

Configuración de ACS 5.2 para la autenticación basada en puerto con un LAP

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Suposición](#)

[Configuration Steps](#)

[Configurar LAP](#)

[Configurar switch](#)

[Configurar servidor RADIUS](#)

[Configurar recursos de red](#)

[Configurar usuarios](#)

[Definición de elementos de política](#)

[Aplicar políticas de acceso](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar un Lightweight Access Point (LAP) como supplicant 802.1x para autenticarse en un servidor RADIUS como un Access Control Server (ACS) 5.2.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar realizar esta configuración:

- Conocimiento básico del controlador de LAN inalámbrica (WLC) y los LAP.
- Tener conocimiento funcional del servidor AAA.
- Poseer un conocimiento profundo de las redes inalámbricas y de los problemas de seguridad inalámbrica.

Componentes Utilizados

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

- Cisco 5508 WLC que ejecuta la versión 7.0.220.0 del firmware

- LAP de la serie 3502 de Cisco
- Cisco Secure ACS que ejecuta la versión 5.2
- Switch Cisco serie 3560

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

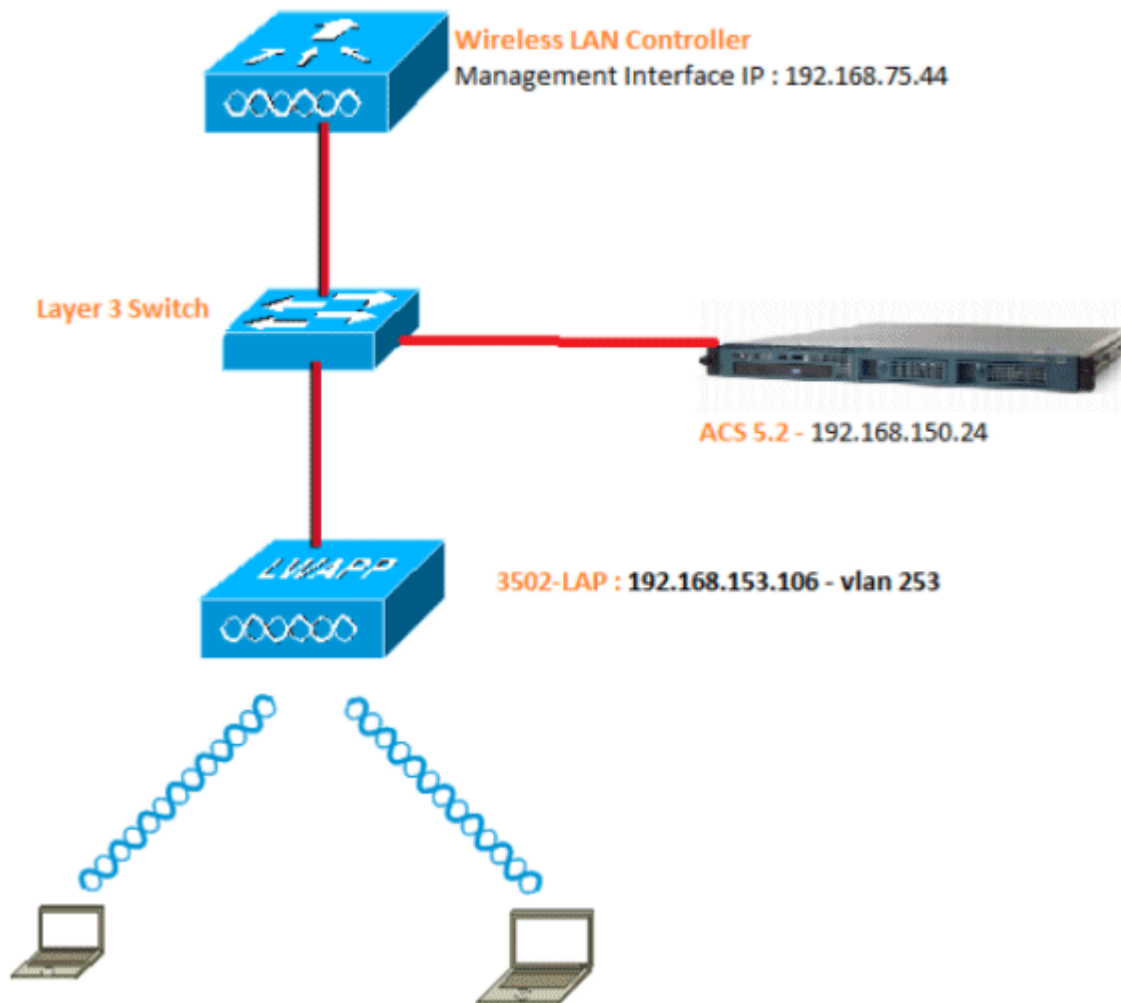
Los LAP tienen instalados de fábrica certificados X.509 - firmados por una clave privada - que se queman en el dispositivo en el momento de la fabricación. Los LAP utilizan este certificado para autenticarse con el WLC en el proceso de unión. Este método describe otra manera de autenticar los LAPs. Con el software WLC, puede configurar la autenticación 802.1x entre un punto de acceso (AP) Cisco Aironet y un switch Cisco. En este caso, el AP actúa como el suplicante 802.1x y es autenticado por el switch contra un servidor RADIUS (ACS) que utiliza EAP-FAST con aprovisionamiento PAC anónimo. Una vez configurado para la autenticación 802.1x, el switch no permite que ningún tráfico que no sea el tráfico 802.1x pase a través del puerto hasta que el dispositivo conectado al puerto se autentique correctamente. Un AP se puede autenticar antes de que se una a un WLC o después de que se haya unido a un WLC, en cuyo caso usted configura 802.1x en el switch después de que el LAP se une al WLC.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Estos son los detalles de configuración de los componentes utilizados en este diagrama:

- La dirección IP del servidor ACS (RADIUS) es 192.168.150.24.
- La dirección de la interfaz de administración y del administrador AP del WLC es 192.168.75.44.
- Los servidores DHCP dirigen 192.168.150.25.
- LAP se coloca en VLAN 253.
- VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.10
- VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

Suposición

- Los switches se configuran para todas las VLAN de Capa 3.
- Al servidor DHCP se le asigna un ámbito DHCP.
- Existe conectividad de capa 3 entre todos los dispositivos de la red.
- El LAP ya está unido al WLC.
- Cada VLAN tiene una máscara /24.

- ACS 5.2 tiene instalado un certificado autofirmado.

Configuration Steps

Esta configuración se divide en tres categorías:

1. [Configure el LAP.](#)
2. [Configure el switch.](#)
3. [Configure el servidor RADIUS.](#)

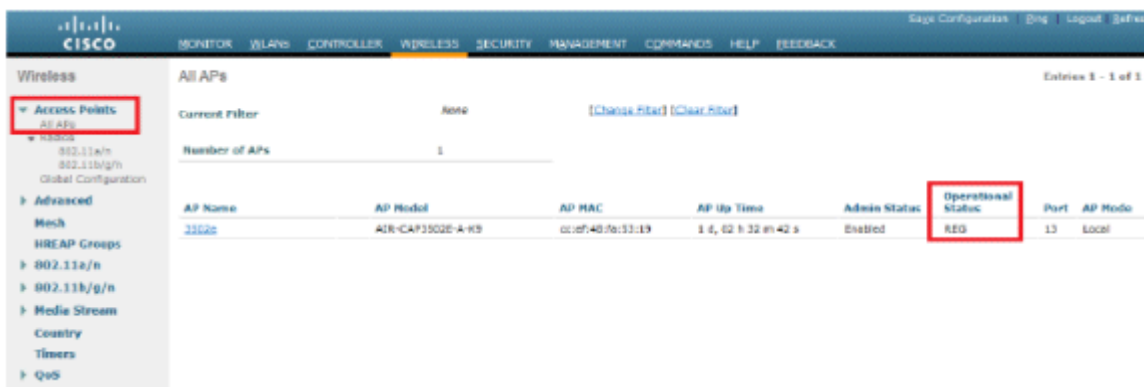
Configurar LAP

Suposiciones

El LAP ya está registrado al WLC usando la opción 43, el DNS, o la IP estáticamente configurada de la interfaz de la administración del WLC.

