Configurar o Access point de pouco peso como um suplicante do 802.1x

Índice

Introdução

Este documento descreve como configurar um Access point de pouco peso (REGAÇO) enquanto um suplicante do 802.1x a fim autenticar contra o server do Identity Services Engine (ISE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controlador do Wireless LAN (WLC) e REGAÇO
- 802.1x em switch Cisco
- ISE
- Extensible Authentication Protocol (EAP) - Autenticação flexível através do Tunelamento seguro (RÁPIDO)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- ISE 2.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

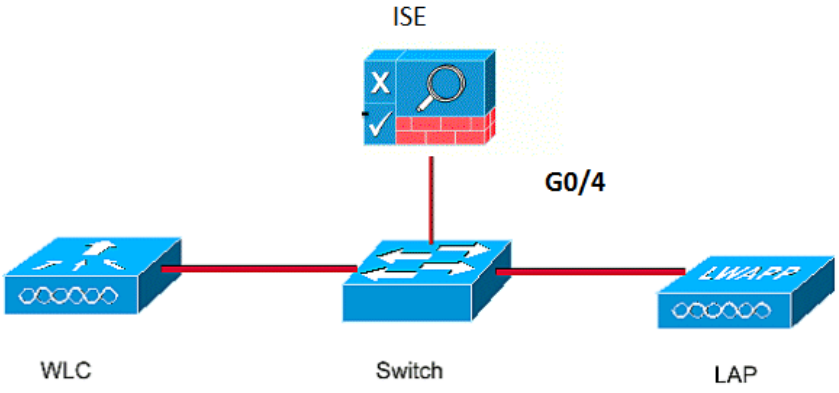
No este setup o Access Point (AP) atua como o suplicante do 802.1x e é autenticado pelo interruptor contra o ISE que usa EAP-FAST com abastecimento protegido anônimo das credenciais do acesso (PAC). Uma vez que a porta é configurada para a autenticação do 802.1x, o interruptor não permite que nenhum tráfego a não ser o tráfego do 802.1x passe através da porta até que o dispositivo conectado à porta autentique com sucesso. Um AP pode ser autenticado ou antes que se junte a um WLC ou depois que se juntou a um WLC, neste caso você configura o 802.1x no interruptor depois que o REGAÇO se junta ao WLC.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

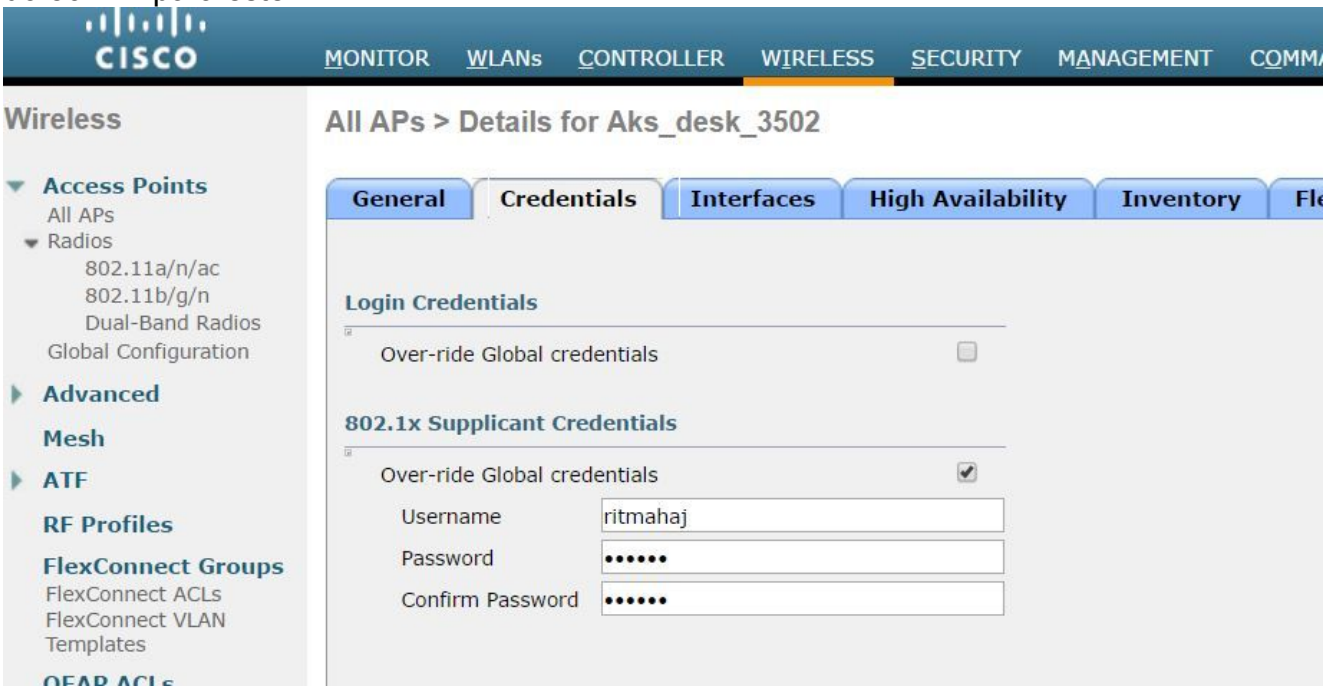
Este documento usa estes endereços IP de Um ou Mais Servidores Cisco ICM NT:

- O endereço IP de Um ou Mais Servidores Cisco ICM NT do interruptor é 10.48.39.141
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do server ISE é 10.48.39.161
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do WLC é 10.48.39.142

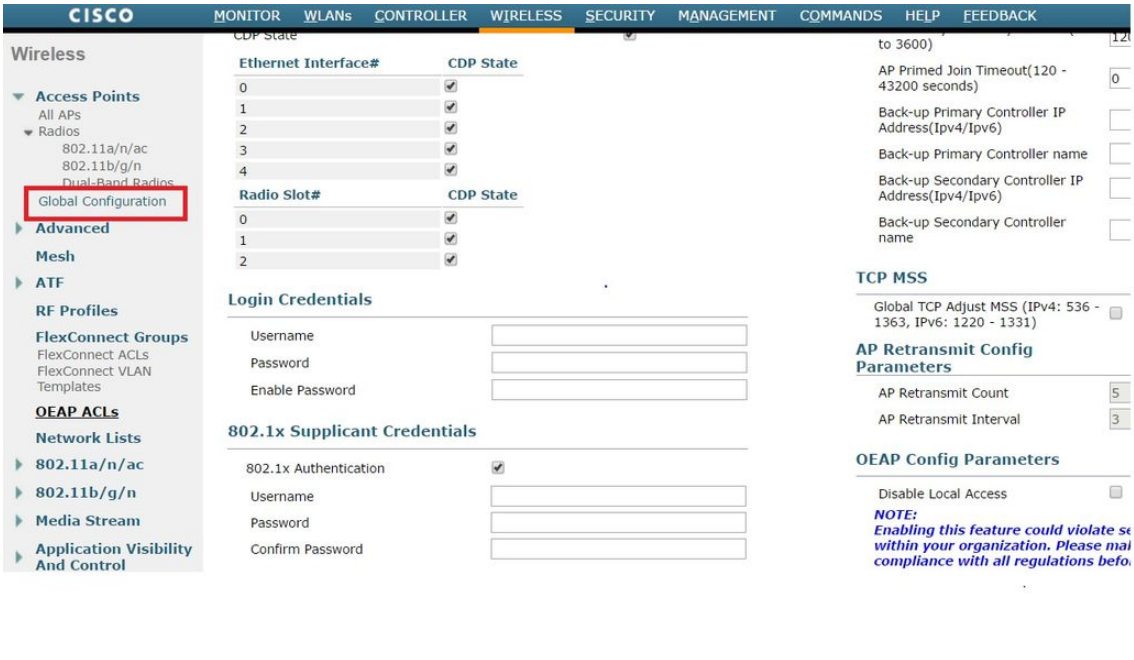
Configurar o REGAÇO

Nesta seção, você é presentado com a informação para configurar o REGAÇO como um suplicante do 802.1x.

1. Se o AP é juntado já ao WLC, vai a aba wireless e clica sobre o AP, vai as credenciais coloca e sob as credenciais do suplicante do 802.1x que dirigem, verifica a caixa de **verificação de credenciais global da ultrapassagem** a fim ajustar o nome de usuário e senha do 802.1x para este AP.



Você pode igualmente ajustar um nome de usuário e senha comum para todos os AP que são juntados ao WLC com o menu da configuração
global.



