Konfigurieren von Catalyst 9800 WLC iPSK mithilfe der ISE

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration eines durch iPSK gesicherten WLAN auf einem Cisco Wireless LAN Controller der Serie 9800 mit der Cisco ISE als RADIUS-Server.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass Sie bereits mit der Basiskonfiguration eines WLAN auf dem 9800 vertraut sind und diese Konfiguration an Ihre Bereitstellung anpassen können.

Verwendete Komponenten

- Cisco 9800-CL WLC mit 17.6.3
- Cisco ISE 3.0

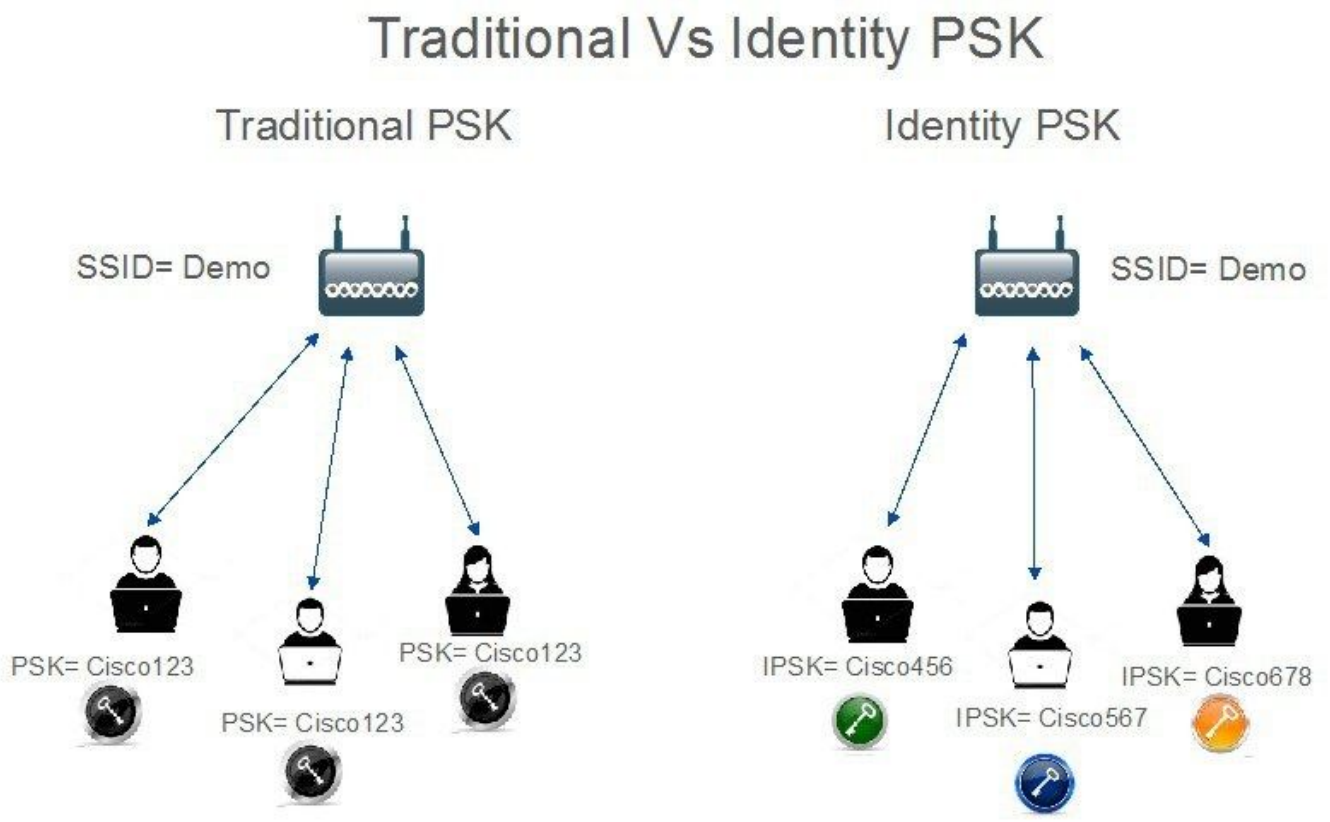
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Verständnis von iPSK und den passenden Szenarien

In herkömmlichen PSK-Netzwerken (Pre-Shared Key) wird für alle verbundenen Clients dasselbe Kennwort verwendet. Dies kann dazu führen, dass der Schlüssel für nicht autorisierte Benutzer freigegeben wird und eine Sicherheitsverletzung sowie nicht autorisierter Zugriff auf das Netzwerk verursacht werden. Die häufigste Abschwächung dieser Sicherheitsverletzung ist die Änderung

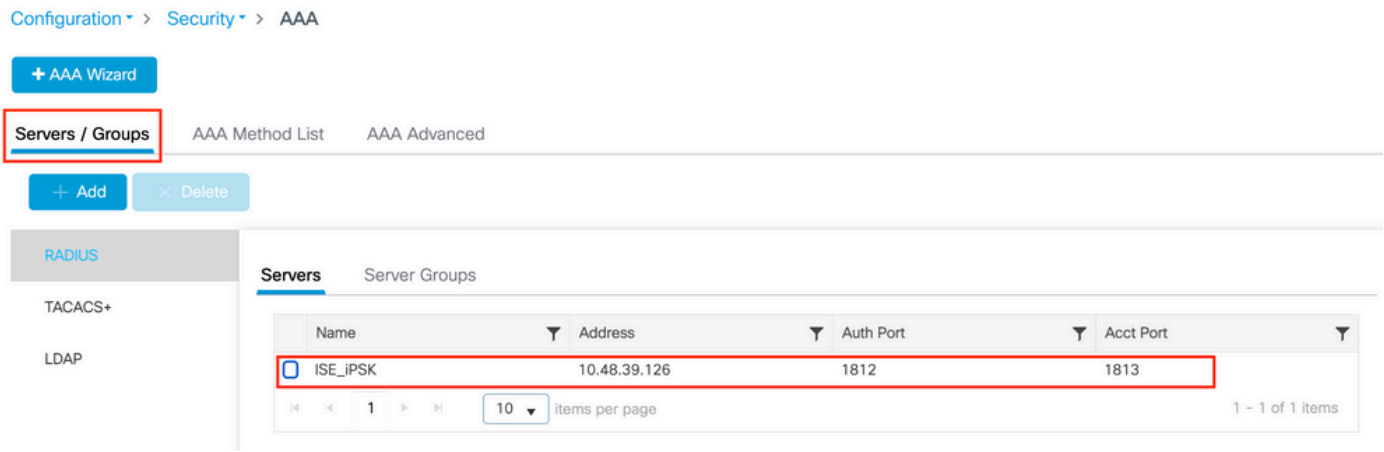
des PSK selbst, eine Änderung, die sich auf alle Benutzer auswirkt, da viele Endgeräte mit dem neuen Schlüssel aktualisiert werden müssen, um wieder auf das Netzwerk zugreifen zu können.

Mit Identity PSK (iPSK) werden mithilfe eines RADIUS-Servers eindeutige vorinstallierte Schlüssel für Einzelpersonen oder eine Gruppe von Benutzern auf derselben SSID erstellt. Diese Art von Konfiguration ist äußerst nützlich in Netzwerken, in denen Endclientgeräte keine 802.1x-Authentifizierung unterstützen, aber ein sichereres und präziseres Authentifizierungsschema erforderlich ist. Aus Client-Sicht ist dieses WLAN mit dem herkömmlichen PSK-Netzwerk identisch. Bei Kompromittierung eines PSKs muss nur dessen PSK aktualisiert werden. Die übrigen mit dem WLAN verbundenen Geräte sind davon nicht betroffen.



