Configure Lightweight Access Point as an 802.1x Supplicant

Introduction

This document describes how to configure a Lightweight Access Point (LAP) as an 802.1x supplicant in order to authenticate against the Identity Services Engine (ISE) server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Wireless Lan Controller (WLC) and LAP
- 802.1x on Cisco switches
- ISE
- Extensible Authentication Protocol (EAP) - Flexible Authentication via Secure Tunneling (FAST)

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

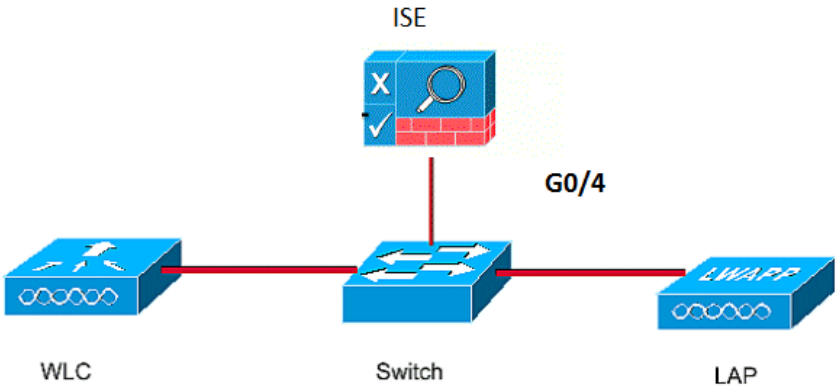
In this setup the access point (AP) acts as the 802.1x supplicant and is authenticated by the switch against the ISE that uses EAP-FAST with anonymous Protected Access Credentials (PAC) provisioning. Once the port is configured for 802.1x authentication, the switch does not allow any traffic other than 802.1x traffic to pass through the port until the device connected to the port authenticates successfully. An AP can be authenticated either before it joins a WLC or after it has joined a WLC, in which case you configure 802.1x on the switch after the LAP joins the WLC.

Configure

In this section, you are presented with the information to configure the features described in this document.

Network Diagram

This document uses this network setup:



Configurations

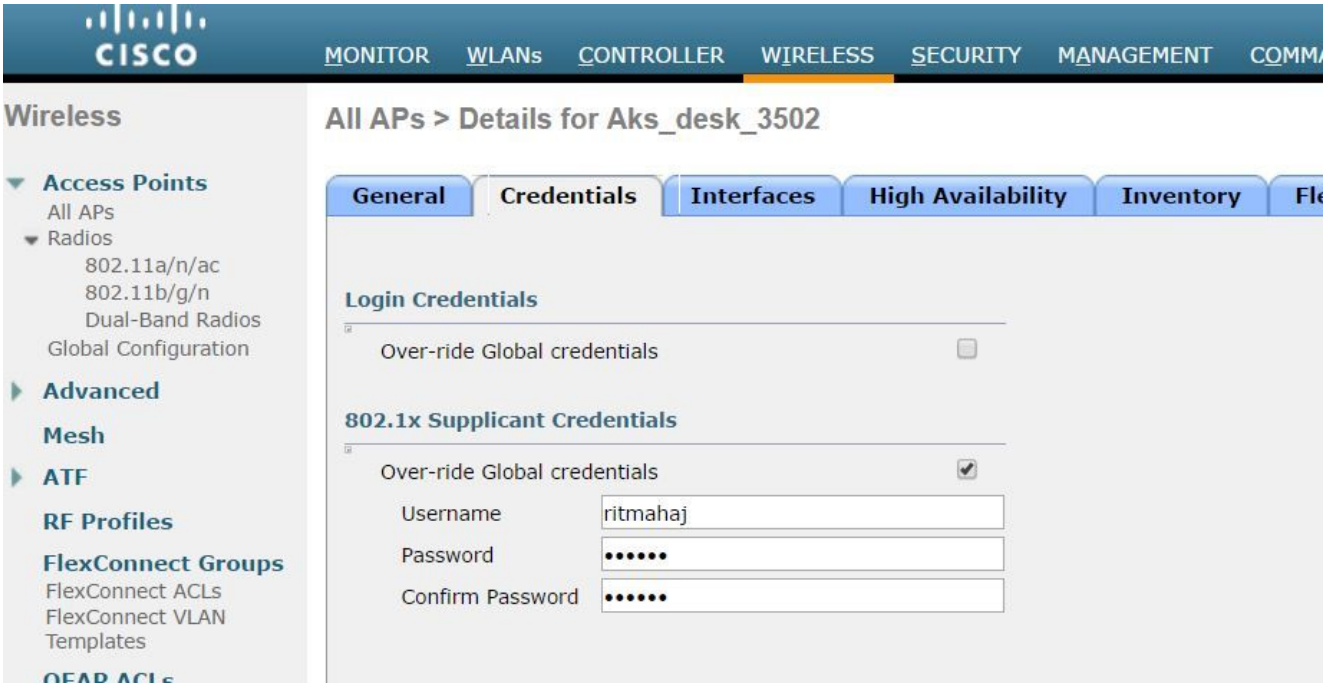
This document uses these IP addresses:

- IP address of the switch is 10.48.39.141
- IP address of the ISE server is 10.48.39.161
- IP address of the WLC is 10.48.39.142

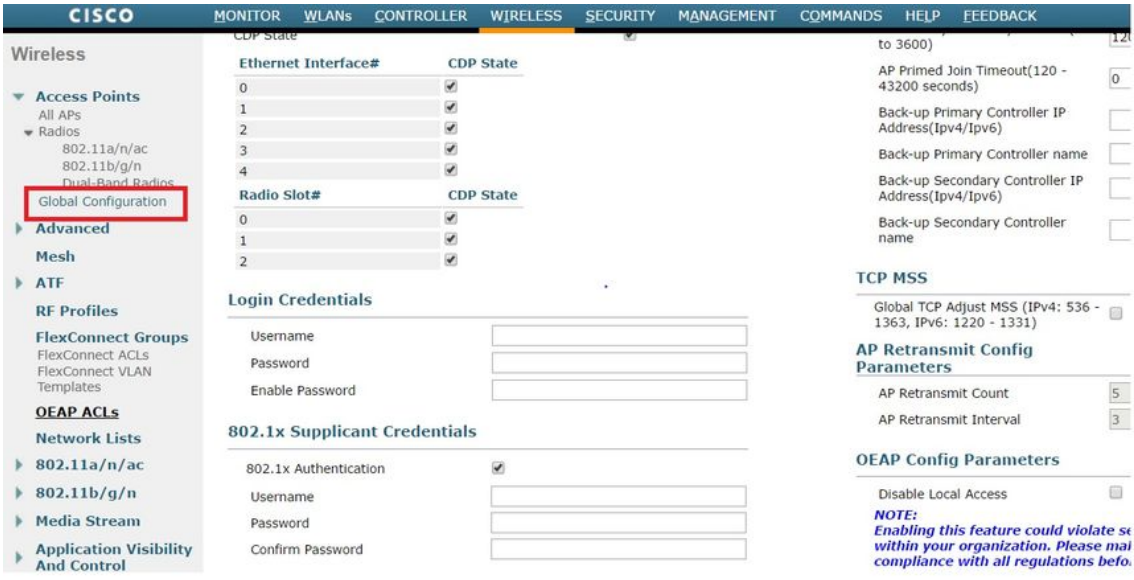
Configure the LAP

In this section, you are presented with the information to configure the LAP as a 802.1x supplicant.

1. If the AP is already joined to the WLC, go the Wireless tab and click on the AP, go the Credentials field and under the 802.1x Supplicant Credentials heading, check the **Over-ride Global credentials** check box in order to set the 802.1x username and password for this AP.



You can also set a common username and password for all the APs that are joined to the WLC with the Global Configuration
menu.



2. If the AP has not joined a WLC yet, you must console into the LAP in order to set the credentials and use these CLI commands:

```
LAP#debug capwap console cli
LAP#capwap ap dot1x username <username> password <password>
```

