Guía de implementación de BYOD inalámbrica para FlexConnect

Contenido

Introducción

Los dispositivos móviles son cada vez más potentes desde el punto de vista de la informática y son más populares entre los consumidores. Millones de estos dispositivos se venden a consumidores con Wi-Fi de alta velocidad para que los usuarios puedan comunicarse y colaborar. Los consumidores ya están acostumbrados a la mejora de la productividad que suponen estos dispositivos móviles en sus vidas y buscan trasladar su experiencia personal al espacio de trabajo. Esto crea las necesidades funcionales de una solución BYOD (Bring Your Own Device) en el lugar de trabajo.

Este documento proporciona la implementación en sucursal para la solución BYOD. Un empleado se conecta a un identificador de conjunto de servicios (SSID) corporativo con su nuevo iPad y se le redirige a un portal de autorregistro. Cisco Identity Services Engine (ISE) autentica al usuario frente a Active Directory (AD) corporativo y descarga un certificado con una dirección MAC y un nombre de usuario de iPad integrados en el iPad, junto con un perfil de solicitante que exige el uso del protocolo de autenticación extensible-seguridad de la capa de transporte (EAP-TLS) como método para la conectividad dot1x. De acuerdo con la política de autorización de ISE, el usuario puede conectarse mediante dot1x y acceder a los recursos adecuados.

Las funcionalidades de ISE de las versiones del software Cisco Wireless LAN Controller anteriores a la 7.2.110.0 no eran compatibles con los clientes de switching locales que se asocian a través de puntos de acceso (AP) FlexConnect. La versión 7.2.110.0 es compatible con estas funcionalidades de ISE para AP FlexConnect para switching local y clientes autenticados centralmente. Además, la versión 7.2.110.0 integrada con ISE 1.1.1 proporciona (sin limitarse a ello) estas funciones de la solución BYOD para redes inalámbricas:

- Perfil y estado del dispositivo
- Registro de dispositivos y aprovisionamiento de suplicantes
- Incorporación de dispositivos personales (dispositivos iOS o Android)

Nota: aunque son compatibles, otros dispositivos, como ordenadores portátiles y estaciones de trabajo inalámbricos PC o Mac, no se incluyen en esta guía.

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.

- Switches Cisco Catalyst
- Controladores de LAN inalámbrica (WLAN) de Cisco
- Software Cisco WLAN Controller (WLC) versión 7.2.110.0 y posteriores
- AP 802.11n en modo FlexConnect
- Software Cisco ISE versión 1.1.1 y posteriores
- Windows 2008 AD con autoridad certificadora (CA)
- Servidor DHCP
- Servidor del Sistema de nombres de dominio (DNS)
- Network Time Protocol (NTP)
- Portátil cliente inalámbrico, smartphone y tablets (Apple iOS, Android, Windows y Mac)

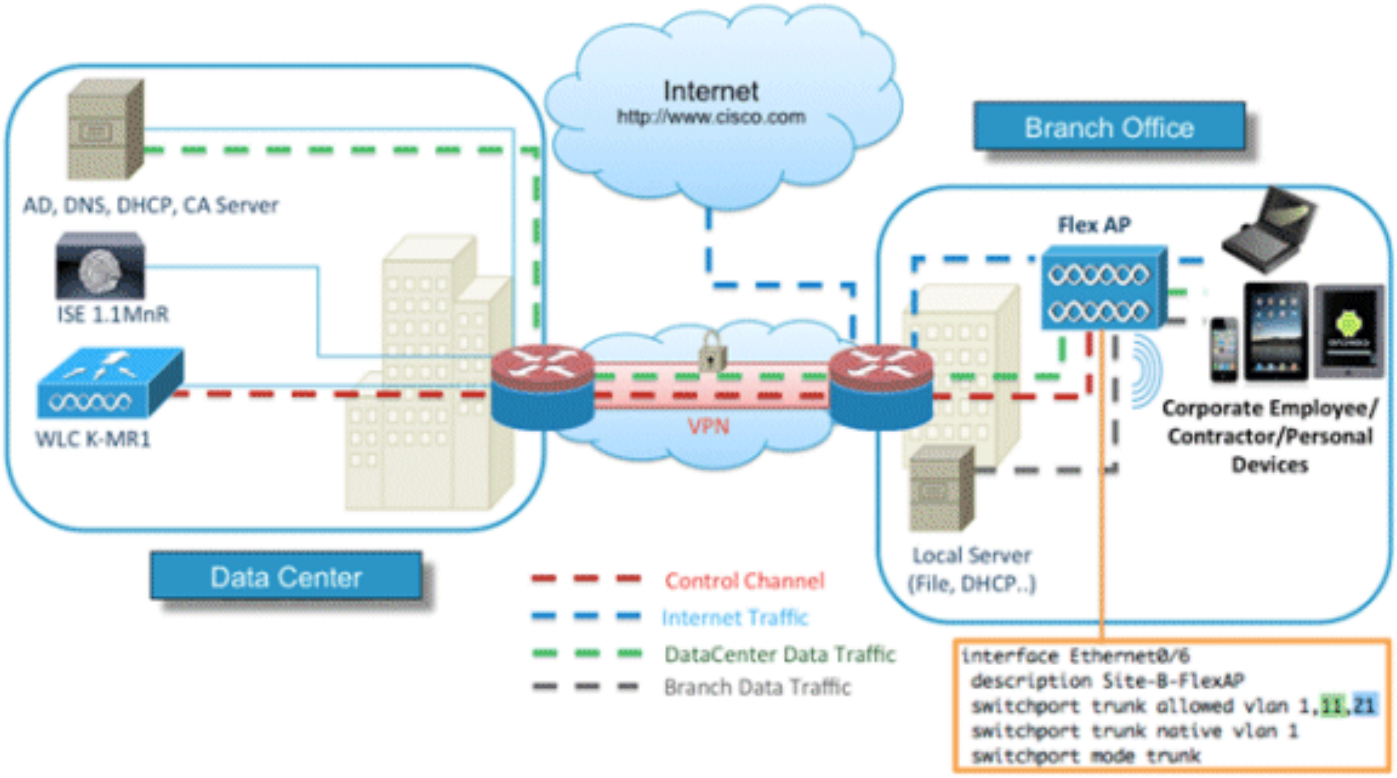
Nota: Consulte Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.2.110.0 para obtener información importante sobre esta versión de

software. Inicie sesión en el sitio Cisco.com para obtener las últimas notas de la versión antes de cargar y probar el software.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Topología

Se requiere una configuración de red mínima, como se muestra en este diagrama, para implementar y probar correctamente estas funciones:



Para esta simulación, necesita una red con un AP FlexConnect, un sitio local/remoto con DHCP local, DNS, el WLC y el ISE. El AP de FlexConnect está conectado a un tronco para probar el switching local con varias VLAN.

Registro de dispositivos y aprovisionamiento de suplicantes

Se debe registrar un dispositivo para que su suplicante nativo pueda aprovisionarse para la autenticación dot1x. De acuerdo con la política de autenticación adecuada, el usuario se redirige a la página de invitado y se autentica mediante las credenciales del empleado. El usuario ve la página de registro del dispositivo, que solicita la información del dispositivo. A continuación, comienza el proceso de aprovisionamiento de dispositivos. Si el sistema operativo (SO) no es compatible con el aprovisionamiento, el usuario se redirige al portal de registro de recursos para marcar ese dispositivo para el acceso de omisión de autenticación MAC (MAB). Si el sistema operativo es compatible, el proceso de inscripción comienza y configura el suplicante nativo del dispositivo para la autenticación dot1x.

Portal de registro de recursos

El portal de registro de activos es el elemento de la plataforma ISE que permite a los empleados iniciar la incorporación de terminales a través de un proceso de autenticación y registro.

Los administradores pueden eliminar recursos de la página de identidades de terminales. Cada empleado puede editar, eliminar y poner en una lista negra los activos que ha registrado. Los extremos de la lista negra se asignan a un grupo de identidades de la lista negra y se crea una política de autorización para impedir el acceso a la red por parte de los extremos de la lista negra.

Portal de autorregistro

En el flujo de Central Web Authentication (CWA), los empleados son redirigidos a un portal que les permite introducir sus credenciales, autenticarse e introducir los datos específicos del activo concreto que desean registrar. Este portal se denomina portal de autoaprovisionamiento y es similar al portal de registro de dispositivos. Permite a los empleados introducir la dirección MAC, así como una descripción significativa del terminal.

Autenticación y aprovisionamiento

Una vez que los empleados seleccionan el portal de autorregistro, se les solicita que proporcionen un conjunto de credenciales de empleado válidas para continuar con la fase de aprovisionamiento. Después de una autenticación correcta, el terminal se puede aprovisionar en la base de datos de terminales y se genera un certificado para el terminal. Un enlace en la página permite al empleado descargar el Asistente de cabecera de suplicante (SPW).

> **Nota**: Consulte el artículo de Cisco FlexConnect Feature Matrix para ver la matriz de funciones más reciente de FlexConnect para BYOD.

Aprovisionamiento para iOS (iPhone/iPad/iPod)

Para la configuración de EAP-TLS, ISE sigue el proceso de inscripción de Apple Over-the-Air (OTA):

- Después de una autenticación correcta, el motor de evaluación evalúa las políticas de aprovisionamiento de clientes, lo que da como resultado un perfil de solicitante.
- Si el perfil del solicitante es para la configuración de EAP-TLS, el proceso OTA determina si ISE está usando firma automática o firmada por una CA desconocida. Si se cumple una de las condiciones, se solicita al usuario que descargue el certificado de ISE o CA antes de que pueda comenzar el proceso de inscripción.
- Para otros métodos EAP, ISE envía el perfil final cuando la autenticación es correcta.

Aprovisionamiento para Android

Por motivos de seguridad, el agente de Android se debe descargar del sitio de Android Marketplace y no se puede aprovisionar desde ISE. Cisco carga una versión candidata a lanzamiento del asistente en Android Marketplace a través de la cuenta de editor de Cisco Android Marketplace.

Este es el proceso de aprovisionamiento de Android:

1. Cisco utiliza el Kit de desarrollo de software (SDK) para crear el paquete de Android con una extensión .apk.
2. Cisco carga un paquete en Android Marketplace.
3. El usuario configura la política en el aprovisionamiento del cliente con los parámetros apropiados.
4. Después del registro del dispositivo, el usuario final se redirige al servicio de aprovisionamiento del cliente cuando falla la autenticación dot1x.
5. La página del portal de aprovisionamiento proporciona un botón que redirige al usuario al portal de Android Marketplace, donde puede descargar el SPW.
6. Se inicia Cisco SPW y realiza el aprovisionamiento del solicitante: SPW detecta el ISE y descarga el perfil de ISE.SPW crea un par certificado/clave para EAP-TLS.SPW realiza una llamada de solicitud de proxy de protocolo simple de inscripción de certificados (SCEP) a ISE y obtiene el certificado.SPW aplica los perfiles inalámbricos.SPW activa la reautenticación si los perfiles se aplican correctamente.El SPW sale.

Registro automático de BYOD inalámbrico con SSID dual

Este es el proceso para el autorregistro de BYOD inalámbrico con SSID dual:

1. El usuario se asocia al SSID de invitado.
2. El usuario abre un navegador y se le redirige al portal de invitados de ISE CWA.
3. El usuario introduce un nombre de usuario y una contraseña de empleado en el portal de invitados.
4. ISE autentica al usuario y, basándose en el hecho de que se trata de un empleado y no de un invitado, redirige al usuario a la página de invitados de registro de dispositivos del empleado.
5. La dirección MAC se rellena automáticamente en la página de invitado Device Registration para DeviceID. El usuario introduce una descripción y acepta la política de uso aceptable (AUP) si es necesario.
6. El usuario selecciona **Accept** y comienza a descargar e instalar el SPW.
7. El solicitante del dispositivo de ese usuario se suministra junto con los certificados.
8. Se produce CoA y el dispositivo se vuelve a asociar al SSID corporativo (CORP) y se autentica con EAP-TLS (u otro método de autorización en uso para ese solicitante).

Registro automático de BYOD inalámbrico SSID único

En esta situación, existe un único SSID para el acceso corporativo (CORP) que admite tanto el protocolo de autenticación ampliable protegido (PEAP) como EAP-TLS. No hay SSID de invitado.

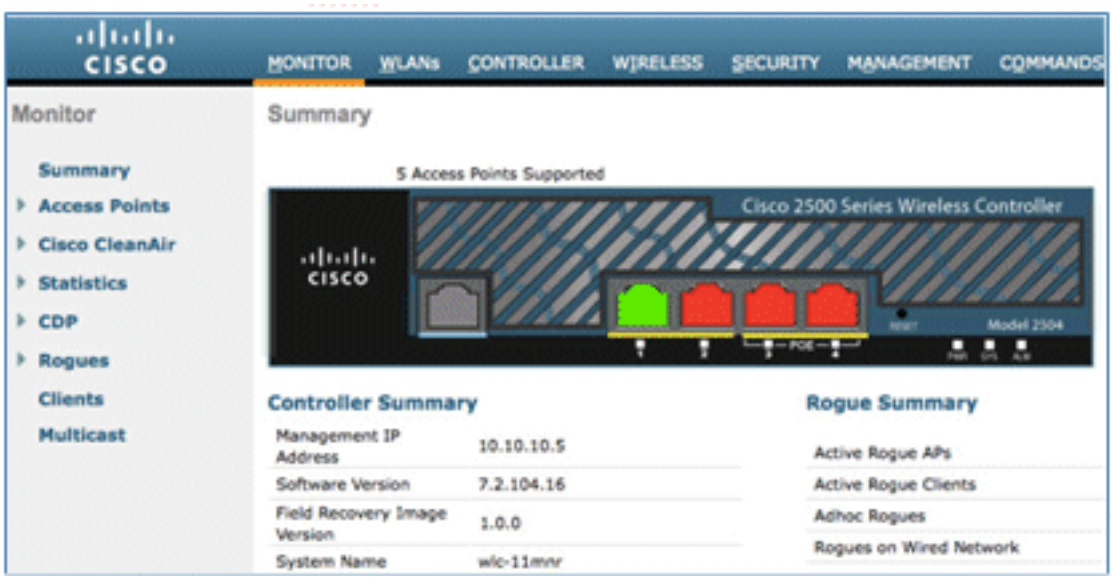
Este es el proceso para el autorregistro de BYOD inalámbrico con un solo SSID:

1. El usuario se asocia a CORP.
2. El usuario introduce un nombre de usuario y una contraseña de empleado en el solicitante para la autenticación PEAP.
3. ISE autentica al usuario y, en función del método PEAP, proporciona una política de autorización de aceptar con redirigir a la página de invitados Registro de dispositivos de empleados.
4. El usuario abre un navegador y se le redirige a la página de invitados Registro de dispositivo de empleado.
5. La dirección MAC se rellena automáticamente en la página de invitado Device Registration para DeviceID. El usuario introduce una descripción y acepta la PUA.
6. El usuario selecciona **Accept** y comienza a descargar e instalar el SPW.
7. El solicitante del dispositivo de ese usuario se suministra junto con los certificados.
8. Se produce CoA y el dispositivo se vuelve a asociar al SSID CORP y se autentica con EAP-TLS.

Configuración de funciones

Complete estos pasos para comenzar la configuración:

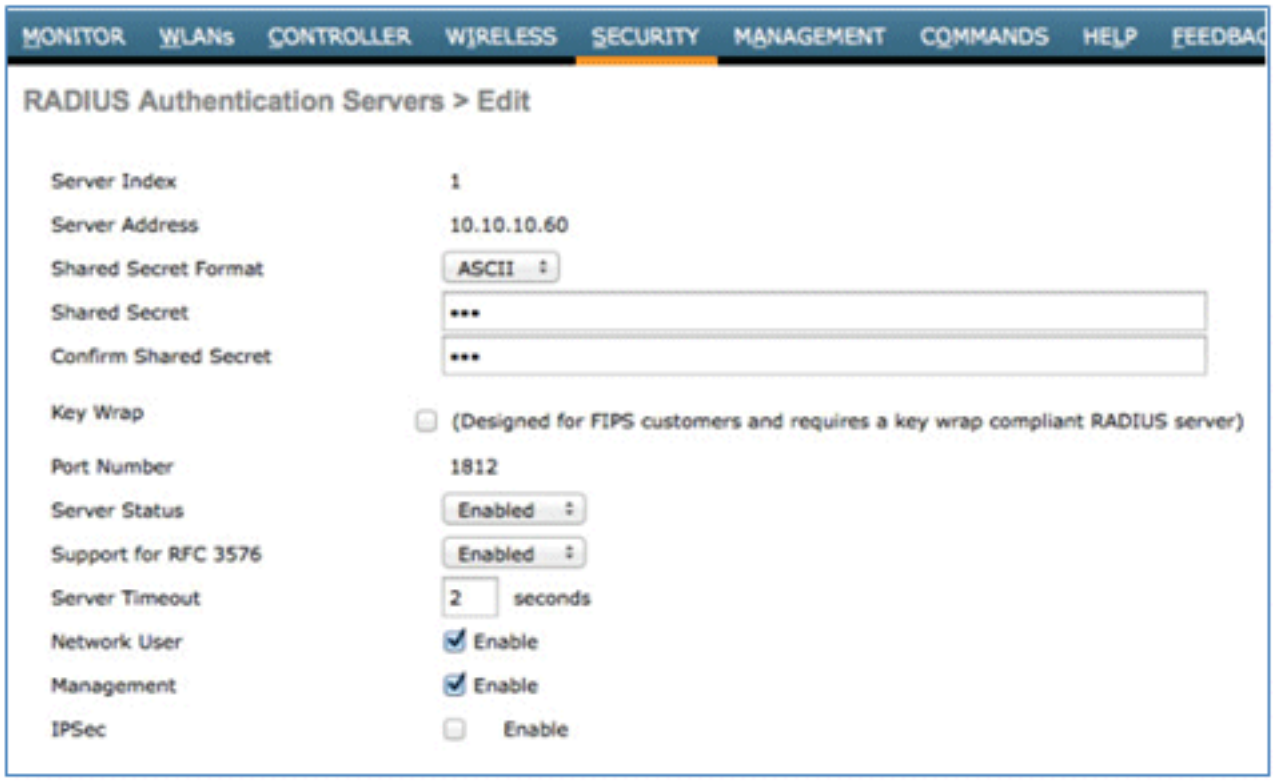
1. Para esta guía, asegúrese de que la versión del WLC es 7.2.110.0 o posterior.



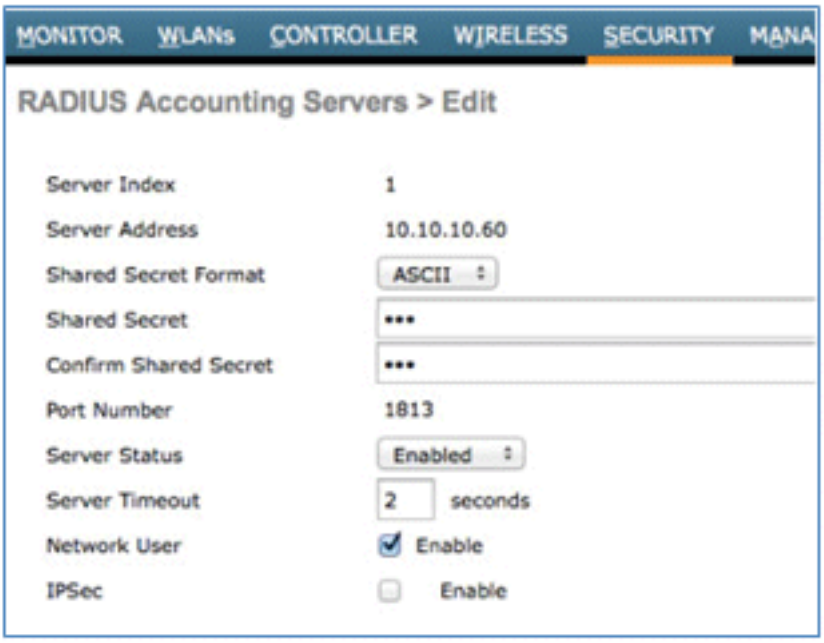
2. Navegue hasta **Seguridad > RADIUS > Autenticación**, y agregue el servidor RADIUS al WLC.

3. Agregue ISE 1.1.1 al WLC:

   Introduzca una clave secreta compartida.Establezca Support for RFC 3576 en **Enabled**.



4. Agregue el mismo servidor ISE que un servidor de cuentas RADIUS.



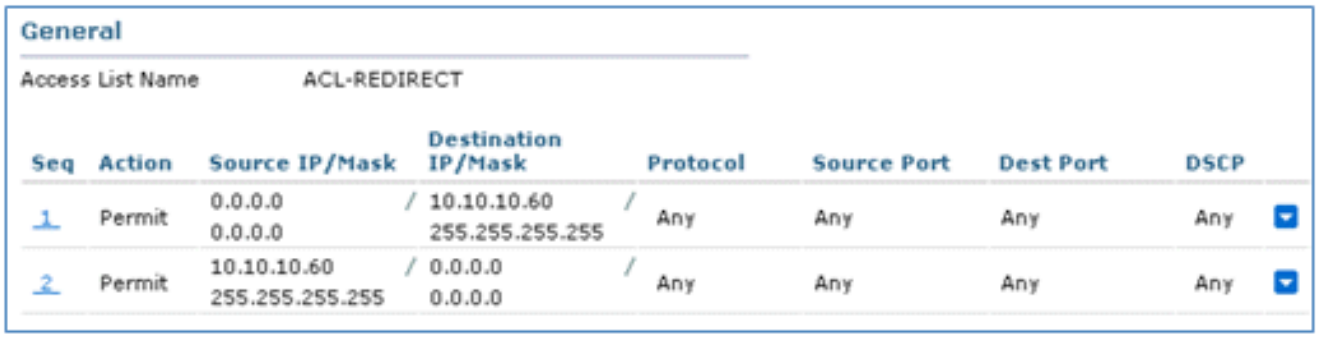
5. Cree una ACL previa a la autenticación WLC para usarla en la política ISE más adelante. Navegue hasta WLC > **Security > Access Control Lists > FlexConnect ACL** y cree una nueva ACL de FlexConnect denominada ACL-REDIRECT (en este ejemplo).

6. En las reglas de ACL, permita todo el tráfico hacia/desde el ISE y permita el tráfico del cliente durante el aprovisionamiento del solicitante.

   Para la primera regla (secuencia 1):

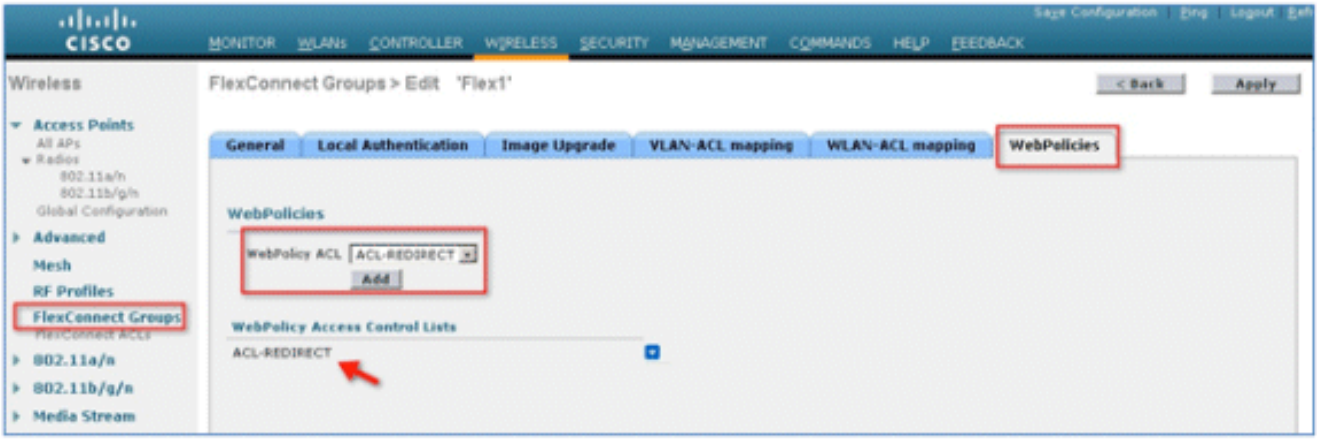
   Establezca Source en **Any**.Establecer IP (dirección ISE)/máscara de red **255.255.255.255**.Establezca Acción en **Permitir**.

Para la segunda regla (secuencia 2), establezca la IP de origen (dirección ISE)/ máscara 255.255.255.255 en **Any** y la acción en **Permit**.



7. Cree un nuevo grupo de FlexConnect denominado Flex1 (en este ejemplo):

   Vaya a la pestaña **FlexConnect Group > WebPolicies**.En el campo WebPolicy ACL, haga clic en **Add** y seleccione **ACL-REDIRECT** o la ACL de FlexConnect creada anteriormente.Confirme que rellena el campo **Listas de control de acceso de WebPolicy**.



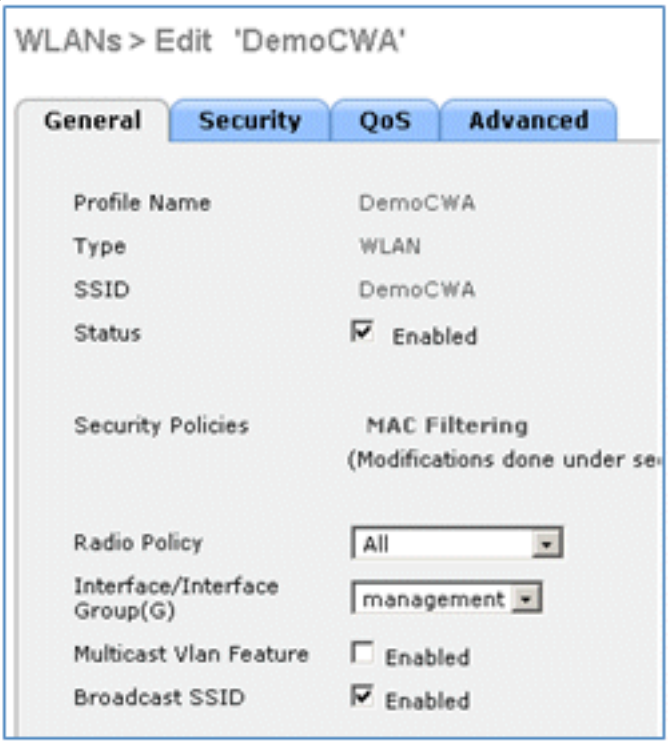
8. Haga clic en **Apply** y **Save Configuration**.

Configuración de WLAN

Complete estos pasos para configurar el WLAN:

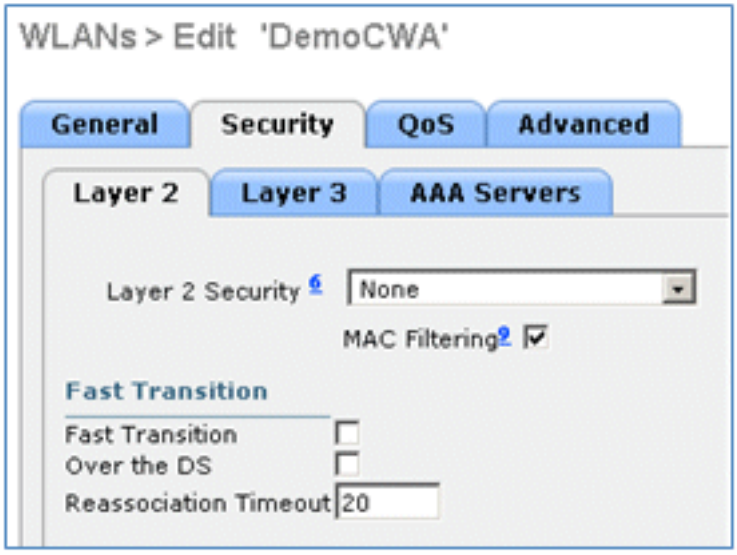
1. Cree un SSID de WLAN abierto para el ejemplo de SSID dual:

   Introduzca un nombre WLAN: **DemoCWA** (en este ejemplo).Seleccione la opción **Activado** para Estado.



