

Configure la autenticación del 802.1x con el 2.1 y el WLC 8.3 PEAP, ISE

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración](#)

[Declare al servidor de RADIUS en el WLC](#)

[Cree el SSID](#)

[Declare el WLC en el ISE](#)

[Cree al usuario nuevo en el ISE](#)

[Cree la regla de la autenticación](#)

[Cree el perfil de la autorización](#)

[Cree la regla de la autorización](#)

[Configuración del dispositivo extremo](#)

[Configuración de dispositivo extremo - Instale el certificado autofirmado ISE](#)

[Configuración de dispositivo extremo - Cree el perfil de la red inalámbrica \(WLAN\)](#)

[Verificación](#)

[Proceso de autenticación en el WLC](#)

[Proceso de autenticación en el ISE](#)

[Troubleshooting](#)

Introducción

Este documento describe cómo configurar un Wireless Local Area Network (red inalámbrica (WLAN)) con la Seguridad del 802.1x y la invalidación de la red de área local virtual (VLAN) con el protocolo extensible authentication protegido (PEAP) como Protocolo de Autenticación Extensible (EAP).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- 802.1x
- PEAP
- Certification Authority (CA)
- Certificados

Componentes Utilizados

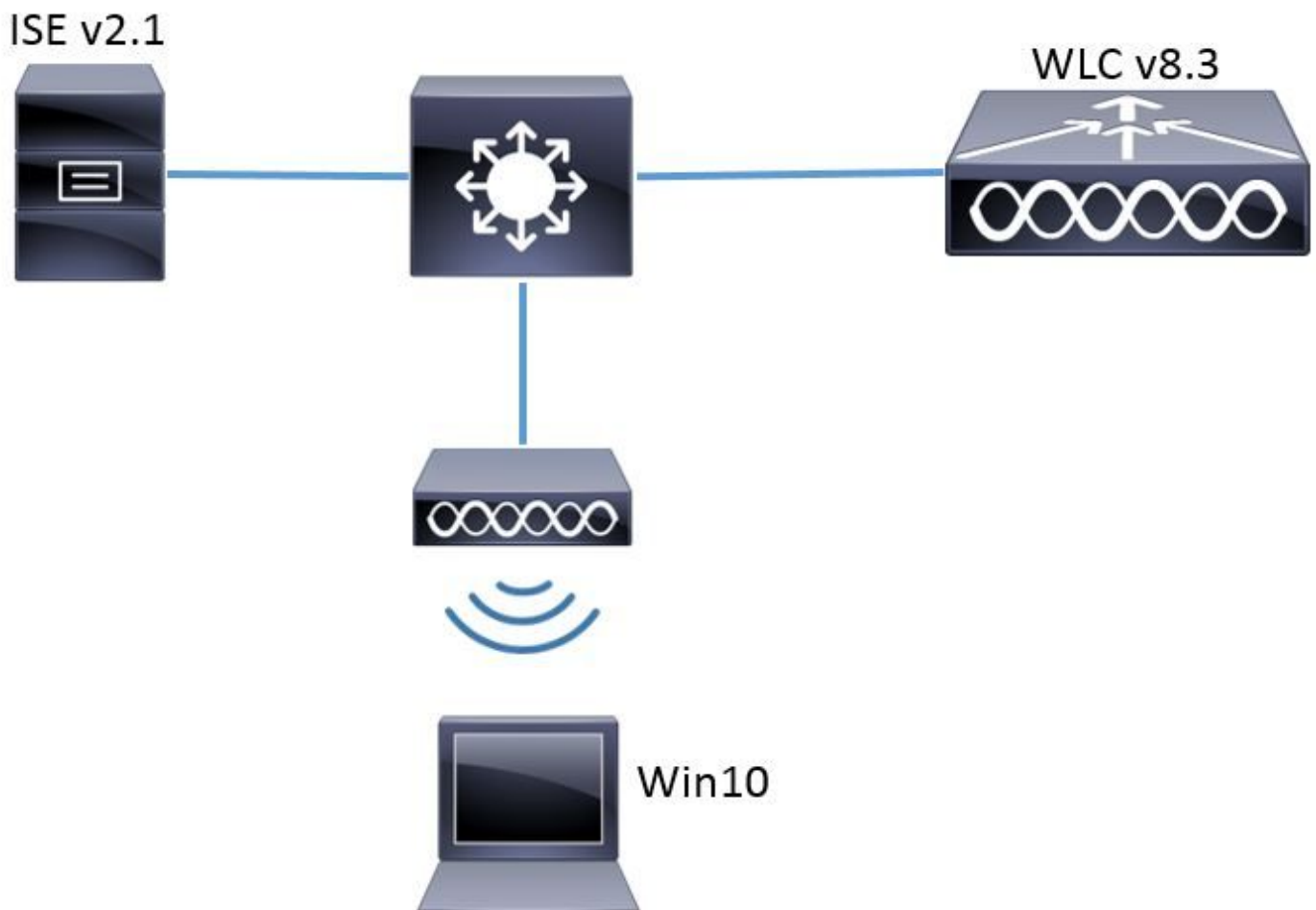
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC v8.3.102.0
- Motor del servicio de la identidad (ISE) v2.1
- Laptop de Windows 10

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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Diagrama de la red



Configuración

Los pasos generales son:

1. Declare al servidor de RADIUS en el WLC y vice versa permitir la comunicación con uno a.
2. Cree el Service Set Identifier (SSID) en el WLC.

