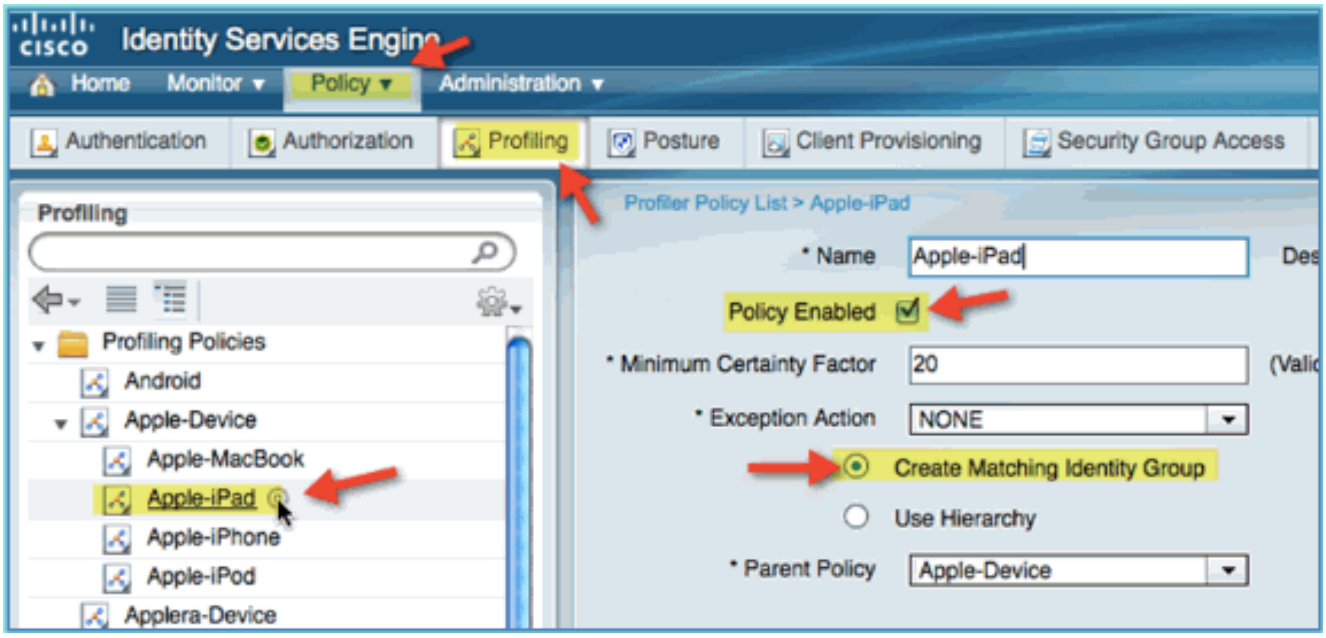
Habilitar políticas de perfil de ISE para dispositivos

De forma inmediata, ISE proporciona una biblioteca de diversos perfiles de terminales. Complete estos pasos para habilitar los perfiles para los dispositivos:

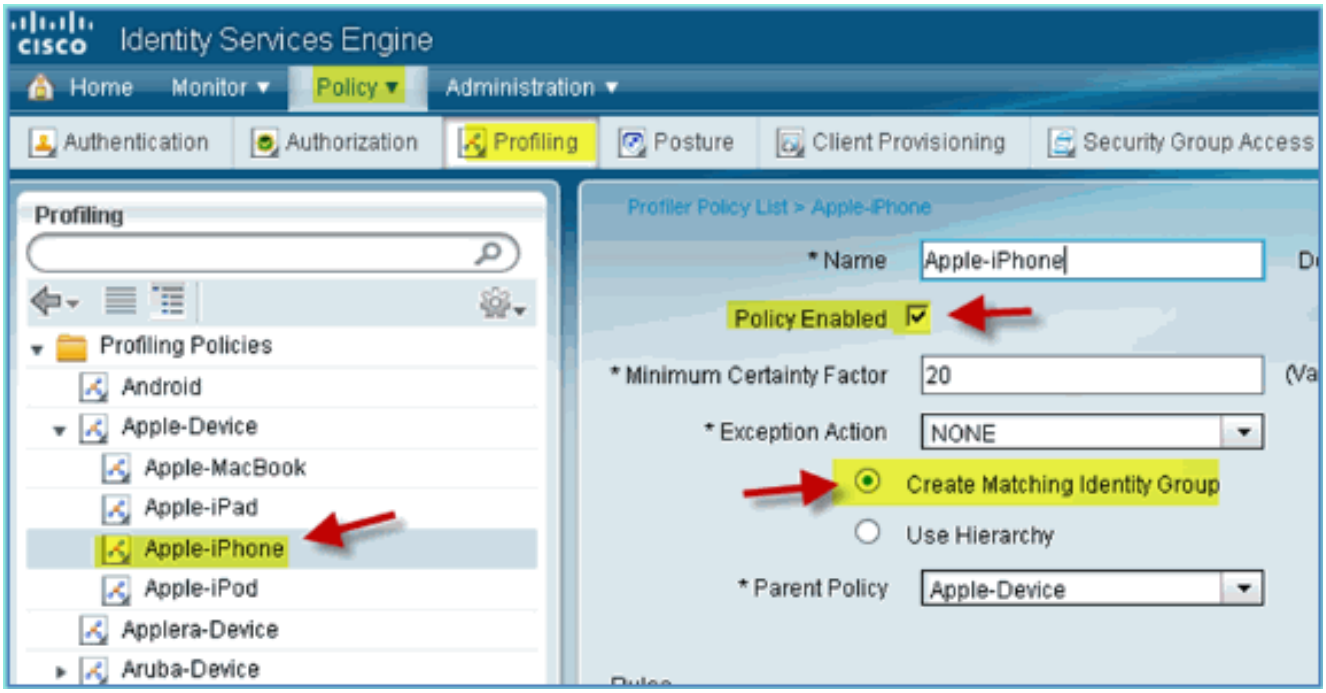
1. En ISE, vaya a **Policy > Profiling**.



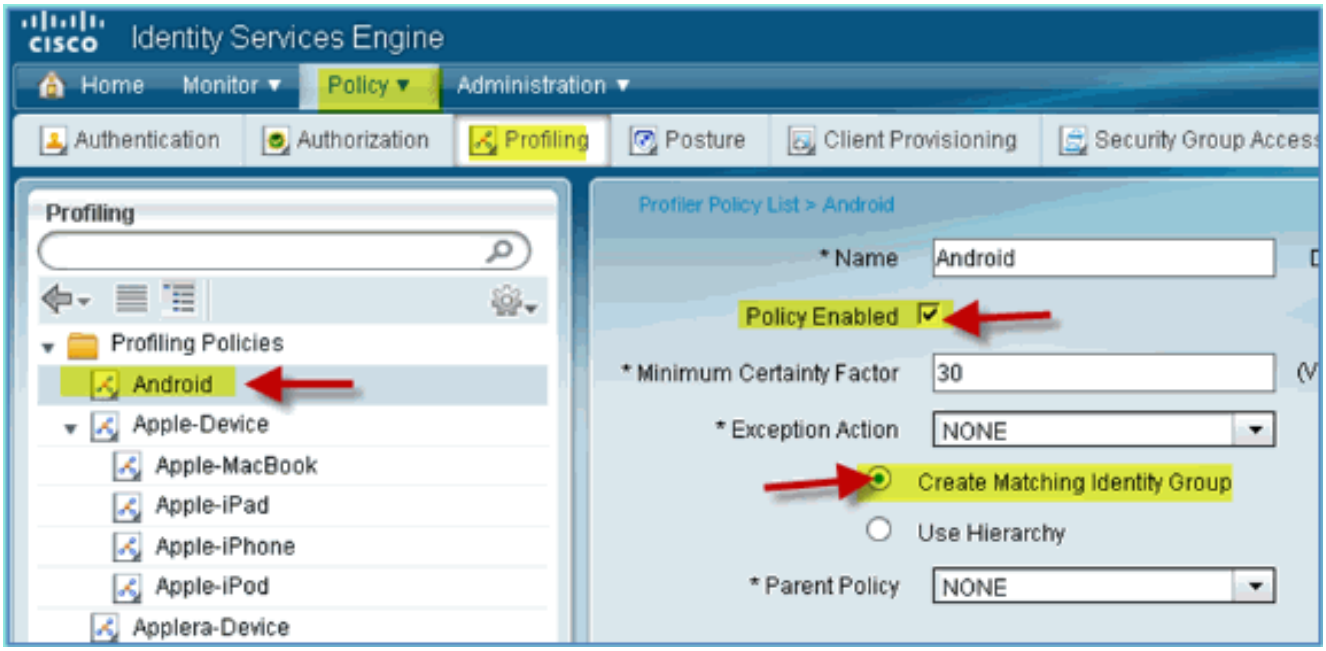
2. En el panel izquierdo, expanda **Directivas de generación de perfiles**.
3. Haga clic en **Apple Device > Apple iPad**, y configure lo siguiente:Política habilitada: habilitadaCrear grupo de identidades coincidente: seleccionado



4. Haga clic en **Apple Device > Apple iPhone**, establezca lo siguiente:Política habilitada: habilitadaCrear grupo de identidades coincidente:
seleccionado



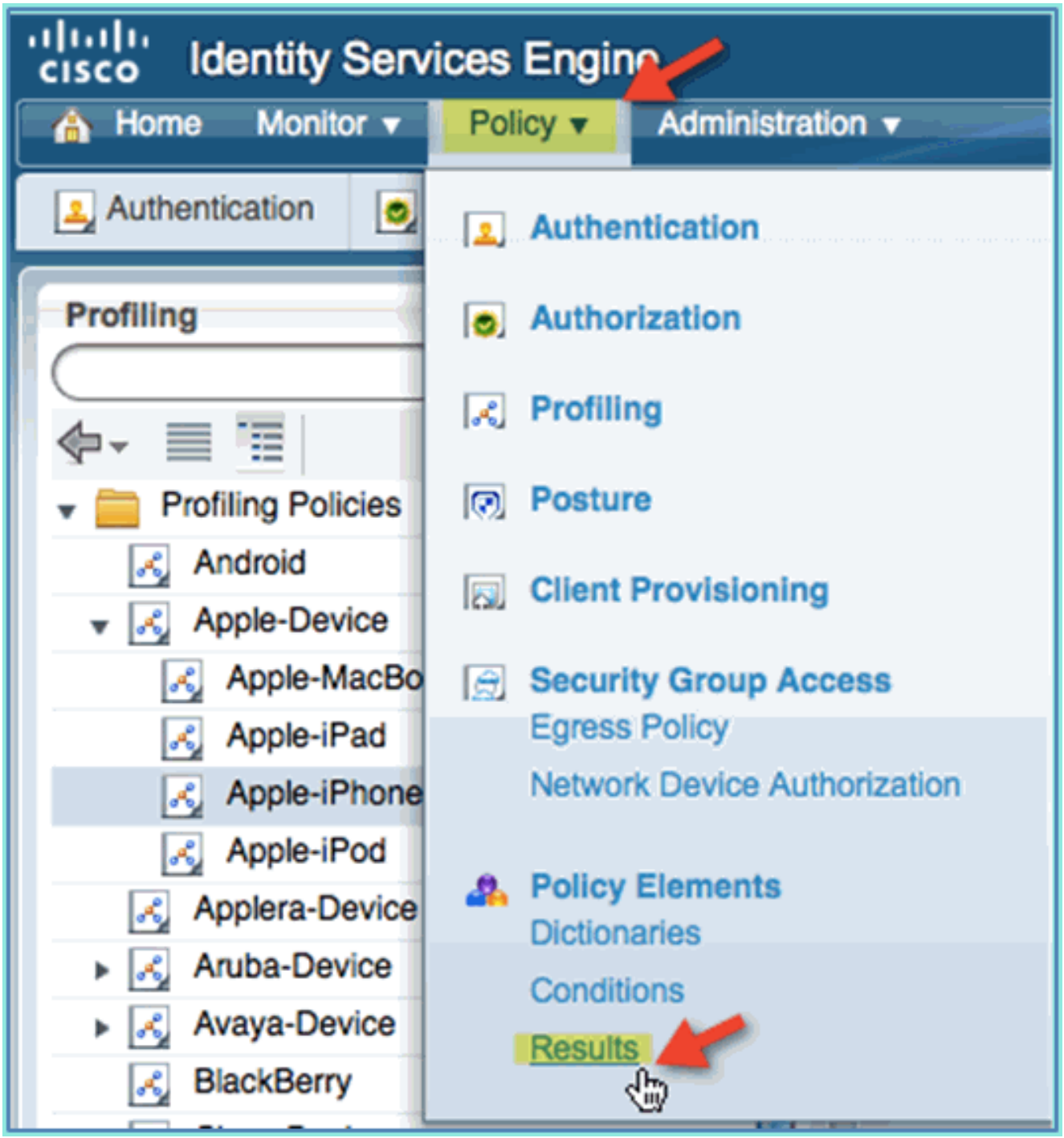
5. Haga clic en **Android**, establezca lo siguiente:Política habilitada: habilitadaCrear grupo de identidades coincidente:
seleccionado



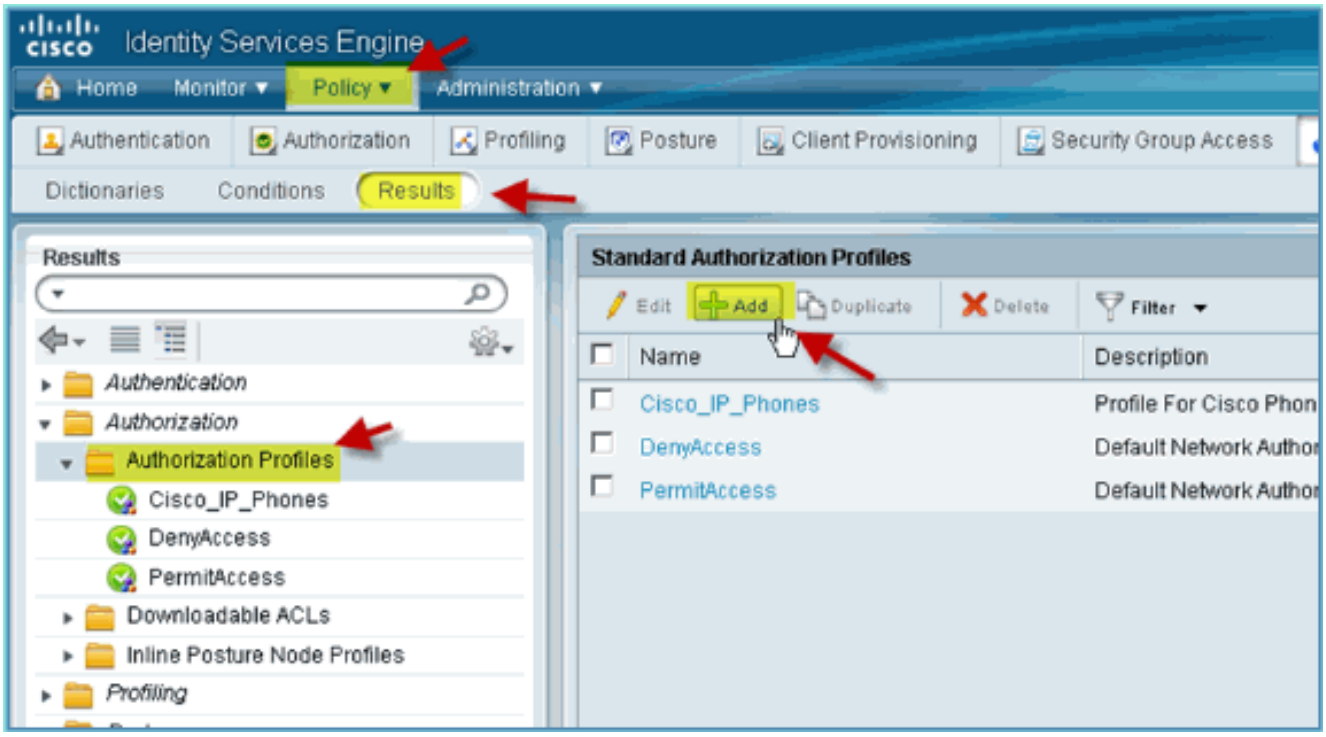
Perfil de autorización de ISE para redirección de detección de estado

Complete estos pasos para configurar una redirección de estado de la política de autorización que permita que los nuevos dispositivos se redireccionen a ISE para la detección y la creación de perfiles adecuadas:

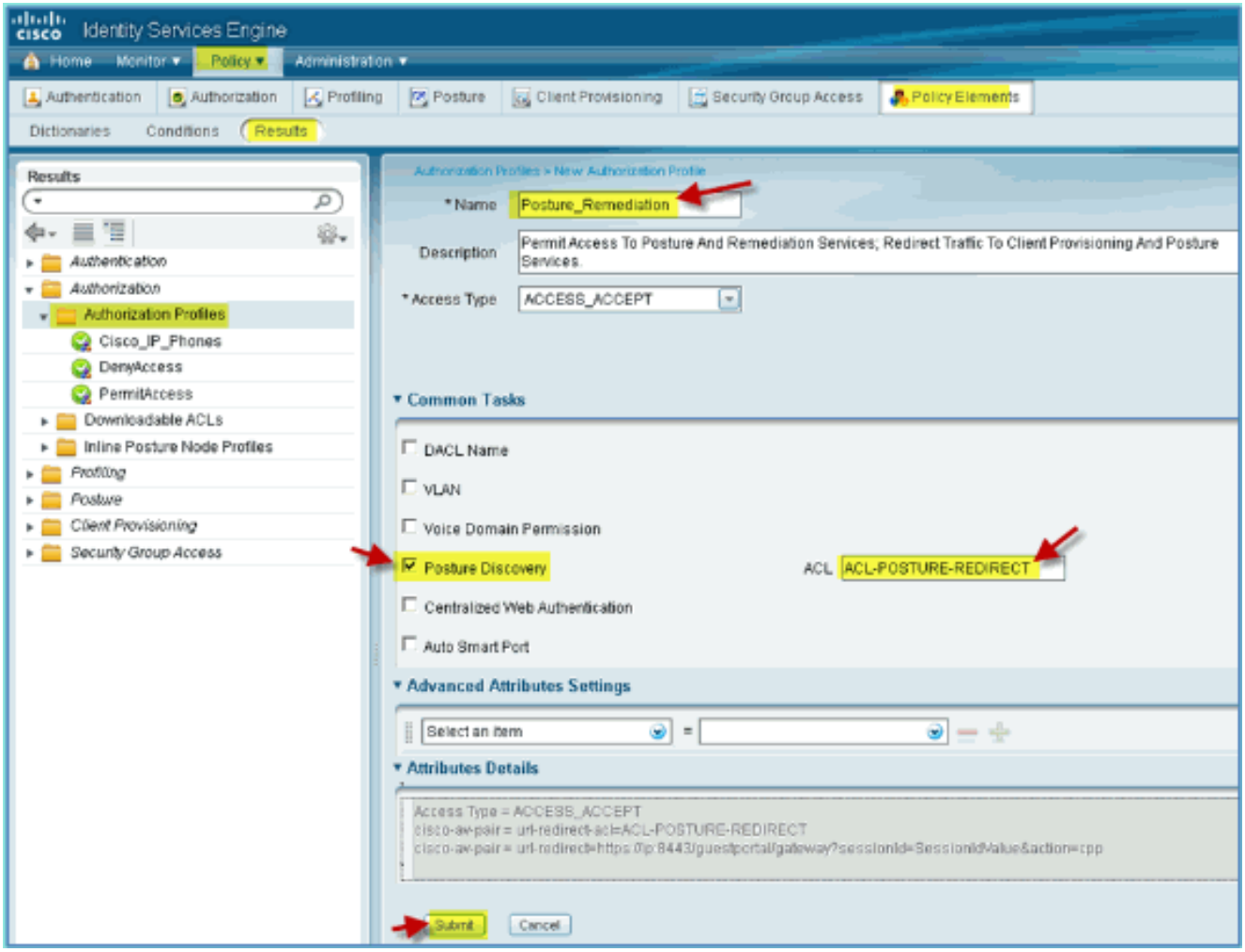
1. Desde ISE, navegue hasta **Política > Elementos de política > Resultados**.



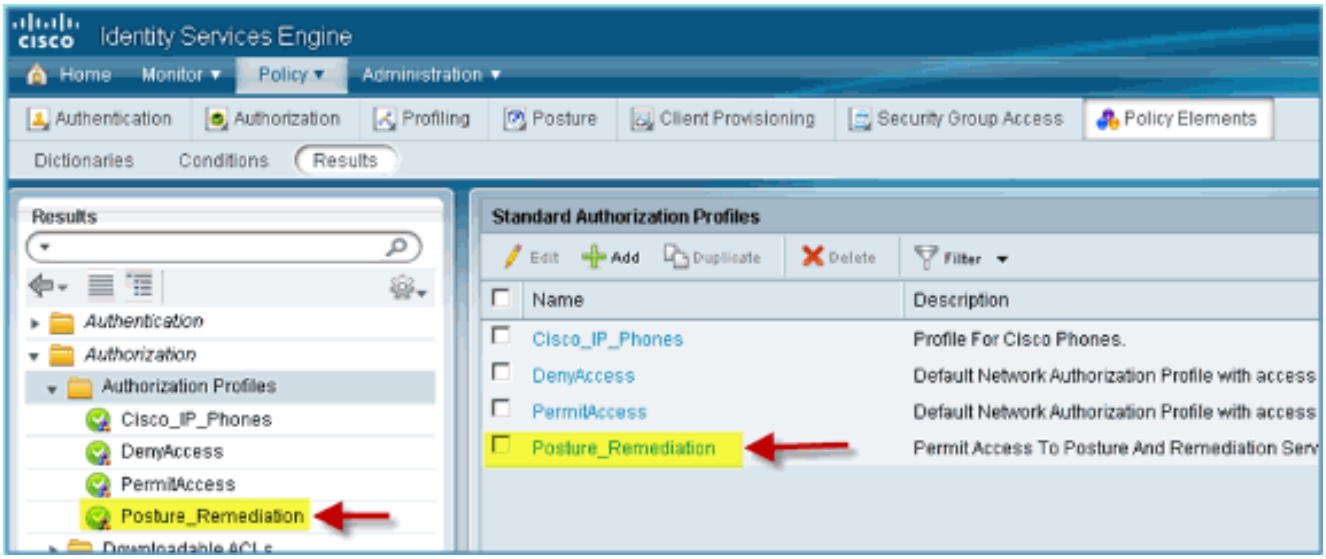
2. Expanda **Autorización**. Haga clic en **Perfiles de autorización** (panel izquierdo) y haga clic en **Agregar**.



3. Cree el perfil de autorización con lo siguiente:Nombre: Posture_RemediationTipo de acceso: Access_AcceptHerramientas comunes:Detección de estado, habilitadaDetección de estado, ACL ACL-POSTURE-
REDIRECT



4. Haga clic en **Enviar** para completar esta tarea.
5. Confirme que se agrega el nuevo perfil de autorización.

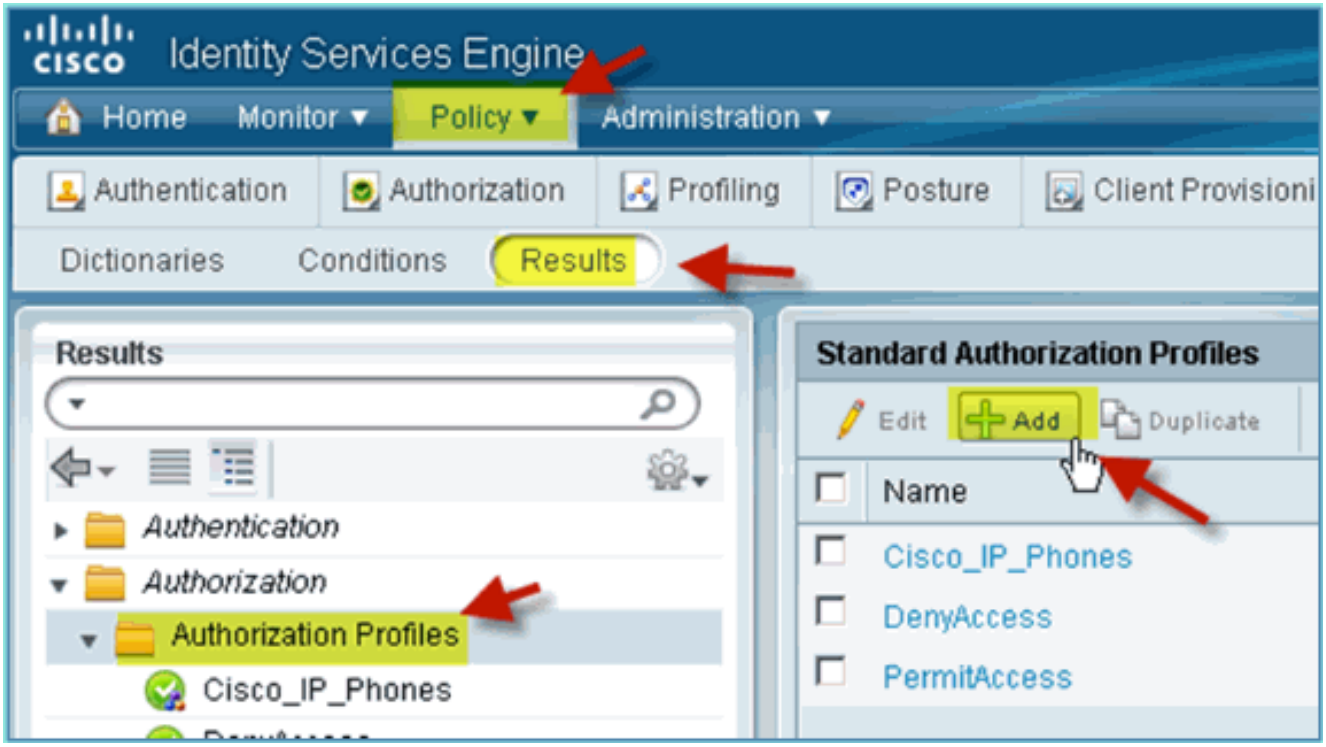


Crear perfil de autorización de ISE para empleados

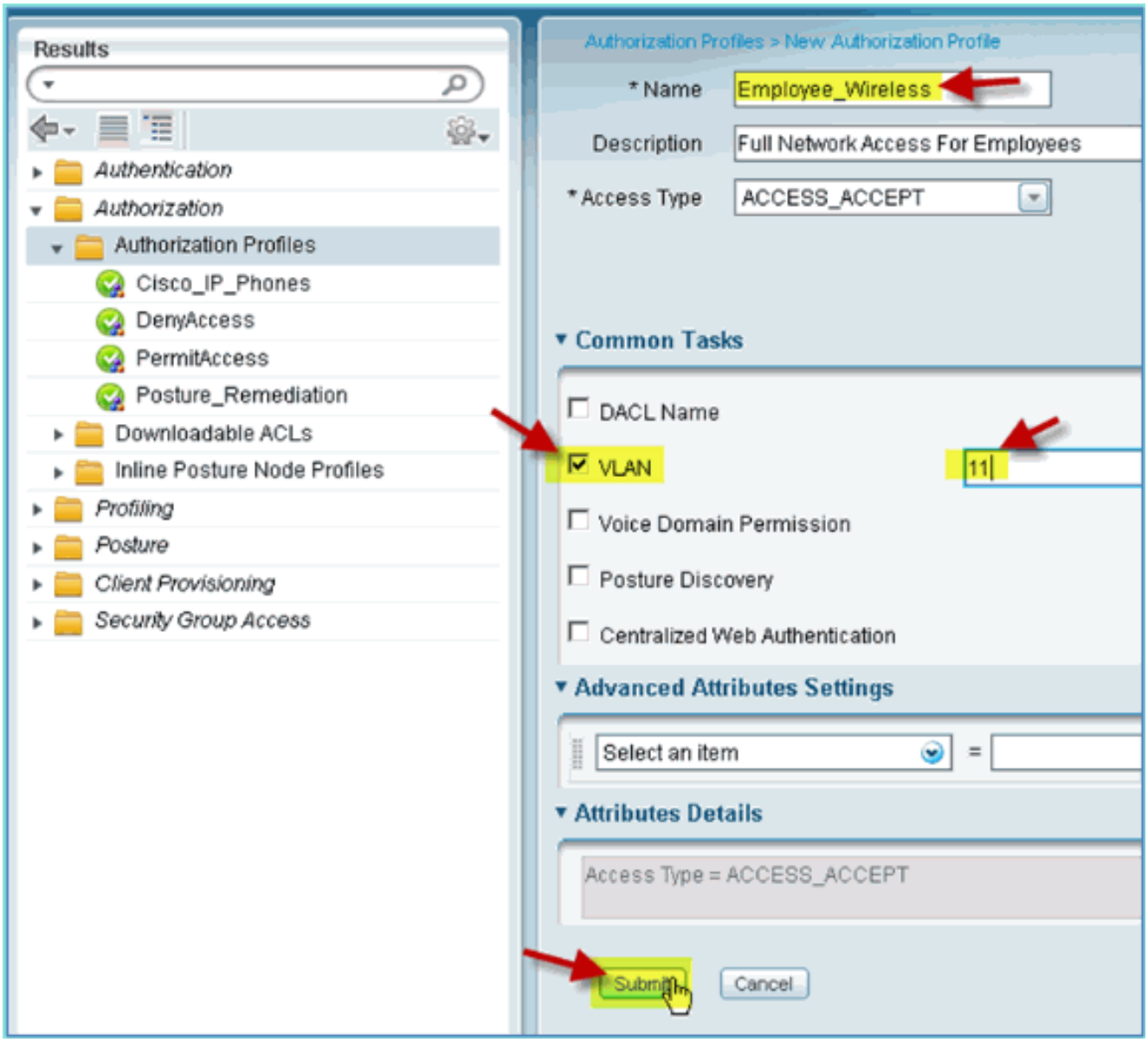
La adición de un perfil de autorización para un empleado permite a ISE autorizar y permitir el acceso con los atributos asignados. En este caso, se asigna la VLAN 11 del empleado.

Complete estos pasos:

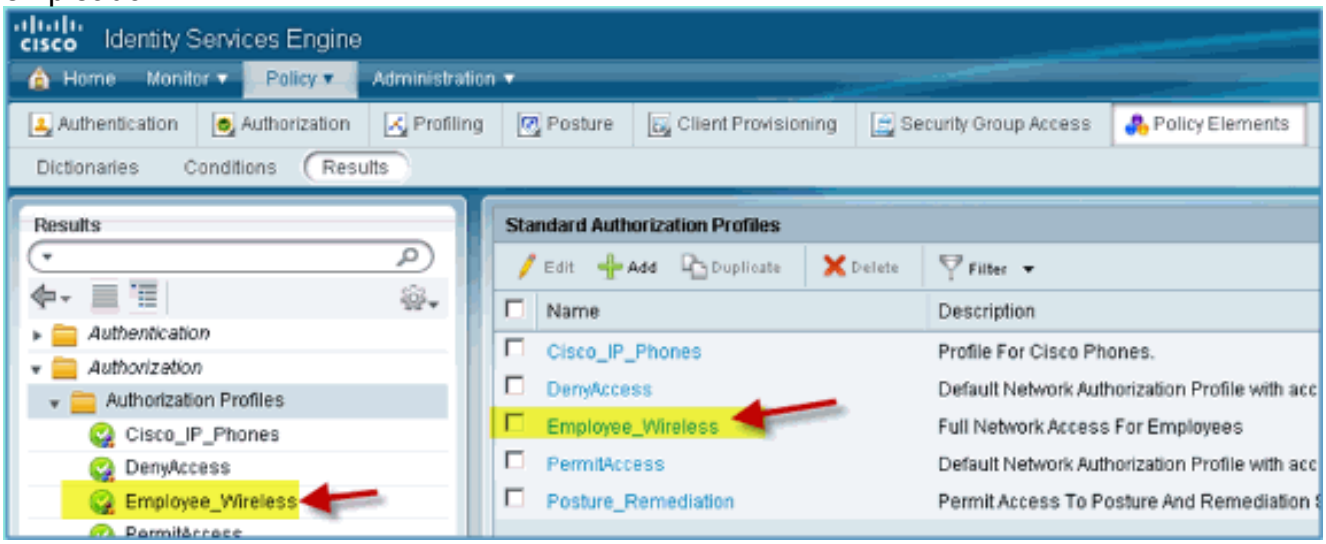
1. En ISE, vaya a **Policy > Results**. Expanda **Authorization**, luego haga clic en **Authorization Profiles** y haga clic en **Add**.



2. Introduzca lo siguiente para el perfil de autorización de empleado:Nombre: Employee_WirelessTareas comunes:VLAN, activadaVLAN, subvalor 11
3. Haga clic en **Enviar** para completar esta tarea.



4. Confirme que se ha creado el nuevo perfil de autorización de empleado.

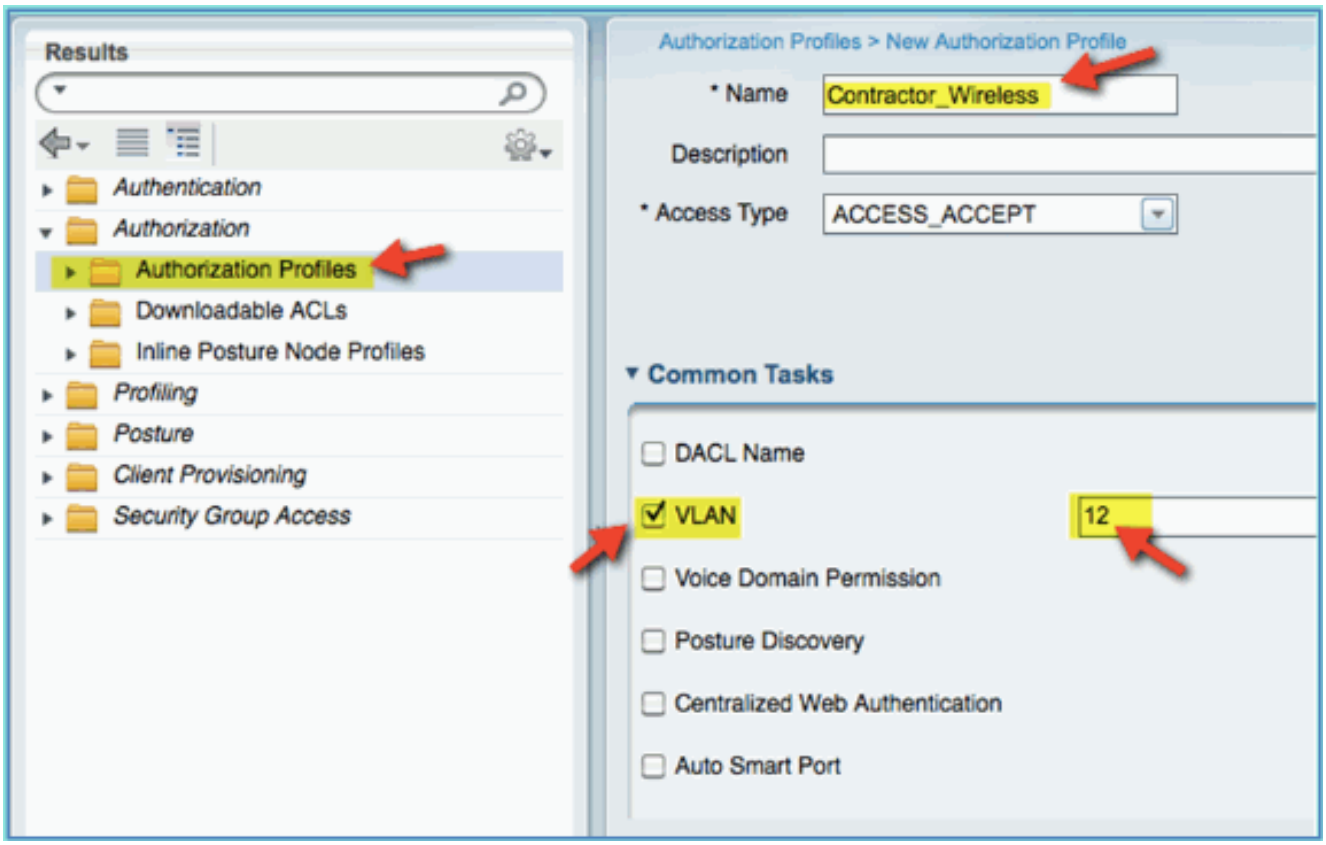


Crear perfil de autorización de ISE para contratista

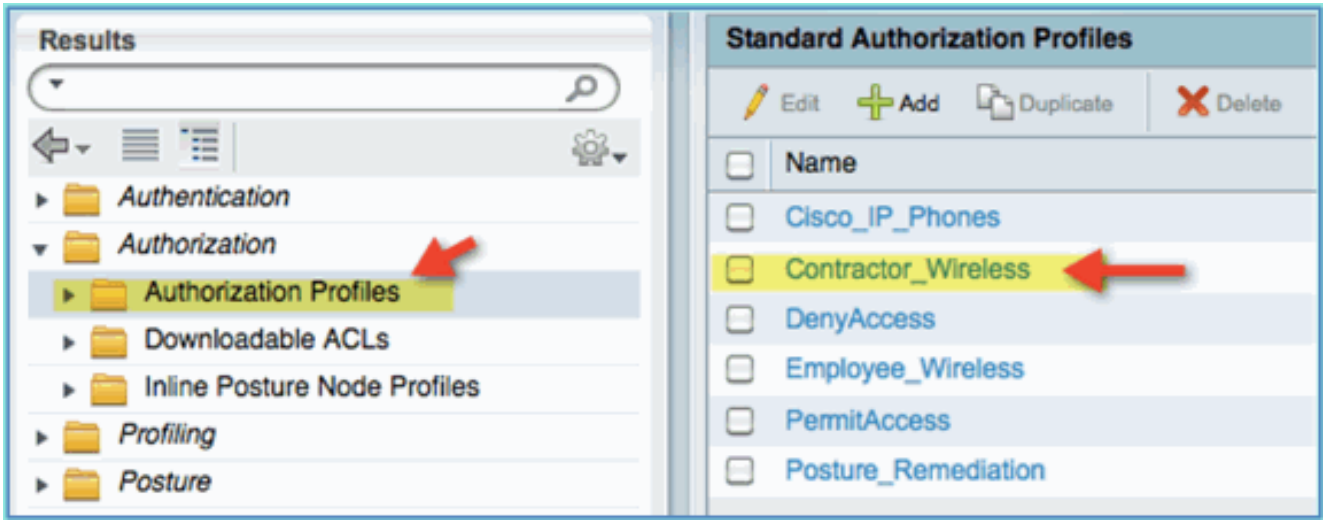
La adición de un perfil de autorización para un contratista permite a ISE autorizar y permitir el acceso con los atributos asignados. En este caso, se asigna la VLAN 12 del contratista.