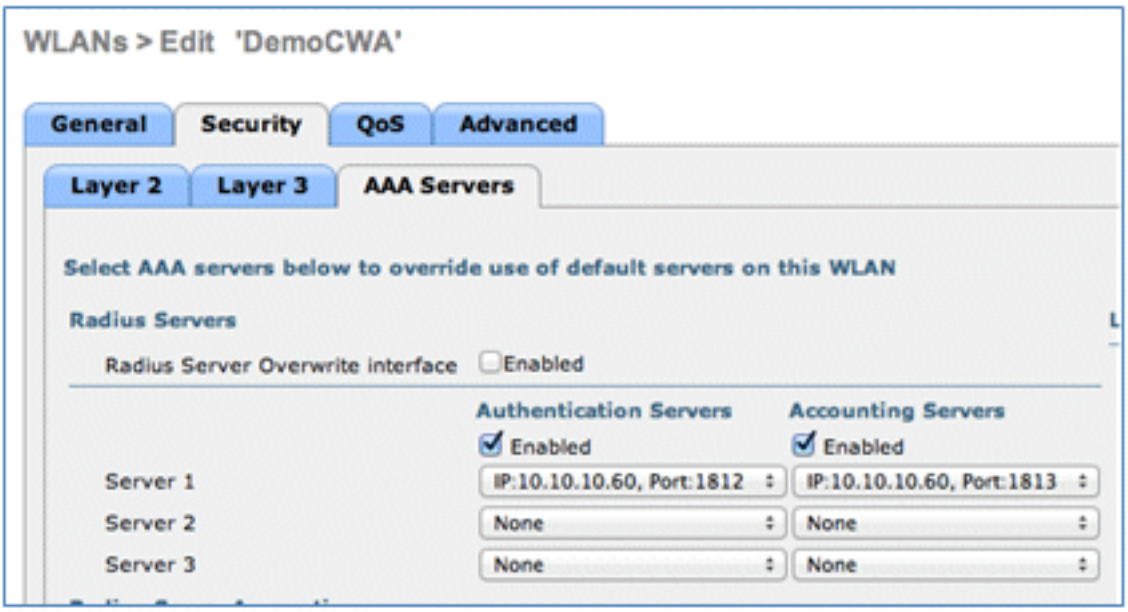
2. Navegue hasta la pestaña **Seguridad** > pestaña **Capa 2** y establezca estos atributos:

   Seguridad de capa 2: **ninguna**Filtrado de MAC: **habilitado** (la casilla está activada)Transición rápida: **Desactivada** (la casilla no está activada)



3. Vaya a la pestaña **AAA Servers** y establezca estos atributos:

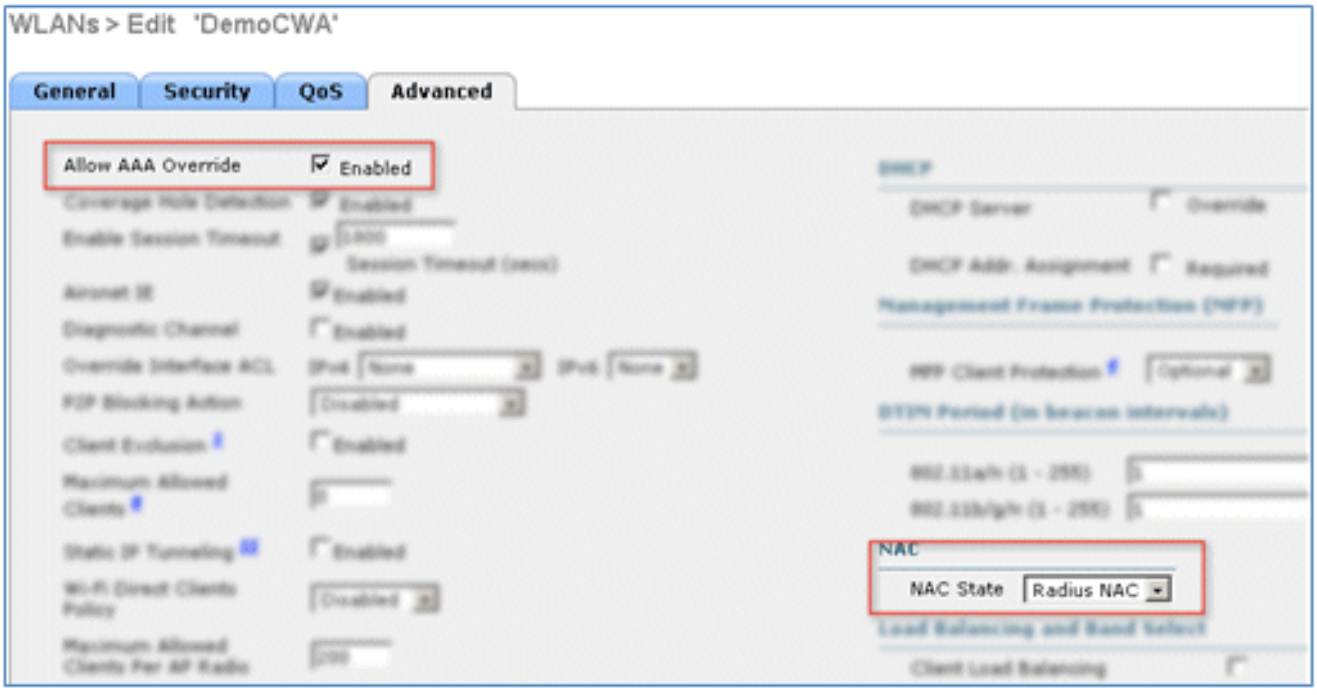
   Servidores de cuentas y autenticación: **Habilitado**Servidor 1: *<dirección IP de ISE>*



4. Desplácese hacia abajo desde la pestaña **AAA Servers**. En Orden de prioridad de autenticación para el usuario de autenticación web, asegúrese de que **RADIUS** se utiliza para la autenticación y de que no se utilizan los demás.

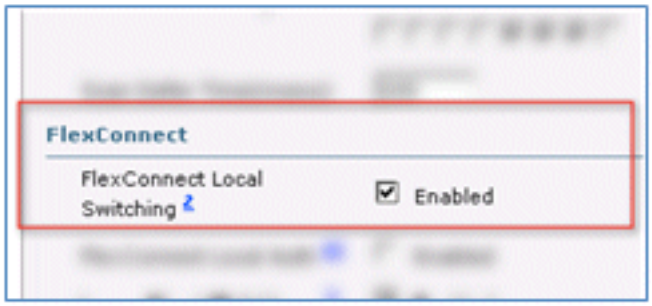
5. Vaya a la pestaña **Advanced** y establezca estos atributos:

Permitir Sustitución de AAA: **Activado**Estado de NAC: **Radius NAC**

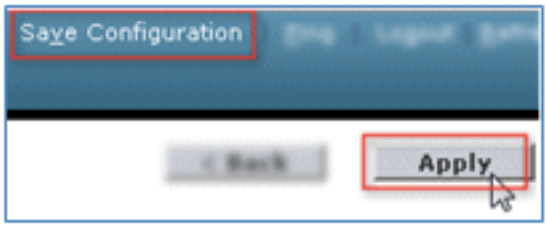


Nota: El control de admisión a la red (NAC) de RADIUS no se admite cuando el punto de acceso de FlexConnect está en modo desconectado. Por lo tanto, si el AP de FlexConnect está en modo autónomo y pierde la conexión con el WLC, todos los clientes se desconectan y el SSID ya no se anuncia.

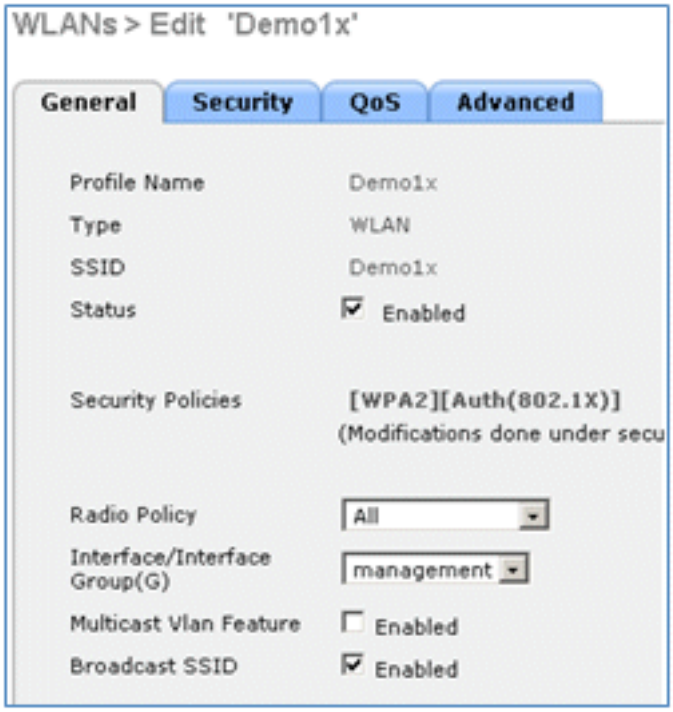
6. Desplácese hacia abajo en la ficha Advanced (Opciones avanzadas) y establezca FlexConnect Local Switching en **Enabled**.



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



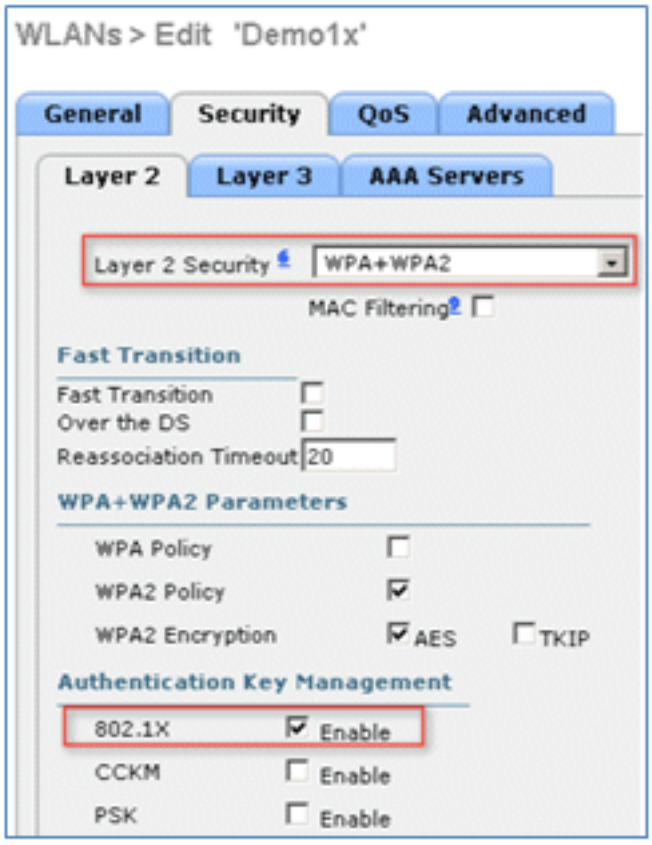
8. Cree un SSID de WLAN 802.1X denominado **Demo1x** (en este ejemplo) para escenarios de SSID único y dual.



9. Navegue hasta la pestaña **Seguridad** > pestaña **Capa 2** y establezca estos atributos:

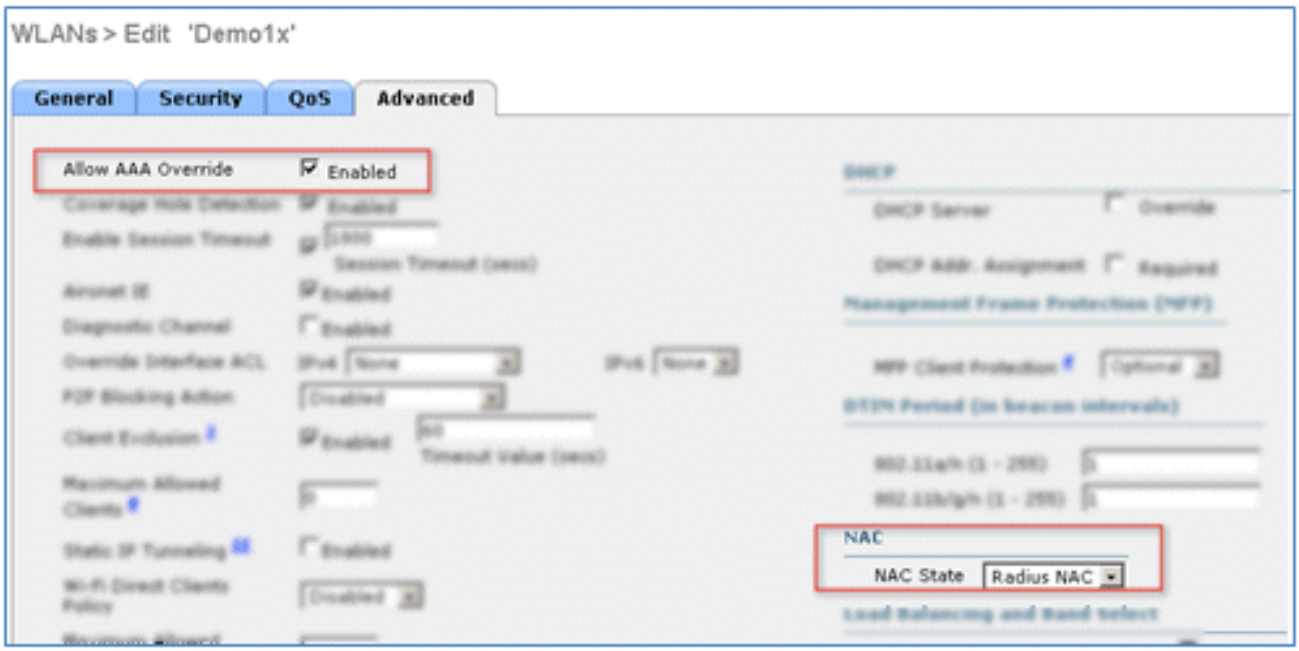
Seguridad de capa 2: **WPA+WPA2**Transición rápida: **Desactivada** (la casilla no está

activada)Administración de claves de autenticación: 802.IX: **Habilitar**

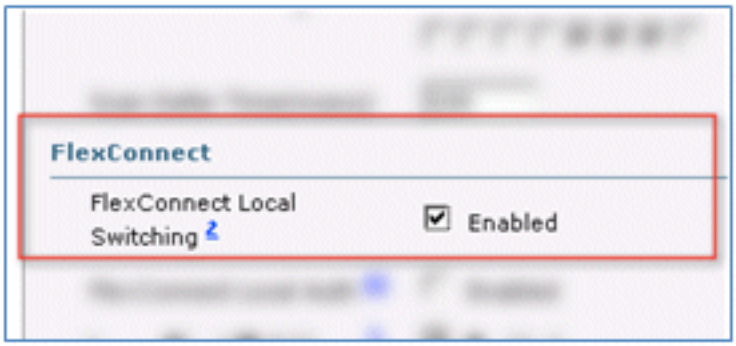


10. Vaya a la pestaña **Advanced** y establezca estos atributos:

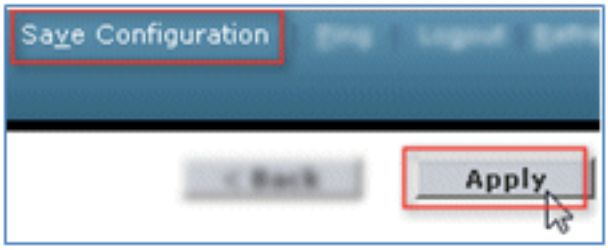
    Permitir Sustitución de AAA: **Activado**Estado de NAC: **Radius NAC**



11. Desplácese hacia abajo en la pestaña **Advanced** y establezca FlexConnect Local Switching en **Enabled**.



12. Haga clic en **Apply** y **Save Configuration**.



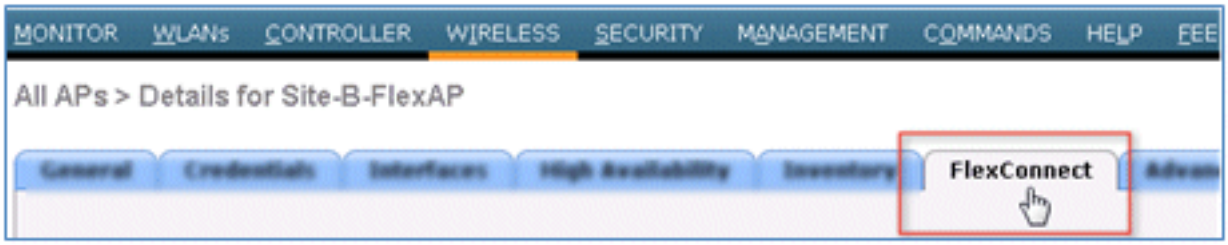
13. Confirme que ambas WLANs nuevas fueron creadas.

Configuración AP de FlexConnect

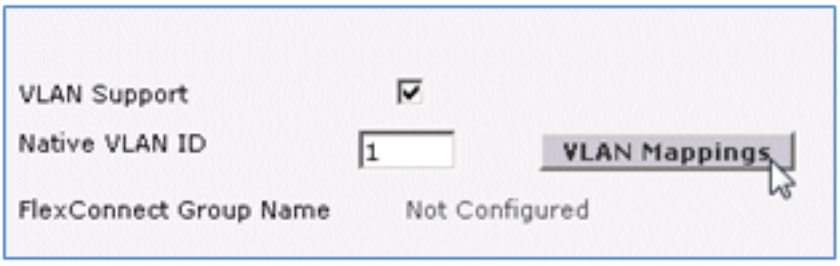
Complete estos pasos para configurar el AP de FlexConnect:

1. Navegue hasta **WLC > Wireless**, y haga clic en el AP FlexConnect de destino.

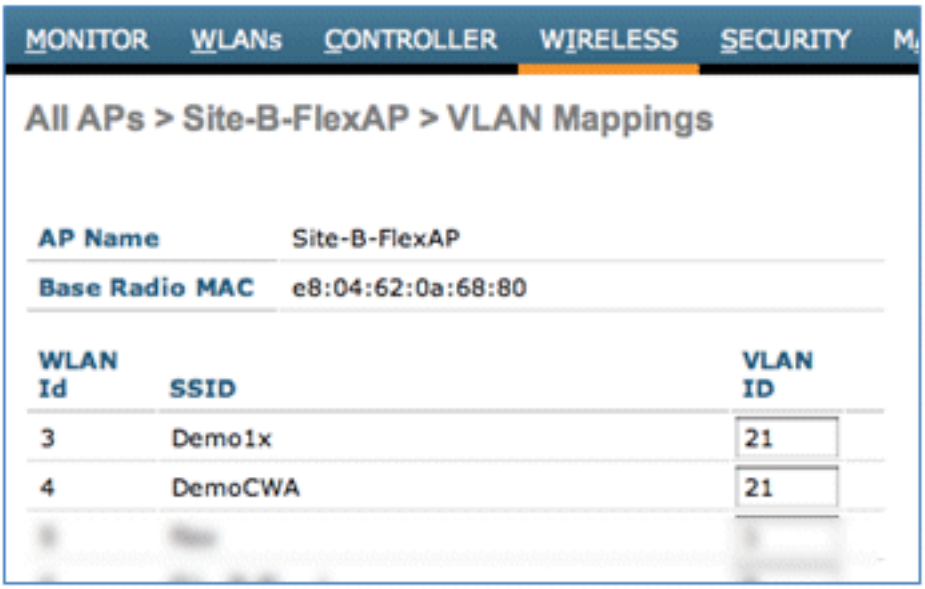
2. Haga clic en la pestaña **FlexConnect**.



3. Habilite el Soporte de VLAN (la casilla está marcada), establezca el ID de VLAN nativa y haga clic en **Asignaciones de VLAN**.



4. Establezca el ID de VLAN en **21** (en este ejemplo) para el SSID para la conmutación local.



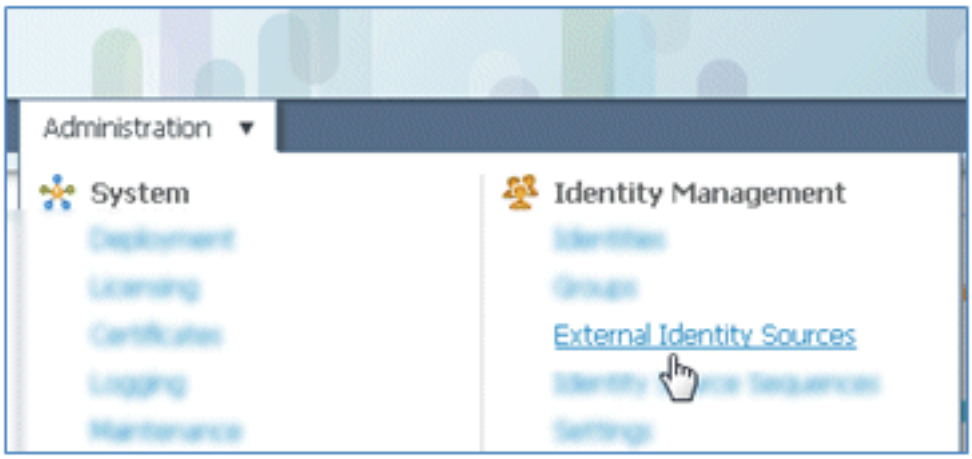
5. Haga clic en **Apply** y **Save Configuration**.

Configuración de ISE

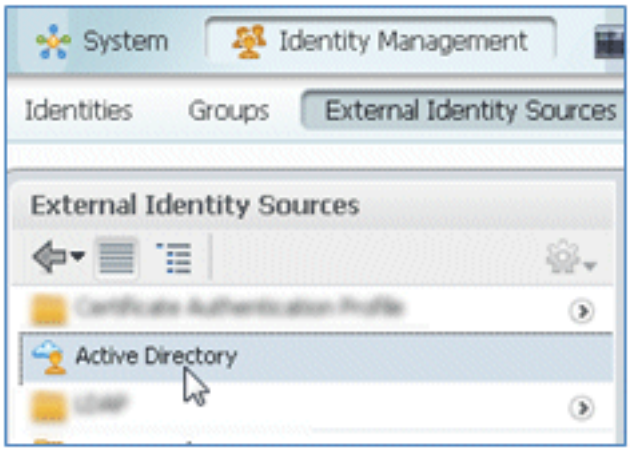
Complete estos pasos para configurar el ISE:

1. Inicie sesión en el servidor de ISE: <*https://ise*>.

2. Vaya a **Administration > Identity Management > External Identity Sources**.

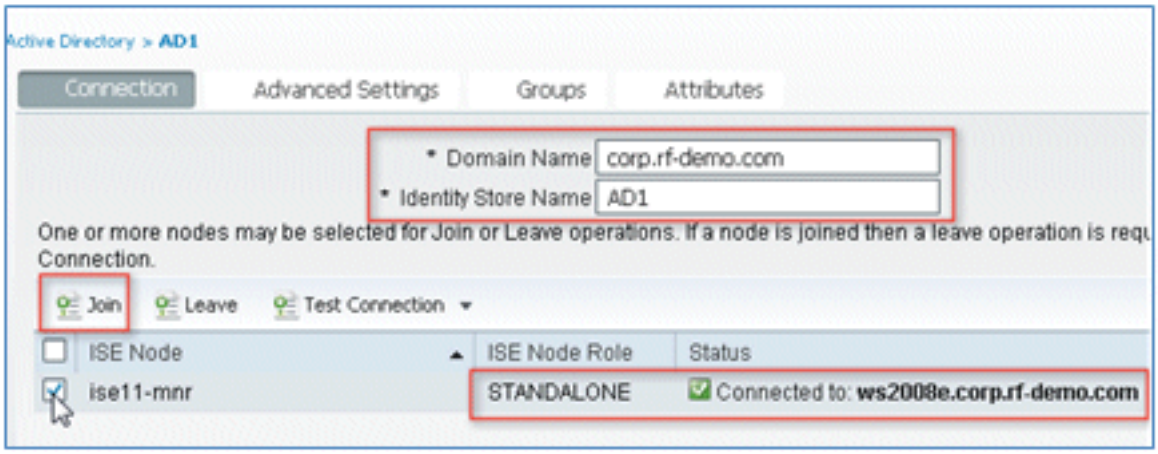


3. Haga clic en **Active Directory**.

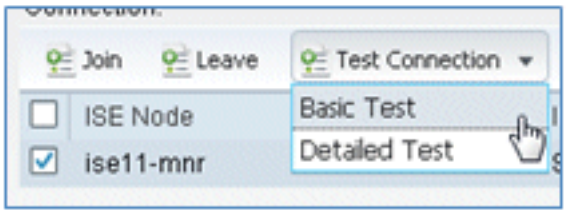


4. En la ficha Conexión:

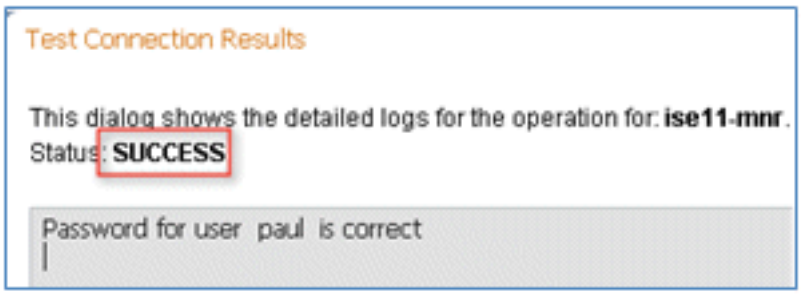
   Agregue el nombre de dominio **corp.rf-demo.com** (en este ejemplo) y cambie el valor predeterminado del nombre de almacén de identidad a **AD1**.Haga clic en **Save Configuration**.Haga clic en **Unirse** y proporcione el nombre de usuario y la contraseña de la cuenta de administrador de AD necesarios para unirse.El estado debe ser verde. Habilitar **Conectado a:** (la casilla está activada).



5. Realice una prueba de conexión básica al AD con un usuario de dominio actual.

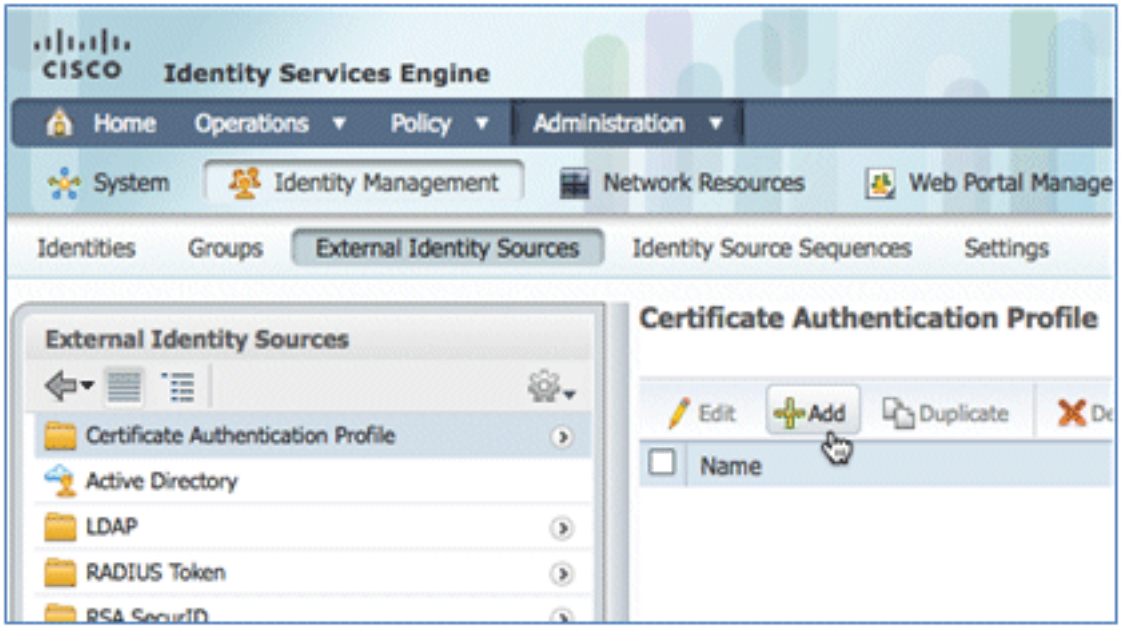


6. Si la conexión a AD se realiza correctamente, un cuadro de diálogo confirma que la contraseña es correcta.

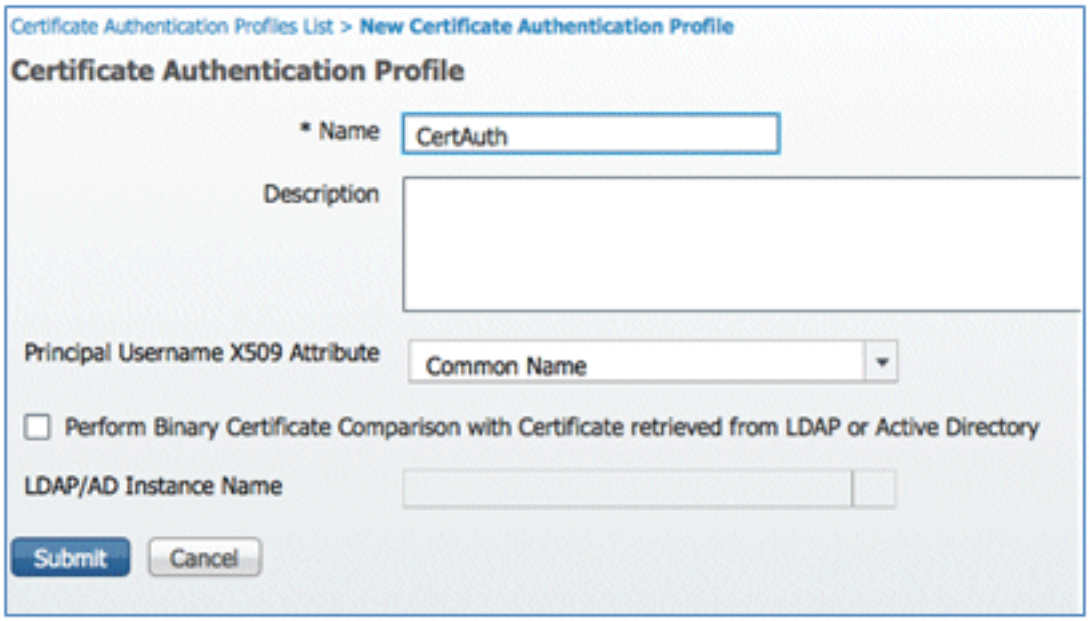


7. Navegue hasta **Administración > Administración de identidades > Orígenes de identidades externas**:

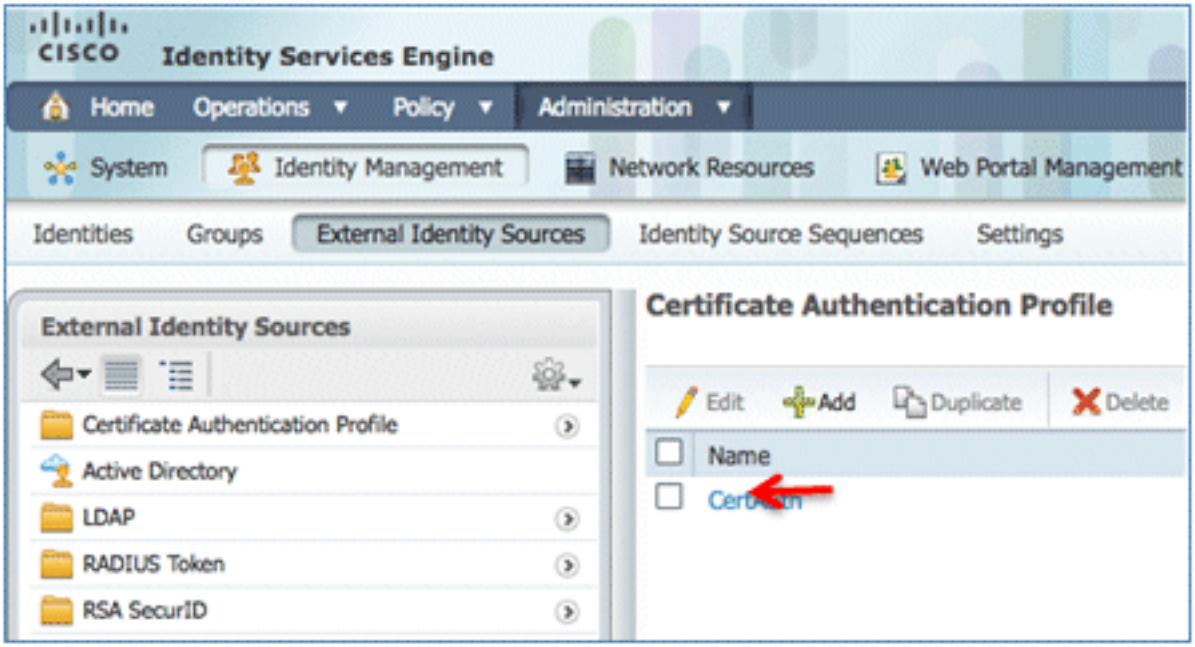
   Haga clic en **Perfil de autenticación de certificado**.Haga clic en **Agregar** para obtener un nuevo perfil de autenticación de certificados (CAP).