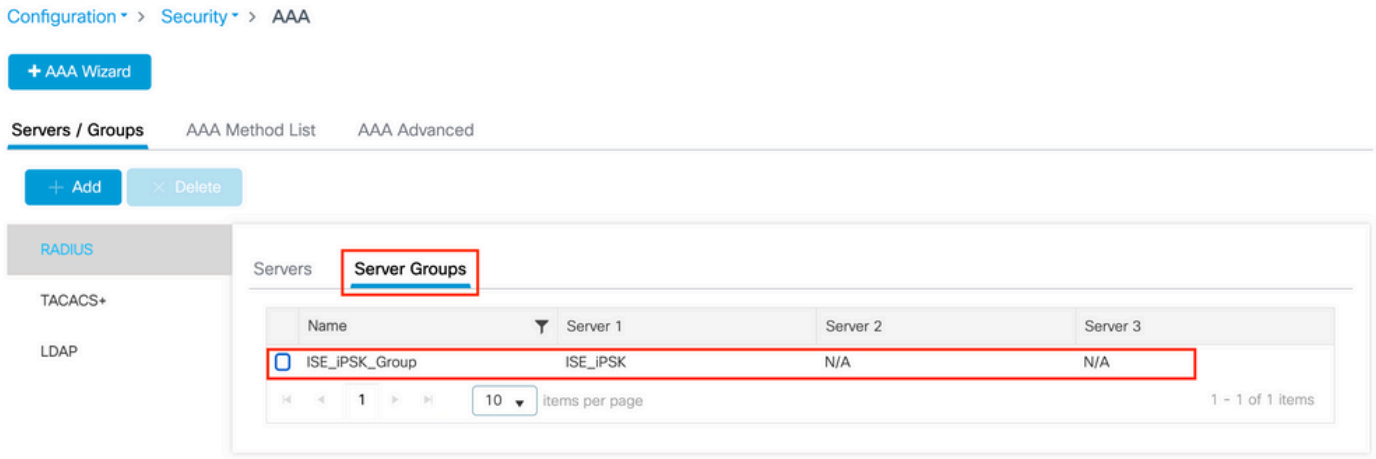
Konfigurieren des 9800 WLC

Fügen Sie unter **Configuration > Security > AAA > Servers/Groups > Servers** die ISE als RADIUS-Server hinzu:

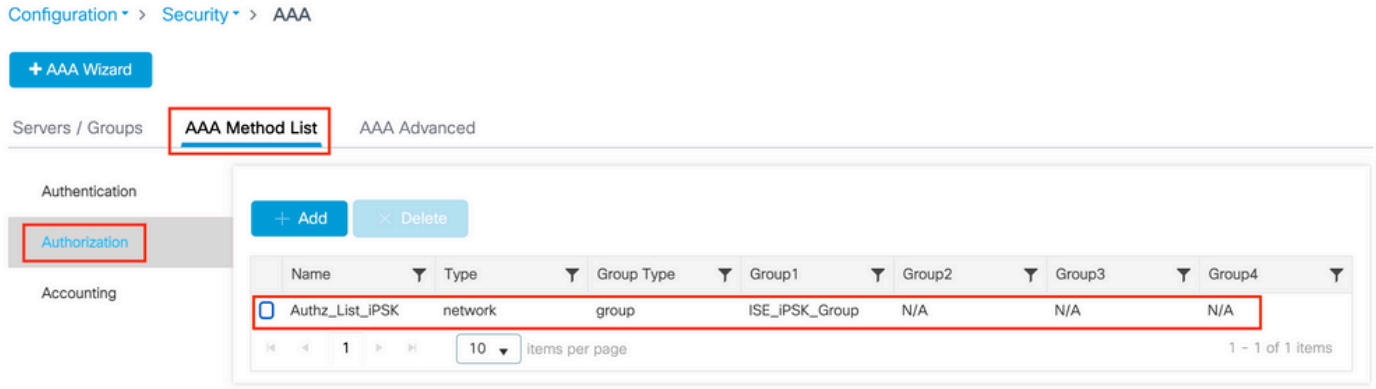


Erstellen Sie unter **Configuration > Security > AAA > Servers/Groups > Server Groups** eine

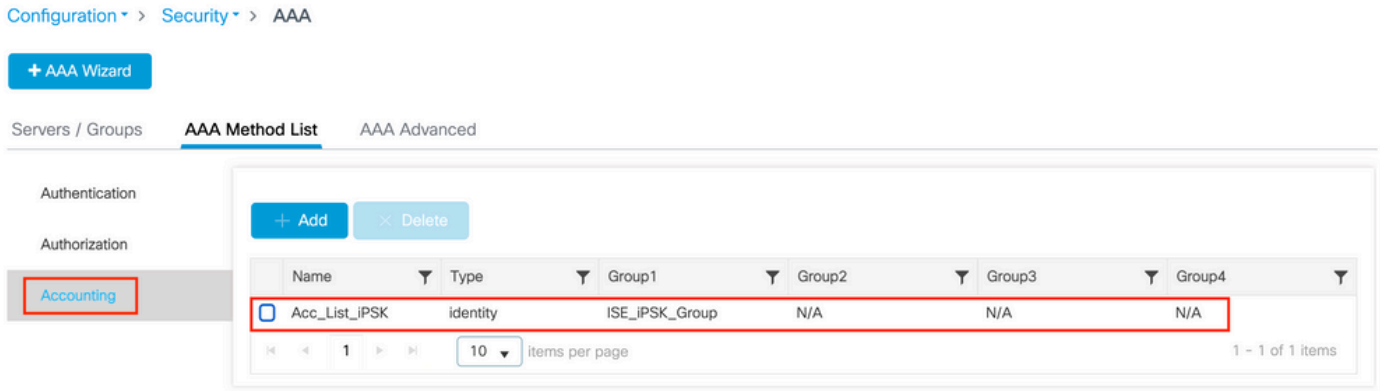
RADIUS-Servergruppe, und fügen Sie ihr den zuvor erstellten ISE-Server hinzu:



Erstellen Sie auf der Registerkarte **AAA Method List** eine **Autorisierungsliste** mit dem Typ "**network**" und dem Gruppentyp "**group**", **der auf die zuvor erstellte RADIUS-Servergruppe verweist:**



Das Einrichten der Kontoführung ist optional, kann jedoch durch Konfigurieren von Type auf "**identity**" und Verweisen auf dieselbe RADIUS-Servergruppe erfolgen:



Dies kann auch über die Befehlszeile mit folgenden Befehlen durchgeführt werden:

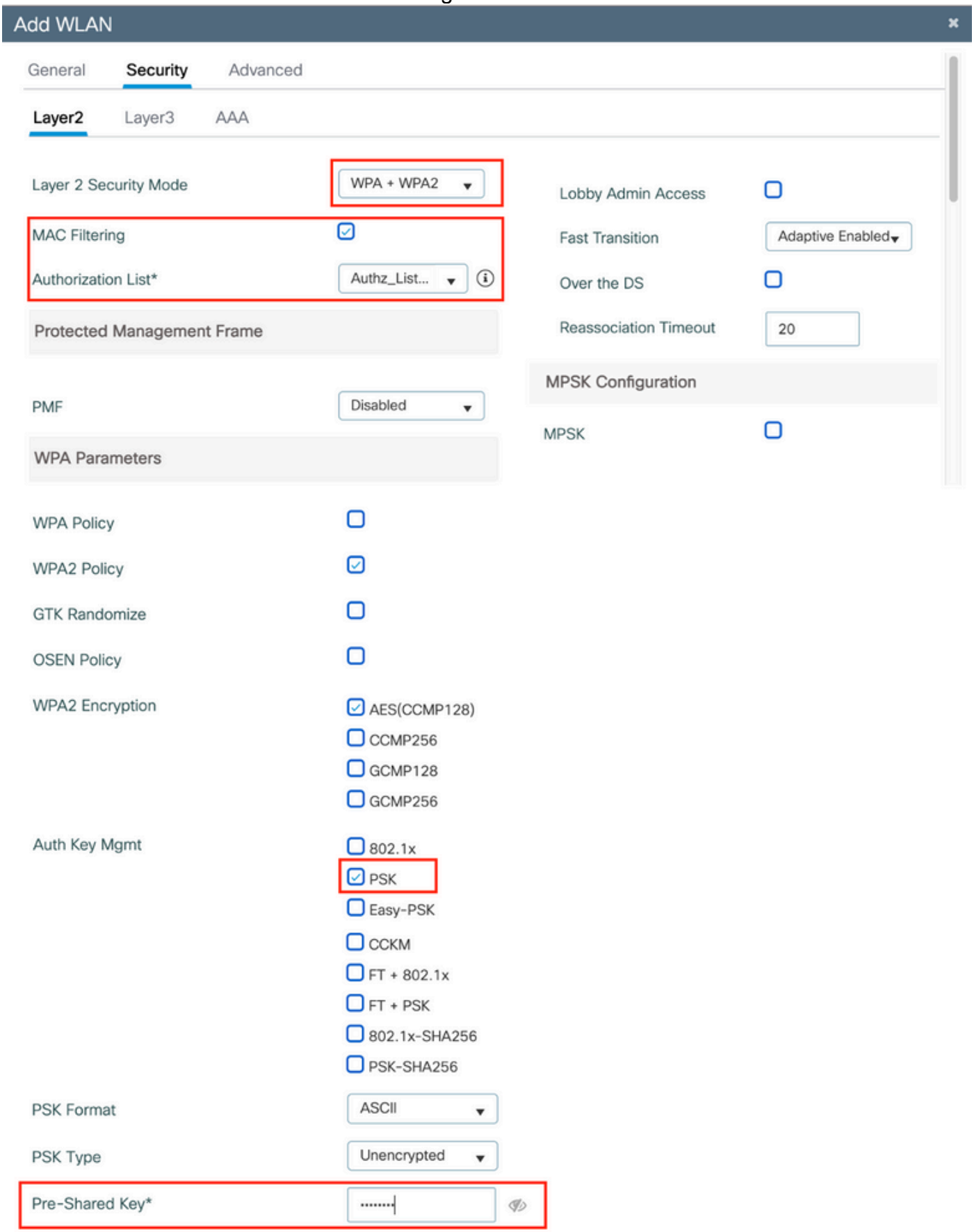
```
radius server
```

Erstellen Sie unter **Configuration > Tags & Profiles > WLANs** ein neues WLAN. Unter Layer 2-Konfiguration:

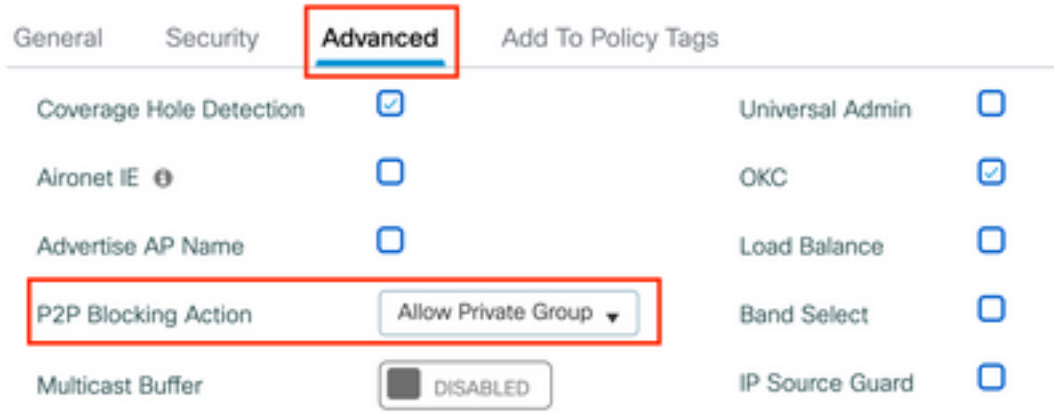
- Aktivieren Sie die MAC-Filterung, und legen Sie die Autorisierungsliste auf die zuvor erstellte

fest.

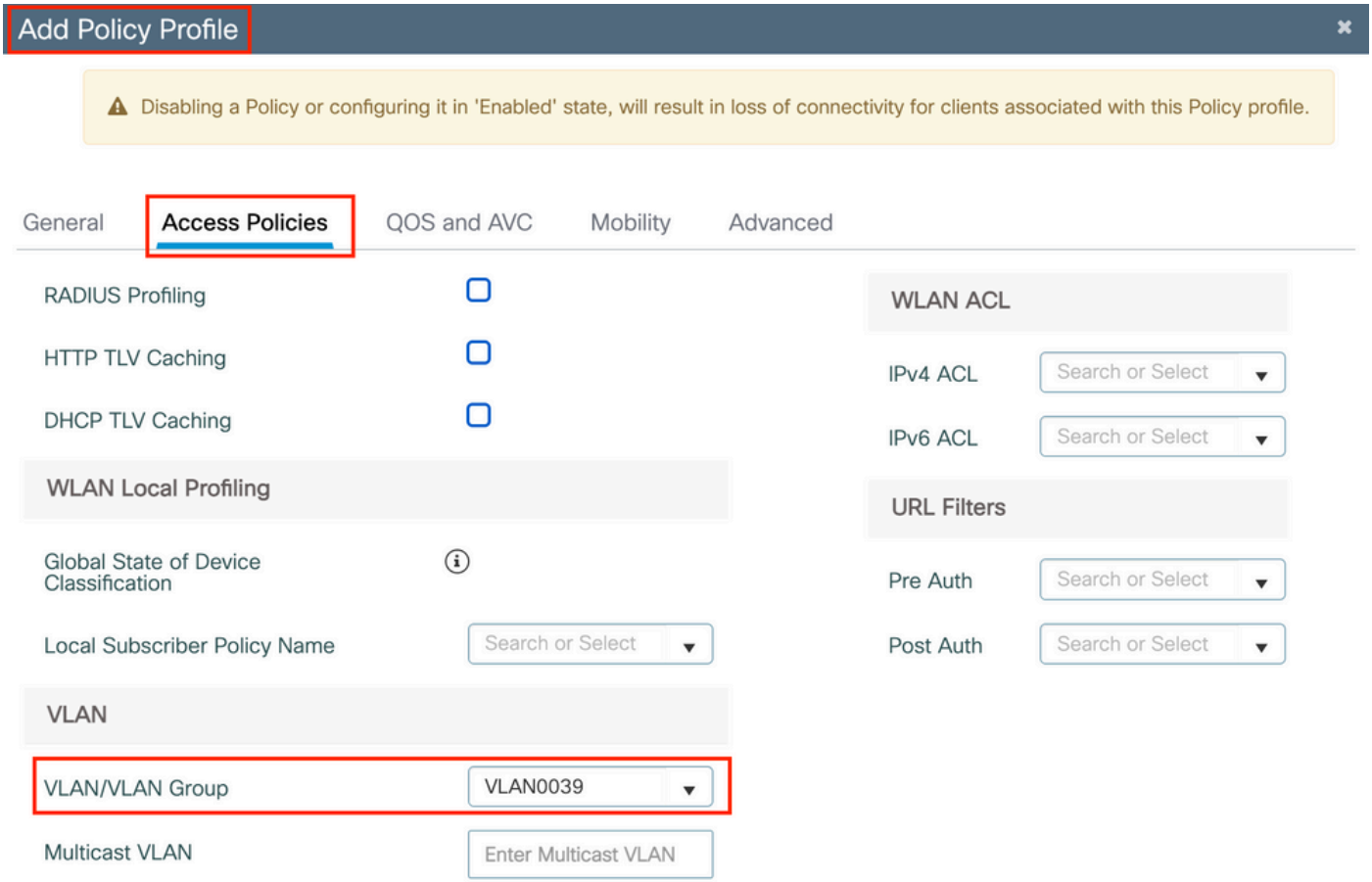
- Aktivieren Sie unter **Auth Key Mgmt** (**Auth-Schlüsselverwaltung**) **PSK.**
- Das Feld für den vorinstallierten Schlüssel kann mit einem beliebigen Wert gefüllt werden. Dies geschieht nur, um die Anforderungen des Web-Interface-Designs zu erfüllen. Kein Benutzer kann sich mit diesem Schlüssel authentifizieren. In diesem Fall wurde der vorinstallierte Schlüssel auf "12345678" gesetzt.