Complete estos pasos:

1. En ISE, vaya a **Policy > Results**. Expanda **Authorization**, luego haga clic en **Authorization Profiles** y haga clic en **Add**.
2. Introduzca lo siguiente para el perfil de autorización de empleado:Nombre: Employee_WirelessTareas comunes:VLAN, activadaVLAN, subvalor 12



3. Haga clic en **Enviar** para completar esta tarea.
4. Confirme que se ha creado el perfil de autorización del contratista.



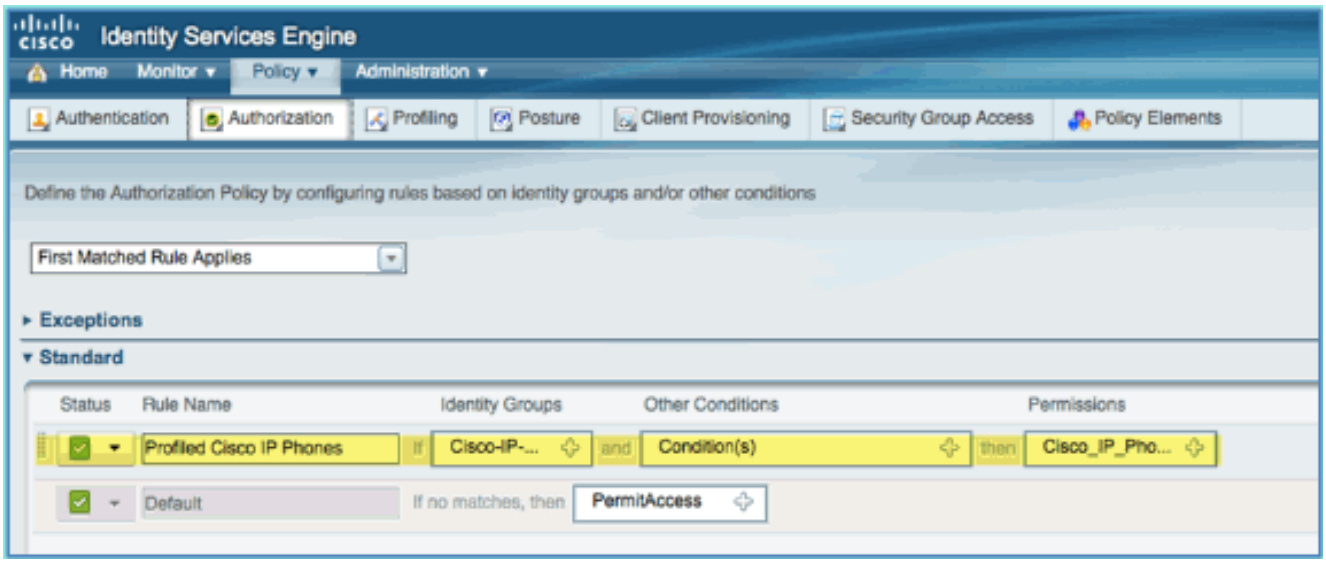
Política de autorización para la condición/definición de perfiles de dispositivos

Se sabe muy poco sobre un nuevo dispositivo cuando entra por primera vez en la red. Un

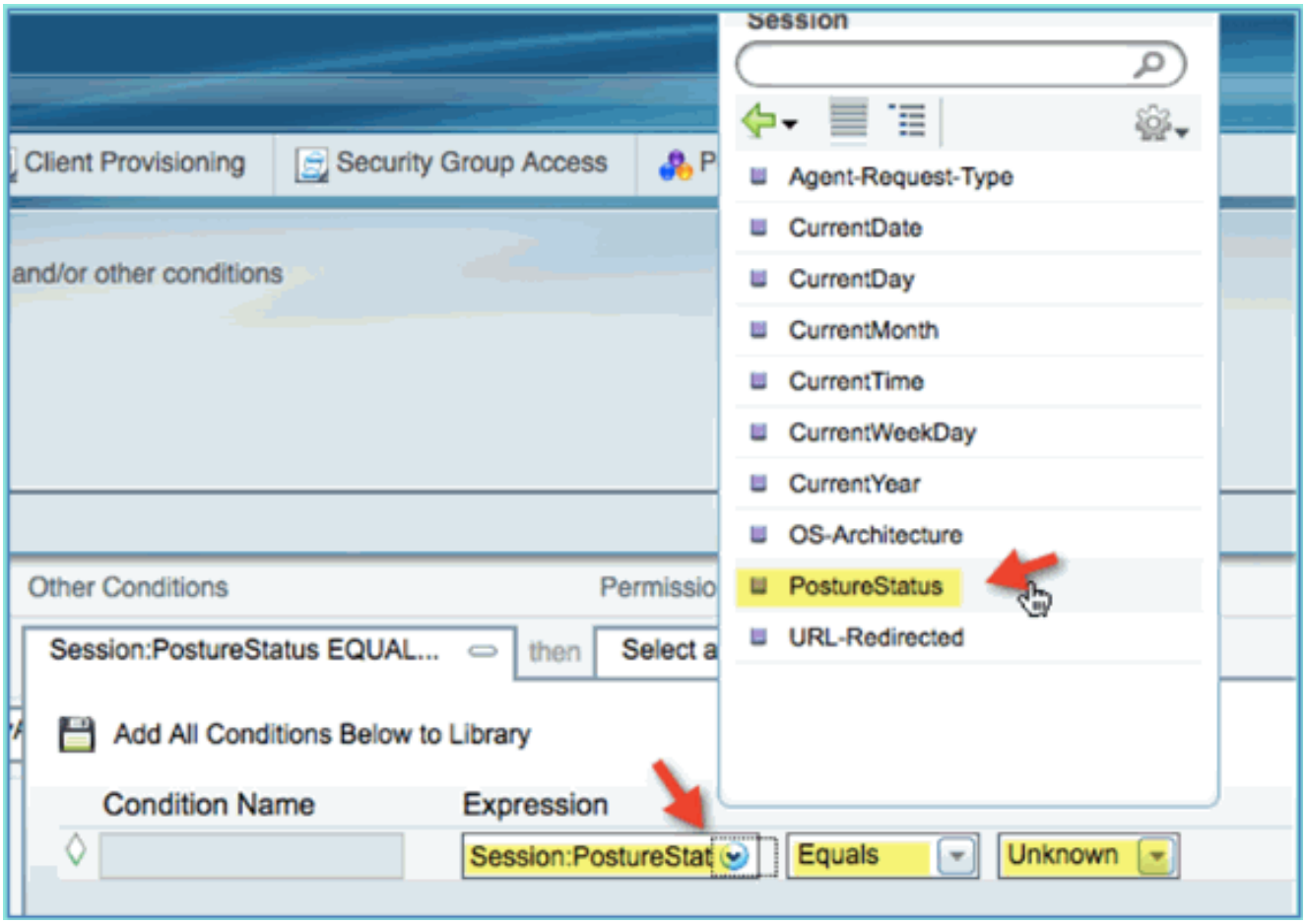
administrador creará la política adecuada para permitir que se identifiquen los terminales desconocidos antes de permitir el acceso. En este ejercicio, se creará la política de autorización para que un nuevo dispositivo se redirija a ISE para la evaluación de estado (para los dispositivos móviles no tienen agente, por lo que solo es relevante la creación de perfiles); los terminales se redirigirán al portal cautivo de ISE y se identificarán.

Complete estos pasos:

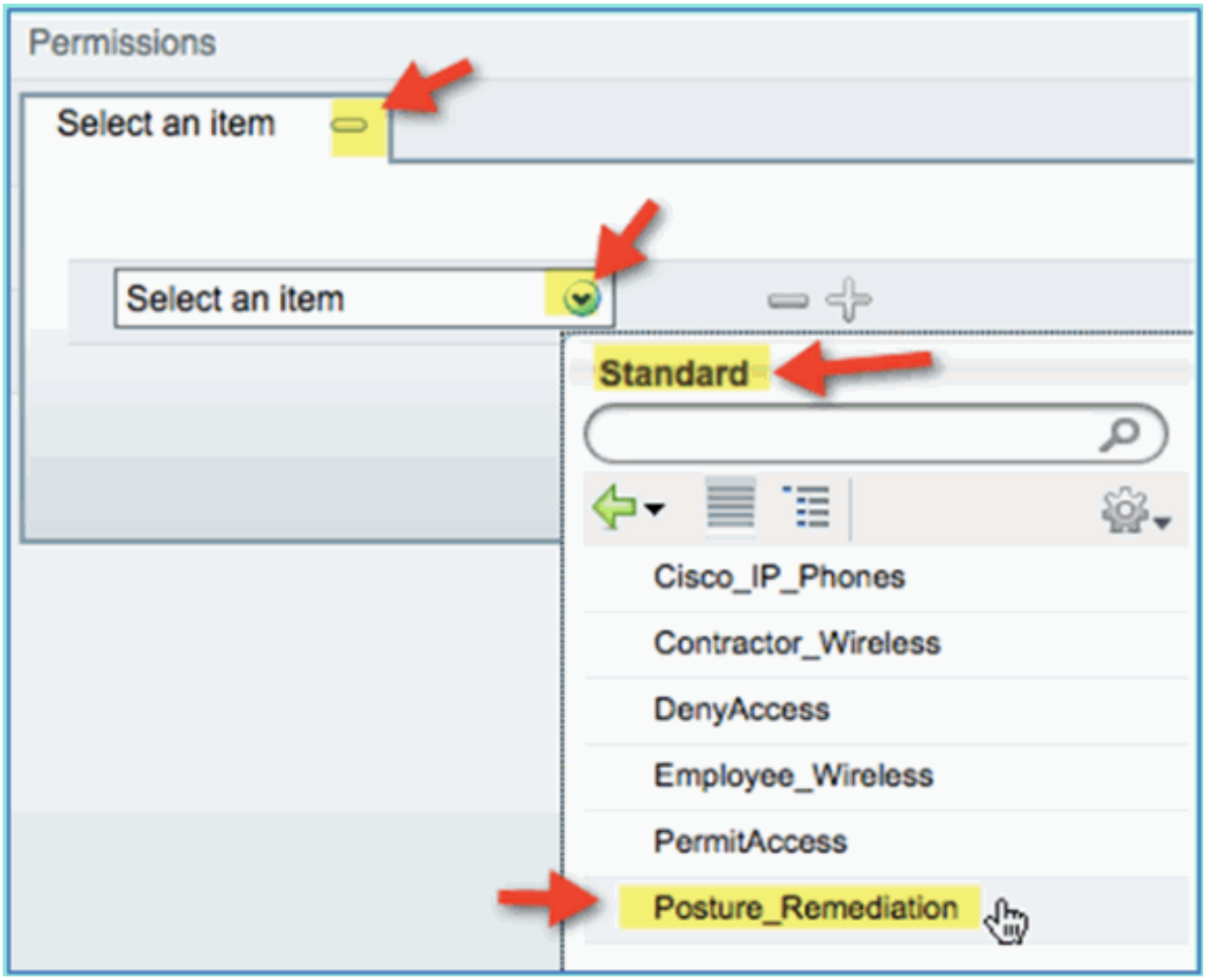
1. En ISE, vaya a **Policy > Authorization**.



2. Existe una política para los teléfonos IP de Cisco con perfil. Esto está fuera de la caja. Edite esto como una política de estado.
3. Introduzca los siguientes valores para esta política:Nombre de regla: Posture_RemediationGrupos de identidades: CualquieraOtras condiciones > Crear nuevo: (Avanzado) Sesión > EstadoCondiciónPostureStatus > Equals: Unknown



4. Establezca lo siguiente para los permisos:Permisos > Estándar: Posture_Remediation

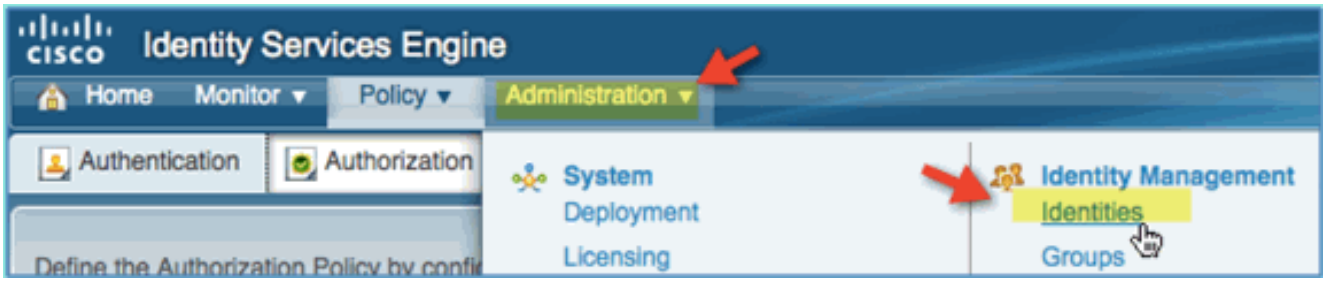


5. Click **Save**.**Nota:** También se pueden crear elementos de política personalizados para facilitar su uso.

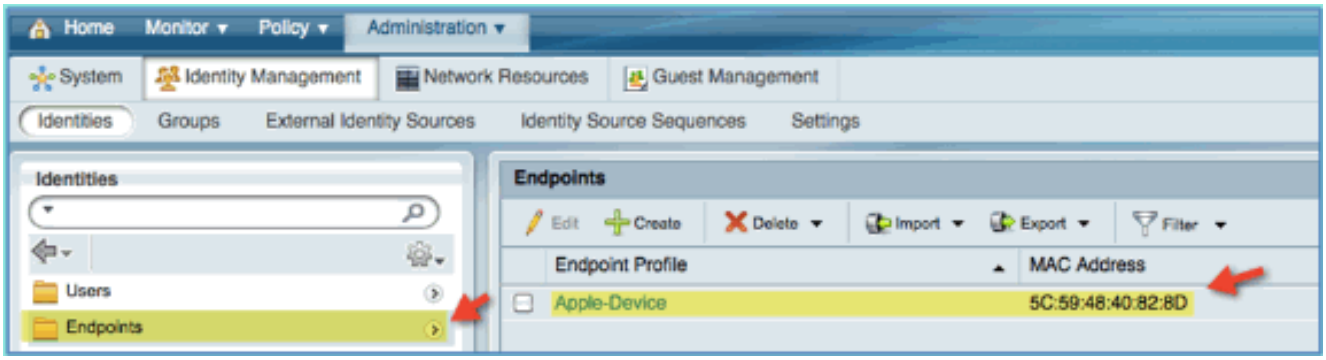
Prueba de la directiva de corrección de estado

Se puede realizar una demostración sencilla para mostrar que ISE está creando un perfil adecuado de un nuevo dispositivo en función de la política de estado.

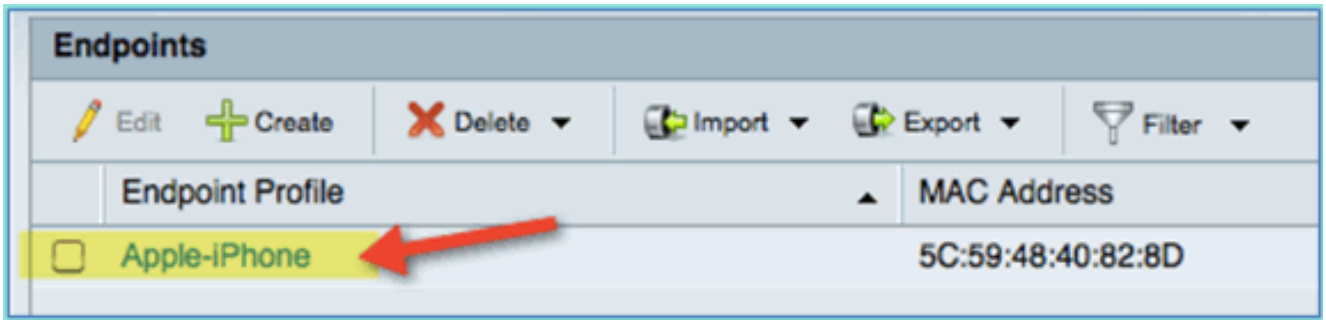
1. En ISE, vaya a **Administration > Identity Management > Identities**.



2. Haga clic en **Terminales**. Asociar y conectar un dispositivo (un iPhone en este ejemplo).



3. Actualice la lista de terminales. Observe qué información se proporciona.
4. En el dispositivo del terminal, vaya a:URL: http://www (o 10.10.10.10)El dispositivo se redirige. Acepte cualquier solicitud de certificados.
5. Una vez que el dispositivo móvil se haya redirigido por completo, desde ISE actualice de nuevo la lista de terminales. Observe lo que ha cambiado. El terminal anterior (por ejemplo, Apple-Device) debería haber cambiado a "Apple-iPhone", etc. La razón es que el sondeo HTTP obtiene efectivamente información de agente de usuario, como parte del proceso de redirección al portal
cautivo.

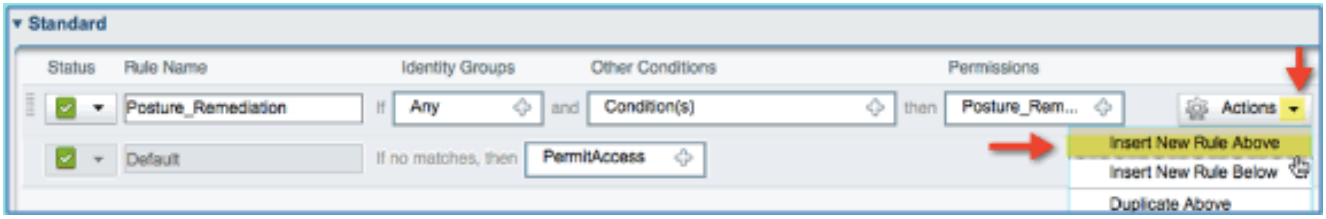


Política de autorización para el acceso diferenciado

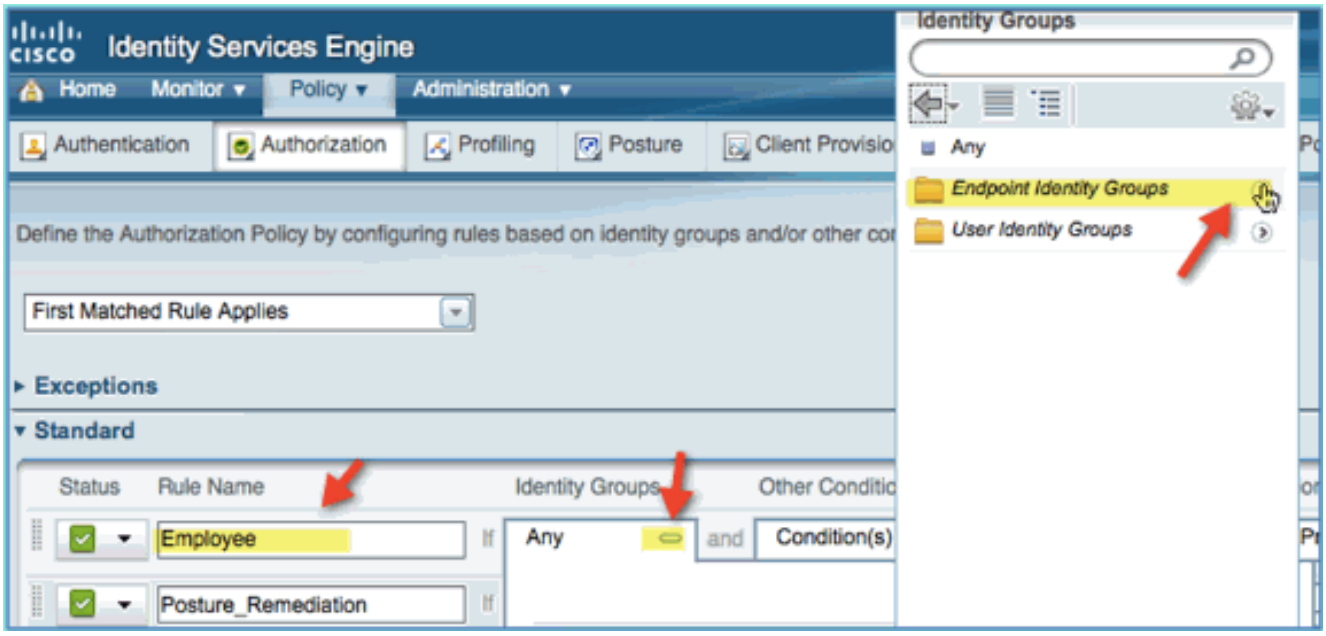
Después de probar correctamente la autorización de estado, continúe creando políticas para admitir el acceso diferenciado para el empleado y el contratista con dispositivos conocidos y diferentes asignaciones de VLAN específicas para el rol de usuario (en este escenario, empleado y contratista).

Complete estos pasos:

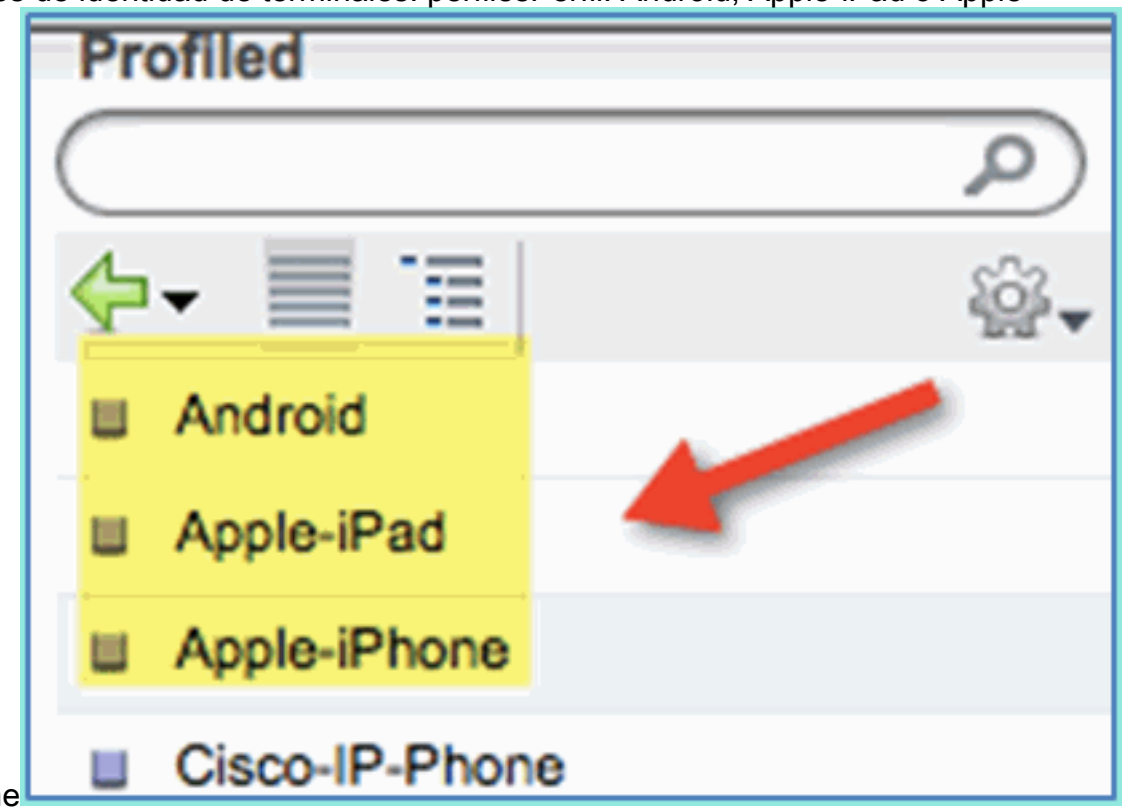
1. Vaya a **ISE > Policy > Authorization**.
2. Agregue o inserte una nueva regla encima de la línea o directiva de corrección de estado.



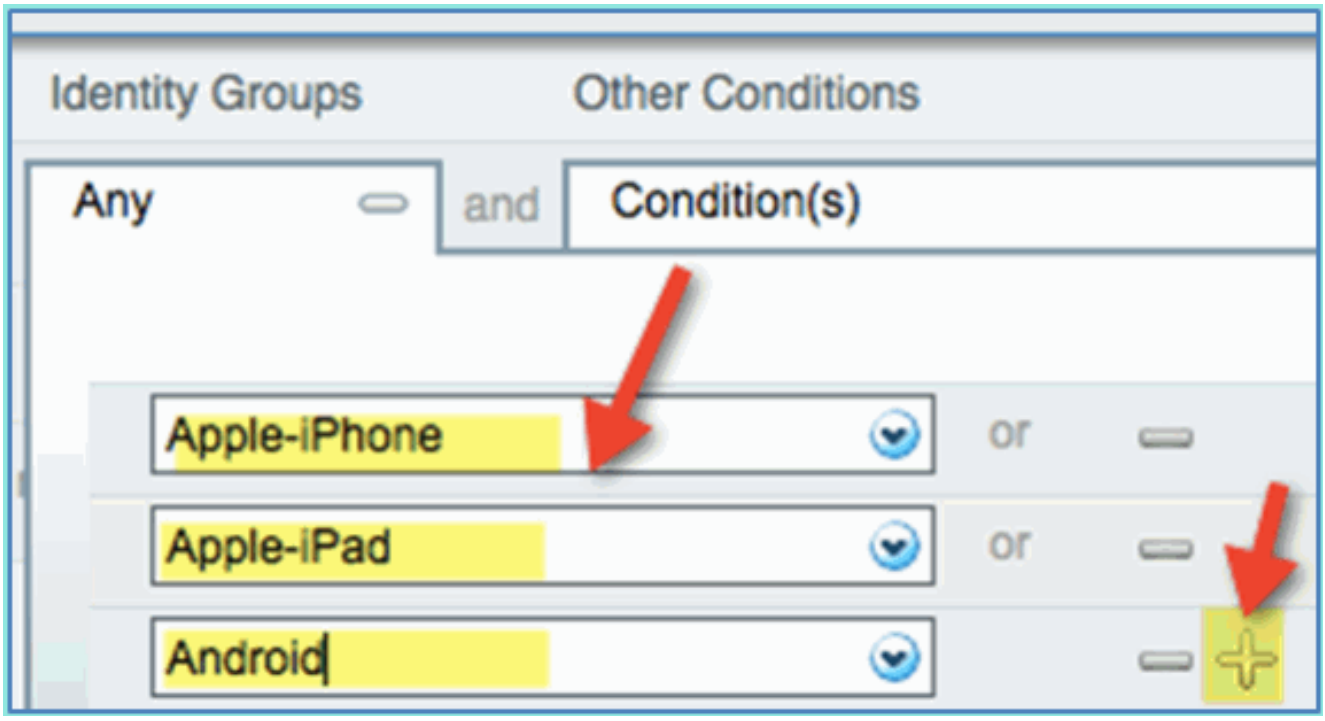
3. Introduzca los siguientes valores para esta política:Nombre de regla: EmpleadoGrupos de identidades (expandir): grupos de identidades de
terminales



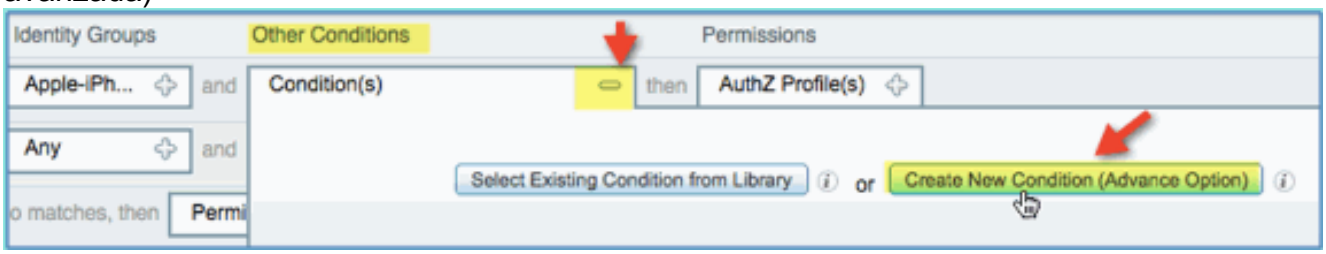
Grupos de identidad de terminales: perfilesPerfil: Android, Apple-iPad o Apple-iPhone



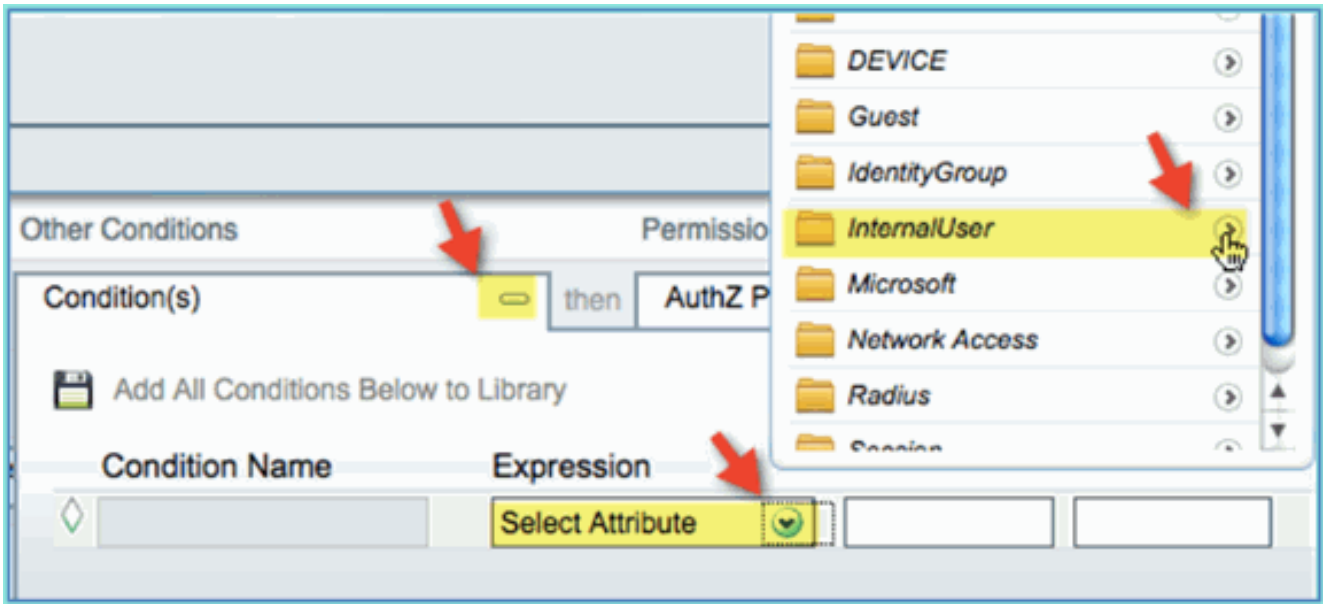
4. Para especificar tipos de dispositivos adicionales, haga clic en **+** y agregue más dispositivos (si es necesario):Grupos de identidad de terminales: perfilesPerfil: Android, Apple-iPad o Apple-iPhone



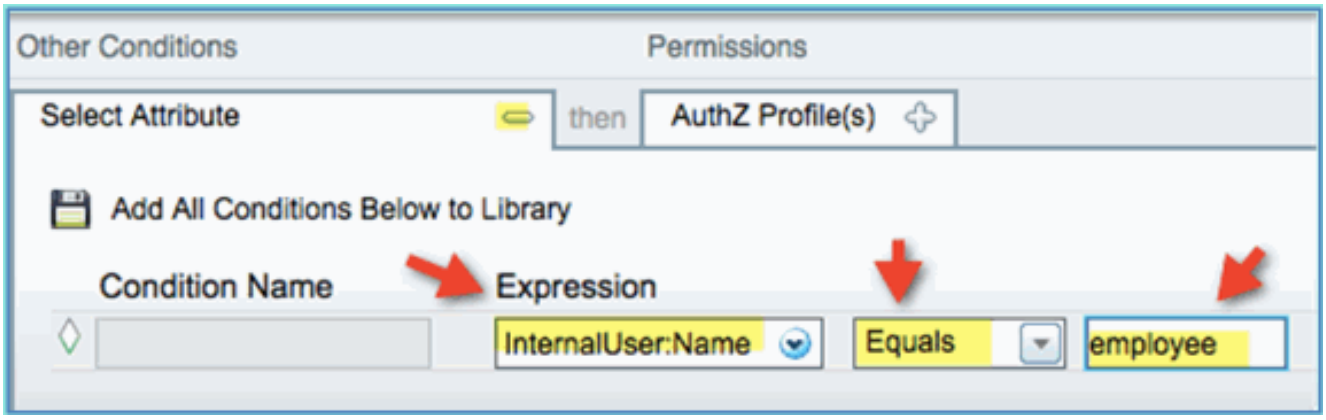
5. Especifique los siguientes valores de permisos para esta directiva:Otras condiciones (ampliar): Crear nueva condición (opción avanzada)



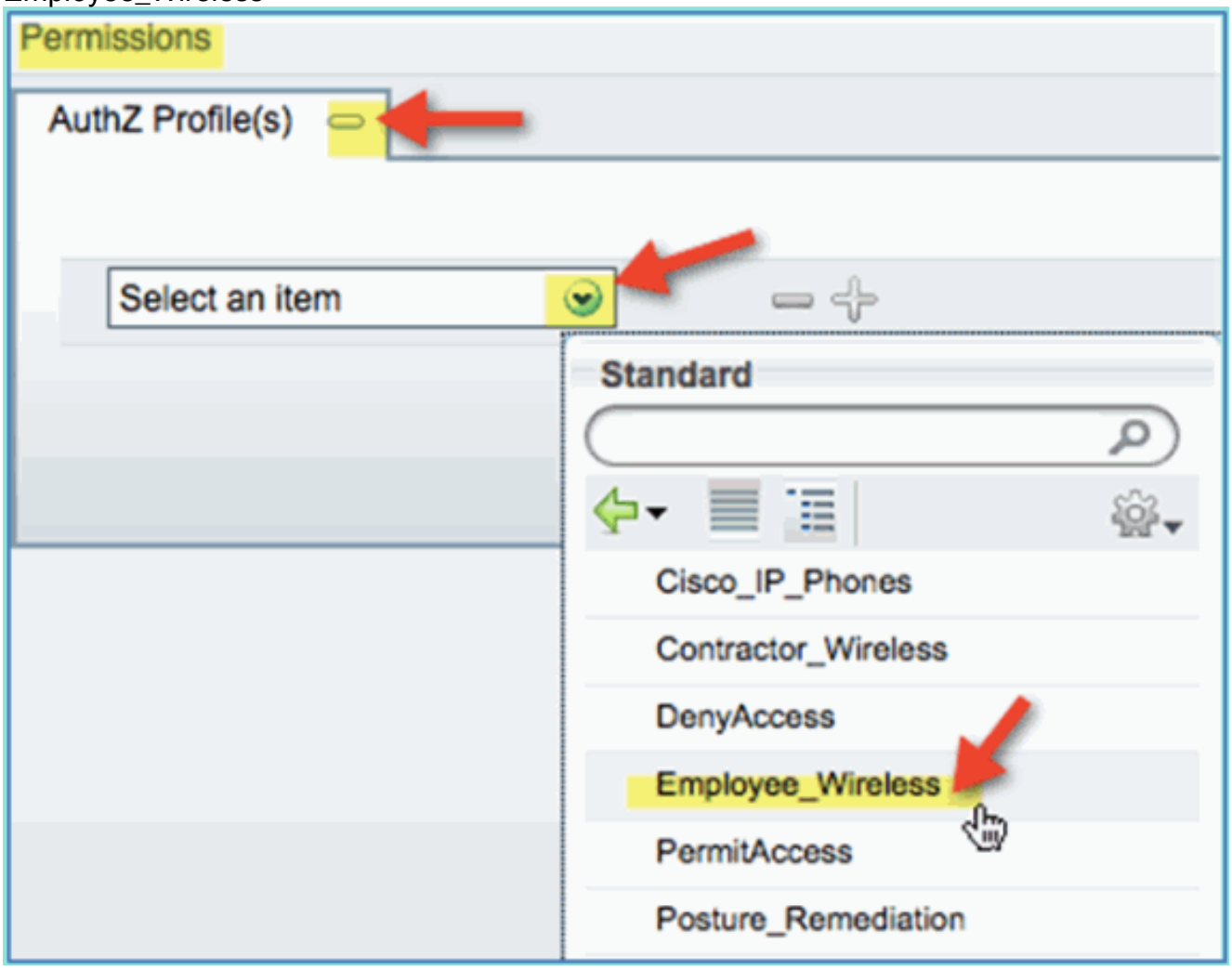
Condición > Expresión (de la lista): UsuarioInterno > Nombre



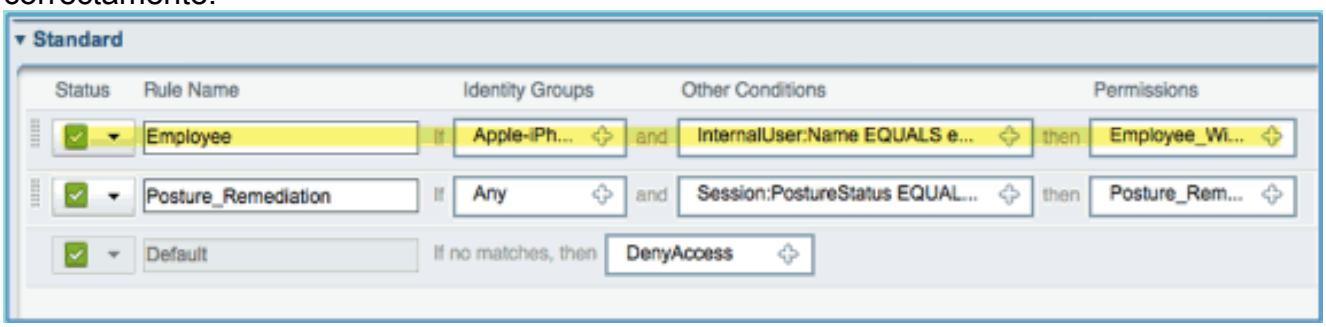
InternalUser > Name: employee



6. Agregar una condición para la sesión de estado Conforme:Permisos > Perfiles > Estándar: Employee_Wireless

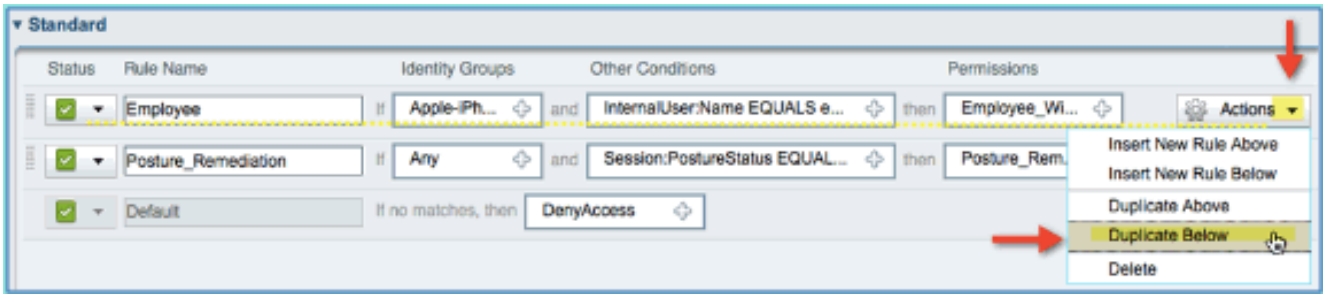


7. Click **Save**. Confirme que la política se ha agregado correctamente.

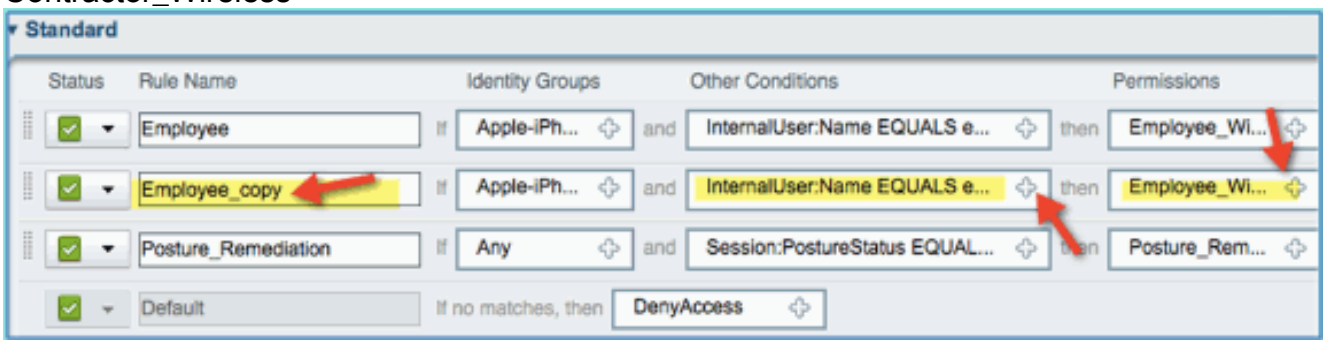


8. Continúe agregando la directiva Contratista. En este documento, la política anterior se duplica para acelerar el proceso (o, puede configurar manualmente para una buena

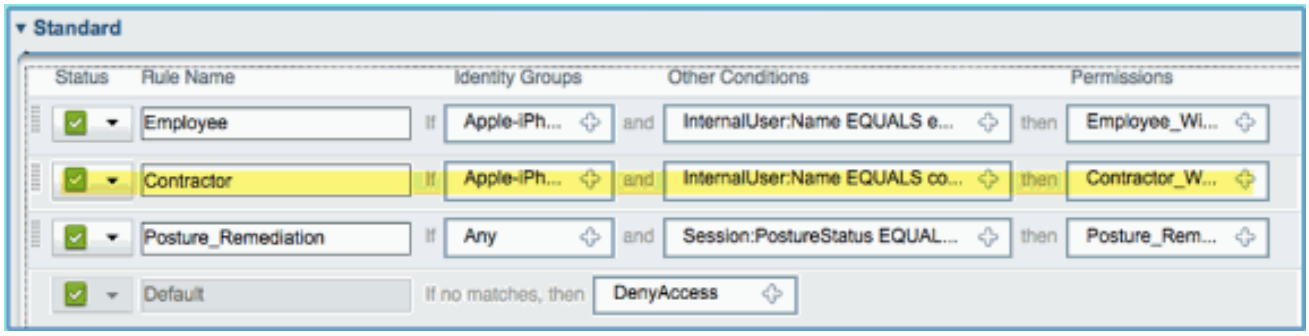
práctica).En la directiva de empleado > Acciones, haga clic en **Duplicar a continuación**.