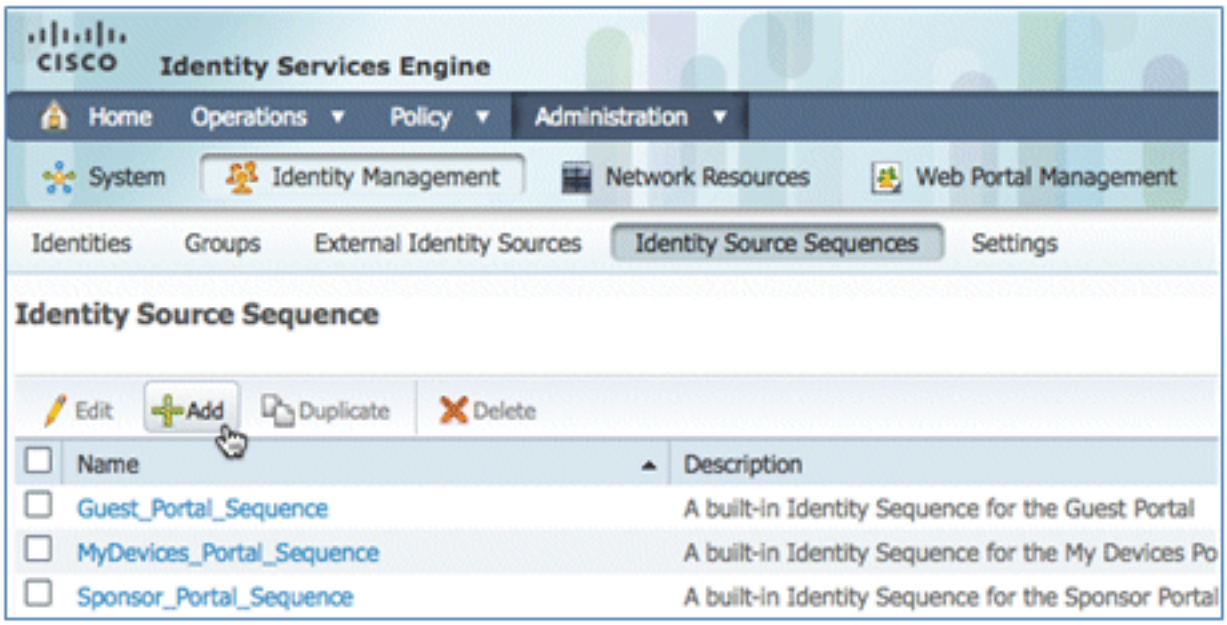
8. Ingrese un nombre de **CertAuth** (en este ejemplo) para el CAP; para el Atributo Principal Username X509, seleccione **Nombre Común**; luego, haga clic en **Enviar**.



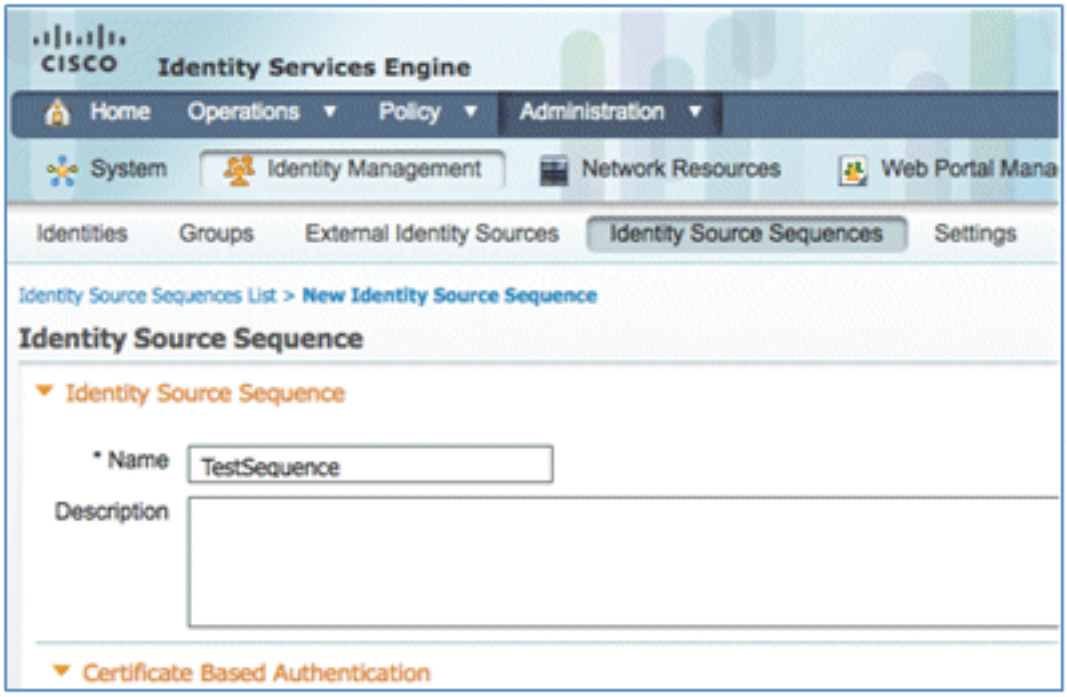
9. Confirme que se ha agregado el nuevo CAP.



10. Navegue hasta **Administration > Identity Management > Identity Source Sequences**, y haga clic en **Add** .

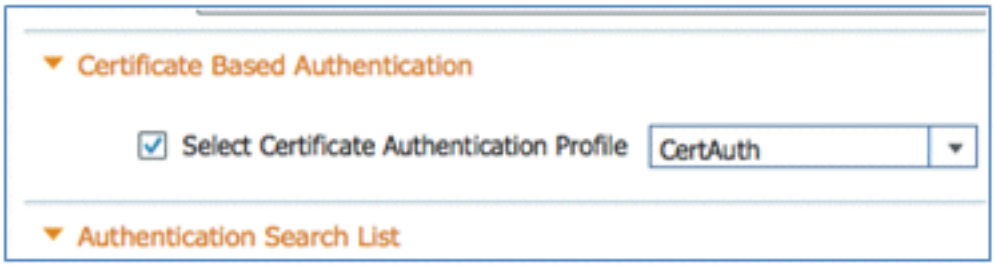


11. Asigne a la secuencia el nombre **TestSequence** (en este ejemplo).



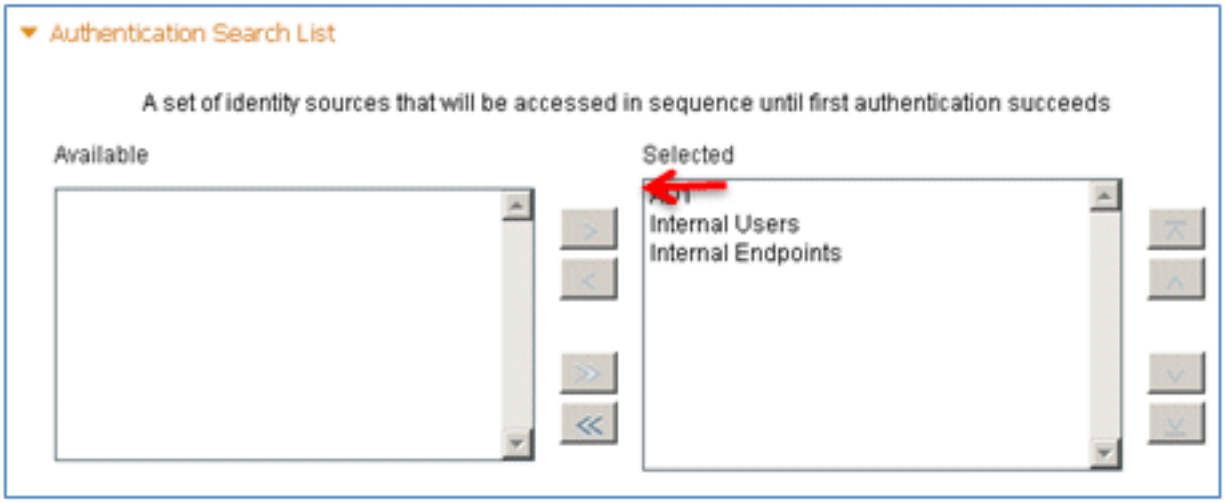
12. Desplácese hacia abajo hasta **Autenticación basada en certificados**:

    Habilitar **Seleccionar perfil de autenticación de certificado** (casilla activada).Seleccione **CertAuth** (u otro perfil CAP creado anteriormente).

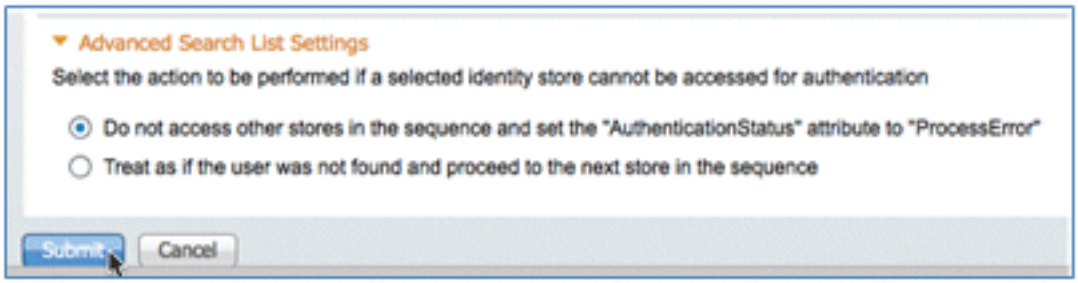


13. Desplácese hacia abajo hasta **Authentication Search List**:

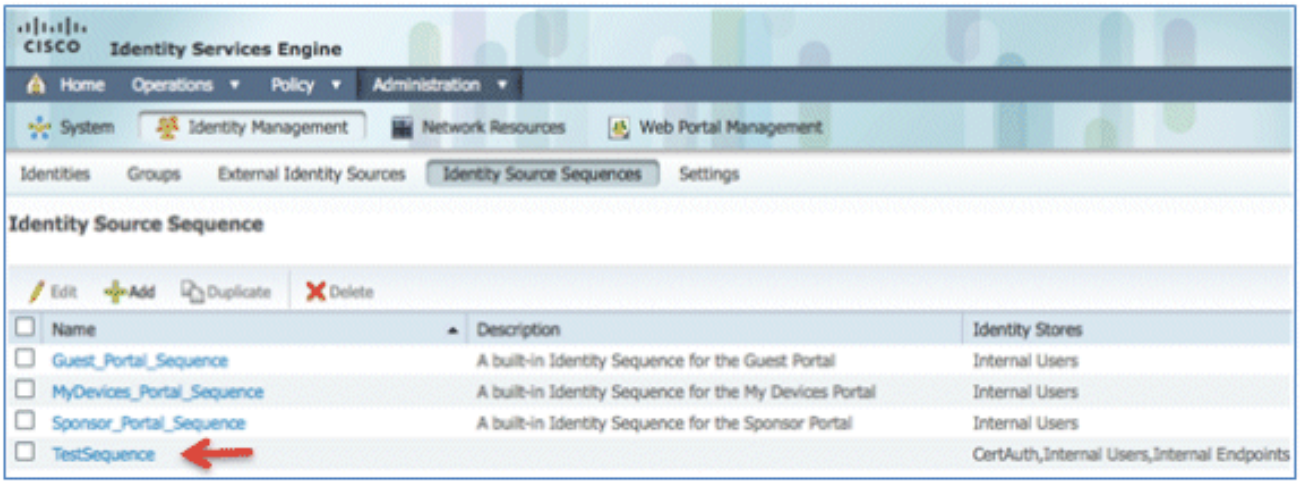
Mover AD1 de Disponible a Seleccionado.Haga clic en el botón arriba para mover AD1 a la prioridad superior.



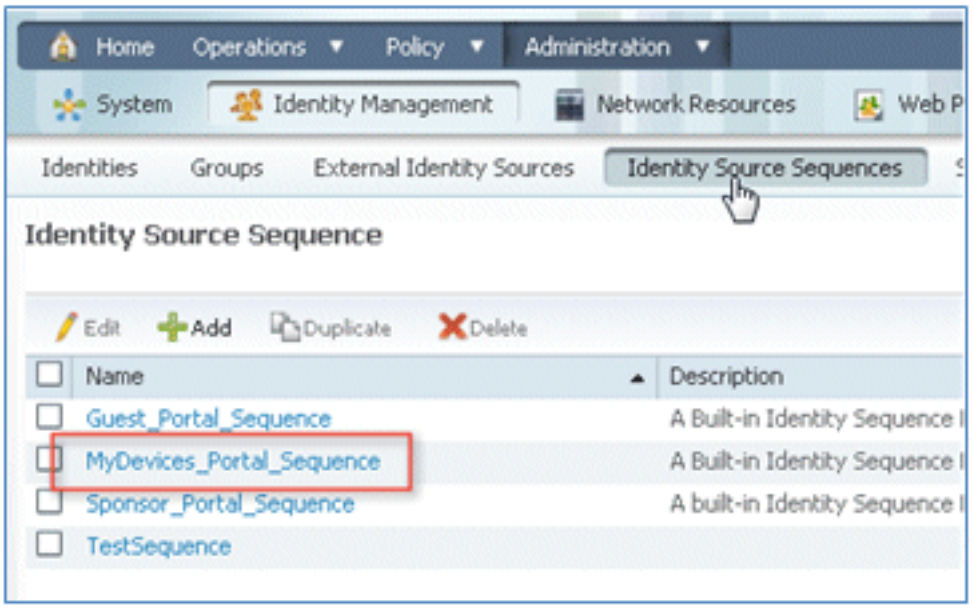
14. Haga clic en **Enviar** para guardar.



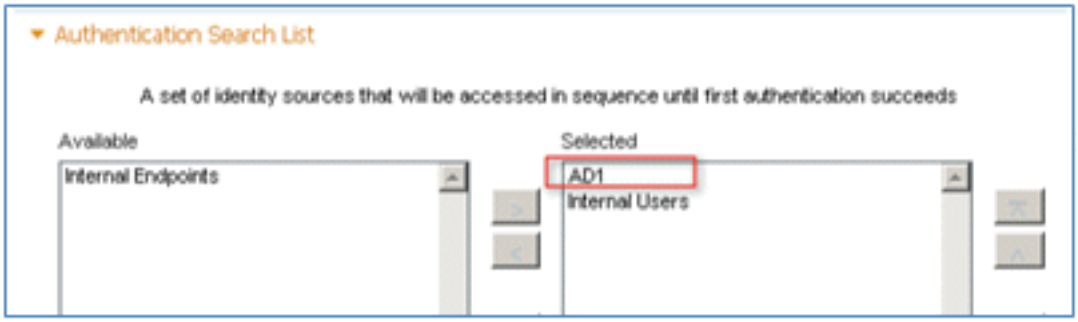
15. Confirme que se ha agregado la nueva secuencia de origen de identidad.



16. Utilice AD para autenticar el portal Mis dispositivos. Vaya a ISE > **Administration** > **Identity Management** > **Identity Source Sequence** y edite MyDevices_Portal_Sequence.



17. Agregue **AD1** a la lista Selected y haga clic en el botón arriba para mover AD1 a la prioridad superior.

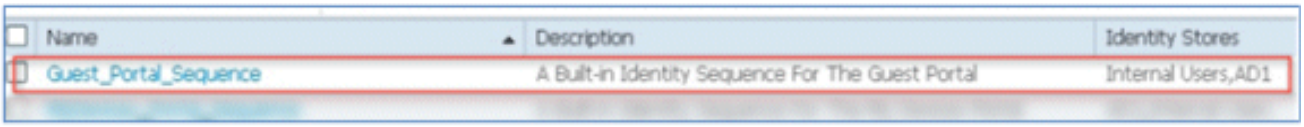


18. Click **Save**.

19. Confirme que la secuencia del almacén de identidades para MyDevices_Portal_Sequence contiene **AD1**.

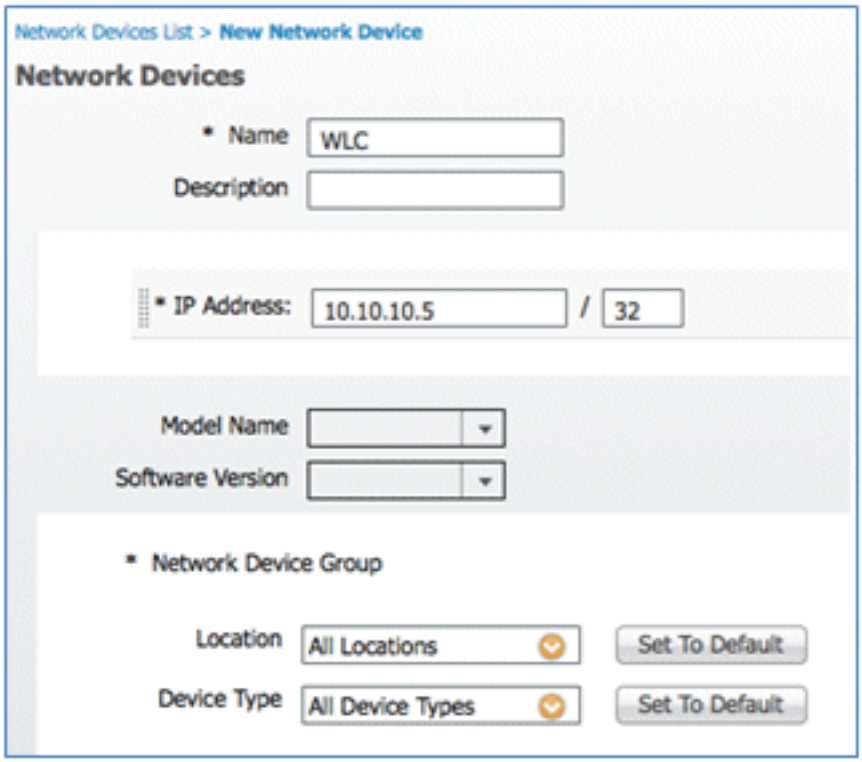
20. Repita los pasos 16-19 para agregar AD1 para Guest_Portal_Sequence y haga clic en **Save**.

21. Confirme que Guest_Portal_Sequence contiene **AD1**.

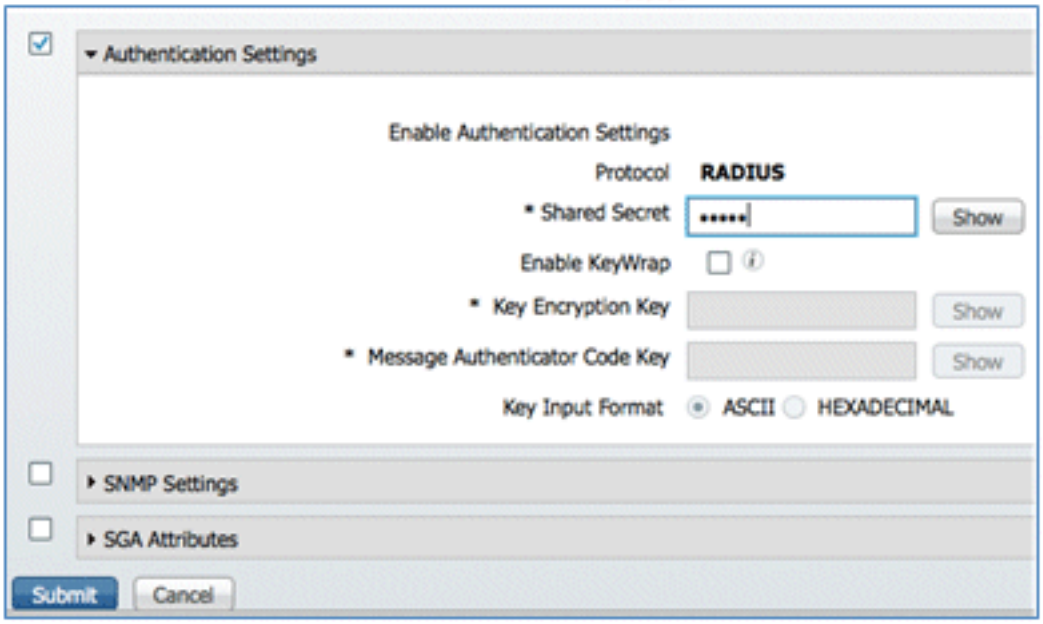


22. Para agregar el WLC al dispositivo de acceso a la red (WLC), navegue hasta **Administración > Recursos de red > Dispositivos de red**, y haga clic **Agregar**.

23. Agregue el nombre del WLC, la dirección IP, la máscara de subred, etc.

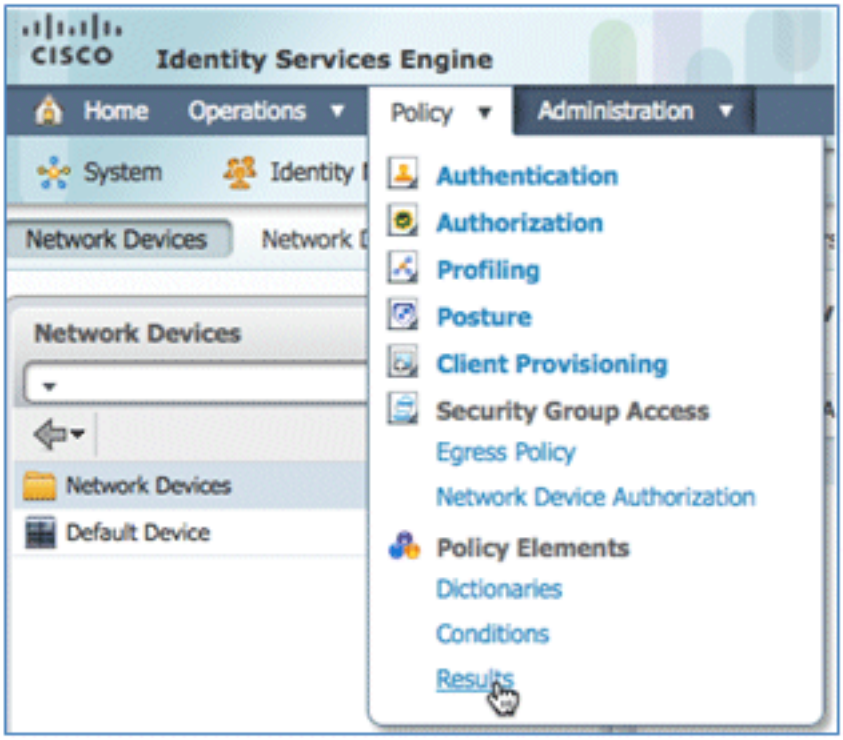


24. Desplácese hasta Configuración de autenticación e introduzca la clave secreta compartida. Debe coincidir con el secreto compartido del WLC RADIUS.

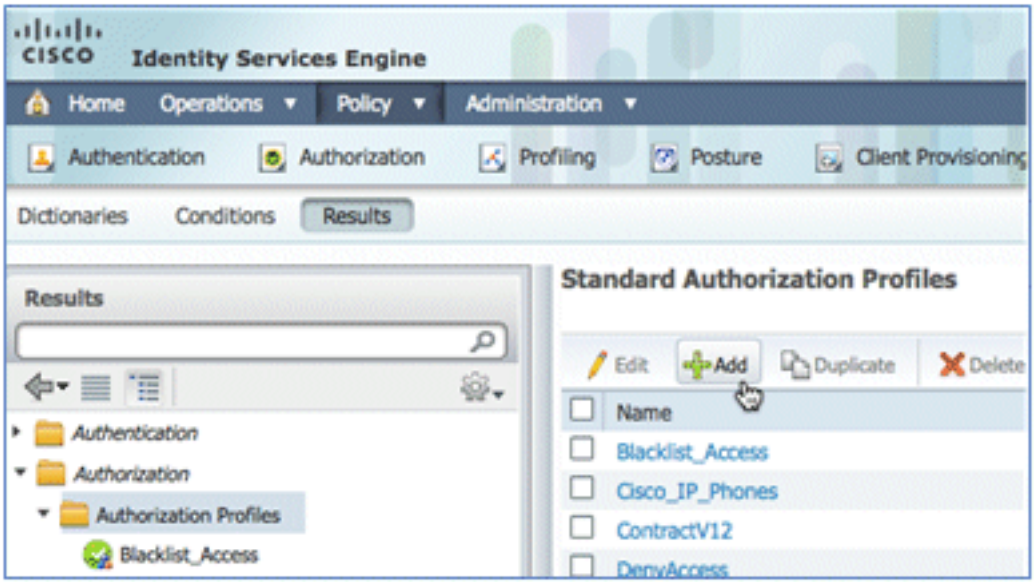


25. Haga clic en Submit (Enviar).

26. Vaya a **ISE > Policy > Policy Elements > Results**.

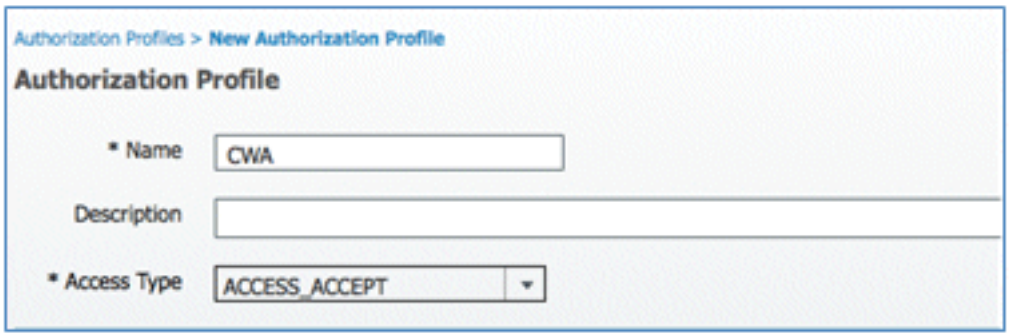


27. Expanda **Resultados** y **Autorización**, haga clic en **Perfiles de Autorización**, y haga clic en **Agregar** para obtener un nuevo perfil.