Complete estos pasos:

1. Vaya a **Inalámbrico > Puntos de acceso > Todos los APs** para verificar el registro del LAP en el WLC.



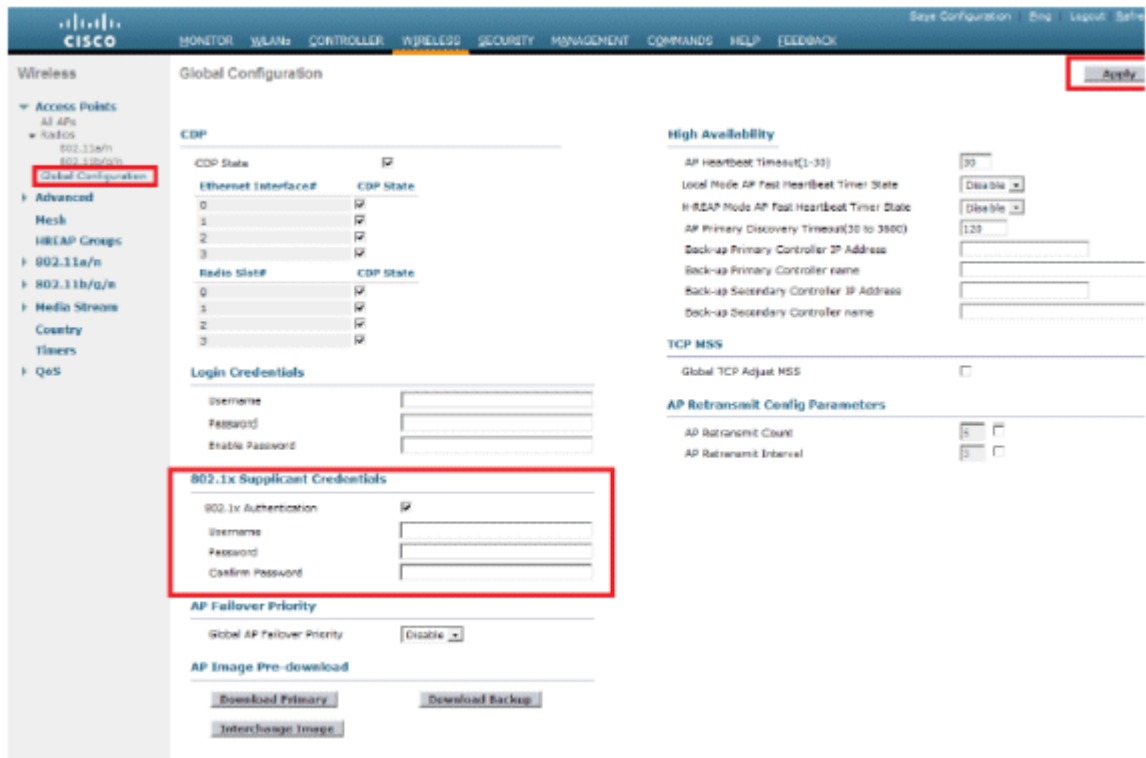
The screenshot shows the Cisco WLC configuration interface. The 'Wireless' menu is expanded, and 'Access Points' is selected. The 'All APs' page displays a table with the following data:

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode
3362e	AIR-CT5502E-A-K9	cc:ef:48:7a:51:19	1 d, 02 h 32 m 42 s	Enabled	REG	13	Local

2. Puede configurar las credenciales 802.1x (es decir, nombre de usuario/contraseña) para todos los LAP de dos maneras:

- **Globalmente**

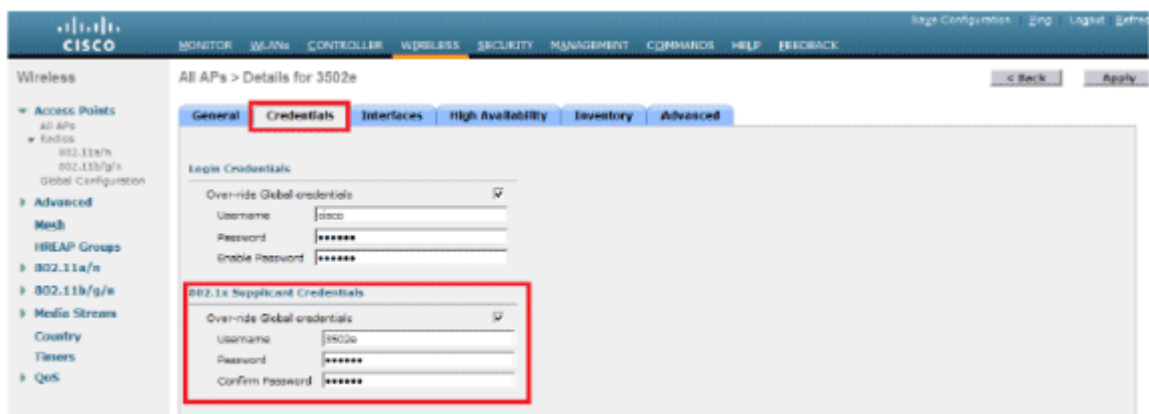
Para un LAP ya unido, puede establecer las credenciales globalmente para que cada LAP que se une al WLC herede esas credenciales.



- **Individualmente**

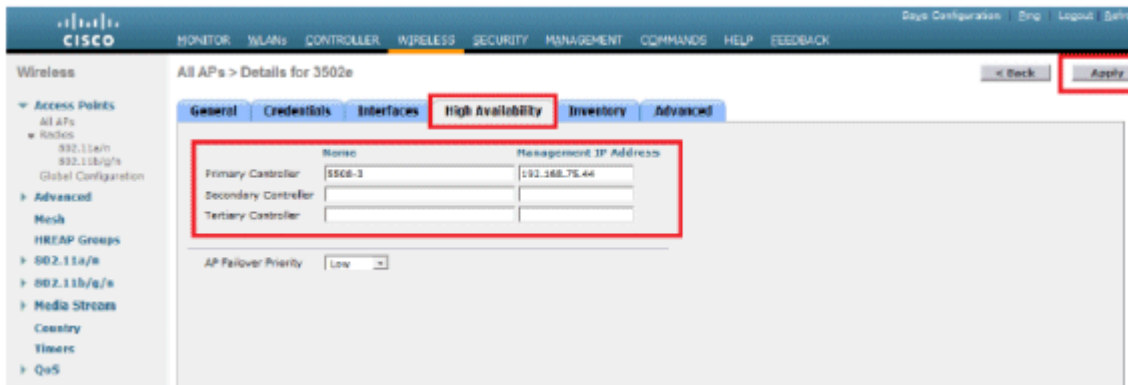
Configuración de perfiles 802.1 x por AP. En nuestro ejemplo, configuraremos las credenciales por AP.

- Vaya a **Wireless > All APs**, y seleccione el AP correspondiente.
- Agregue el nombre de usuario y la contraseña en los campos **802.1x Supplicant Credentials**.



Nota: Las credenciales de inicio de sesión se utilizan para Telnet, SSH o la consola en el AP.

3. Configure la sección High Availability y haga clic en **Apply**.



Nota: Una vez guardadas, estas credenciales se retienen en el WLC y el AP se reinicia. Las credenciales cambian solamente cuando el LAP se une a un nuevo WLC. El LAP asume el nombre de usuario y la contraseña que fueron configurados en el nuevo WLC.

Si el AP aún no se ha unido a un WLC, debe iniciar la consola en el LAP para establecer las credenciales. Ejecute este comando CLI en el modo de habilitación:

```
LAP#lwapp ap dot1x username <username> password <password>
```

or

```
LAP#capwap ap dot1x username <username> password <password>
```

Nota: Este comando está disponible solamente para los AP que ejecutan la imagen de recuperación.

El nombre de usuario y la contraseña predeterminados para el LAP son cisco y Cisco, respectivamente.

Configurar switch

El switch actúa como un autenticador para el LAP y autentica el LAP contra un servidor RADIUS. Si el switch no tiene el software compatible, actualice el switch. En la CLI del switch, ejecute estos comandos para habilitar la autenticación 802.1x en un puerto del switch:

```
<#root>
```

```
switch#
```

```
configure terminal
```

```
switch(config)#
```

```
dot1x system-auth-control
```

```
switch(config)#
```

```
aaa new-model
```

```
!--- Enables 802.1x on the Switch.
```

```
switch(config)#
```

```
aaa authentication dot1x default group radius
```

```
switch(config)#
```

```
radius server host 192.168.150.24 key cisco
```

!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x information

```
switch(config)#
```

```
ip radius source-interface vlan 253
```

!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.

```
switch(config)interface gigabitEthernet 0/11
```

```
switch(config-if)switchport mode access
```

```
switch(config-if)switchport access vlan 253
```

```
switch(config-if)mls qos trust dscp
```

```
switch(config-if)spanning-tree portfast
```

!--- gig0/11 is the port number on which the AP is connected.

```
switch(config-if)dot1x pae authenticator
```

!--- Configures dot1x authentication.

```
switch(config-if)dot1x port-control auto
```

!--- With this command, the switch initiates the 802.1x authentication.