Configure the Switch

1. Enable dot1x on the switch globally and add the ISE server to the 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
```

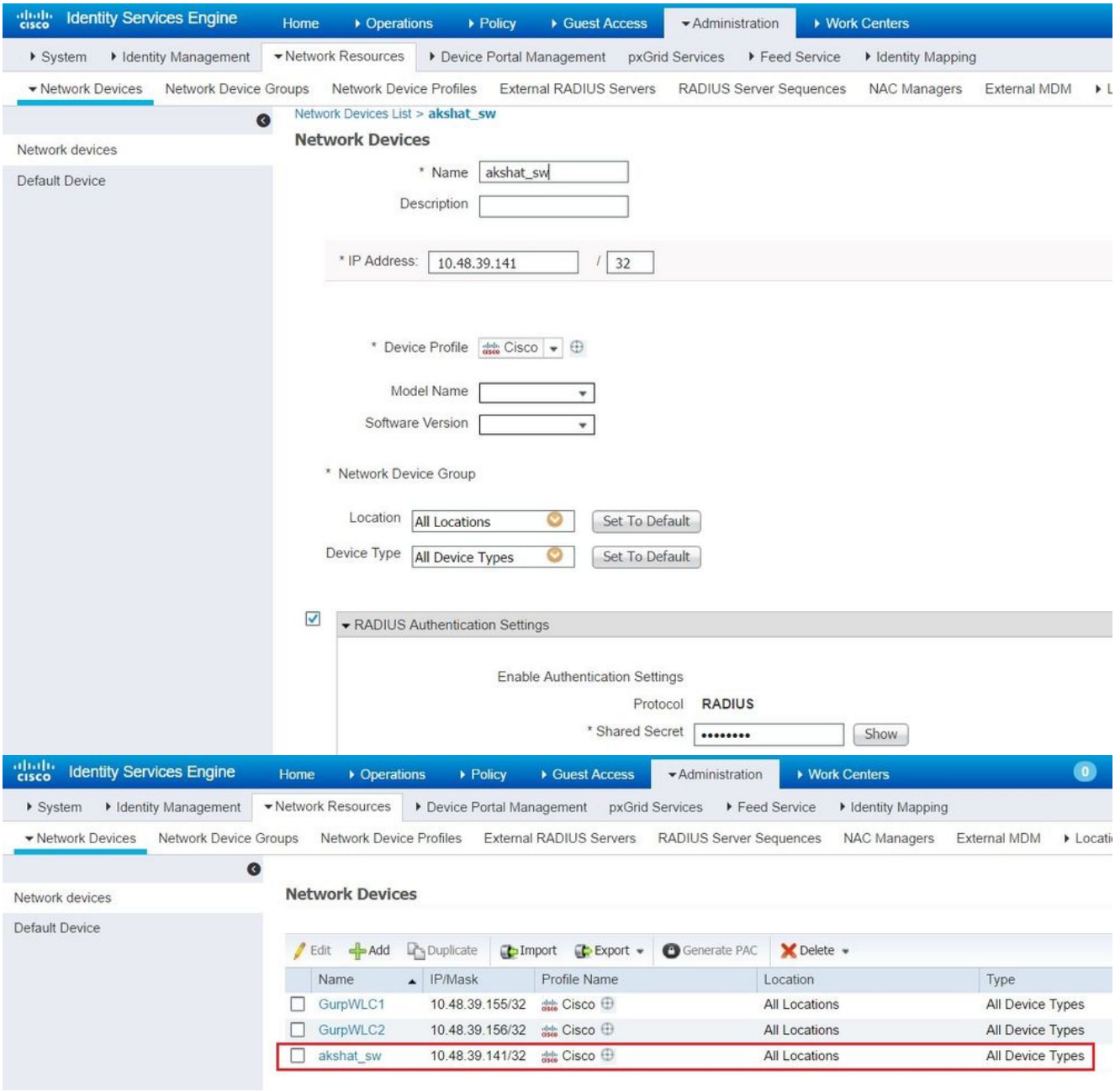
2. Now, configure the AP switch port.

