Konfigurieren eines Lightweight Access Points als 802.1x-Komponente

Einführung

In diesem Dokument wird beschrieben, wie ein Lightweight Access Point (LAP) als 802.1x-Komponente konfiguriert wird, um sich gegen den ISE-Server (Identity Services Engine) zu authentifizieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Wireless LAN Controller (WLC) und LAP
- 802.1x auf Cisco Switches
- ISE
- Extensible Authentication Protocol (EAP) - Flexible Authentication via Secure Tunneling (FAST)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

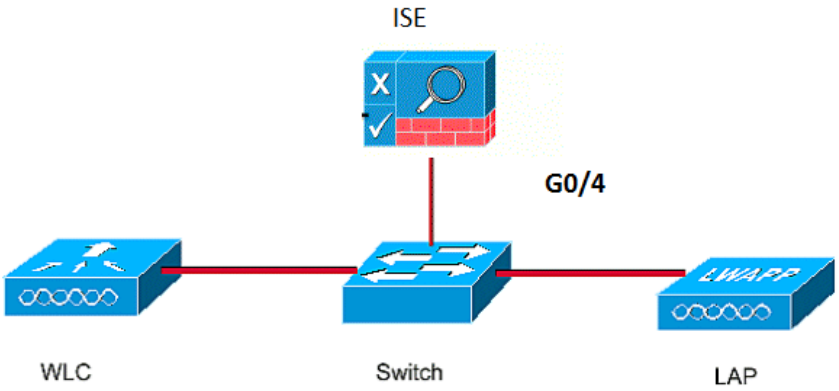
In dieser Konfiguration fungiert der Access Point (AP) als 802.1x-Komponente und wird vom Switch gegenüber der ISE authentifiziert, die EAP-FAST mit anonymer PAC-Bereitstellung (Protected Access Credentials, anonyme geschützte Zugriffsberechtigungen) verwendet. Nachdem der Port für die 802.1x-Authentifizierung konfiguriert wurde, lässt der Switch zu, dass außer 802.1x-Datenverkehr kein Datenverkehr den Port durchläuft, bis das mit dem Port verbundene Gerät erfolgreich authentifiziert wird. Ein WAP kann entweder authentifiziert werden, bevor er einem WLC beitritt, oder nachdem er einem WLC beigetreten ist. In diesem Fall konfigurieren Sie 802.1x auf dem Switch, nachdem die LAP dem WLC beitritt.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende IP-Adressen verwendet:

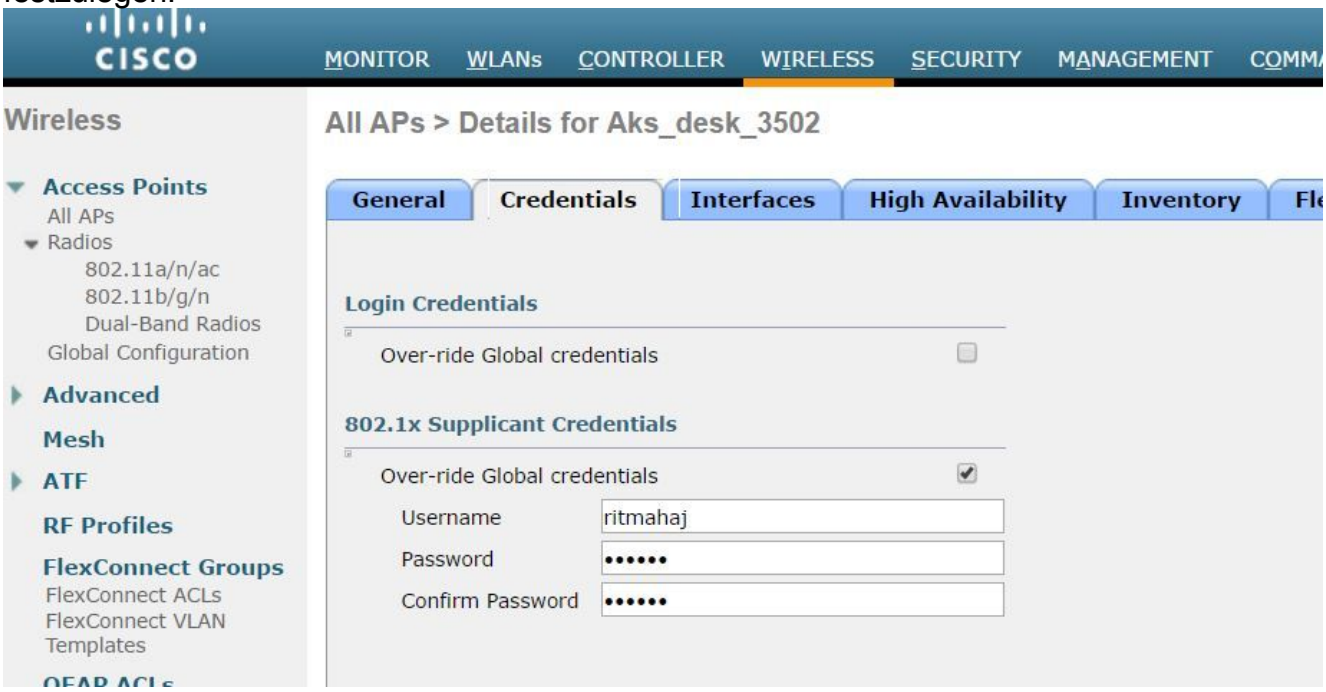
- Die IP-Adresse des Switches lautet 10.48.39.141.
- Die IP-Adresse des ISE-Servers lautet 10.48.39.161.
- Die IP-Adresse des WLC lautet 10.48.39.142.

Konfigurieren der LAP

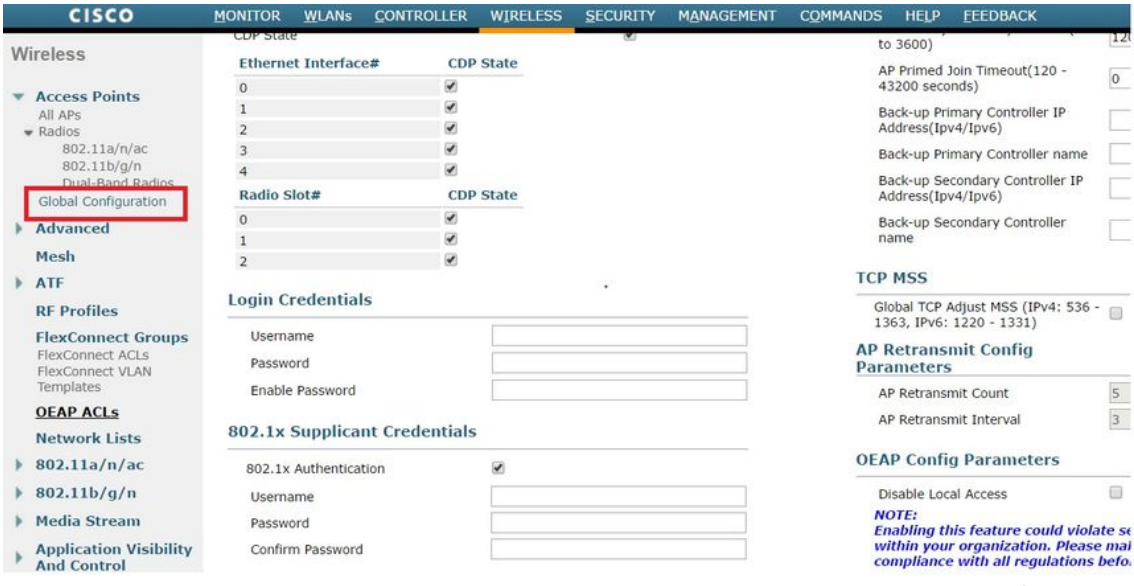
In diesem Abschnitt erhalten Sie Informationen zur Konfiguration der LAP als 802.1x-Komponente.