2. Se o AP não se juntou a um WLC ainda, você deve consolar no REGAÇO a fim ajustar as credenciais e usar estes comandos CLI:
   LAP#**debug capwap console cli**
   LAP#**capwap ap dot1x username <username> password <password>**

Configurar o interruptor

1. Permita o dot1x no interruptor globalmente e adicionar o server ISE ao interruptor.

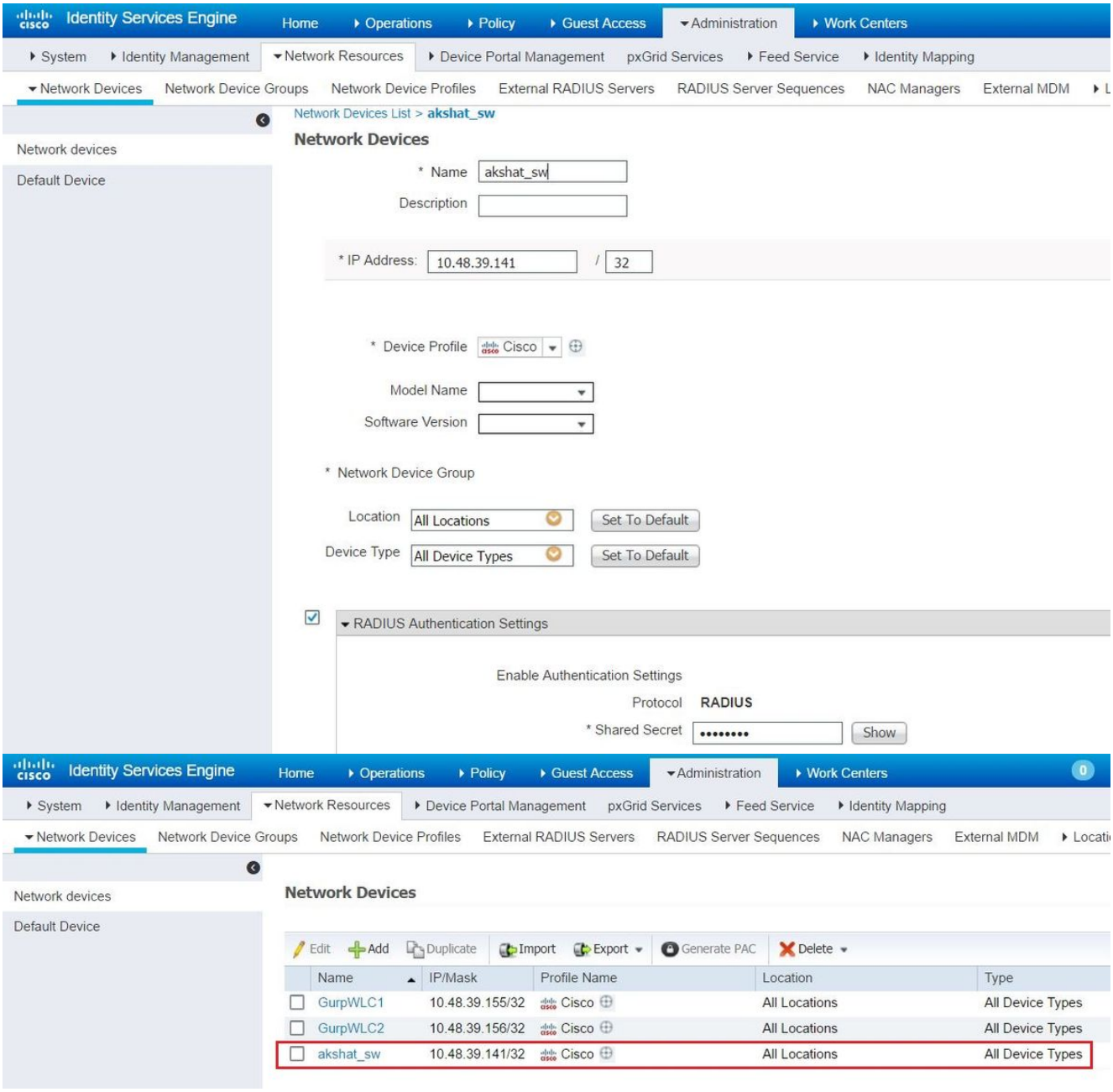
```
aaa new-model
!
aaa authentication dot1x default group radius
!
dot1x system-auth-control
!
radius server ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
  key 7 123A0C0411045D5679
```

