Ejemplo de Configuración de ACS Version 5.2 y WLC para la Autenticación por WLAN

Contenido

Introducción

Este documento proporciona un ejemplo de configuración para restringir el acceso por usuario a una LAN inalámbrica (WLAN) basado en el identificador del conjunto de servicios (SSID).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo configurar el controlador de LAN inalámbrica (WLC) y el punto de acceso ligero (LAP) para el funcionamiento básico
- Cómo configurar Cisco Secure Access Control Server (ACS)
- Métodos de seguridad inalámbrica y protocolo ligero de punto de acceso (LWAPP)

Componentes Utilizados

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

- WLC de la serie 5500 de Cisco que ejecuta la versión 7.4.110 del firmware
- LAP de la serie 1142 de Cisco
- Servidor Cisco Secure ACS versión 5.2.0.26.11

Configurar

Para configurar los dispositivos para esta configuración, debe:

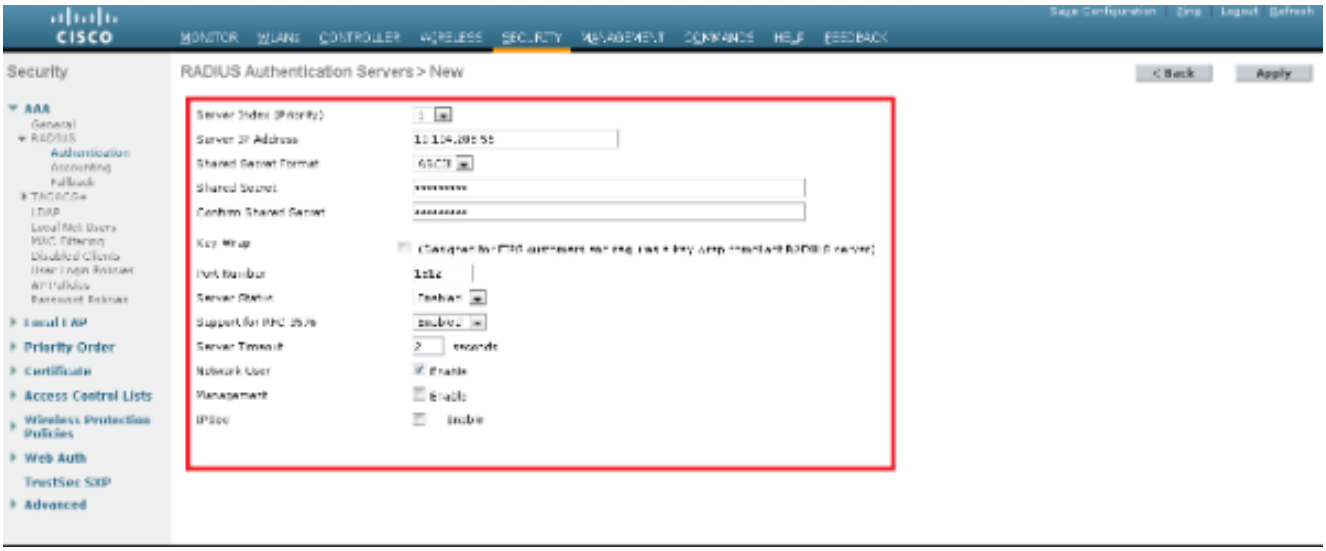
1. Configure el WLC para los dos WLAN y el servidor RADIUS.
2. Configure Cisco Secure ACS.
3. Configure los clientes inalámbricos y verifique la configuración.

Configurar la WLC

Complete estos pasos para configurar el WLC para esta configuración:

1. Configure el WLC para reenviar las credenciales del usuario a un servidor RADIUS externo. El servidor RADIUS externo (Cisco Secure ACS en este caso) valida las credenciales del usuario y proporciona acceso a los clientes inalámbricos. Complete estos pasos: Seleccione **Security > RADIUS Authentication** desde la GUI del controlador para mostrar la página RADIUS Authentication Servers .

Haga clic en **Nuevo** para definir los parámetros del servidor RADIUS. Estos parámetros incluyen la dirección IP del servidor RADIUS, el secreto compartido, el número de puerto y el estado del servidor. Las casillas de verificación Usuario de red y Administración determinan si la autenticación basada en RADIUS se aplica a los usuarios de red y de administración. Este ejemplo utiliza Cisco Secure ACS como el servidor RADIUS con la dirección IP 10.104.208.56.



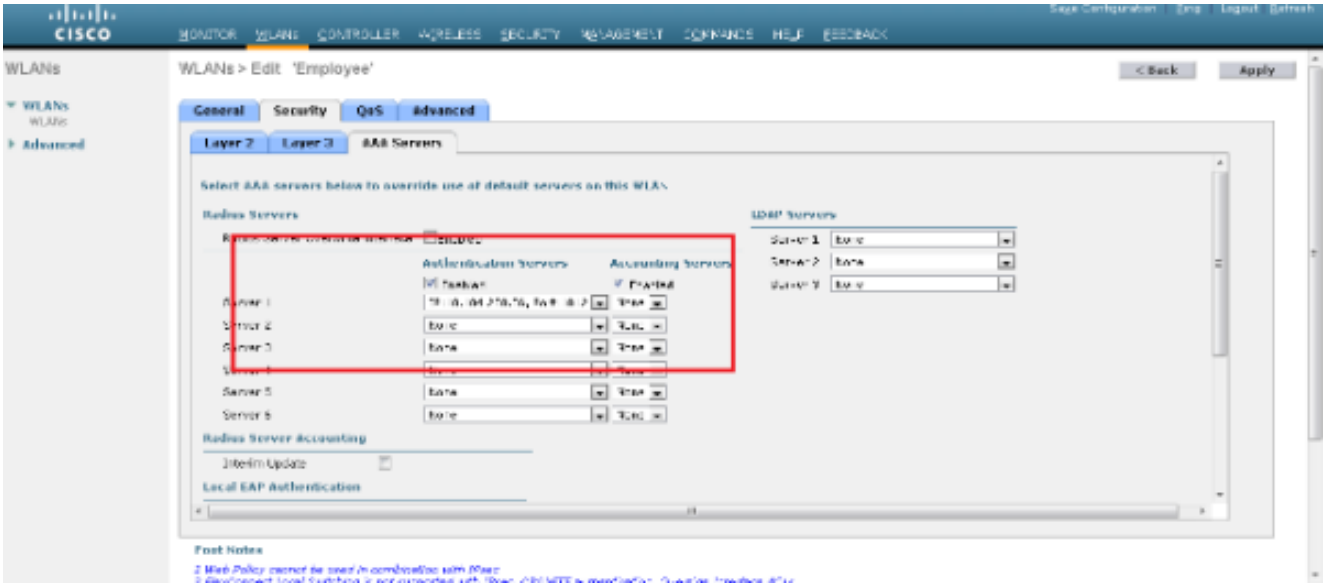
Haga clic en Apply (Aplicar).

2. Complete estos pasos para configurar una WLAN para el Empleado con **Empleado** SSID y la otra WLAN para Contratistas con **Contratista** SSID. Haga clic en **WLAN en la GUI para crear**

una WLAN. Aparece la ventana WLAN. Esta ventana enumera las WLAN configuradas en el controlador.Haga clic en **Nuevo para configurar una WLAN nueva.**Este ejemplo crea una WLAN denominada Employee y el ID de WLAN es 1. Haga clic en Apply (Aplicar).

Seleccione la ventana **WLAN > Edit** y defina los parámetros específicos de la WLAN: En la pestaña Layer 2 Security , seleccione **802.1x**. De forma predeterminada, la opción de seguridad de capa 2 es 802.1x. Esto habilita las autenticaciones 802.1 x/protocolo de autenticación extensible (EAP) para la WLAN.