Nota: Si tiene otros AP en el mismo switch y no desea que utilicen 802.1x, puede dejar el puerto sin configurar para 802.1x o ejecutar este comando:

```
<#root>
```

```
switch(config-if)authentication port-control force-authorized
```

Configurar servidor RADIUS

El LAP se autentica con EAP-FAST. Asegúrese de que el servidor RADIUS que utiliza admite este método EAP si no utiliza Cisco ACS 5.2.

La configuración del servidor RADIUS se divide en cuatro pasos:

1. [Configure los recursos de red.](#)
2. [Configurar usuarios.](#)
3. [Definir elementos de política.](#)
4. [Aplique políticas de acceso.](#)

ACS 5.x es un ACS basado en políticas. En otras palabras, ACS 5.x utiliza un modelo de política basado en reglas en lugar del modelo basado en grupos utilizado en las versiones 4.x.

El modelo de políticas basadas en reglas ACS 5.x proporciona un control de acceso más potente y flexible

en comparación con el antiguo enfoque basado en grupos.

En el modelo basado en grupos más antiguo, un grupo define la política porque contiene y une tres tipos de información:

- **Información de identidad:** esta información puede estar basada en la pertenencia a grupos AD o LDAP o en una asignación estática para usuarios internos de ACS.
- **Otras restricciones o condiciones:** restricciones de tiempo, restricciones de dispositivos, etc.
- **Permisos:** VLAN o niveles de privilegio de Cisco IOS®.

El modelo de políticas de ACS 5.x se basa en reglas con el formato:

Si la condición entonces resultado

Por ejemplo, utilizamos la información descrita para el modelo basado en grupos:

Si identity-condition, restricted-condition, authorization-profile.

Como resultado, esto nos da flexibilidad para limitar las condiciones en las que el usuario puede acceder a la red y también qué nivel de autorización se permite cuando se cumplen condiciones específicas.

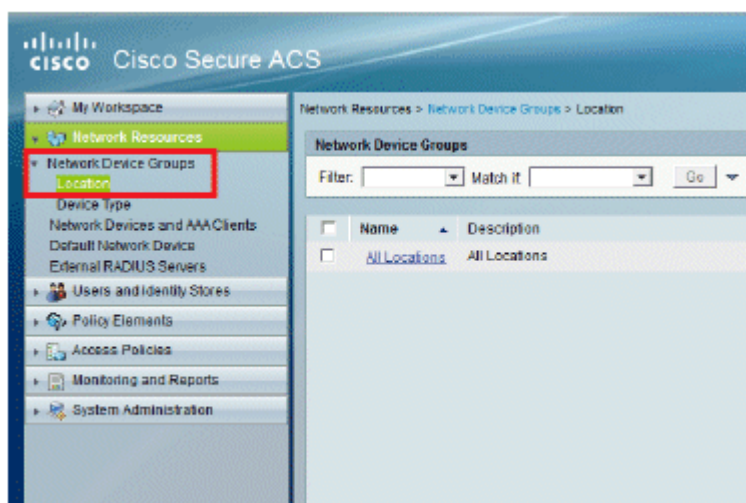
Configurar recursos de red

En esta sección, configuramos el cliente AAA para el switch en el servidor RADIUS.

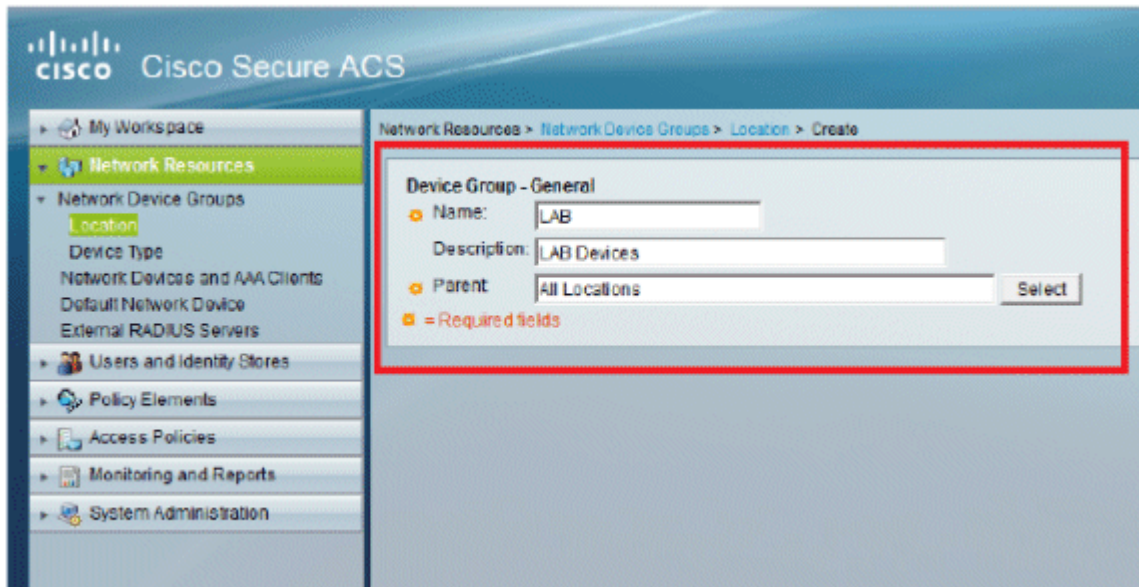
Este procedimiento explica cómo agregar el switch como cliente AAA en el servidor RADIUS para que el switch pueda pasar las credenciales de usuario del LAP al servidor RADIUS.

Complete estos pasos:

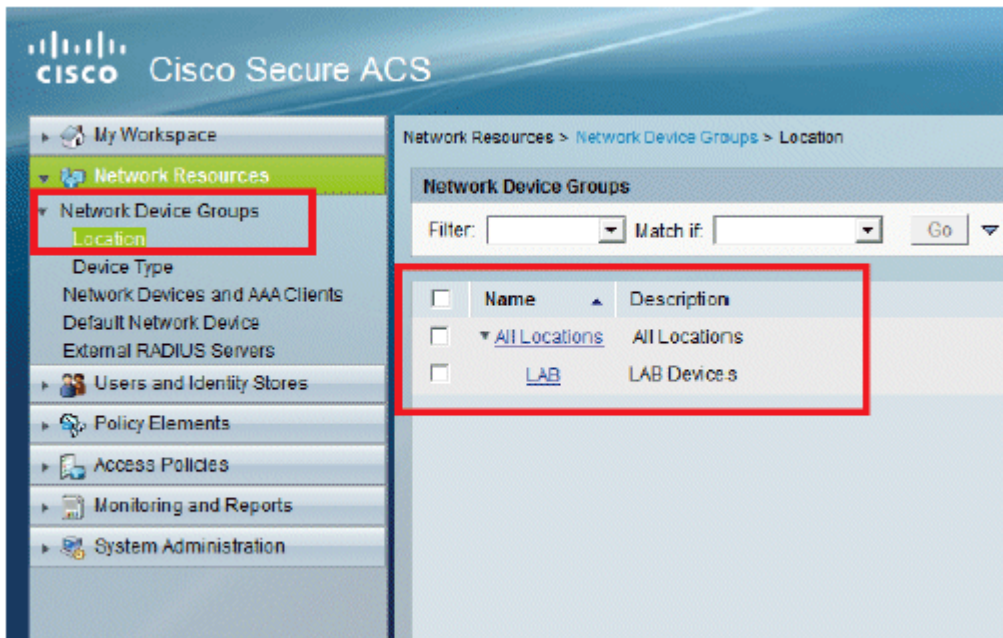
1. Desde la GUI de ACS, haga clic en **Network Resources**.
2. Haga clic en **Network Device Groups**.
3. Vaya a **Ubicación** > **Crear** (en la parte inferior).