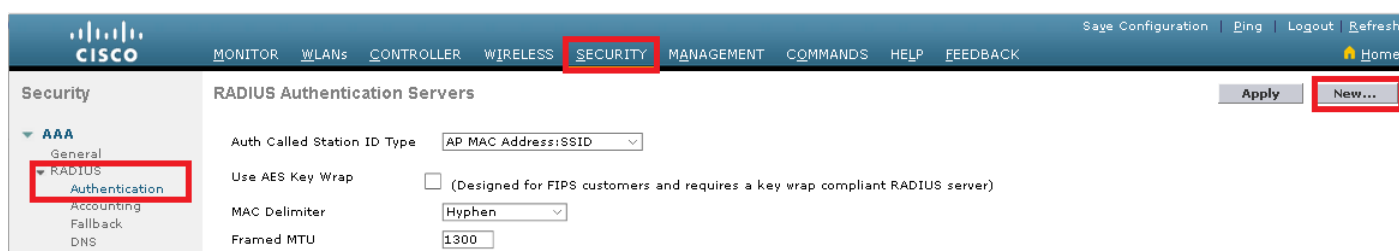
3. Cree la regla de la autenticación en el ISE.
4. Cree el perfil de la autorización en el ISE.
5. Cree la regla de la autorización en el ISE.
6. Configure el punto final.

Declare al servidor de RADIUS en el WLC

Para permitir la comunicación entre el servidor de RADIUS y el WLC, es necesario registrar al servidor de RADIUS en el WLC y vice versa.

GUI:

Paso 1. Abra el GUI del WLC y navegue a la **SEGURIDAD > al RADIUS > a la autenticación > nuevo** tal y como se muestra en de la imagen.



Paso 2. Ingrese la información del servidor de RADIUS tal y como se muestra en de la imagen.

RADIUS Authentication Servers > New

Server Index (Priority)

Server IP Address(Ipv4/Ipv6)

Shared Secret Format

Shared Secret

Confirm Shared Secret

Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number

Server Status

Support for CoA

Server Timeout seconds

Network User Enable

Management Enable

Management Retransmit Timeout seconds

IPSec Enable

CLI:

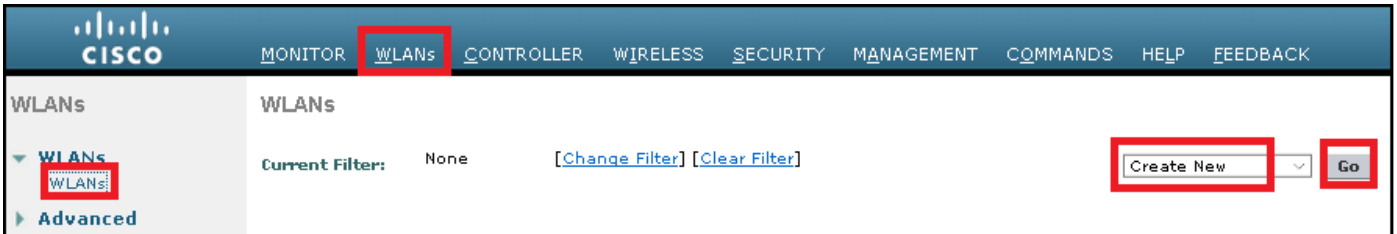
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

<a.b.c.d> corresponde al servidor de RADIUS.

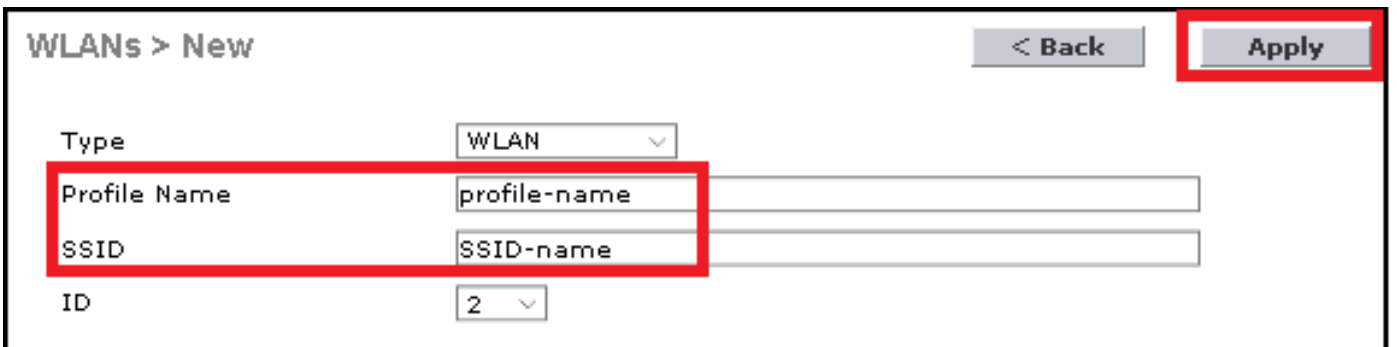
Cree el SSID

GUI:

Paso 1. Abra el GUI del WLC y navegue a los **WLAN > crean nuevo > van tal** y como se muestra en de la imagen.