En la pestaña de servidores AAA, seleccione el servidor RADIUS apropiado de la lista desplegable en Servidores RADIUS. Los otros parámetros se pueden modificar en función de los requisitos de la red WLAN. Haga clic en Apply (Aplicar).



Del mismo modo, para crear una WLAN para los contratistas, repita los pasos b a d.

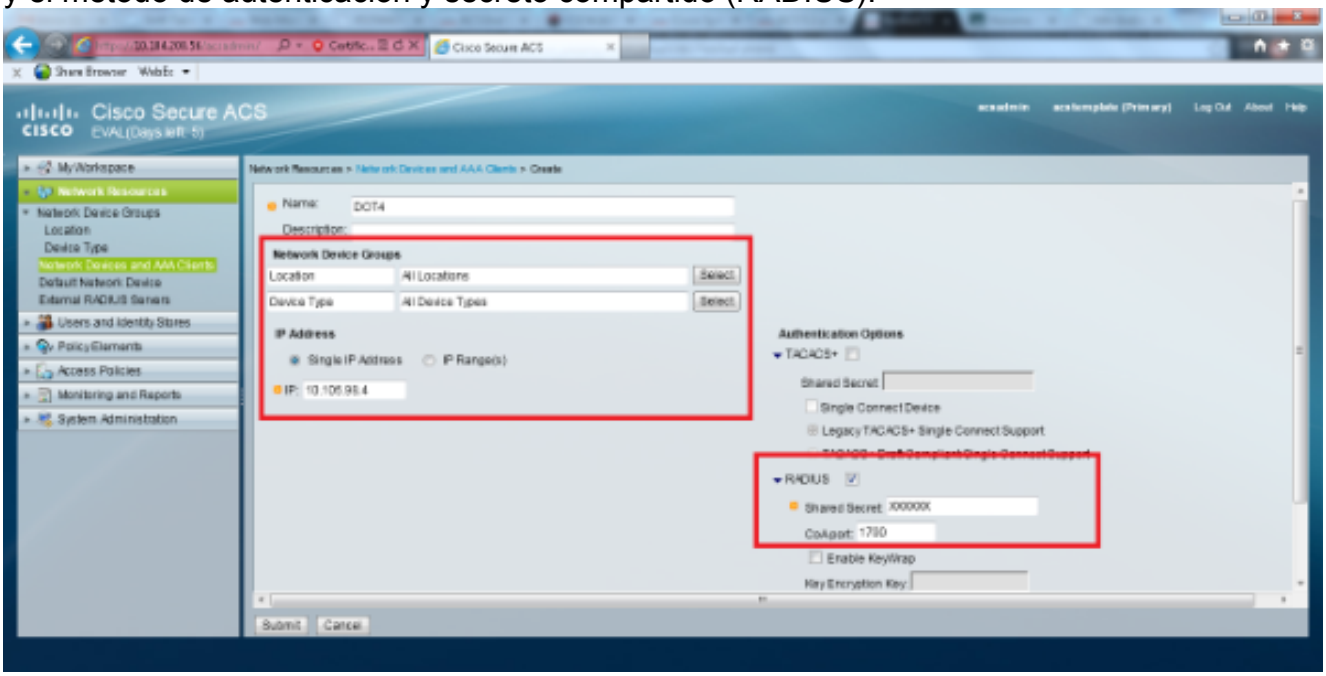
Configuración de Cisco Secure ACS

En el servidor Cisco Secure ACS, debe:

1. Configure el WLC como un cliente AAA.
2. Cree la base de datos de usuario (Credenciales) para la autenticación basada en SSID.
3. Habilite la autenticación EAP.

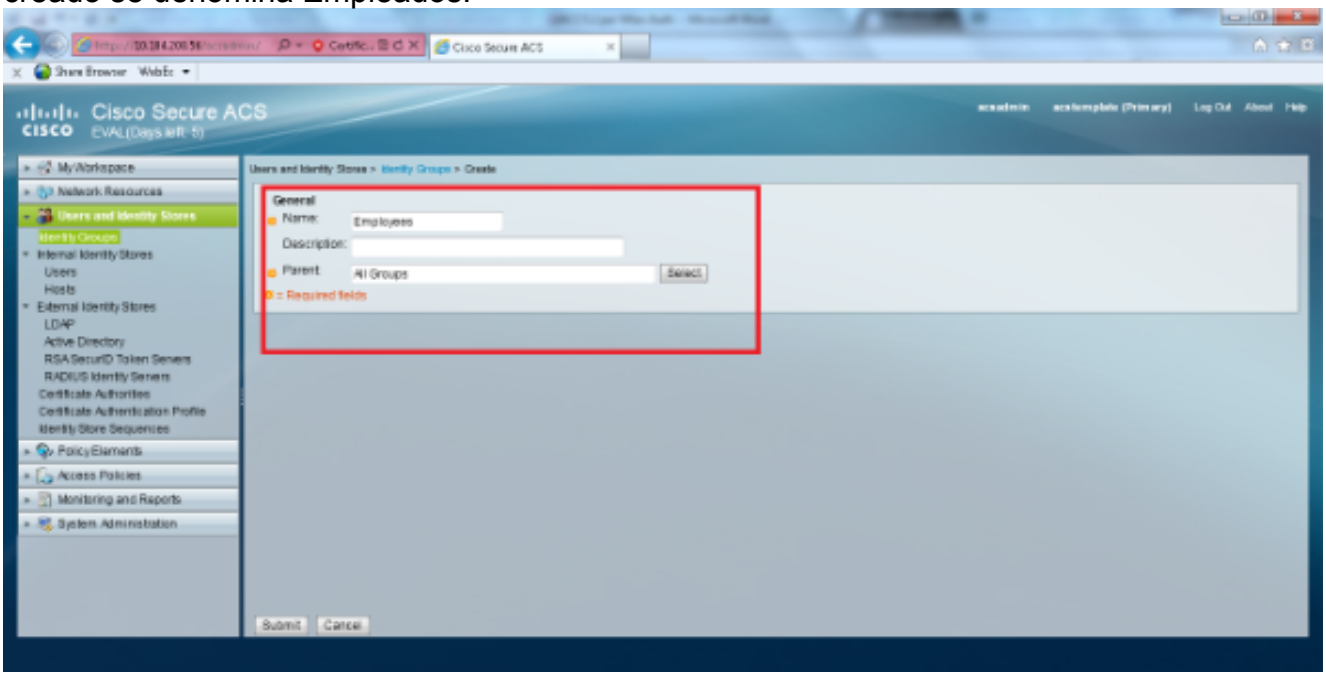
Complete estos pasos en Cisco Secure ACS:

1. Para definir el controlador como un cliente AAA en el servidor ACS, seleccione **Recursos de Red > Dispositivos de Red y Clientes AAA** de la GUI ACS. En Network Devices y AAA Clients**,** haga clic en **Create.**
2. Cuando aparezca la página Configuración de red, defina el nombre del WLC, la dirección IP y el método de autenticación y secreto compartido (RADIUS).

