Lightweight Access Point de la configuración como supplicant del 802.1x

Contenido

Introducción

Este documento describe cómo configurar un Lightweight Access Point (REVESTIMIENTO) mientras que un supplicant del 802.1x para autenticar contra el servidor del Identity Services Engine (ISE).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Regulador del Wireless LAN (WLC) y REVESTIMIENTO
- 802.1x en los switches Cisco
- ISE
- Protocolo de Autenticación Extensible (EAP) - Autenticación flexible vía el Tunelización seguro (RÁPIDO)

Componentes Utilizados

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

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0

- ISE 2.0

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.

Antecedentes

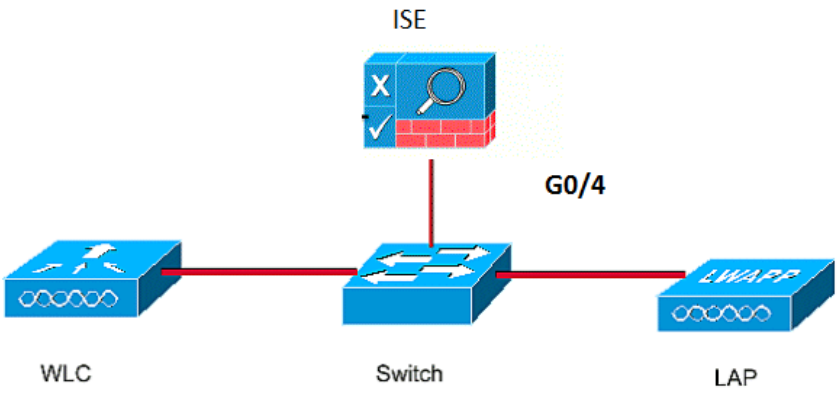
En este puesto el punto de acceso actúa como el supplicant del 802.1x y es autenticado por el Switch contra el ISE que utiliza el EAP-FAST con la disposición protegida anónima de las credenciales del acceso (PAC). El puerto se configura una vez para la autenticación del 802.1x, el Switch no permite que ningún tráfico con excepción del tráfico del 802.1x pase a través del puerto hasta que el dispositivo conectado con el puerto autentique con éxito. Un AP se puede autenticar o antes de que se una a un WLC o después de que se ha unido a un WLC, en este caso usted configura el 802.1x en el Switch después de que el REVESTIMIENTO se una 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:



Configuraciones

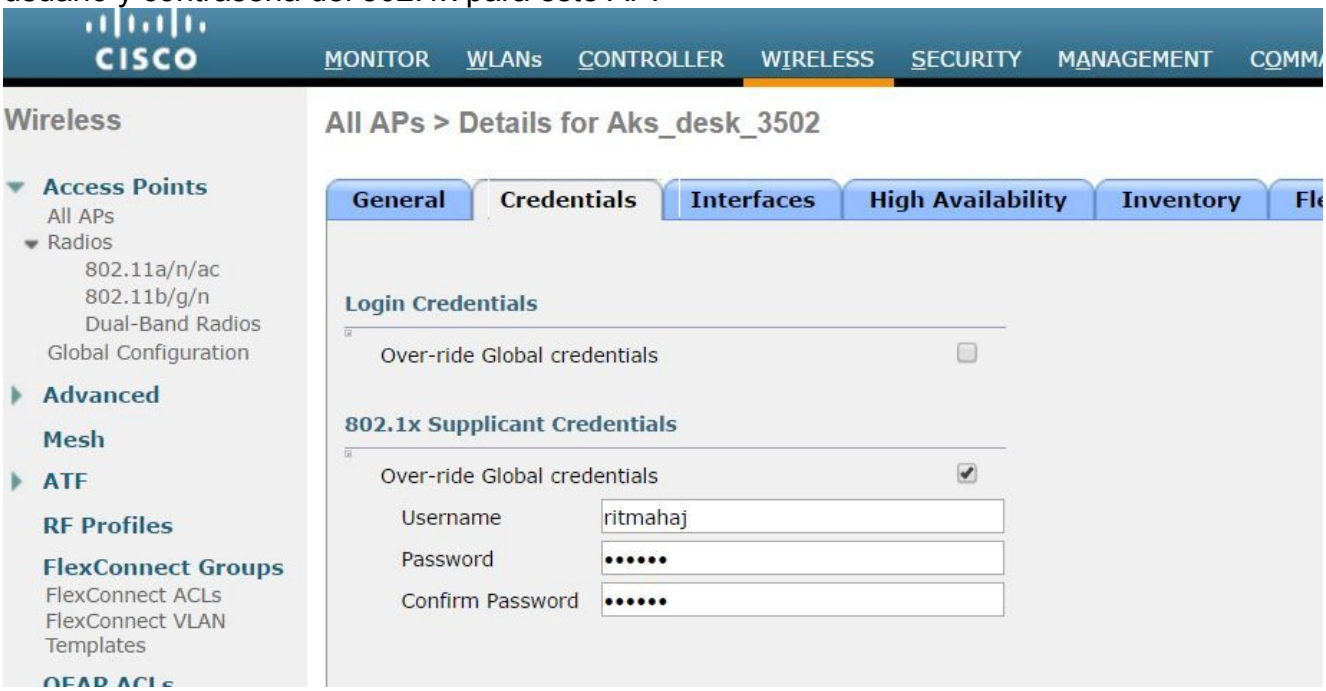
Este documento utiliza estos IP Addresses:

- La dirección IP del Switch es 10.48.39.141
- La dirección IP del servidor ISE es 10.48.39.161
- La dirección IP del WLC es 10.48.39.142

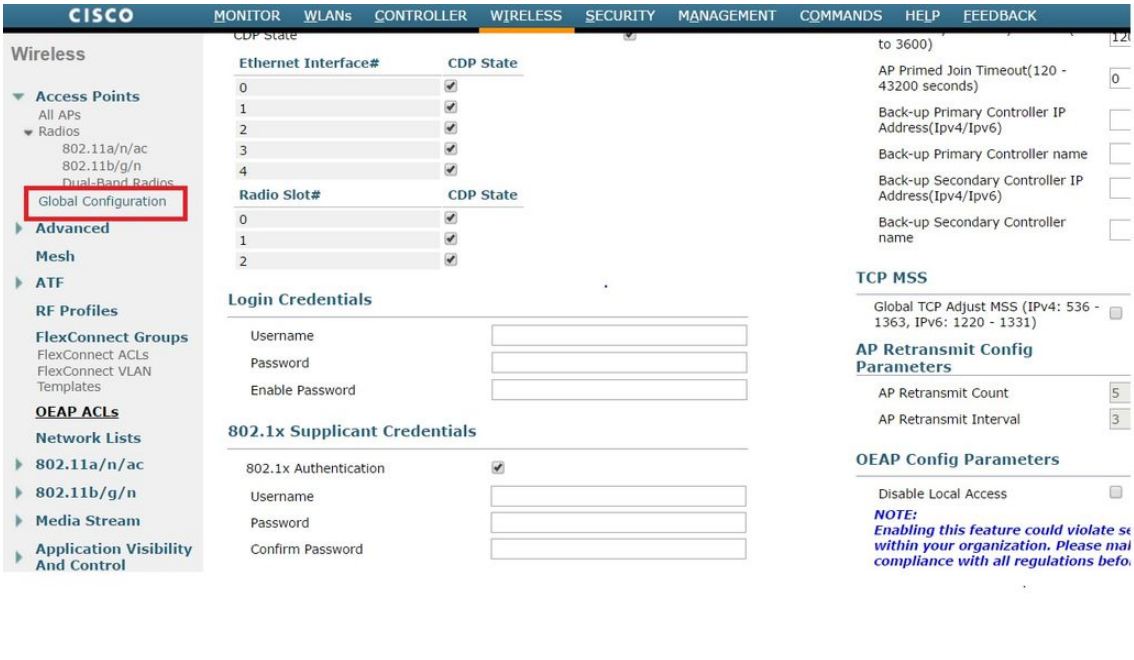
Configure el REVESTIMIENTO

En esta sección, le presentan con la información para configurar el REVESTIMIENTO como supplicant del 802.1x.