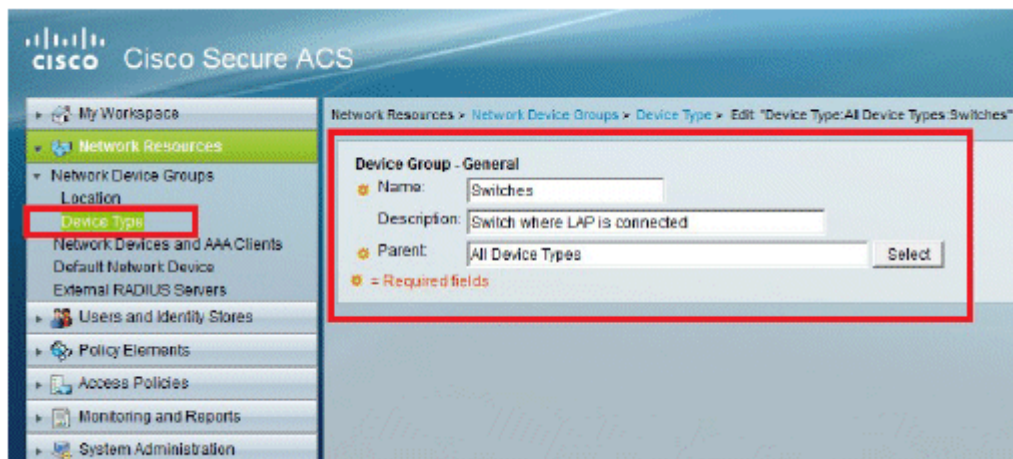
4. Agregue los campos obligatorios y haga clic en **Enviar**.



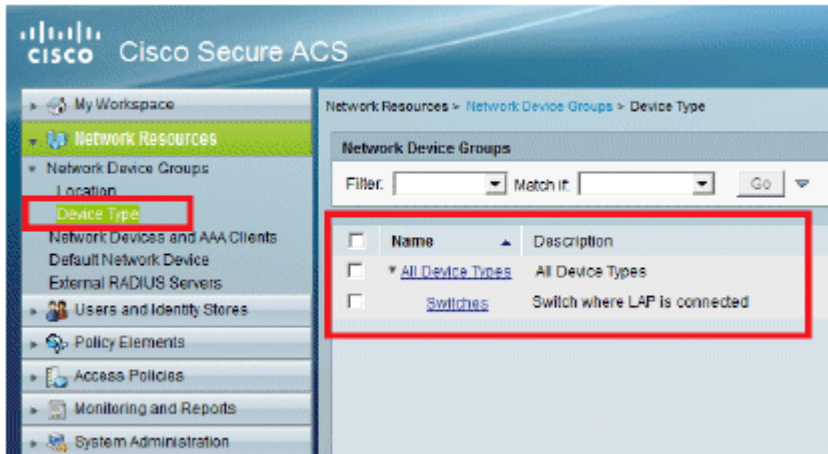
5. La ventana se actualiza:



6. Haga clic en **Tipo de dispositivo > Crear**.

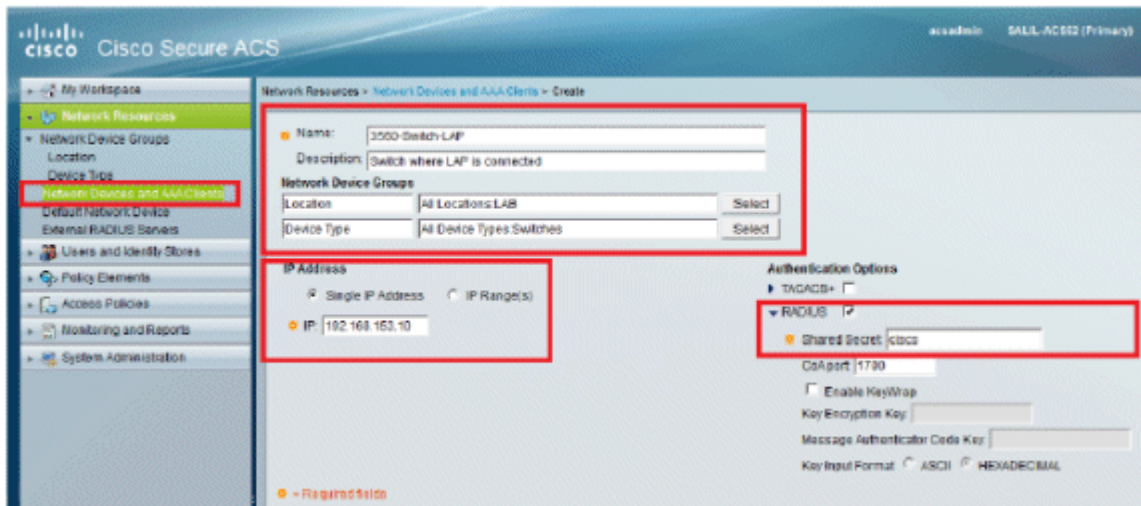


7. Haga clic en Submit (Enviar). Una vez completada, la ventana se actualiza:

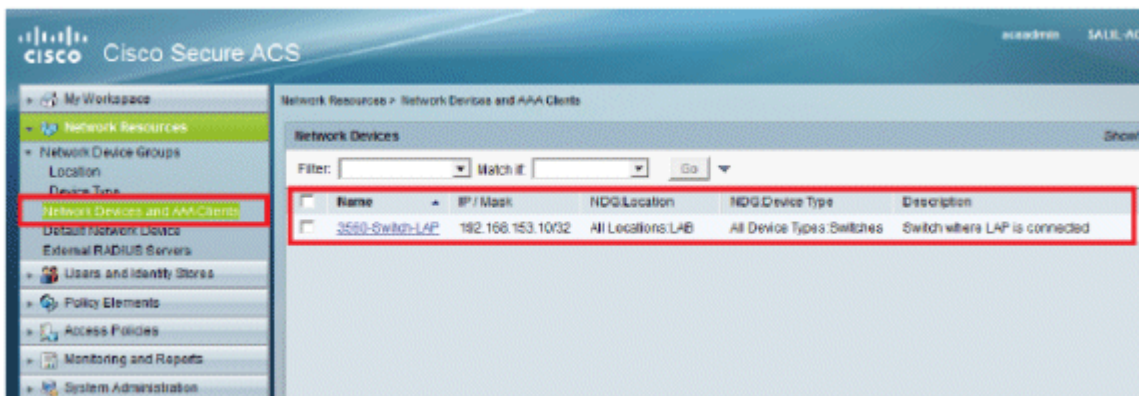


8. Vaya a **Recursos de red > Dispositivos de red y clientes AAA**.

9. Haga clic en **Create** y rellene los detalles como se muestra aquí:



10. Haga clic en Submit (Enviar). La ventana se actualiza:

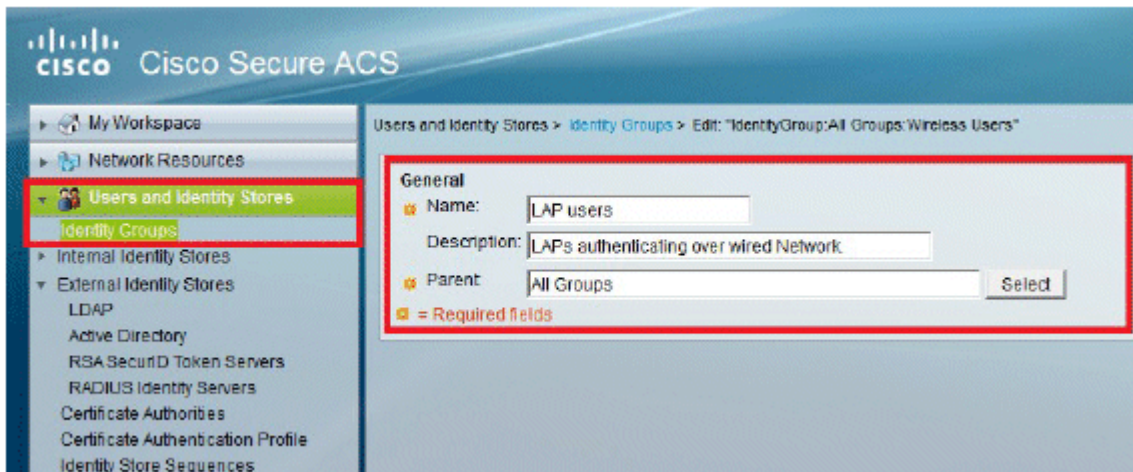


Configurar usuarios

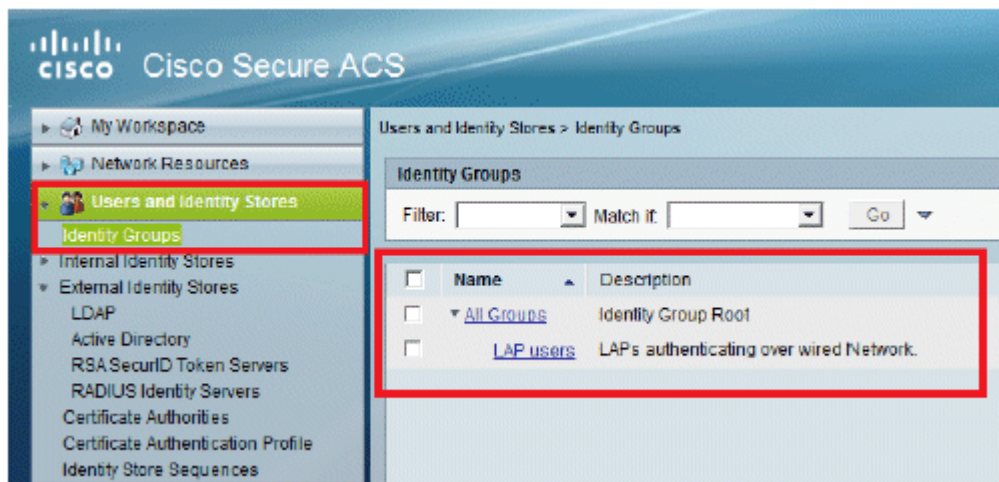
En esta sección, verá cómo crear un usuario en el ACS configurado previamente. Asignará el usuario a un grupo llamado "usuarios LAP".

Complete estos pasos:

1. Vaya a **Usuarios y almacenes de identidad > Grupos de identidad > Crear.**

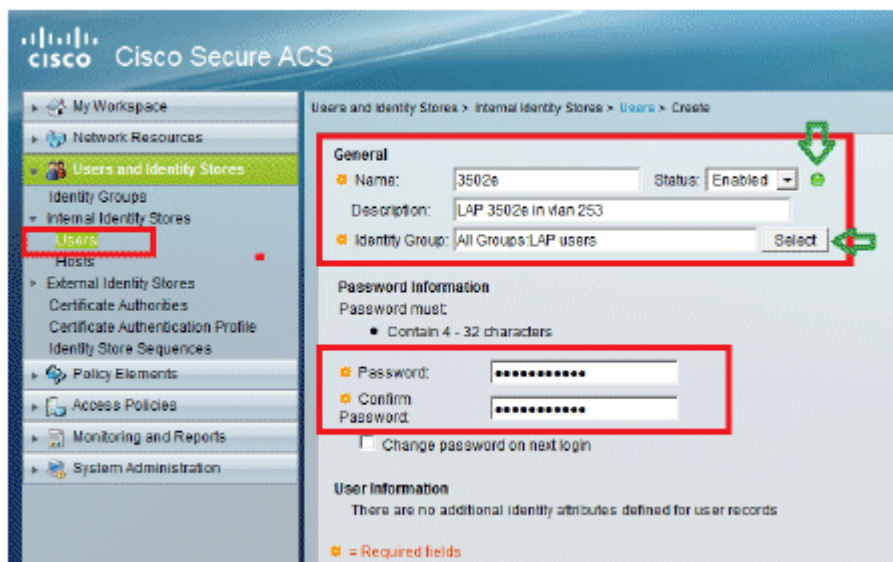


2. Haga clic en Submit (Enviar).

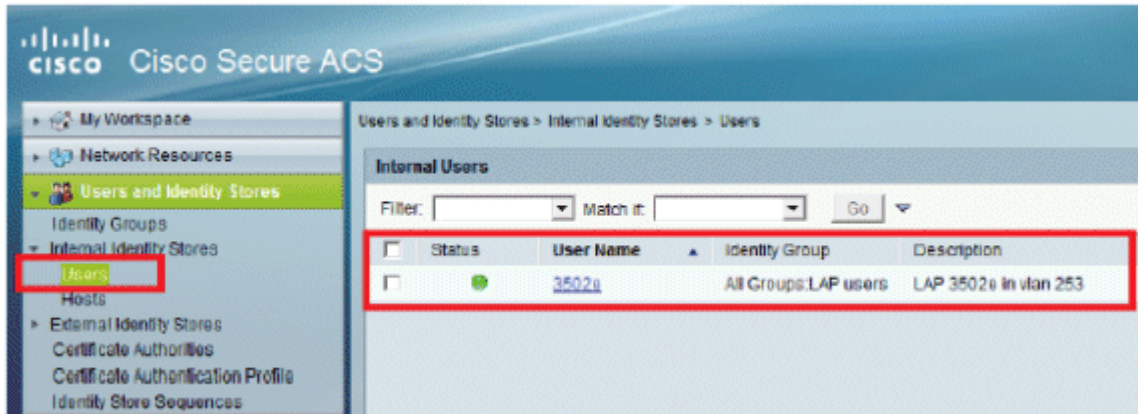


3. Cree **3502e** y asígnelo al grupo "usuarios LAP".

4. Vaya a **Usuarios y almacenes de identidad > Grupos de identidad > Usuarios > Crear.**

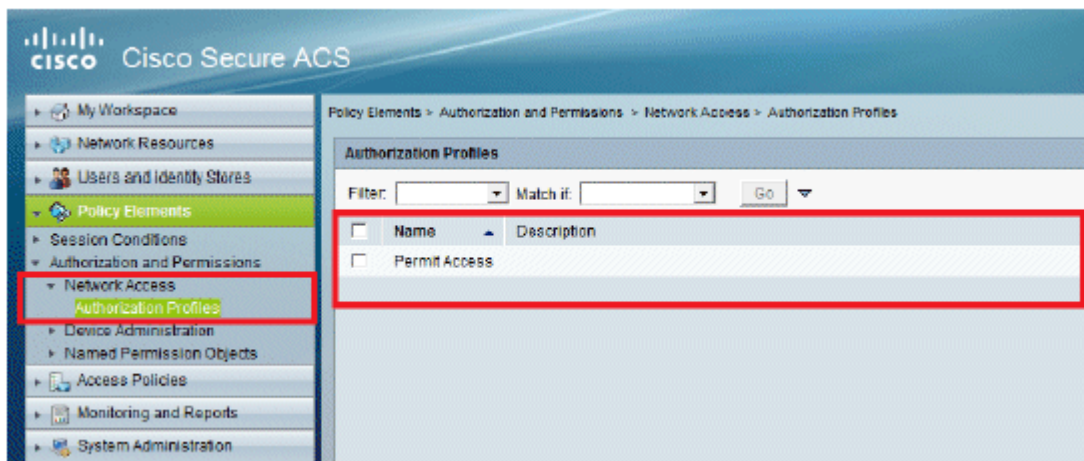


5. Verá la información actualizada:



Definición de elementos de política

Verifique que **Permit Access** esté configurado.