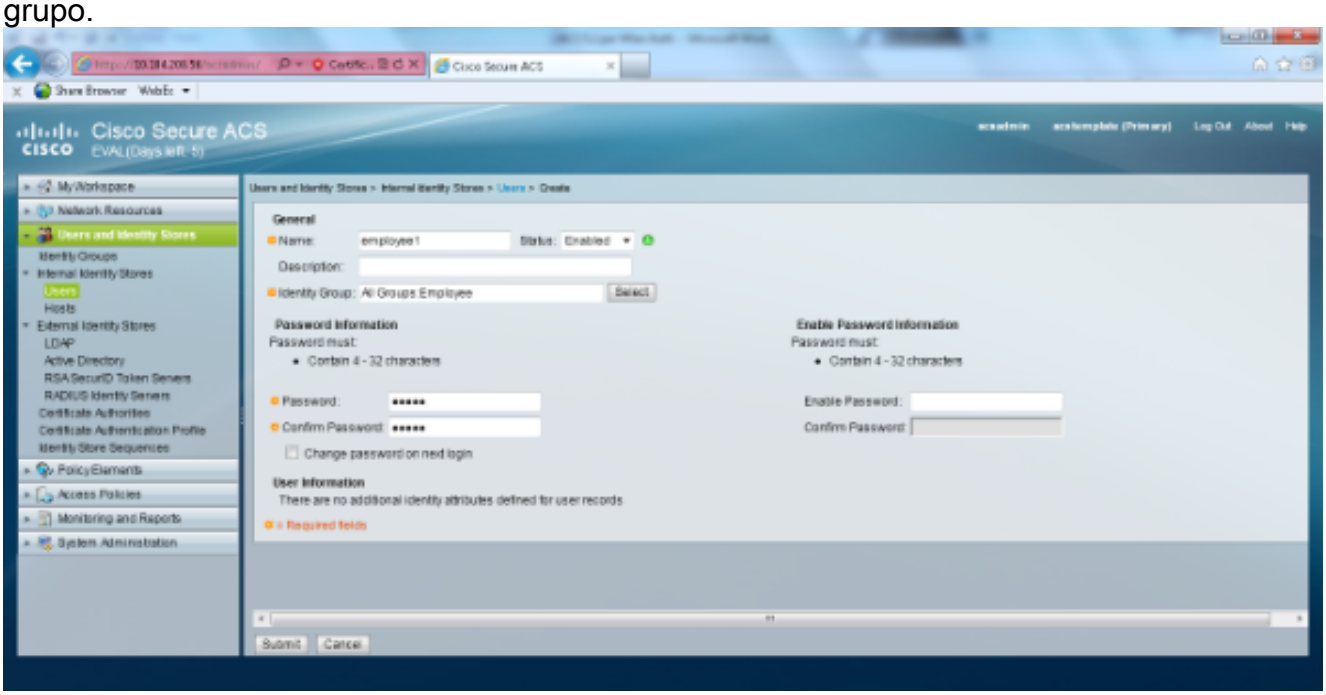


3. Seleccione **Users and Identity Stores > Identity Groups** en la GUI de ACS. Cree los grupos respectivos para Empleado y Contratista y haga clic en **Crear**. En este ejemplo, el grupo

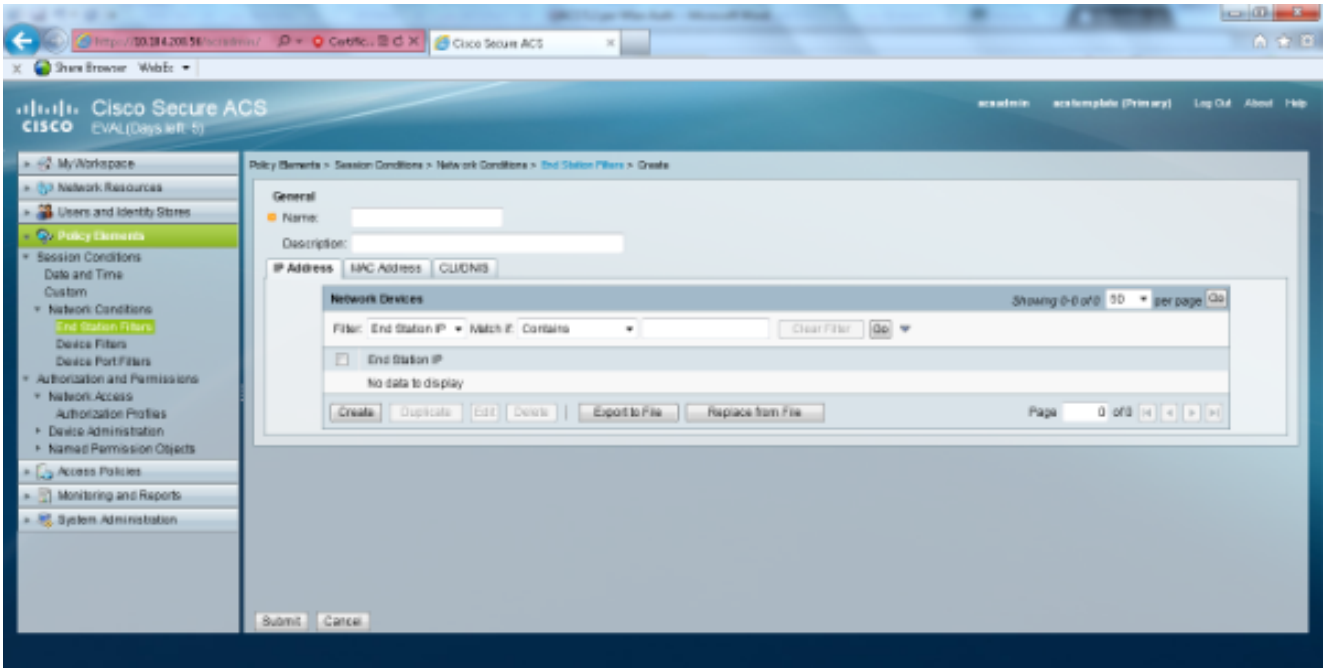
creado se denomina Empleados.



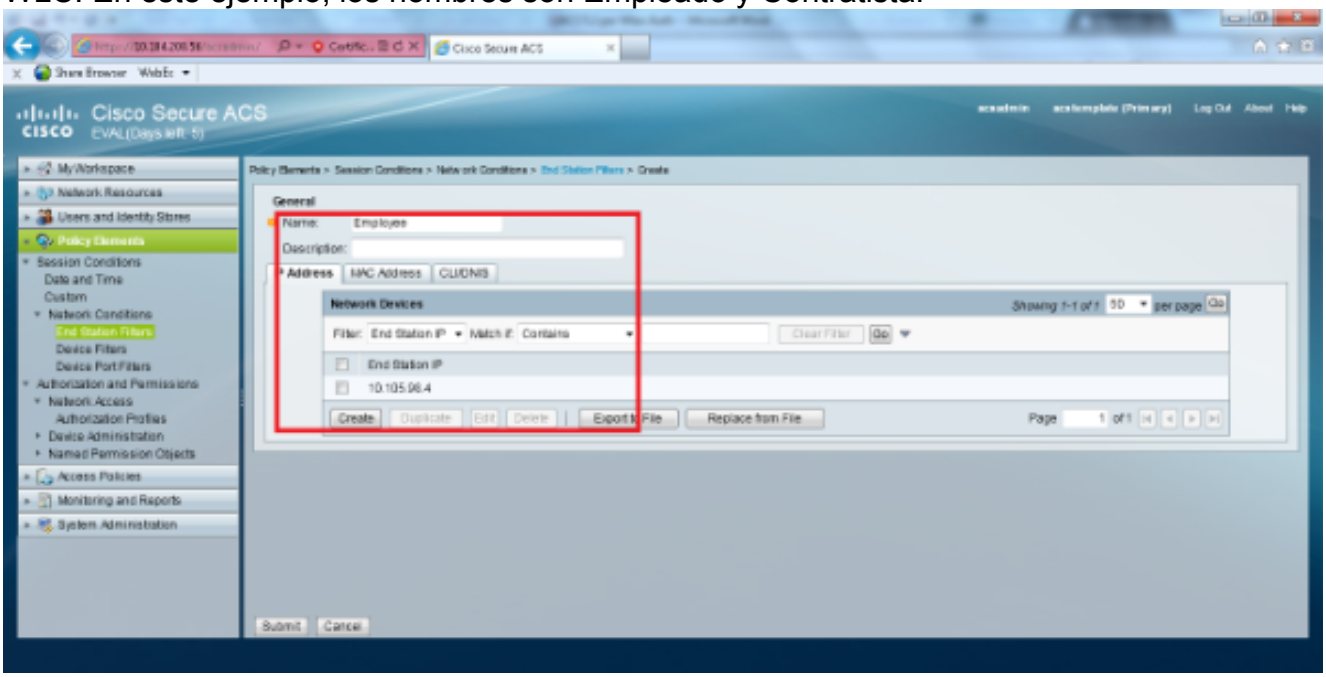
4. Seleccione **Users and Identity Stores > Internal Identity Stores**. Haga clic en **Crear** e ingrese el nombre de usuario. Colóquelos en el grupo correcto, defina su contraseña y haga clic en **Enviar**.En este ejemplo se crea un usuario denominado empleado1 en el grupo Empleado. Del mismo modo, cree un usuario denominado contratista1 en los contratistas del grupo.