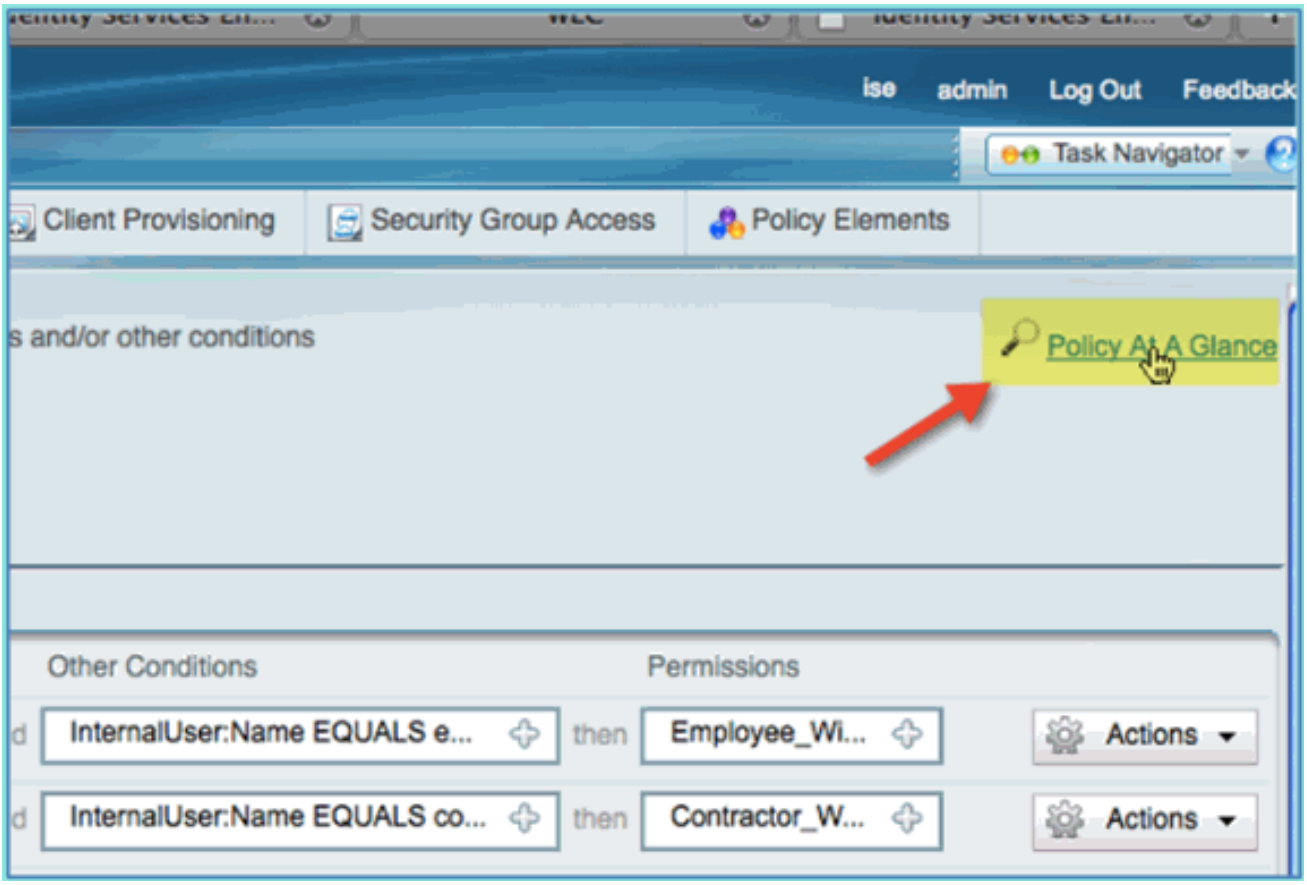
9. Edite los campos siguientes de esta directiva (copia duplicada):Nombre de regla: ContratistaOtras condiciones > Usuario interno > Nombre: contratistaPermisos: Contractor_Wireless



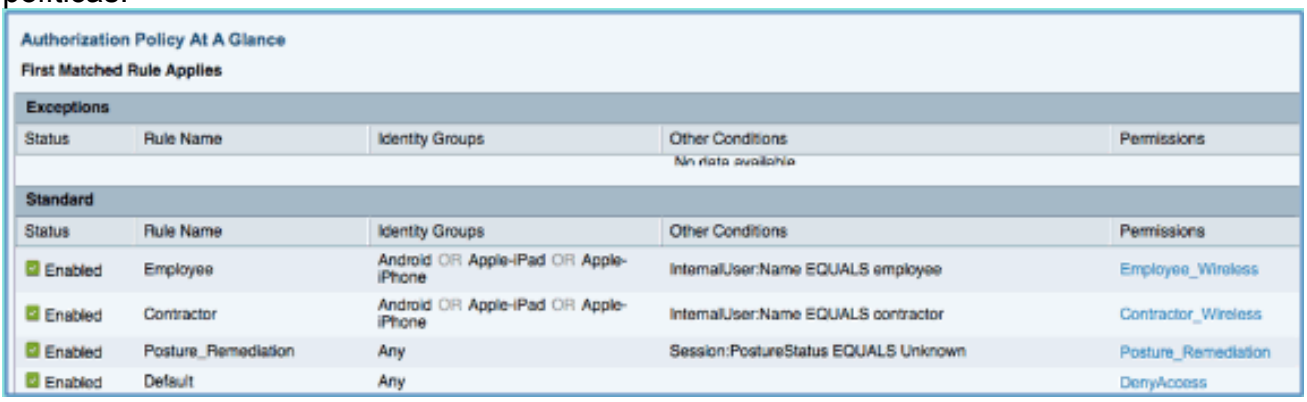
10. Click **Save**. Confirme que la copia duplicada anterior (o la nueva directiva) esté configurada correctamente.



11. Para obtener una vista previa de las directivas, haga clic en **Policy-at-a-Glance**.



La vista de resumen de políticas ofrece un resumen consolidado y facilita la visualización de las
políticas.



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
Enabled	Employee	Android OR Apple-iPad OR Apple-iPhone	InternalUser:Name EQUALS employee	Employee_Wireless
Enabled	Contractor	Android OR Apple-iPad OR Apple-iPhone	InternalUser:Name EQUALS contractor	Contractor_Wireless
Enabled	Posture_Remediation	Any	Session:PostureStatus EQUALS Unknown	Posture_Remediation
Enabled	Default	Any		DenyAccess

Prueba de CoA para el acceso diferenciado

Con las políticas y los perfiles de autorización preparados para diferenciar el acceso, es el momento de realizar pruebas. Al tener una única WLAN segura, se asignará a un empleado la VLAN del empleado y a un contratista la VLAN del contratista. En los siguientes ejemplos se utiliza un iPhone/iPad de Apple.

Complete estos pasos:

1. Conéctese a la WLAN segura (POD1x) con el dispositivo móvil y utilice estas credenciales:Nombre de usuario: empleadoContraseña:
   XXXXX

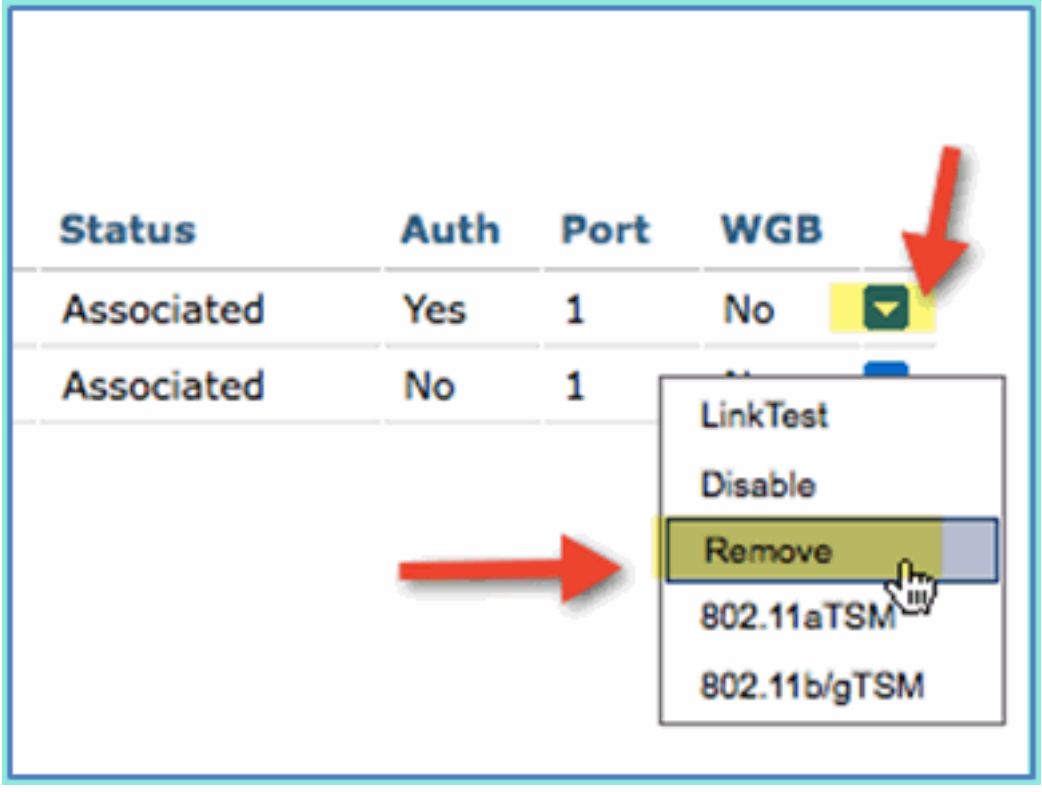
2. Haga clic en **Unirse**. Confirme que se ha asignado al empleado la VLAN 11 (VLAN de empleado).

3. Haga clic en **Olvidar esta red**. Confirme haciendo clic en

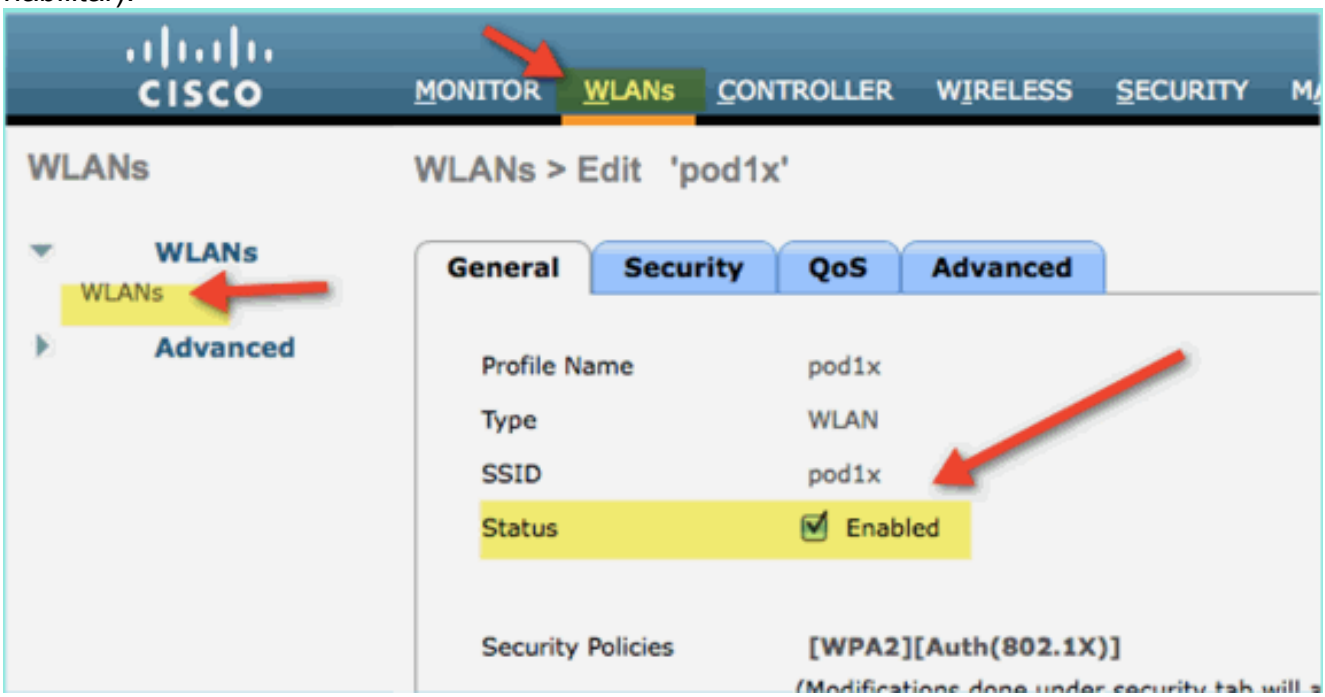
Olvidar.

4. Vaya a WLC y quite las conexiones de cliente existentes (si se utilizó la misma en los pasos anteriores). Navegue hasta **Monitor > Clients > MAC address**, luego haga clic en **Remove**.


CISCO
MONITOR
WLANs
Monitor
Clients
Summary
Current Filter
Access Points
Cisco CleanAir
Client MAC Addr
Statistics
44:2a:60:f7:3a:4a
CDP
5c:59:48:40:82:8d
Rogues
Clients
Multicast


Status
Auth
Port
WGB
Associated
Yes
1
No
Associated
No
1
LinkTest
Disable
Remove
802.11aTSM
802.11b/gTSM

5. Otra forma segura de borrar las sesiones de cliente anteriores es inhabilitar/habilitar la WLAN.Vaya a **WLC > WLAN > WLAN**, después haga clic en el WLAN para editar.Desactive **Activado > Aplicar** (para desactivar).Marque la casilla de verificación **Enabled > Apply** (para volver a
habilitar).

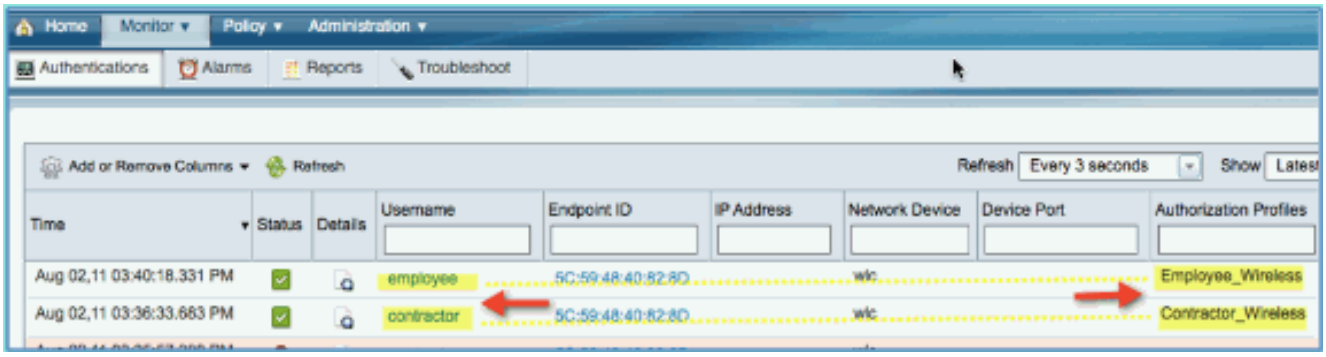


6. Vuelva al dispositivo móvil. Vuelva a conectarse a la misma WLAN con estas credenciales:Nombre de usuario: contratistaContraseña:

XXXX

7. Haga clic en **Unirse**. Confirme que al usuario del contratista se le asigna la VLAN 12 (VLAN de
contratista/invitado).

8. Puede consultar la vista de registro en tiempo real de ISE en **ISE > Monitor > Authorization**. Debería ver a los usuarios individuales (empleado, contratista) obtener perfiles de autorización diferenciados (Employee_Wireless vsContractor_Wireless) en diferentes VLAN.



WLAN de invitado WLC

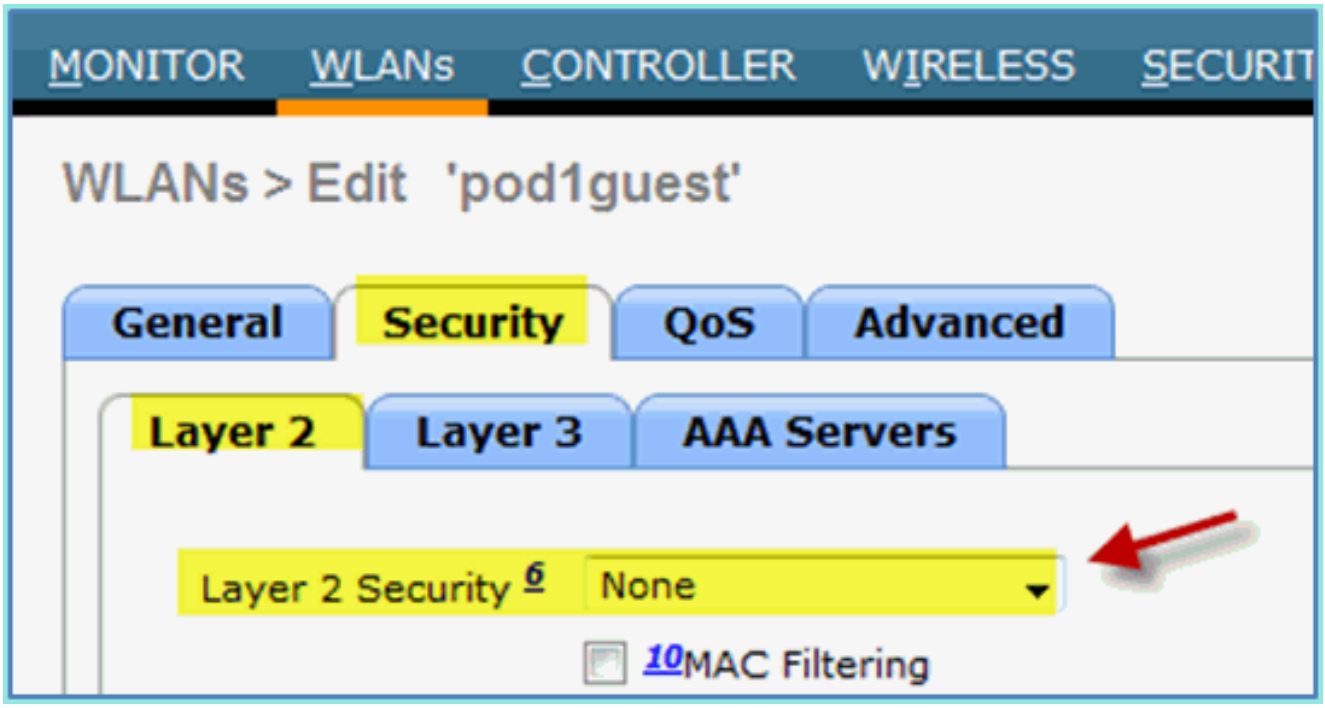
Complete estos pasos para agregar una WLAN de invitado para permitir que los invitados

accedan al Portal de invitados del patrocinador de ISE:

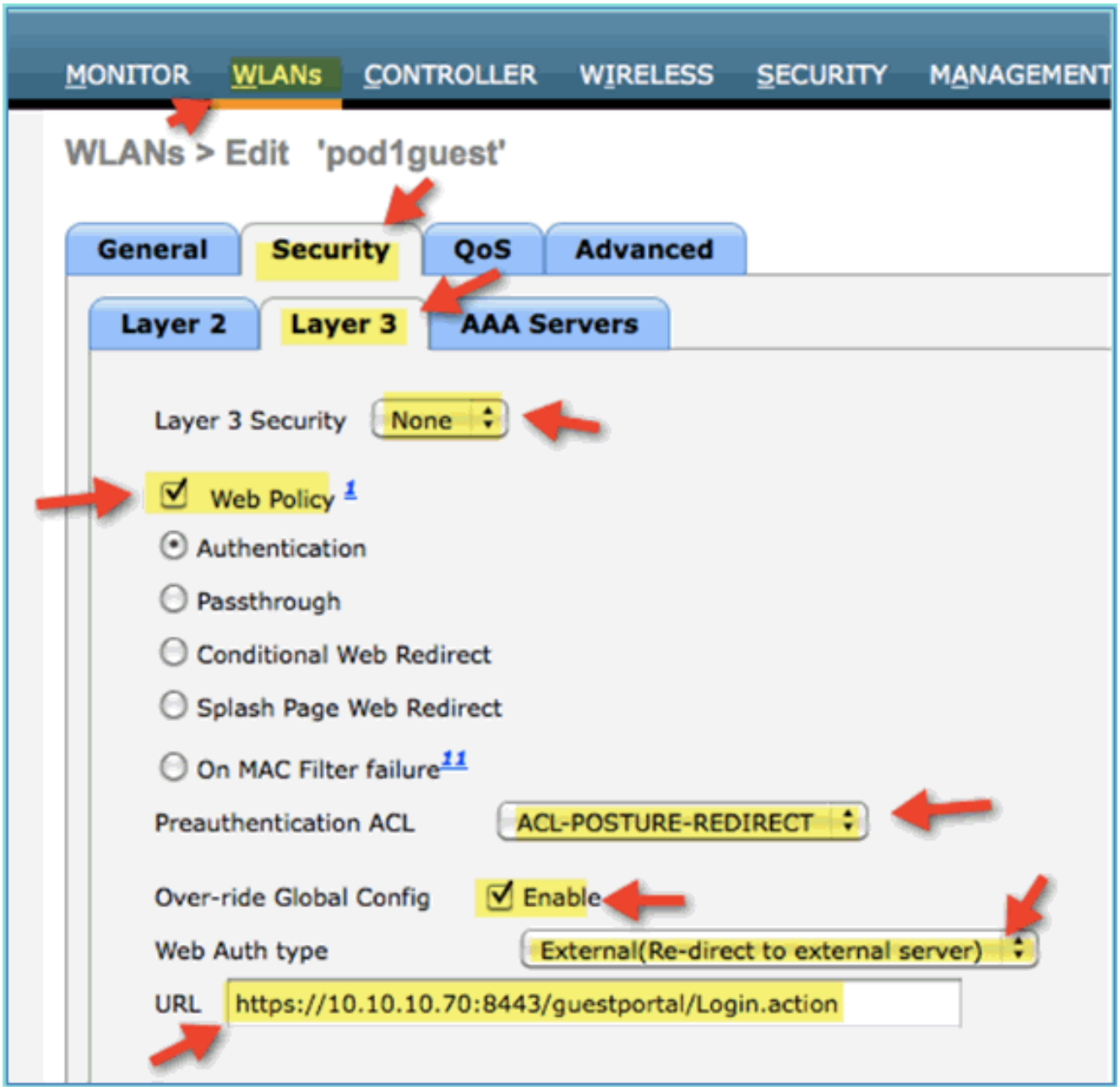
1. Desde WLC, navegue hasta **WLAN > WLAN > Add New**.
2. Introduzca lo siguiente para la nueva WLAN de invitado:Nombre del perfil: pod1guestSSID: pod1guest

3. Haga clic en Apply (Aplicar).
4. Introduzca lo siguiente en la ficha WLAN > General de invitado:Estado: DesactivadoInterfaz/Grupo de interfaces: Invitado

5. Navegue hasta **WLAN > Security > Layer2** de invitado e ingrese lo siguiente:Seguridad de capa 2:
   ninguna



6. Navegue hasta **WLAN > Security > Layer3** tab e ingrese lo siguiente:Seguridad de capa 3: ningunaPolítica web: habilitadaSubvalor de política web: autenticaciónACL de autenticación previa: ACL-POSTURE-REDIRECTTipo de autenticación web: externa (redirección a servidor externo)URL: https://10.10.10.70:8443/guestportal/Login.action



7. Haga clic en Apply (Aplicar).
8. Asegúrese de **guardar la configuración del WLC**.

Prueba de la WLAN de invitado y el portal de invitados

Ahora puede probar la configuración de la WLAN de invitado. Debe redirigir a los invitados al portal de invitados de ISE.

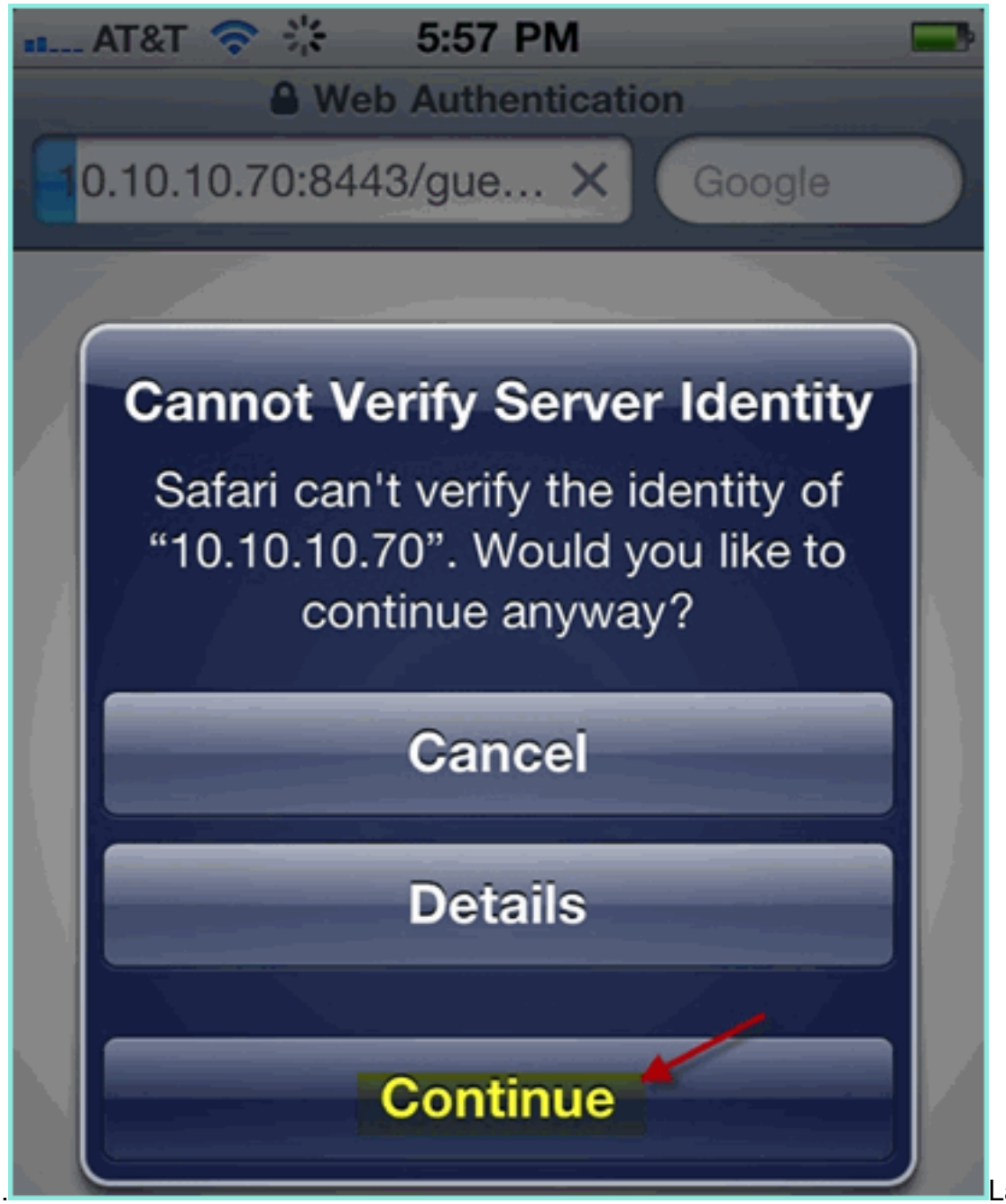
Complete estos pasos:

1. Desde un dispositivo iOS como un iPhone, navegue hasta **Wi-Fi Networks > Enable**. A continuación, seleccione la red de invitado de

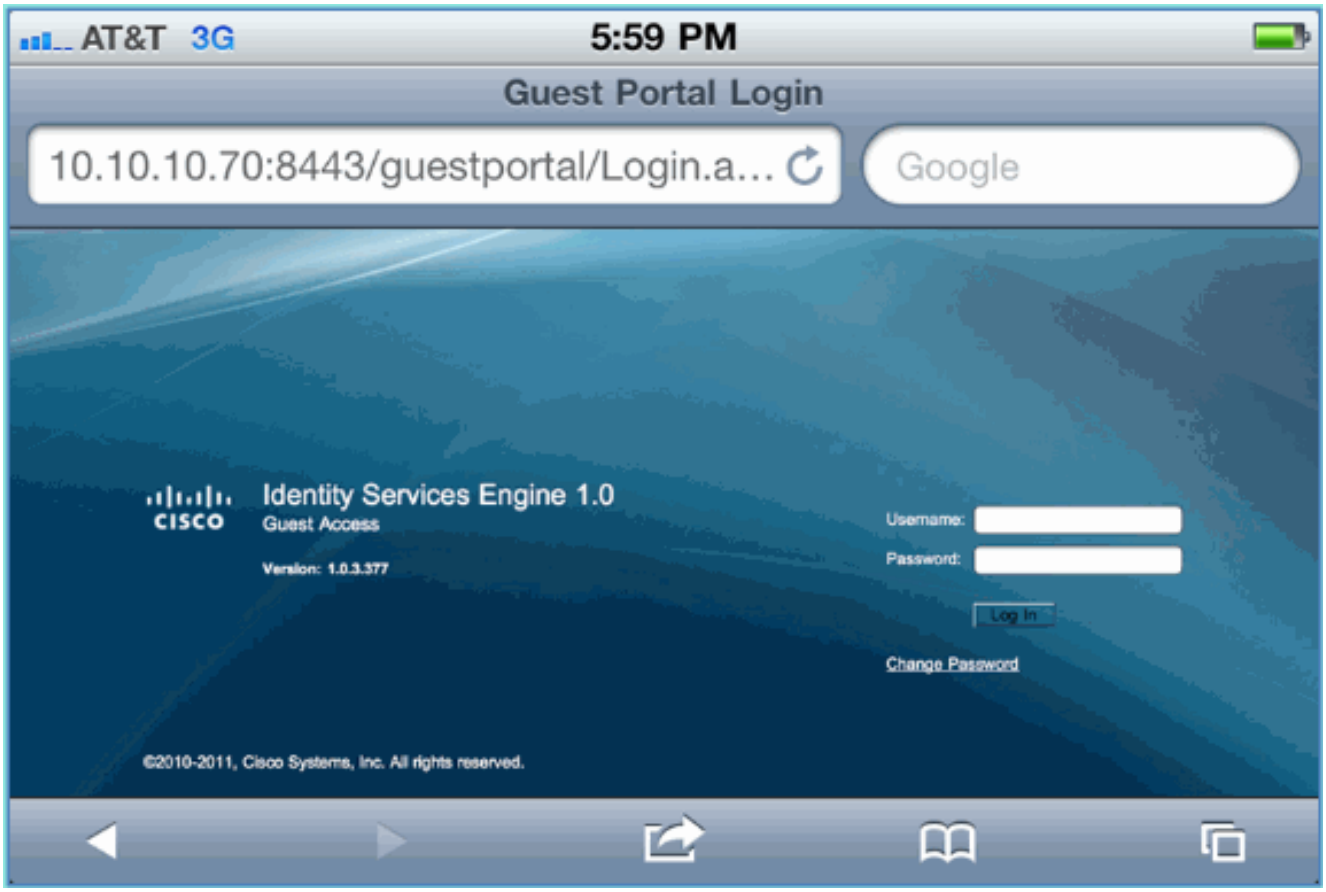
POD.

2. El dispositivo con iOS debe mostrar una dirección IP válida de la VLAN de invitado (10.10.12.0/24).

3. Abra el navegador Safari y conéctese a:URL: http://10.10.10.10Aparece una redirección de autenticación Web.
4. Haga clic en **Continuar** hasta que llegue a la página del portal de invitados de



ISE. La siguiente captura de pantalla de ejemplo muestra el dispositivo iOS en un inicio de sesión en el portal de invitados. Esto confirma que la configuración correcta para WLAN e ISE Guest Portal está
activa.

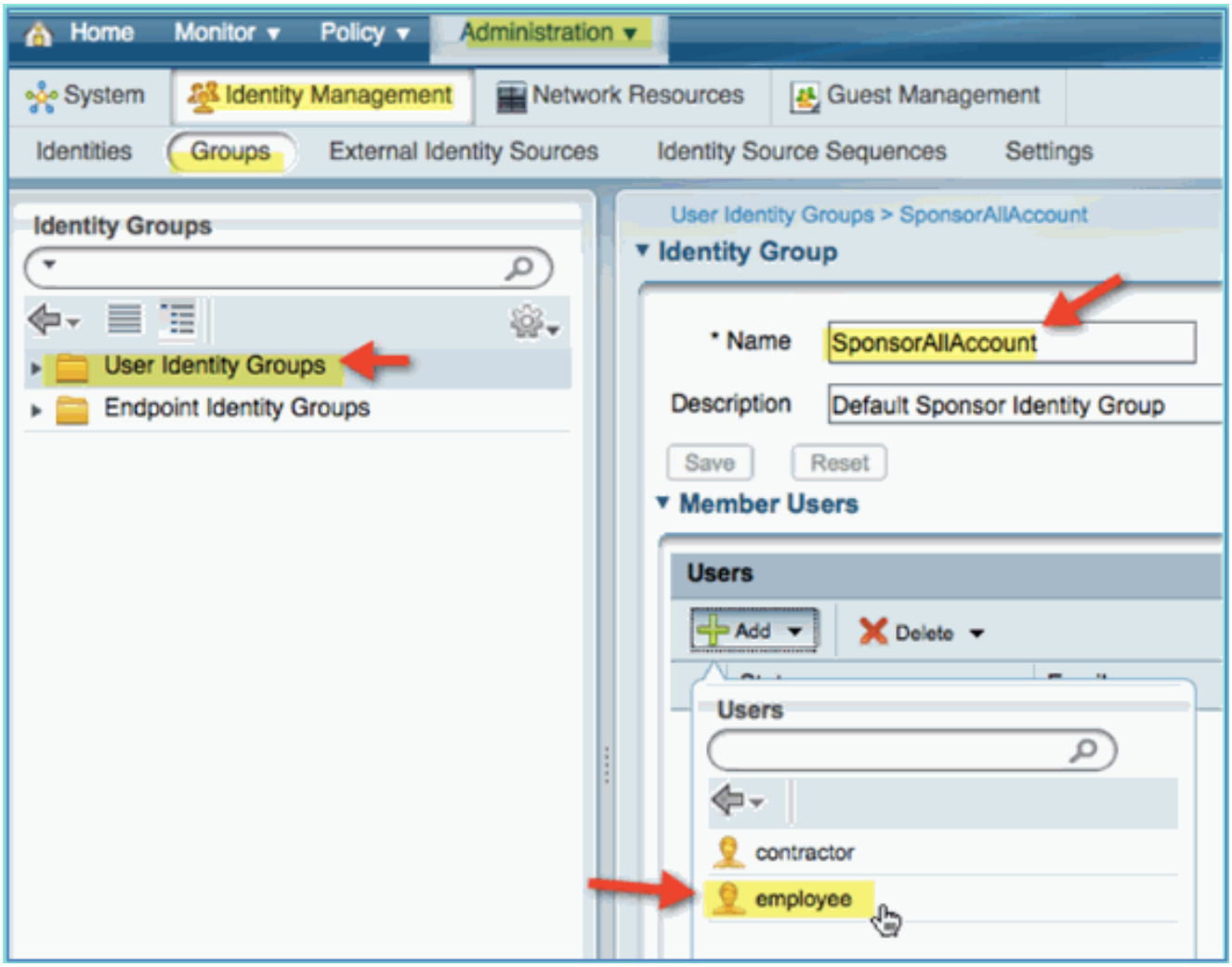


Acceso de invitados patrocinado por tecnología inalámbrica ISE

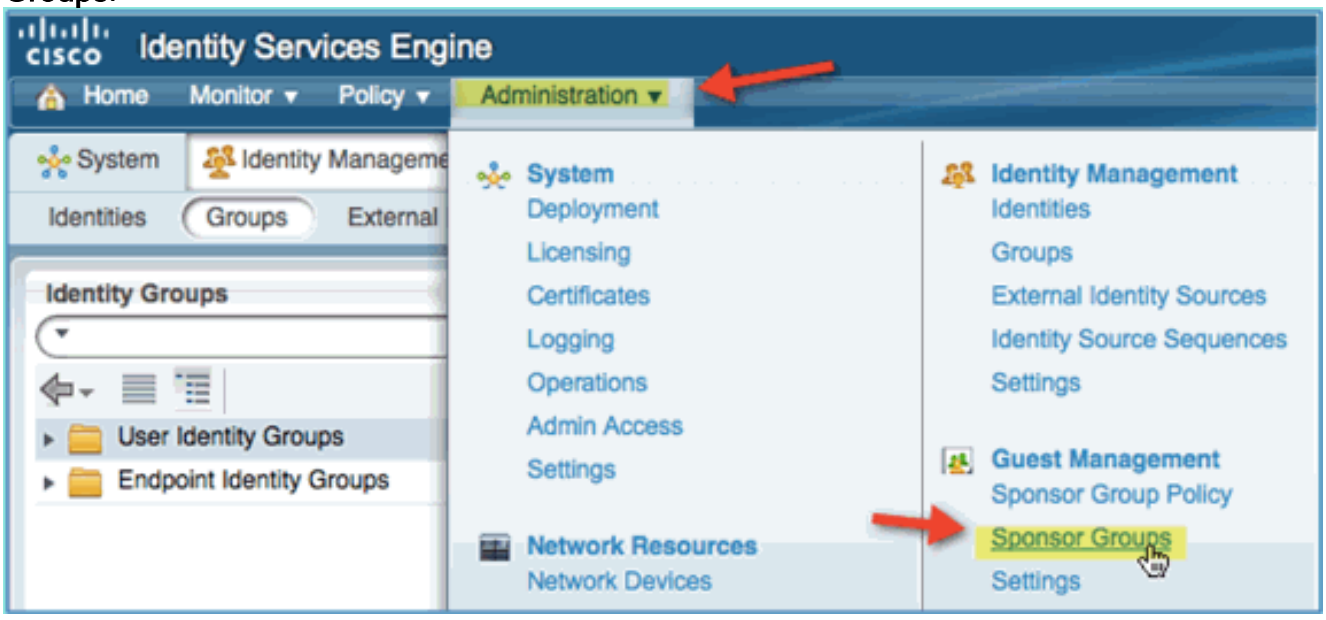
ISE se puede configurar para que los invitados puedan recibir patrocinio. En este caso, configurará las políticas de invitado de ISE para permitir que los usuarios internos o de dominio AD (si están integrados) patrocinen el acceso de invitado. También configurará ISE para permitir que los patrocinadores vean la contraseña de invitado (opcional), lo que resulta útil para este laboratorio.