1. Wenn der Access Point bereits dem WLC beigetreten ist, wechseln Sie zur Registerkarte Wireless und klicken Sie auf den Access Point. Wechseln Sie dann zum Feld Credentials (Anmeldeinformationen für 802.1x), und aktivieren Sie unter der Überschrift 802.1x Supplicant Credentials (Anmeldeinformationen für 802.1x-Zusatzkomponenten) das Kontrollkästchen **Over-ride Global**, um den Benutzernamen und das Kennwort für diesen AP

festzulegen.



Sie können auch einen gemeinsamen Benutzernamen und ein gemeinsames Kennwort für alle APs festlegen, die dem WLC über das Menü "Global Configuration" (Globale Konfiguration) zugeordnet
sind.



2. Wenn der Access Point noch nicht einem WLC beigetreten ist, müssen Sie sich in die LAP einwählen, um die Anmeldeinformationen festzulegen und die folgenden CLI-Befehle zu verwenden:

LAP#**debug capwap console cli**
LAP#**capwap ap dot1x username**

Switch konfigurieren

1. Aktivieren Sie dot1x auf dem Switch global, und fügen Sie den ISE-Server zum Switch hinzu.

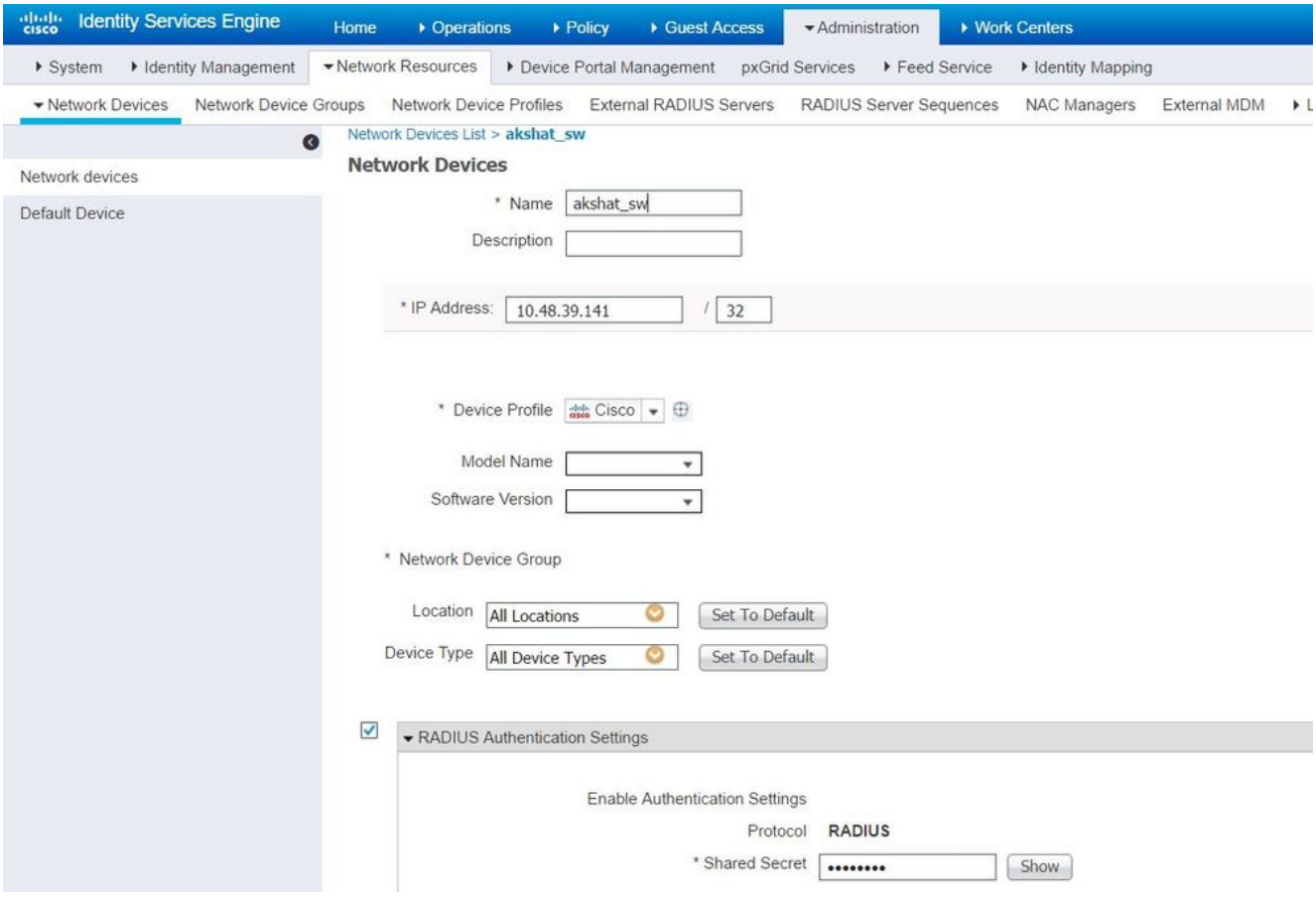
```
aaa new-model
!
aaa authentication dot1x default group radius
!
dot1x system-auth-control
!
radius server ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
  key 7 123A0C0411045D5679
```