```
interface GigabitEthernet0/4


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

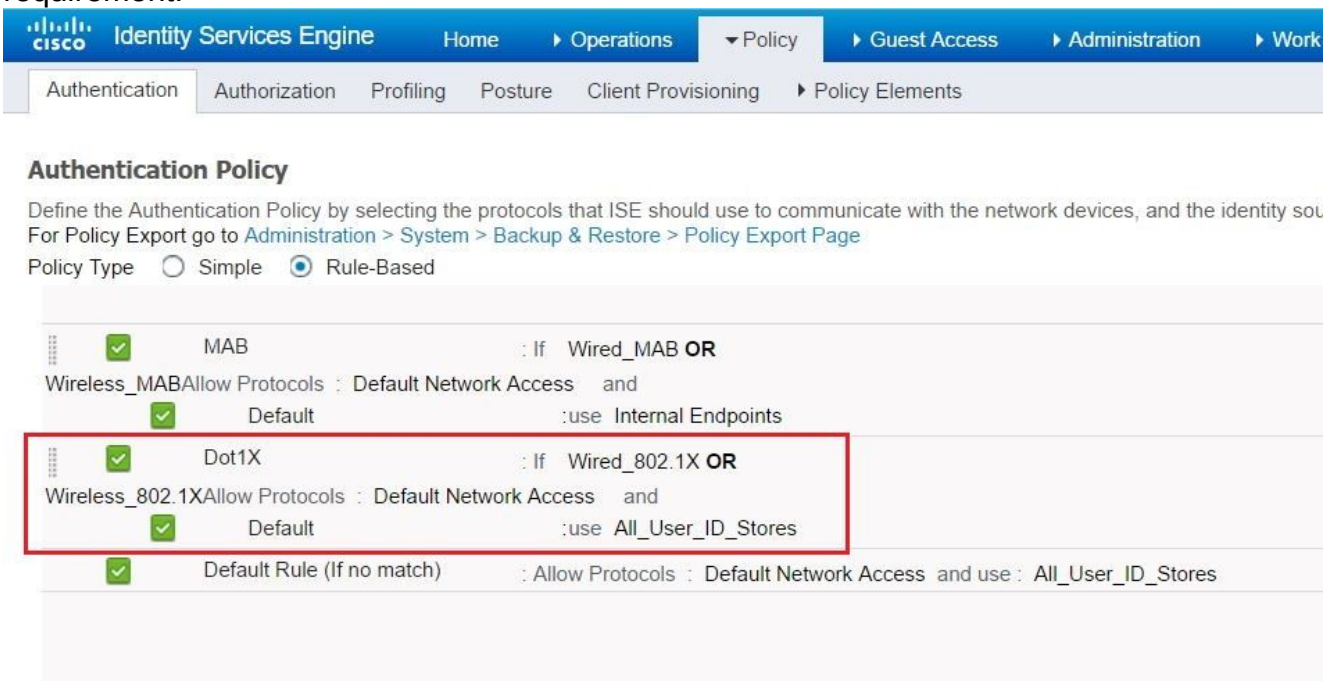
Configure the ISE Server

1. Add the switch as an Authentication, Authorization, and Accounting (AAA) client on the ISE server.