Complete estos pasos:

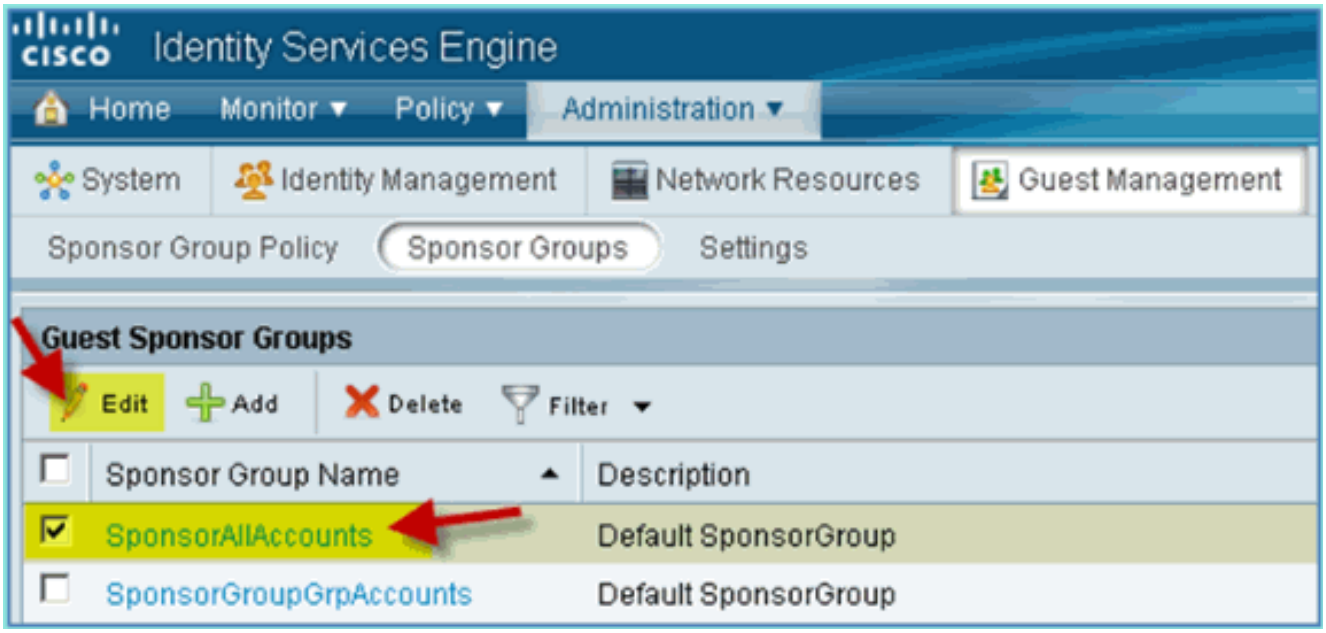
1. Agregue el usuario empleado al grupo PatrocinadorTodasLasCuentas. Hay diferentes formas de hacerlo: ir directamente al grupo o editar el usuario y asignar el grupo. Para este ejemplo, navegue hasta **Administration > Identity Management > Groups > User Identity Groups**. A continuación, haga clic en **SponsorAllAccount** y agregue el usuario de empleado.



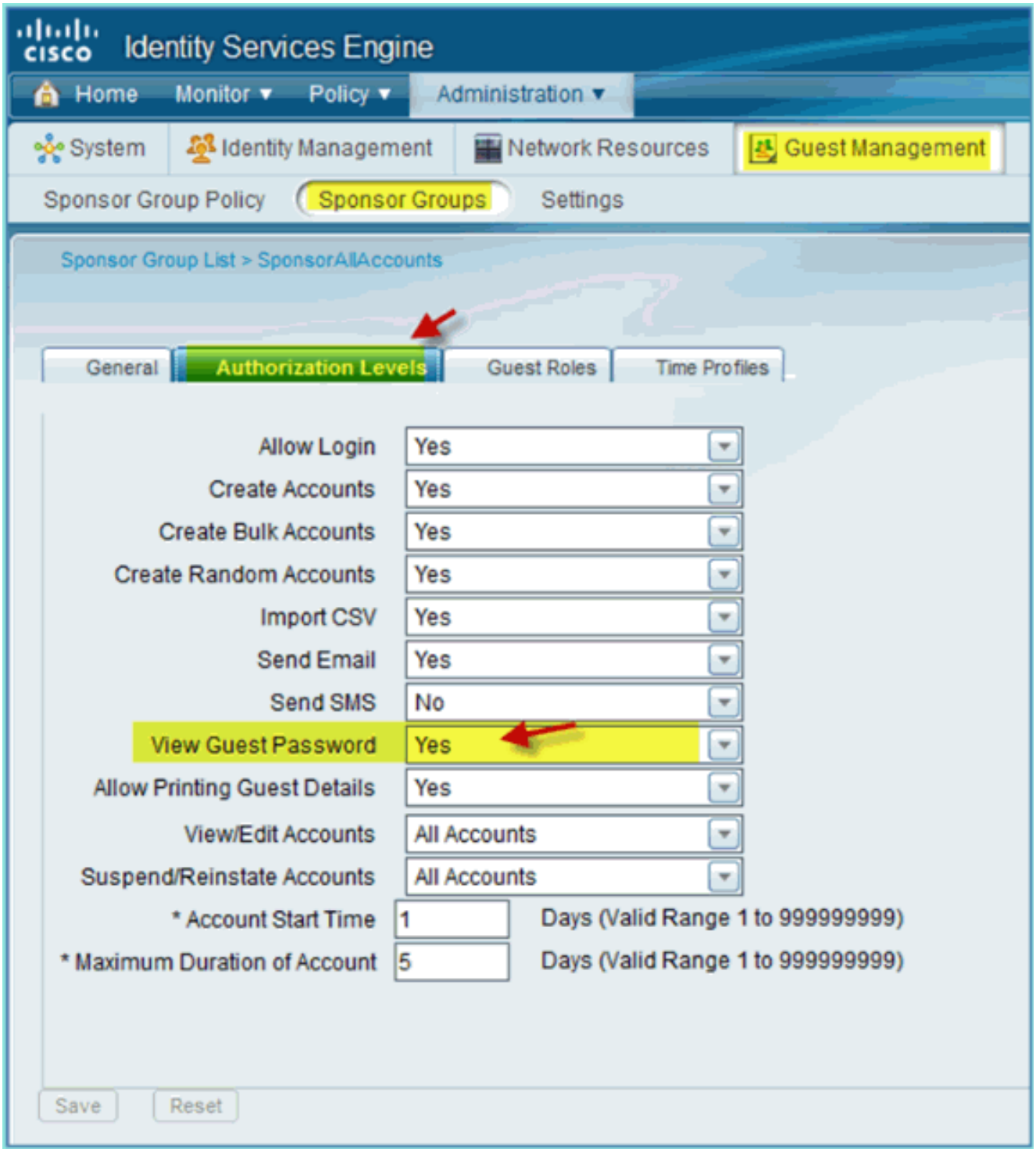
2. Vaya a **Administration > Guest Management > Sponsor Groups**.



3. Haga clic en **Editar** y, a continuación, seleccione **PatrocinadorTodasCuentas**.



4. Seleccione Niveles de autorización y establezca lo siguiente:Ver contraseña de invitado: Sí



5. Haga clic en **Guardar** para completar esta tarea.

Invitado patrocinador

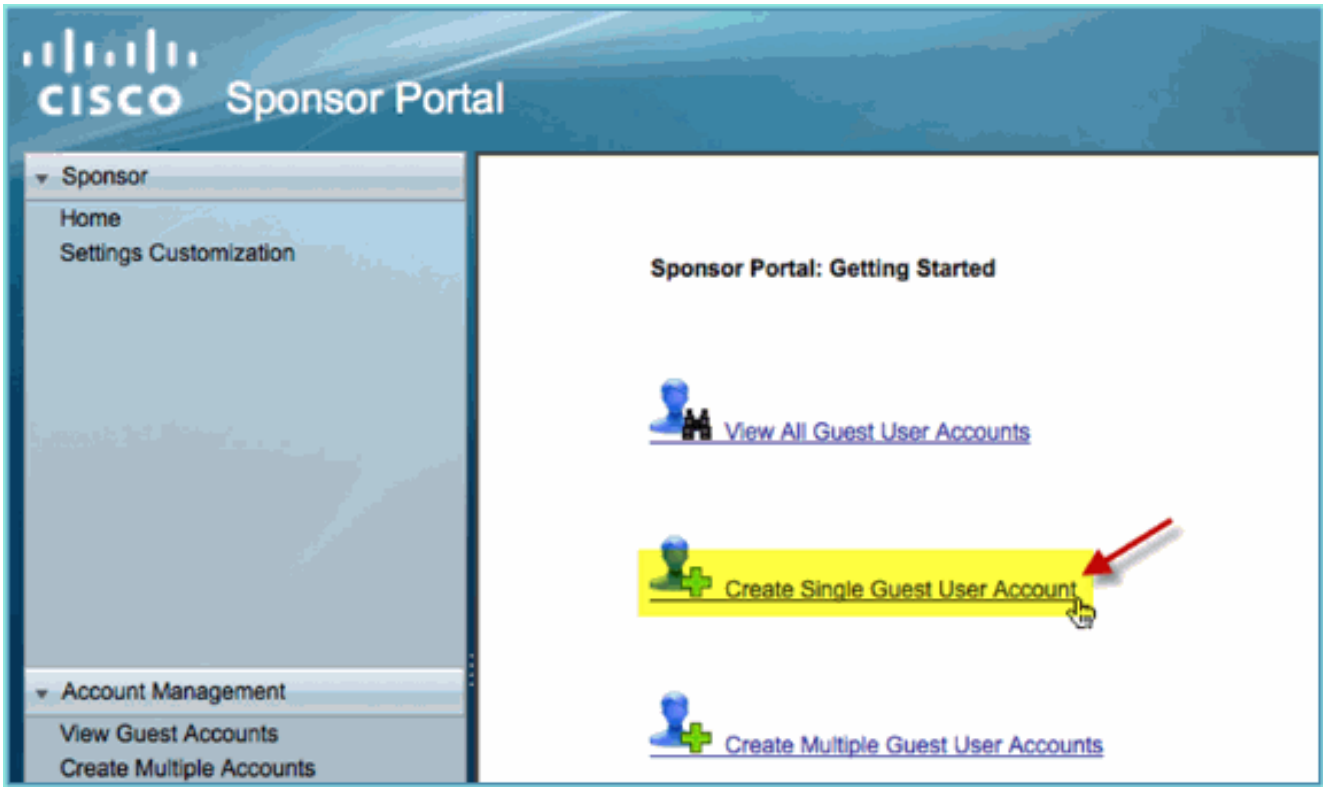
Anteriormente, ha configurado la política y los grupos de invitados adecuados para permitir que los usuarios del dominio AD patrocinen invitados temporales. A continuación, accederá al portal de patrocinadores y creará un acceso de invitado temporal.

Complete estos pasos:

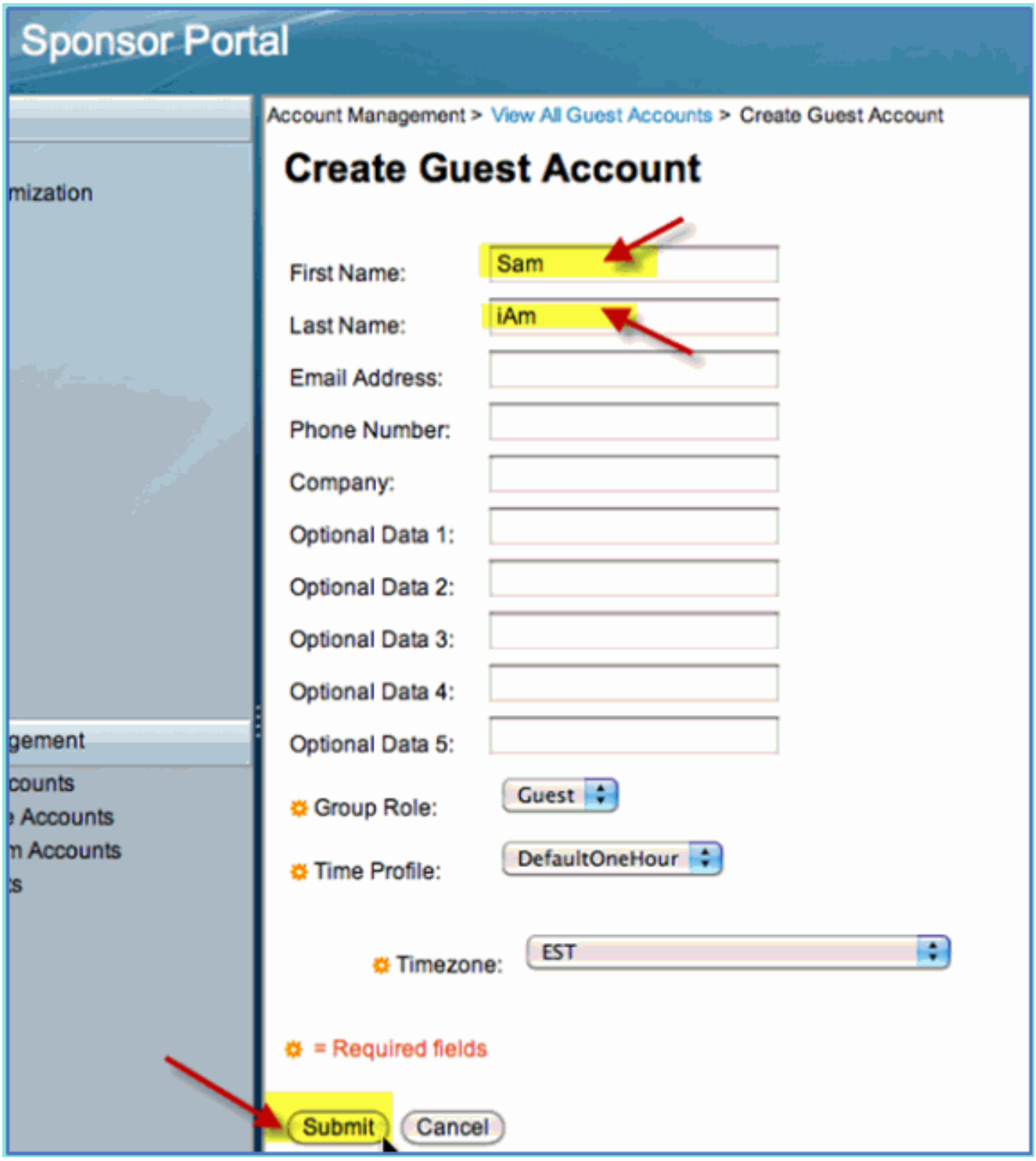
1. Desde un navegador, navegue hasta cualquiera de estas URL: http://<ise ip>:8080/patroportal/ **o** https://<ise ip>:8443/patroportal/. A continuación, inicie sesión con lo siguiente:Nombre de usuario: aduser (Active Directory), employee (Internal

User)Contraseña:
XXXX

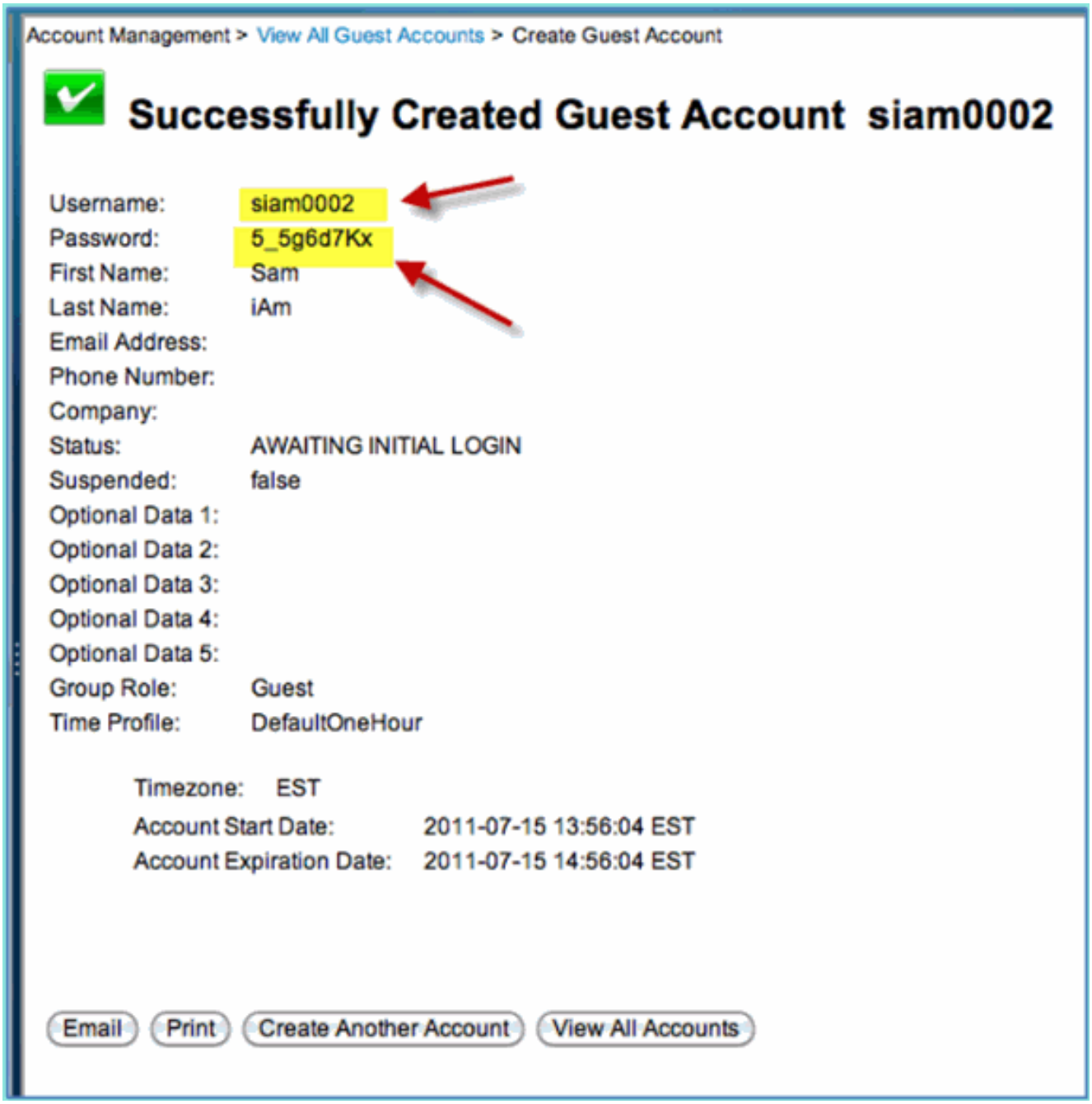
2. En la página Patrocinador, haga clic en **Crear cuenta de usuario de invitado única**.



3. Para un invitado temporal, agregue lo siguiente:Nombre: Obligatorio (por ejemplo, Juan)Apellidos: Obligatorio (por ejemplo, José)Función de grupo: InvitadoPerfil de tiempo: DefaultOneHourZona horaria: Cualquiera/Por
defecto



4. Haga clic en Submit (Enviar).
5. Se crea una cuenta de invitado basada en su entrada anterior. Tenga en cuenta que la contraseña está visible (del ejercicio anterior) en lugar del hash ***.
6. Deje esta ventana abierta mostrando el nombre de usuario y la contraseña del invitado. Los utilizará para probar el inicio de sesión en el portal de invitados (siguiente).



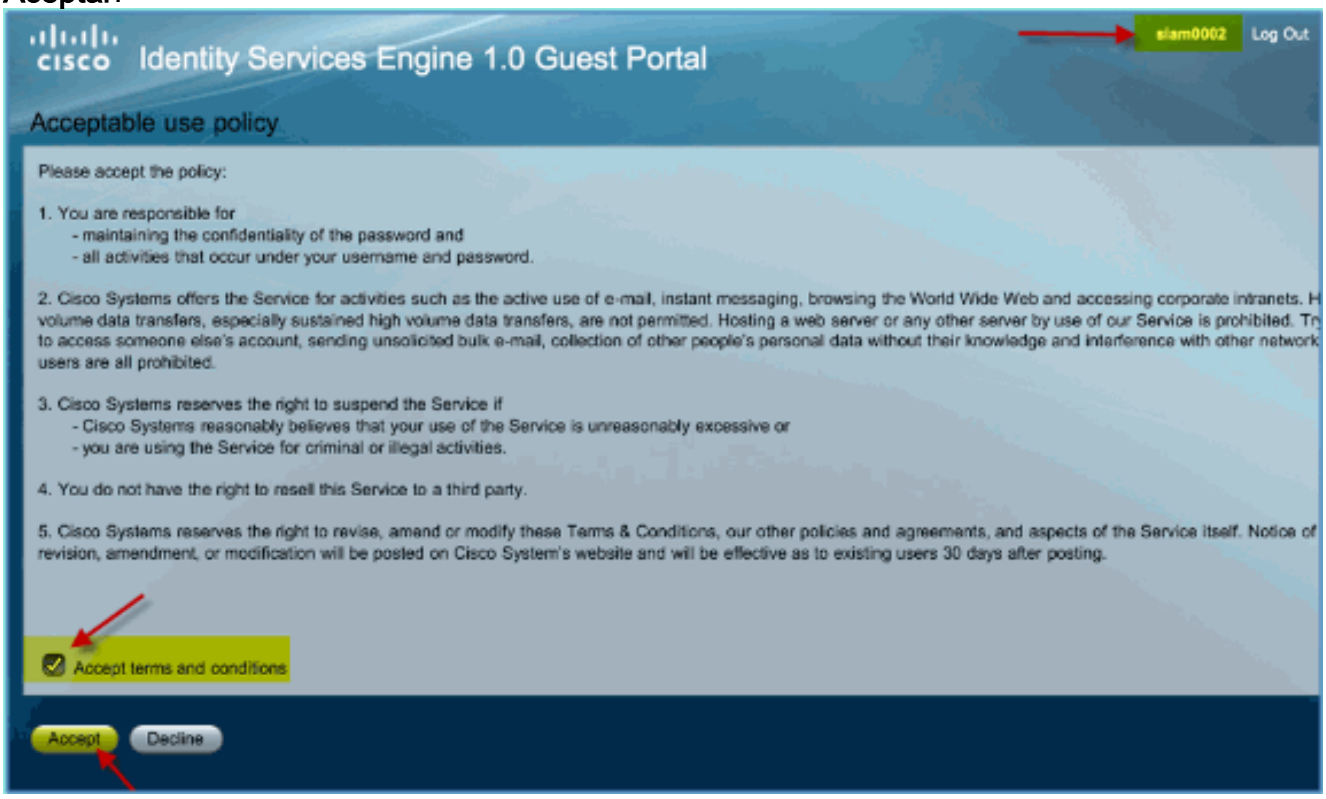
Prueba del acceso al portal de invitados

Con la nueva cuenta de invitado creada por un usuario/patrocinador de AD, es hora de probar el portal de invitados y el acceso.

Complete estos pasos:

1. En un dispositivo preferido (en este caso, un iOS/iPad de Apple), conéctese al SSID de invitado de grupo y compruebe la dirección IP/conectividad.
2. Utilice el explorador e intente navegar hasta http://www.Se le redirigirá a la página de inicio de sesión del portal de
invitados.

3. Inicie sesión con la cuenta de invitado creada en el ejercicio anterior.Si se realiza correctamente, aparecerá la página de políticas de uso aceptable.
4. Marque **Aceptar términos y condiciones** y, a continuación, haga clic en **Aceptar**.



Se completa la URL original y se permite el acceso al terminal como invitado.

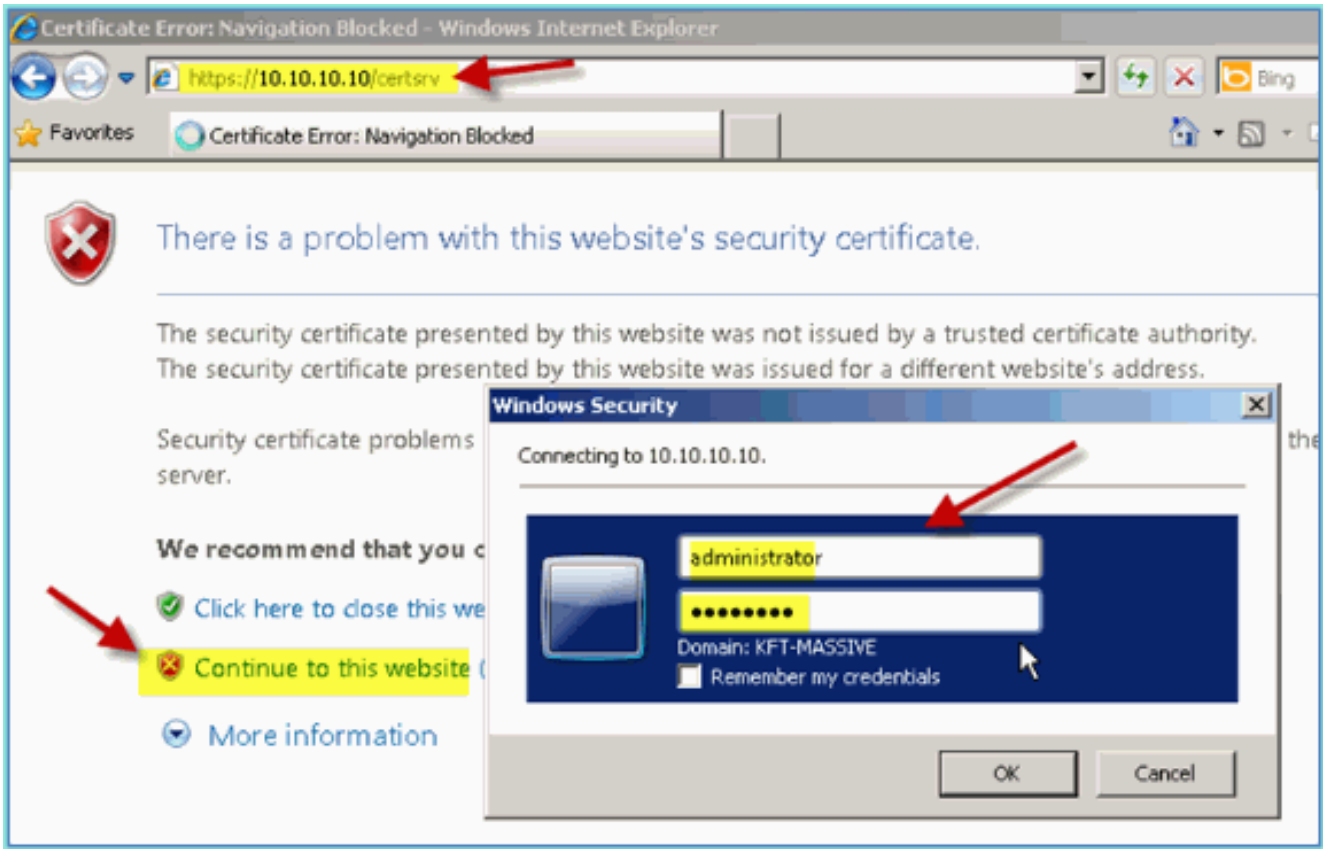
Configuración del certificado

Para proteger las comunicaciones con ISE, determine si la comunicación está relacionada con la autenticación o con la administración de ISE. Por ejemplo, para la configuración mediante la interfaz de usuario web de ISE, es necesario configurar los certificados X.509 y las cadenas de confianza de certificados para habilitar el cifrado asimétrico.

Complete estos pasos:

1. Desde el PC conectado por cable, abra una ventana del navegador a https://AD/certsrv.**Nota:** Utilice el protocolo HTTP seguro.**Nota:** Utilice Mozilla Firefox o MS Internet Explorer para acceder a ISE.
2. Inicie sesión como

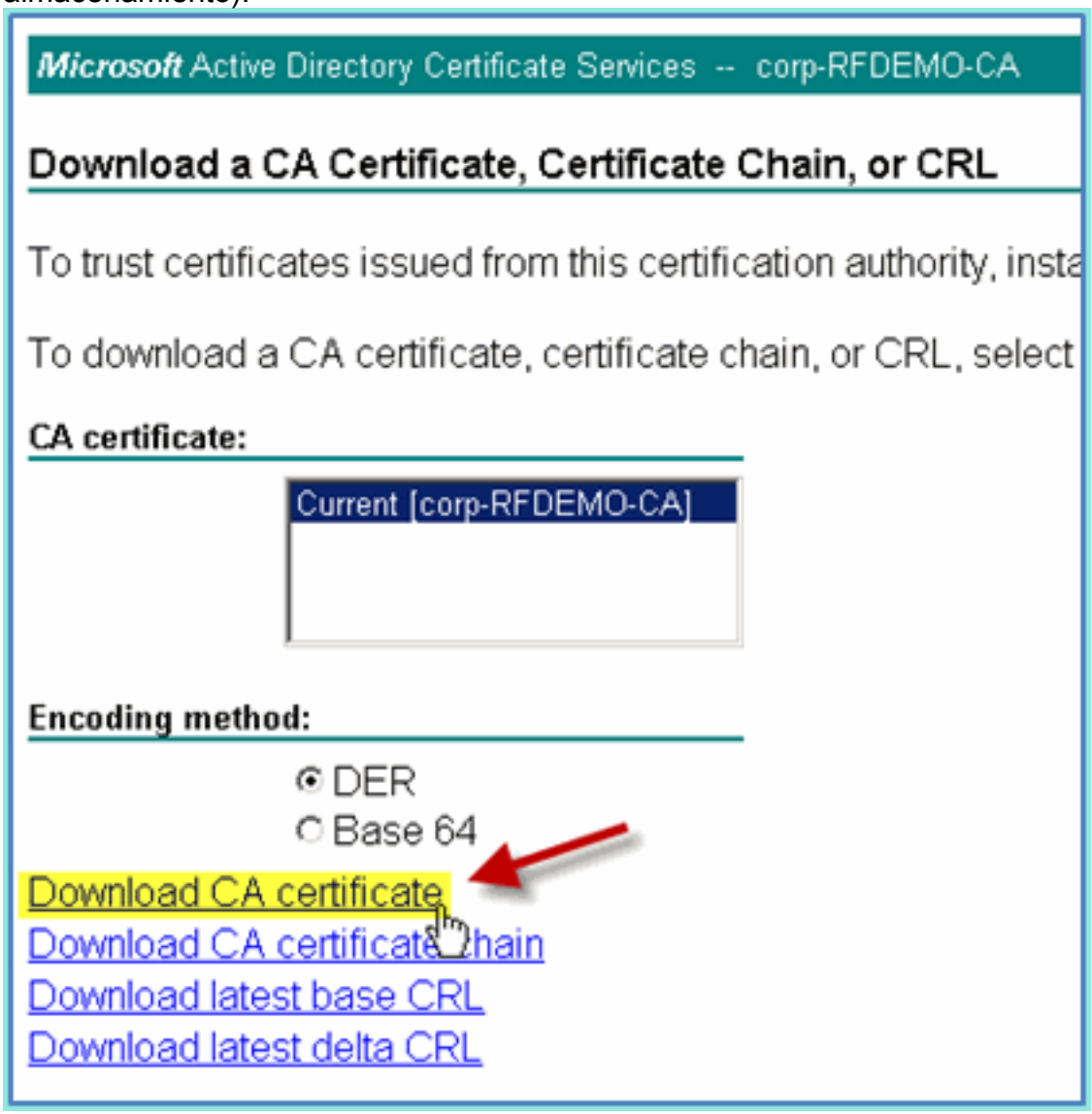
administrator/Cisco123.



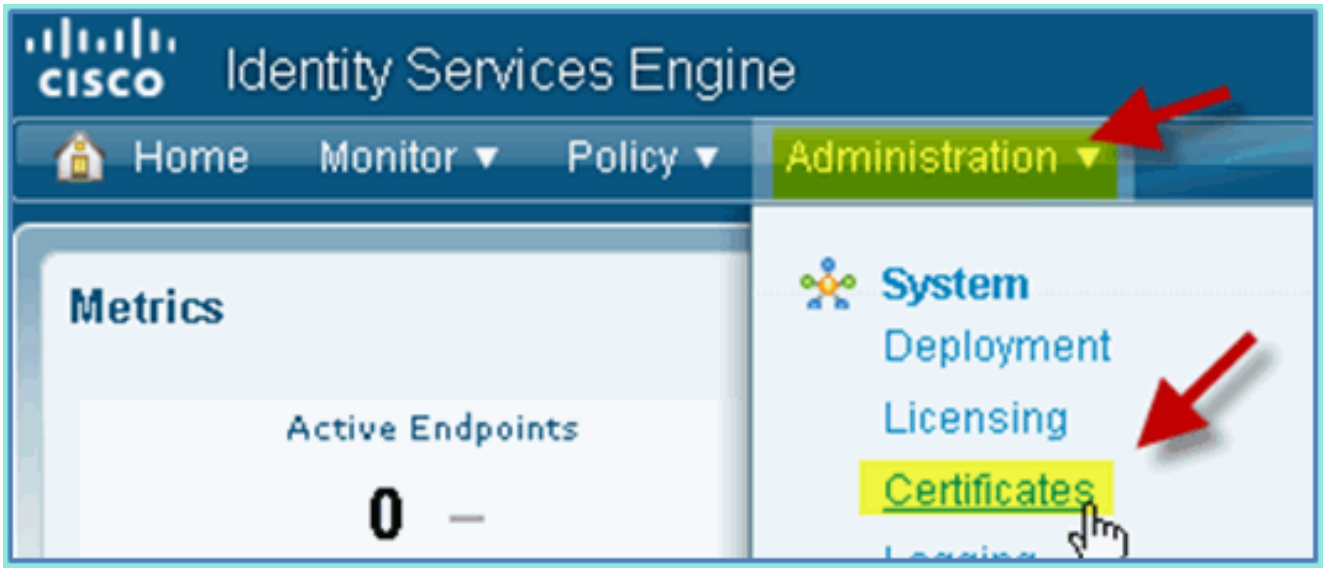
3. Haga clic en **Descargar un certificado de CA, cadena de certificados o CRL**.

4. Haga clic en **Descargar certificado de CA** y guárdelo (observe la ubicación de

almacenamiento).



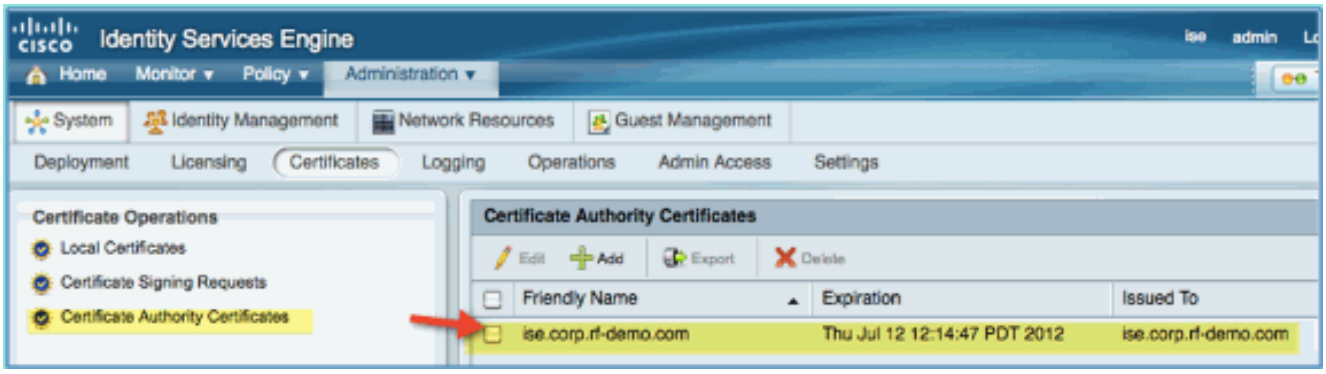
5. Abra una ventana del navegador en https://<Pod-ISE>.
6. Vaya a **Administration > System > Certificates > Certificates Authority Certificates**.