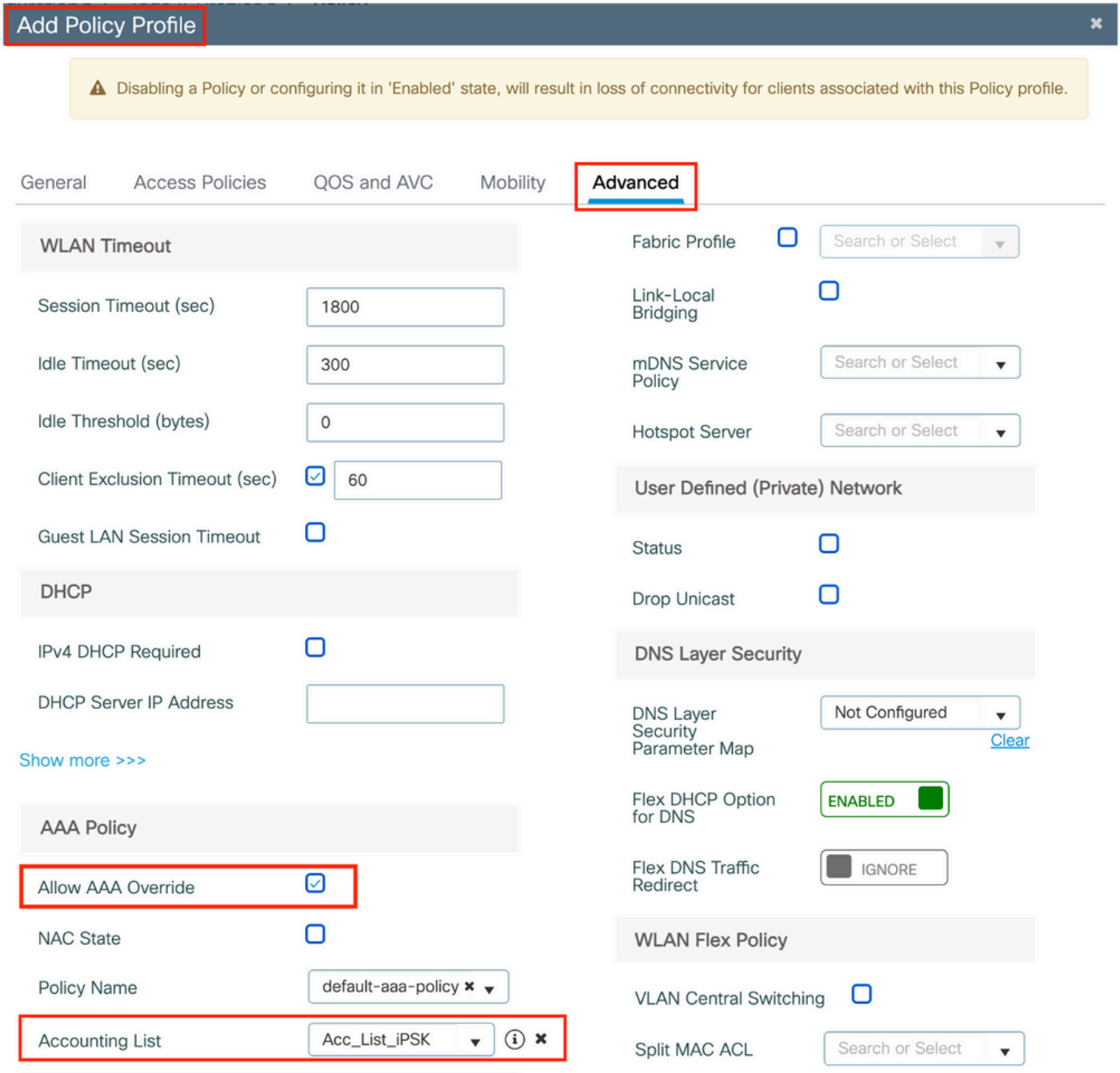
Die Benutzersegregation kann auf der Registerkarte **Erweitert** erreicht werden. Wenn Sie diese Einstellung auf Allow Private Group (Private Gruppe zulassen) festlegen, können Benutzer, die den gleichen PSK verwenden, miteinander kommunizieren, während Benutzer, die einen anderen PSK verwenden, blockiert werden:



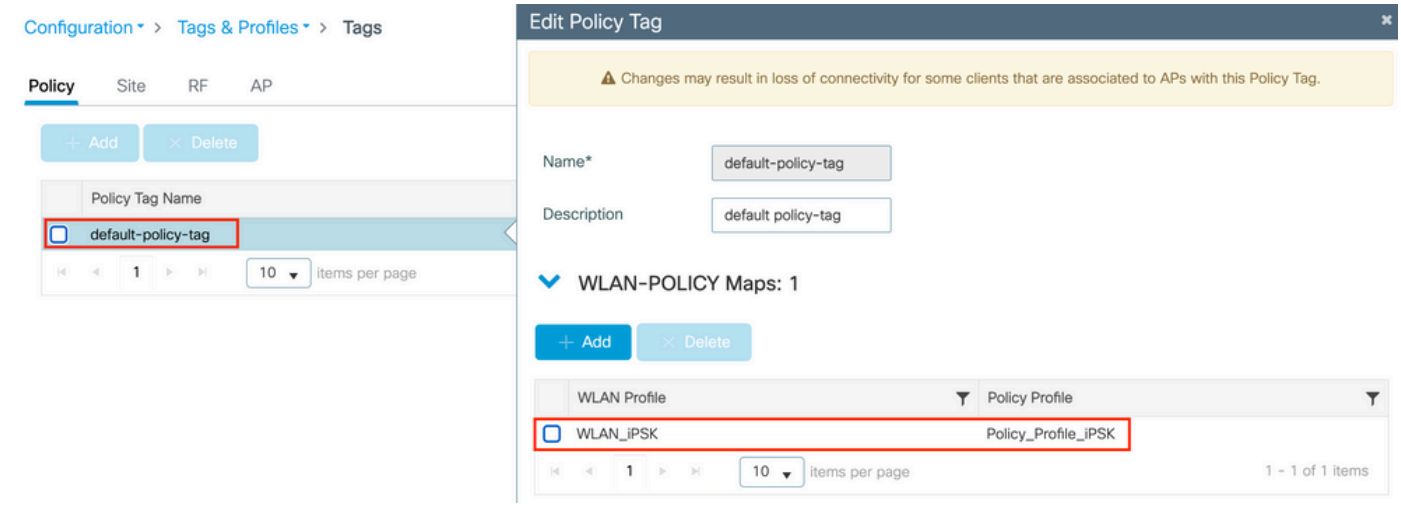
Erstellen Sie unter **Configuration > Tags & Profiles > Policy** (**Konfiguration > Tags & Profile >** Richtlinie) ein neues Richtlinienprofil. Legen Sie auf der Registerkarte **Access Policies (Zugriffsrichtlinien**) die VLAN- oder VLAN-Gruppe fest, die von diesem WLAN verwendet wird:



Aktivieren Sie auf der Registerkarte **Erweitert** die Option AAA-Überschreiben, und fügen Sie die Abrechnungsliste hinzu, falls zuvor erstellt:



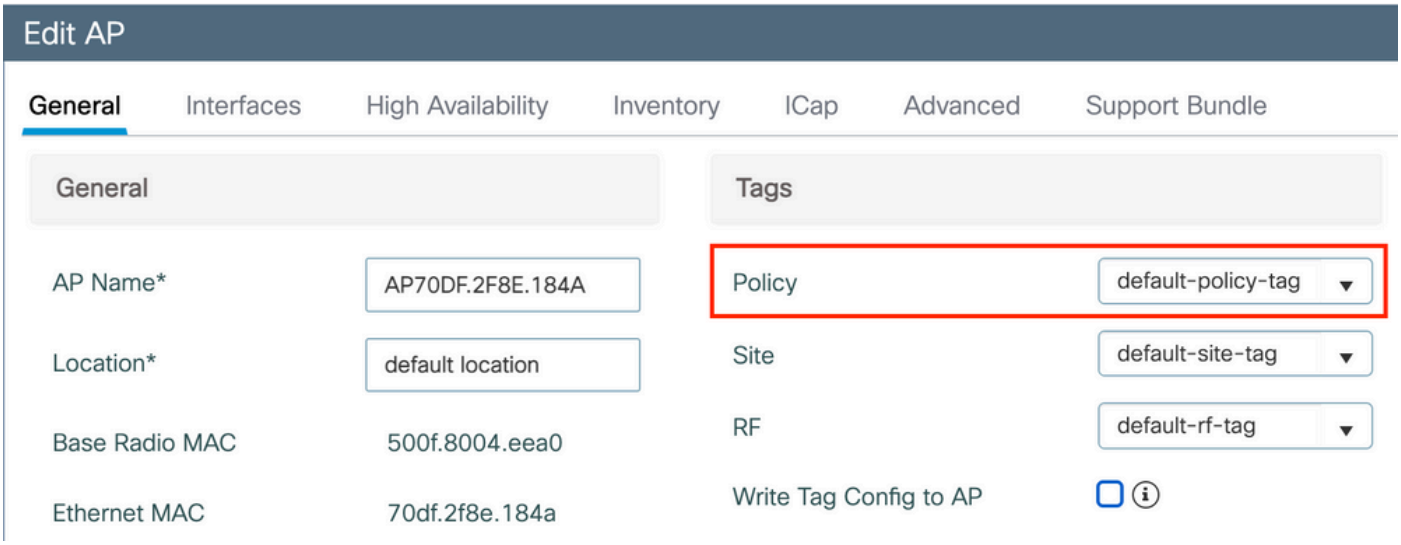
Vergewissern Sie sich unter **Configuration > Tags & Profiles > Tags > Policy**, dass das WLAN dem von Ihnen erstellten Richtlinienprofil zugeordnet ist:



Dies kann auch über die Befehlszeile mit folgenden Befehlen durchgeführt werden:

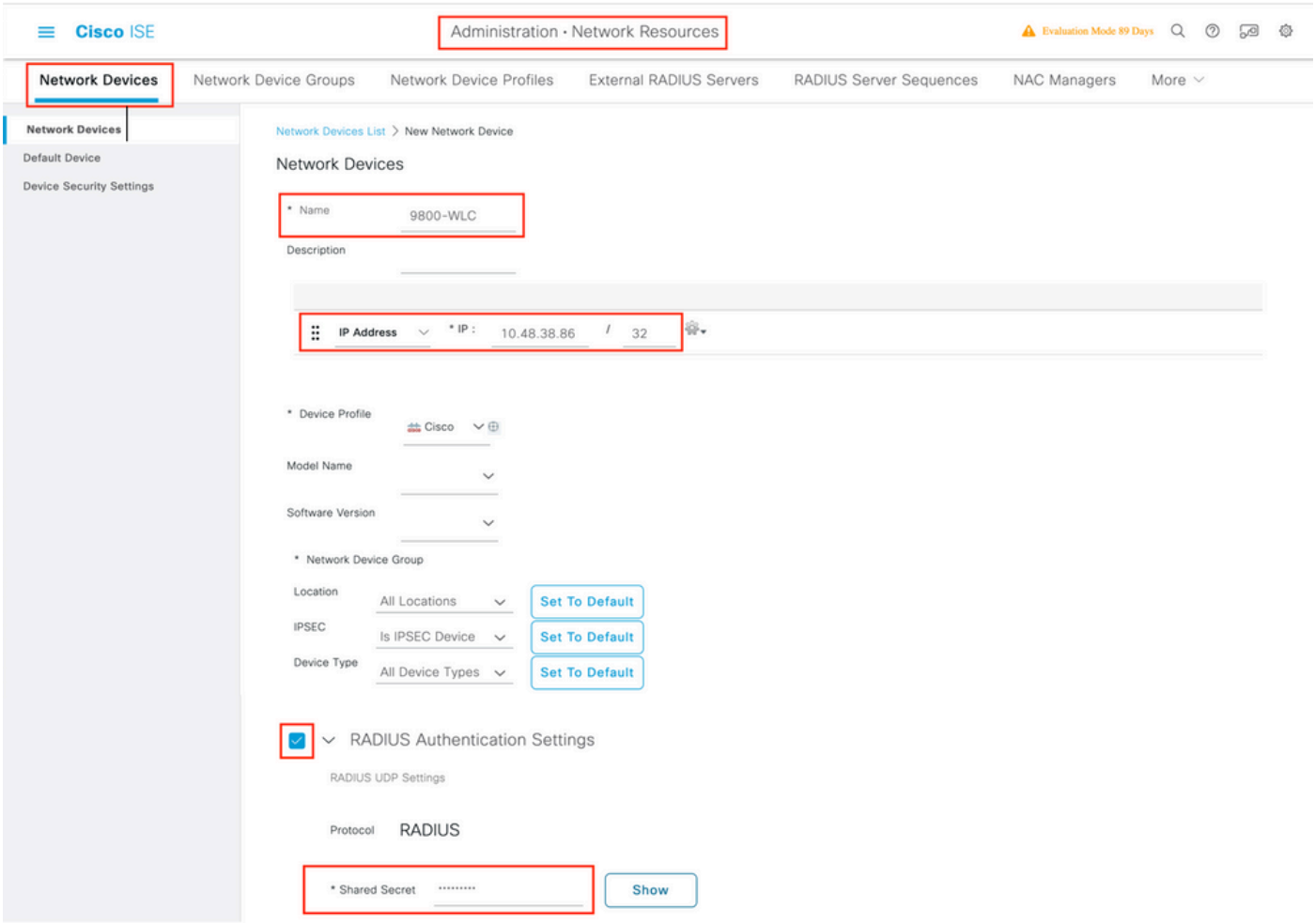
```
wlan
```

Vergewissern Sie sich unter **Konfiguration > Wireless > Access Points**, dass dieser Tag auf die Access Points angewendet wurde, auf die das WLAN übertragen werden muss:

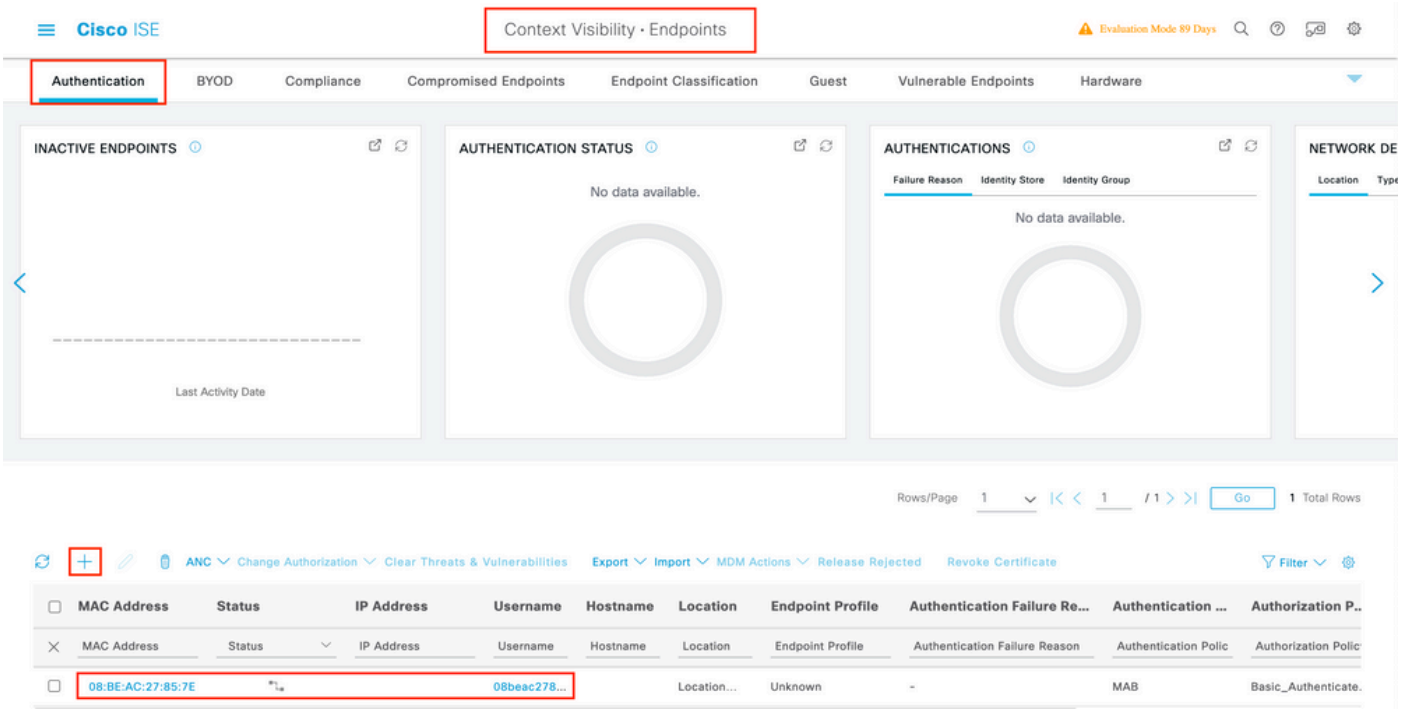


ISE-Konfiguration

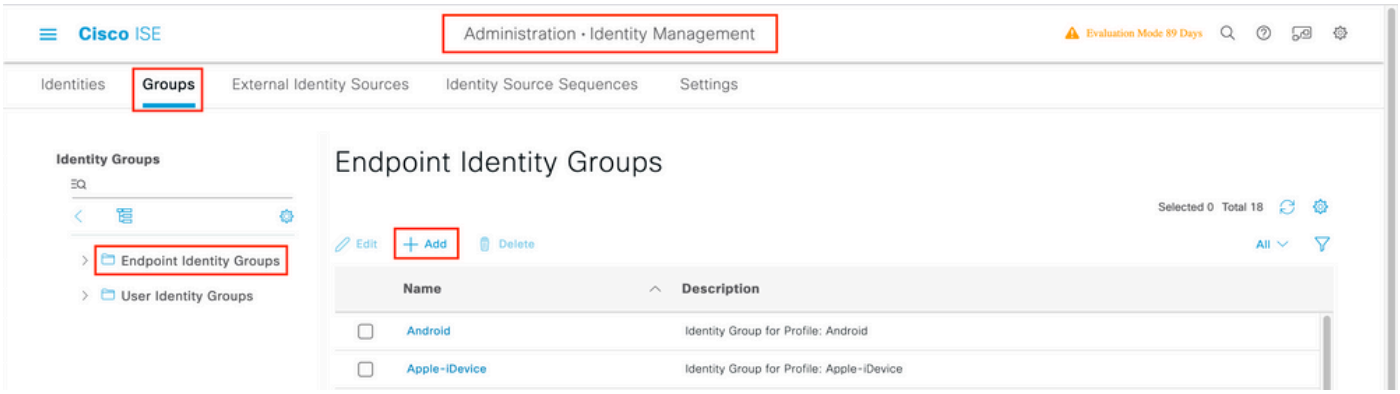
In diesem Konfigurationsleitfaden wird ein Szenario beschrieben, in dem der PSK des Geräts anhand der Client-MAC-Adresse bestimmt wird. Unter **Administration > Netzwerkressourcen > Netzwerkgeräte** fügen Sie ein neues Gerät hinzu, geben die IP-Adresse an, aktivieren die RADIUS-Authentifizierungseinstellungen und geben einen gemeinsamen RADIUS-Schlüssel an:

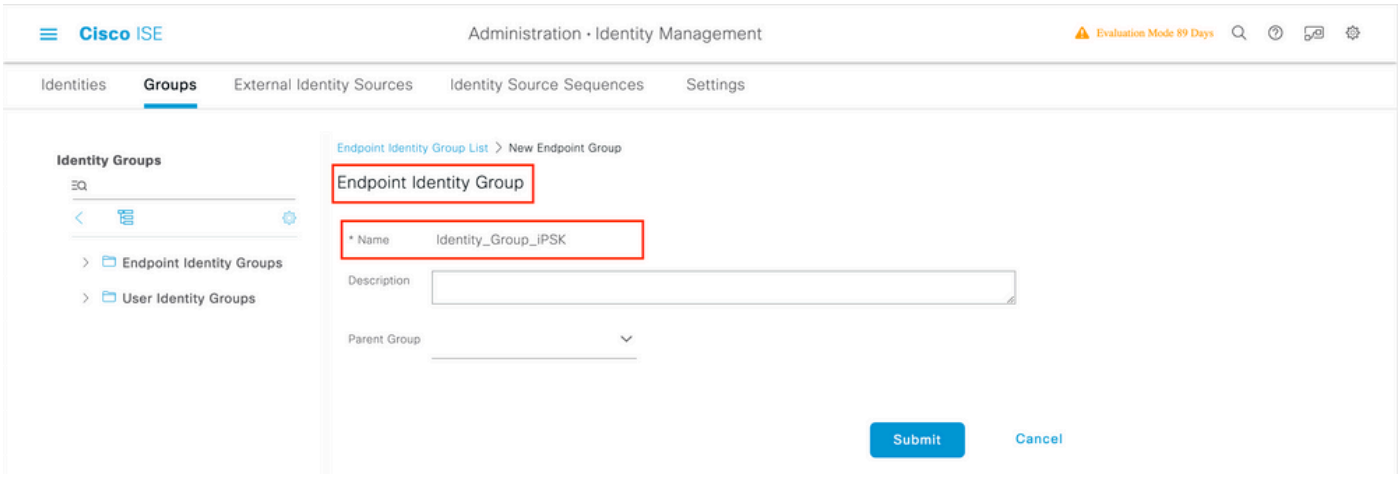


Fügen Sie unter **Context Visibility > Endpoints > Authentication** (**Kontextsichtbarkeit >** Endpunkte **>** Authentifizierung) die MAC-Adressen aller Geräte (Clients) hinzu, die eine Verbindung zum iPSK-Netzwerk herstellen:

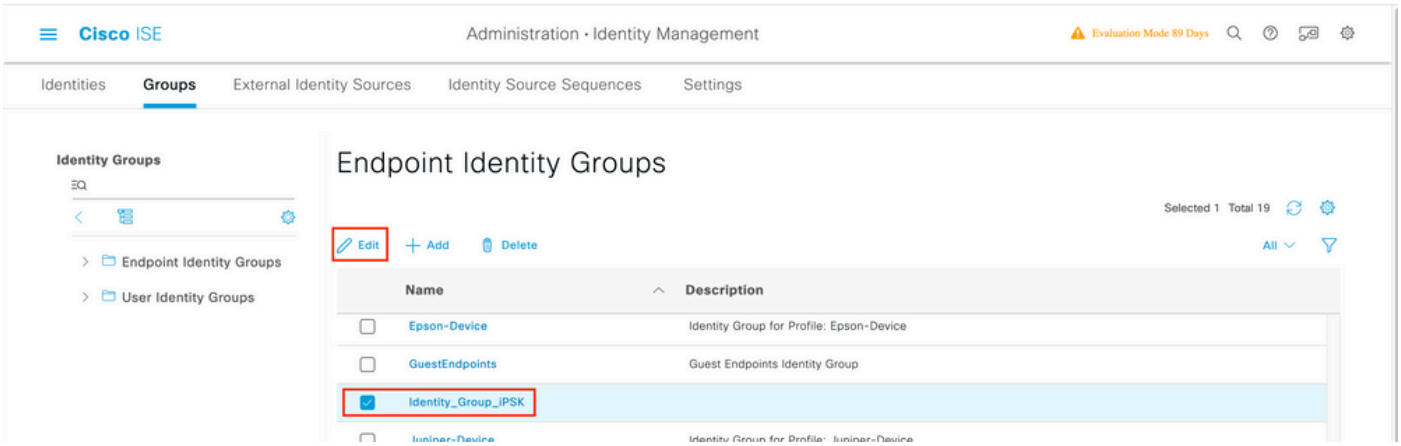


Erstellen Sie unter **Administration > Identity Management > Groups > Endpoint Identity Groups** eine oder mehrere Gruppen, und weisen Sie ihnen Benutzer zu. Jede Gruppe kann später für die Verwendung eines anderen PSK für die Verbindung mit dem Netzwerk konfiguriert werden.

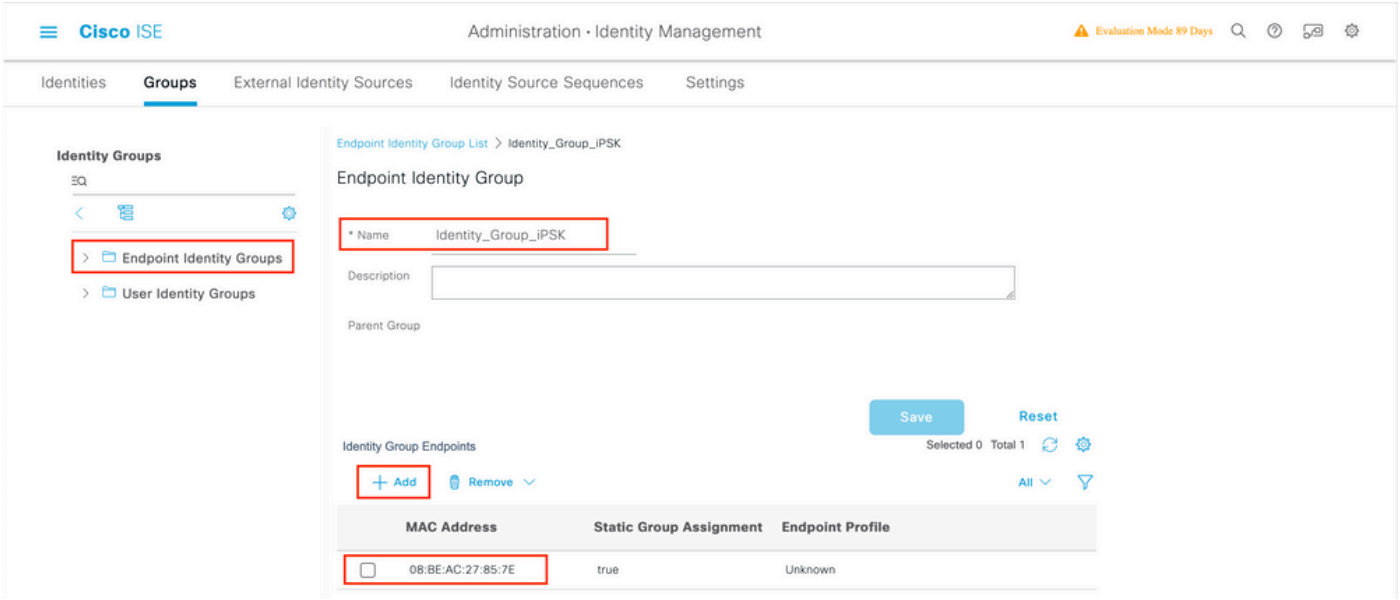




Nachdem die Gruppe erstellt wurde, können Sie ihnen Benutzer zuweisen. Wählen Sie die Gruppe, die Sie erstellt haben, und klicken Sie auf "Bearbeiten":