2. Agora, configurar a porta de switch AP.

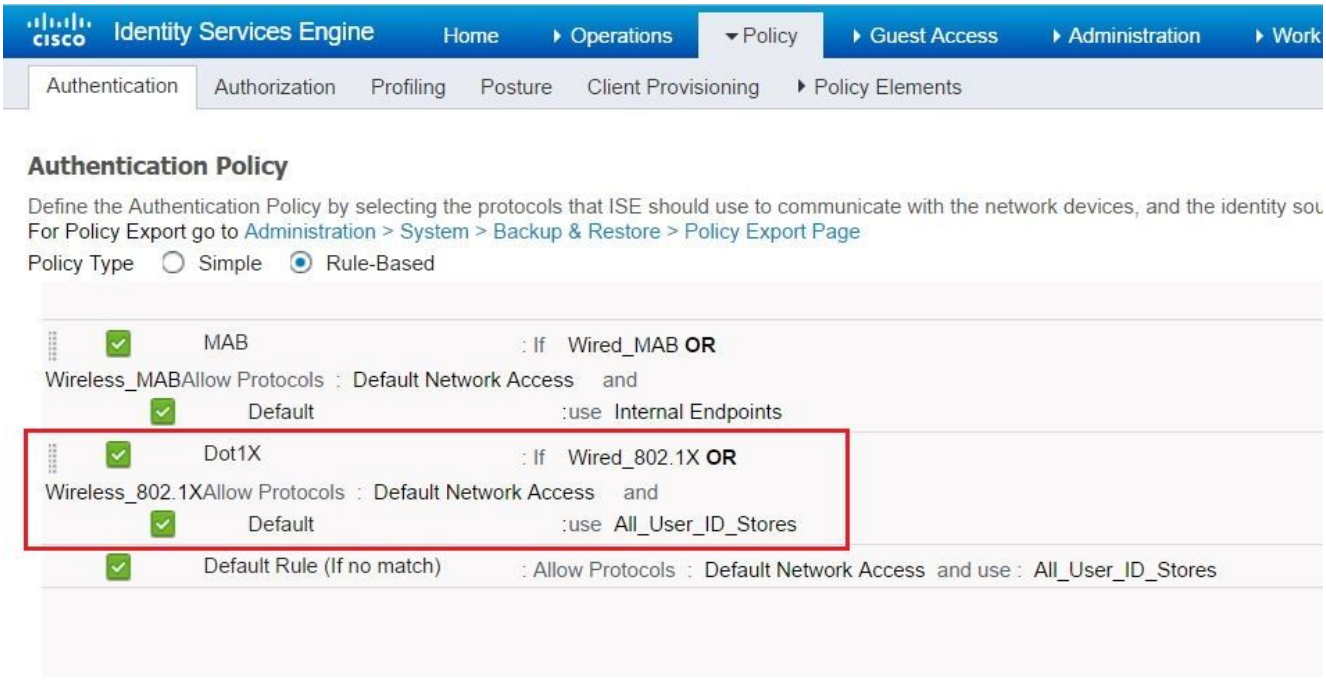
```
interface GigabitEthernet0/4


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

Configurar o server ISE

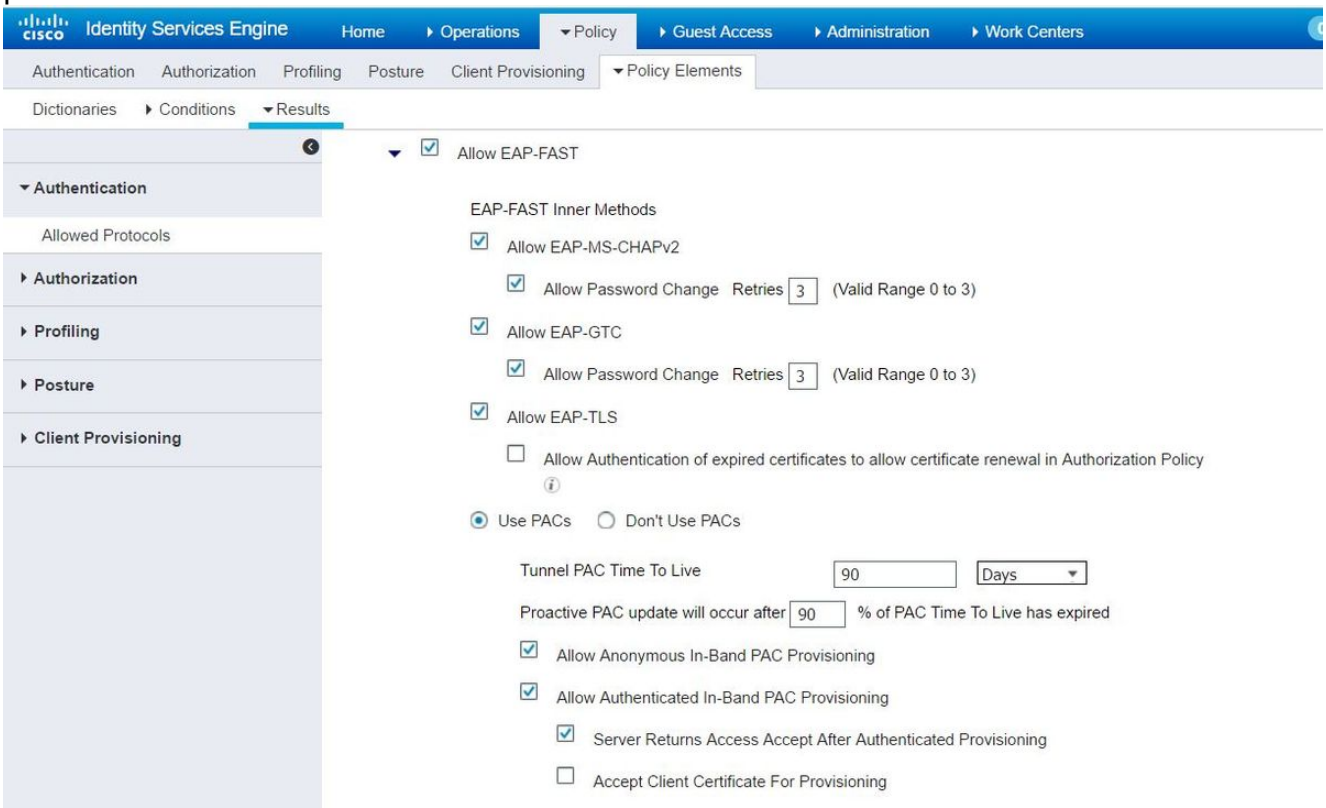
1. Adicionar o interruptor como um cliente do Authentication, Authorization, and Accounting (AAA) no server ISE.



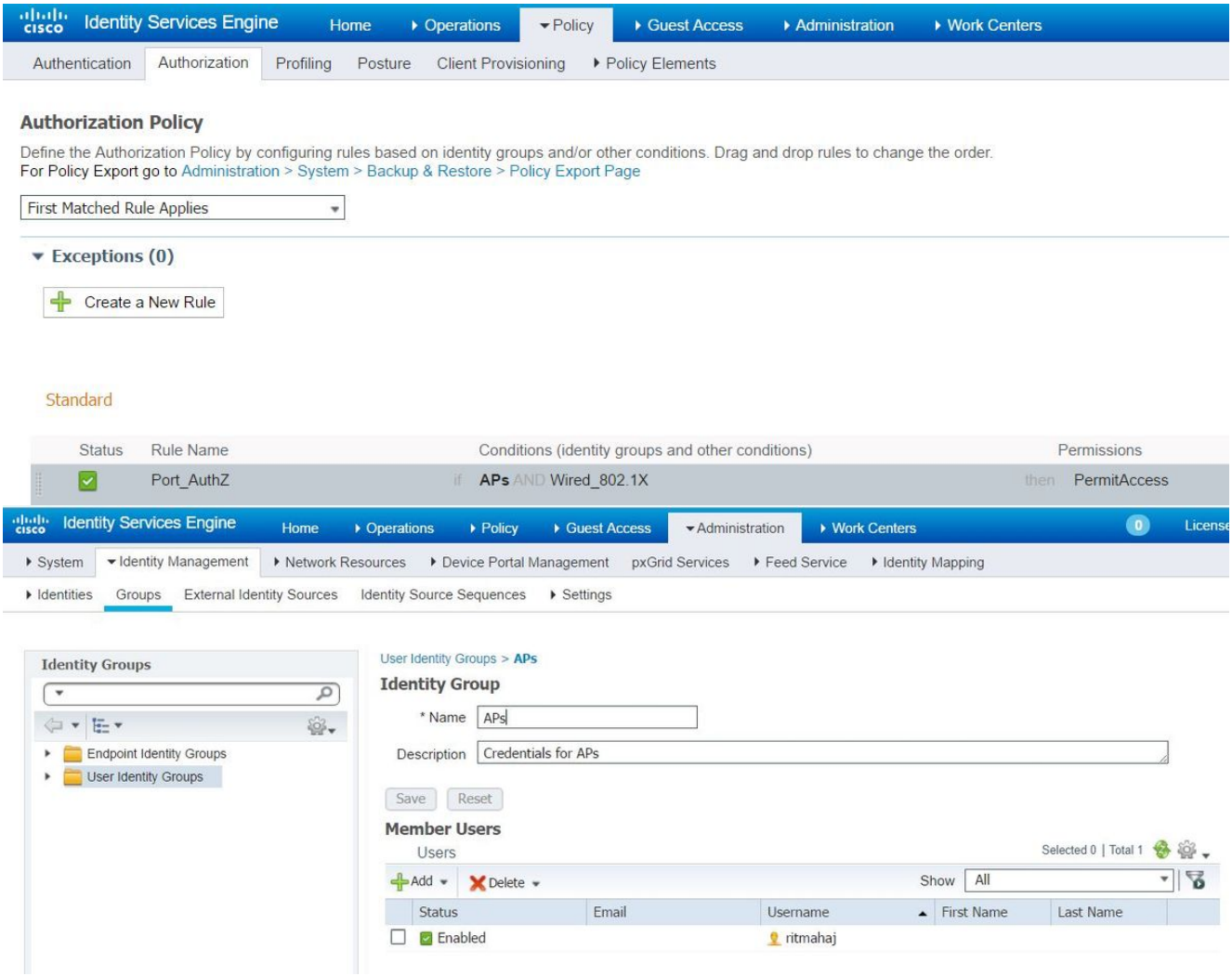
2. No ISE, configurar a política da política de autenticação e da autorização. Neste caso, a regra da autenticação padrão que é dot.1x prendido é usada, mas um pode personalizá-lo conforme a exigência.



Assegure isso nos protocolos permitidos que o acesso de rede padrão, EAP-FAST são permitidos.



3. Quanto para à política da autorização (Port_AuthZ), as credenciais AP foram adicionadas neste caso a um grupo de usuário (AP). A circunstância usada era “se o usuário