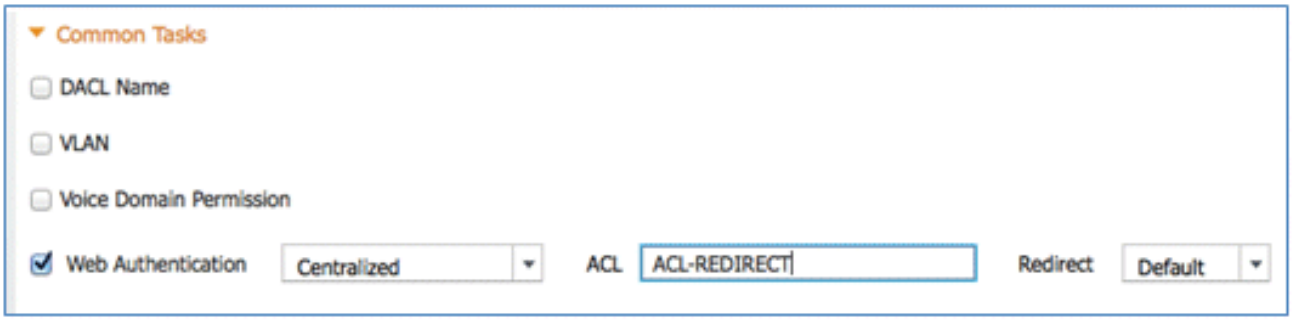
28. Proporcione a este perfil estos valores:

    Nombre: **CWA**

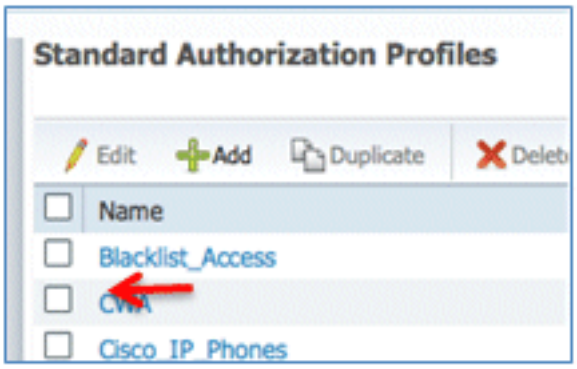


Habilitar autenticación Web (casilla activada):

Autenticación web: **centralizada**ACL: **ACL-REDIRECT** (Debe coincidir con el nombre de ACL de autenticación previa del WLC.)Redirigir: **Predeterminado**



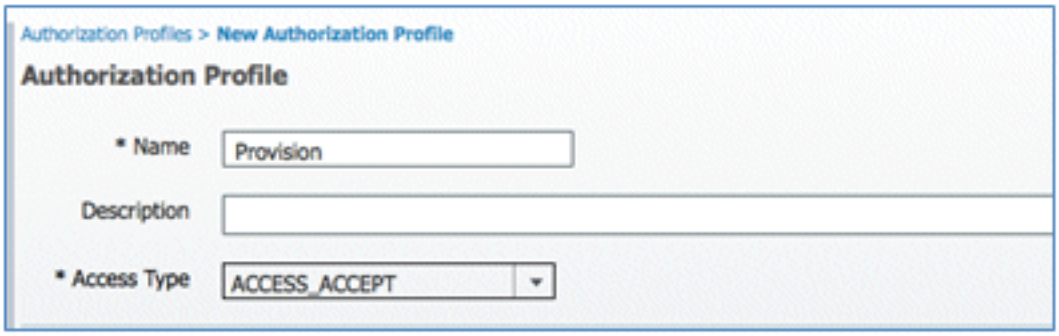
29. Haga clic en **Submit** y confirme que se ha agregado el perfil de autorización de CWA.



30. Haga clic en **Agregar** para crear un nuevo perfil de autorización.

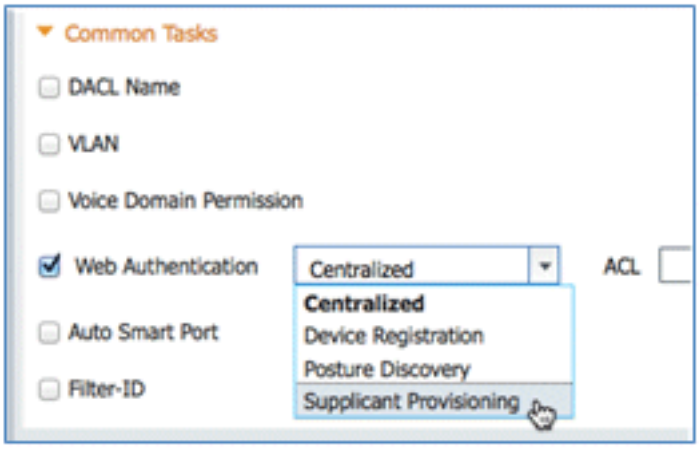
31. Proporcione a este perfil estos valores:

    Nombre: **Provisión**

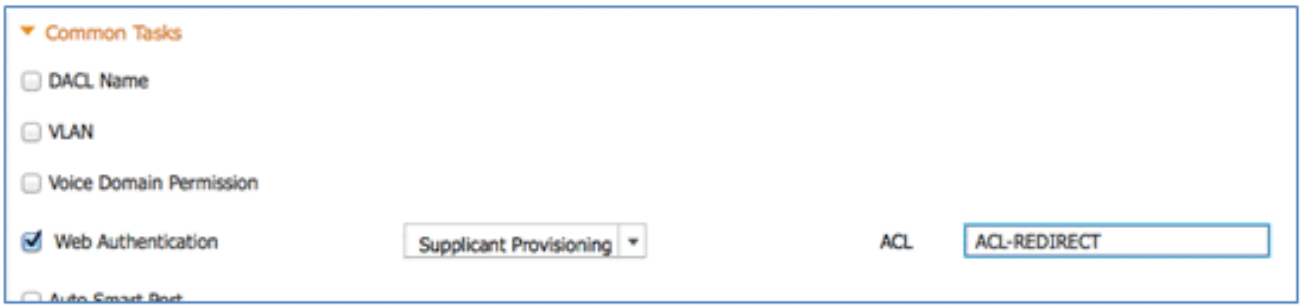


    Habilitar autenticación Web (casilla activada):

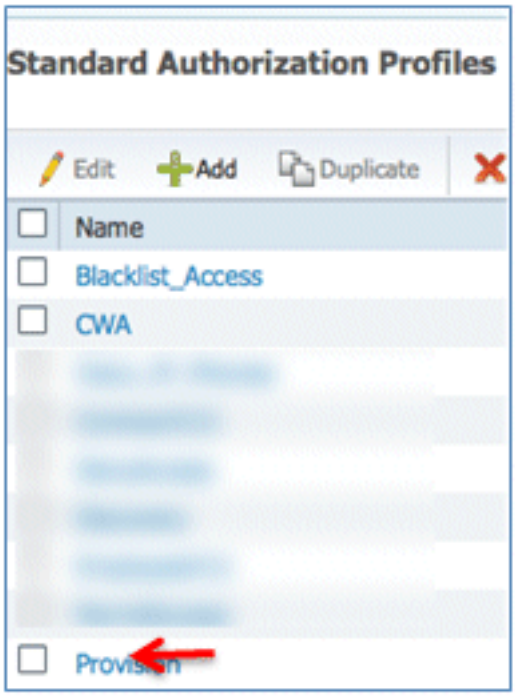
    Valor de autenticación web: **aprovisionamiento de suplicante**



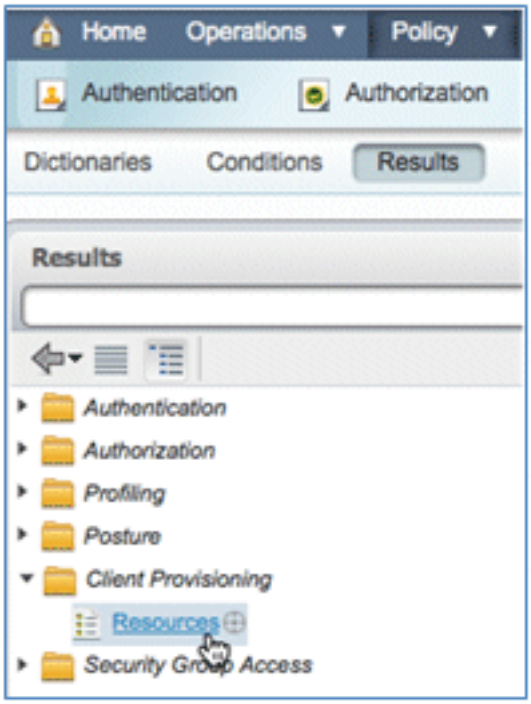
    ACL: **ACL-REDIRECT** (Debe coincidir con el nombre de ACL de autenticación previa del WLC.)



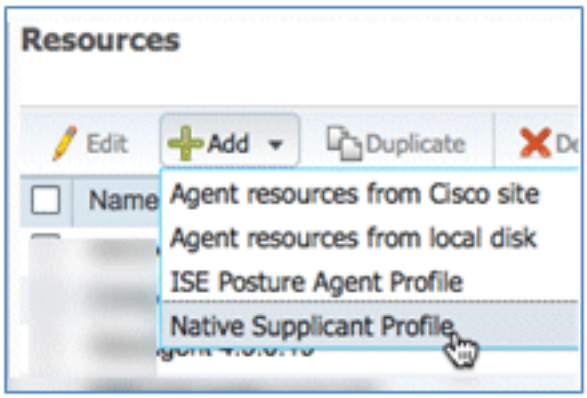
32. Haga clic en **Submit** y confirme que se ha agregado el perfil de autorización de provisiones.



33. Desplácese hacia abajo en Resultados, expanda **Aprovisionamiento del cliente** y haga clic en **Recursos**.



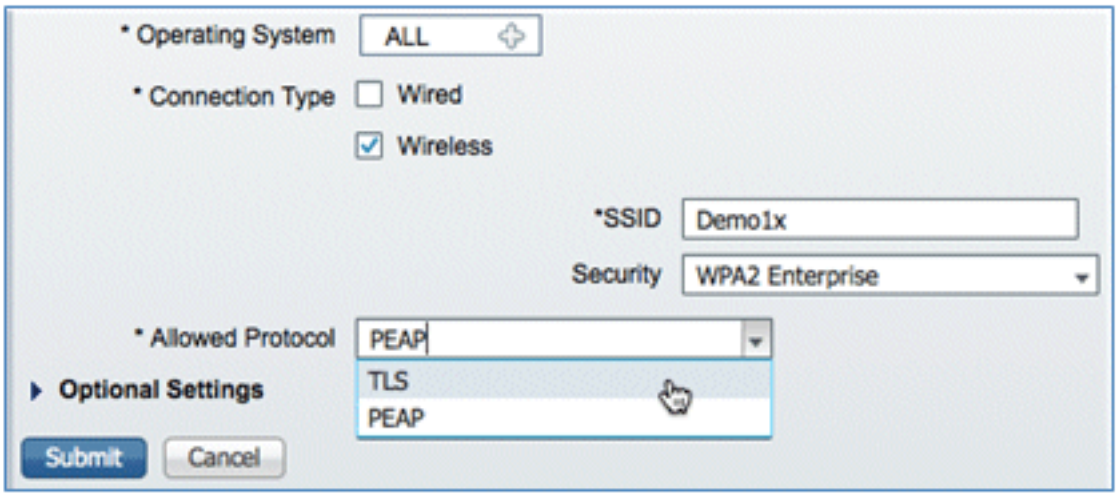
34. Seleccione **Native Supplicant Profile**.



35. Dé al perfil el nombre de **WirelessSP** (en este ejemplo).

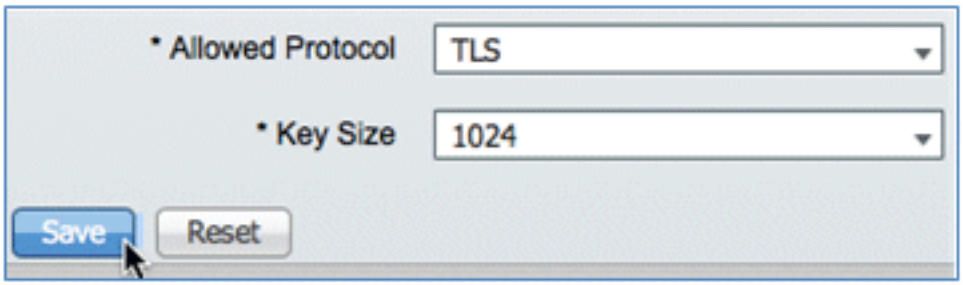
36. Introduzca estos valores:

    Tipo de conexión: **inalámbrica**SSID: **Demo1x** (este valor proviene de la configuración WLAN WLC 802.1x)Protocolo permitido: **TLS**Tamaño de clave: **1024**

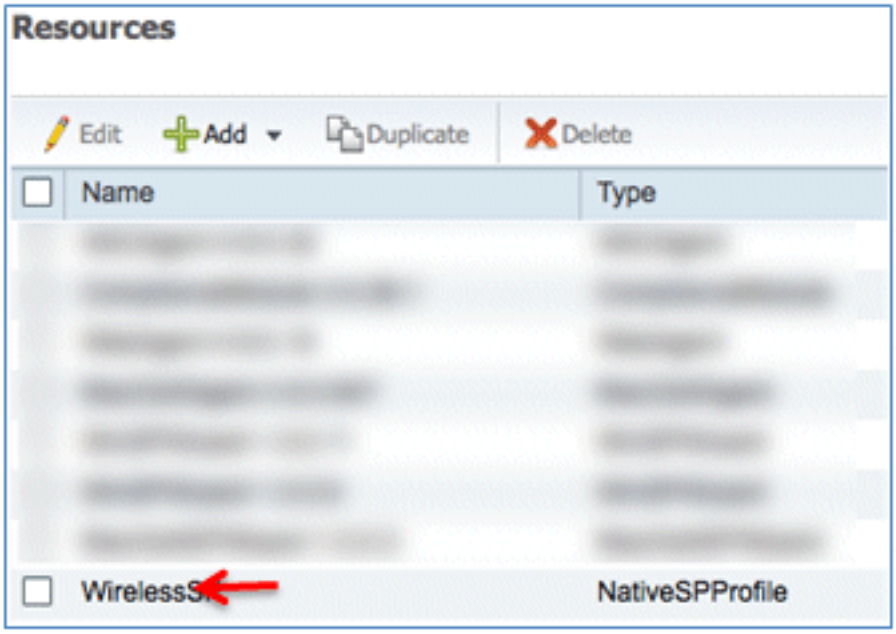


37. Haga clic en Submit (Enviar).

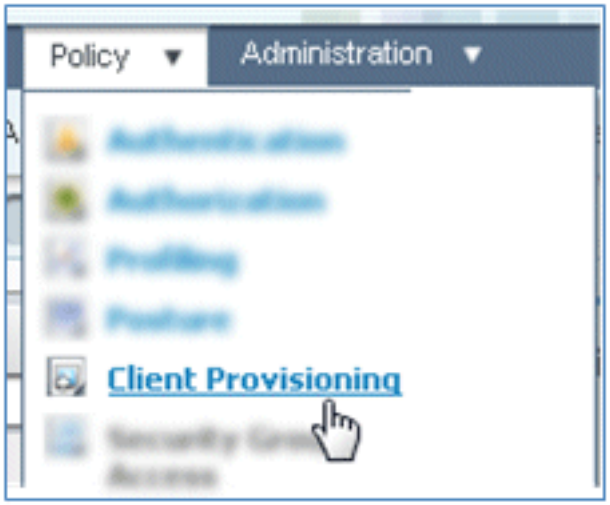
38. Click **Save**.



39. Confirme que se ha agregado el nuevo perfil.

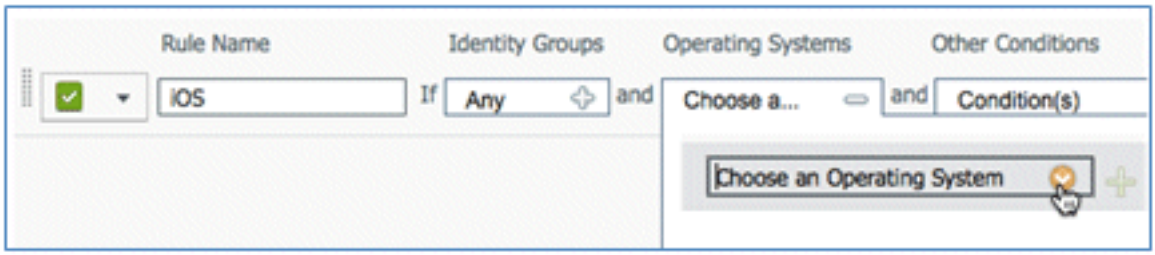


40. Vaya a **Policy > Client Provisioning**.

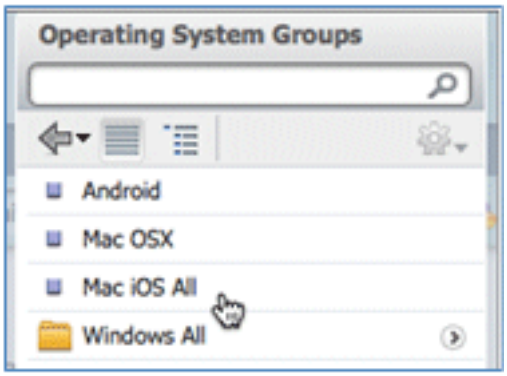


41. Introduzca estos valores para la regla de aprovisionamiento de dispositivos iOS:

    Nombre de regla: **iOS**Grupos de identidad: **Cualquiera**

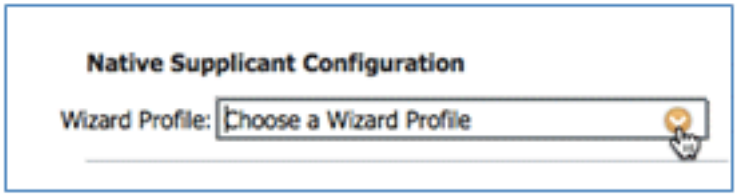


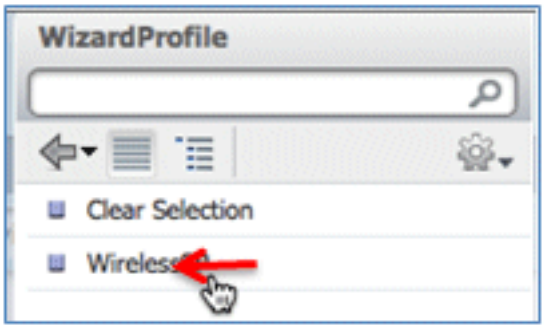
Sistemas operativos: **Mac iOS Todo**



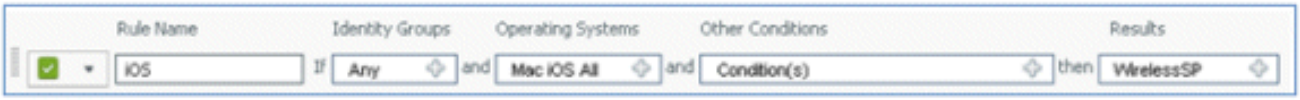
Resultados: **WirelessSP** (este es el perfil de suplicante nativo creado anteriormente)

Vaya a **Results** > **Wizard Profile** (Lista desplegable) > **WirelessSP**.

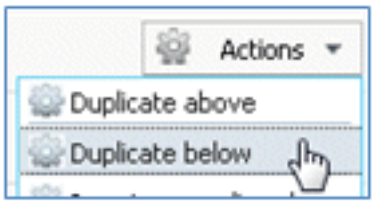




42. Confirme que se ha agregado el perfil de abastecimiento de iOS.

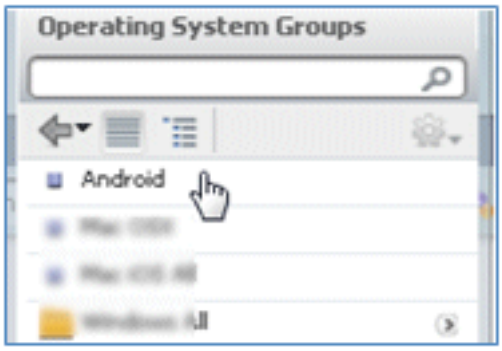


43. En el lado derecho de la primera regla, localice la lista desplegable Acciones y seleccione **Duplicar a continuación** (o arriba).



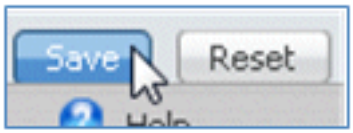
44. Cambie el nombre de la nueva regla a **Android**.

45. Cambie los sistemas operativos a **Android**.

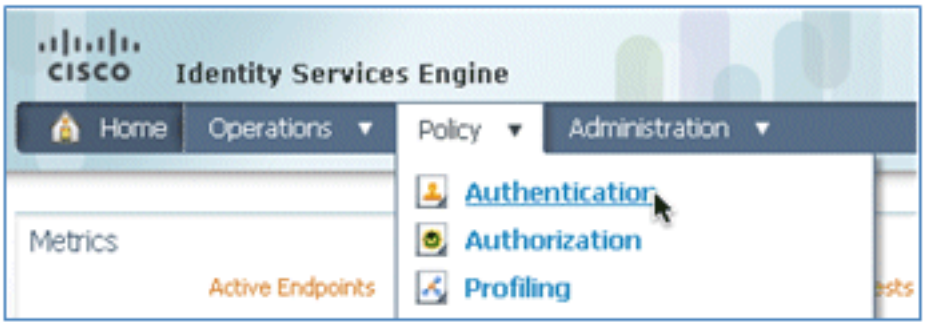


46. No modifique otros valores.

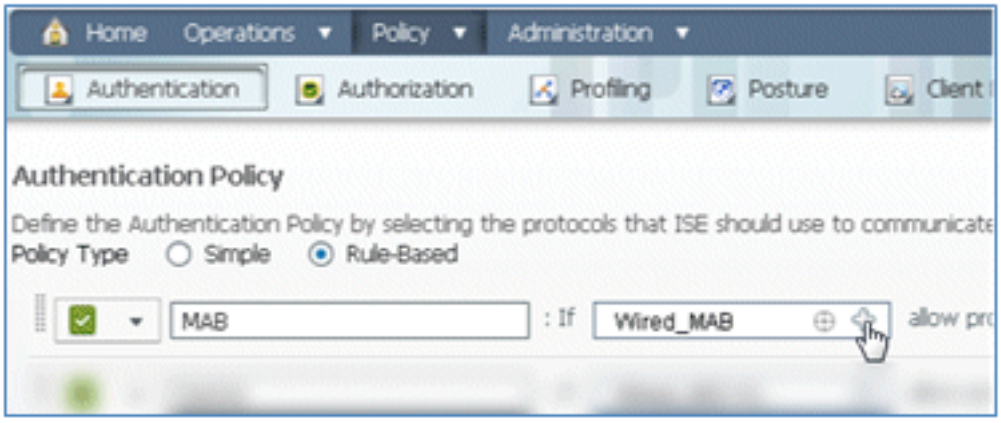
47. Haga clic en **Save** (pantalla inferior izquierda).



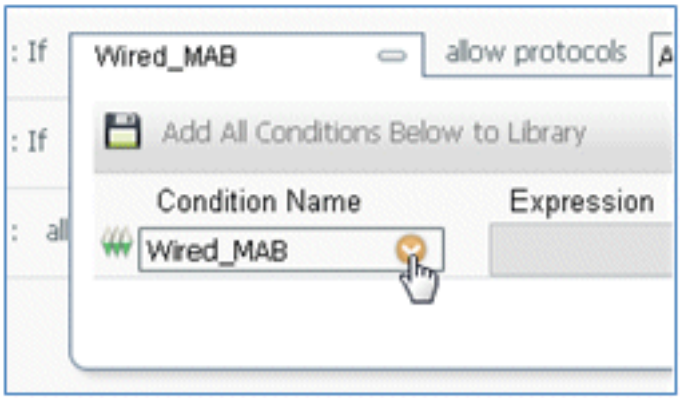
48. Vaya a **ISE > Policy > Authentication**.



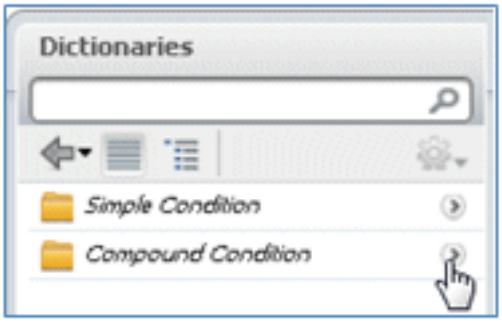
49. Modifique la condición para incluir Wireless_MAB y expanda **Wired_MAB**.



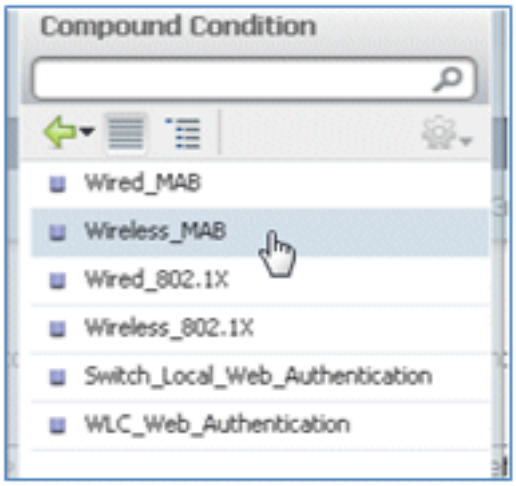
50. Haga clic en la lista desplegable **Nombre de condición**.



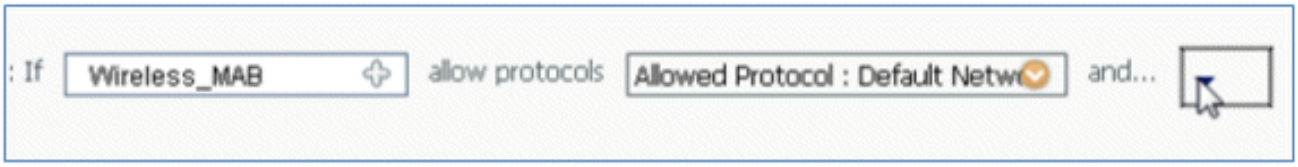
51. Seleccione **Diccionarios > Condición compuesta**.