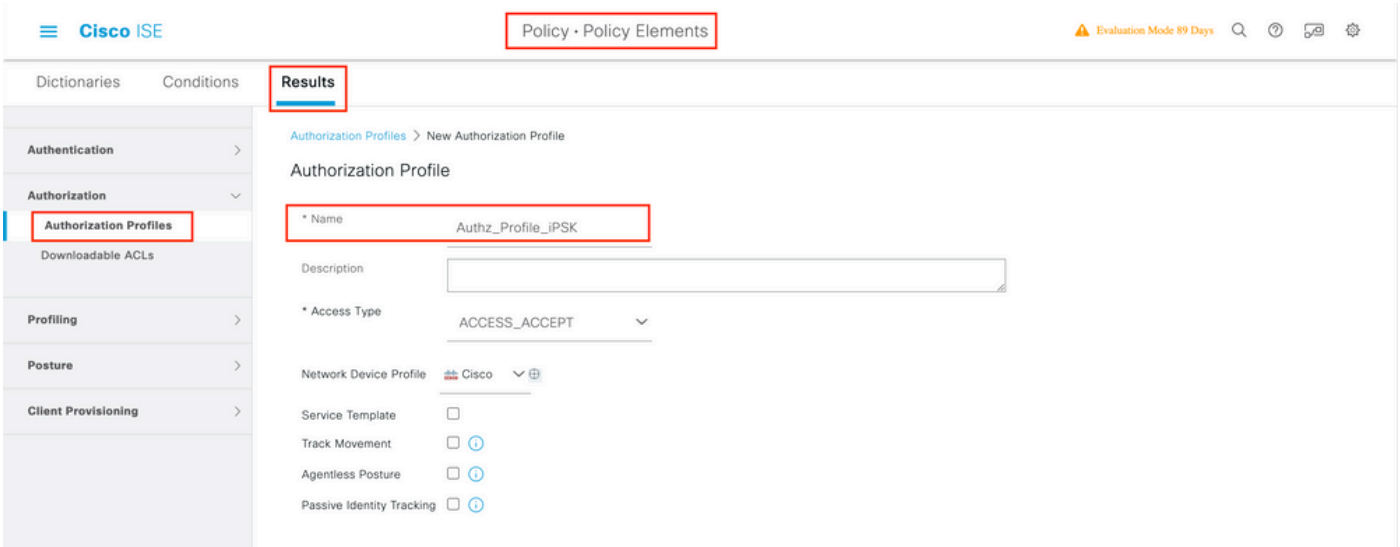
Fügen Sie in der Gruppenkonfiguration die MAC-Adresse der Clients hinzu, die Sie dieser Gruppe zuweisen möchten. Klicken Sie dazu auf die Schaltfläche "Hinzufügen":

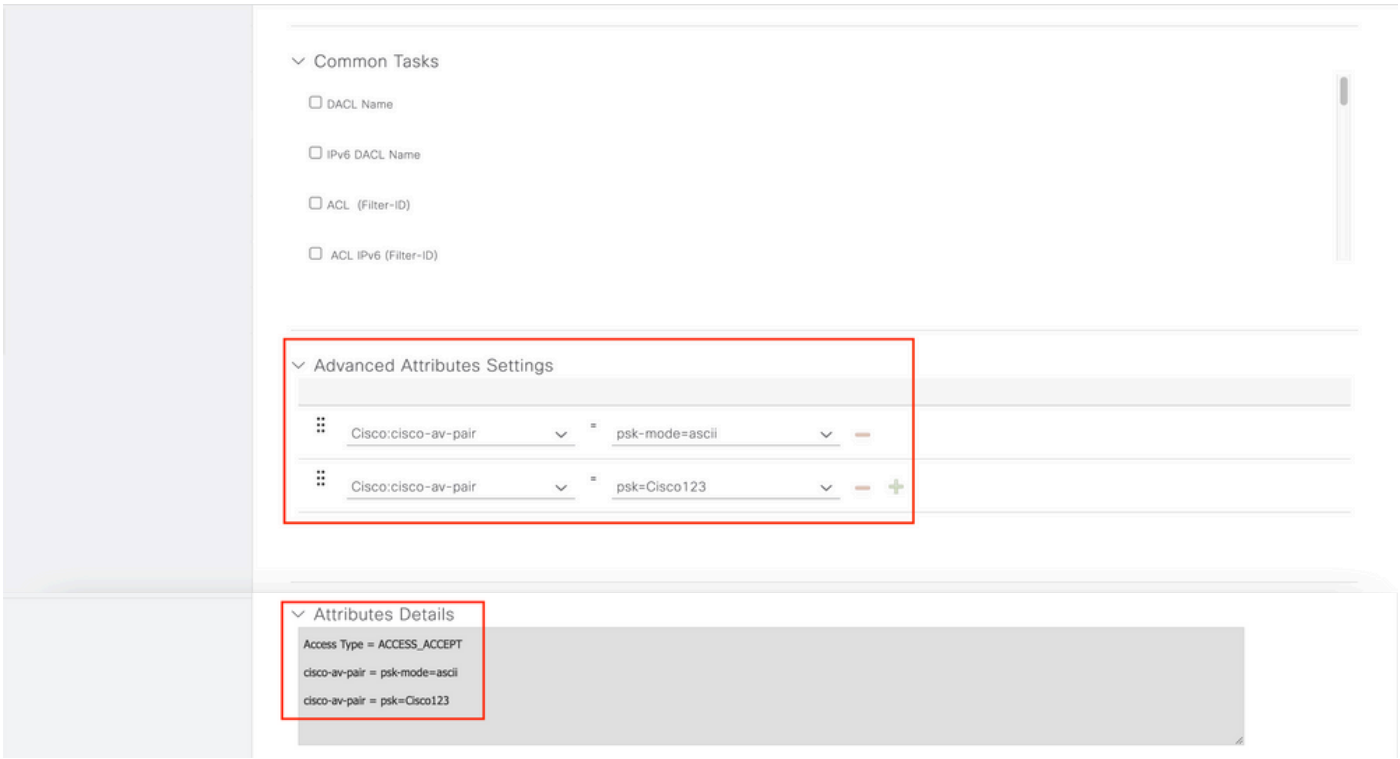


Erstellen Sie unter Policy > **Policy Elements > Results > Authorization > Authorization Profiles (Richtlinie** > Richtlinienelemente > **Ergebnisse > Autorisierung > Autorisierungsprofile**) ein neues Autorisierungsprofil. Attribute festlegen auf:

```
access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=
```

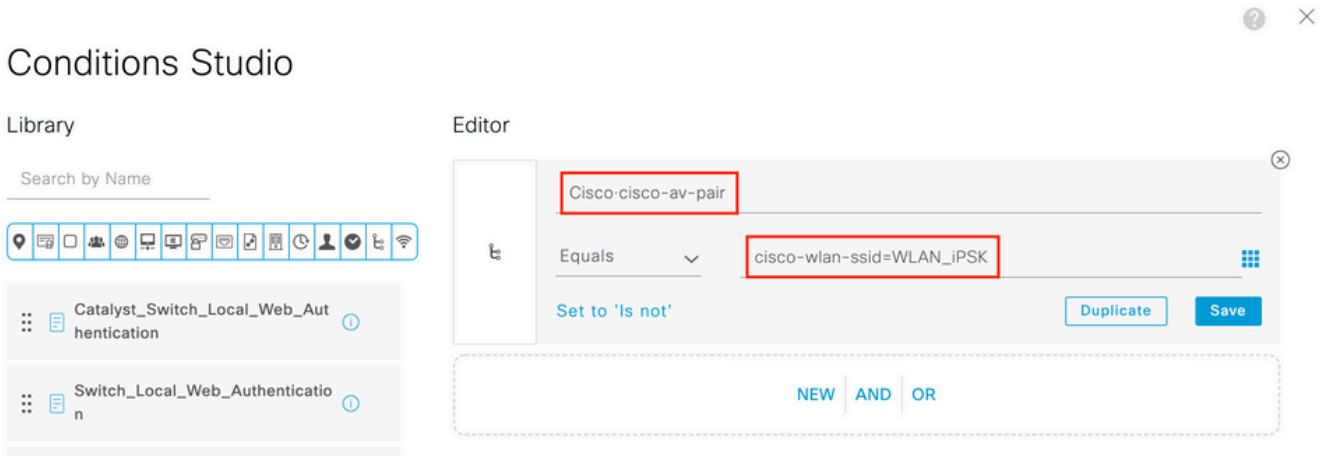
Erstellen Sie für jede Benutzergruppe, die einen anderen PSK verwenden muss, ein zusätzliches Ergebnis mit einem anderen PSK-AV-Paar. Hier können auch zusätzliche Parameter wie ACL und VLAN Override konfiguriert werden.