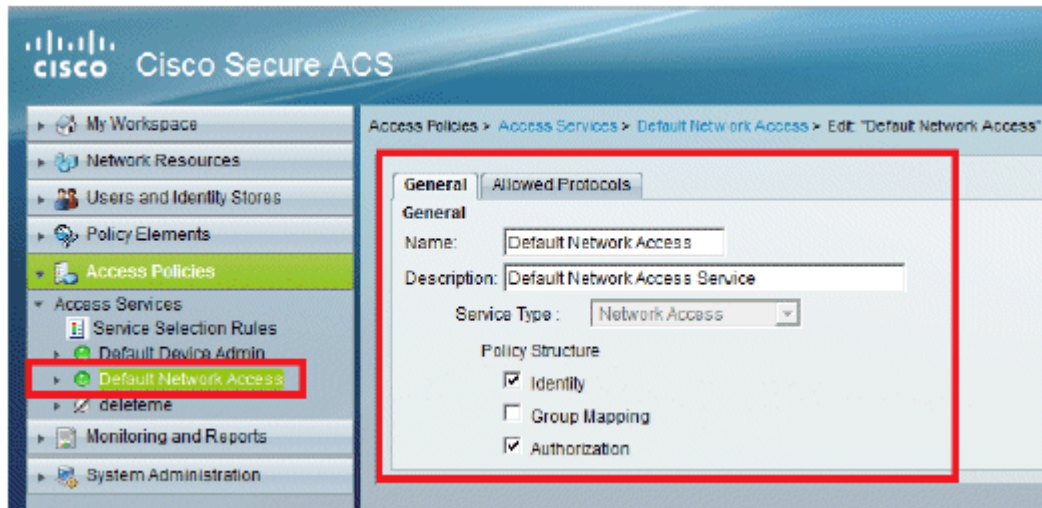


Aplicar políticas de acceso

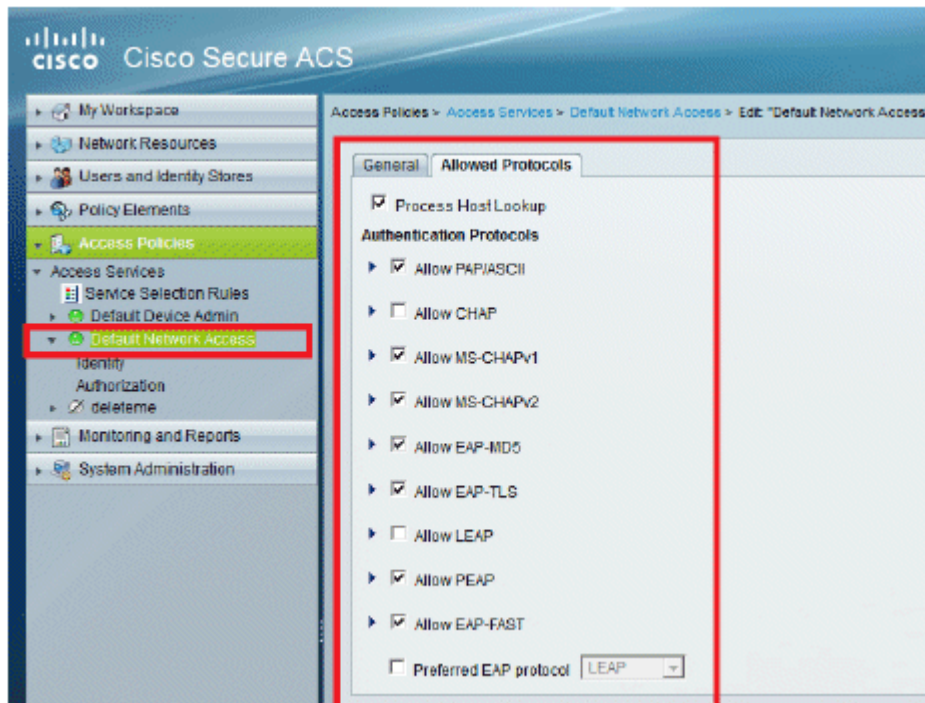
En esta sección, seleccionará EAP-FAST como el método de autenticación utilizado para los LAPs para autenticar. A continuación, creará reglas basadas en los pasos anteriores.

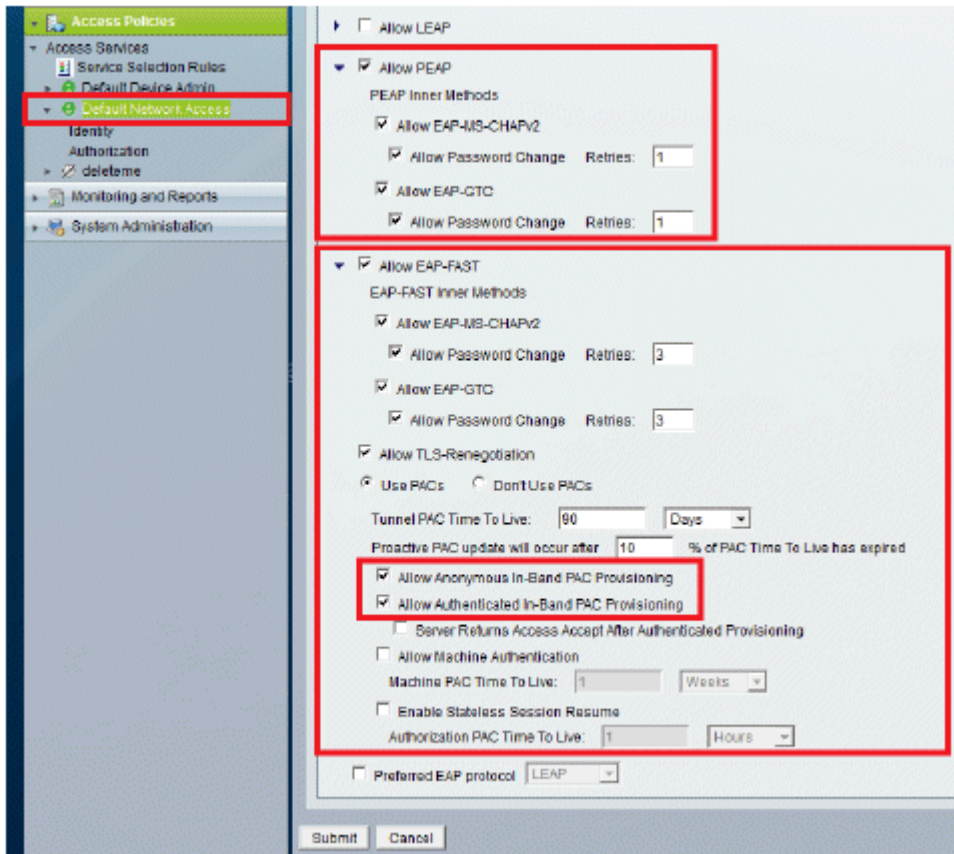
Complete estos pasos:

1. Vaya a **Políticas de acceso > Servicios de acceso > Acceso a la red predeterminado > Editar: "Acceso a la red predeterminado"**.



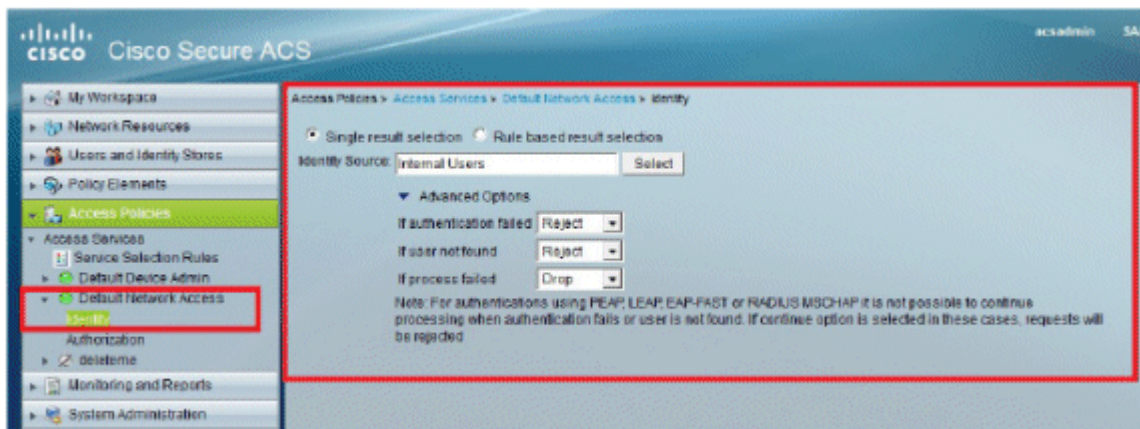
2. Asegúrese de haber habilitado **EAP-FAST** y **Anonymous In-Band PAC Provisioning**.





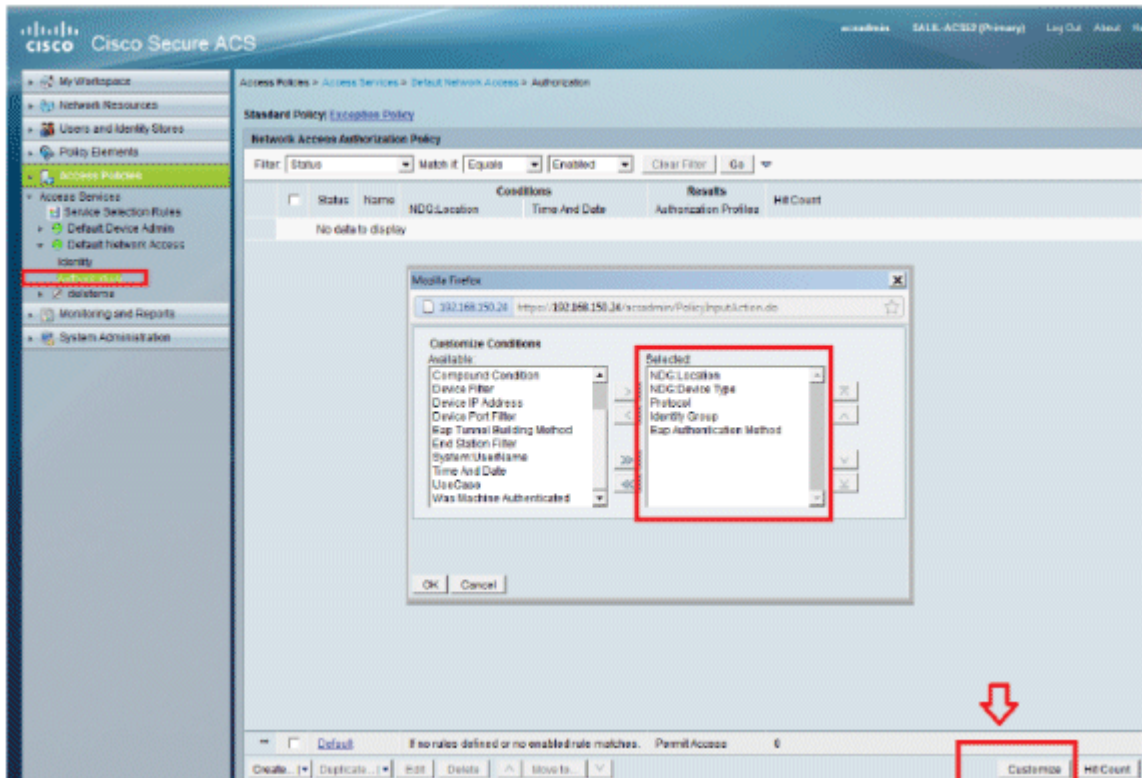
3. Haga clic en Submit (Enviar).