52. Seleccione **Wireless_MAB**.

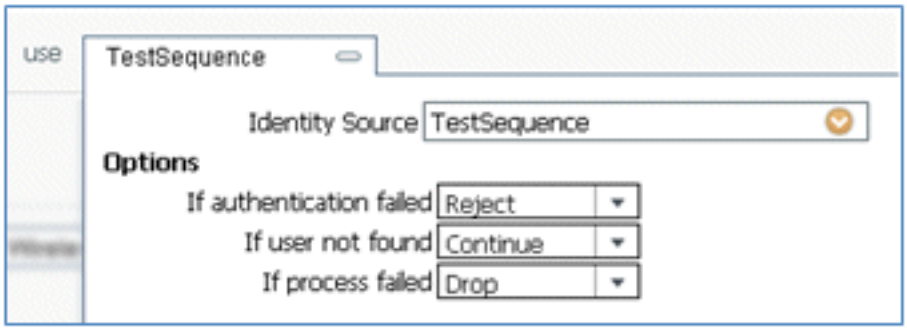


53. A la derecha de la regla, seleccione la flecha para expandir.

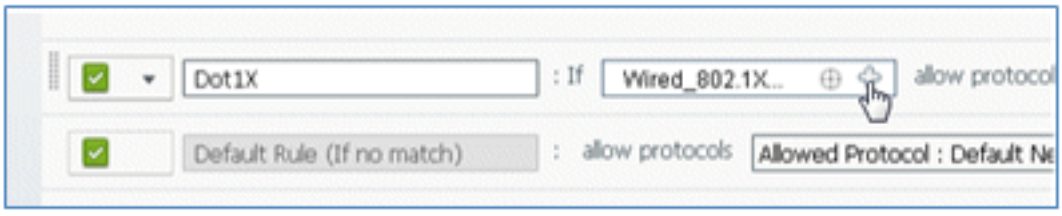


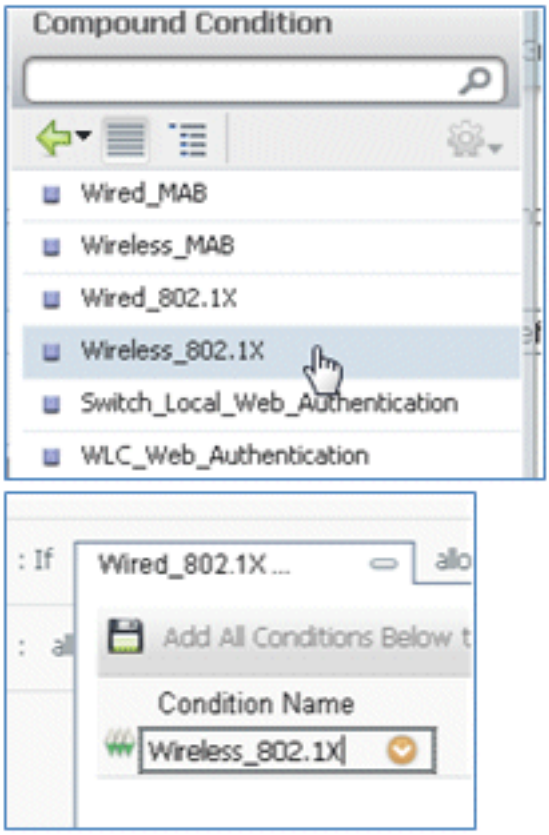
54. Seleccione estos valores en la lista desplegable:

    Origen de identidad: **TestSequence** (este es el valor creado anteriormente)Si falla la autenticación: **Rechazar**Si no se encuentra el usuario: **Continuar**Si el proceso ha fallado: **Eliminar**



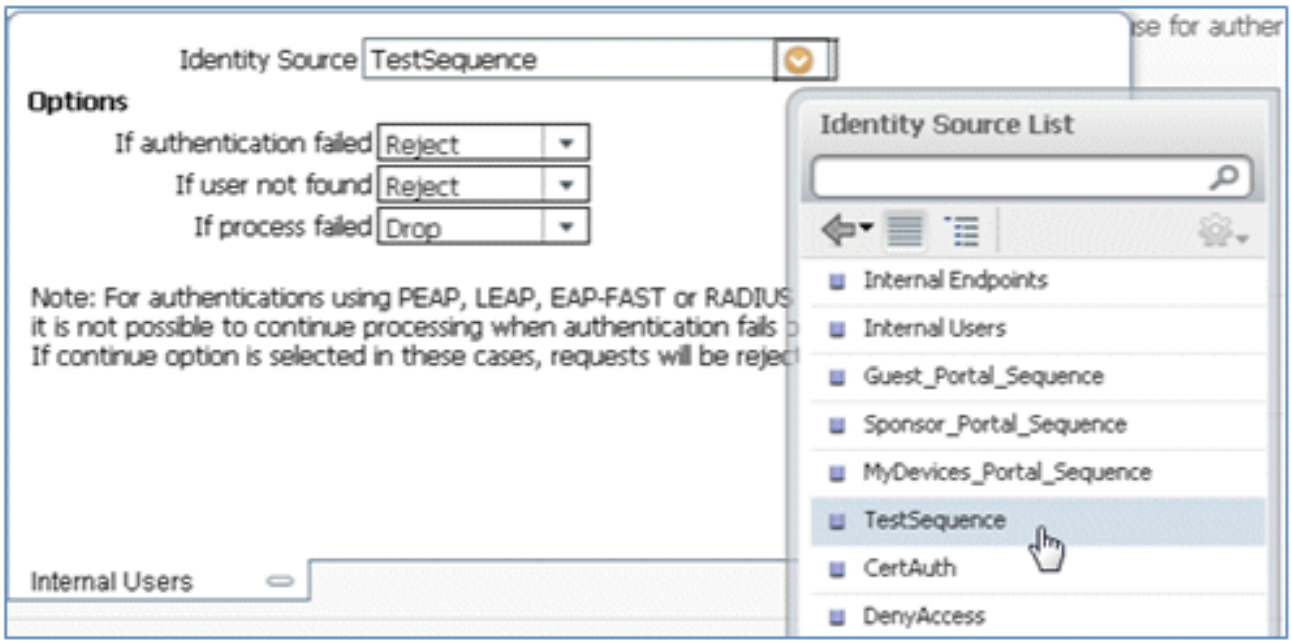
55. Vaya a la regla **Dot1X** y cambie estos valores:





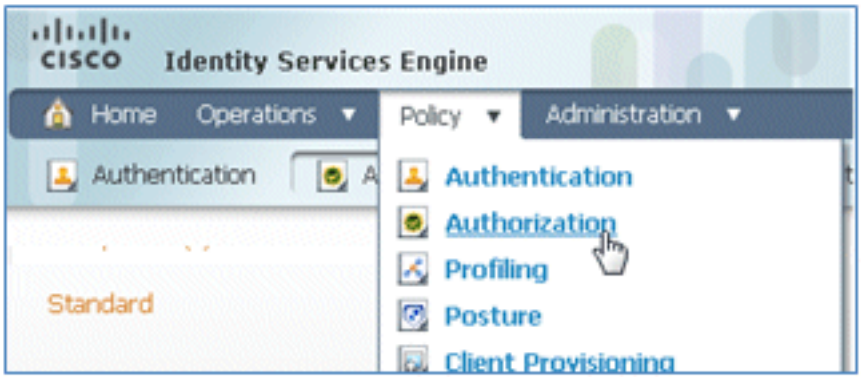
Condición: **Wireless_802.1X**

Origen de identidad: **TestSequence**

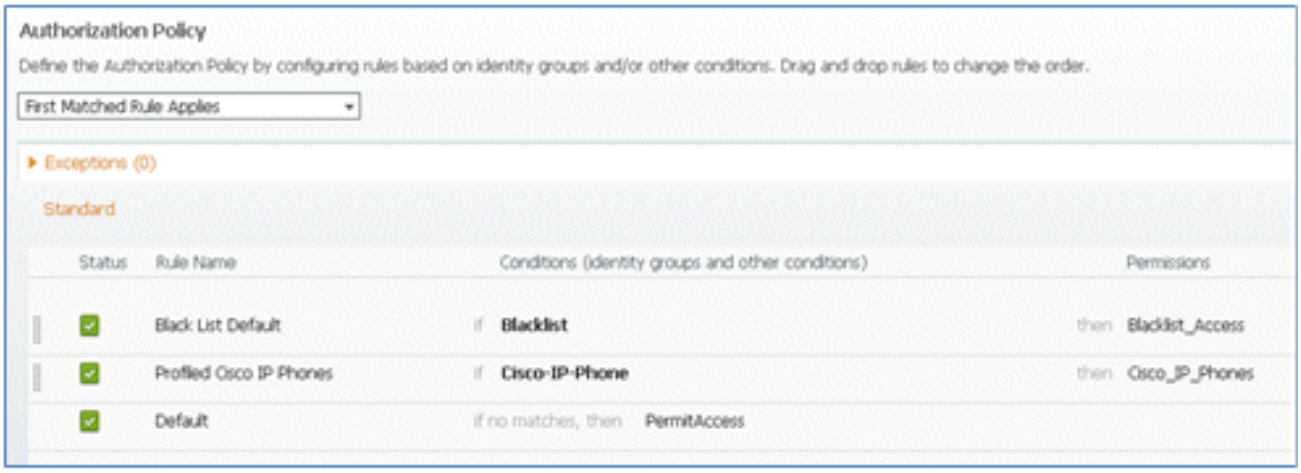


56. Click **Save**.

57. Vaya a **ISE > Policy > Authorization**.



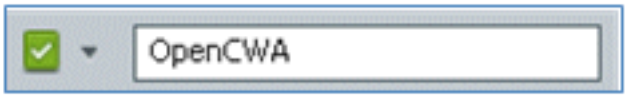
58. Las reglas predeterminadas (como Lista negra predeterminada, Perfil y Predeterminada) ya están configuradas desde la instalación; las dos primeras se pueden omitir; la regla predeterminada se editará más adelante.



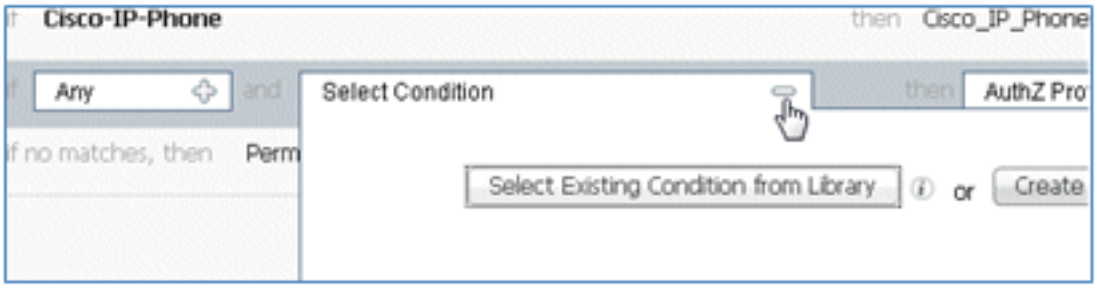
59. A la derecha de la segunda regla (Teléfonos IP de Cisco con perfil), haga clic en la flecha hacia abajo junto a Editar y seleccione **Insertar nueva regla debajo**.

Se agrega un nuevo nº de regla estándar.

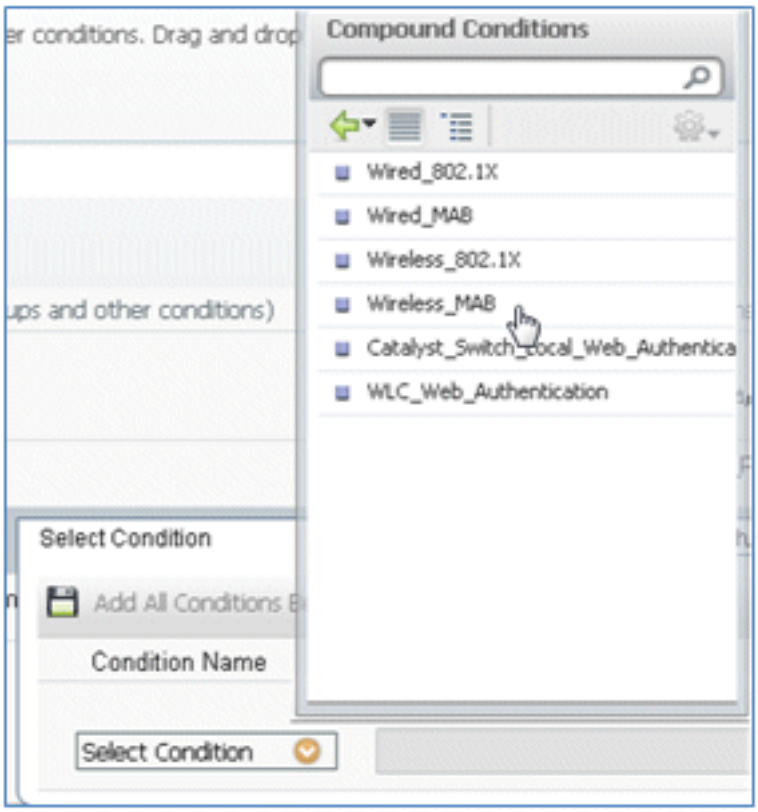
60. Cambie el nombre de la regla de nº de regla estándar a **OpenCWA**. Esta regla inicia el proceso de registro en la WLAN abierta (SSID dual) para los usuarios que llegan a la red de invitado para tener dispositivos aprovisionados.



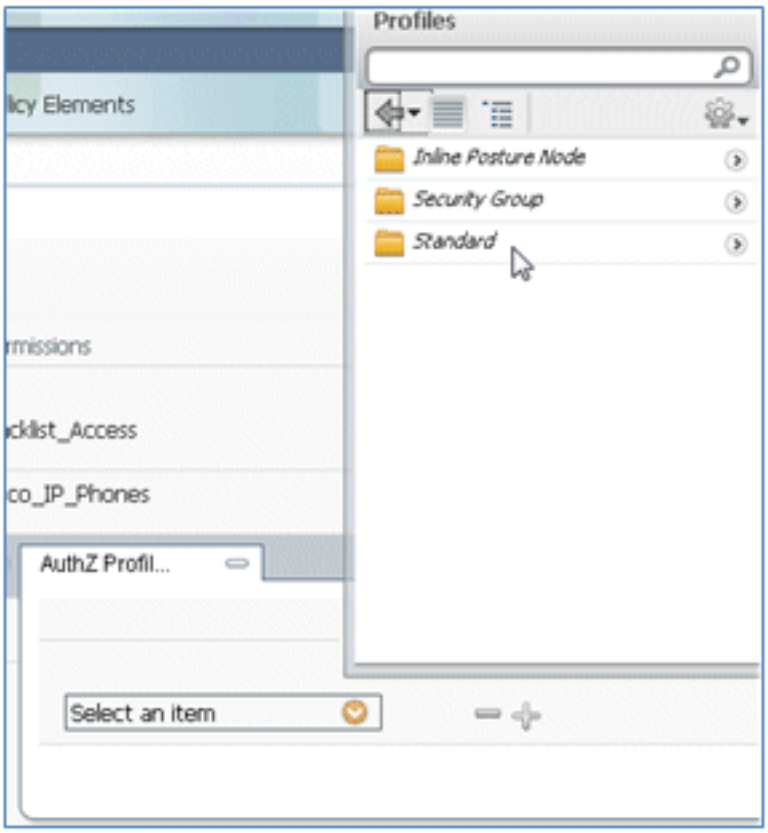
61. Haga clic en el signo más (**+**) de Condición(s) y haga clic en **Seleccionar condición existente de la biblioteca**.



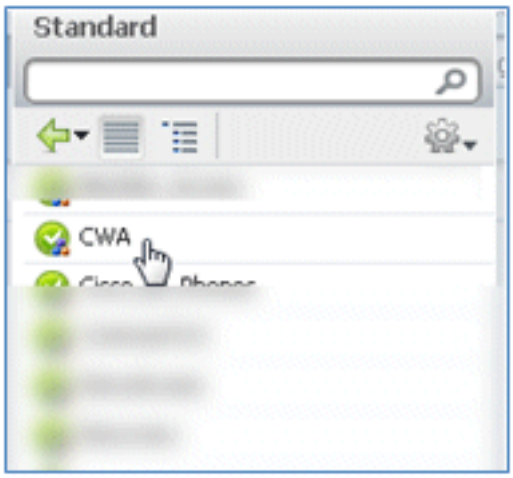
62. Seleccione **Condiciones compuestas** > **Wireless_MAB**.



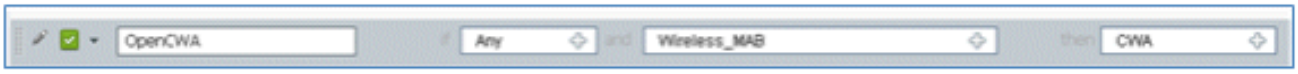
63. En el perfil AuthZ, haga clic en el signo más (**+**) y seleccione **Standard**.



64. Seleccione el **CWA** estándar (este es el perfil de autorización creado anteriormente).



65. Confirme que la regla se ha agregado con las condiciones y la autorización correctas.

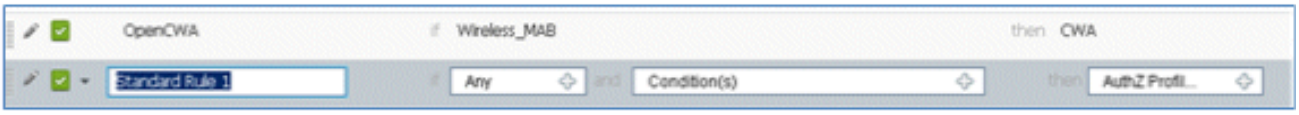


66. Haga clic en **Finalizado** (en el lado derecho de la regla).

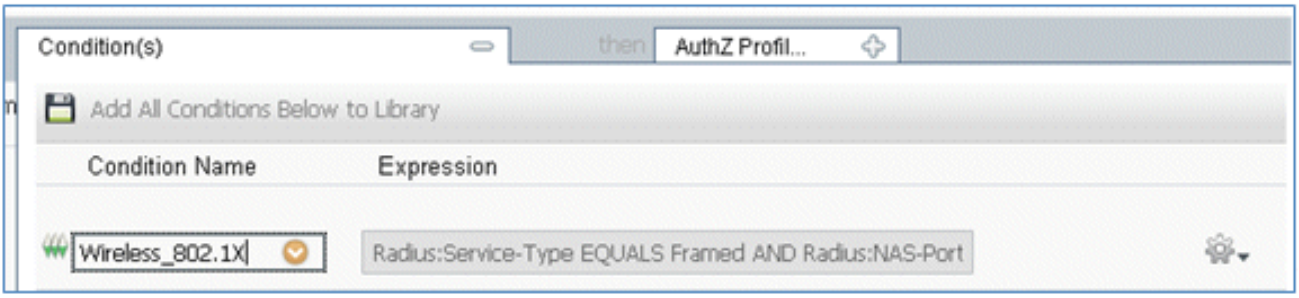
67. A la derecha de la misma regla, haga clic en la flecha hacia abajo junto a Editar y

seleccione **Insertar nueva regla debajo**.

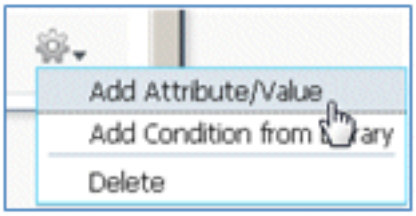
68. Cambie el nombre de la regla de n.º de regla estándar a **PEAPrule** (en este ejemplo). Esta regla es para PEAP (también se utiliza para el escenario SSID único) para comprobar que la autenticación de 802.1X sin seguridad de la capa de transporte (TLS) y el aprovisionamiento del suplicante de red se inicia con el perfil de autorización de provisión creado anteriormente.



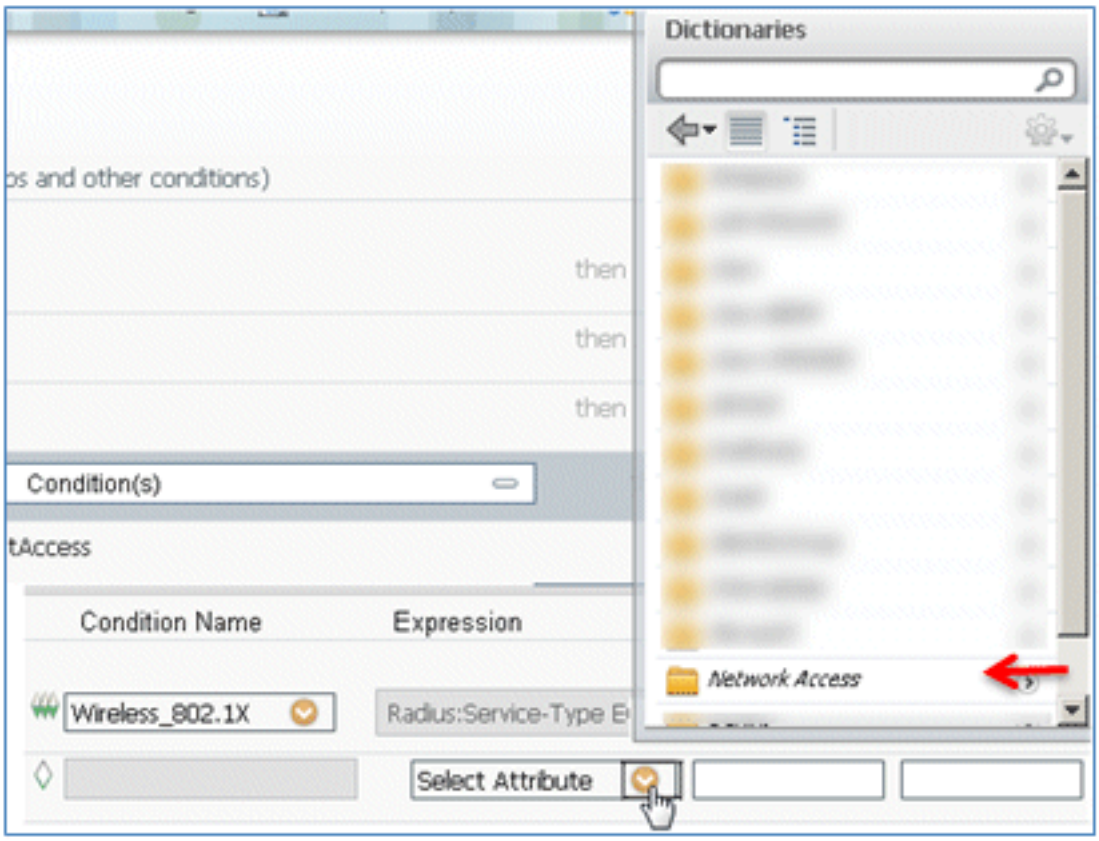
69. Cambie la condición a **Wireless_802.1X**.



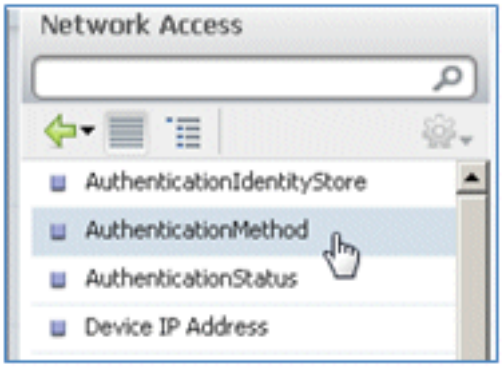
70. Haga clic en el icono de engranaje en el lado derecho de la condición y seleccione **Agregar atributo/valor**. Se trata de una condición 'and', no 'or'.



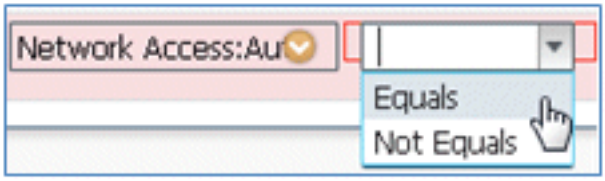
71. Localice y seleccione **Network Access**.



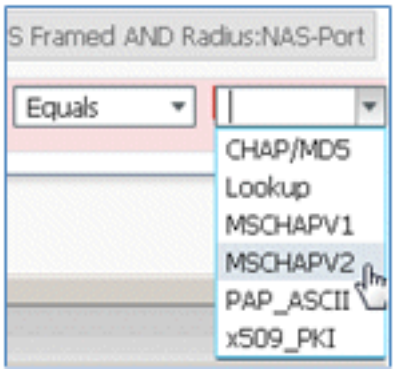
72. Seleccione **AuthenticationMethod** e ingrese estos valores:



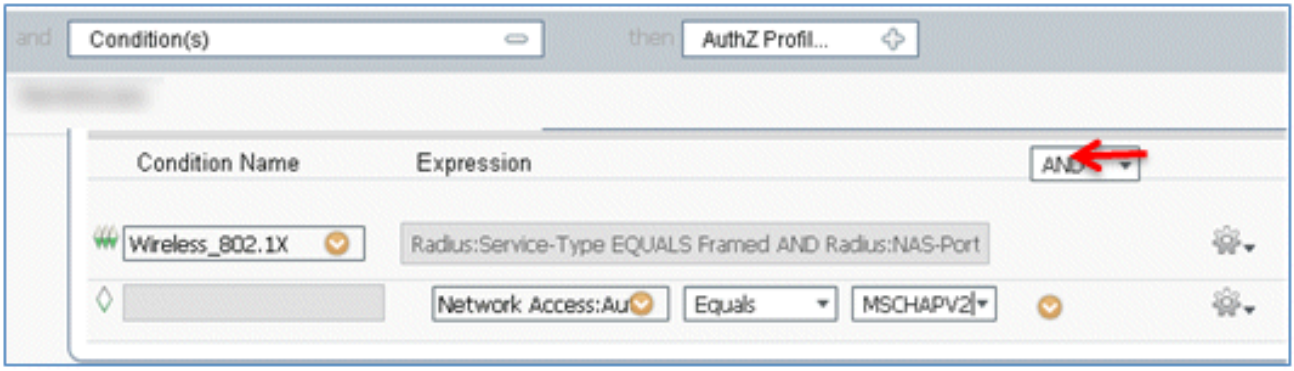
AuthenticationMethod: **Igual a**



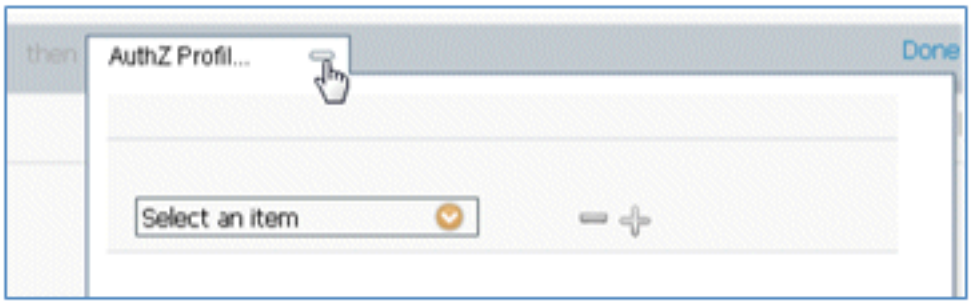
Seleccione **MSCHAPV2**.

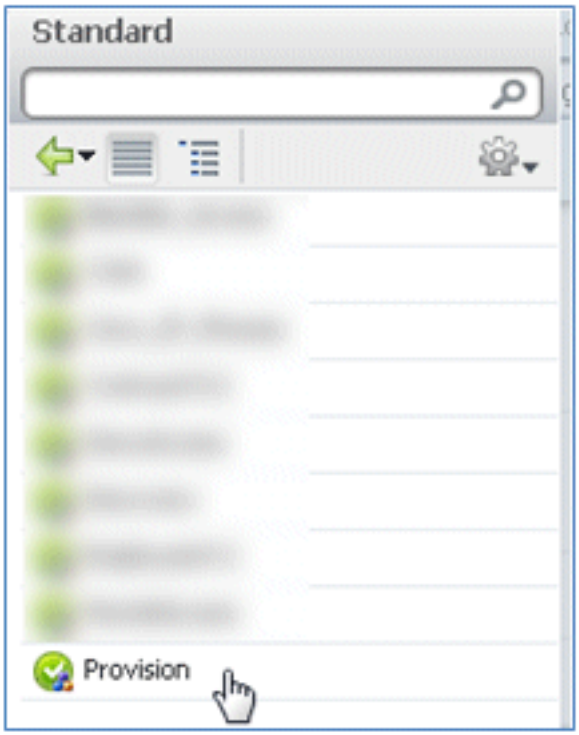


Este es un ejemplo de la regla; asegúrese de confirmar que la condición es AND.



73. En AuthZ Profile, seleccione **Standard** > **Provisioning** (este es el perfil de autorización creado anteriormente).

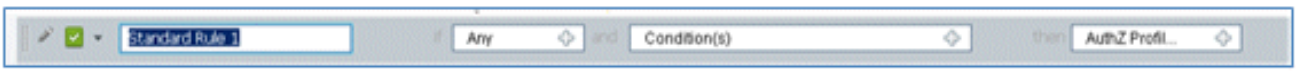




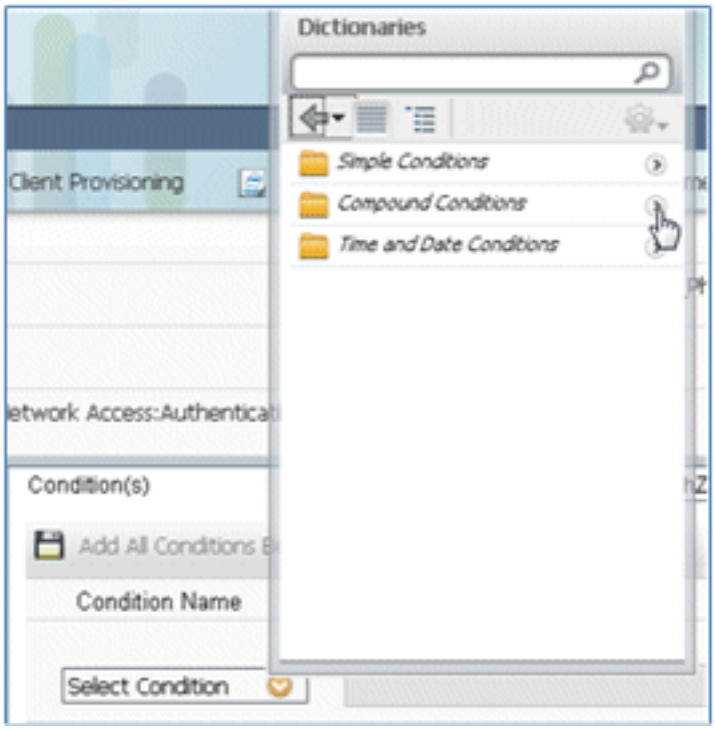
74. Haga clic en Done (Listo).

75. A la derecha de la regla PEAP, haga clic en la flecha hacia abajo junto a Editar y seleccione **Insertar nueva regla debajo**.

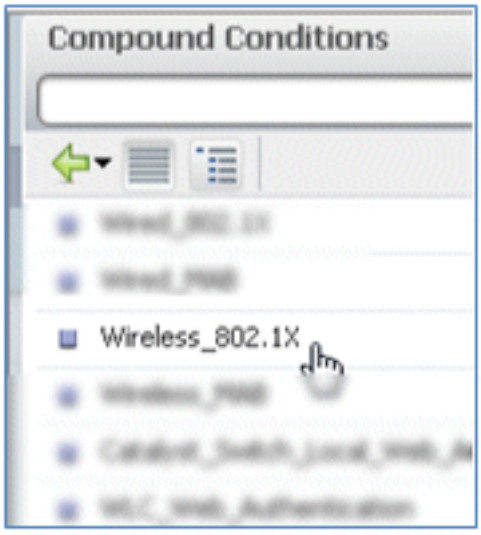
76. Cambie el Nombre de regla de Nº de regla estándar a **AllowRule** (en este ejemplo). Esta regla se utilizará para permitir el acceso a los dispositivos registrados con certificados instalados.