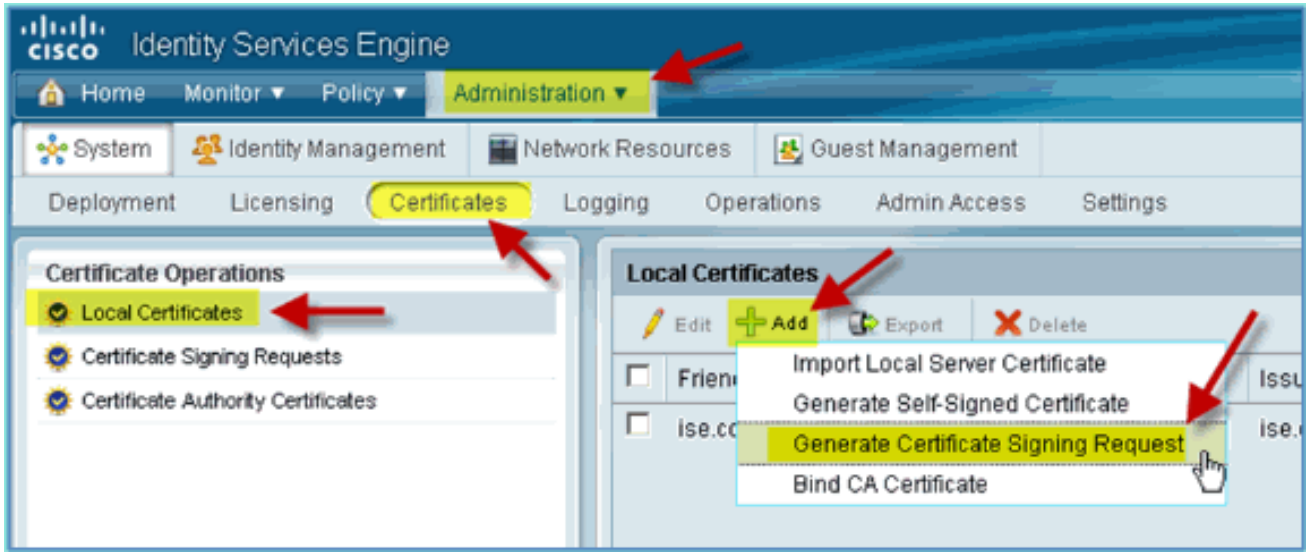
7. Seleccione la operación **Certificate Authority Certificates** y busque el certificado de CA descargado anteriormente.
8. Seleccione **Confianza para el cliente con EAP-TLS** y, a continuación,

envíe.

9. Confirme que la CA se ha agregado como de confianza como CA raíz.



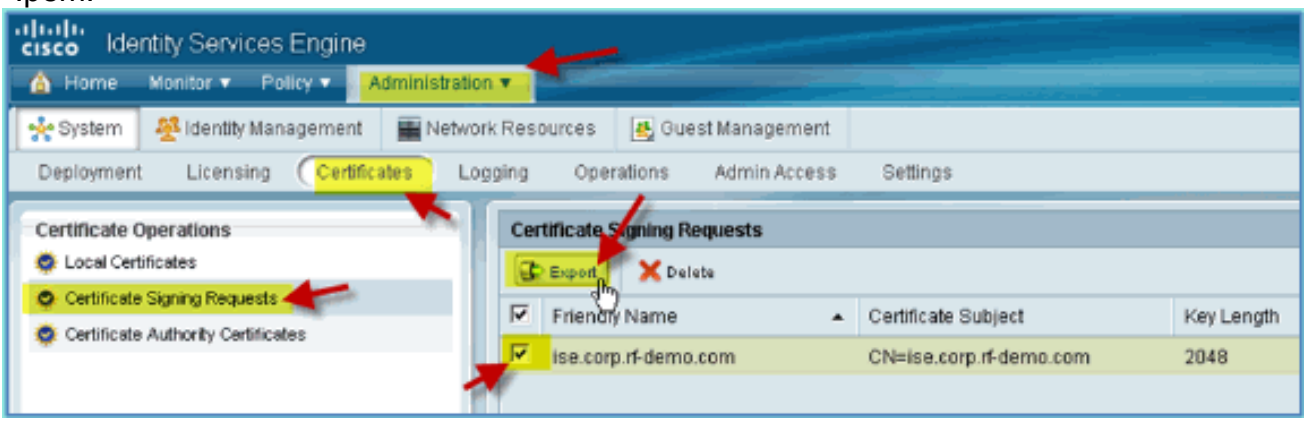
10. Desde un navegador, vaya a **Administration > System > Certificates > Certificates Authority Certificates**.
11. Haga clic en **Agregar** y luego en **Generar solicitud de firma de certificado**.



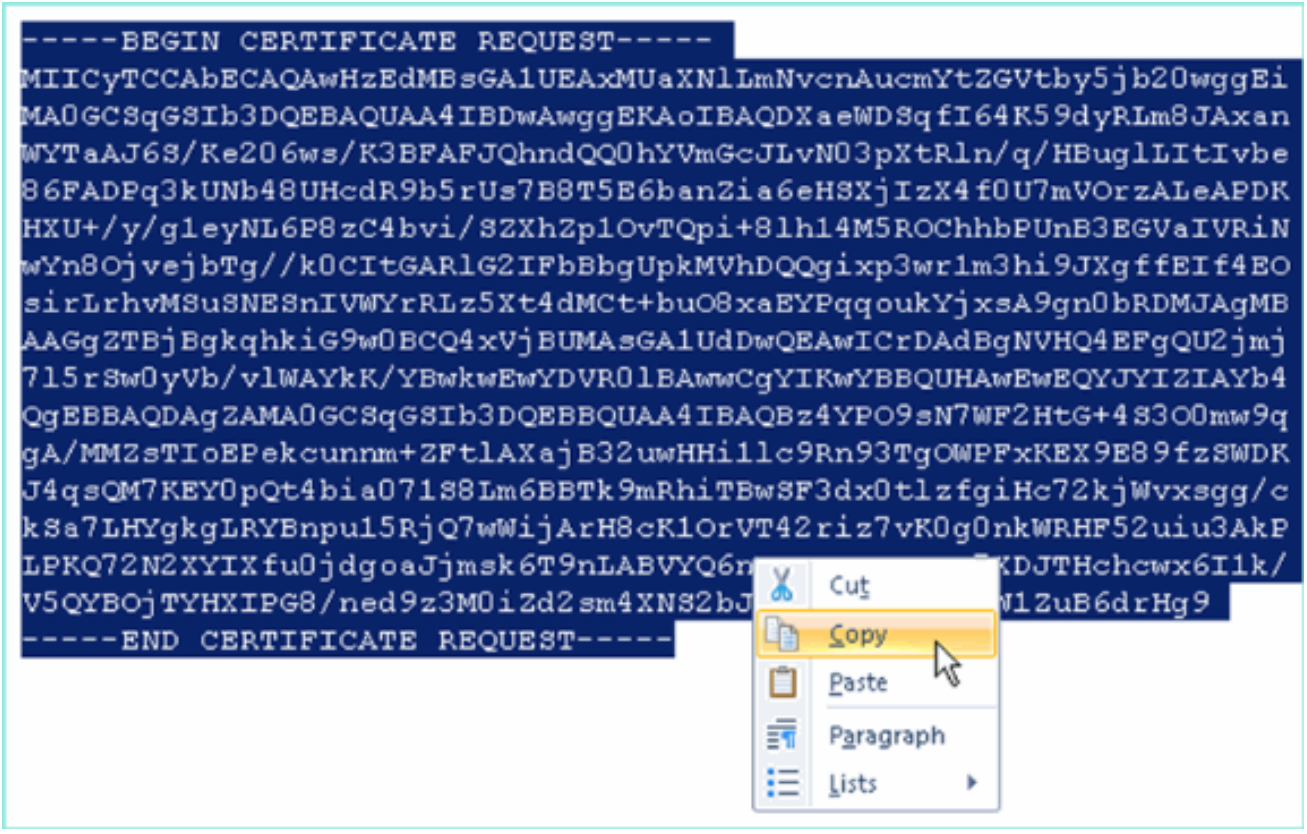
12. Envíe estos valores:Asunto del certificado: CN=ise.corp.rf-demo.comLongitud de la clave: 2048

13. ISE indica que CSR está disponible en la página CSR. Click OK.

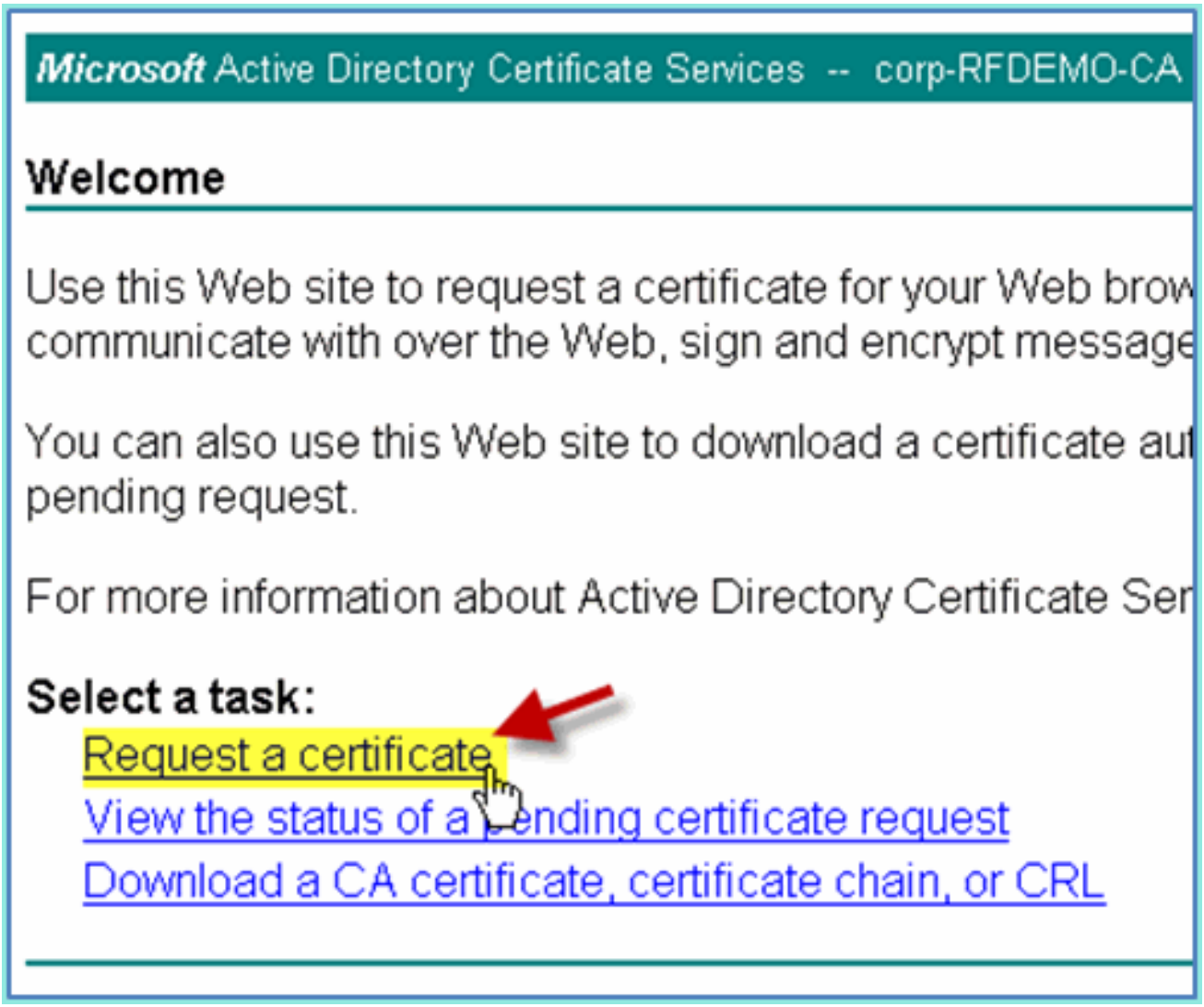
14. Seleccione el CSR en la página CSR de ISE y haga clic en **Exportar**.
15. Guarde el archivo en cualquier ubicación (por ejemplo, Descargas, etc.)
16. El archivo se guardará como *.pem.



17. Busque el archivo CSR y edítelo con Bloc de notas/Wordpad/TextEdit.
18. Copiar el contenido (Seleccionar todo > Copiar).

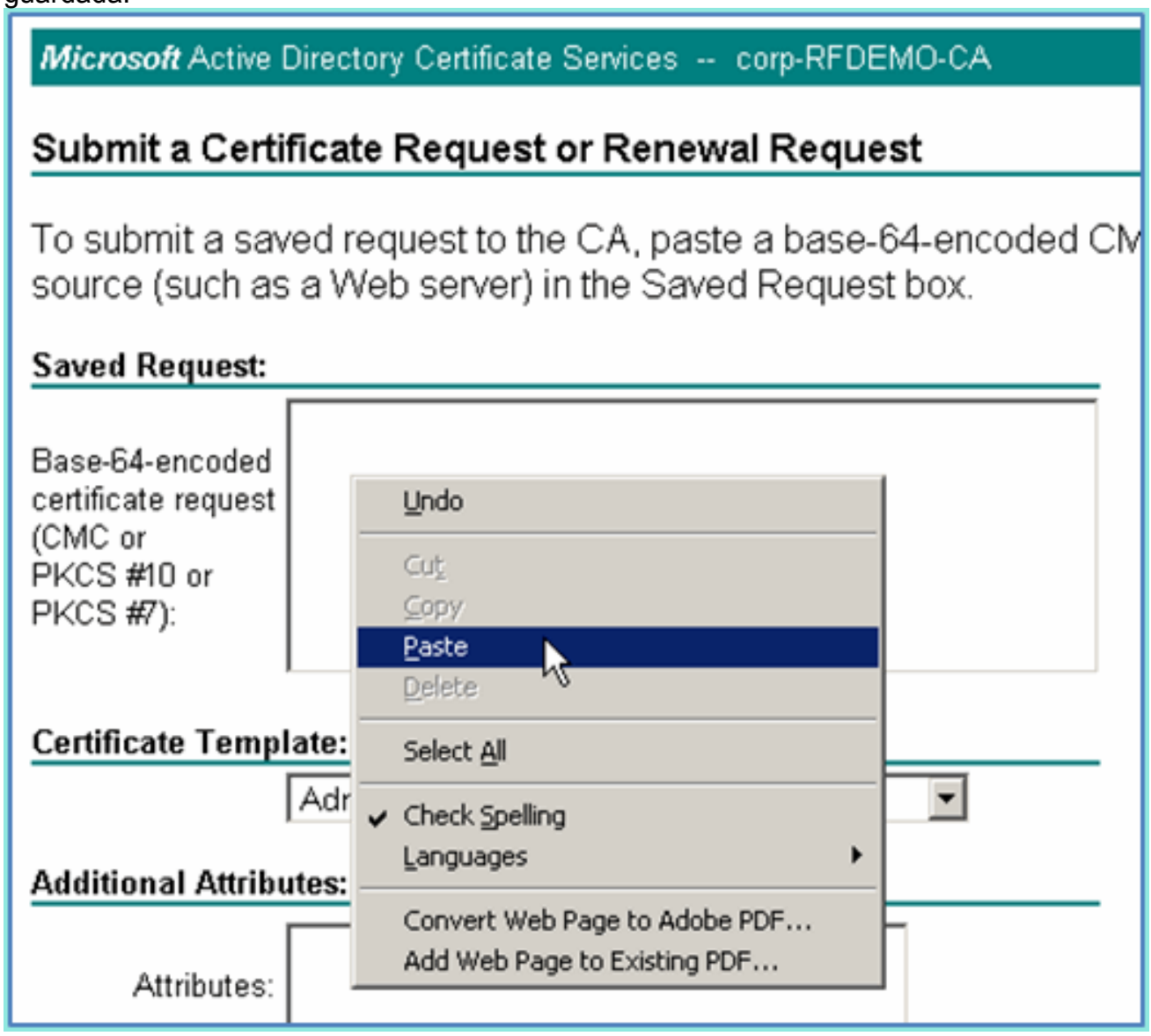


19. Abra una ventana del navegador en https://<Pod-AD>/certsrv.
20. Haga clic en **Solicitar un certificado**.

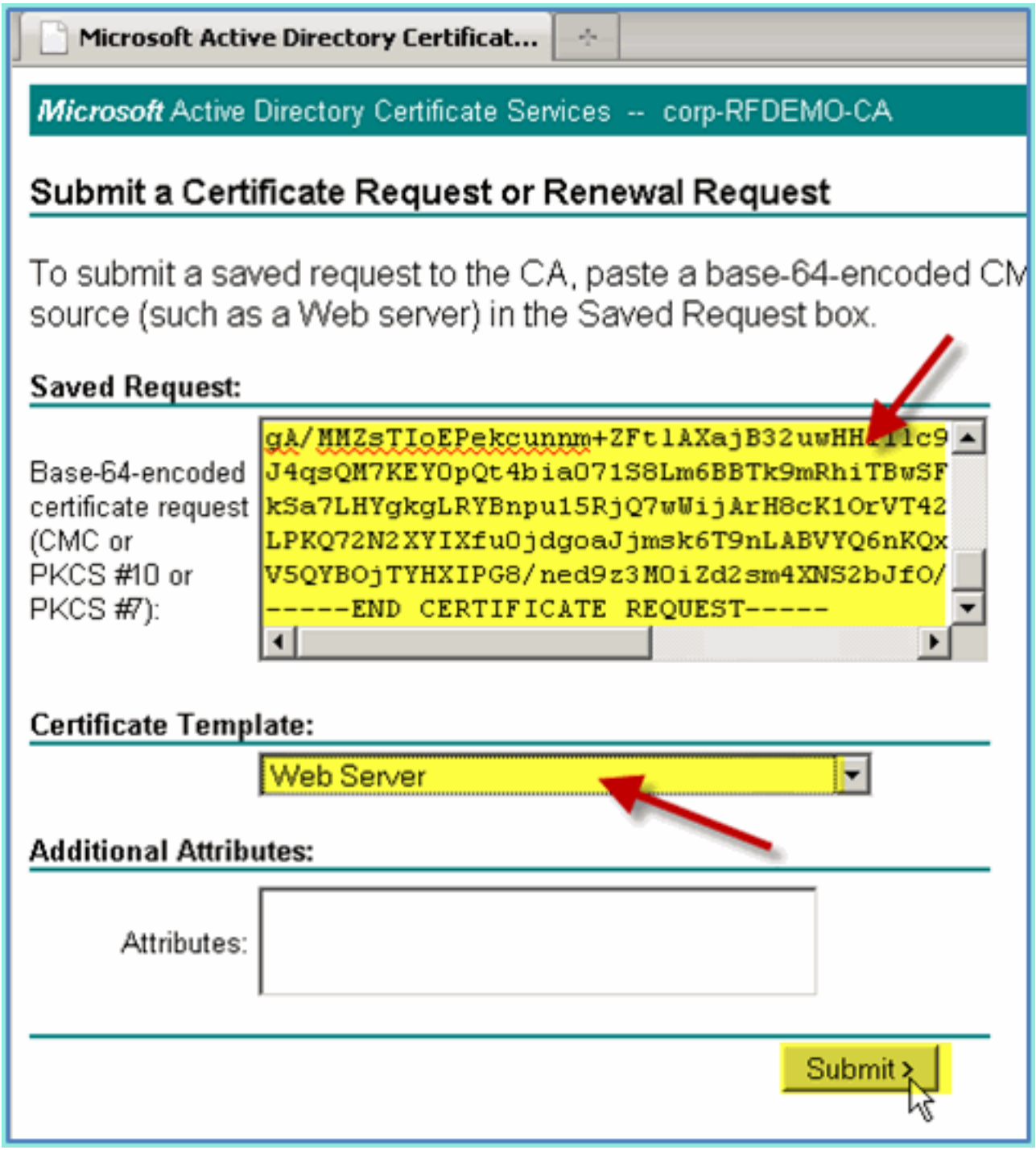


21. Haga clic para enviar una **solicitud de certificado avanzada**.

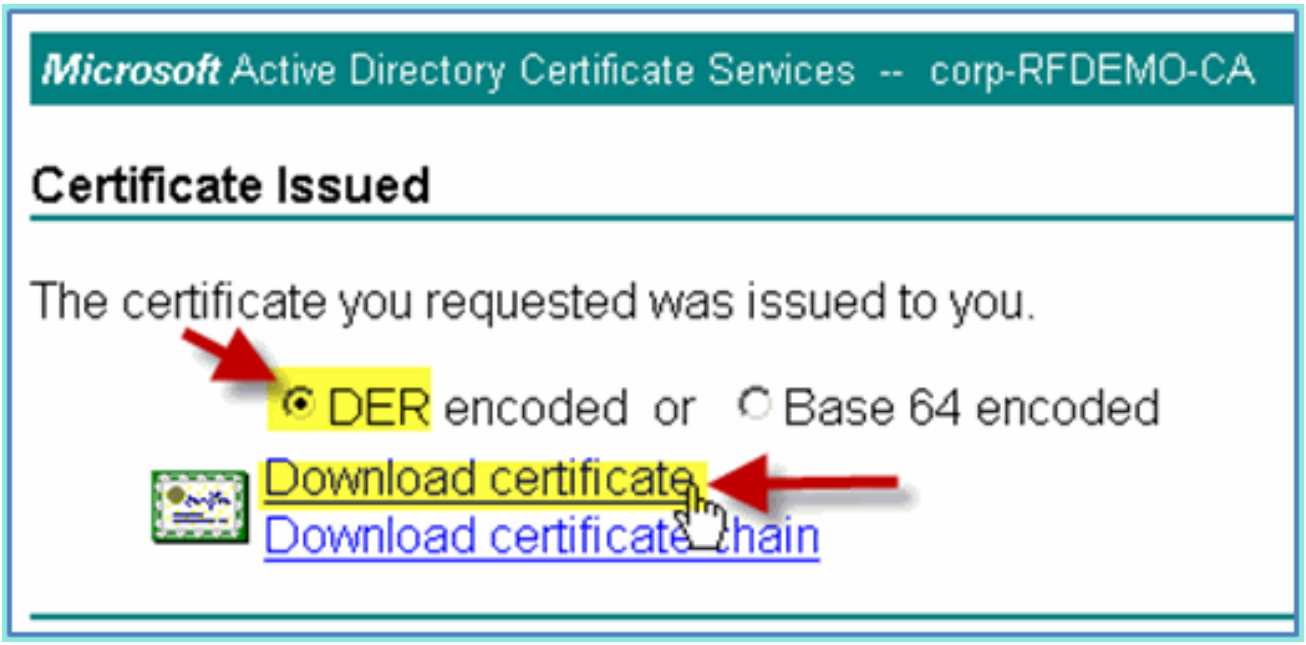
22. Pegue el contenido CSR en el campo de solicitud guardada.



23. Seleccione **Web Server** como la plantilla de certificado y, a continuación, haga clic en **Submit**.

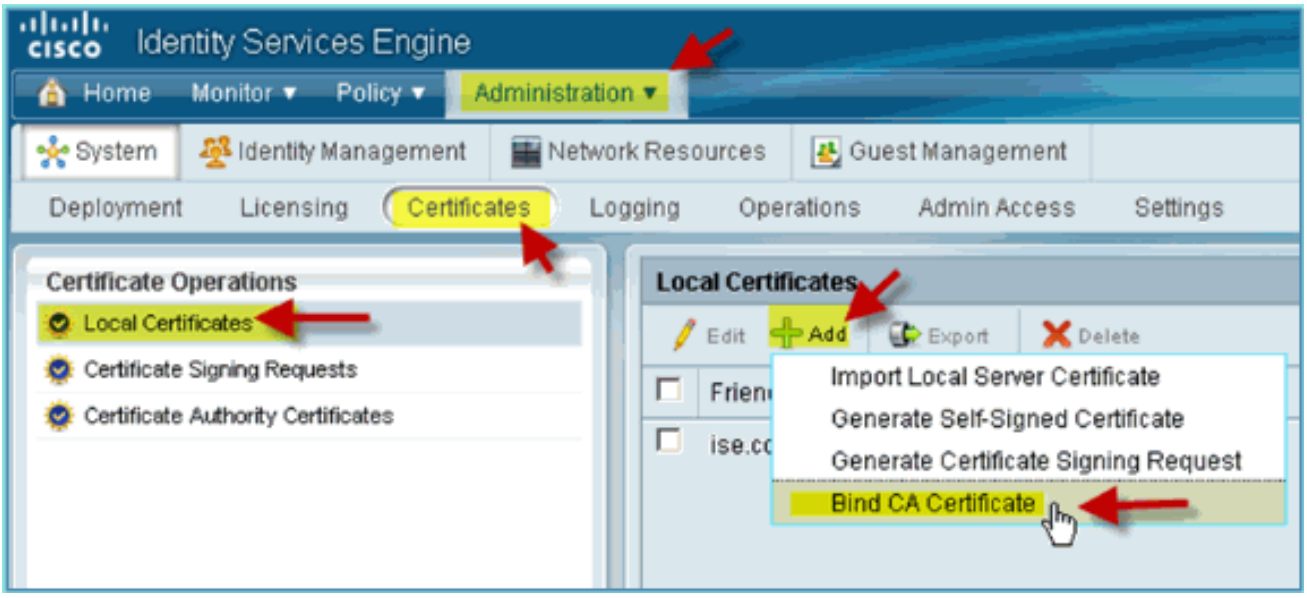


24. Seleccione **DER codificado** y haga clic en **Descargar certificado**.

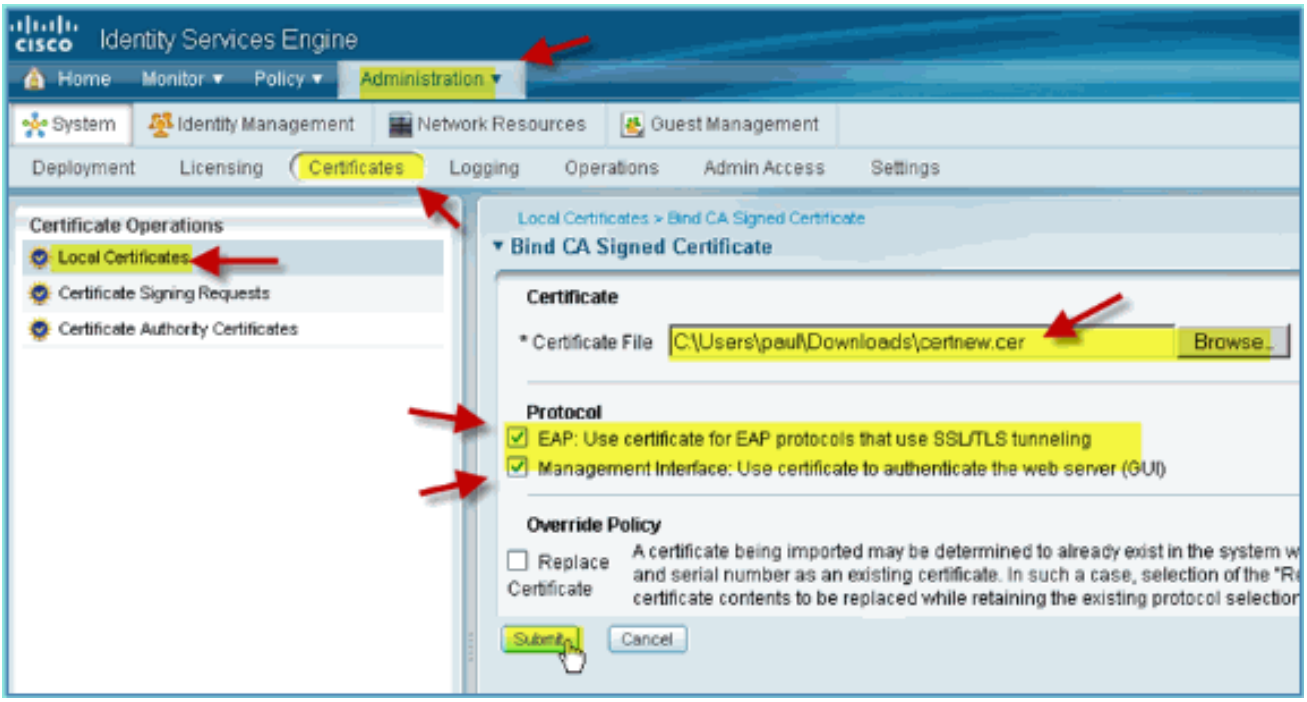


25. Guarde el archivo en una ubicación conocida (por ejemplo, Descargas)
26. Vaya a **Administration > System > Certificates > Certificates Authority Certificates**.

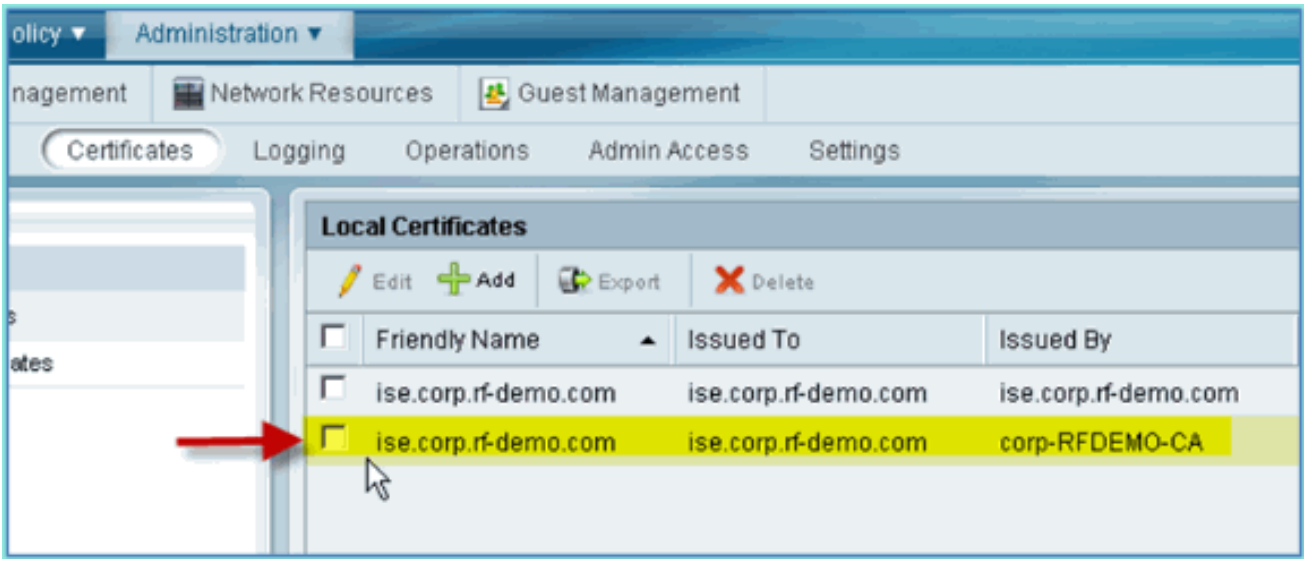
27. Haga clic en **Agregar > Enlazar certificado de CA**.



28. Busque el certificado de CA descargado anteriormente.



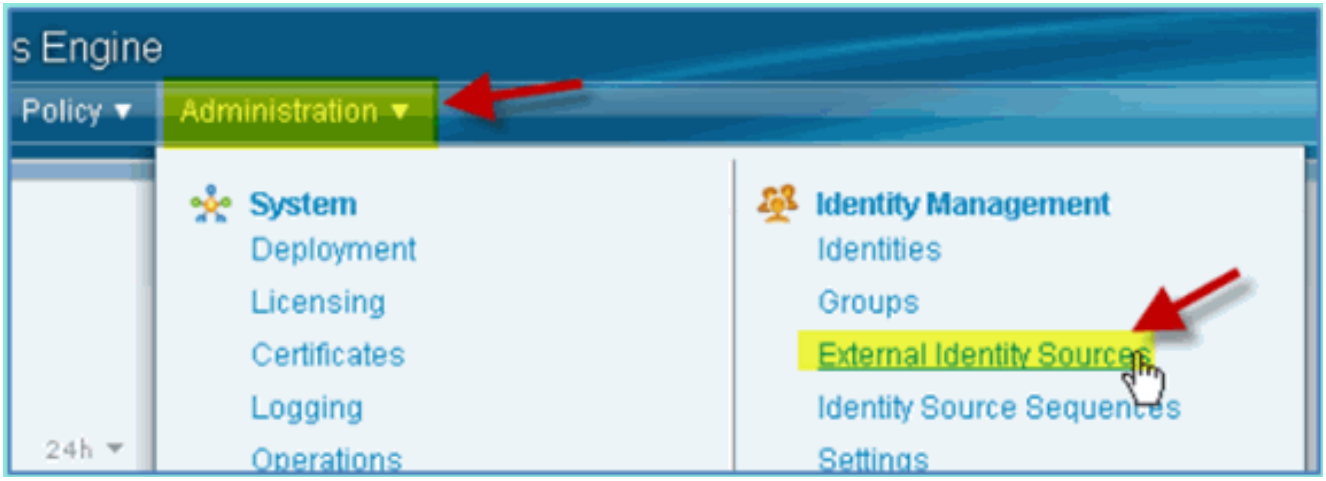
29. Seleccione **Protocol EAP** y **Management Interface** y haga clic en **Submit**.
30. Confirme que la CA se ha agregado como de confianza como CA raíz.



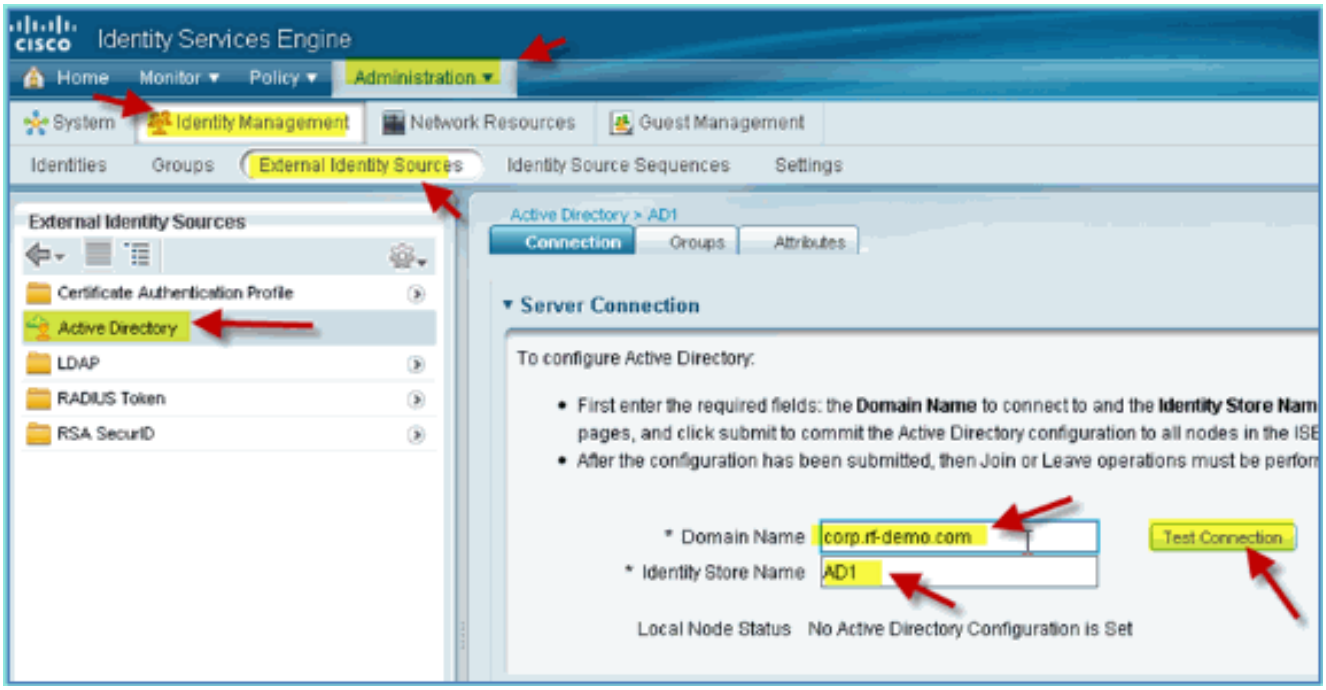
Integración de Windows 2008 Active Directory

ISE puede comunicarse directamente con Active Directory (AD) para la autenticación de usuario/equipo o para recuperar información de autorización o atributos de usuario. Para comunicarse con AD, ISE debe estar "unido" a un dominio AD. En este ejercicio, unirá ISE a un dominio AD y confirmará que la comunicación AD funciona correctamente.