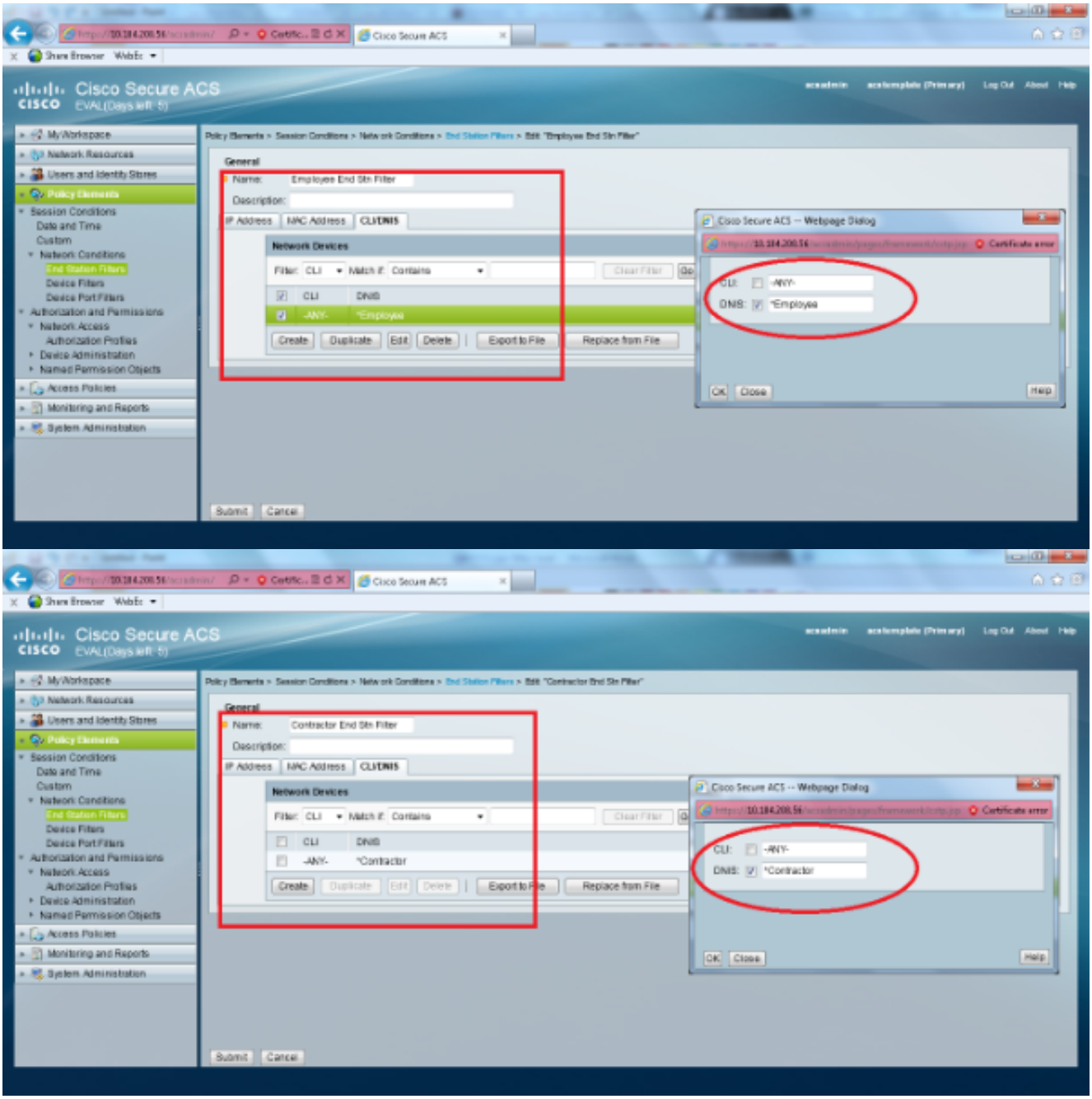
5. Seleccione **Elementos de política > Condiciones de red > Filtros de estación final**. Haga clic en **Crear**.



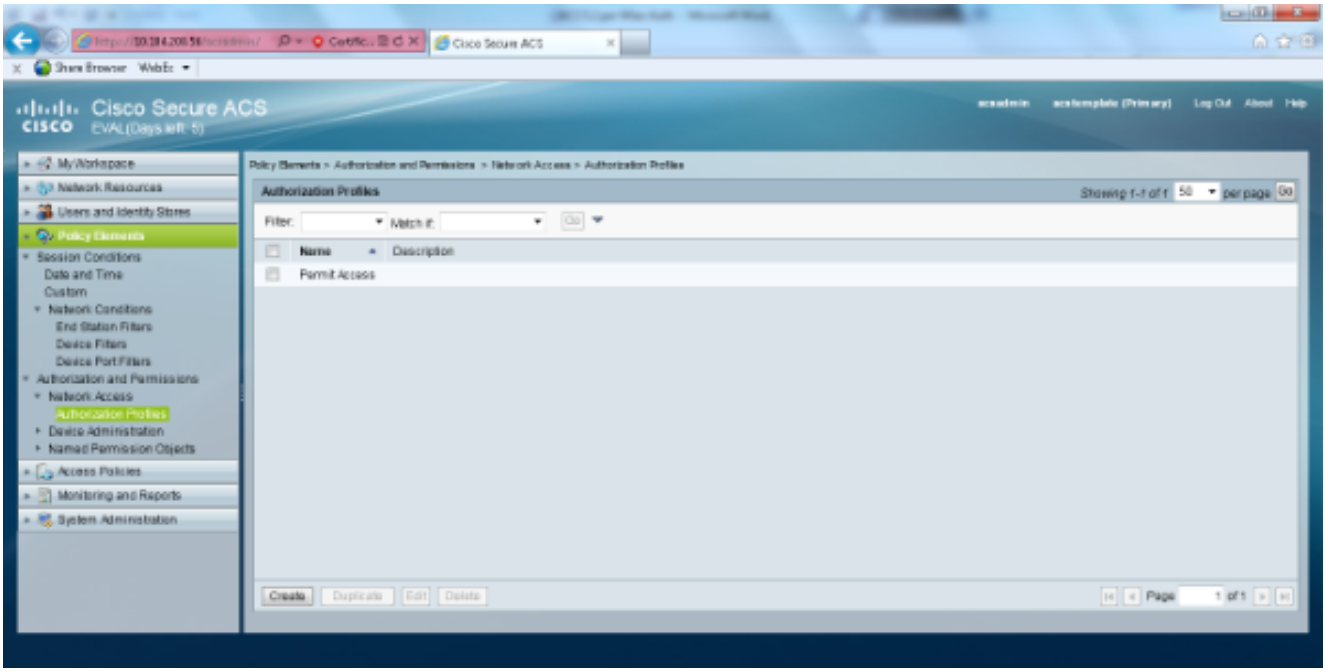
Ingrese un nombre significativo y bajo la pestaña **dirección IP** ingrese la dirección IP del WLC. En este ejemplo, los nombres son Empleado y Contratista.