1. Si el AP se une a ya al WLC, va la lengueta sin hilos y hace clic en el AP, va las credenciales coloca y bajo las credenciales del supplicant del 802.1x que dirigen, marca el rectángulo de **verificación de credenciales global de la invalidación** para fijar el nombre de usuario y contraseña del 802.1x para este AP.



Usted puede también fijar un nombre de usuario y contraseña común para todos los AP que se unen a al WLC con el menú de la configuración
global.



2. Si el AP no se ha unido a un WLC todavía, usted debe consolar en el REVESTIMIENTO para fijar las credenciales y utilizar estos comandos CLI:
   LAP#**debug capwap console cli**
   LAP#**capwap ap dot1x username <username> password <password>**

Configure el Switch

1. Habilite el dot1x en el Switch global y agregue el servidor ISE al Switch.

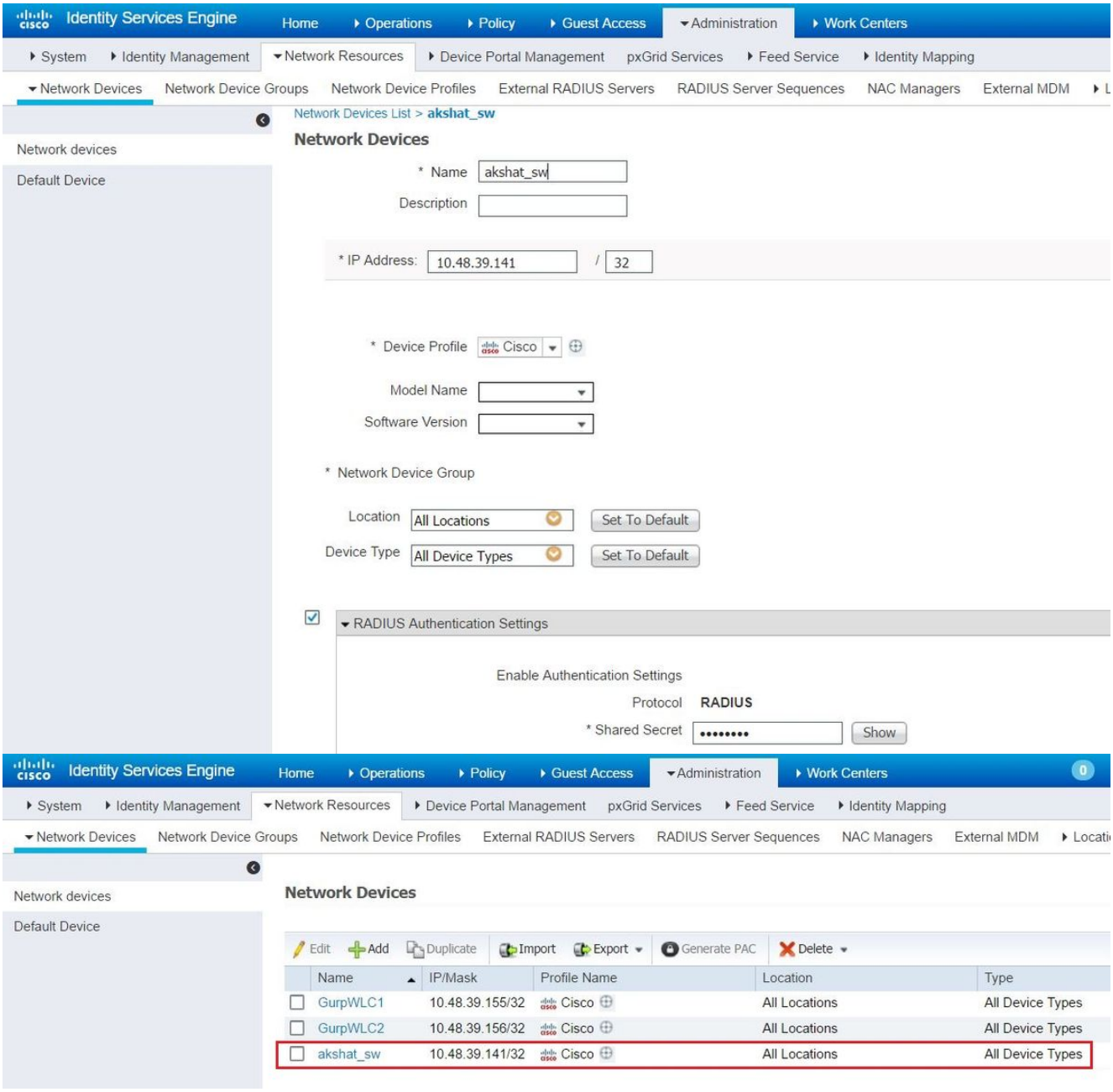
```
aaa new-model
!
aaa authentication dot1x default group radius
!
dot1x system-auth-control
!
radius server ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
  key 7 123A0C0411045D5679
```