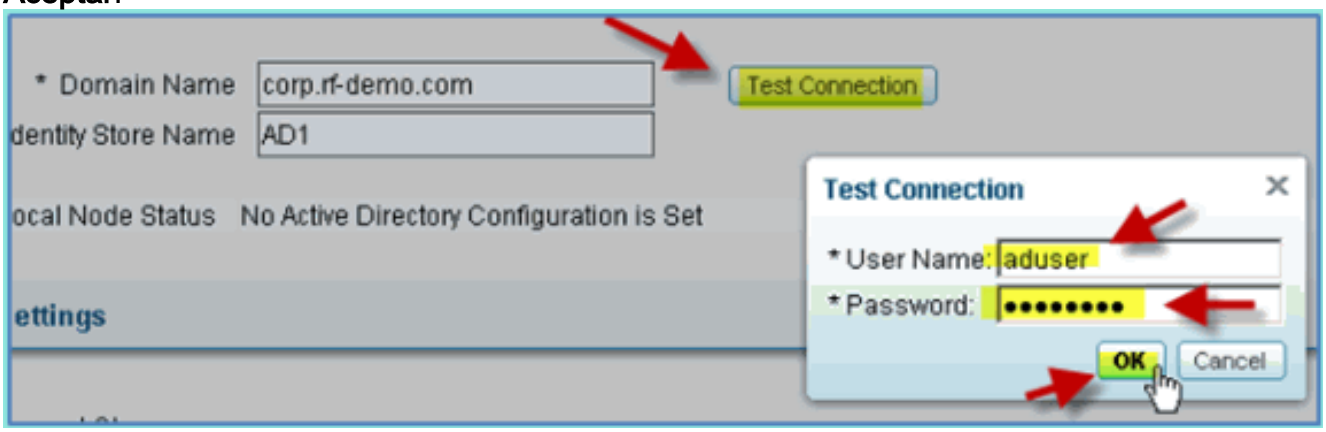
Complete estos pasos:

1. Para unir ISE al dominio AD, desde ISE vaya a **Administration > Identity Management > External Identity Sources**.


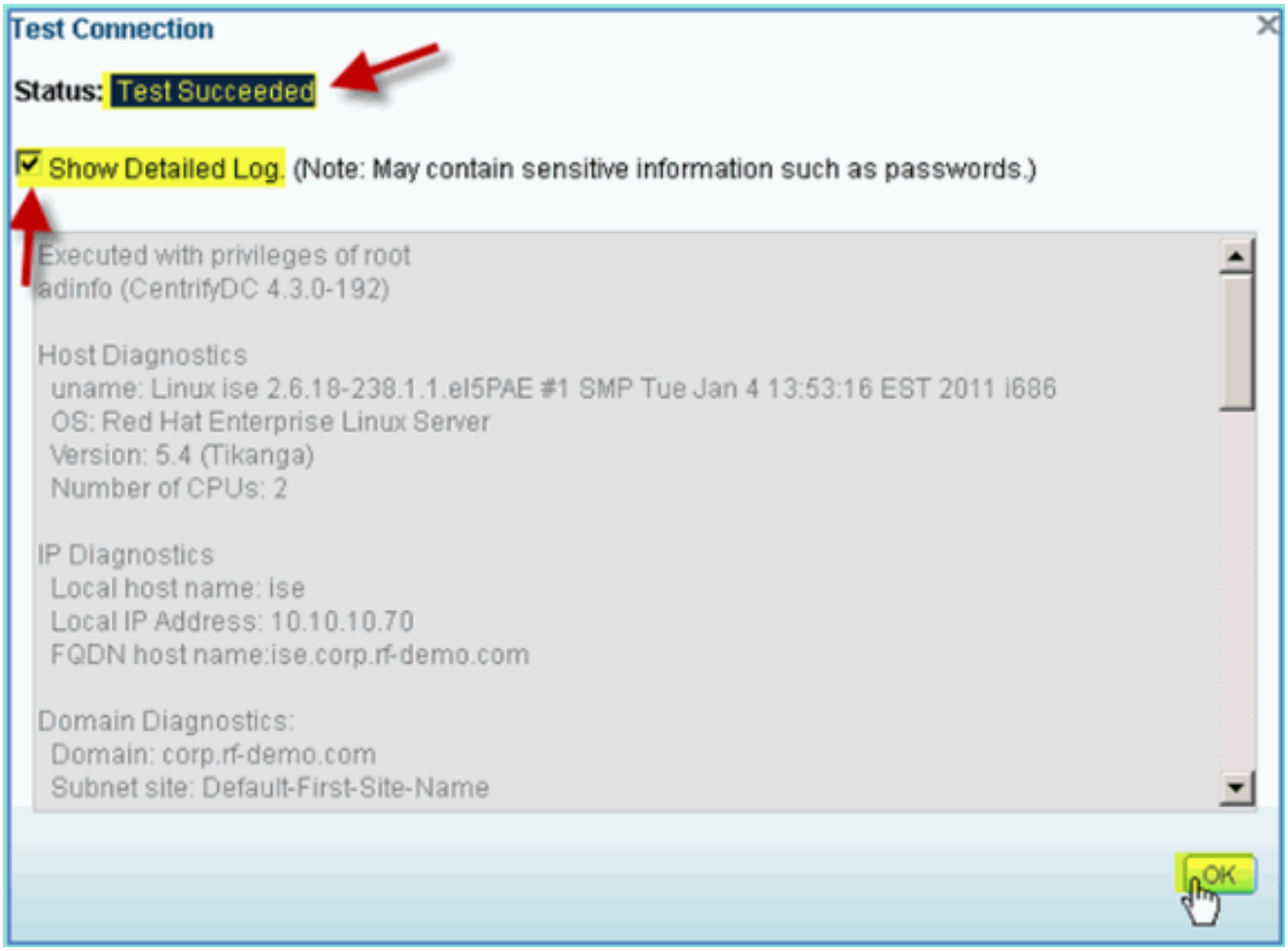
2. En el panel izquierdo (Orígenes de identidad externos), seleccione **Active Directory**.
3. En el lado derecho, seleccione la pestaña **Connection** e ingrese lo siguiente:Nombre de dominio: corp.rf-demo.comNombre del almacén de identidades: AD1



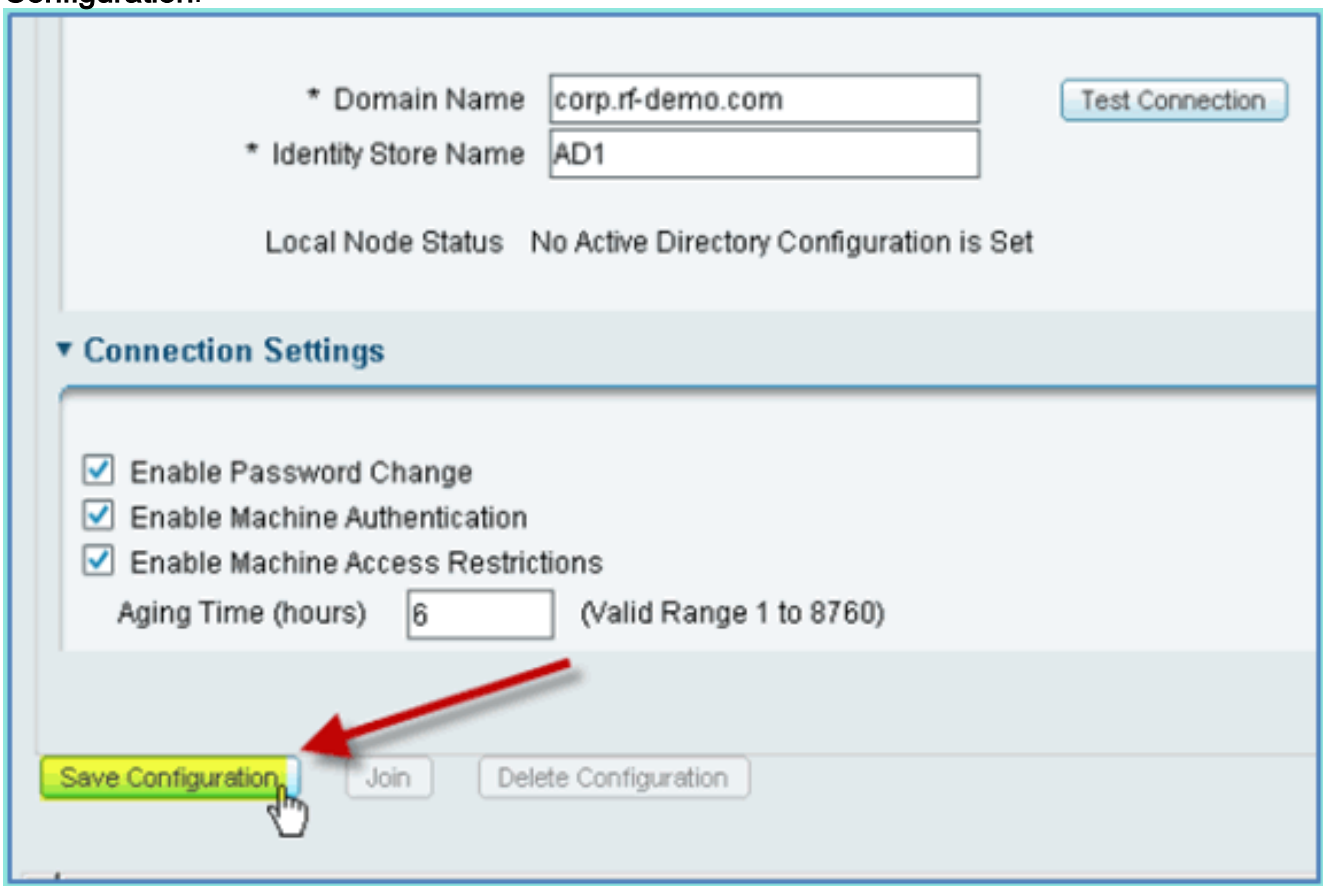
4. Haga clic en **Probar conexión**. Introduzca el nombre de usuario de AD (aduser/Cisco123) y, a continuación, haga clic en **Aceptar**.



5. Confirme que Estado de la prueba muestre **Prueba realizada correctamente**.
6. Seleccione Mostrar registro detallado y observe los detalles útiles para solucionar problemas. Para continuar, haga clic en OK (Aceptar).

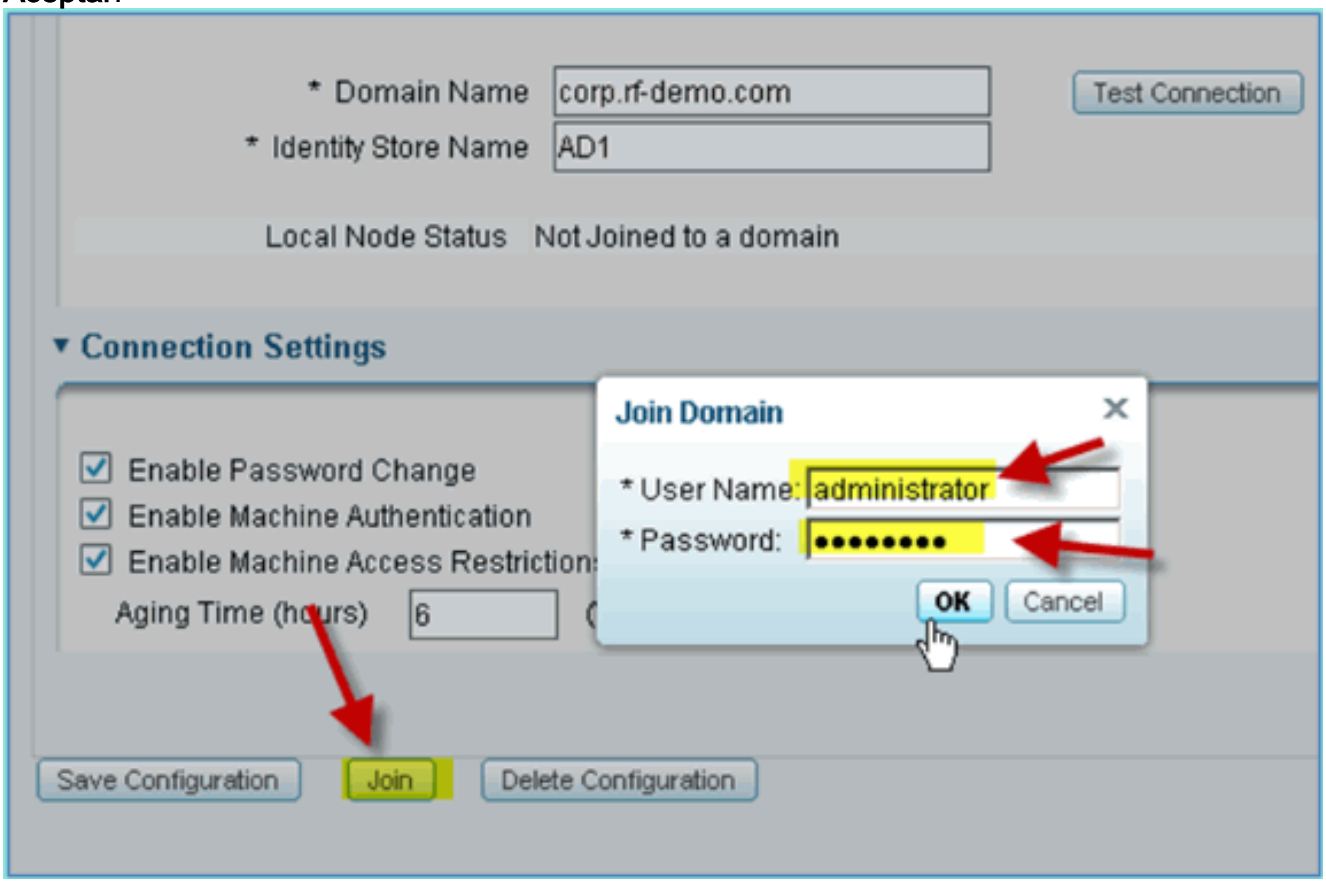


7. Haga clic en **Save Configuration**.

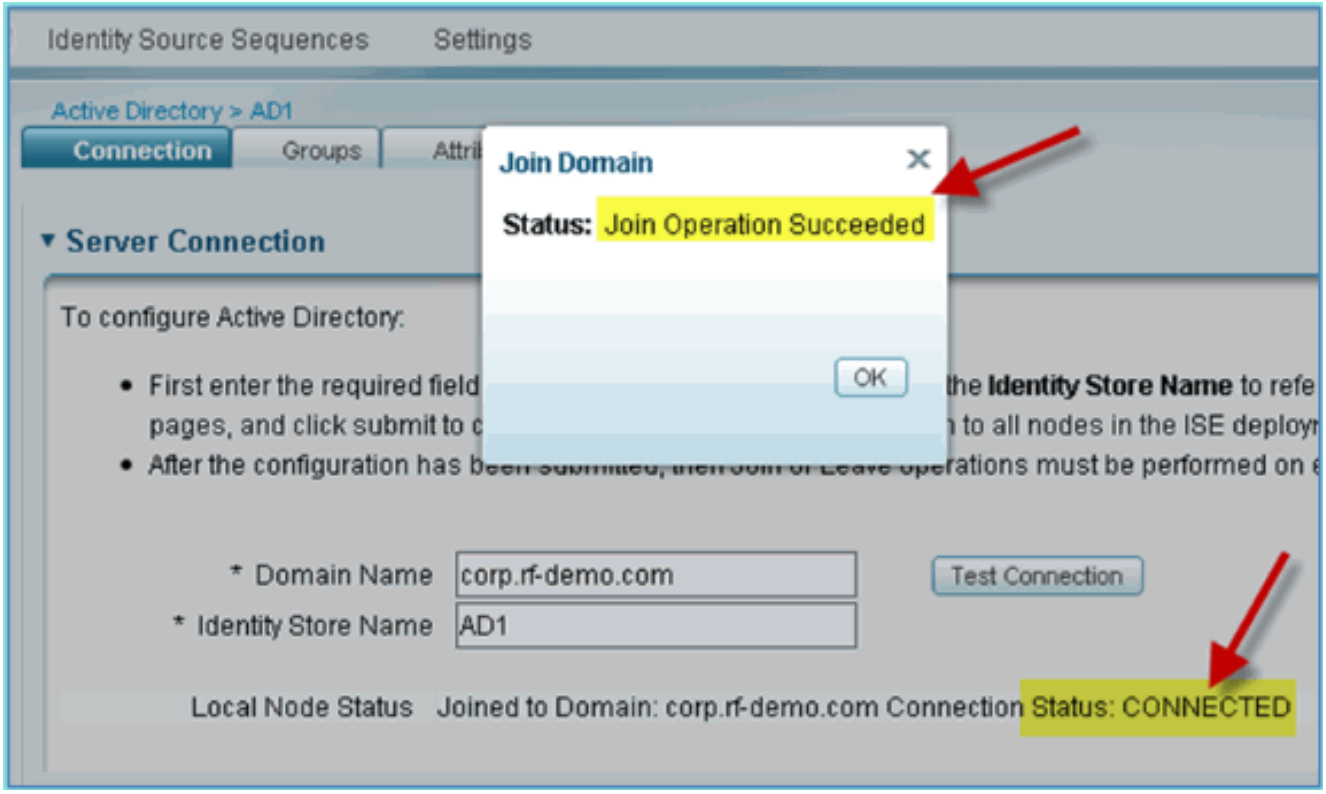


8. Haga clic en **Unirse**. Introduzca el usuario de AD (administrator/Cisco123) y, a continuación, haga clic en

Aceptar.



9. Confirme que Unirse al estado de la operación aparece como **Correcto** y, a continuación, haga clic en **Aceptar** para continuar.El Estado de conexión del servidor muestra **CONECTADO**. Si este estado cambia en cualquier momento, una conexión de prueba le ayudará a resolver problemas con las operaciones de AD.



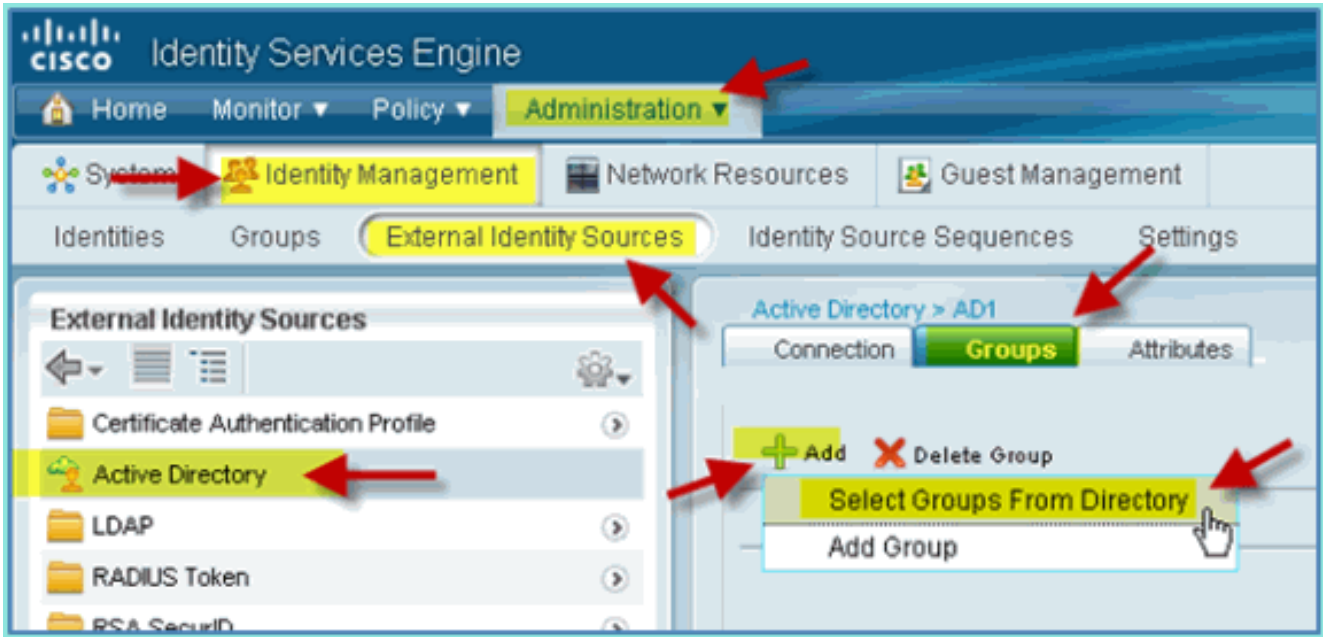
Agregar grupos de Active Directory

Cuando se agregan grupos de AD, se permite un control más granular de las políticas de ISE. Por ejemplo, los grupos AD se pueden diferenciar por funciones funcionales, como los grupos de empleados o contratistas, sin que el error relacionado se haya producido en ejercicios anteriores de ISE 1.0, donde las políticas se limitaban solo a los usuarios.

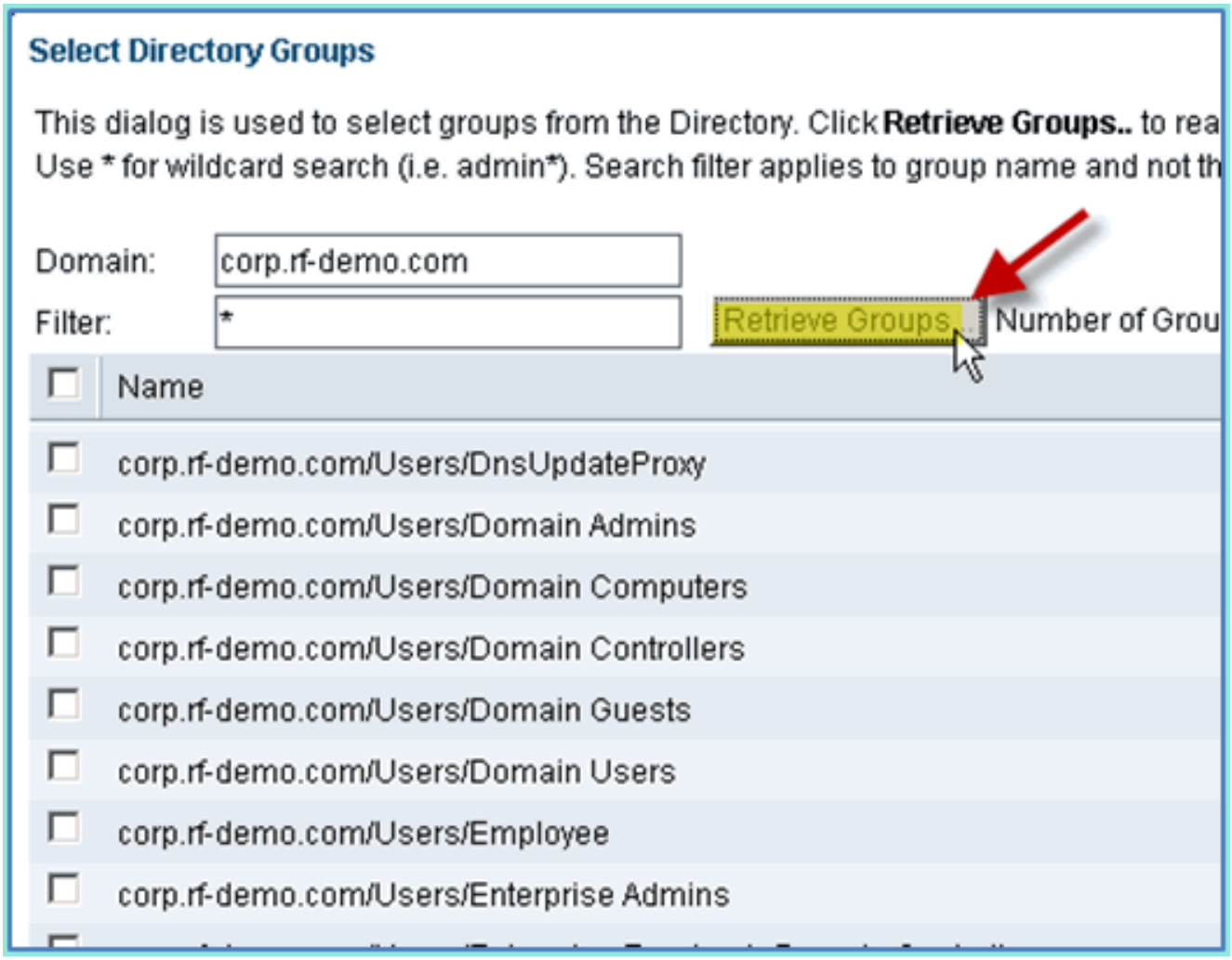
En este laboratorio, sólo se utilizan los usuarios del dominio y/o el grupo de empleados.

Complete estos pasos:

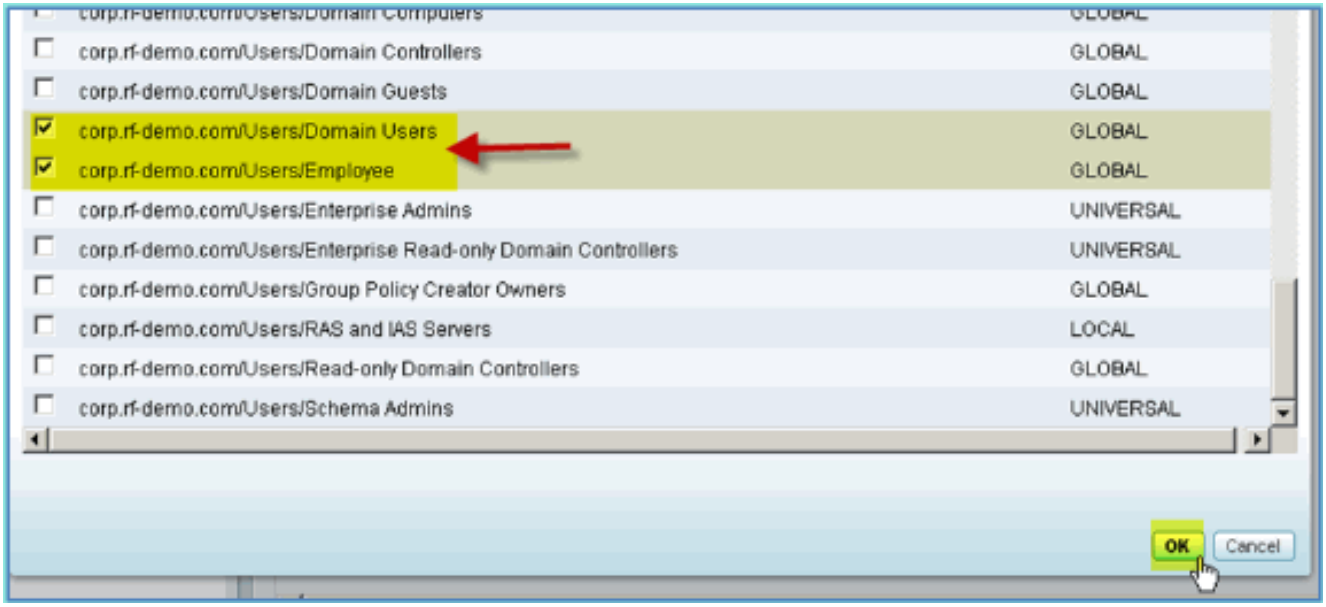
1. Desde ISE, vaya a **Administration > Identity Management > External Identity Sources**.
2. Seleccione la pestaña **Active Directory > Groups**.
3. Haga clic en **+Agregar** y, a continuación, en **Seleccionar grupos del directorio**.



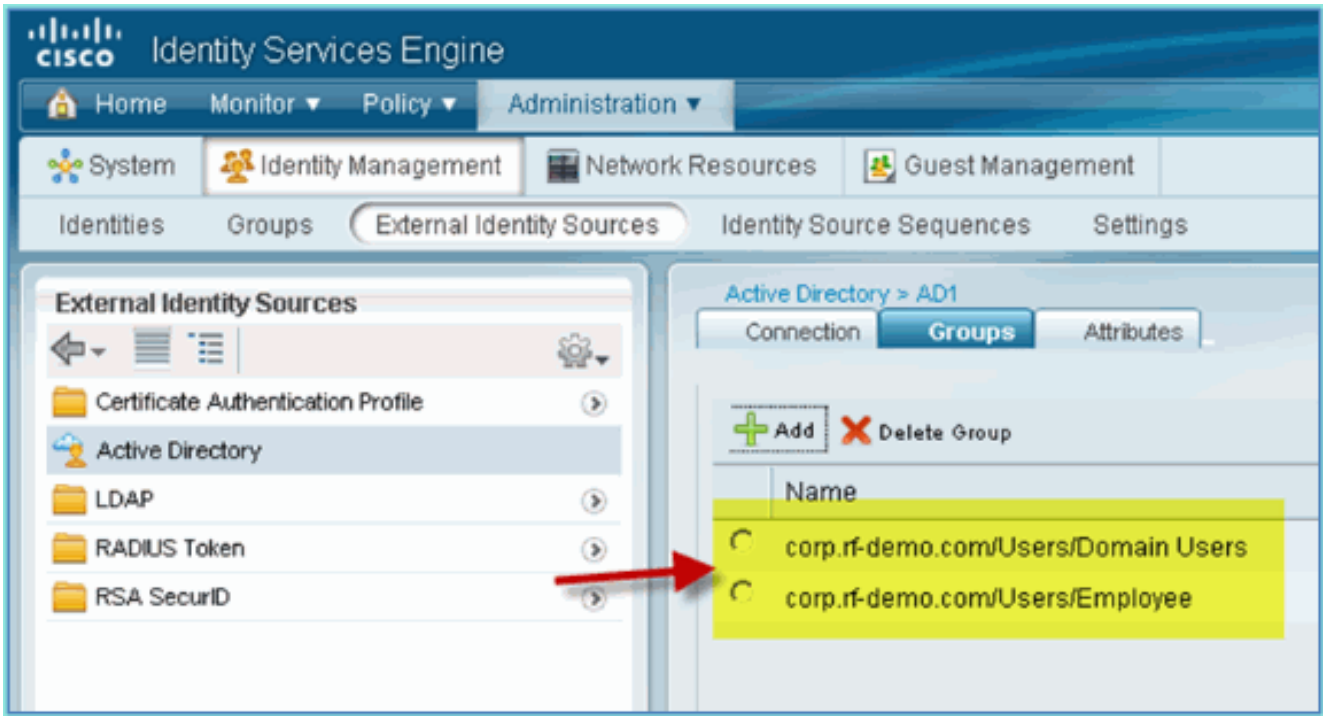
4. En la ventana de seguimiento (Seleccionar grupos de directorio), acepte los valores predeterminados para dominio (corp-rf-demo.com) y Filtro (*). A continuación, haga clic en **Recuperar grupos**.



5. Active las casillas de verificación **Usuarios de dominio** y grupos **Empleados**. Haga clic en **Aceptar** cuando termine.



6. Confirme que los grupos se han agregado a la lista.

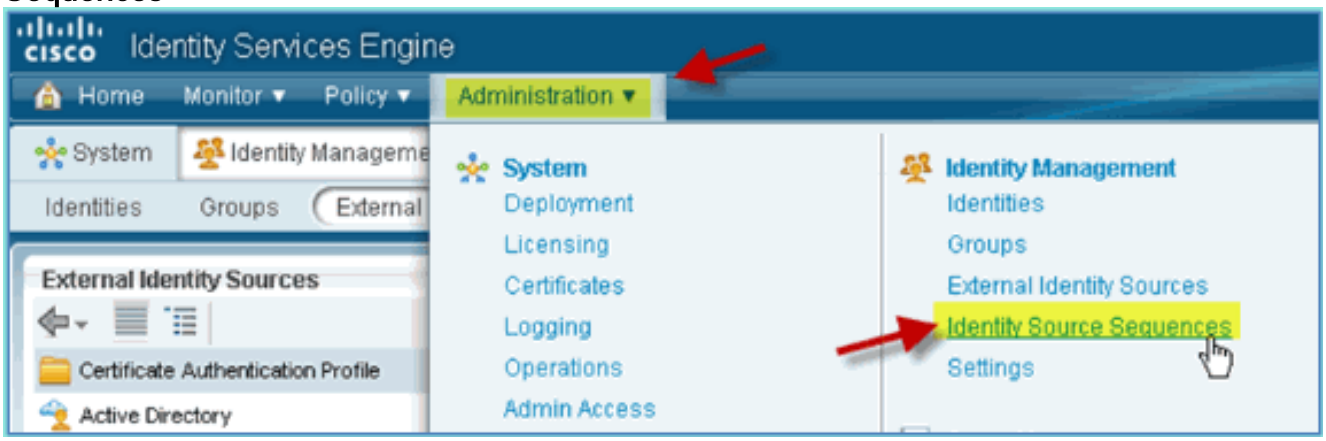


Agregar secuencia de origen de identidad

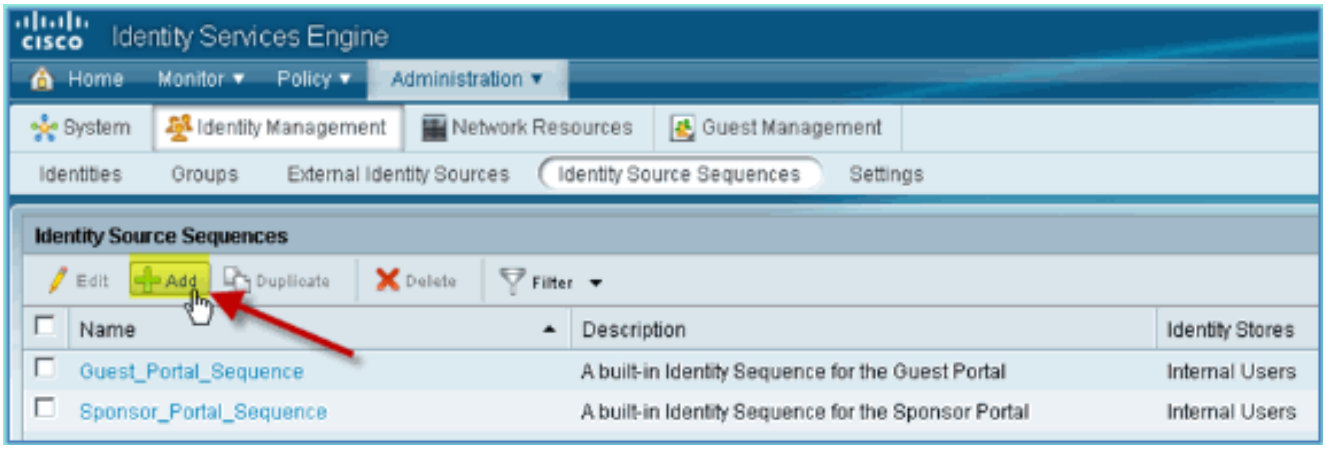
De forma predeterminada, ISE está configurado para utilizar usuarios internos para el almacén de autenticación. Si se agrega AD, se puede crear un orden de prioridad de secuencia para incluir AD que ISE utilizará para comprobar la autenticación.

Complete estos pasos:

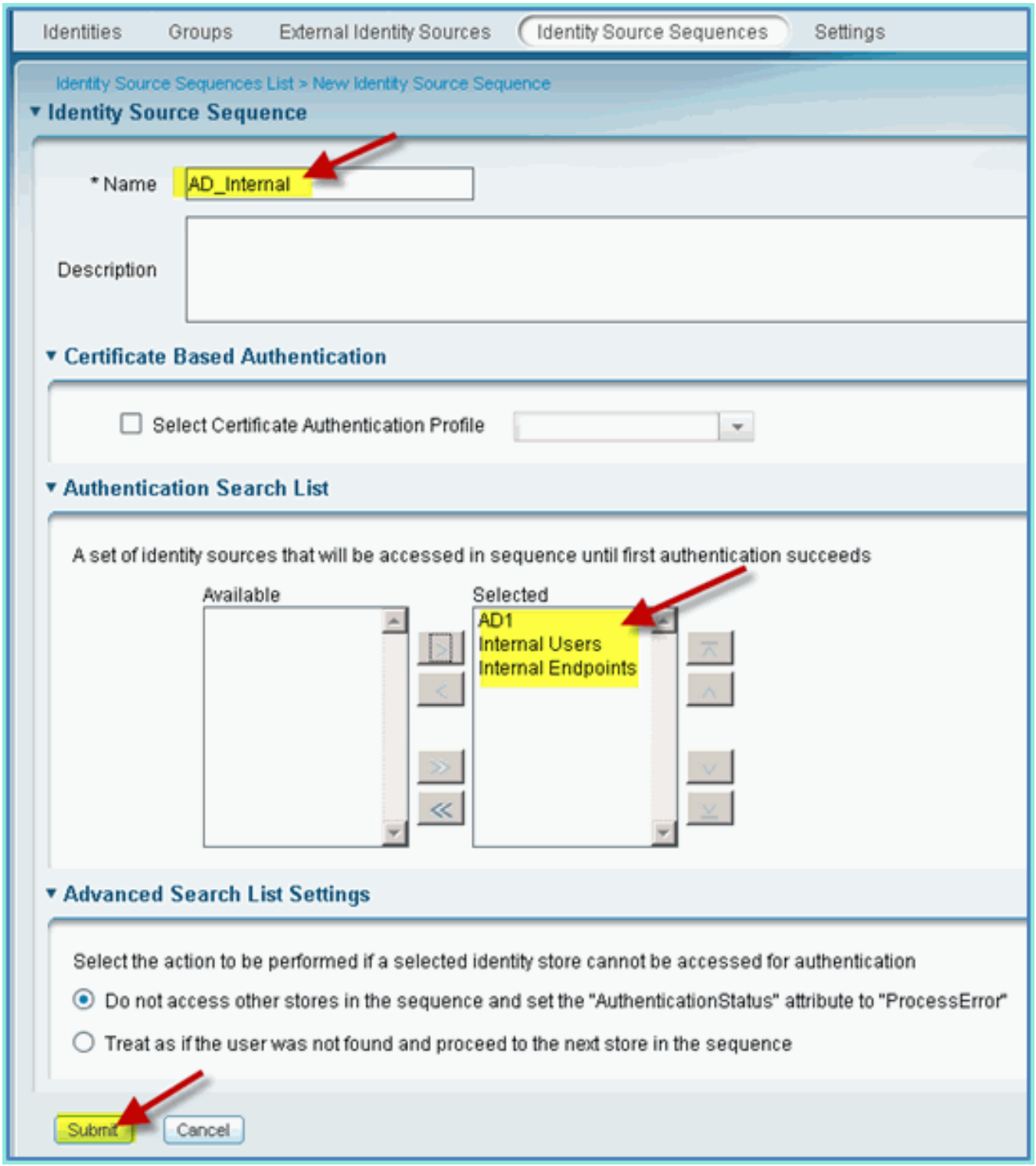
1. En ISE, vaya a **Administration > Identity Management > Identity Source Sequences**.



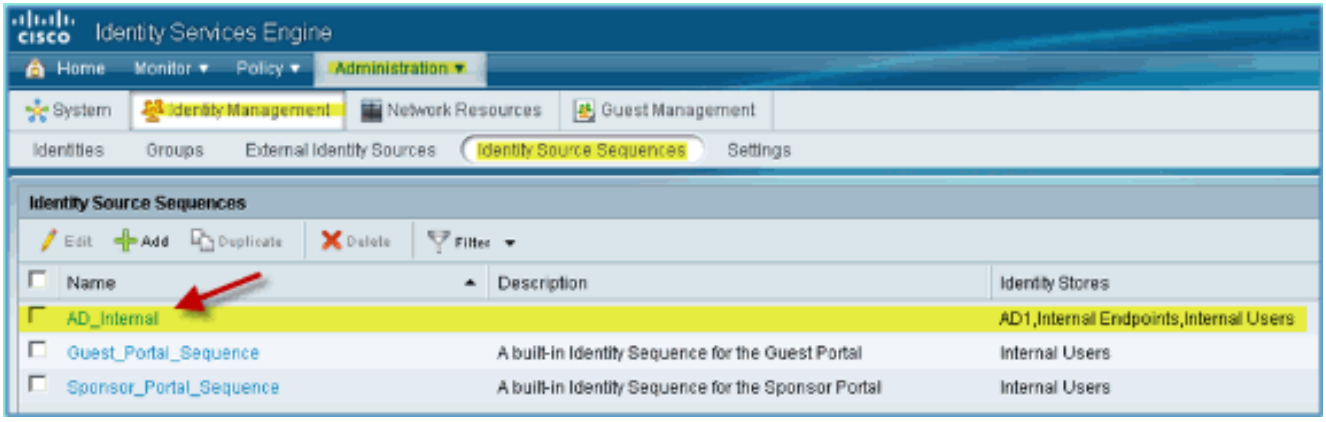
2. Haga clic en **+Add** para agregar una nueva secuencia.



3. Introduzca el nuevo nombre: **AD_Internal**. Agregue todos los orígenes disponibles al campo Seleccionado. A continuación, cambie el orden según sea necesario para que AD1 se mueva al principio de la lista. Haga clic en Submit
(Enviar).