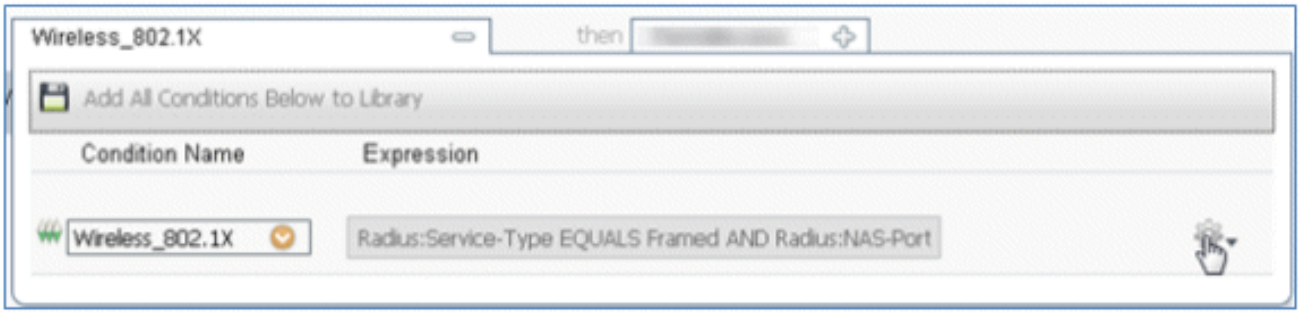
77. En Condición(s), seleccione **Condiciones compuestas**.



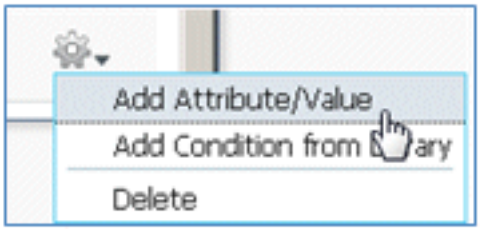
78. Seleccione **Wireless_802.1X**.



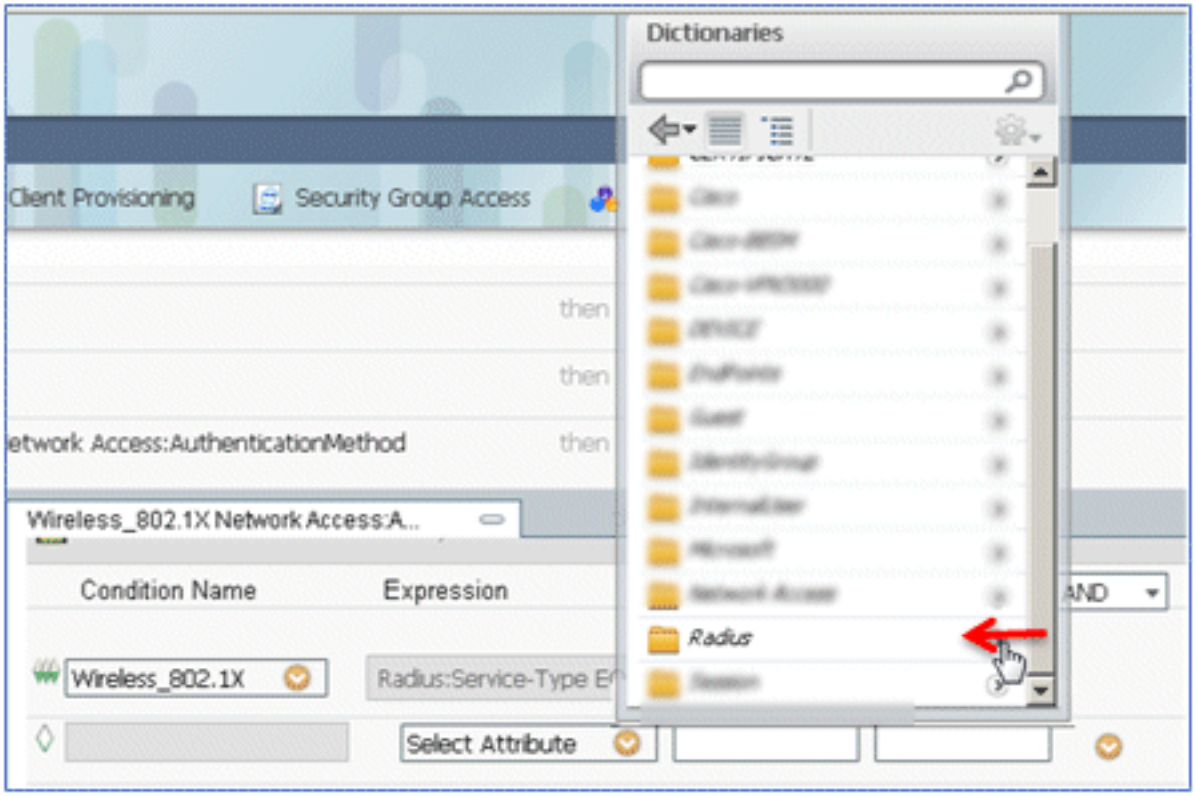
79. Agregue un atributo AND.



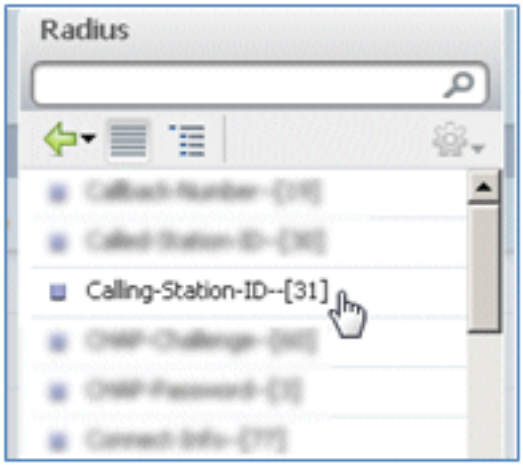
80. Haga clic en el icono de engranaje en el lado derecho de la condición y seleccione **Agregar atributo/valor**.



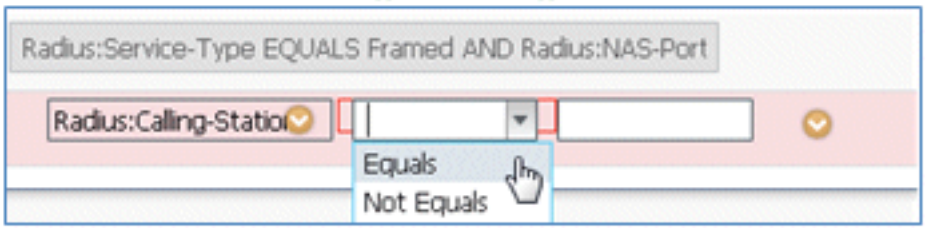
81. Localice y seleccione **Radius**.



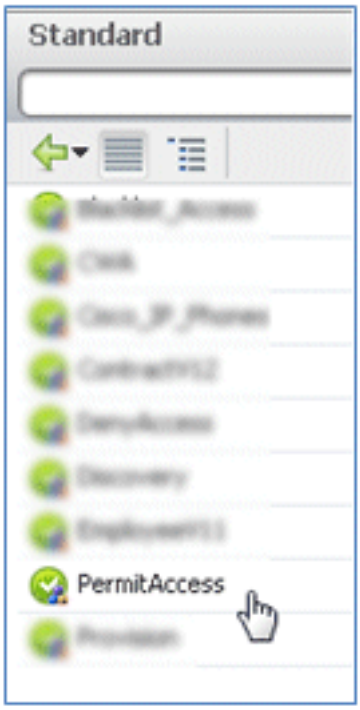
82. Seleccione **Calling-Station-ID—[31]**.



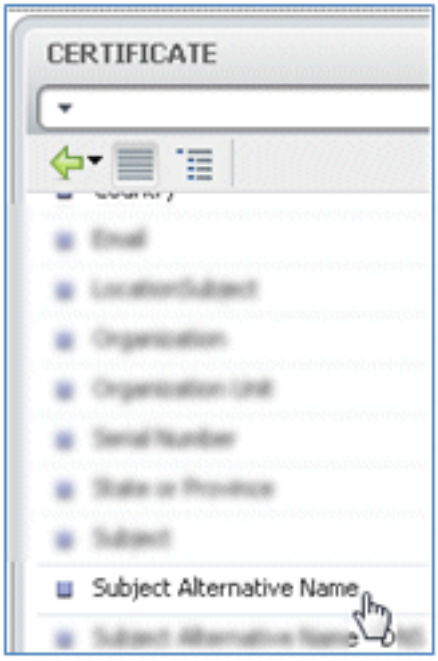
83. Seleccione **Equals**.



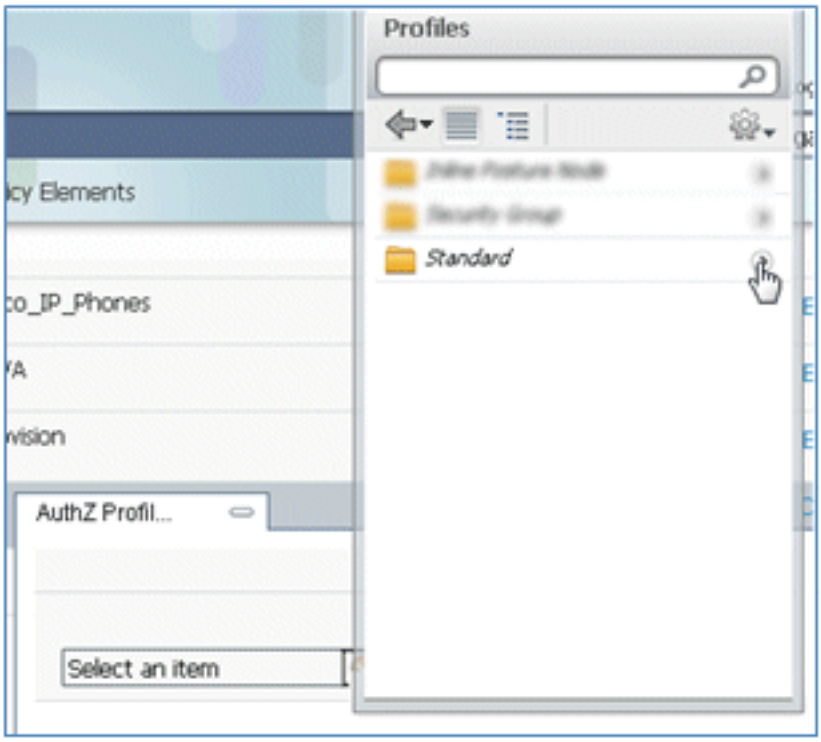
84. Vaya a **CERTIFICATE** y haga clic en la flecha derecha.



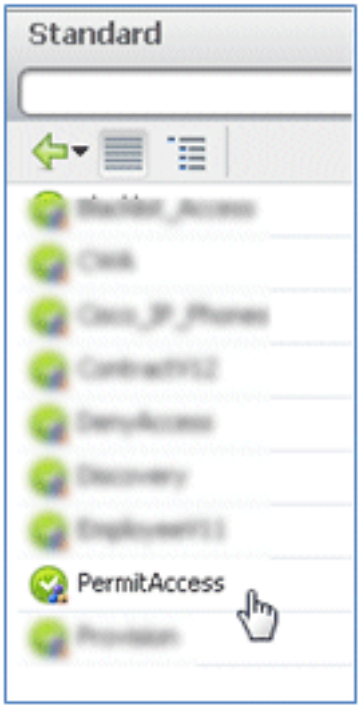
85. Seleccione **Nombre alternativo del asunto**.



86. Para el perfil AuthZ, seleccione **Standard**.



87. Seleccione **Permitir acceso**.

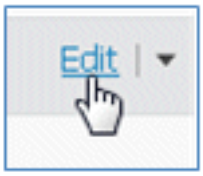


88. Haga clic en Done (Listo).

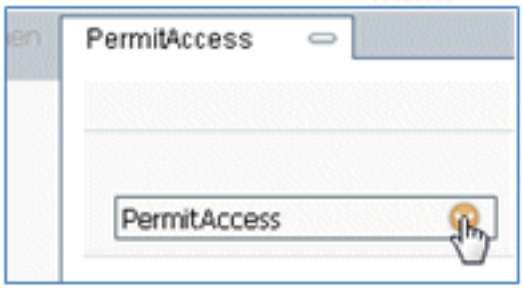
Este es un ejemplo de la regla:

89. Busque la regla predeterminada para cambiar PermitAccess a DenyAccess.

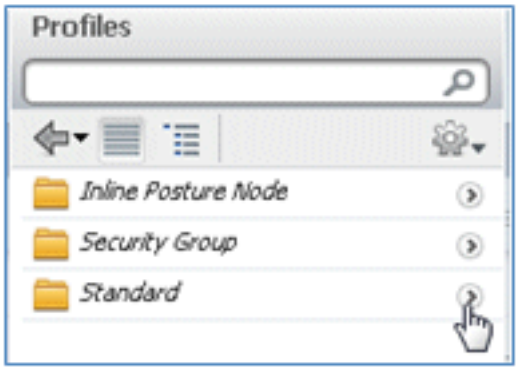
90. Haga clic en **Edit** para editar la regla predeterminada.



91. Vaya al perfil AuthZ existente de PermitAccess.



92. Seleccione **Estándar**.



93. Seleccione **Denegar acceso**.

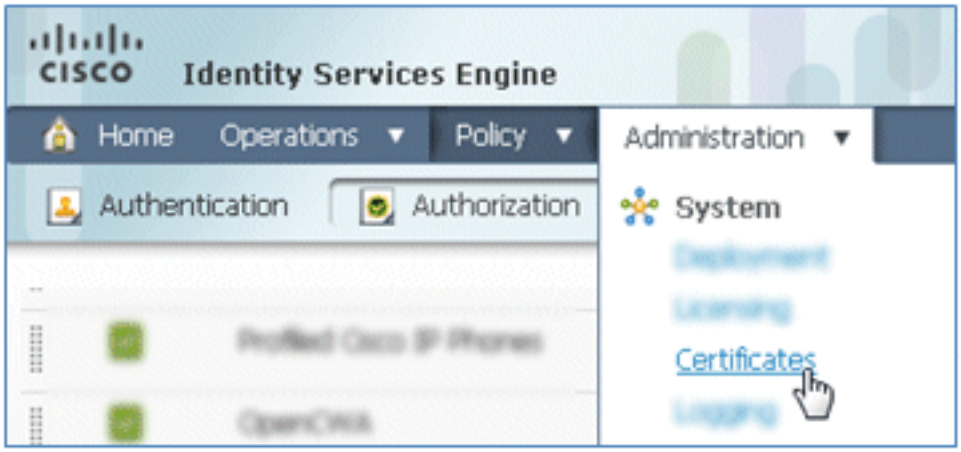
94. Confirme que la regla predeterminada tenga DenyAccess si no se encuentra ninguna coincidencia.

95. Haga clic en Done (Listo).

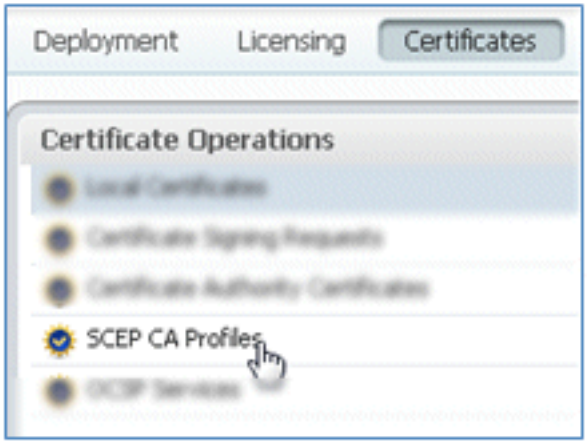
Este es un ejemplo de las reglas principales requeridas para esta prueba; son aplicables para un escenario SSID único o SSID dual.

96. Click **Save**.

97. Navegue hasta **ISE > Administration > System > Certificates** para configurar el servidor ISE con un perfil SCEP.



98. En Operaciones de certificados, haga clic en **Perfiles de CA de SCEP**.



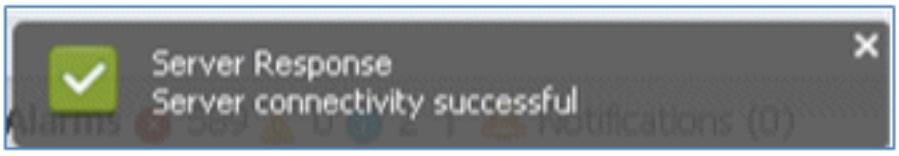
99. Haga clic en Add (Agregar).

100. Introduzca estos valores para este perfil:

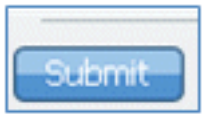
Nombre: **mySCEP** (en este ejemplo)URL: **https://**<ca-server>**/CertSrv/mscep/** (Compruebe la configuración del servidor de la CA para obtener la dirección correcta).

101. Haga clic en **Probar Conectividad** para probar la conectividad de la conexión SCEP.

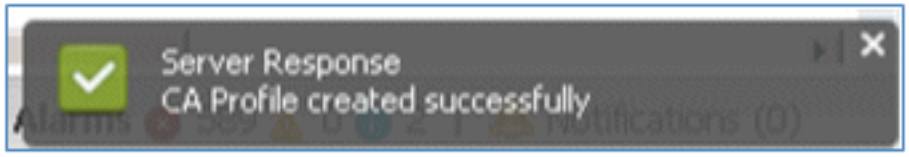
102. Esta respuesta muestra que la conectividad del servidor se ha realizado correctamente.



103. Haga clic en Submit (Enviar).



104. El servidor responde que el perfil de la CA se creó correctamente.



105. Confirme que se ha agregado el perfil de CA de SCEP.

Experiencia de usuario: aprovisionamiento de iOS

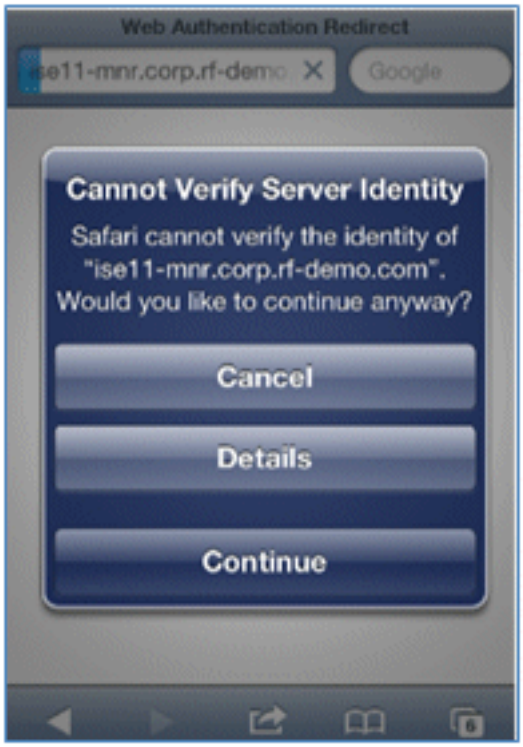
SSID doble

En esta sección se trata el SSID dual y se describe cómo conectarse al invitado que se va a aprovisionar y cómo conectarse a una WLAN 802.1x.

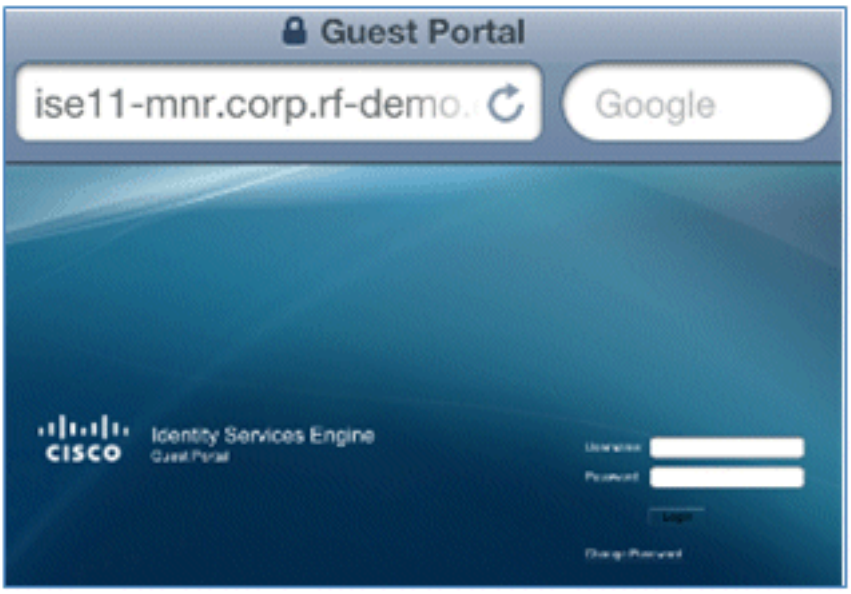
Complete estos pasos para aprovisionar iOS en el escenario de SSID dual:

1. En el dispositivo iOS, vaya a **Wi-Fi Networks**, y seleccione **DemoCWA** (WLAN abierta configurada en WLC).

2. Abra el navegador Safari en el dispositivo con iOS y visite una URL accesible (por ejemplo, un servidor web interno/externo). ISE le redirige al portal. Haga clic en **Continue** (Continuar).



3. Se le redirigirá al portal de invitados para iniciar sesión.



4. Inicie sesión con una cuenta de usuario y una contraseña de AD. Instale el perfil de la CA cuando se le solicite.

5. Haga clic en **Instalar** certificado de confianza del servidor de la CA.

6. Haga clic en **Finalizado** una vez que el perfil esté completamente instalado.

7. Vuelva al explorador y haga clic en **Register** (**Registrar)**. Anote el ID de dispositivo que contiene la dirección MAC del dispositivo.

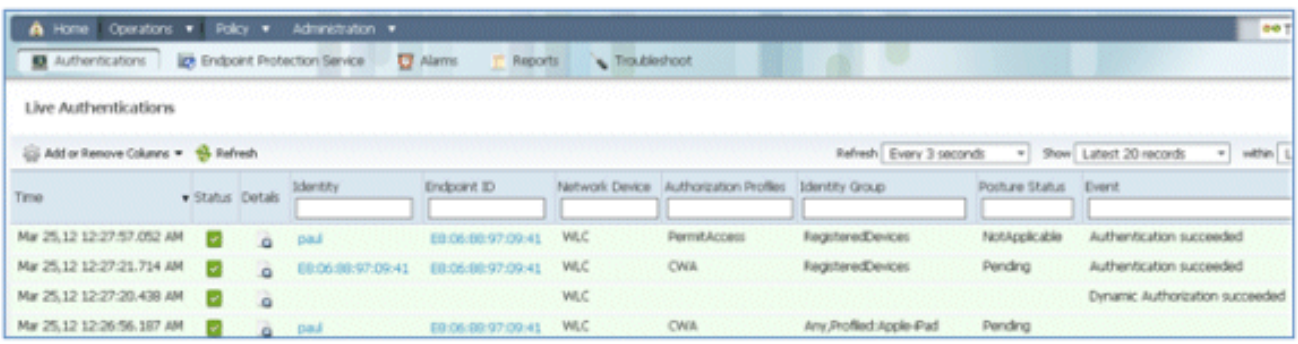
8. Haga clic en **Install** para instalar el perfil verificado.

9. Haga clic en **Instalar ahora**.

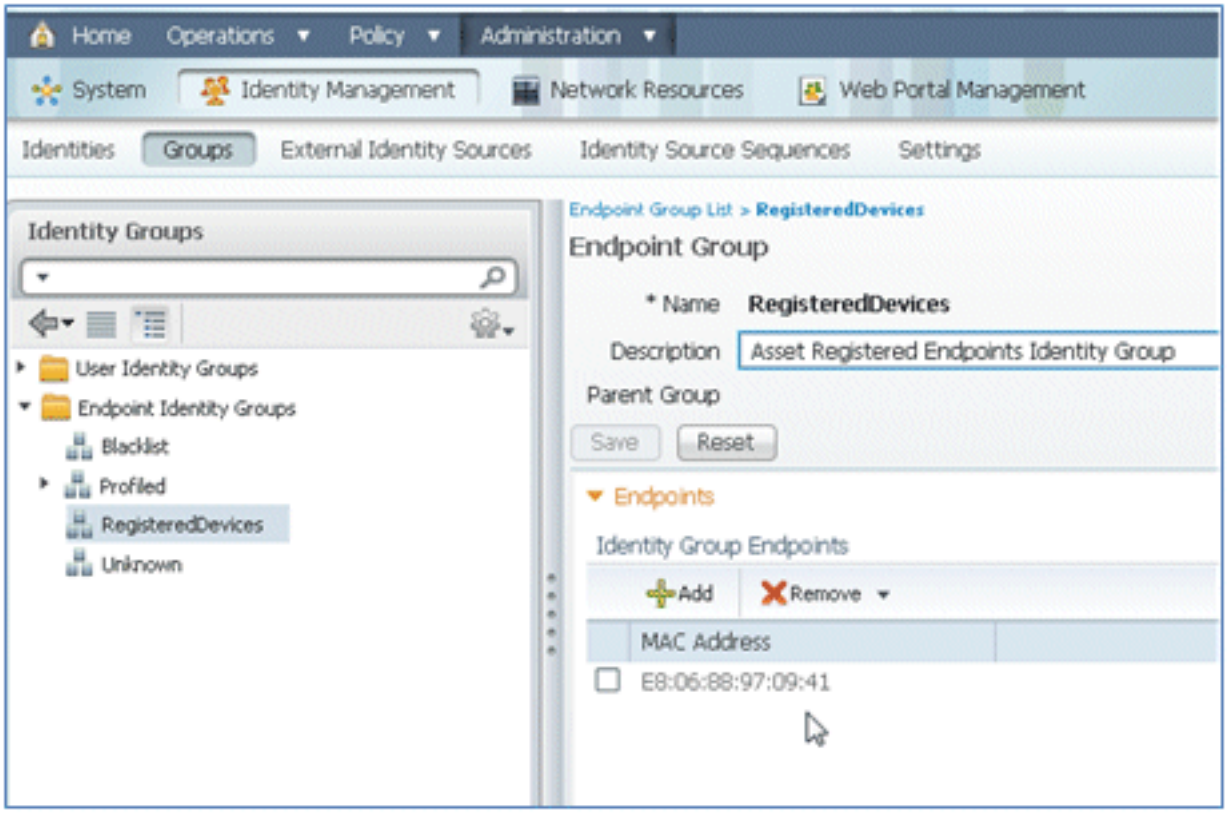
10. Una vez finalizado el proceso, el perfil de WirelessSP confirma que el perfil está instalado. Haga clic en Done (Listo).

11. Vaya a **Wi-Fi Networks** y cambie la red a **Demo1x**. El dispositivo ya está conectado y utiliza TLS.

12. En ISE, vaya a **Operaciones > Autenticaciones**. Los eventos muestran el proceso en el que el dispositivo está conectado a la red abierta de invitados, pasa por el proceso de registro con aprovisionamiento de suplicante y se le permite el acceso a los permisos después del registro.



13. Vaya a ISE > Administration > Identity Management > **Groups** > **Endpoint Identity Groups** > RegisteredDevices. La dirección MAC se ha agregado a la base de datos.

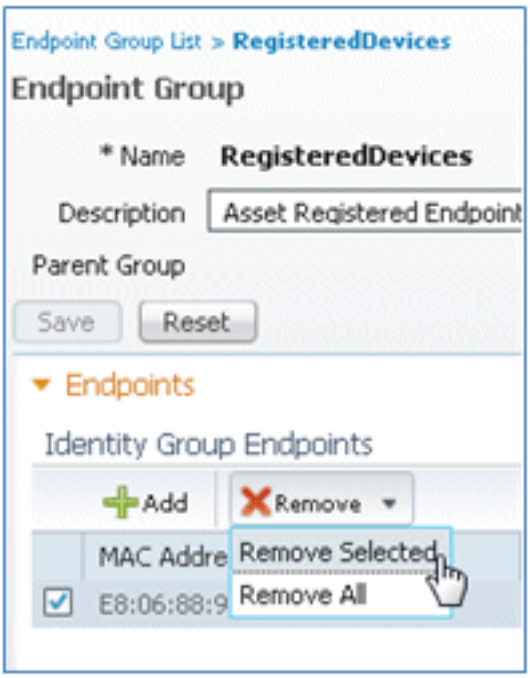


SSID único

En esta sección se trata un SSID único y se describe cómo conectarse directamente a una WLAN 802.1x, proporcionar un nombre de usuario/contraseña de AD para la autenticación PEAP, aprovisionar a través de una cuenta de invitado y volver a conectar con TLS.

Complete estos pasos para aprovisionar iOS en el escenario de SSID único:

1. Si utiliza el mismo dispositivo iOS, elimine el terminal de los dispositivos registrados.



2. En el dispositivo con iOS, navegue hasta **Configuración > Generales > Perfiles**. Quite los perfiles instalados en este ejemplo.