4. Verifique el grupo de identidad que ha seleccionado. En este ejemplo, utilice **Internal Users** (que fue creado en ACS) y guarde los cambios.



5. Vaya a **Access Políticas > Access Services > Default Network Access > Authorization** para verificar el perfil de autorización.

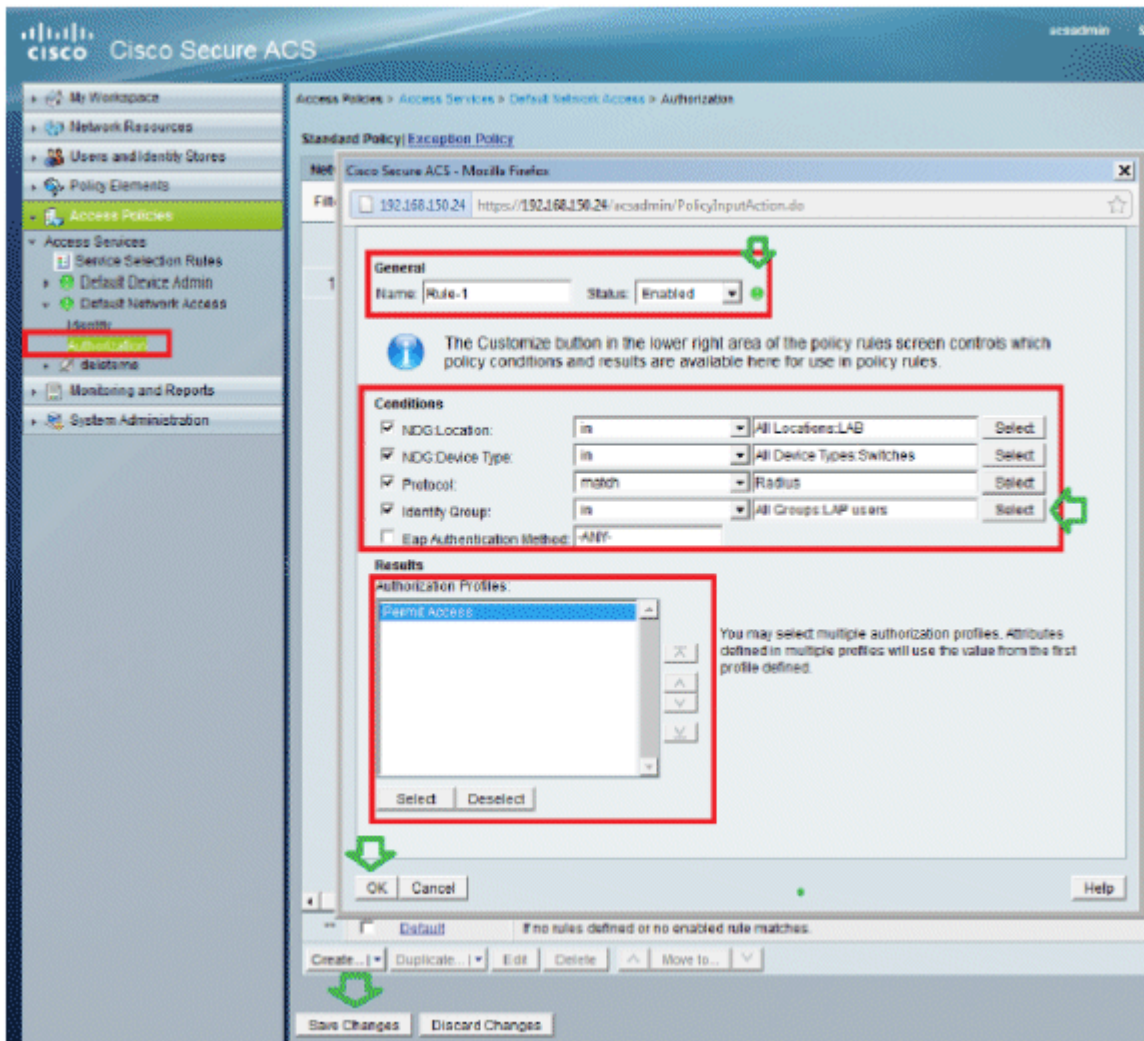
Puede personalizar en qué condiciones permitirá el acceso de un usuario a la red y qué perfil de autorización (atributos) pasará una vez autenticado. Esta granularidad sólo está disponible en ACS 5.x. En este ejemplo, se seleccionan Location, **Device Type**, **Protocol**, **Identity Group** y EAP Authentication Method.



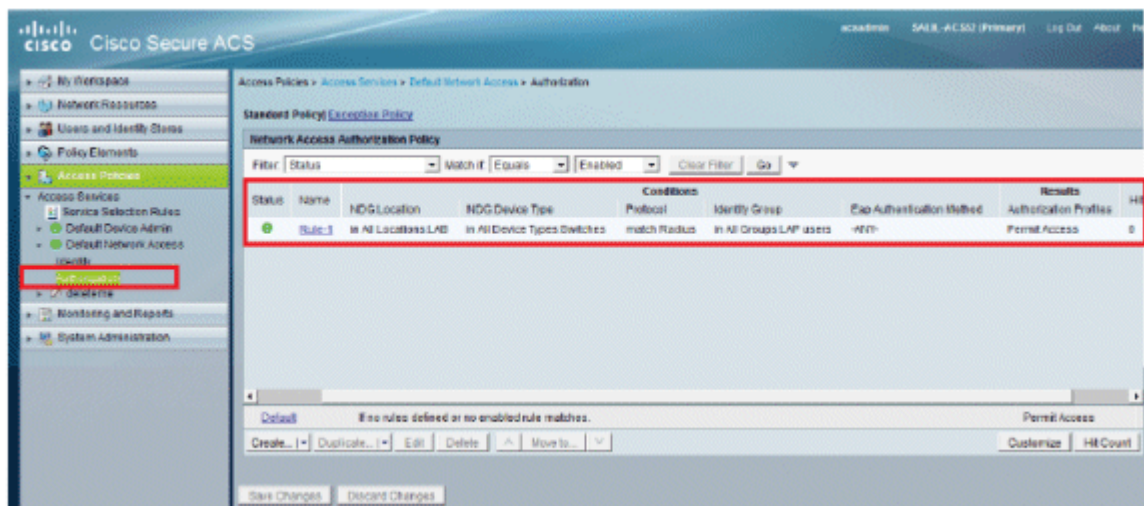
6. Haga clic en **Aceptar** y **Guardar cambios**.

7. El siguiente paso consiste en crear una regla. Si no se define ninguna regla, el LAP se permite el acceso sin ninguna condición.