Paso 2. Elija un nombre para el SSID y el perfil, después haga clic **se aplican** tal y como se muestra en de la imagen.



CLI:

```
> config wlan create <id> <profile-name> <ssid-name>
```

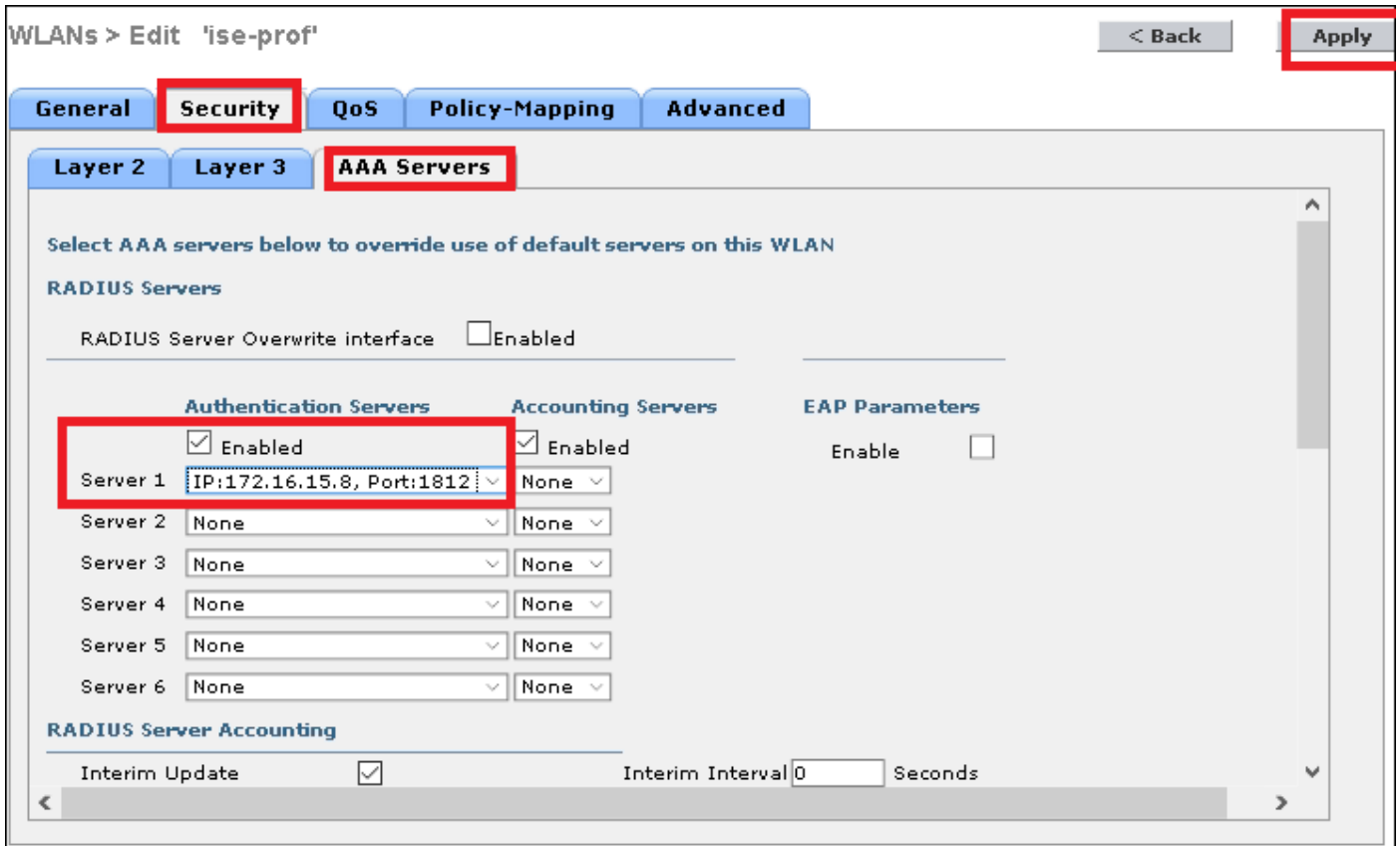
Paso 3. Asigne al servidor de RADIUS a la red inalámbrica (WLAN).

CLI:

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```

GUI:

Navegue a los **servidores de la Seguridad >AAA** y elija al servidor de RADIUS deseado, después el golpe **se aplica** tal y como se muestra en de la imagen.