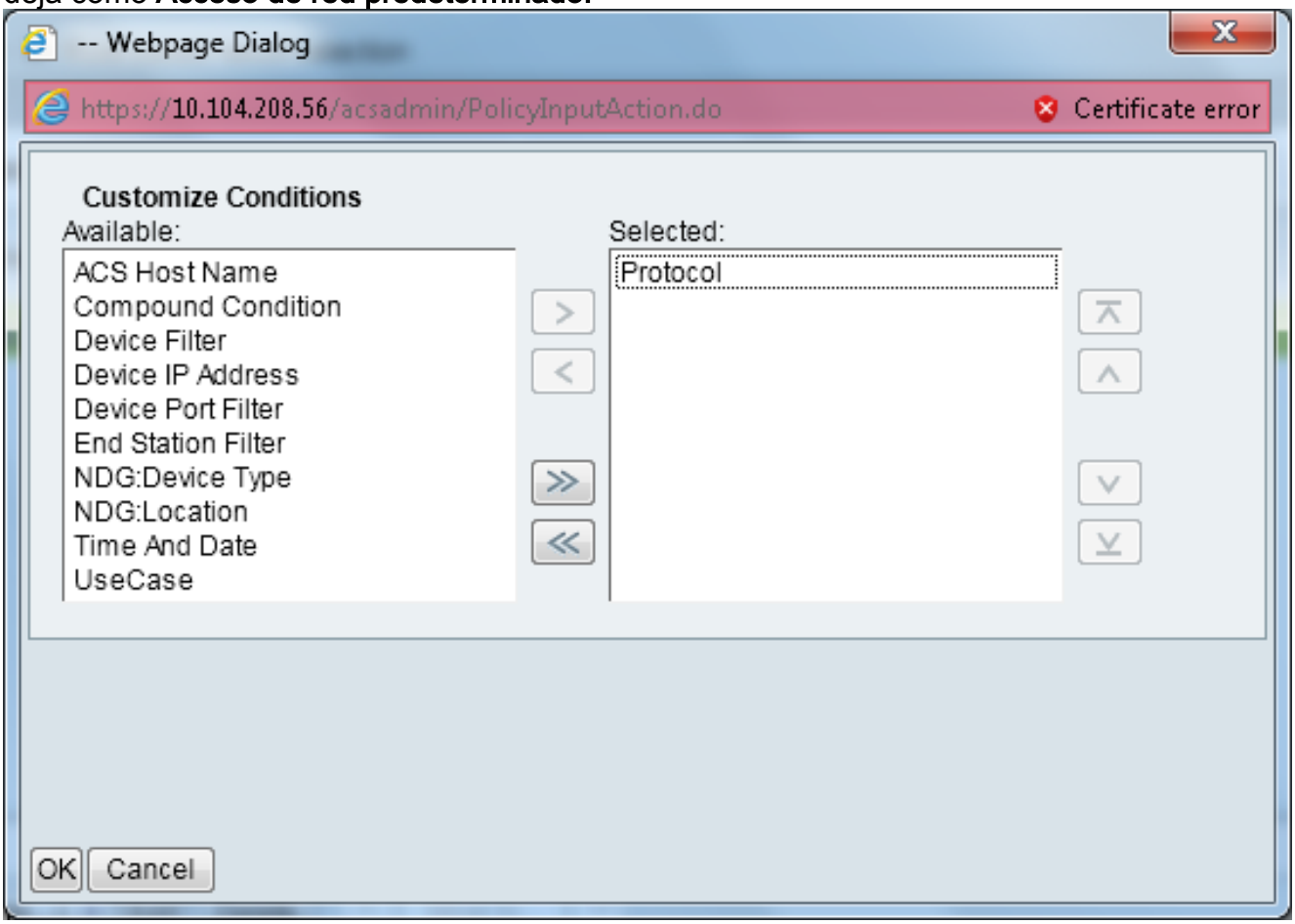
En la ficha CLI/DNIS, deje CLI como -ANY- e introduzca DNIS como *<SSID>. En este ejemplo, el campo DNIS se introduce como *Empleado, ya que este filtro de estación final se utiliza para restringir el acceso sólo a la WLAN del empleado. El atributo DNIS define el SSID al que el usuario puede acceder. El WLC envía el SSID en el atributo DNIS al servidor RADIUS.Repita los mismos pasos para el filtro de la estación final del contratista.