pertence ao grupo AP e fazer o dot1x prendido, a seguir empurra o acesso da licença do perfil da autorização do padrão.” Além disso, isto pode ser personalizado conforme a exigência.



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Uma vez que o 802.1x é permitido na porta de switch, todo o tráfego a não ser que o tráfego do 802.1x seja obstruído através da porta. O REGAÇO, que se já registrado ao WLC, obtém dissociado. Somente depois que uma autenticação bem sucedida do 802.1x é o outro tráfego permitido passar completamente. O registro bem-sucedido do REGAÇO ao WLC depois que o 802.1x é permitido no interruptor indica que a autenticação do REGAÇO é bem sucedida. Você pode igualmente usar estes métodos a fim verificar se o REGAÇO autenticou.

1. No interruptor, inscreva um dos **comandos show** a fim verificar se a porta foi autenticada ou não.

```
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. No ISE, escolha **operações > raio Livelogs** e veja que a autenticação é bem sucedida e o perfil correto da autorização está empurrado.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

1. Inscreva o **comando ping** a fim verificar se o server ISE é alcançável do interruptor.
2. Certifique-se de que o interruptor está configurado como um cliente de AAA no server ISE.
3. Assegure-se de que o segredo compartilhado seja o mesmo entre o interruptor e o servidor ACS.
4. Verifique se EAP-FAST é permitido no server ISE.
5. Verifique se as credenciais do 802.1x são configuradas para o REGAÇO e são mesmas no server ISE. **Note**: O nome de usuário e senha é diferenciando maiúsculas e minúsculas.
6. Se a autenticação falha, incorpore estes comandos no interruptor: **debugar o dot1x** e o **debug authentication**.