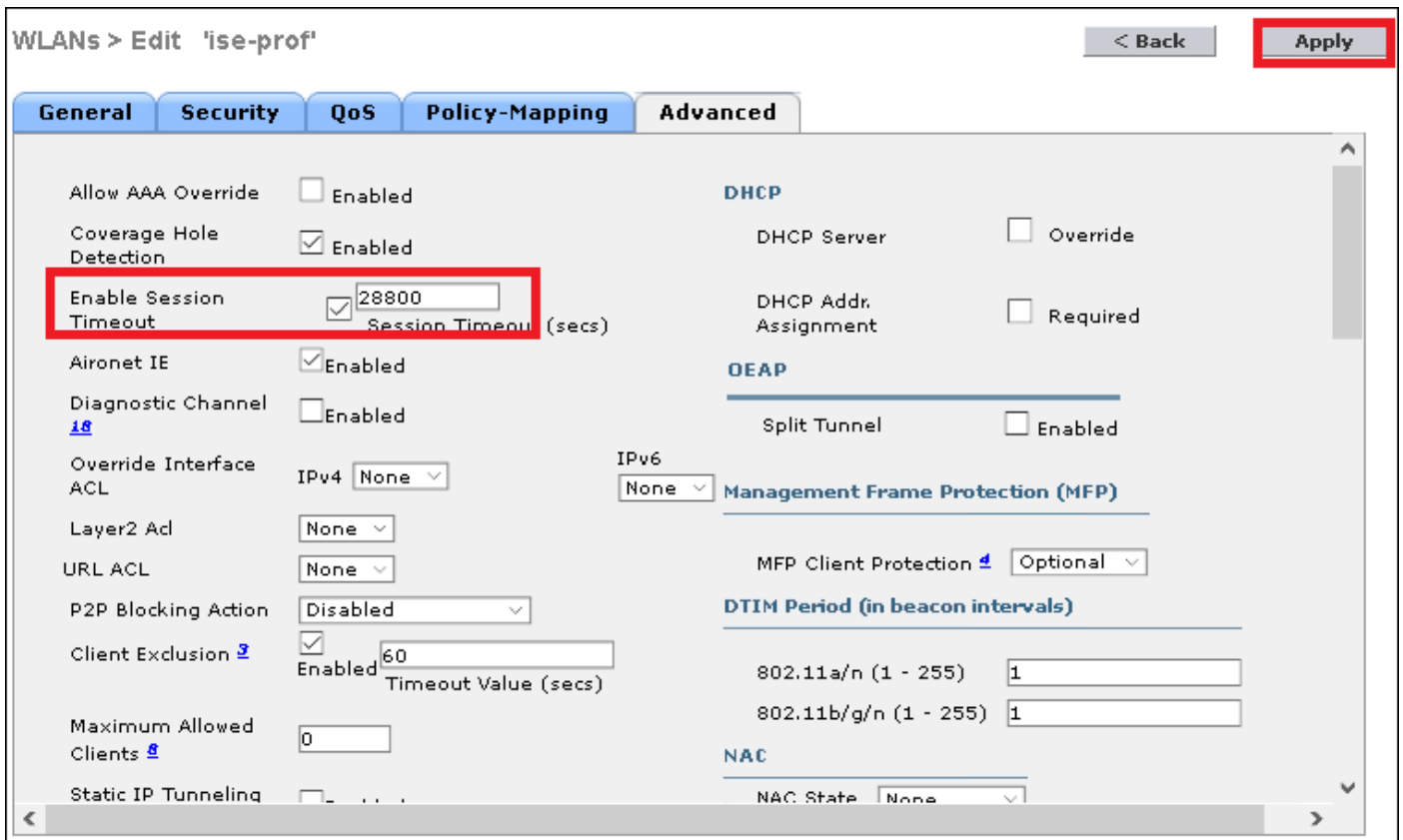
Paso 4. Aumente opcionalmente el tiempo de espera de la sesión

CLI:

```
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

Navegue a los **WLAN > ID DE WLAN > avanzó** y especifican el tiempo de espera de la sesión tal y como se muestra en de la imagen.



Paso 5. Habilite la red inalámbrica (WLAN).

CLI:

```
> config wlan enable <wlan-id>
```

GUI:

Navegue a los **WLAN > ID DE WLAN > general** y habilite el SSID tal y como se muestra en de la imagen.

WLANs > Edit 'ise-prof' < Back Apply

General Security QoS Policy-Mapping Advanced

Profile Name: ise-prof
 Type: WLAN
 SSID: ise-ssid
Status: Enabled

Security Policies: [WPA2][Auth(802.1X)]
 (Modifications done under security tab will appear after applying the changes.)

Radio Policy: All
 Interface/Interface Group(G): management
 Multicast Vlan Feature: Enabled
 Broadcast SSID: Enabled
 NAS-ID: none

Declare el WLC en el ISE

Paso 1. Abra la consola ISE y navegue a la **administración > a los recursos de red > a los dispositivos de red > Add** tal y como se muestra en de la imagen.

Identity Services Engine Home Context Visibility Operations Policy Administration World

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences

Network devices

Default Device

Edit
+ Add
 Duplicate
 Import
 Export
 Generate PAC
 Delete

Paso 2. Ingrese los valores.

Opcionalmente, puede ser un nombre modelo especificado, versión de software, descripción y asignar a los grupos de dispositivos de red basados en los tipos de dispositivo, la ubicación o el WLCs.

el a.b.c.d corresponde a la interfaz WLC que envía la autenticación pedida. Por abandono es la interfaz de administración tal y como se muestra en de la imagen.

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

WLCs

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

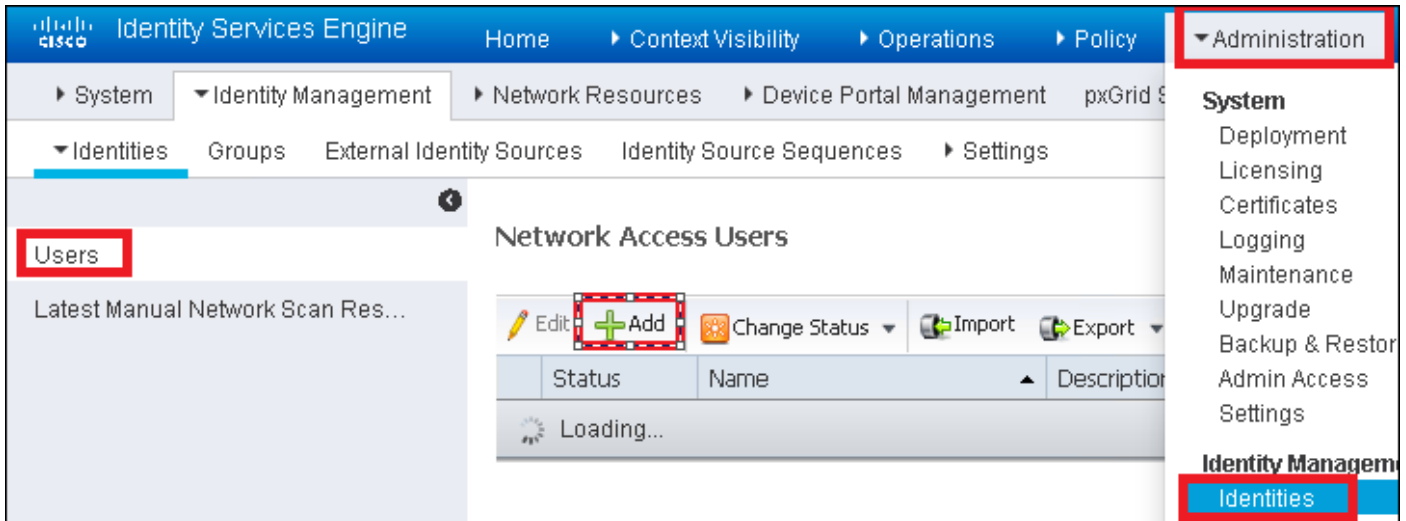
CoA Port

Para más información sobre los **grupos de dispositivos de red** revise este link:

[ISE - Grupos de dispositivos de red](#)

Cree al usuario nuevo en el ISE

Paso 1. Navegue a la **administración** > a la **Administración de la identidad** > a las **identidades** > **Users** > **Add** tal y como se muestra en de la imagen.



Paso 2. Ingrese la información.

En este ejemplo, este usuario pertenece a un grupo llamado ALL_ACCOUNTS pero puede ser ajustado según las necesidades tal y como se muestra en de la imagen.

▼ **Network Access User**

* Name

Status Enabled ▼

Email

▼ **Passwords**

Password Type: ▼

Password

Re-Enter Passw

* Login Password

Enable Password

▼ **User Information**

First Name

Last Name

▼ **Account Options**

Description

Change password on next login

▼ **Account Disable Policy**

Disable account if date exceeds

▼ **User Groups**