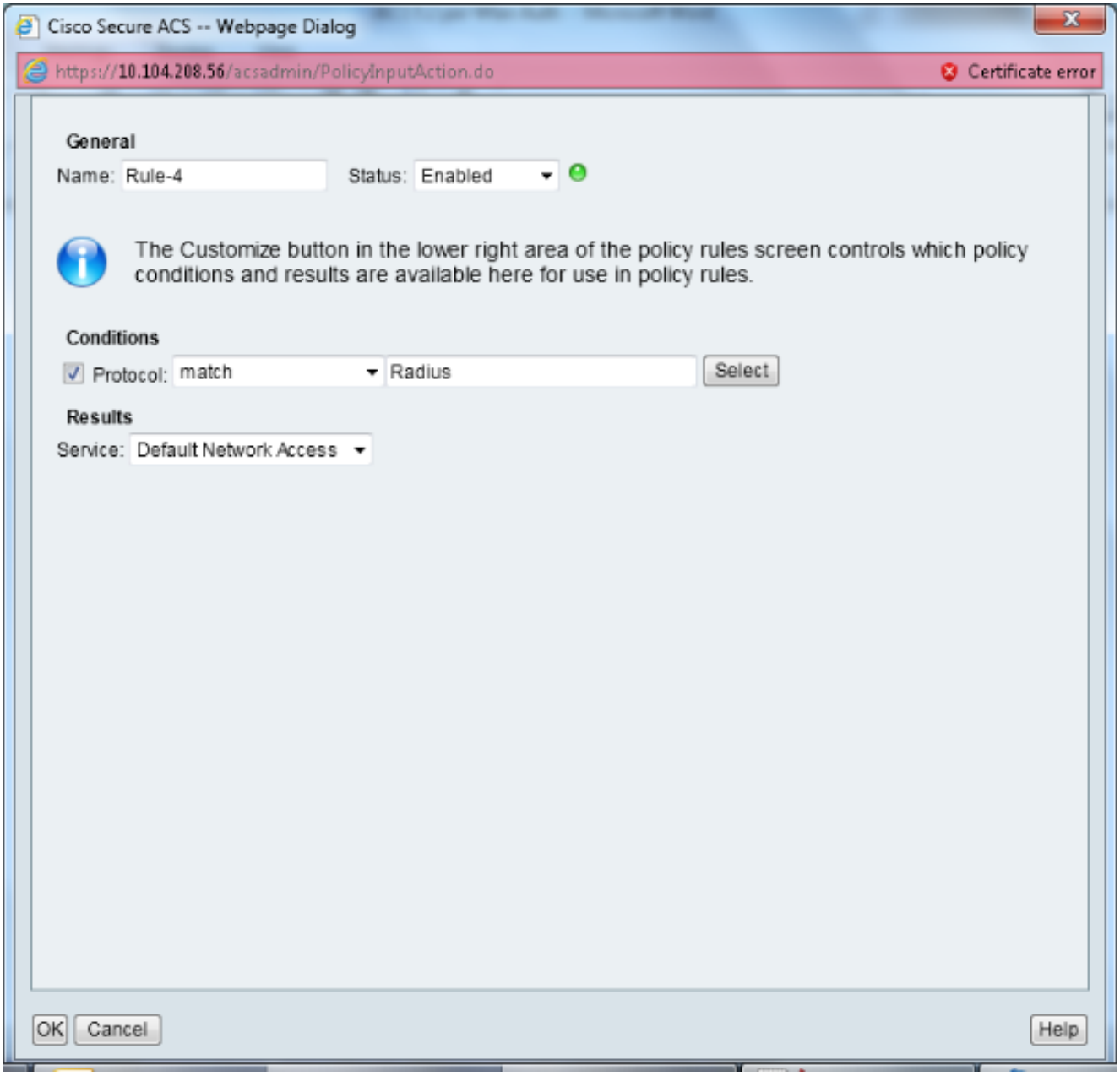


6. Seleccione **Elementos de política > Autorización y permisos > Acceso de red > Perfiles de autorización**. Debe haber un perfil predeterminado para Permit Access (Permitir acceso).

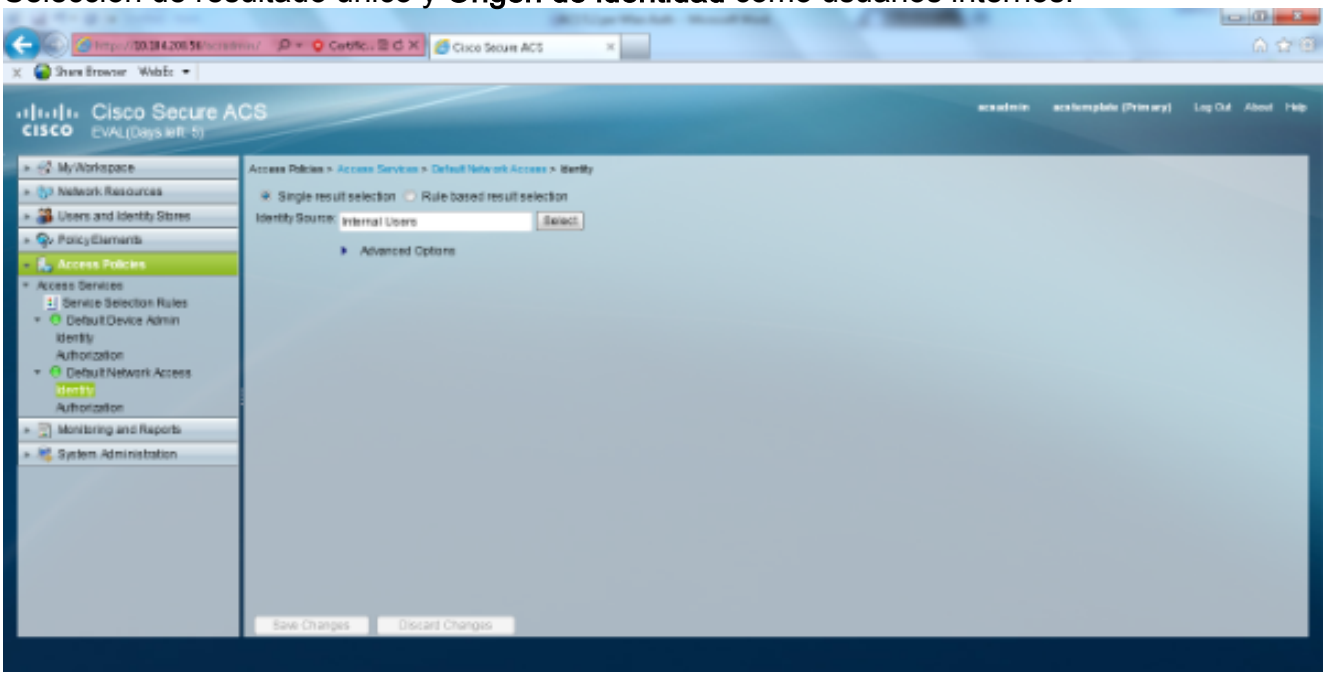


7. Seleccione **Access Policies > Access Services > Service Selection Rules**. Haga clic en **Personalizar**. Agregue cualquier condición adecuada. Este ejemplo utiliza Protocol as Radius como condición coincidente.Haga clic en **Crear**. Nombre la regla. Seleccione **Protocol** y seleccione **Radius.**En **Resultados**, elija el servicio de acceso adecuado. En este ejemplo, se deja como **Acceso de red predeterminado.**