2. Ahora, configure el puerto del switch AP.

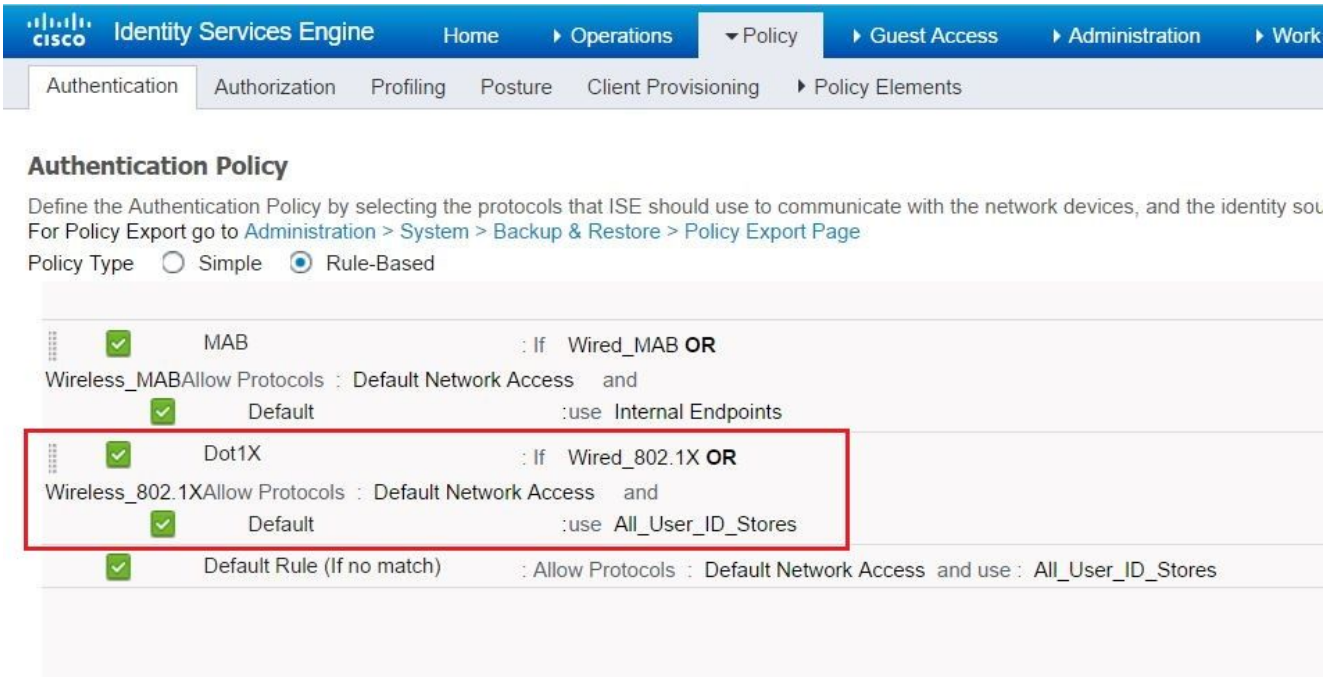
```
interface GigabitEthernet0/4


switchport access vlan 231
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Configure el servidor ISE

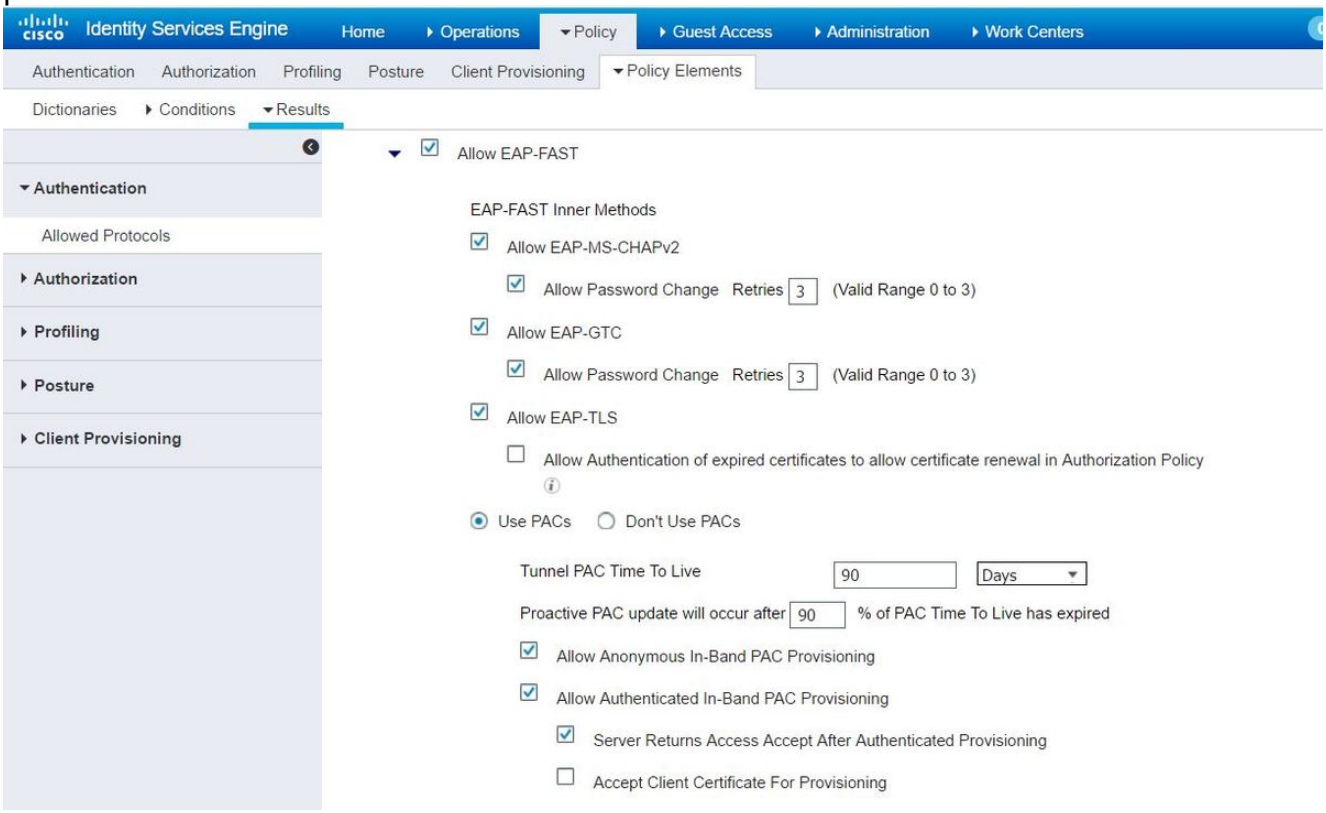
1. Agregue el Switch como cliente del Authentication, Authorization, and Accounting (AAA) en el servidor ISE.



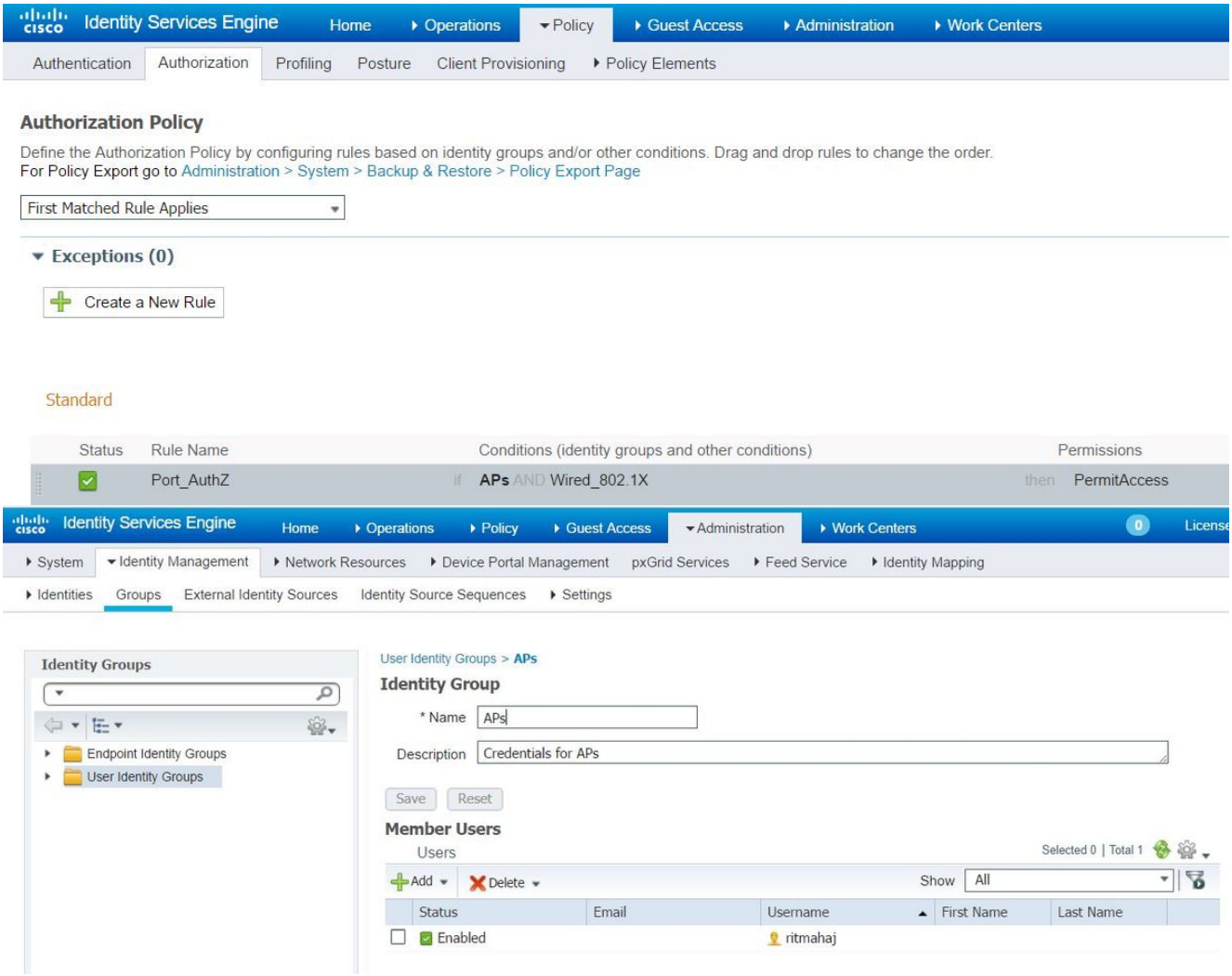
2. En el ISE, configure la directiva de la política de autenticación y de la autorización. En este caso, se utiliza la regla de la autenticación predeterminada que es dot.1x atado con alambre, solamente uno puede personalizarlo según el requisito.