4. Confirme que la secuencia se ha agregado a la lista.

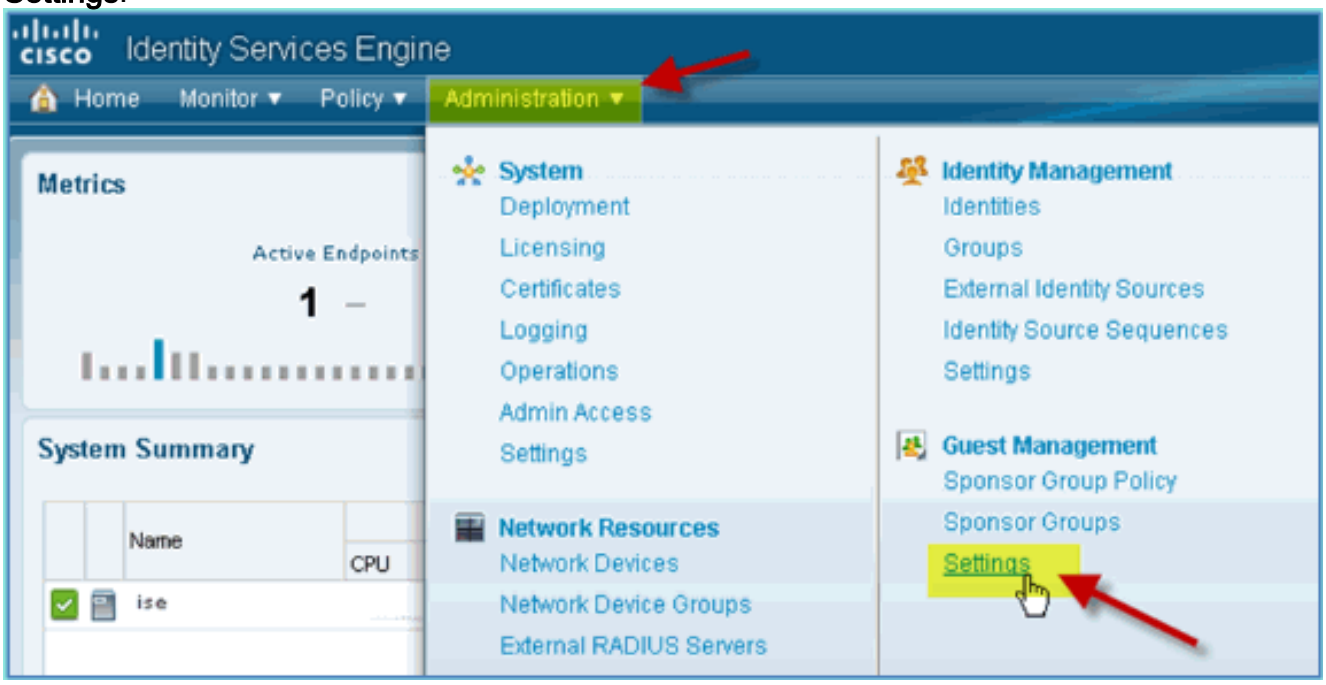


Acceso de invitados patrocinado por tecnología inalámbrica ISE con AD integrado

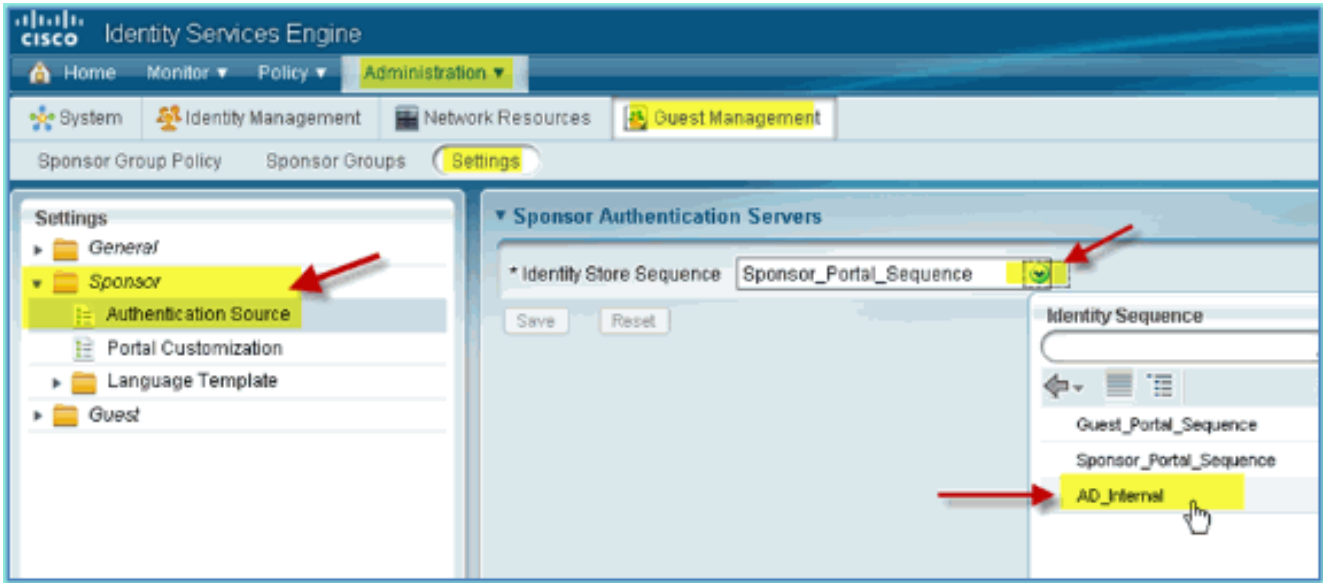
ISE se puede configurar para permitir que los invitados sean patrocinados con políticas para permitir que los usuarios del dominio AD patrocinen el acceso de invitados.

Complete estos pasos:

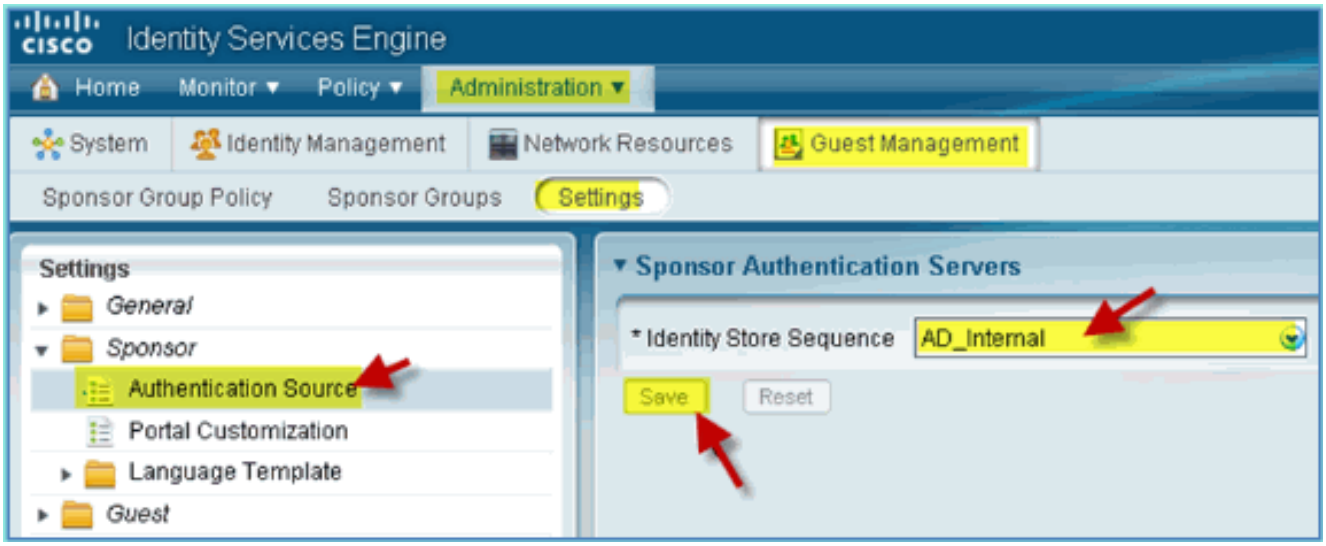
1. En ISE, vaya a **Administration > Guest Management > Settings**.



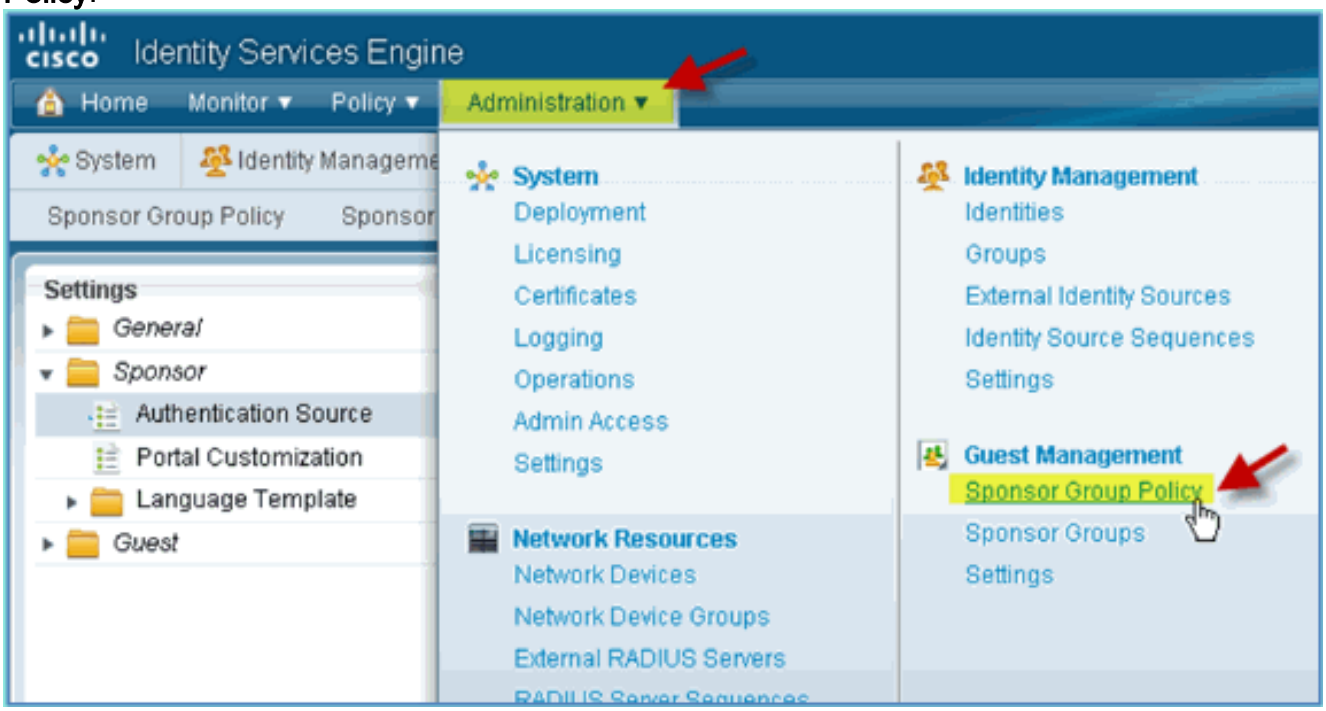
2. Expanda **Patrocinador** y haga clic en **Origen de autenticación**. A continuación, seleccione **AD_Internal** como secuencia de almacén de identidades.



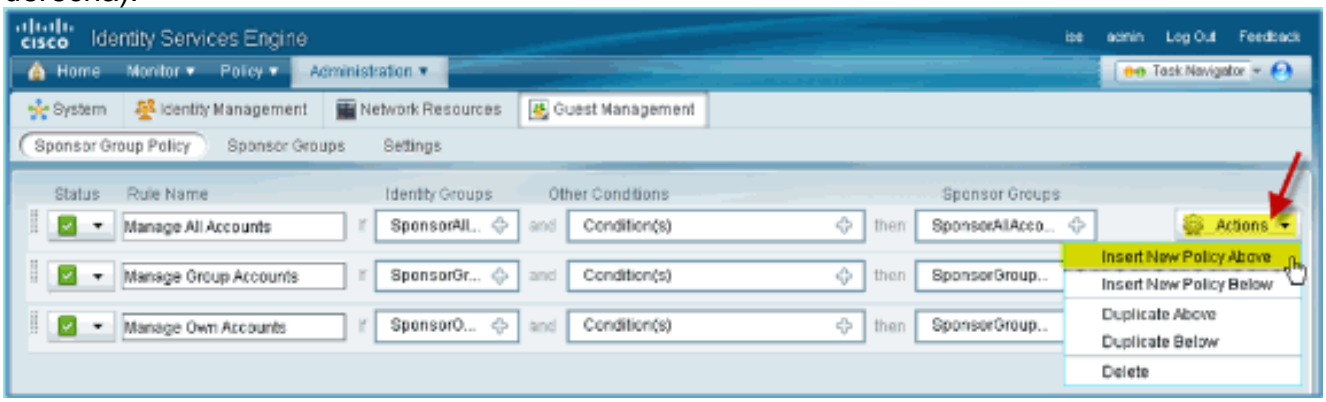
3. Confirme AD_Internal como la secuencia de almacén de identidades. Click **Save**.



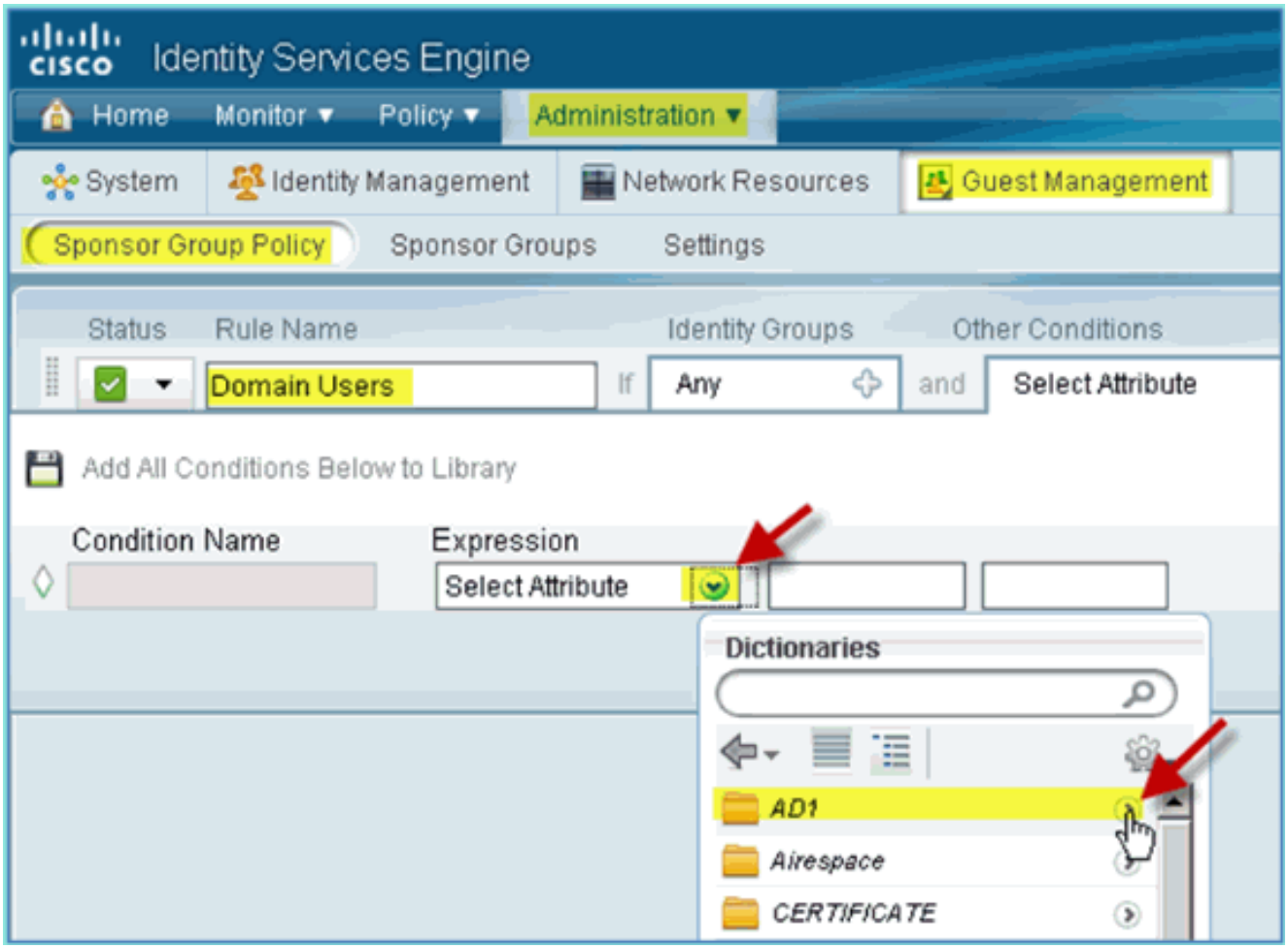
4. Vaya a **Administration > Guest Management > Sponsor Group Policy**.



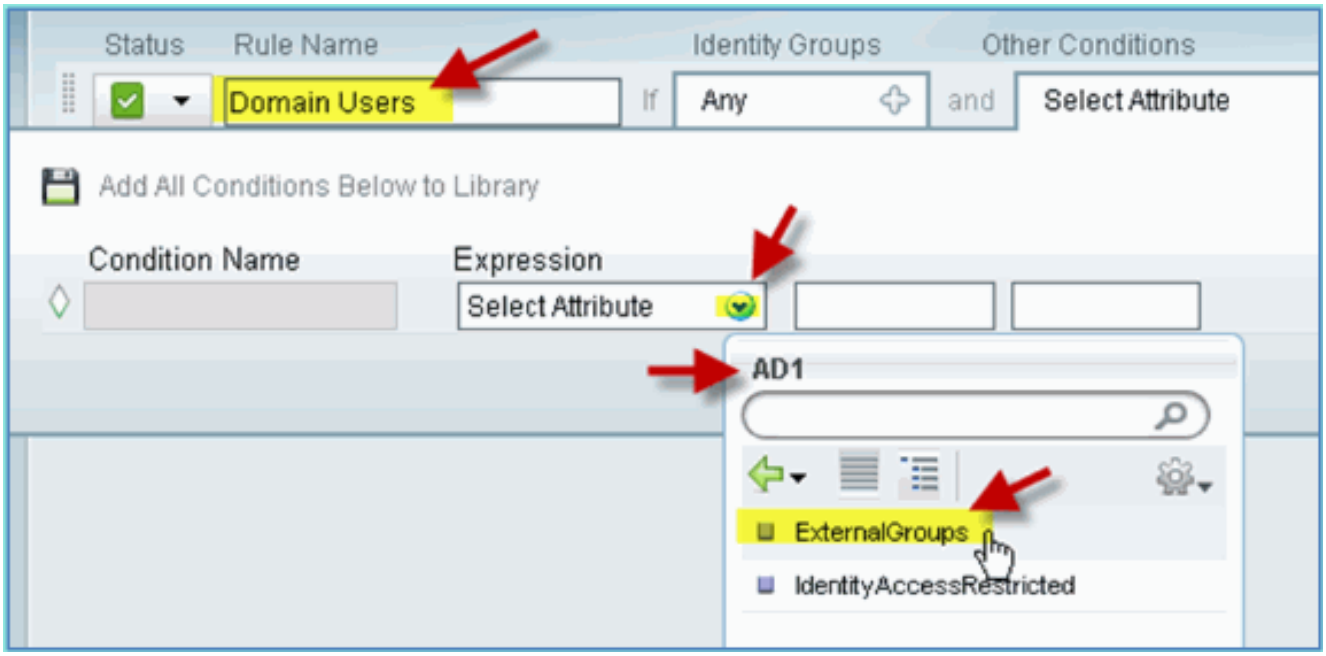
5. Insertar nueva directiva encima de la primera regla (haga clic en el icono **Acciones** de la derecha).



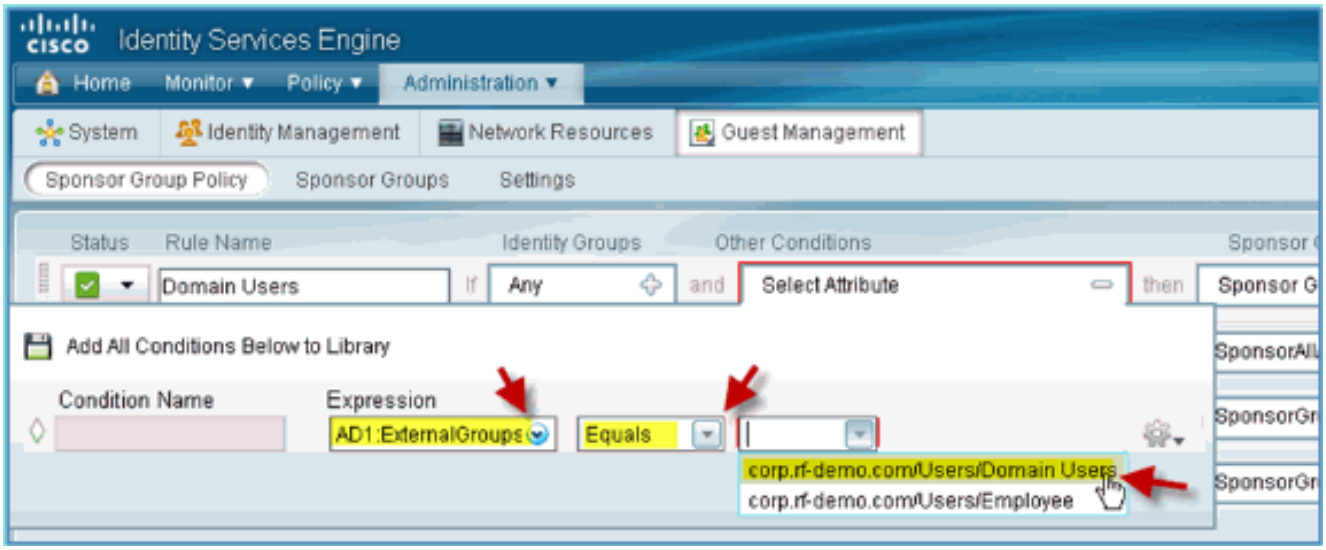
6. Para la nueva directiva de grupo de patrocinadores, cree lo siguiente:Nombre de regla: usuarios de dominioGrupos de identidades: CualquieraOtras condiciones: (Crear nuevo/Avanzado) >
AD1



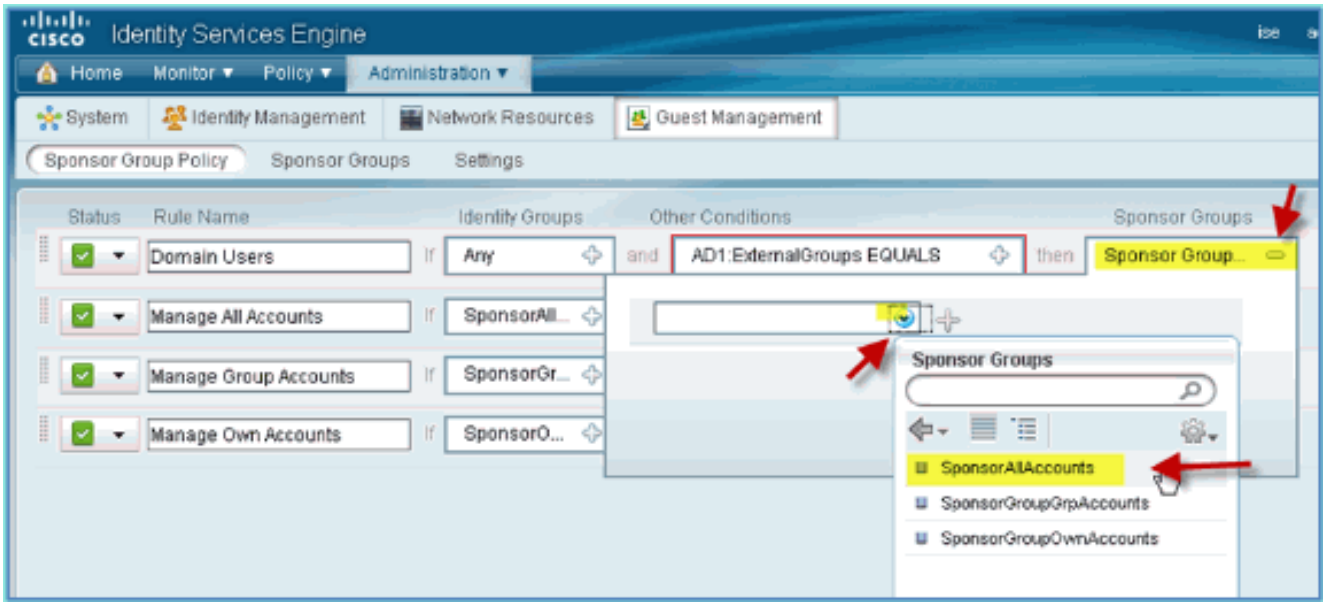
AD1: grupos externos



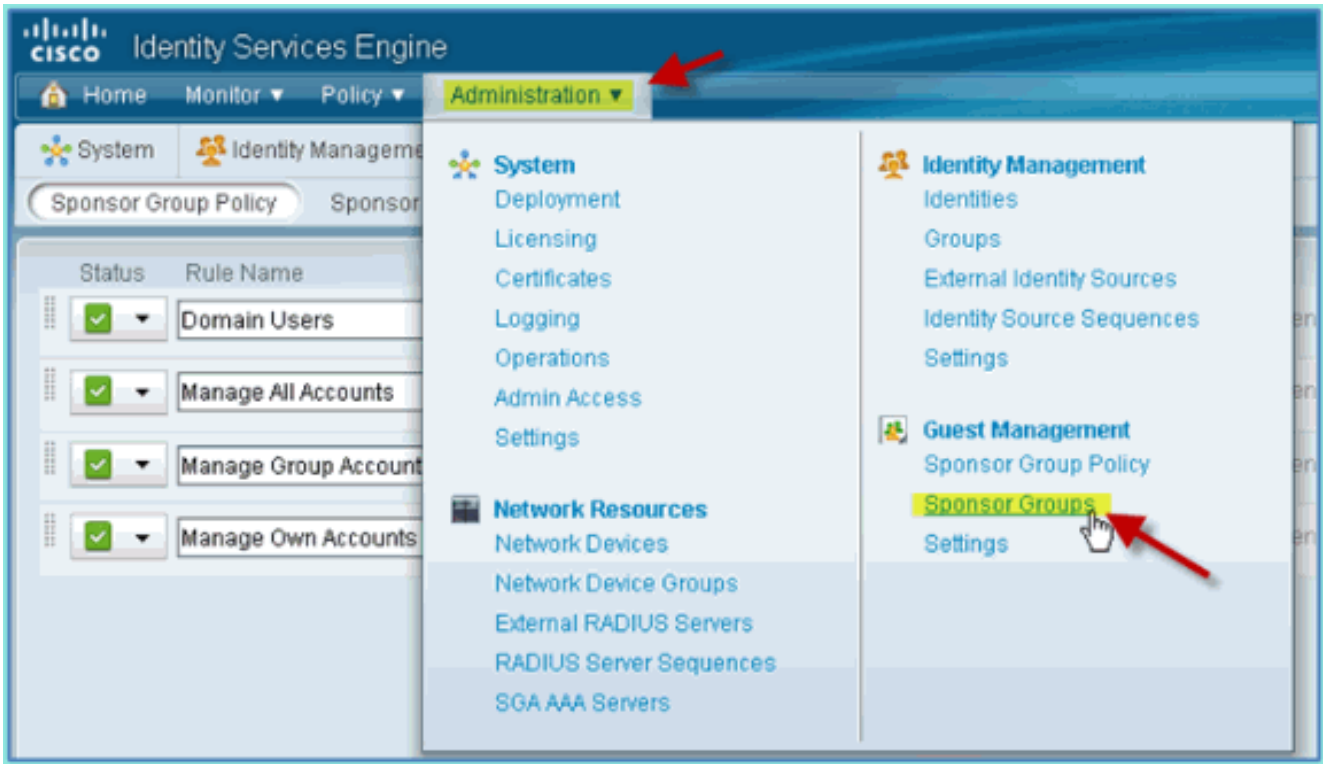
Grupos externos de AD1 > Igual a > corp.rf-demo.com/Users/Domain usuarios



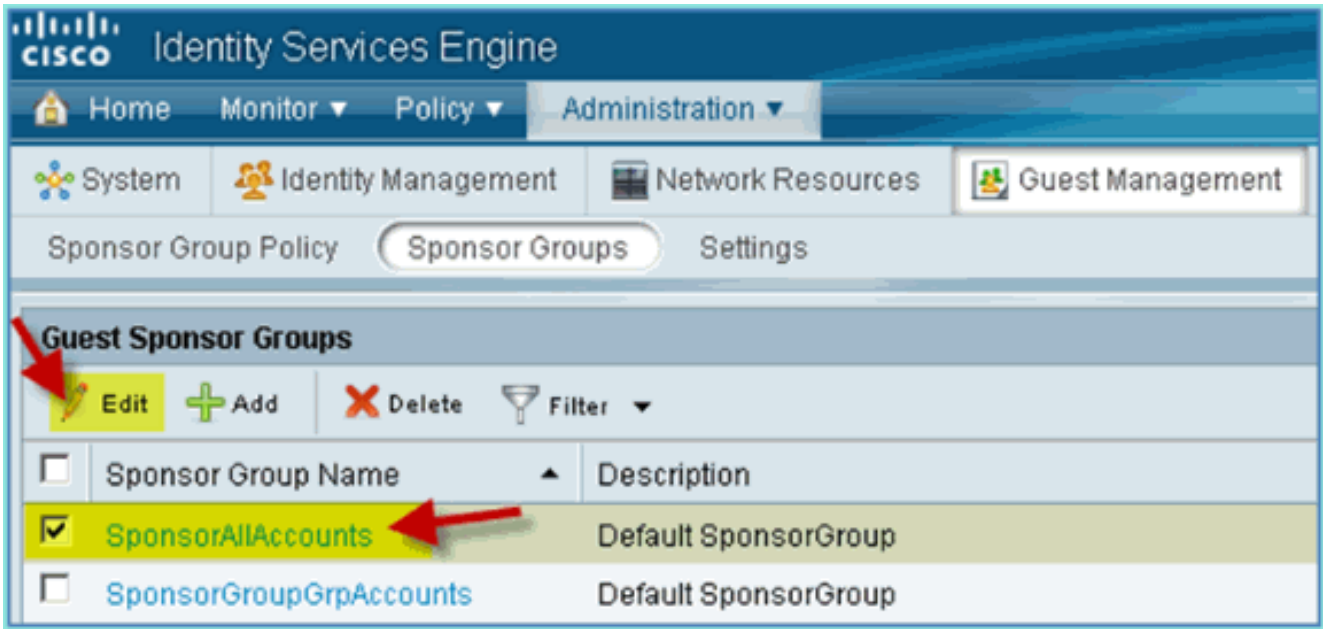
7. En Grupos de patrocinadores, establezca lo siguiente:Grupos de patrocinadores: PatrocinadorTodasLasCuentas



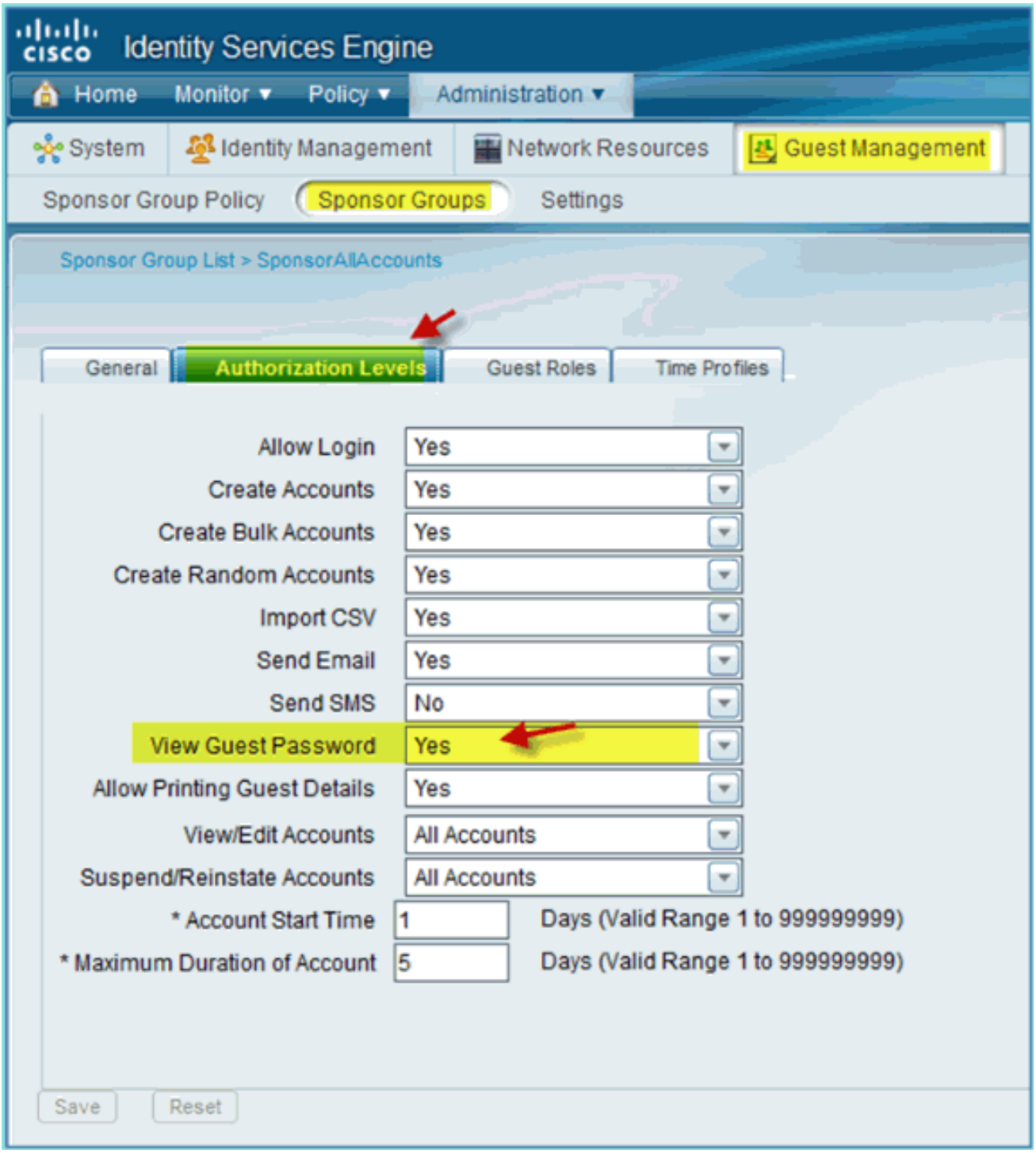
8. Vaya a **Administration > Guest Management > Sponsor Groups**.



9. Seleccione Edición > **PatrocinadorTodasLasCuentas**.



10. Seleccione Niveles de autorización y establezca lo siguiente:Ver contraseña de invitado: Sí



Configuración de SPAN en el switch

Configuración de SPAN: la interfaz de gestión/sonda de ISE es de nivel 2 adyacente a la interfaz de gestión de WLC. El switch se puede configurar para SPAN y otras interfaces, como VLAN de interfaz de invitado y de empleado.

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

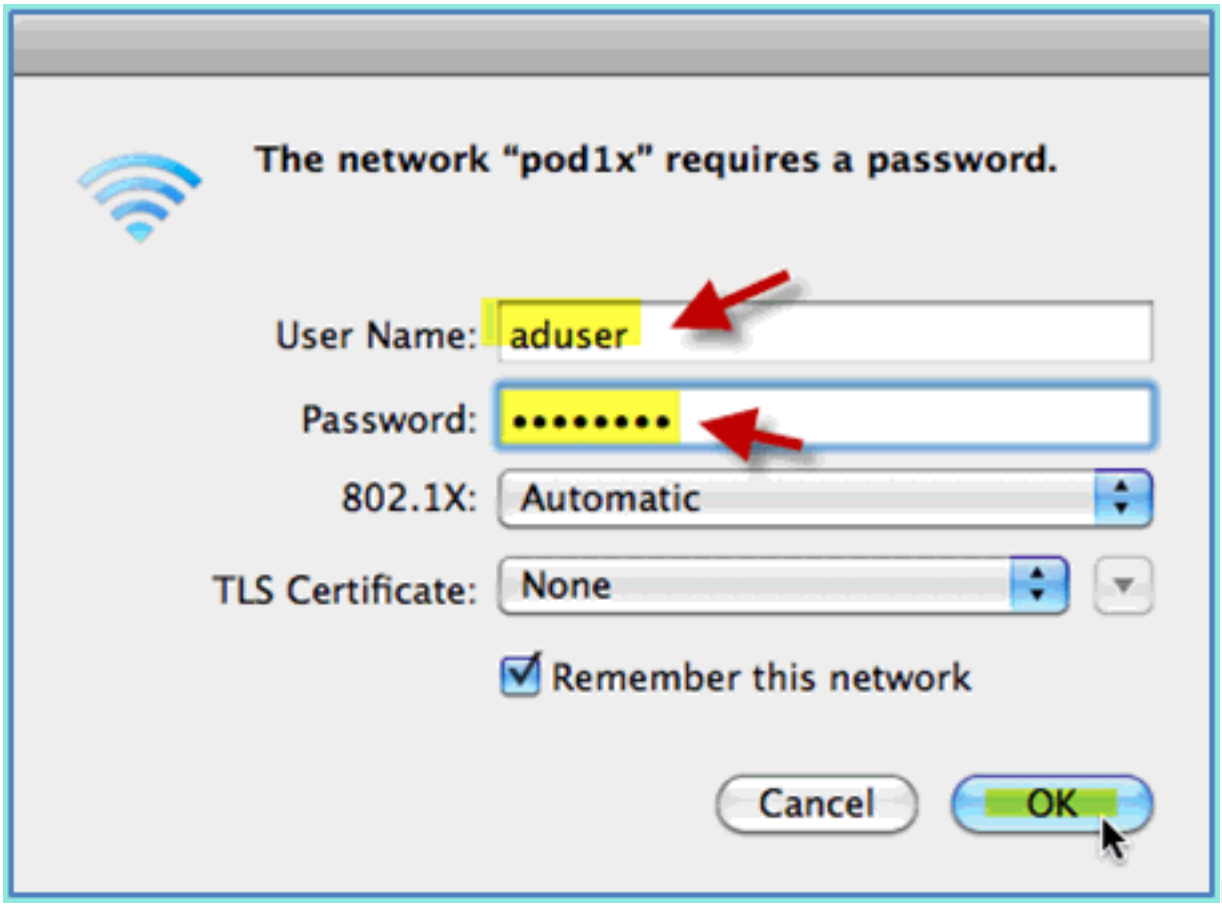
Referencia: Autenticación inalámbrica para Apple MAC OS X

Asociarse al WLC a través de un SSID autenticado como un usuario INTERNO (o integrado,

usuario AD) usando un Apple Mac OS X portátil inalámbrico. Sáltese si no procede.

1. En un Mac, vaya a la configuración de WLAN. Active WIFI y, a continuación, seleccione y conéctese al SSID de POD compatible con 802.1X creado en el ejercicio anterior.