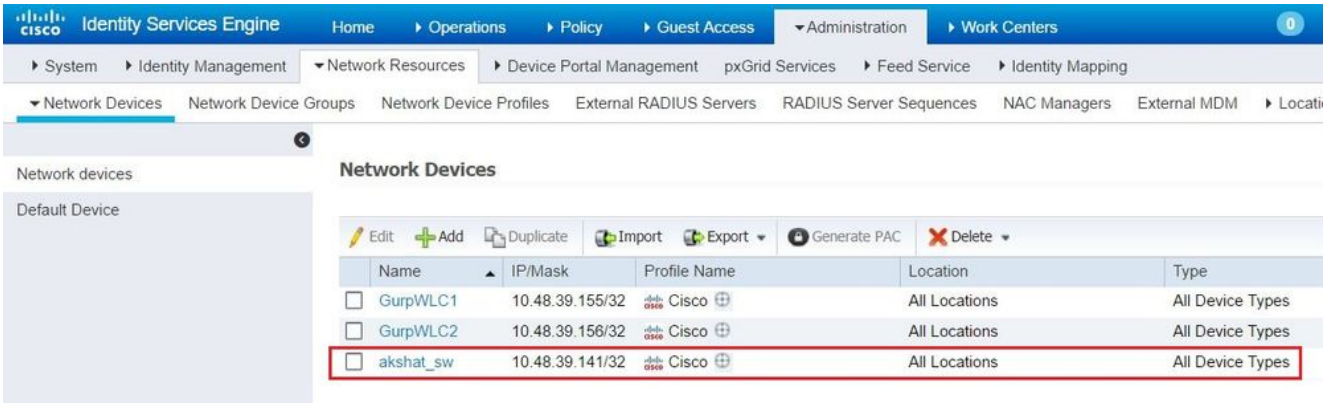
2. Konfigurieren Sie jetzt den AP-Switch-Port.

```
interface GigabitEthernet0/4


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

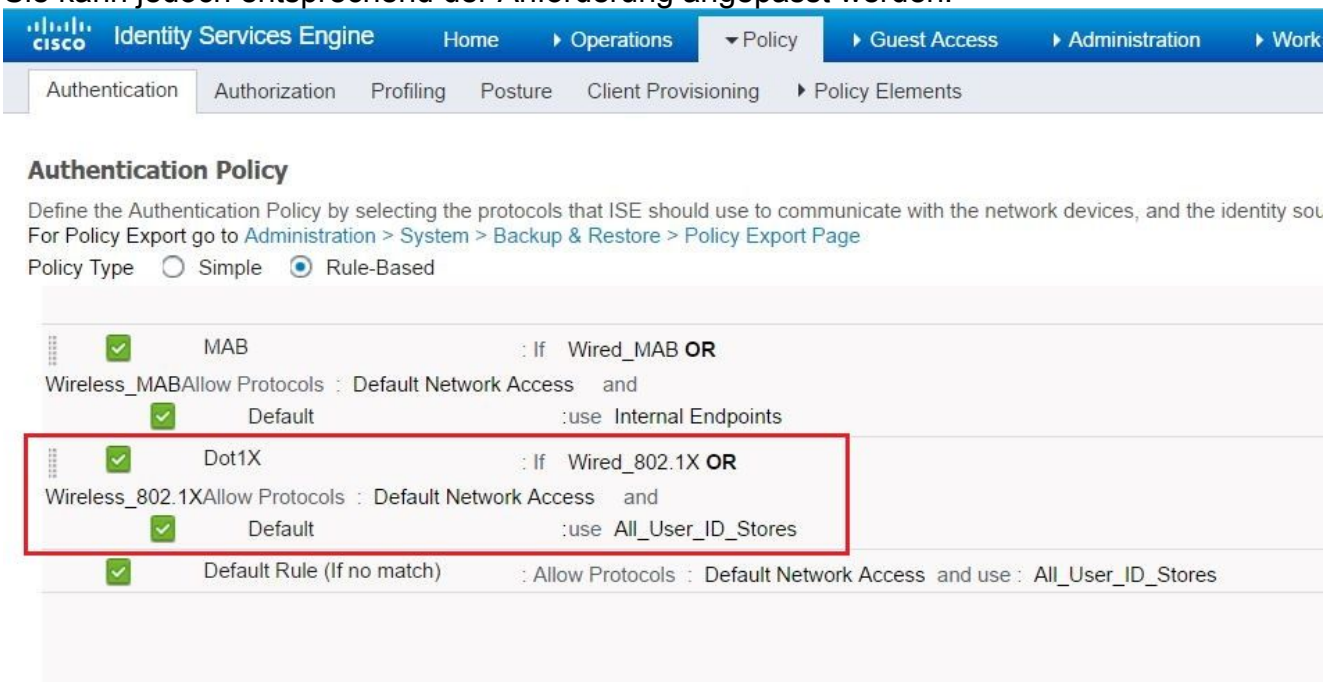
Konfigurieren des ISE-Servers

1. Fügen Sie den Switch als AAA-Client (Authentication, Authorization, and Accounting) auf dem ISE-Server hinzu.

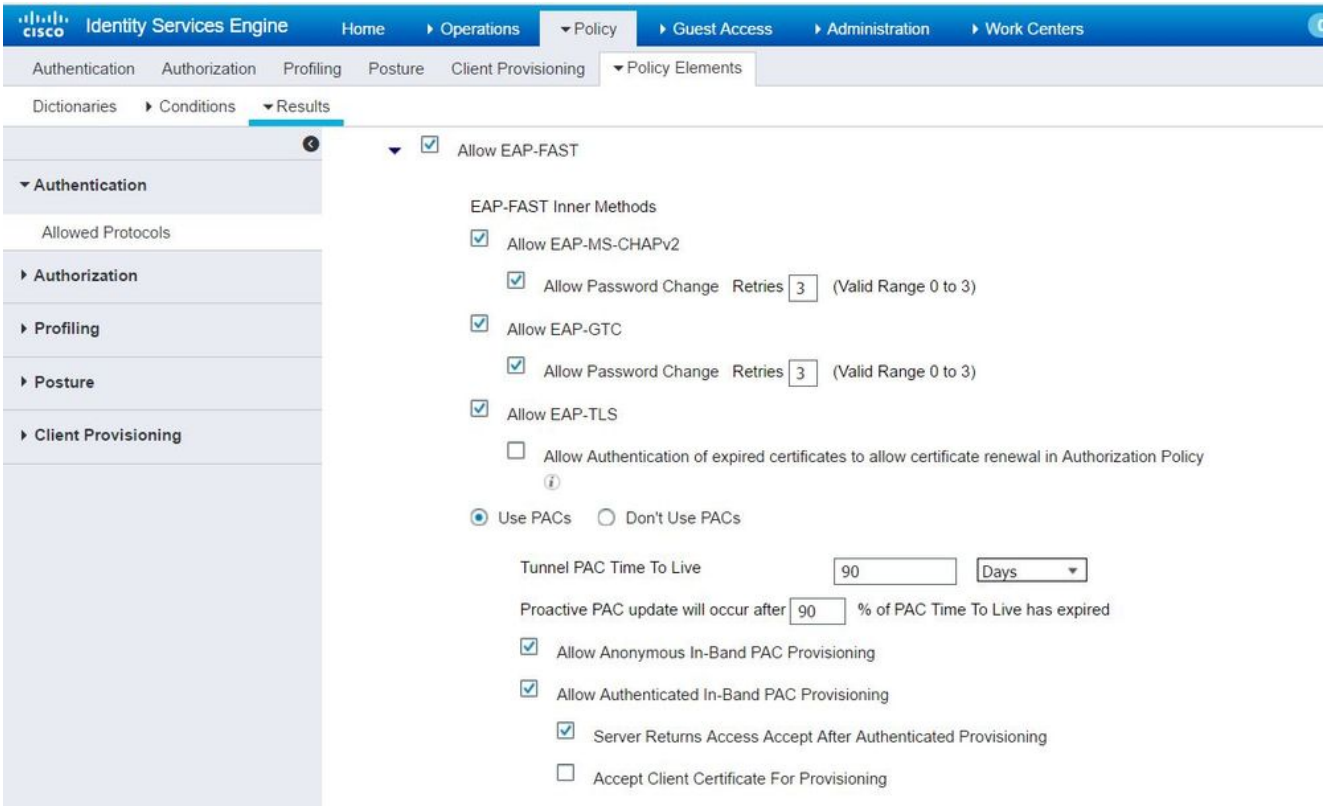




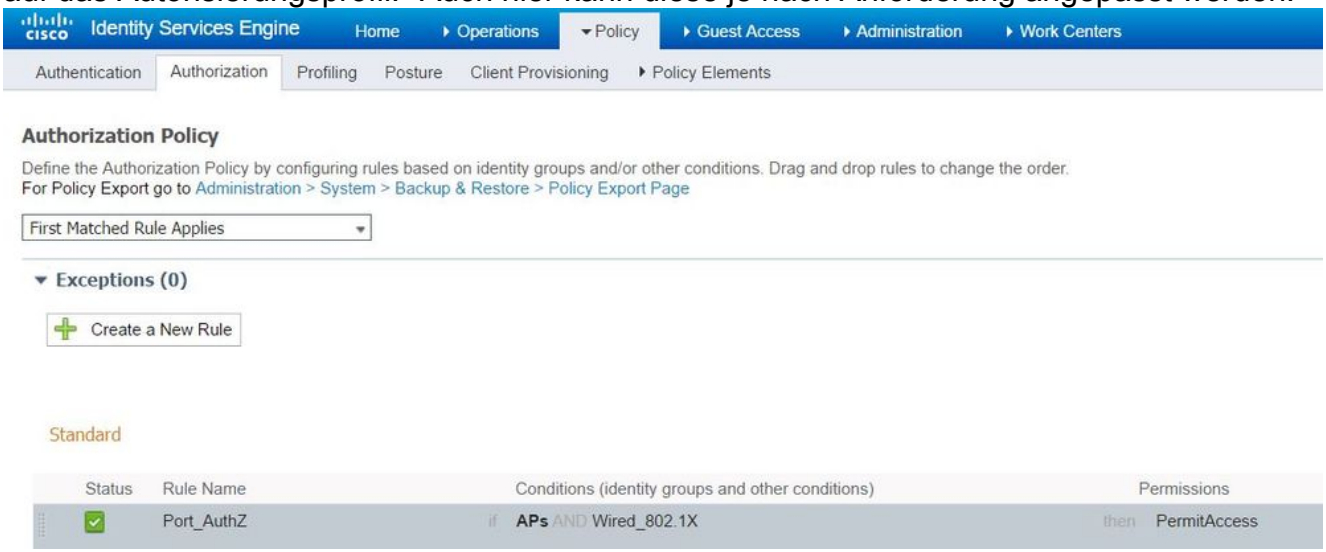
2. Konfigurieren Sie auf der ISE die Authentifizierungsrichtlinie und die Autorisierungsrichtlinie. In diesem Fall wird die Standardauthentifizierungsregel