Asegure eso en los protocolos permitidos que el acceso de red predeterminada, EAP-FAST no se
prohibe.



3. En cuanto a la directiva de la autorización (Port_AuthZ), en este caso las credenciales AP fueron agregadas a un (APS) del grupo de usuarios. La condición usada era “si el usuario pertenece al grupo AP y hacer el dot1x atado con alambre, después avanza el acceso predeterminado del permiso del perfil de la autorización.” Una vez más esto se puede personalizar según el requisito.



Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

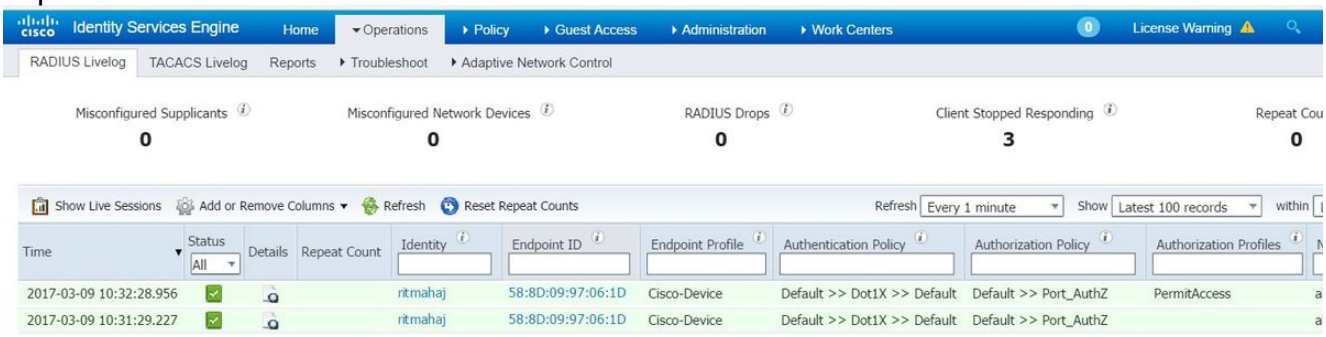
Una vez que el 802.1x se habilita en el puerto del switch, todo el tráfico a menos que el tráfico del 802.1x se bloquee a través del puerto. El REVESTIMIENTO, que si está registrado ya al WLC, consigue desasociado. Solamente después que una autenticación acertada del 802.1x es el otro tráfico permitido pasar a través. El registro exitoso del REVESTIMIENTO al WLC después de que el 802.1x se habilite en el Switch indica que la autenticación del REVESTIMIENTO es acertada. Usted puede también utilizar estos métodos para verificar si el REVESTIMIENTO autenticó.

1. En el Switch, ingrese uno de los **comandos show** para verificar si se ha autenticado el puerto o no.