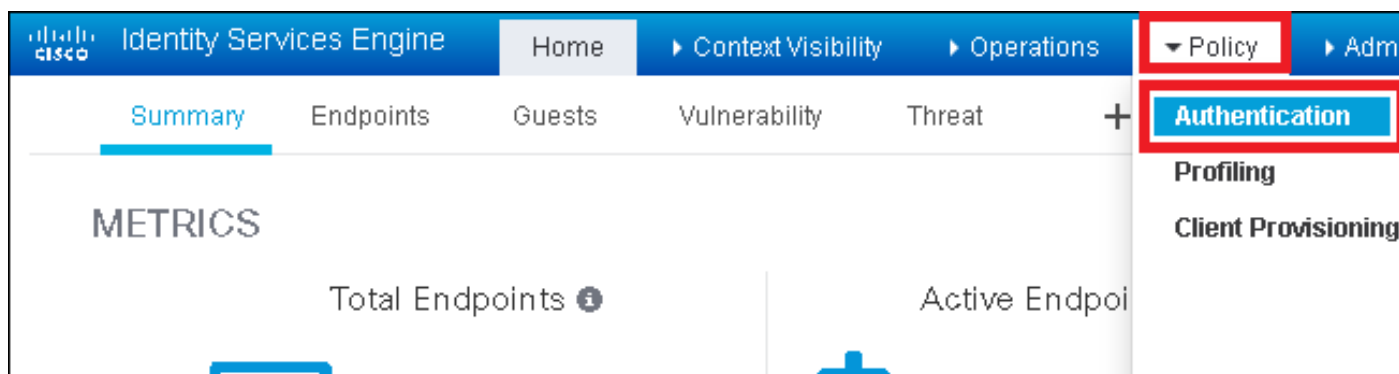
+

Cree la regla de la autenticación

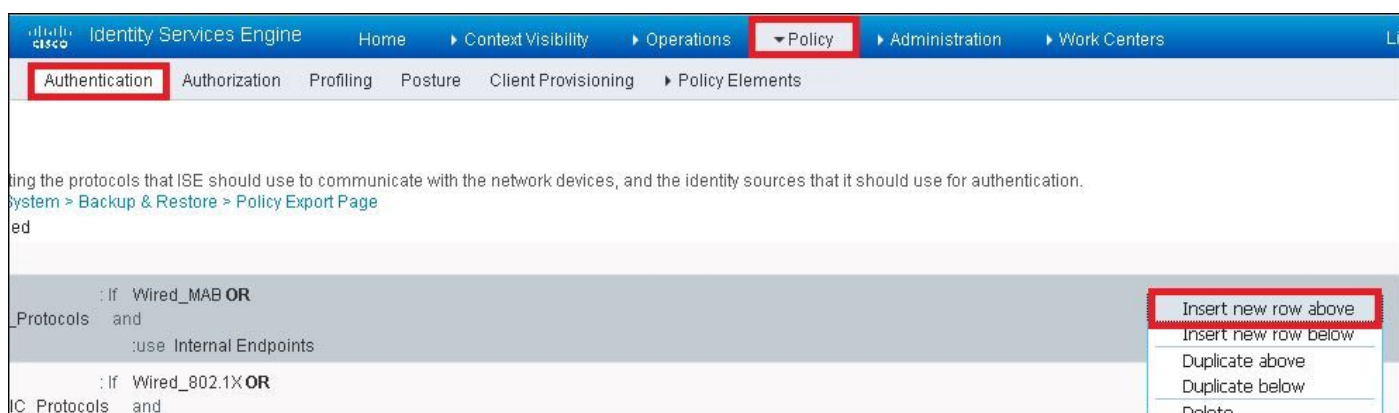
Las reglas de la autenticación se utilizan para verificar si las credenciales de los usuarios correcto (verifique si el usuario es realmente quién lo dice es) y limitar los métodos de autenticación que

se permiten ser utilizados por él.

Paso 1. Navegue a la **directiva > a la autenticación** tal y como se muestra en de la imagen.

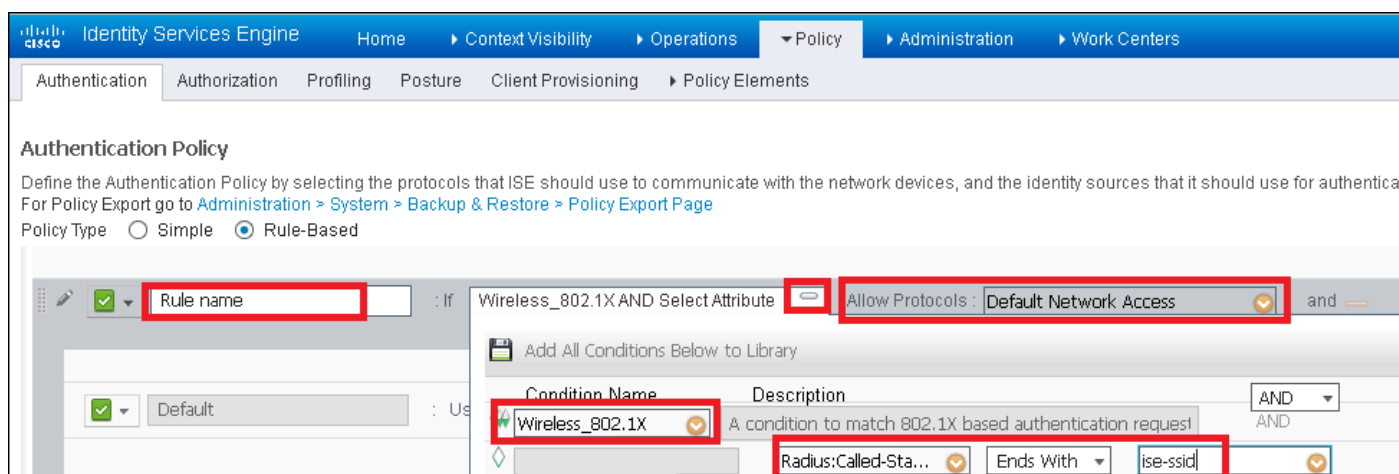


Paso 2. Inserte una nueva regla de la autenticación tal y como se muestra en de la imagen.

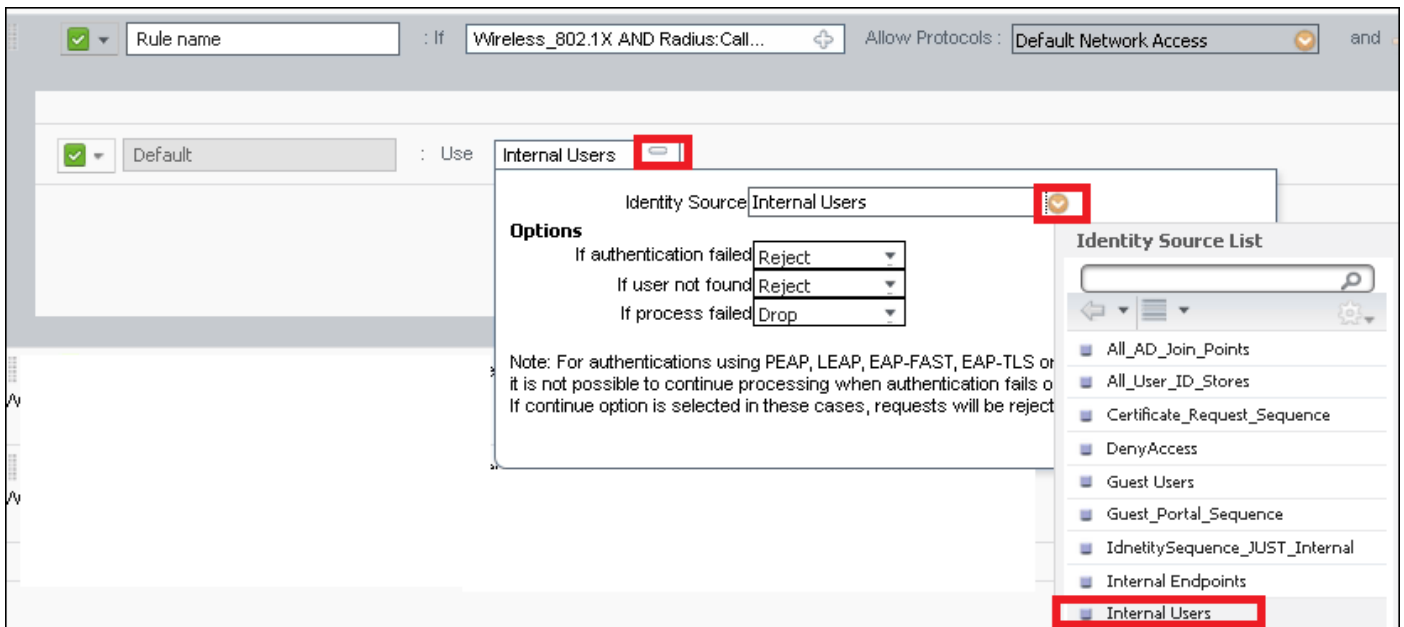


Paso 3. Ingrese los valores.

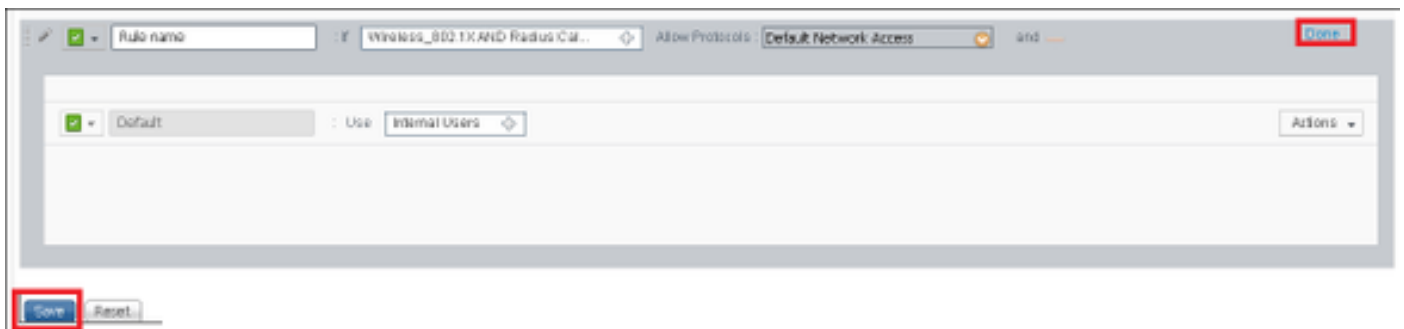
Esta regla de la autenticación permite todos los protocolos enumerados conforme a la **lista de acceso de la red predeterminada**, ésta se aplica al pedido de autenticación para los clientes inalámbricos del 802.1x y con el Llamar-Estación-ID y los extremos con ISE-SSID tal y como se muestra en de la imagen.



También, elija la fuente de la identidad para los clientes que hace juego esta regla de la autenticación. Este ejemplo utiliza la lista de origen de la identidad de los **usuarios internos** tal y como se muestra en de la imagen.