3. Haga clic en **Quitar** para quitar los perfiles anteriores.

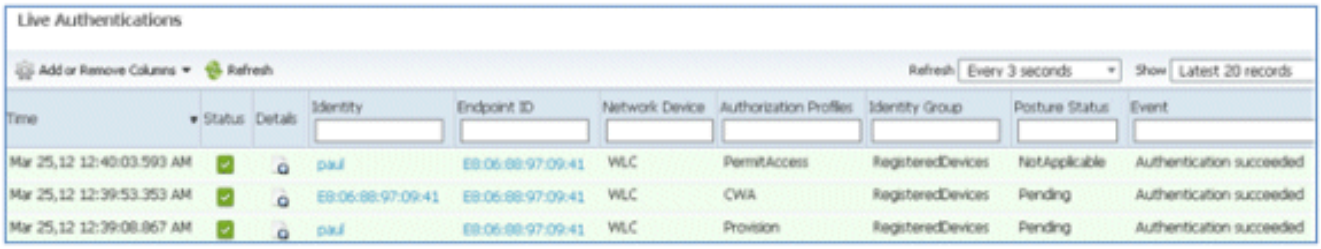
4. Conéctese directamente al 802.1x con el dispositivo existente (desactivado) o con un nuevo dispositivo iOS.

5. Conéctese a **Dot1x**, ingrese un nombre de usuario y contraseña, y haga clic en **Unirse**.

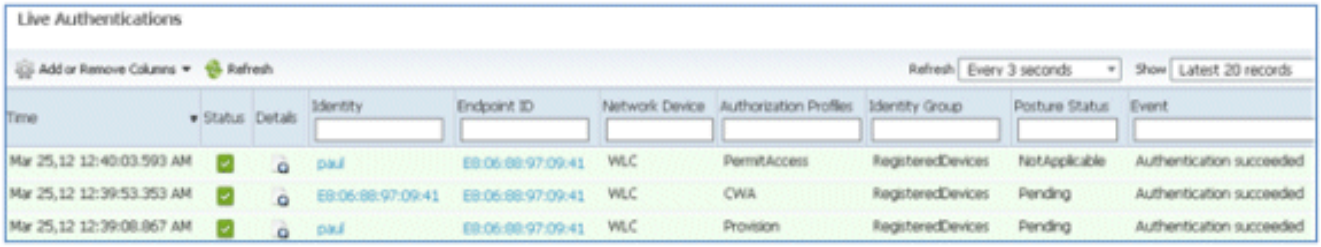
6. Repita los pasos 90 y siguientes desde la sección Configuración de ISE hasta que los

perfiles adecuados estén completamente instalados.

7. Navegue hasta **ISE > Operaciones > Autenticaciones** para monitorear el proceso. En este ejemplo se muestra el cliente que está conectado directamente a WLAN 802.1X mientras se aprovisiona, se desconecta y se vuelve a conectar a la misma WLAN con el uso de TLS.



8. Navegue hasta **WLC > Monitor > [Client MAC]**. En los detalles del cliente, observe que el cliente está en el estado RUN, que el switching de datos está configurado en local y que la autenticación es central. Esto se aplica a los clientes que se conectan a FlexConnect AP.



Experiencia de usuario: aprovisionamiento de Android

SSID doble

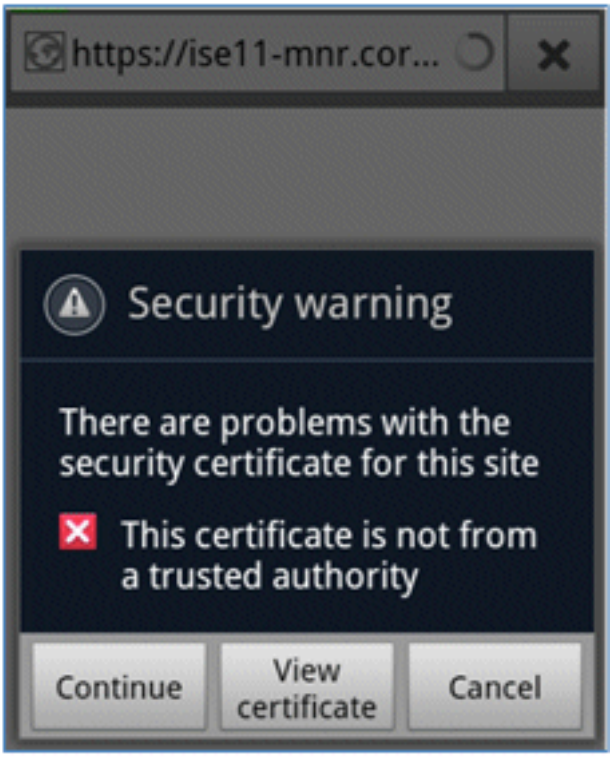
En esta sección se trata el SSID dual y se describe cómo conectarse al invitado que se va a aprovisionar y cómo conectarse a una WLAN 802.1x.

El proceso de conexión para el dispositivo Android es muy similar al de un dispositivo iOS (SSID único o dual). Sin embargo, una diferencia importante es que el dispositivo Android requiere acceso a Internet para acceder a Google Marketplace (ahora Google Play) y descargar el agente solicitante.

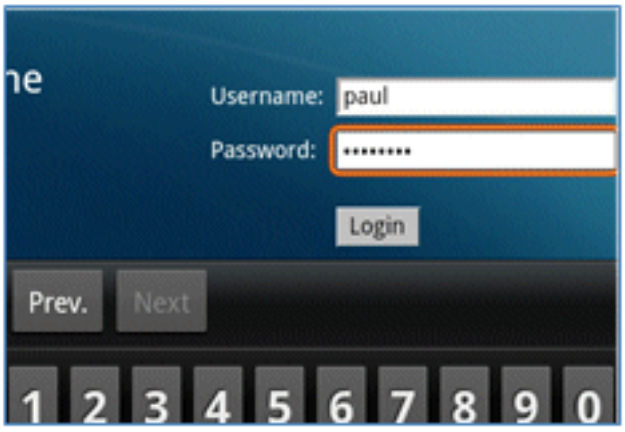
Complete estos pasos para aprovisionar un dispositivo Android (como el Samsung Galaxy en este ejemplo) en el escenario SSID dual:

1. En el dispositivo Android, use Wi-Fi para conectarse a **DemoCWA**, y abra la WLAN de invitado.

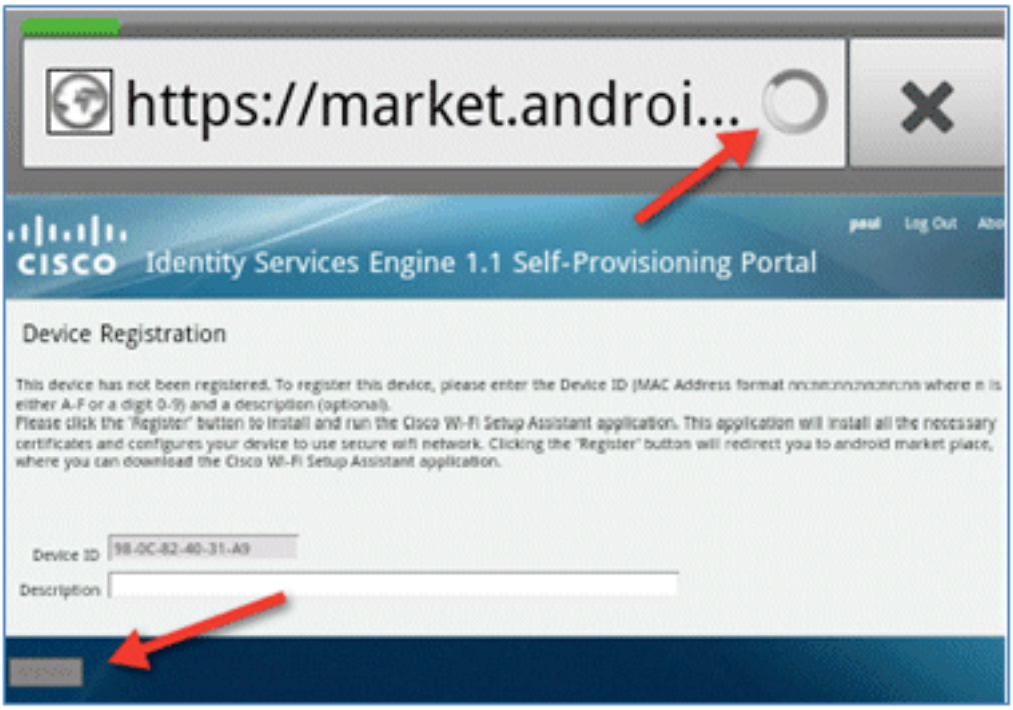
2. Acepte cualquier certificado para conectarse a ISE.



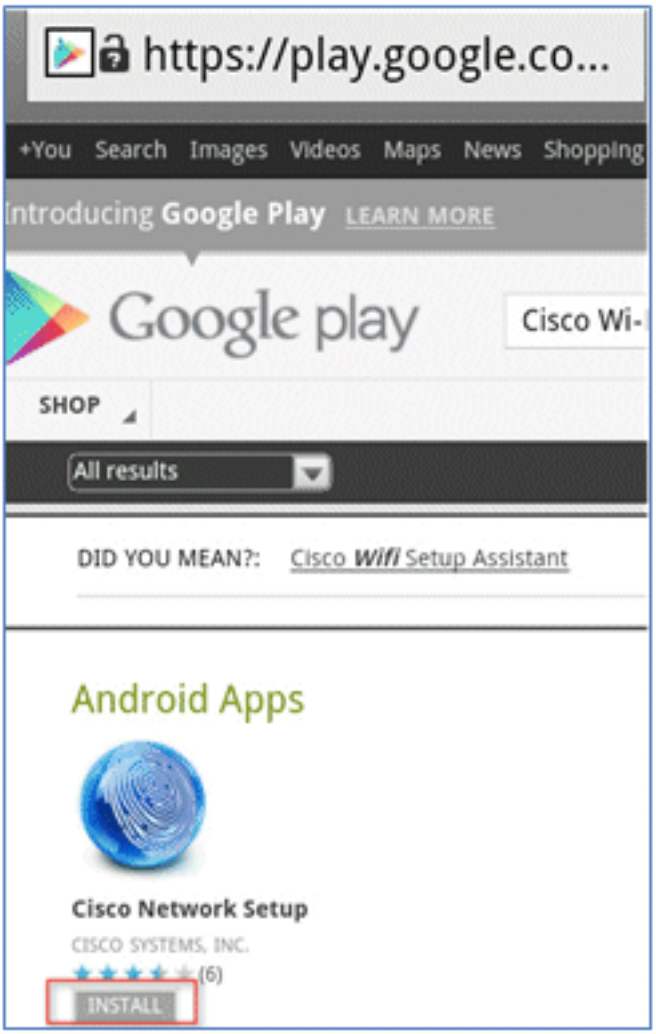
3. Introduzca un nombre de usuario y una contraseña en el portal de invitados para iniciar sesión.



4. Haga clic en **Register**. El dispositivo intenta acceder a Internet para acceder a Google Marketplace. Agregue cualquier regla adicional a la ACL Pre-Auth (como ACL-REDIRECT) en el controlador para permitir el acceso a Internet.

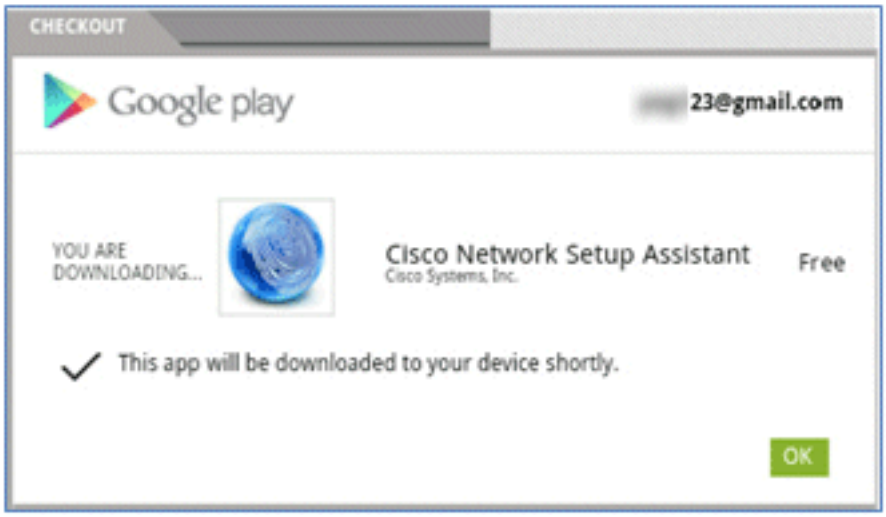


5. Google enumera Cisco Network Setup como una aplicación para Android. Haga clic en **INSTALL**.

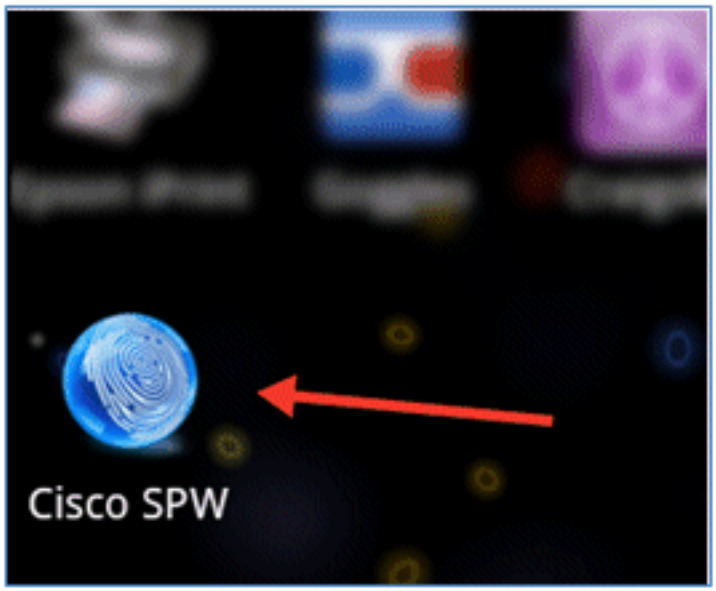


6. Inicie sesión en Google y haga clic en **INSTALAR**.

7. Click OK.



8. En el dispositivo Android, busque la aplicación **Cisco SPW** instalada y ábrala.



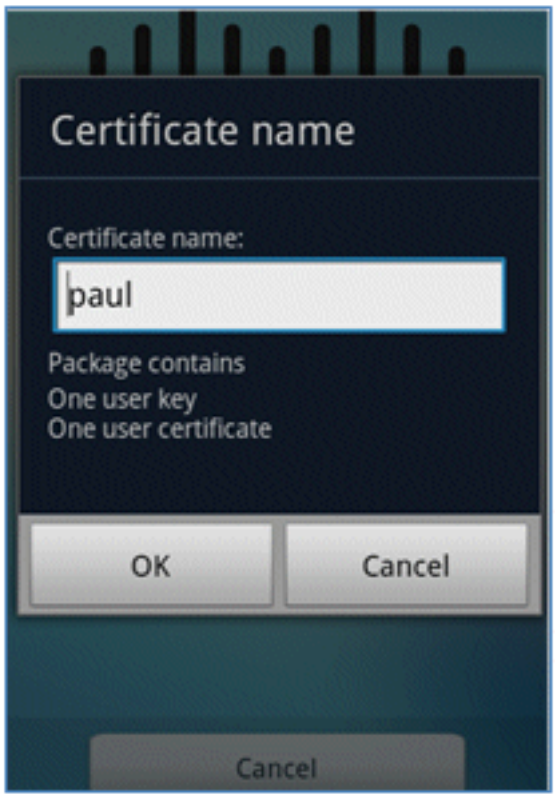
9. Asegúrese de que sigue conectado al portal de invitados desde su dispositivo Android.

10. Haga clic en **Start** para iniciar el Wi-Fi Setup Assistant.

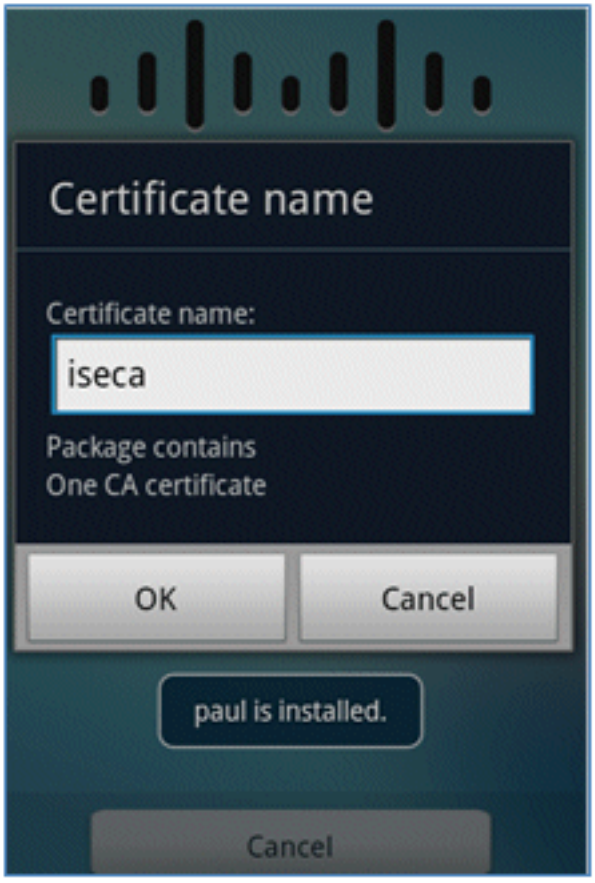
11. Cisco SPW comienza a instalar certificados.

12. Cuando se le solicite, establezca una contraseña para el almacenamiento de credenciales.

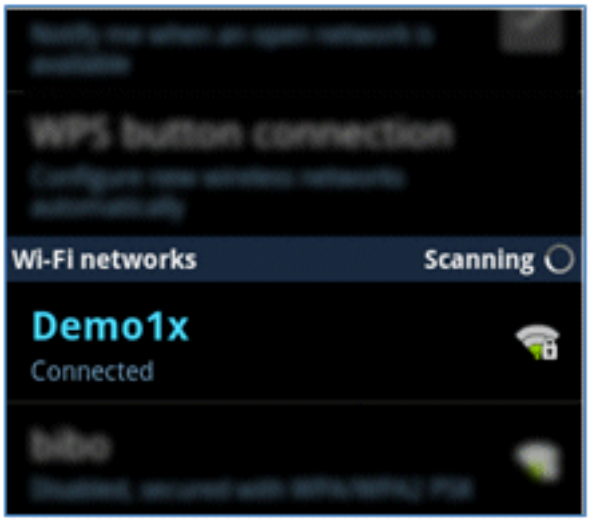
13. Cisco SPW devuelve con un nombre de certificado, que contiene la clave de usuario y el certificado de usuario. Haga clic en Aceptar para confirmar.



14. Cisco SPW continúa y solicita otro nombre de certificado, que contiene el certificado de la CA. Ingrese el nombre **iseca** (en este ejemplo), luego haga clic en **Aceptar** para continuar.



15. El dispositivo Android ya está conectado.

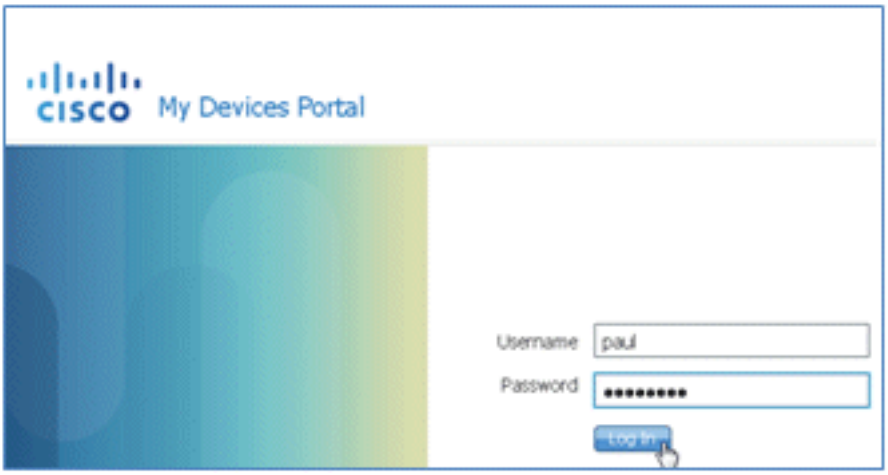


Portal Mis dispositivos

El portal Mis dispositivos permite a los usuarios incluir en una lista negra los dispositivos registrados anteriormente en caso de pérdida o robo. También permite a los usuarios volver a inscribirse si es necesario.

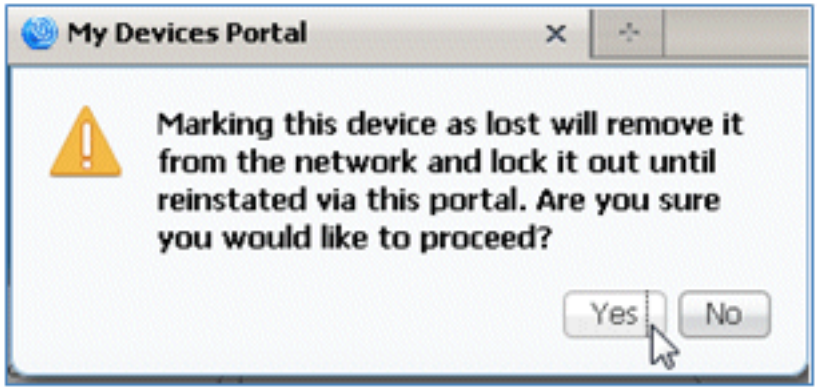
Complete estos pasos para poner en la lista negra un dispositivo:

1. Para iniciar sesión en el portal Mis dispositivos, abra un explorador, conéctese a https://ise-server:8443/mydevices (observe el número de puerto 8443) e inicie sesión con una cuenta de AD.



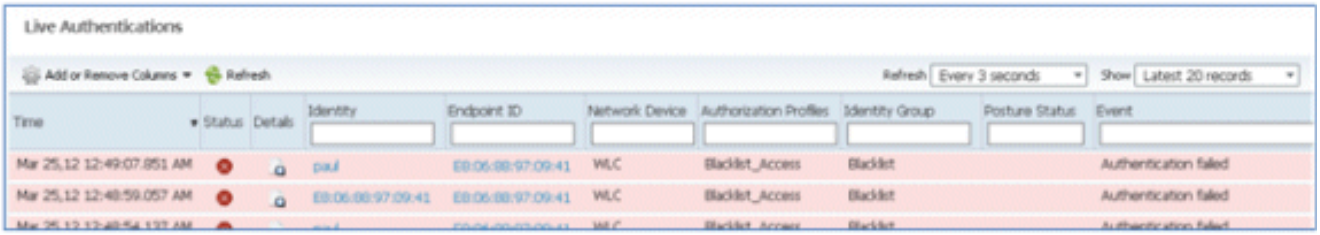
2. Localice el dispositivo bajo Device ID, y haga clic en **Lost?** para iniciar la lista negra de un dispositivo.

3. Cuando ISE solicite una advertencia, haga clic en **Yes** para continuar.



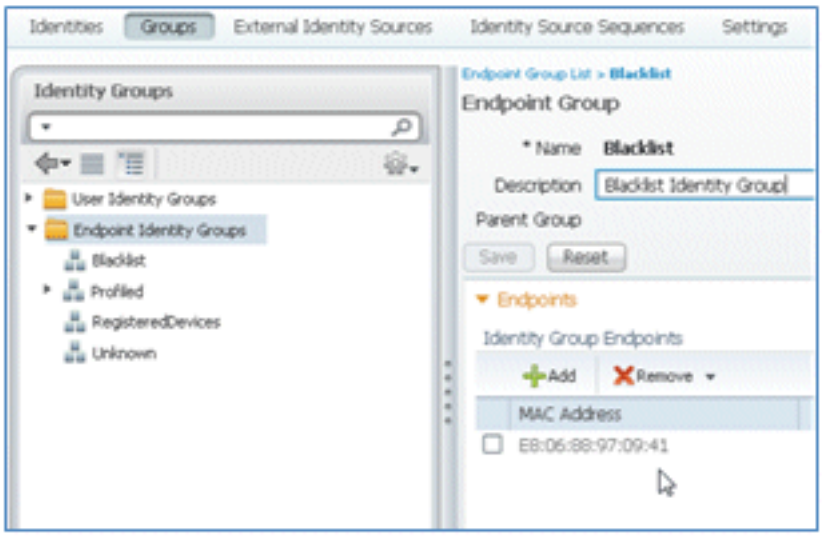
4. ISE confirma que el dispositivo está marcado como **perdido**.

5. Se bloquea cualquier intento de conexión a la red con el dispositivo registrado anteriormente, incluso si hay instalado un certificado válido. Este es un ejemplo de un dispositivo en la lista negra que falla la autenticación:



6. Un administrador puede navegar hasta ISE > Administration > Identity Management > **Groups**, hacer clic en **Endpoint Identity Groups** > Blacklist y ver que el dispositivo está en la

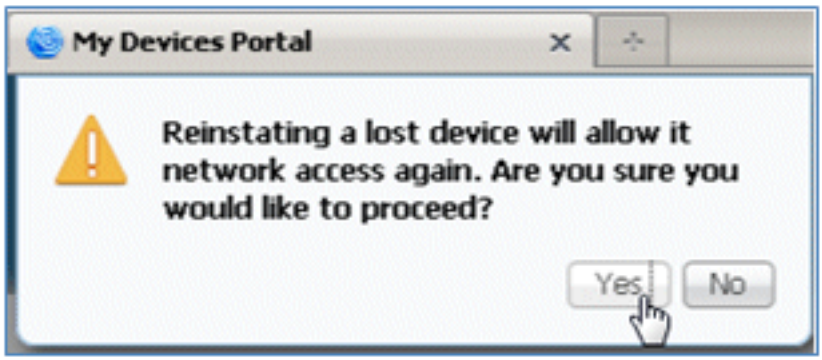
lista negra.



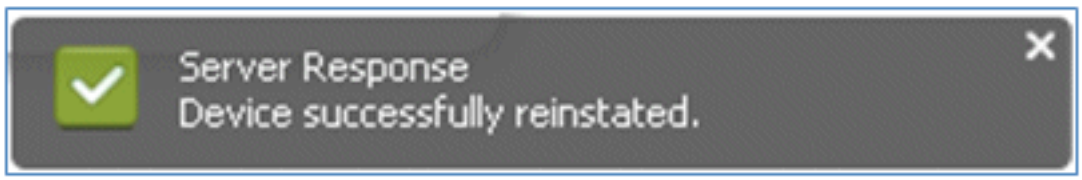
Complete estos pasos para restablecer un dispositivo en la lista negra:

1. En el portal Mis dispositivos, haga clic en **Restablecer** para ese dispositivo.

2. Cuando ISE solicite una advertencia, haga clic en **Yes** para continuar.



3. ISE confirma que el dispositivo se ha restablecido correctamente. Conecte el dispositivo restablecido a la red para probar que el dispositivo ahora estará permitido.

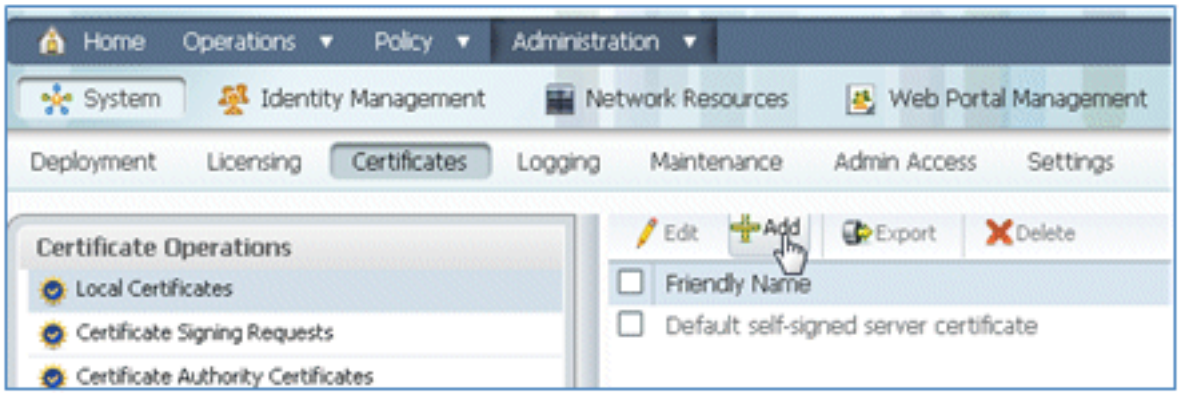


Referencia - Certificados

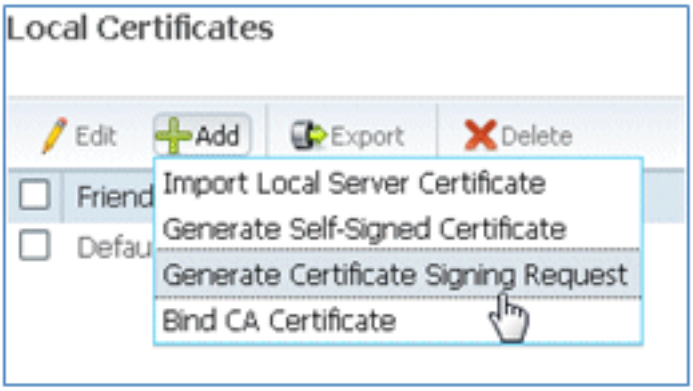
ISE no solo requiere un certificado raíz de CA válido, sino también un certificado válido firmado por CA.