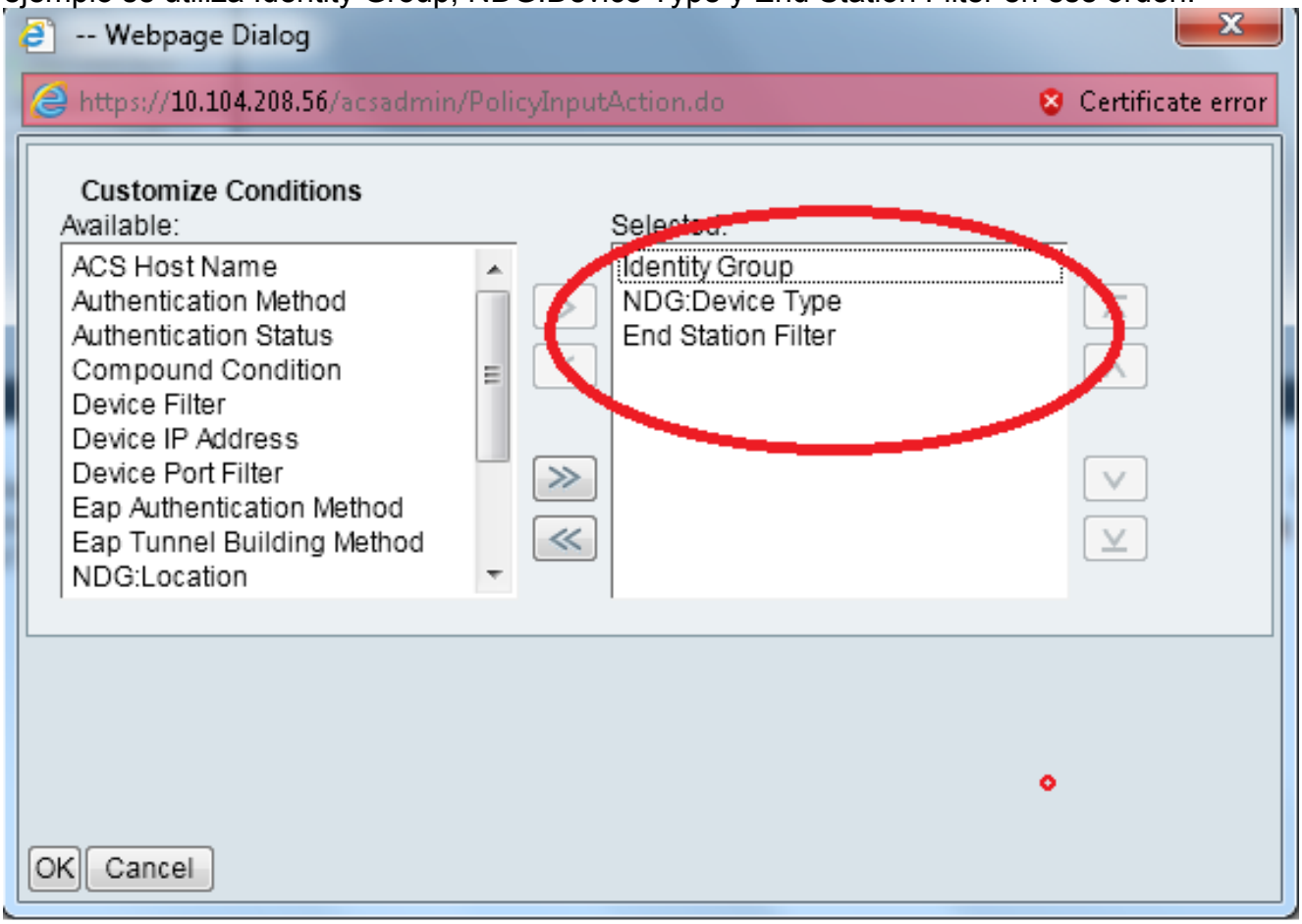




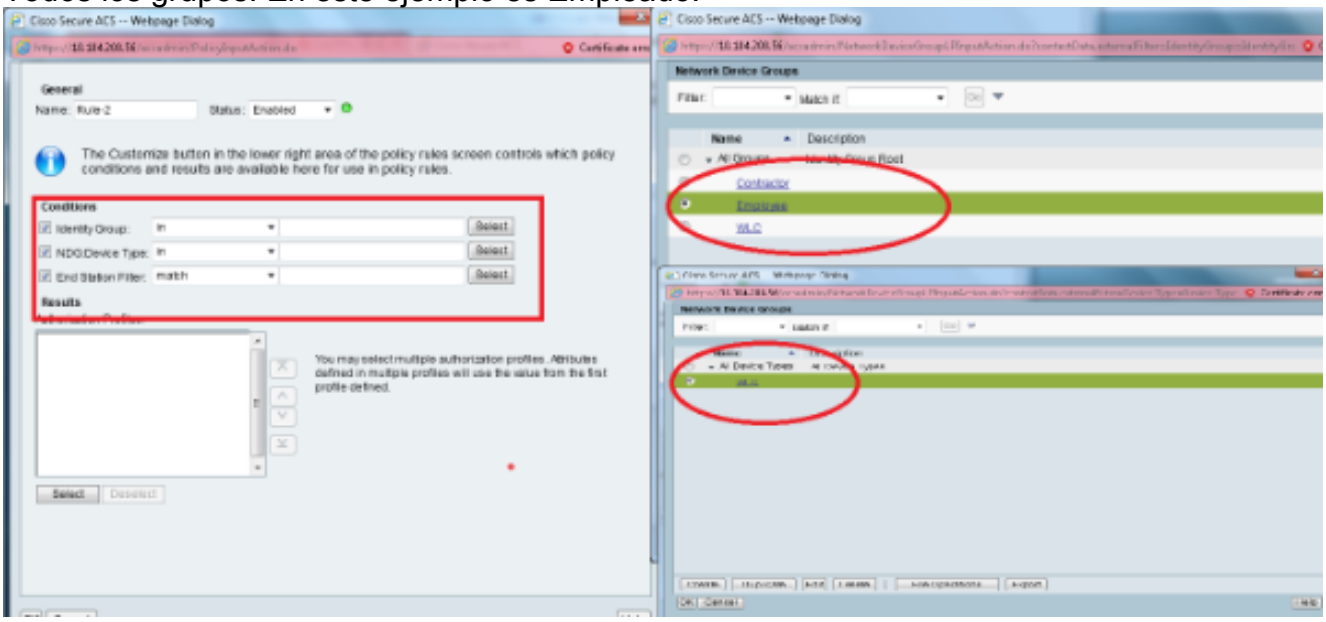
8. Seleccione **Access Policies > Access Services > Default Network Access > Identity** . Elija Selección de resultado único y **Origen de identidad** como usuarios internos.



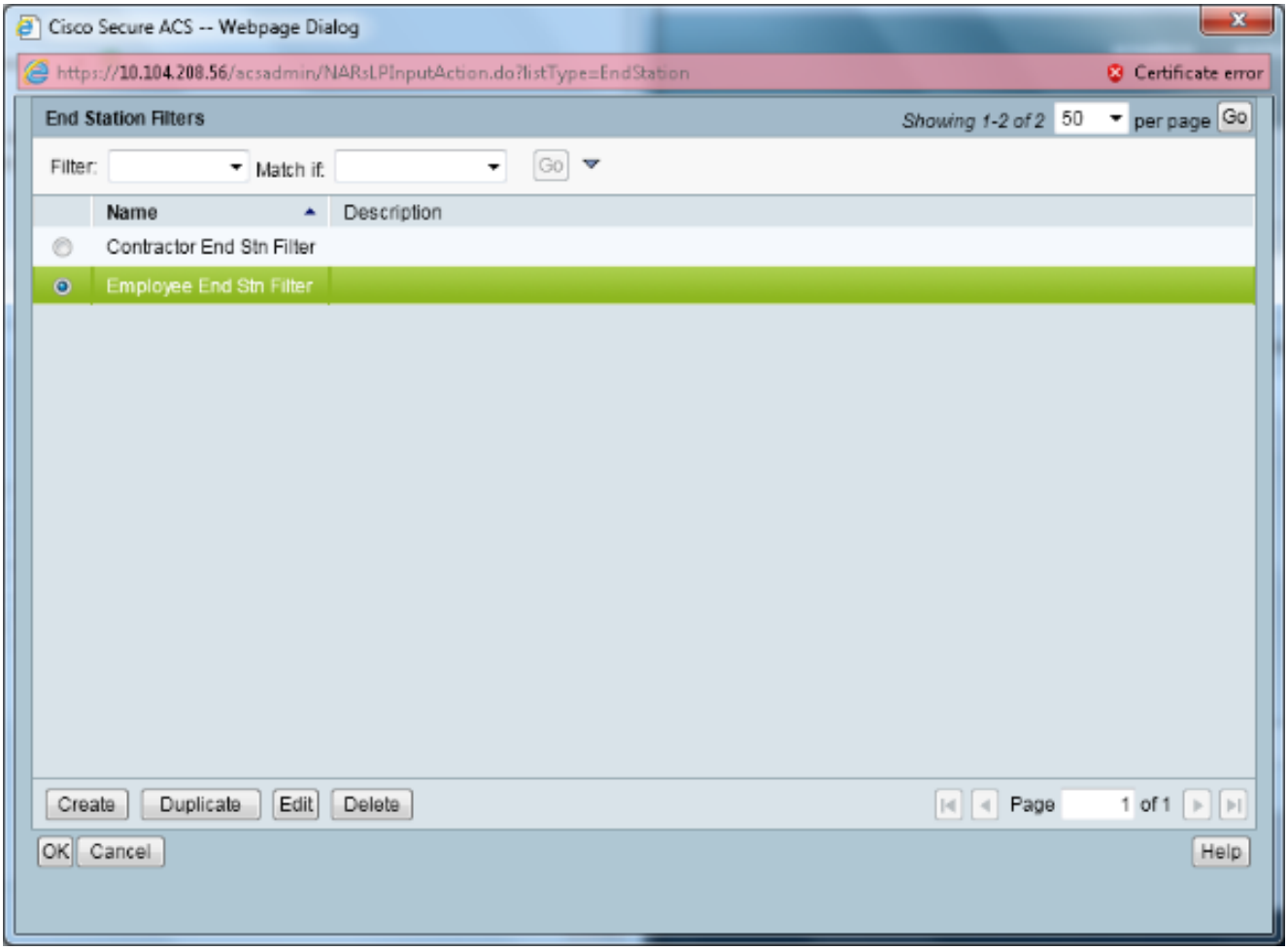
Seleccione **Access Policies > Access Services > Default Network Access > Authorization.** Haga clic en **Personalizar** y agregue las condiciones Personalizadas. En este ejemplo se utiliza Identity Group, NDG:Device Type y End Station Filter en ese orden.