Una vez que está acabado, haga clic **hecho** y **salve** tal y como se muestra en de la imagen.



Para más información sobre permita los protocolos que las directivas consultan este link:

[Servicio permitido de los protocolos](#)

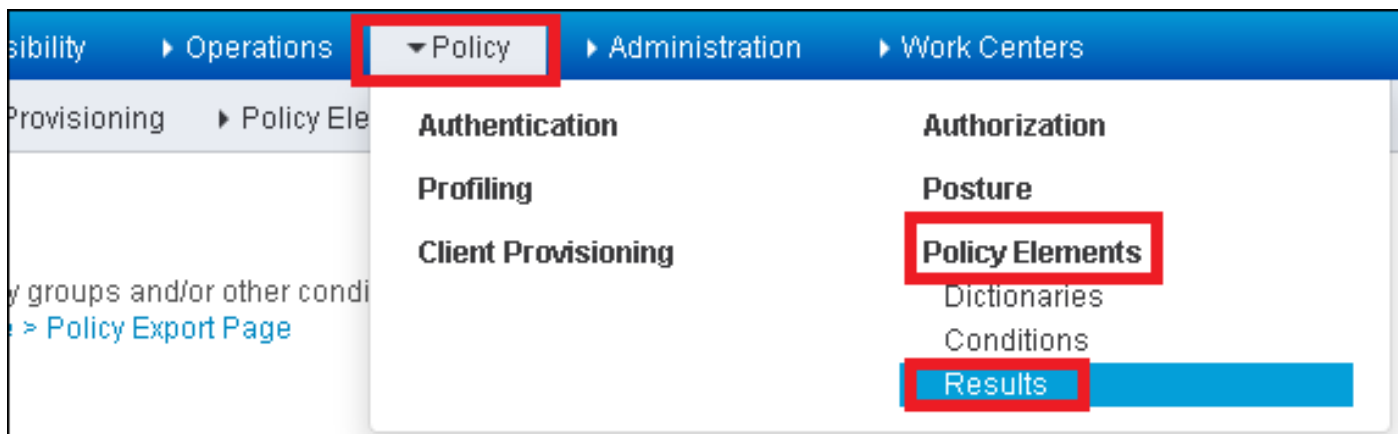
Para más información sobre la identidad las fuentes consultan este link:

[Cree un grupo de la Identificación del usuario](#)

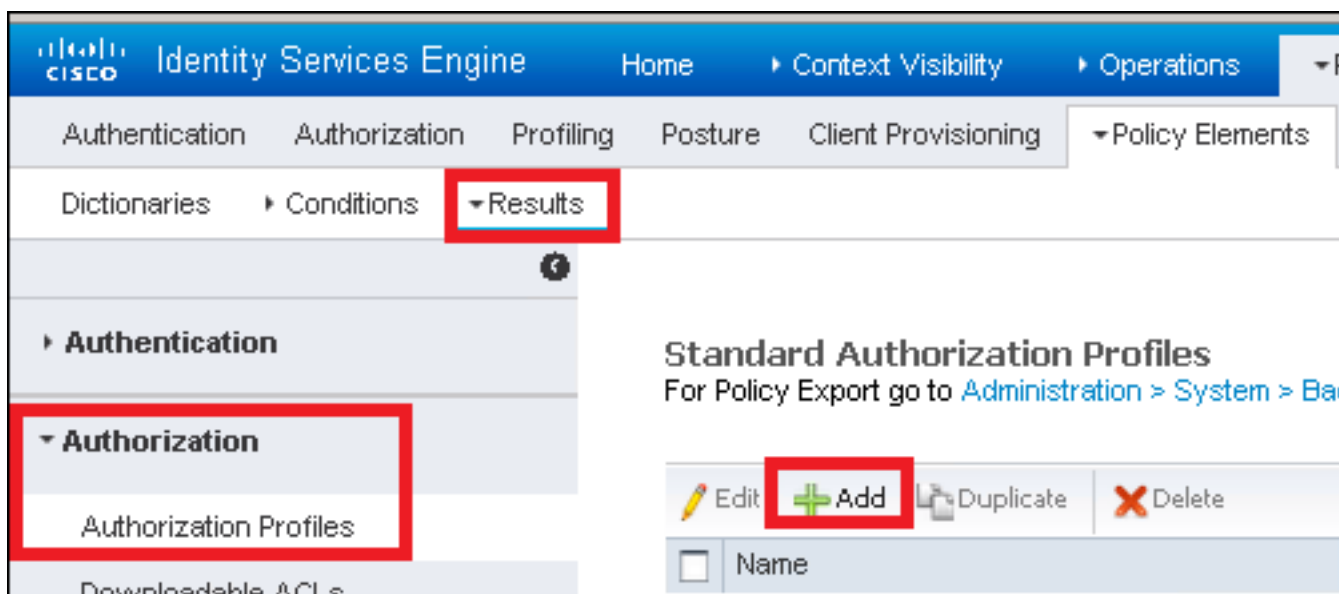
Cree el perfil de la autorización

El perfil de la autorización determina si el cliente tiene acceso o no a la red, al Listas de control de acceso (ACL) del empuje, a la invalidación del VLA N o a cualquier otro parámetro. El perfil de la autorización mostrado en este ejemplo envía un acceso valida para el cliente y asigna al cliente al VLA N 2404.

Paso 1. Navegue a la **directiva > a los elementos > a los resultados de la directiva** tal y como se muestra en de la imagen.



Paso 2. Agregue un nuevo perfil de la autorización. Navegue a la **autorización** > a los **perfiles de la autorización** > **Add** tal y como se muestra en de la imagen.



Paso 3. Ingrese los valores tal y como se muestra en de la imagen.