Complete estos pasos para agregar, vincular e importar el nuevo certificado de CA de confianza:

1. Vaya a ISE > Administration > System > **Certificates**, haga clic en **Local Certificates** y luego en Add.

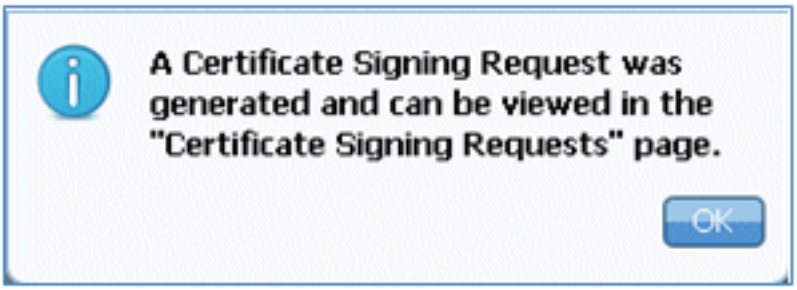


2. Seleccione **Generar solicitud de firma de certificado** (CSR).

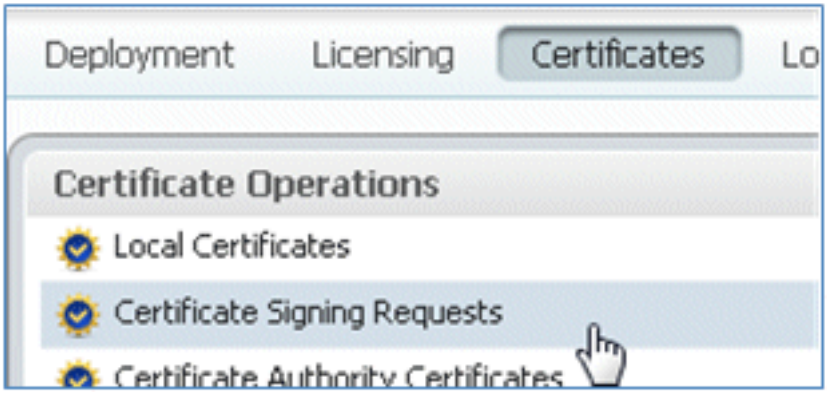


3. Introduzca el asunto del certificado **CN=<***ISE-SERVER hostname.FQDN***>**. Para los demás campos, puede utilizar el valor predeterminado o los valores requeridos por la configuración de CA. Haga clic en Submit (Enviar).

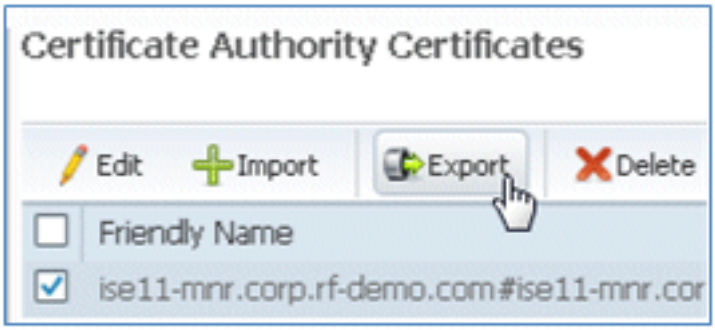
4. ISE comprueba que se ha generado la CSR.



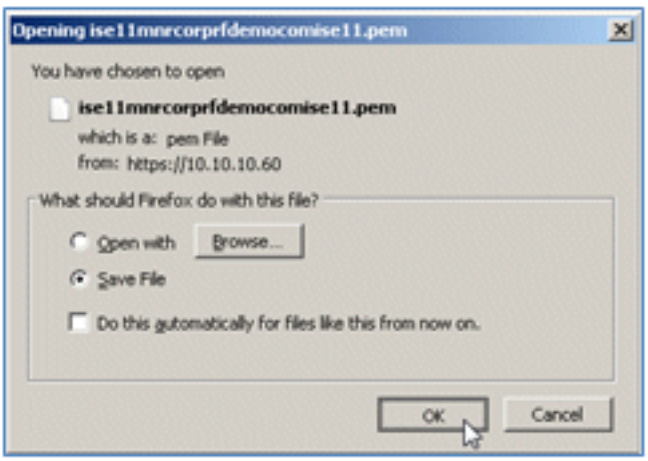
5. Para acceder al CSR, haga clic en las operaciones **Solicitud de firma de certificado**.



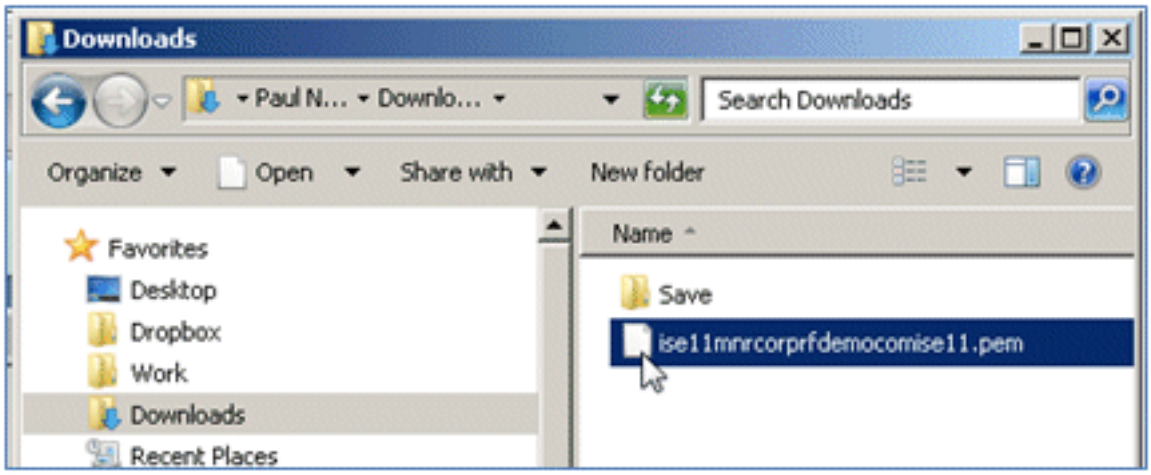
6. Seleccione el CSR creado recientemente y, a continuación, haga clic en **Exportar**.



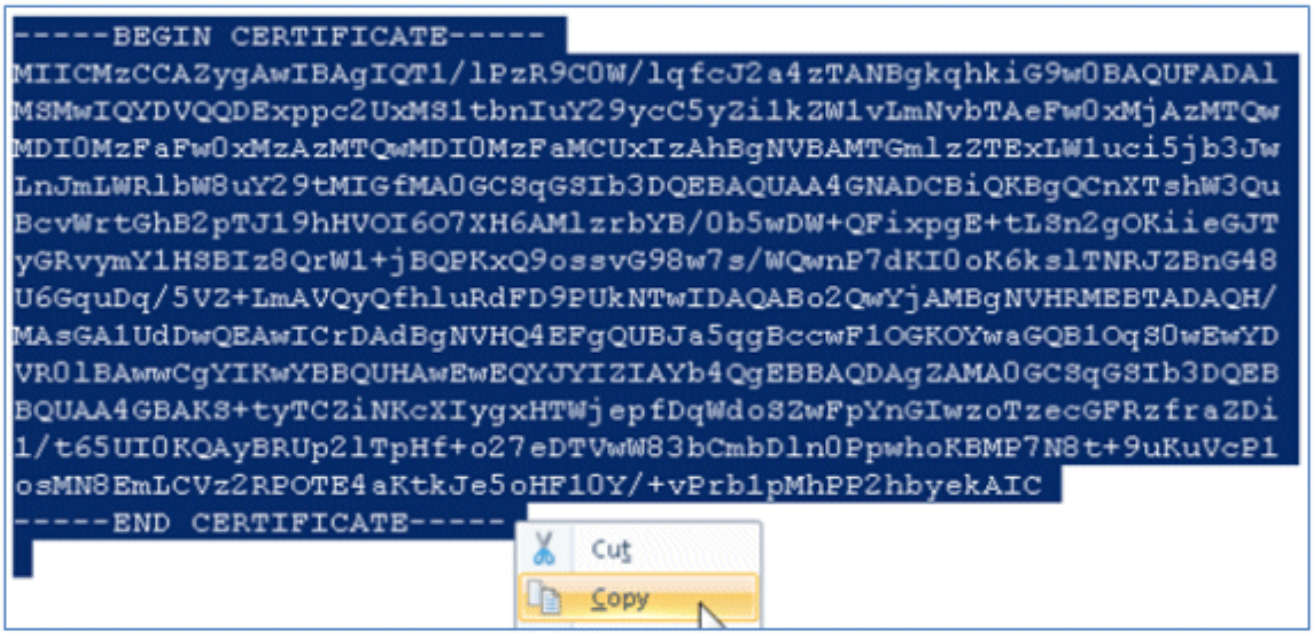
7. ISE exporta la CSR a un archivo .pem. Haga clic en **Guardar archivo**, luego haga clic en **Aceptar** para guardar el archivo en la máquina local.



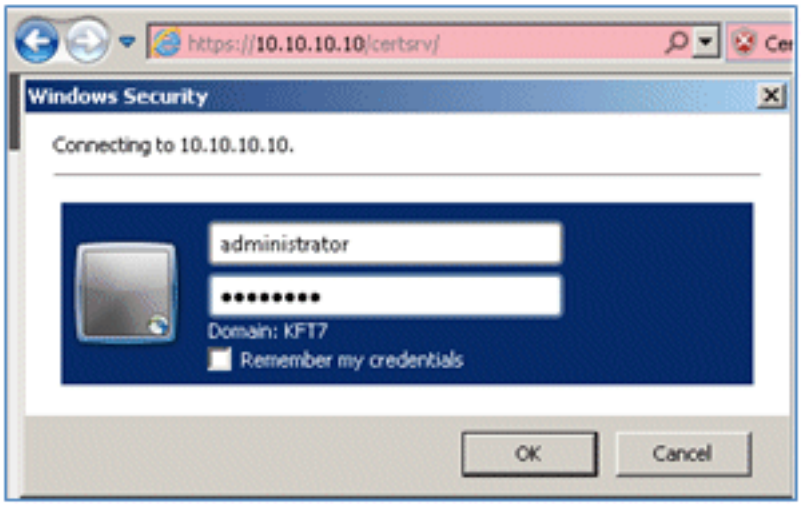
8. Busque y abra el archivo de certificado de ISE con un editor de texto.



9. Copie todo el contenido del certificado.

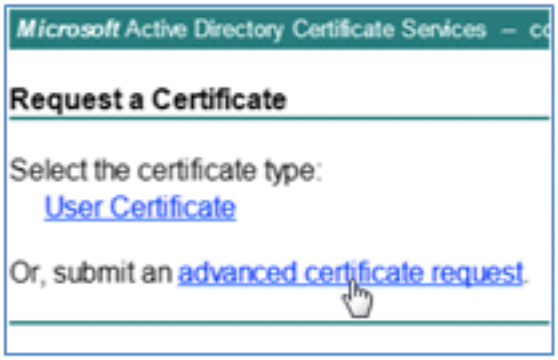


10. Conéctese al servidor de la CA e inicie sesión con una cuenta de administrador. El servidor es una CA de Microsoft 2008 en https://10.10.10.10/certsrv (en este ejemplo).

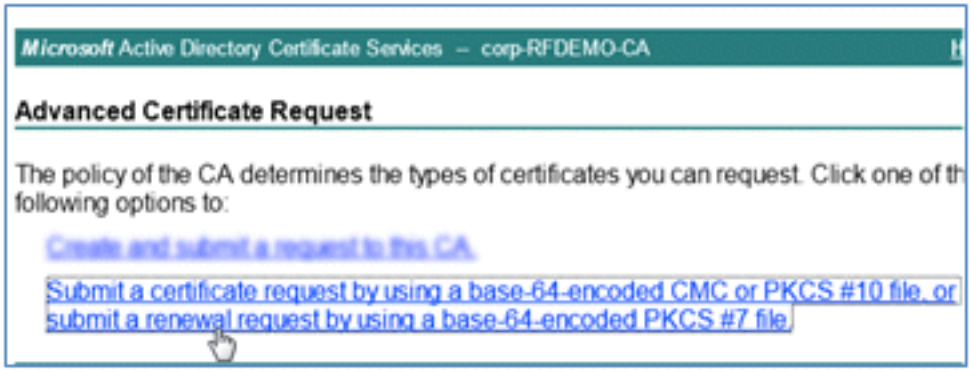


11. Haga clic en **Solicitar un certificado**.

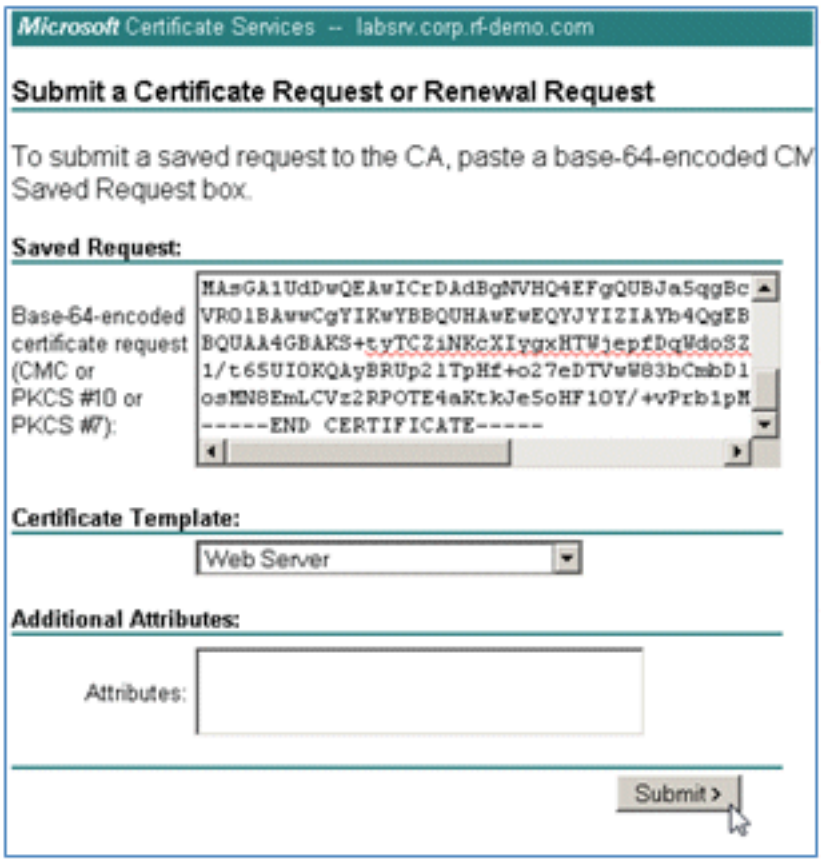
12. Haga clic en **Advanced Certificate Request**.



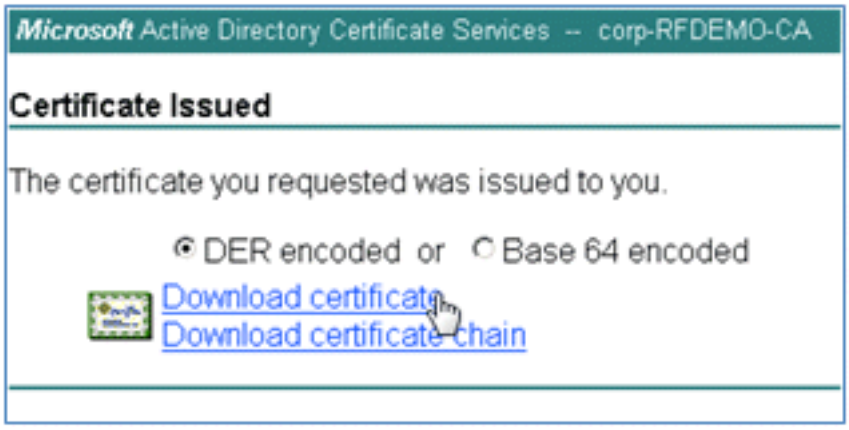
13. Haga clic en la segunda opción para **enviar una solicitud de certificado mediante un CMC codificado en base 64 o ...** .



14. Pegue el contenido del archivo de certificado de ISE (.pem) en el campo Solicitud guardada, asegúrese de que la plantilla de certificado es **Servidor web** y haga clic en **Enviar**.

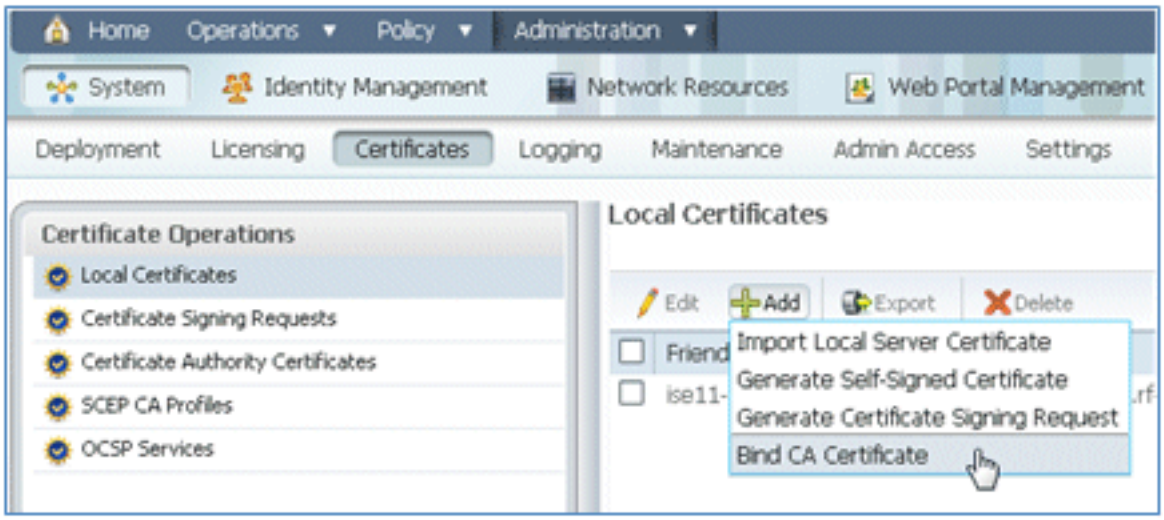


15. Haga clic en **Descargar certificado**.

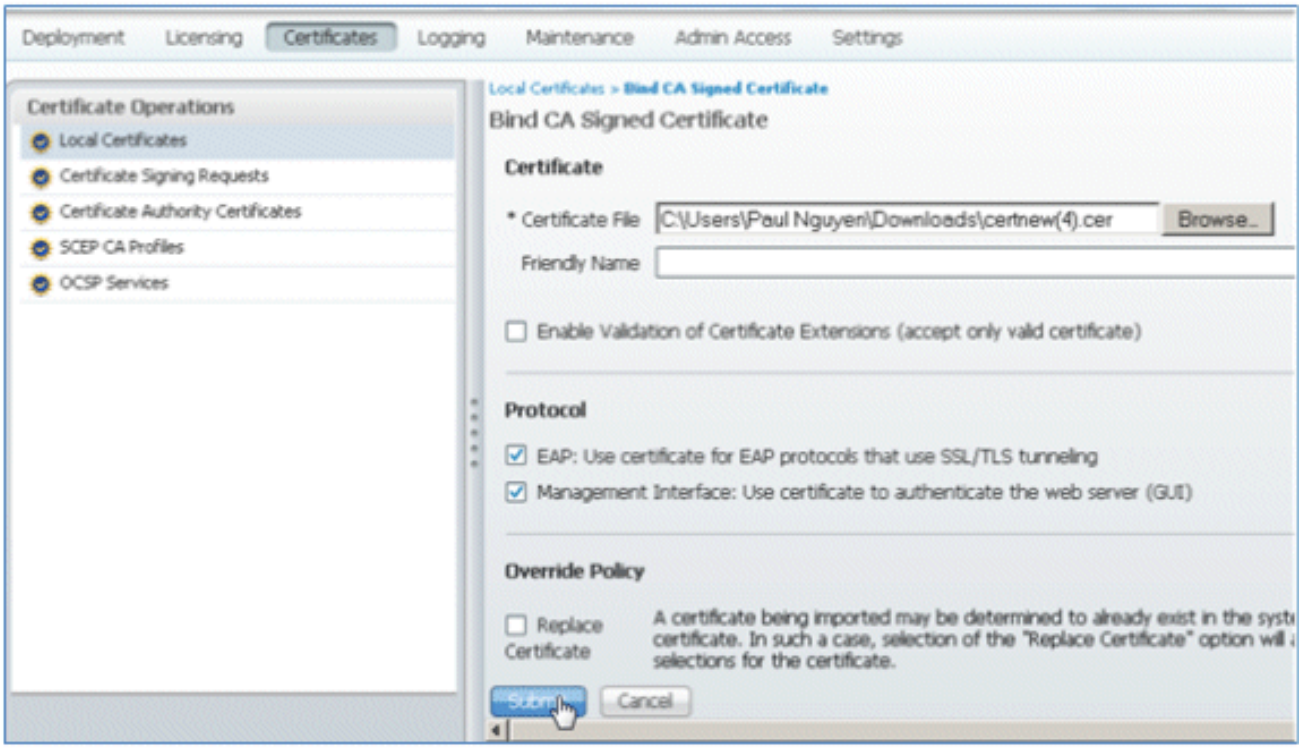


16. Guarde el archivo certnew.cer; se utilizará más adelante para enlazar con ISE.

17. En **Certificados de** ISE, vaya a **Certificados locales** y haga clic en **Agregar > Enlazar certificado de CA**.



18. Busque el certificado que se guardó en el equipo local en el paso anterior, habilite los protocolos **EAP** y **Management Interface** (las casillas están activadas) y haga clic en **Submit**. ISE puede tardar varios minutos o más en reiniciar los servicios.

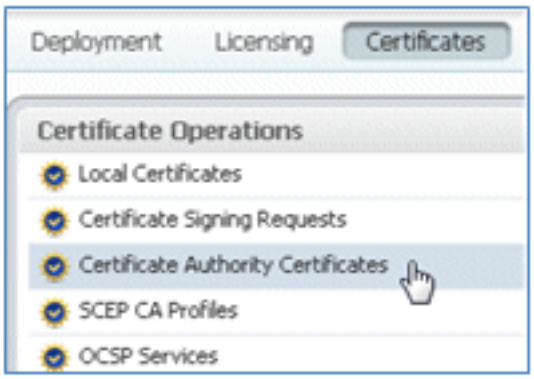


19. Vuelva a la página de inicio de la CA (https://CA/certsrv/) y haga clic en **Descargar un certificado de CA, cadena de certificados o CRL**.

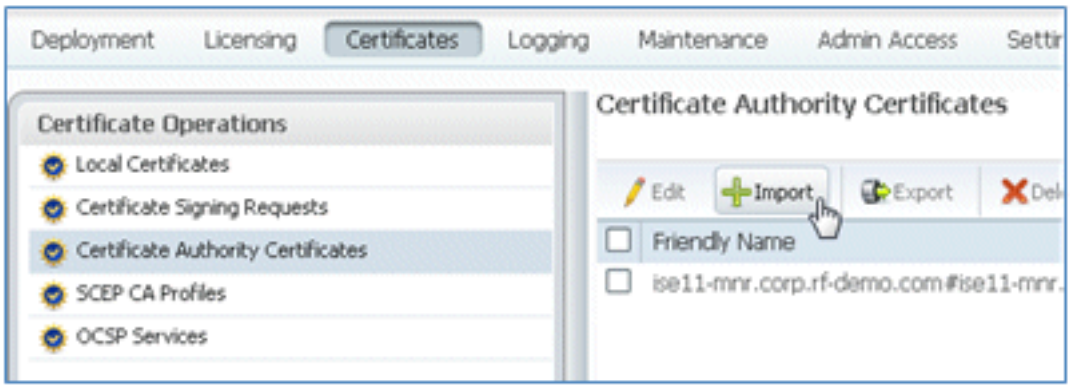
20. Haga clic en **Descargar certificado de CA**.

21. **Guarde** el archivo en el equipo local.

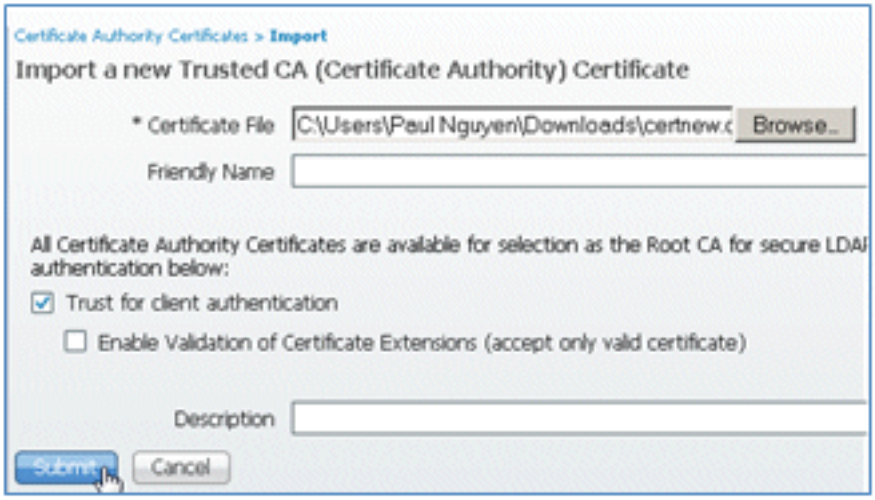
22. Con el servidor ISE online, vaya a **Certificates** y haga clic en **Certificate Authority Certificates**.



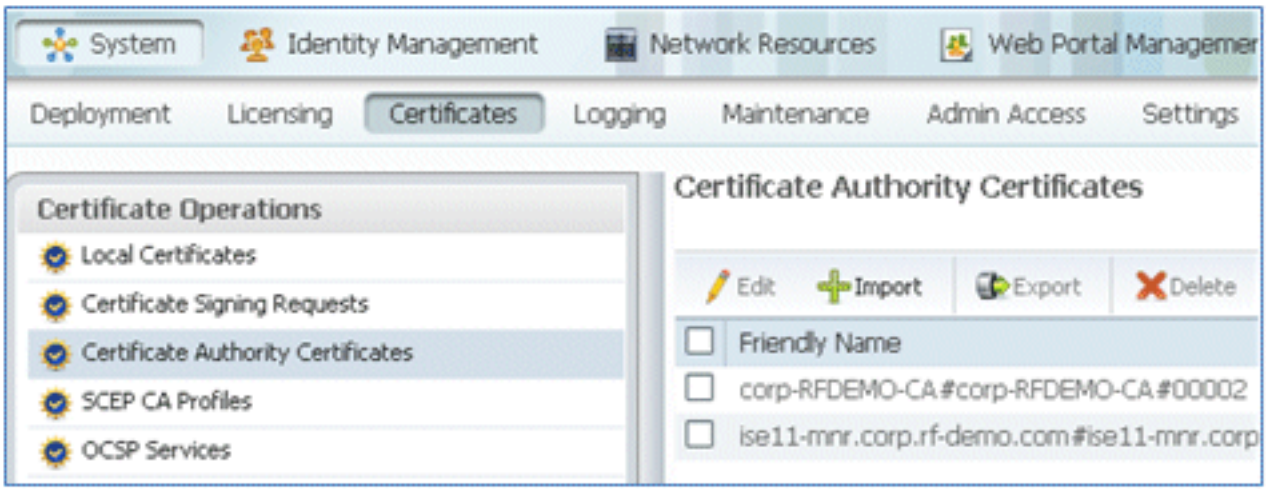
23. Haga clic en **Importar**.



24. Busque el certificado de la CA, habilite **Confianza para la autenticación del cliente** (la casilla está marcada) y haga clic en **Enviar**.



25. Confirme que se ha agregado el nuevo certificado de CA de confianza.



Información Relacionada

- Guía de instalación de hardware de Cisco Identity Services Engine, versión 1.0.4
- Controladores LAN inalámbricos Cisco de la serie 2000
- Controladores LAN inalámbricos Cisco de la serie 4400
- Cisco Aironet 3500 Series
- Guía de implementación del controlador de sucursal inalámbrica Flex 7500
- Traiga su propio dispositivo: autenticación de dispositivo unificada y experiencia de acceso uniforme
- BYOD inalámbrico con Identity Services Engine
- 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).