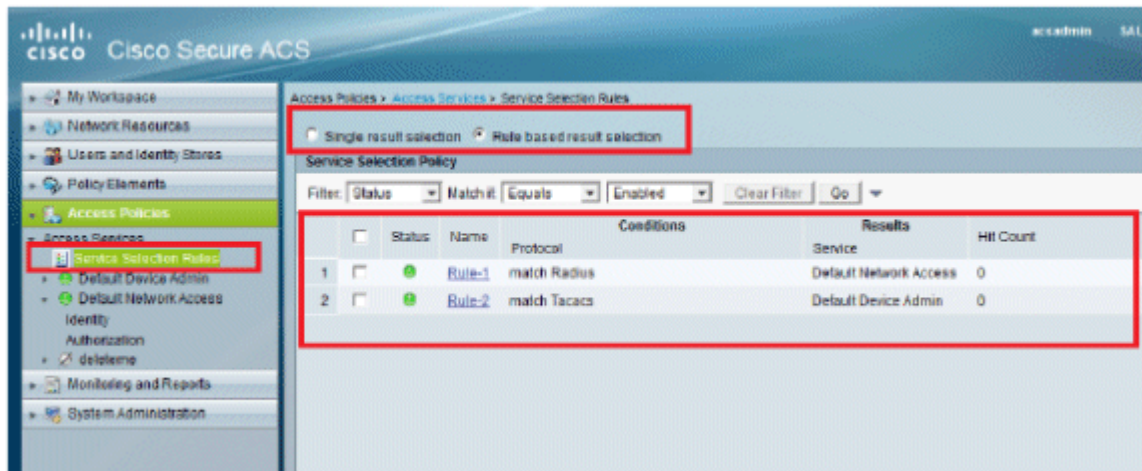
8. Haga clic en **Create** > **Rule-1**. Esta regla es para los usuarios del grupo "usuarios LAP".



9. Haga clic en **Guardar cambios**. Si desea que se denieguen los usuarios que no cumplan las condiciones, edite la regla predeterminada para que diga "Denegar acceso".



10. El último paso consiste en definir reglas de selección de servicios. Utilice esta página para configurar una política simple o basada en reglas para determinar qué servicio se debe aplicar a las solicitudes entrantes. Por ejemplo:



Verificación

Una vez que 802.1x está habilitado en el puerto del switch, todo el tráfico, excepto el tráfico 802.1x, se bloquea a través del puerto. El LAP, que ya está registrado en el WLC, se desasocia. Sólo después de una autenticación 802.1x correcta se permite el paso de otro tráfico. El registro exitoso del LAP al WLC después de que 802.1x esté habilitado en el switch indica que la autenticación del LAP es exitosa.

Consola de AP:

```
<#root>
```

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
192.168.75.44:5246
```

```
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
192.168.75.44:5247
```

```
!--- AP disconnects upon adding dot1x information in the gig0/11.
```

```
*Jan 29 09:10:30.104: %WIDS-5-DISABLED: IDS Signature is removed and disabled.
```

```
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
```

```
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
```

```
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
```

```
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
administratively down
```

```
*Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
reset
```

```
*Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
```

```
*Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
```

```
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
reset
```

```
Translating "CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25)
```

```
*Jan 29 09:10:36.203: status of voice_diag_test from WLC is false
```

```
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST] *Jan 29
```

```
!--- Authentication is successful and the AP gets an IP.
```

```
Translating "CISCO-CAPWAP-CONTROLLER.Wlab"...domain server (192.168.150.25)
```

```
*Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent
peer_ip: 192.168.75.44 peer_port: 5246
```

```
*Jan 29 09:11:37.000: %CAPWAP-5-CHANGED: CAPWAP changed state to
```

```
*Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS connection created
  successfully peer_ip: 192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.578: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44

*Jan 29 09:11:37.578: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN

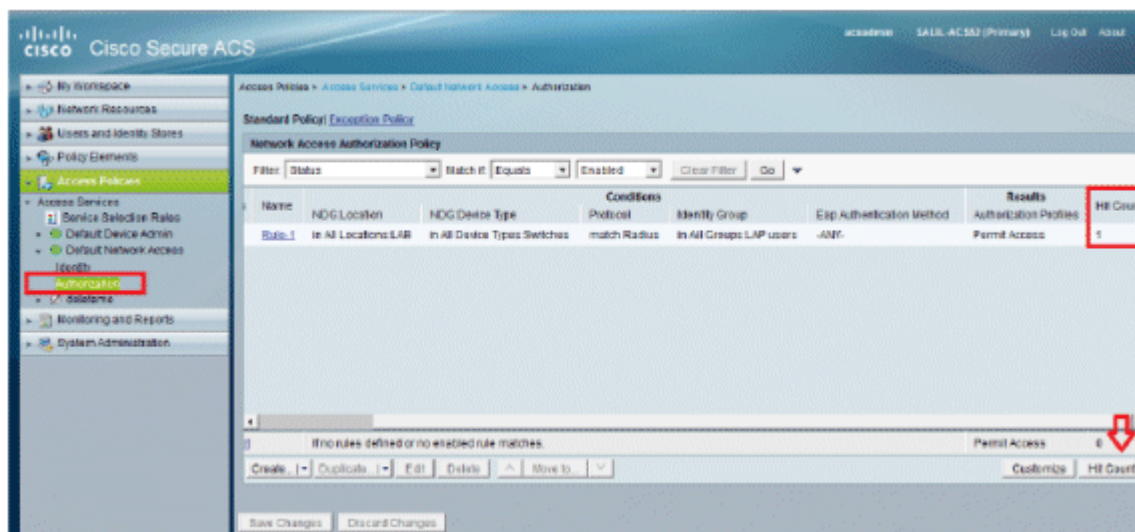
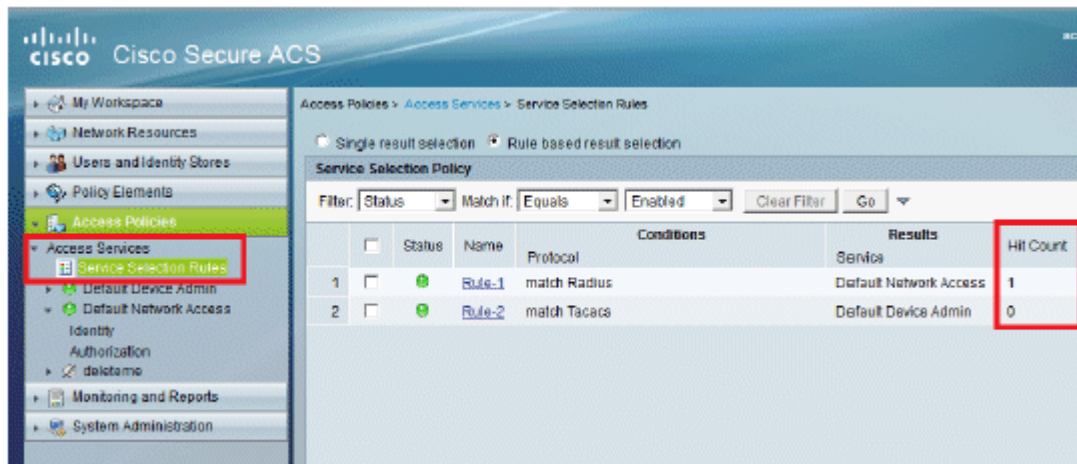
*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled
```

!--- AP joins the 5508-3 WLC.

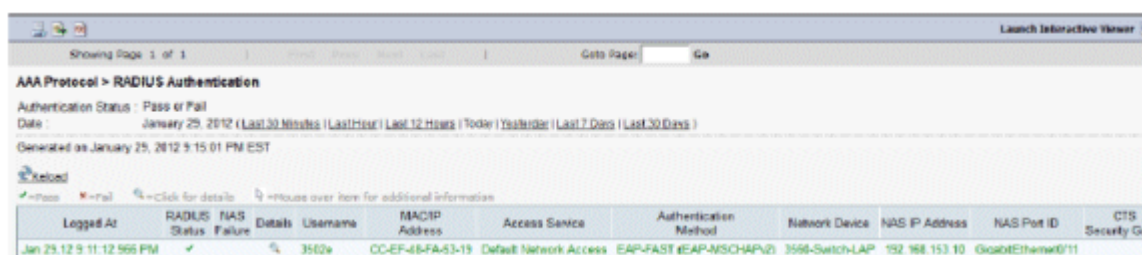
Registros de ACS:

1. Ver los recuentos de visitas:

Si está comprobando los registros en los 15 minutos siguientes a la autenticación, asegúrese de actualizar el número de visitas. En la misma página, en la parte inferior tiene una pestaña **Hit Count**.



2. Haga clic en **Supervisión e informes** y aparecerá una nueva ventana emergente. Haga clic en **Autenticaciones -RADIUS -Hoy**. También puede hacer clic en **Detalles** para verificar qué regla de selección de servicio se aplicó.



Troubleshoot

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

Información Relacionada

- [Cisco Secure Access Control System](#)
- [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).