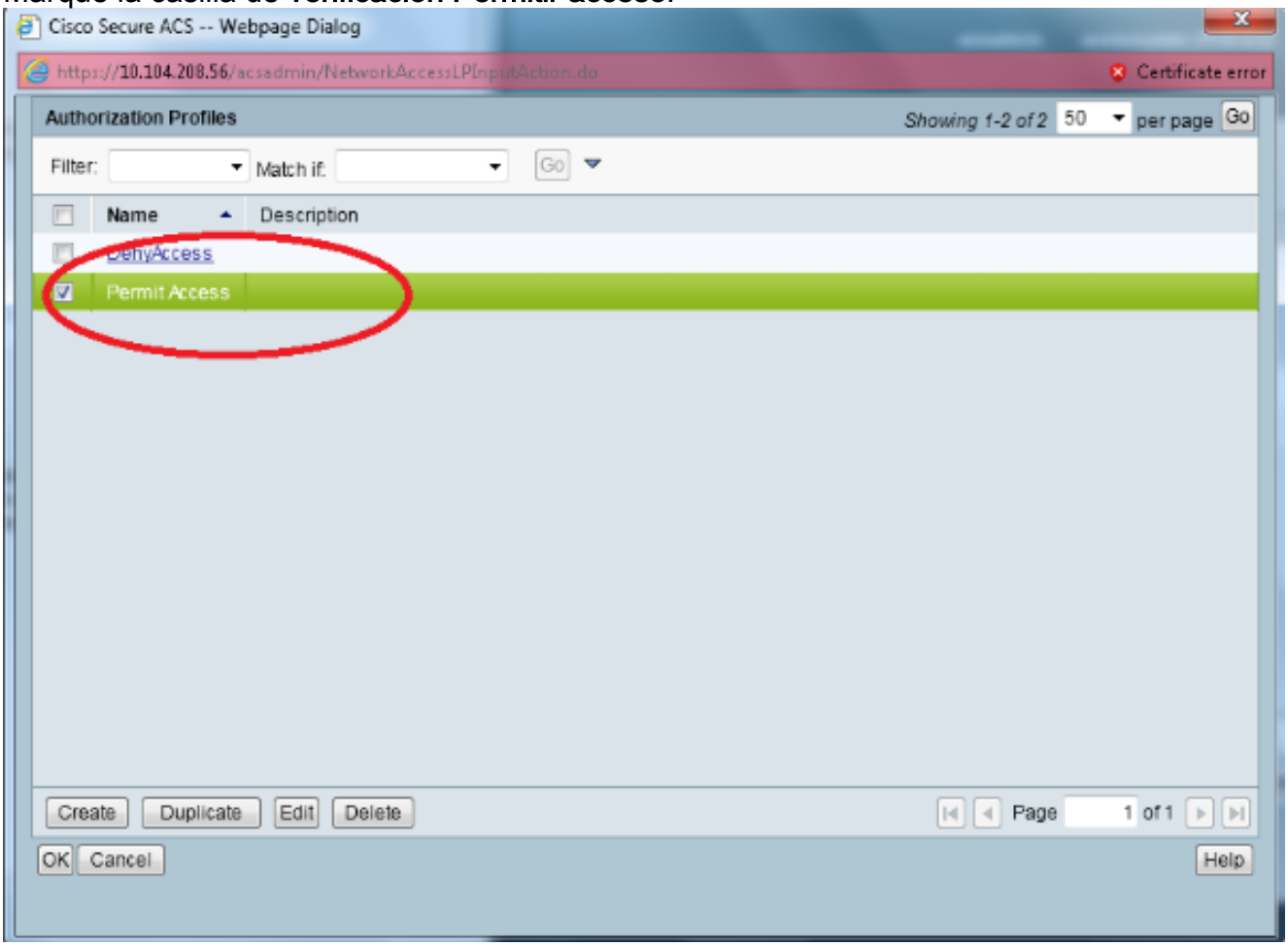
Haga clic en **Crear**. Asigne un nombre a la regla y elija el grupo de identidad adecuado en Todos los grupos. En este ejemplo es Empleado.



Haga clic en el botón de radio **Employee End Stn Filter** o ingrese el nombre que ingresó en el Paso1b en la sección "Configure the WLC".

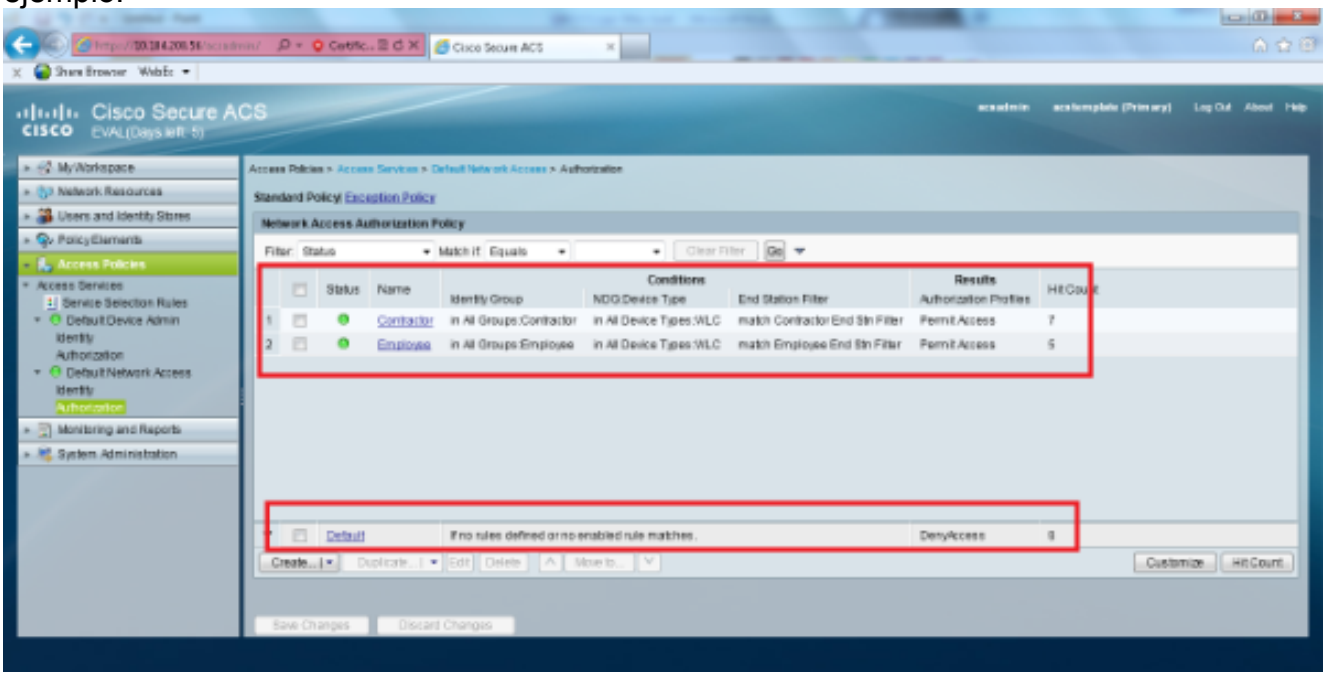


Marque la casilla de **verificación Permitir acceso**.



Repita los mismos pasos anteriores para las Reglas del Contratista. Asegúrese de que la

acción predeterminada es **Denegar acceso**. Una vez que haya completado el paso e, las reglas deben verse como en este
ejemplo:



Esto concluye la configuración. Después de esta sección, el cliente necesita ser configurado en consecuencia con el SSID y los parámetros de seguridad para conectarse.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.