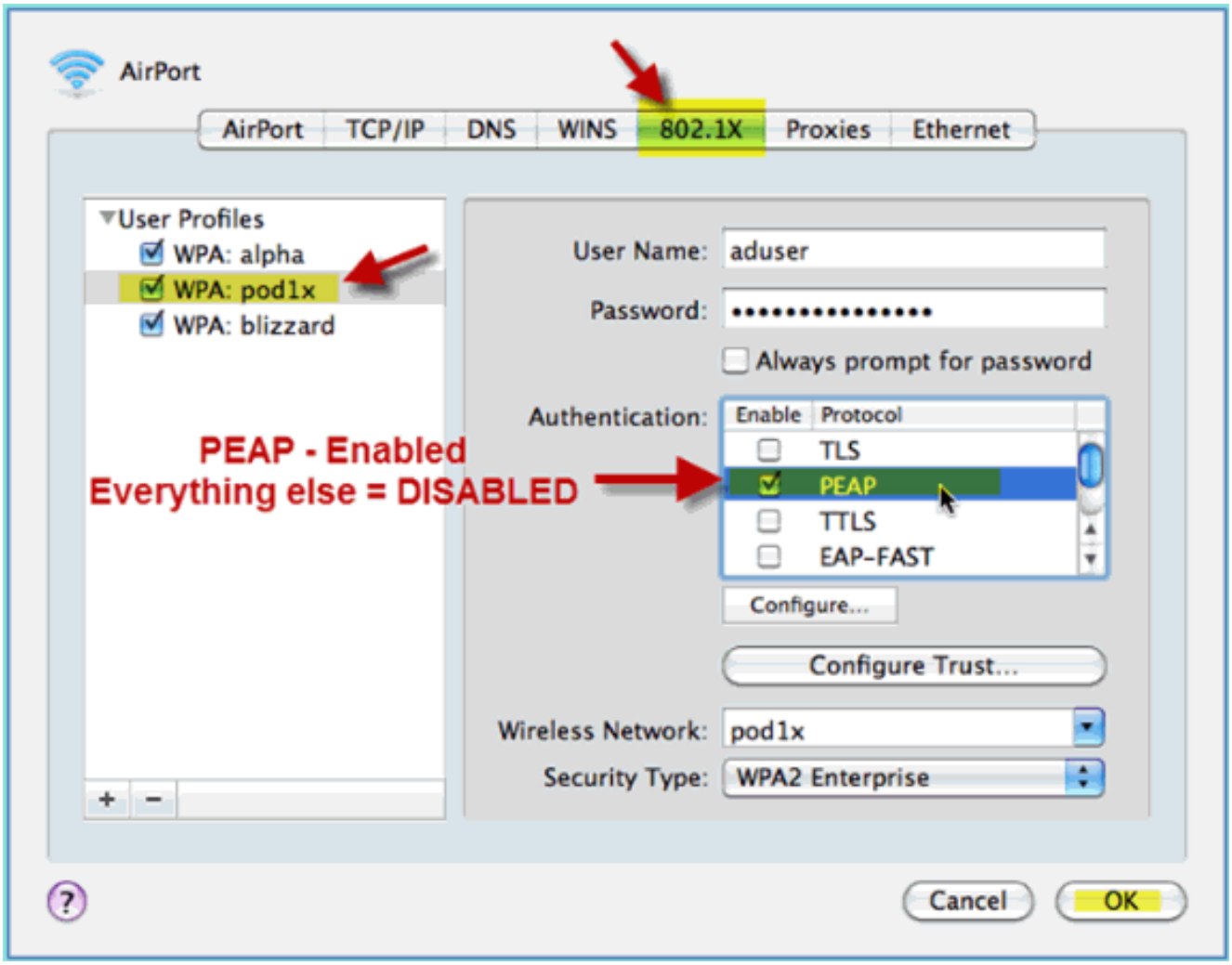
2. Proporcione la siguiente información para conectarse:Nombre de usuario: aduser (si utiliza AD), empleado (interno - Empleado), contratista (interno - Contratista)Contraseña: XXXX802.1X: AutomáticoCertificado TLS:
Ninguno



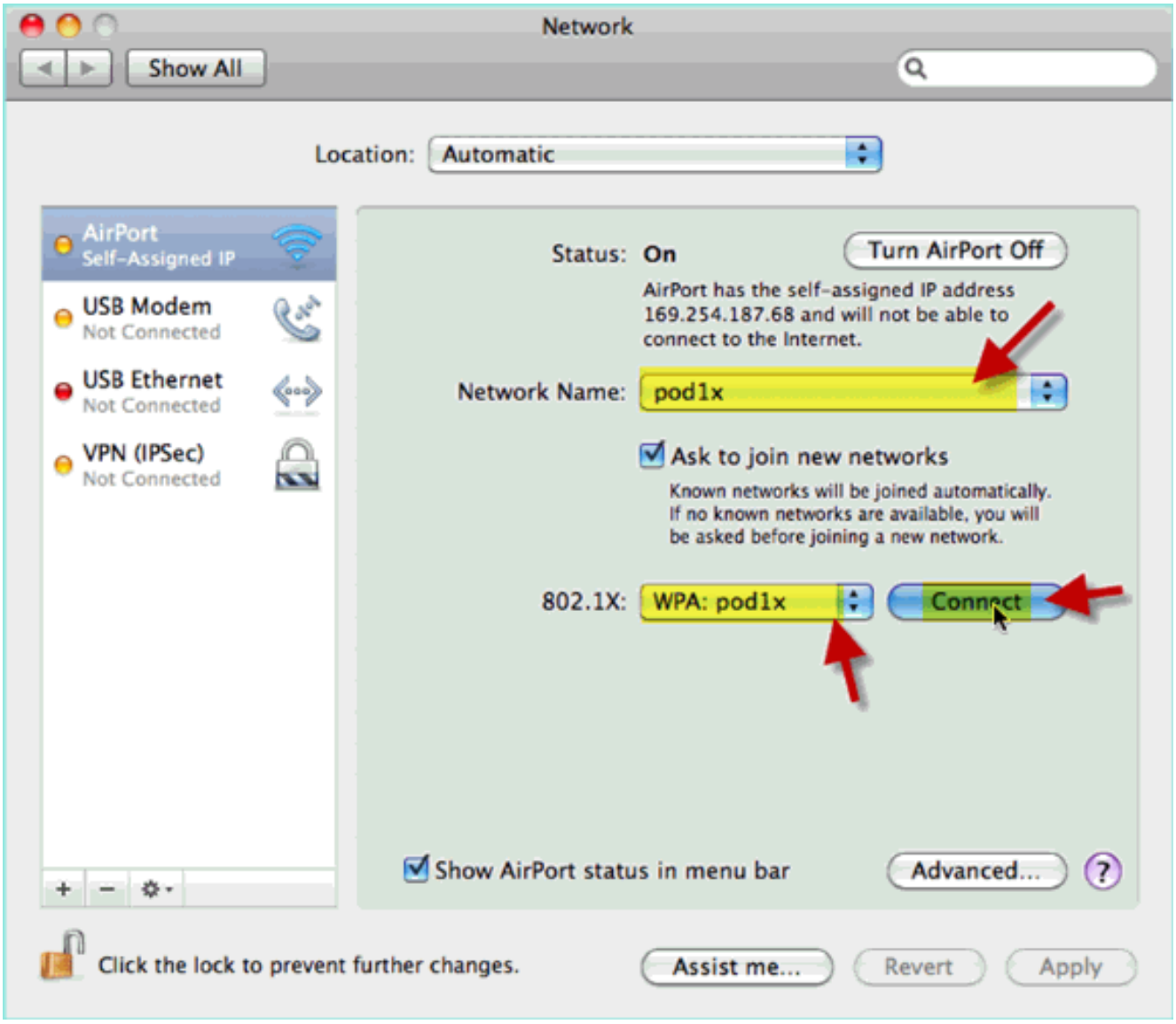
En este momento, es posible que el portátil no se conecte. Además, ISE puede producir un evento fallido como se indica a continuación:

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

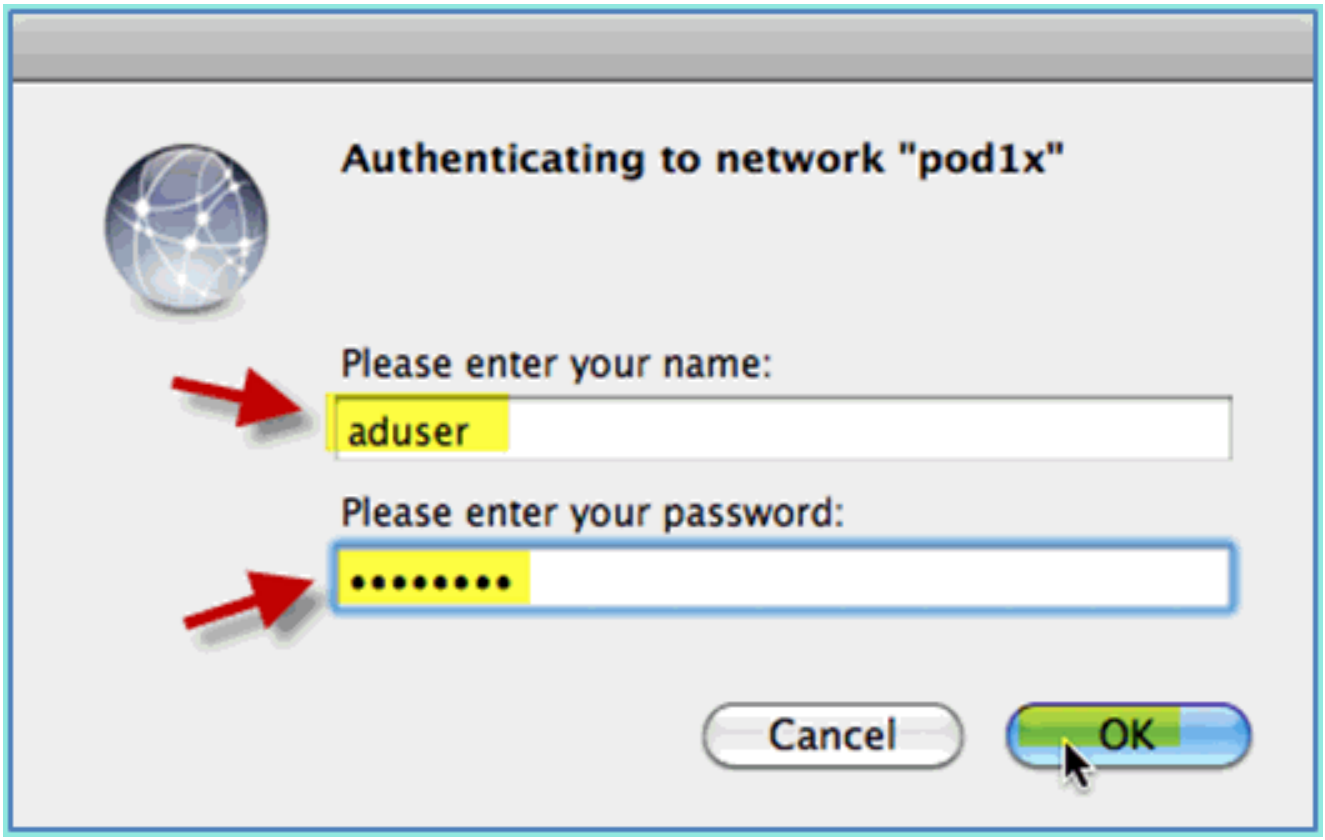
3. Vaya a **System Preferences > Network > Airport > 802.1X** y establezca la nueva autenticación de perfil POD SSID/ WPA como:TLS: deshabilitadoPEAP: habilitadoTTLS: desactivadoEAP-FAST:
desactivado



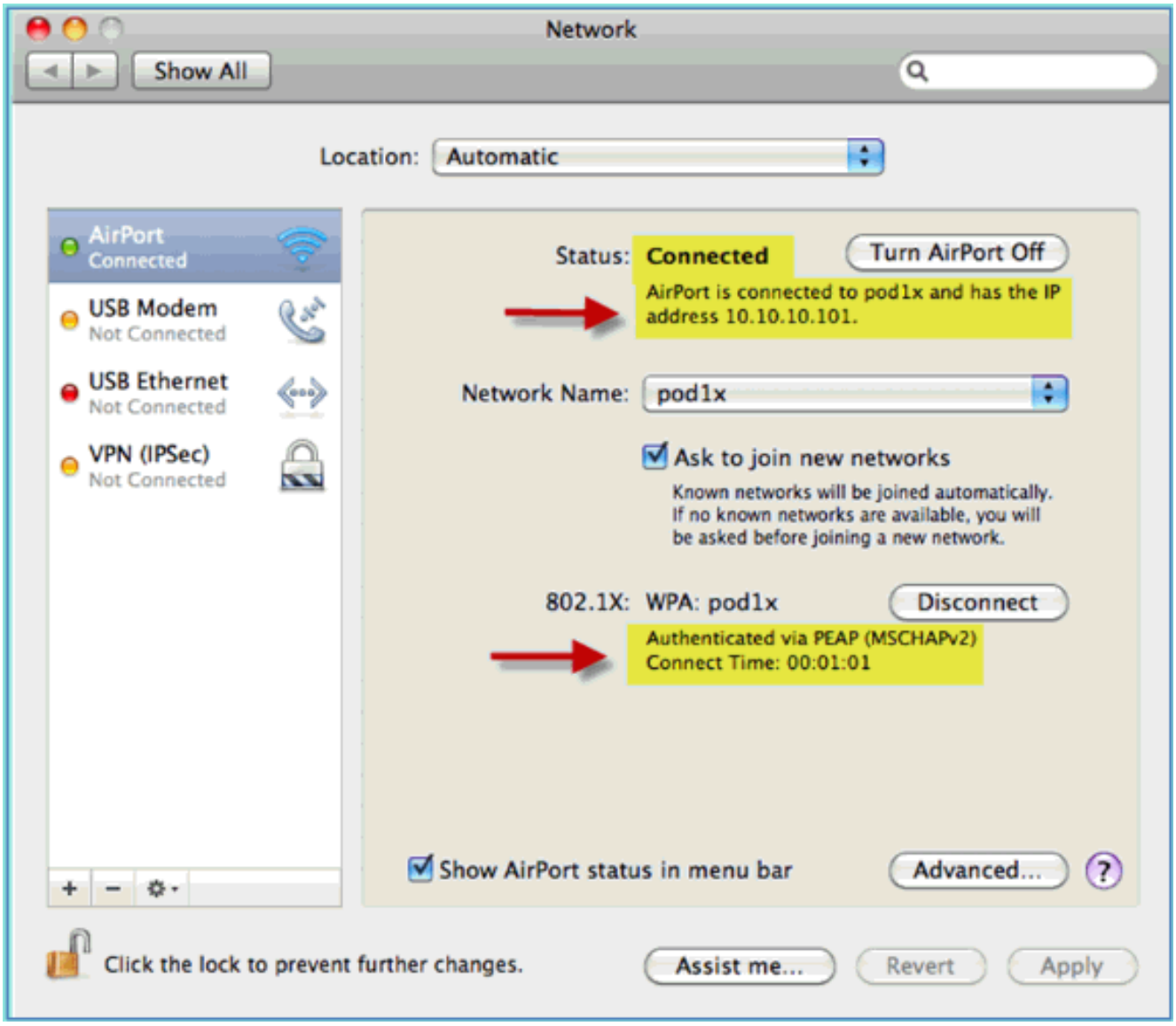
4. Haga clic en **Aceptar** para continuar y permitir que se guarde la configuración.
5. En la pantalla Network (Red), seleccione el SSID + perfil WPA 802.1X adecuado y haga clic en **Connect**
   (Conectar).



6. El sistema puede solicitar un nombre de usuario y una contraseña. Introduzca el usuario y la contraseña de AD (aduser/XXXX) y, a continuación, haga clic en **Aceptar**.



El cliente debe mostrar **Connected** via PEAP con una dirección IP válida.

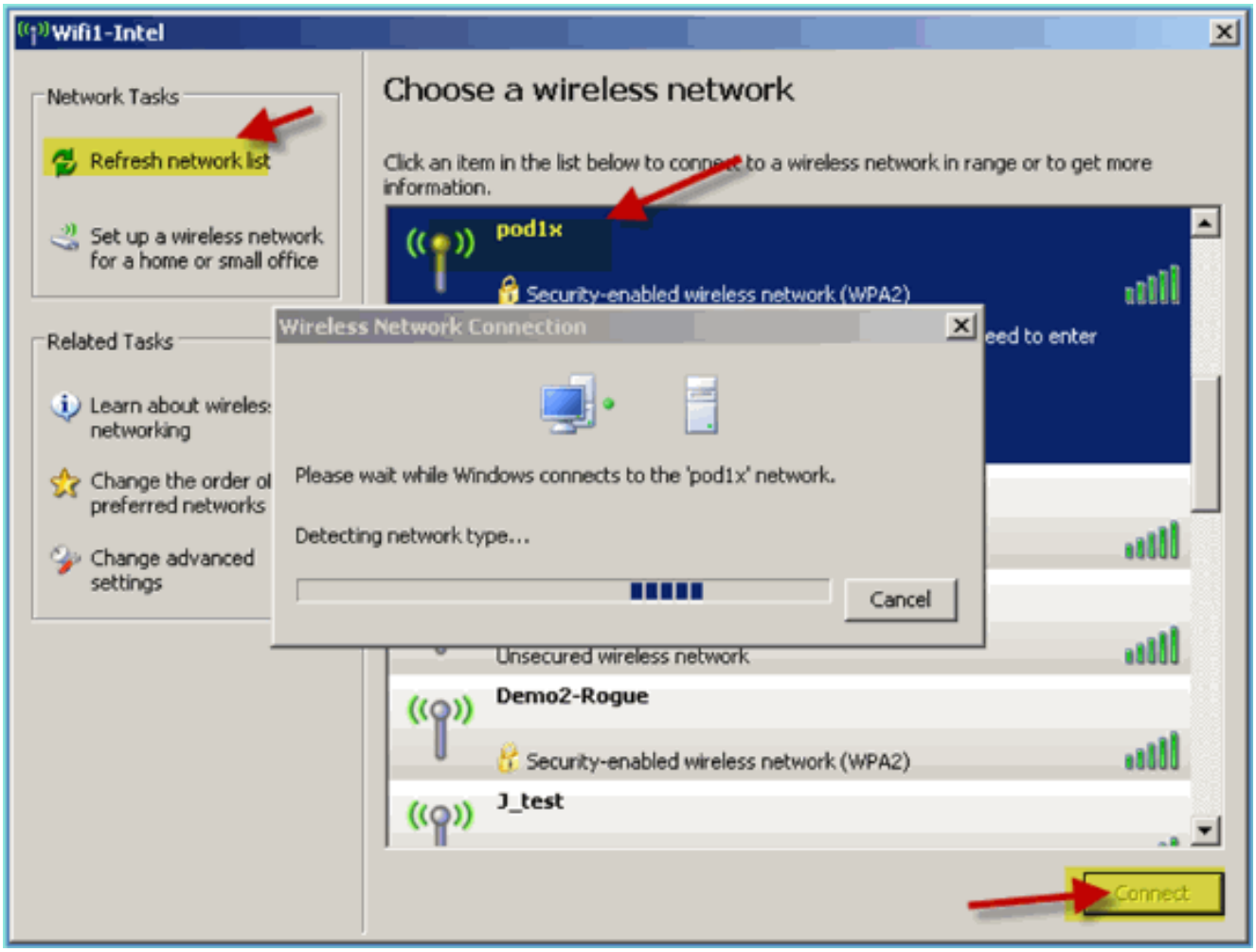


Referencia: Autenticación inalámbrica para Microsoft Windows XP

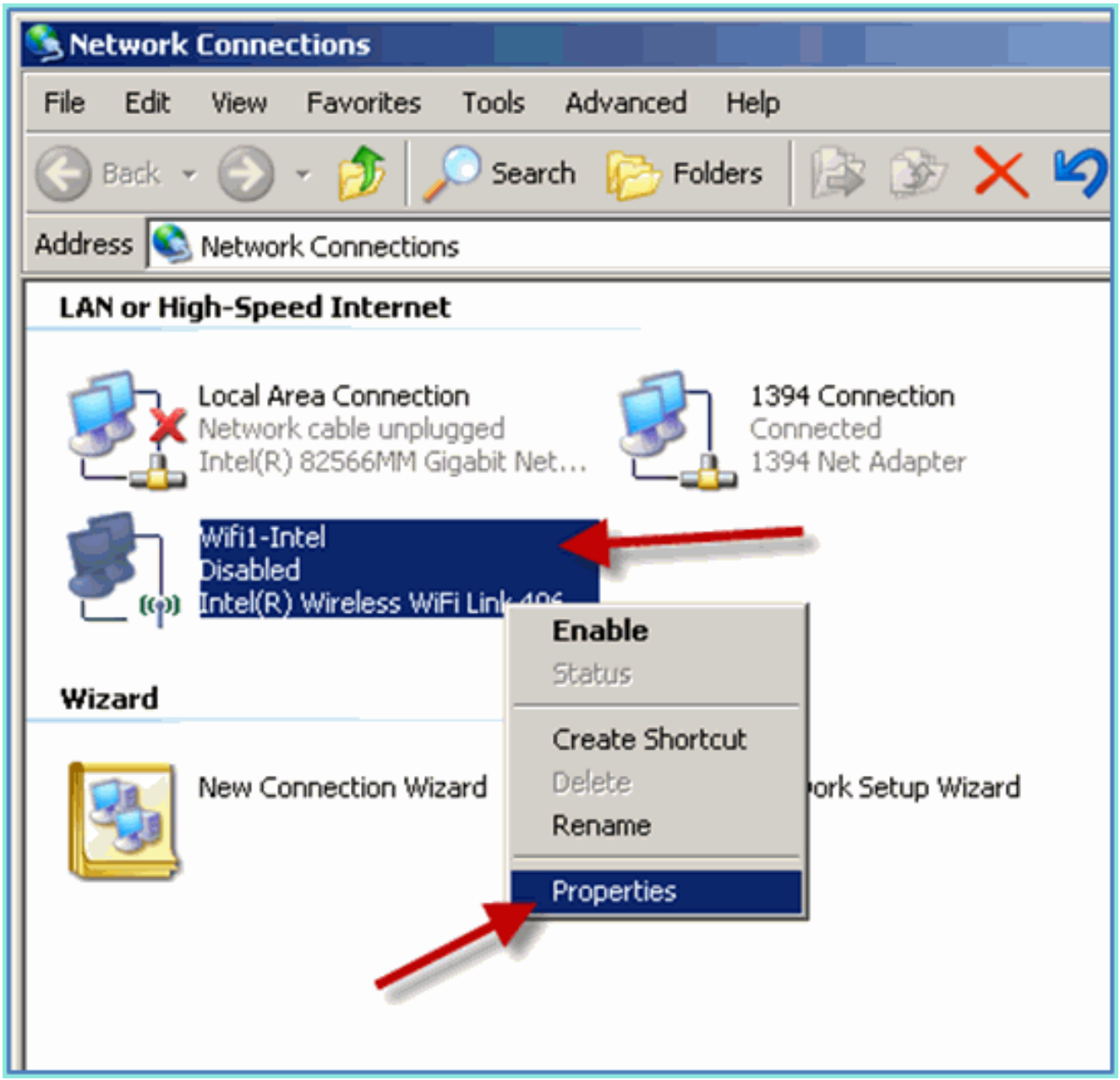
Asociarse al WLC a través de un SSID autenticado como un usuario INTERNO (o integrado, usuario AD) usando un portátil inalámbrico Windows XP. Sáltese si no procede.

Complete estos pasos:

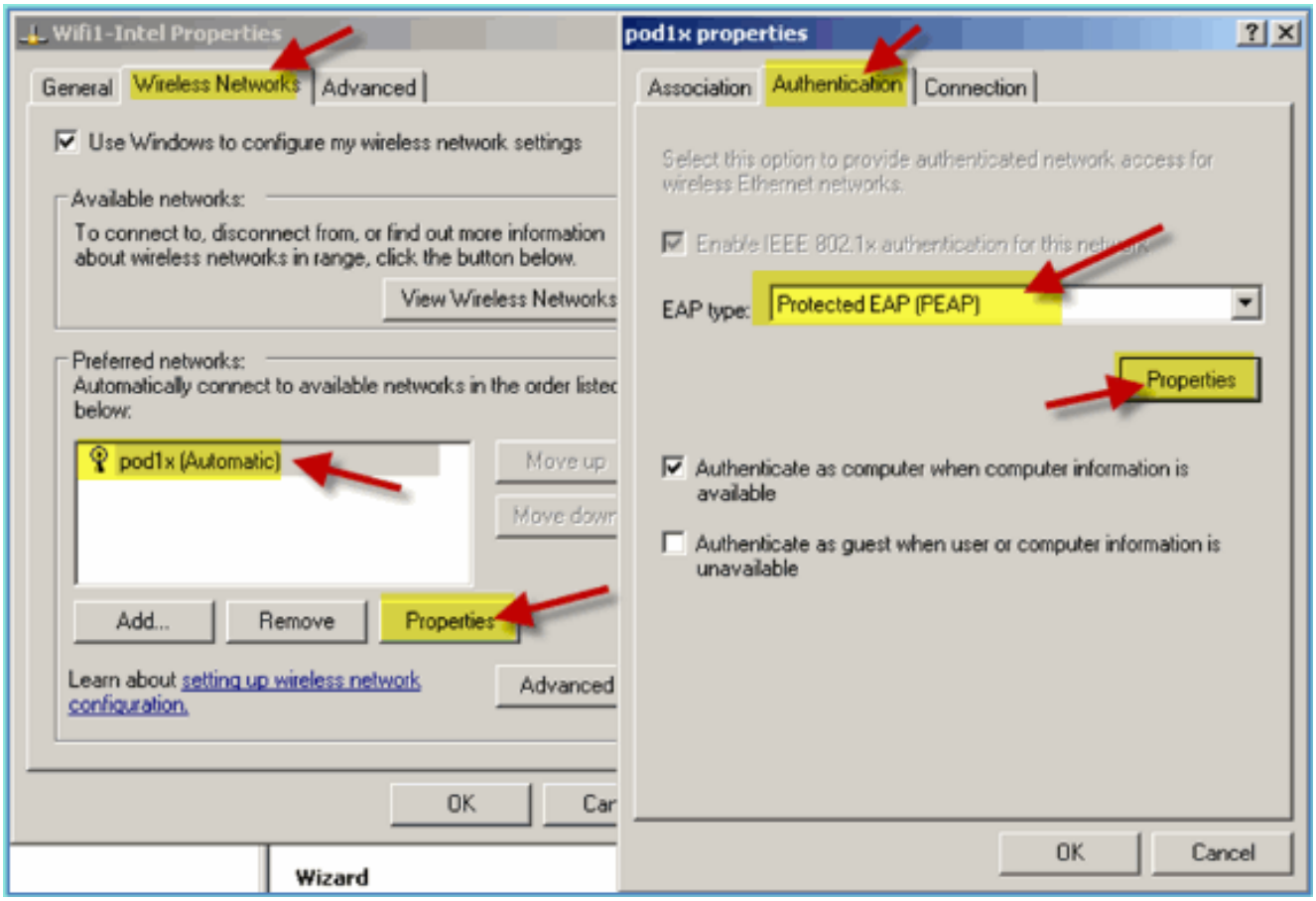
1. En el portátil, vaya a la configuración de WLAN. Active WIFI y conéctese al SSID de POD habilitado para 802.1X creado en el ejercicio anterior.



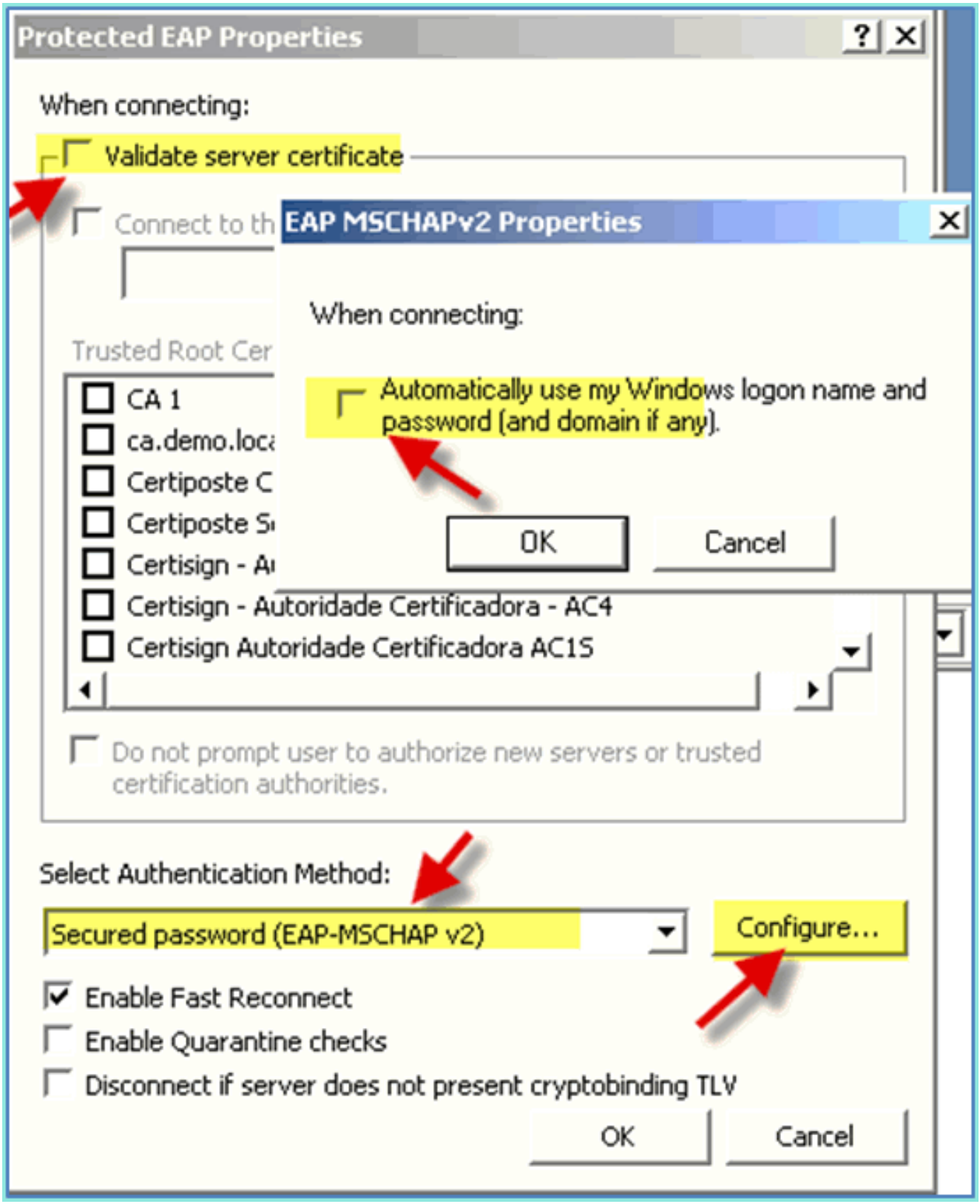
2. Acceda a las propiedades de red de la interfaz WIFI.



3. Vaya a la pestaña **Wireless Networks**. Seleccione las propiedades de red del POD SSID > ficha Autenticación > Tipo de EAP = EAP protegido (PEAP).



4. Haga clic en EAP Properties .
5. Establezca lo siguiente:Validar certificado de servidor: deshabilitadoMétodo de autenticación: contraseña segura (EAP-MSCHAP v2)

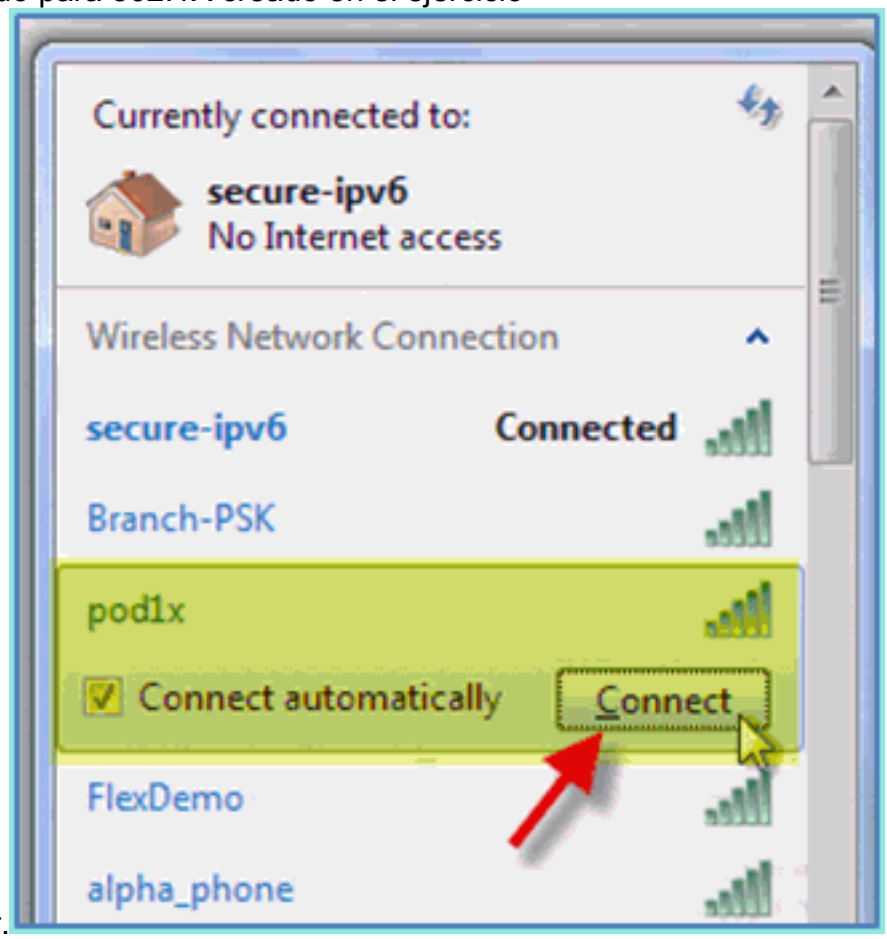


6. Haga clic en **Aceptar** en todas las ventanas para completar esta tarea de configuración.
7. El cliente de Windows XP solicita el nombre de usuario y la contraseña. En este ejemplo, es aduser/XXXX.
8. Confirme la conectividad de red y el direccionamiento IP (v4).

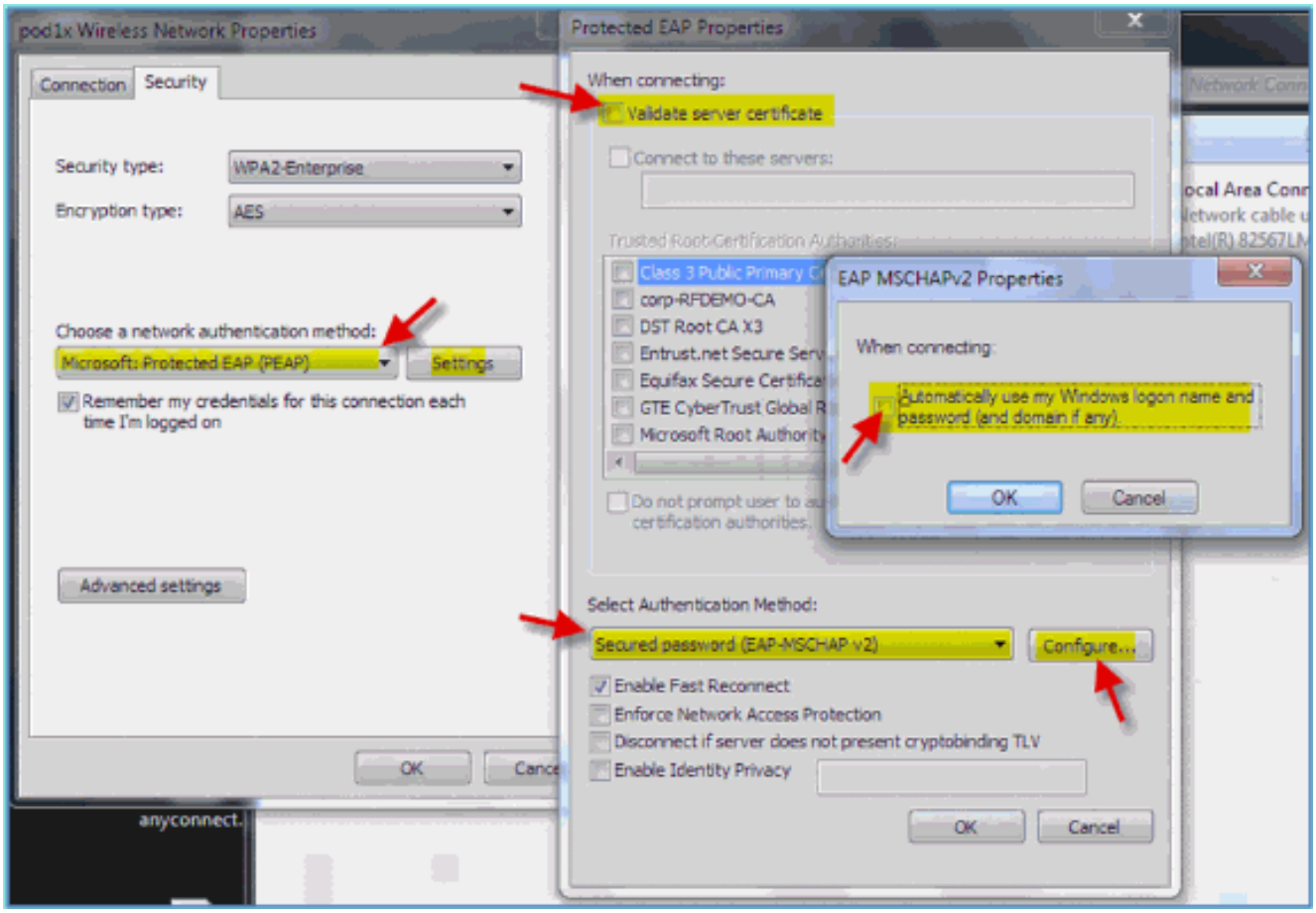
Referencia: Autenticación inalámbrica para Microsoft Windows 7

Asociarse al WLC a través de un SSID autenticado como un usuario INTERNO (o integrado, usuario AD) usando un portátil inalámbrico Windows 7.

1. En el portátil, vaya a la configuración de WLAN. Active WIFI y conéctese al SSID de POD habilitado para 802.1X creado en el ejercicio anterior.



2. Acceda al administrador inalámbrico y edite el nuevo perfil inalámbrico del POD.
3. Establezca lo siguiente:Método de autenticación: PEAPRecordar mis credenciales...: DeshabilitadoValidar certificado de servidor (configuración avanzada): deshabilitadoMétodo de autenticación (configuración avanzada): EAP-MSCHAP v2Usar automáticamente mi inicio de sesión de Windows...:
   Deshabilitado



Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).