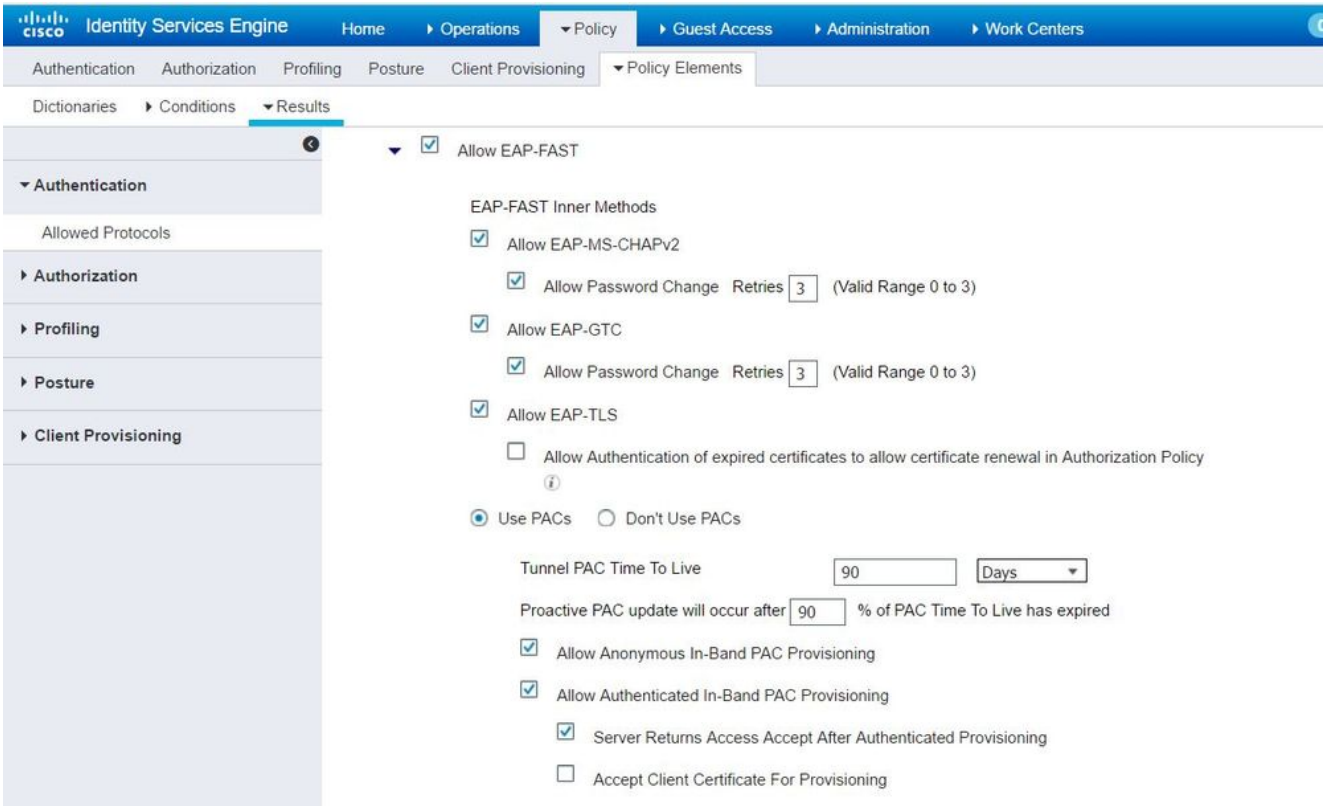


2. On ISE, configure the Authentication policy and Authorization policy. In this case, the default

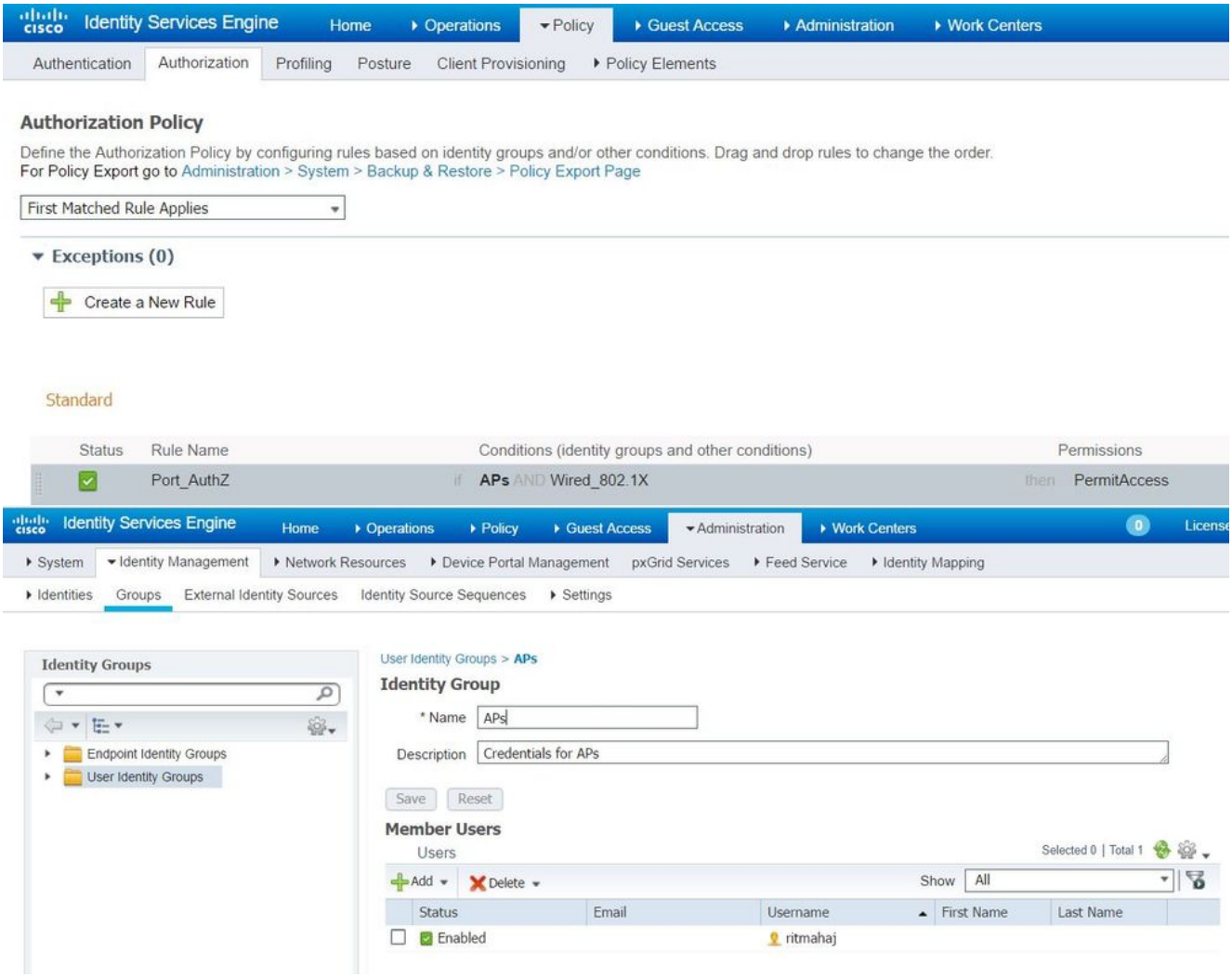
authentication rule which is wired dot.1x is used, but one can customize it as per the requirement.