verwendet, die dot.1x verkabelt ist. Sie kann jedoch entsprechend der Anforderung angepasst werden.

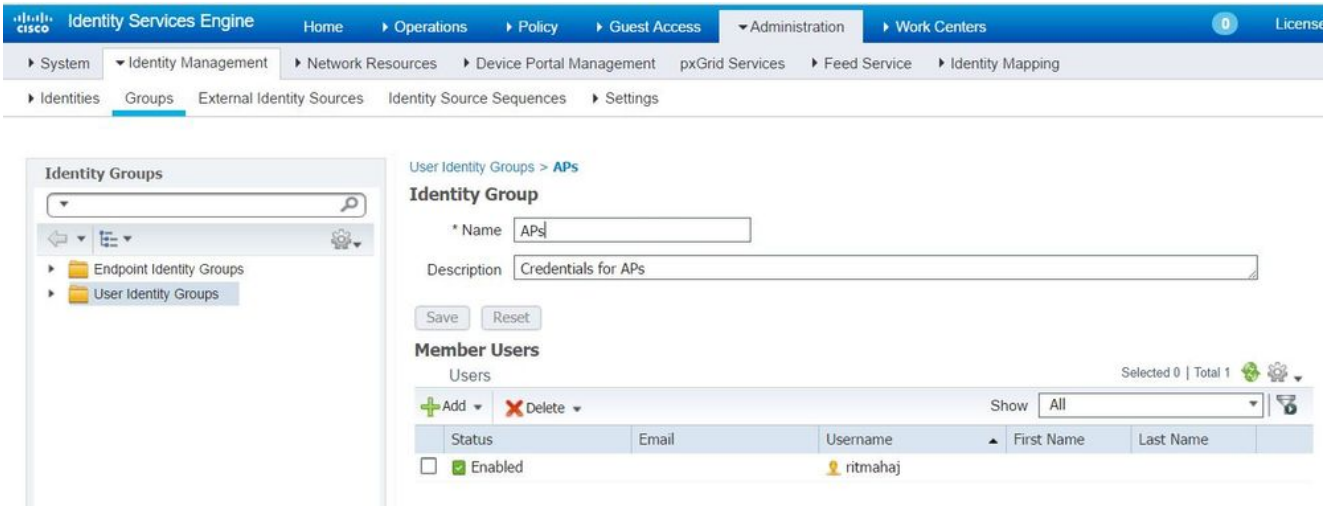


Stellen Sie sicher, dass in den zulässigen Protokollen, die Standard-Netzwerkzugriff, EAP-FAST zulässig
ist.



3. Wie bei der Autorisierungsrichtlinie (Port_AuthZ) wurden in diesem Fall AP-Anmeldeinformationen zu einer Benutzergruppe (APs) hinzugefügt. Die verwendete Bedingung lautete: "Wenn der Benutzer zur Gruppe Access Point gehört und einen kabelgebundenen dot1x-Vorgang durchführt, drücken Sie dann den standardmäßigen Zugriff auf das Autorisierungsprofil." Auch hier kann diese je nach Anforderung angepasst werden.





Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

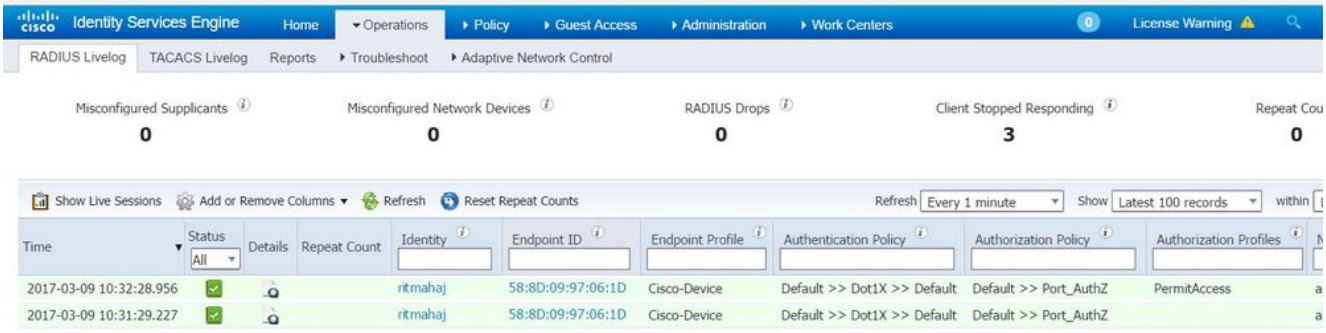
Wenn 802.1x auf dem Switch-Port aktiviert ist, wird der gesamte Datenverkehr bis auf 802.1x über den Port blockiert. Die LAP, die bereits beim WLC registriert ist, wird getrennt. Nur nach erfolgreicher 802.1x-Authentifizierung darf anderer Datenverkehr passieren. Die erfolgreiche Registrierung der LAP beim WLC nach dem Aktivieren des 802.1x-Standards auf dem Switch zeigt an, dass die LAP-Authentifizierung erfolgreich ist. Sie können diese Methoden auch verwenden, um zu überprüfen, ob die LAP authentifiziert wurde.

1. Geben Sie auf dem Switch einen der **show**-Befehle ein, um zu überprüfen, ob der Port authentifiziert wurde oder nicht.

```
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. Wählen Sie in ISE **Operations > Radius Livelogs** aus, und prüfen Sie, ob die Authentifizierung erfolgreich ist und das richtige Authorization-Profil gedrückt wird.



Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

1. Geben Sie den Befehl **ping ein**, um zu überprüfen, ob der ISE-Server vom Switch aus erreichbar ist.
2. Stellen Sie sicher, dass der Switch als AAA-Client auf dem ISE-Server konfiguriert ist.
3. Stellen Sie sicher, dass der gemeinsame geheime Schlüssel zwischen Switch und ACS-Server identisch ist.
4. Überprüfen Sie, ob EAP-FAST auf dem ISE-Server aktiviert ist.
5. Überprüfen Sie, ob die 802.1x-Anmeldeinformationen für die LAP konfiguriert sind und auf dem ISE-Server identisch sind. **Hinweis**: Bei Benutzername und Kennwort wird zwischen Groß- und Kleinschreibung unterschieden.
6. Wenn die Authentifizierung fehlschlägt, geben Sie diese Befehle auf dem Switch ein: **debug dot1x** und **Debug-Authentifizierung**.