```
akshat_sw#show dot1x interface g0/4

Dot1x Info for GigabitEthernet0/4
-----------------------------------
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

```
akshat_sw#show dot1x interface g0/4 details

Dot1x Info for GigabitEthernet0/4
-----------------------------------
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30


Dot1x Authenticator Client List
-------------------------------
EAP Method = FAST
Supplicant = 588d.0997.061d
Session ID = 0A30278D000000A088F1F604
Auth SM State = AUTHENTICATED
Auth BEND SM State = IDLE


akshat_sw#show authentication sessions

Interface MAC Address Method Domain Status Fg Session ID
Gi0/4 588d.0997.061d dot1x DATA Auth 0A30278D000000A088F1F604
```

2. En el ISE, elija las **operaciones > el radio Livelogs** y vea que la autenticación es acertada y el perfil correcto de la autorización está avanzado.



Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

1. Ingrese el **comando ping** para marcar si el servidor ISE es accesible del Switch.
2. Aseegurese que el Switch está configurado como cliente AAA en el servidor ISE.
3. Asegúrese de que el secreto compartido sea lo mismo entre el Switch y el servidor ACS.
4. Marque si el EAP-FAST se habilita en el servidor ISE.
5. Marque si las credenciales del 802.1x se configuran para el REVESTIMIENTO y son lo mismo en el servidor ISE. **Note**: El nombre de usuario y contraseña es con diferenciación entre mayúsculas y minúsculas.
6. Si la autenticación falla, ingrese estos comandos en el Switch: **haga el debug del dot1x** y el **debug authentication**.