Ensure that in the allowed protocols that Default Network Access, EAP-FAST is allowed.



3. As for the Authorization policy (Port_AuthZ), in this case AP credentials were added to a user group (APs). The condition used was "If the user belongs to the group AP and doing wired dot1x, then push the default Authorization Profile permit access." Again, this can be customized as per the requirement.



Verify

Use this section in order to confirm that your configuration works properly.

Once 802.1x is enabled on the switch port, all the traffic except the 802.1x traffic is blocked through the port. The LAP, which if already registered to the WLC, gets disassociated. Only after a successful 802.1x authentication is other traffic allowed to pass through. Successful registration of the LAP to the WLC after the 802.1x is enabled on the switch indicates that the LAP authentication is successful. You can also use these methods in order to verify if the LAP authenticated.

1. On the switch, enter one of the **show** commands in order to verify if the port has been authenticated or not.

```
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
```

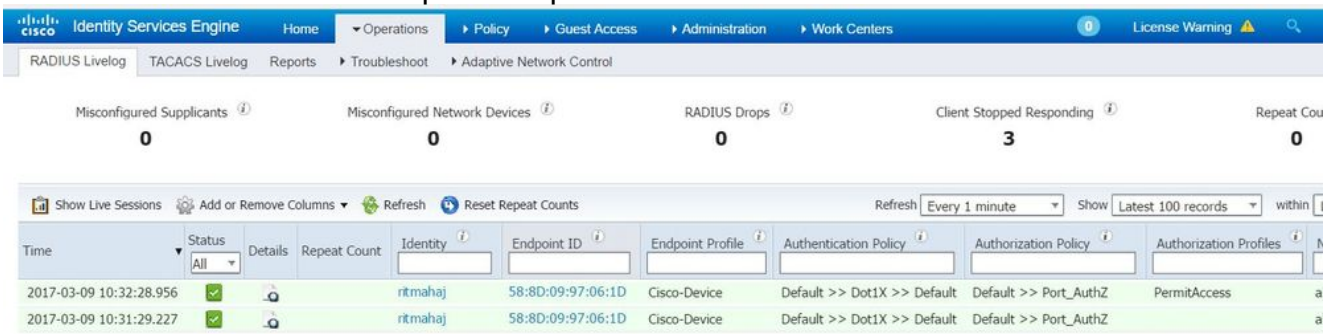
```
Dot1x Info for GigabitEthernet0/4
-----------------------------------
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30


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. In ISE, choose **Operations > Radius Livelogs** and see that the authentication is successful and the correct Authorization profile is pushed.



Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

1. Enter the **ping** command in order to check if the ISE server is reachable from the switch.
2. Make sure that the switch is configured as an AAA client on the ISE server.
3. Ensure that the shared secret is the same between switch and the ACS server.
4. Check if EAP-FAST is enabled on the ISE server.
5. Check if the 802.1x credentials are configured for the LAP and are same on the ISE server. **Note**: The username and password are case sensitive.
6. If authentication fails, enter these commands on the switch: **debug dot1x** and **debug authentication**.