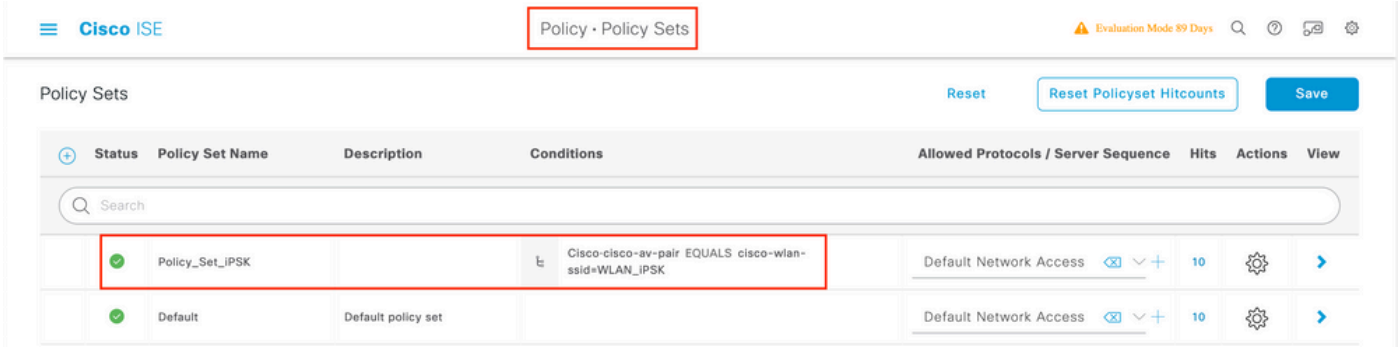


Erstellen Sie unter **Richtlinie > Richtliniensätze** eine neue Richtlinie. Um sicherzustellen, dass der Client mit dem Richtliniensatz übereinstimmt, wird diese Bedingung verwendet:

```
Cisco:cisco-av-pair EQUALS cisco-wlan-ssid=WLAN_iPSK    // "WLAN_iPSK" is WLAN name
```



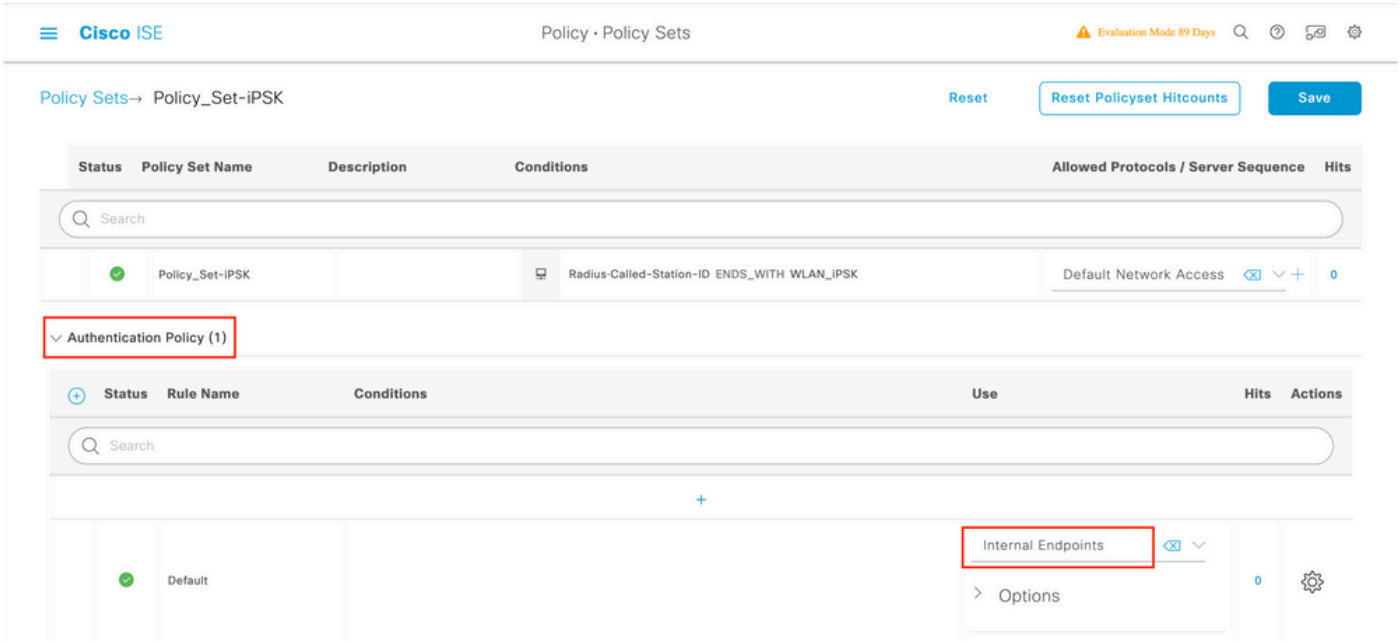
Es können weitere Bedingungen hinzugefügt werden, um die Richtlinienzuordnung sicherer zu machen.



Öffnen Sie die neu erstellte iPSK-Konfiguration für den Richtliniensatz, indem Sie auf den blauen

Pfeil rechts neben der Zeile Richtliniensatz klicken:

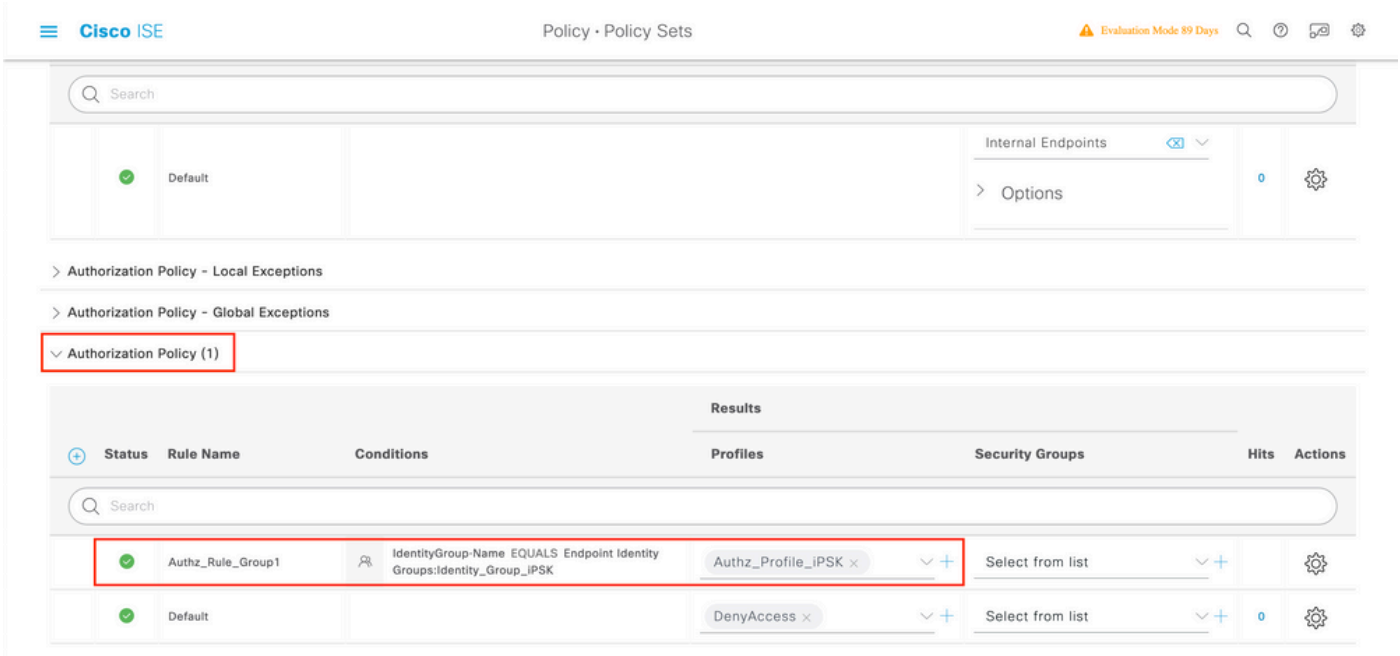
Stellen Sie sicher, dass die **Authentifizierungsrichtlinie** auf "Interne Endpunkte" festgelegt ist:



Erstellen Sie unter **Autorisierungsrichtlinie** eine neue Regel für jede Benutzergruppe. Als Bedingung:

```
IdentityGroup-Name EQUALS Endpoint Identity Group:Identity_Group_iPSK      //
"Identity_Group_iPSK" is name of the created endpoint group
```

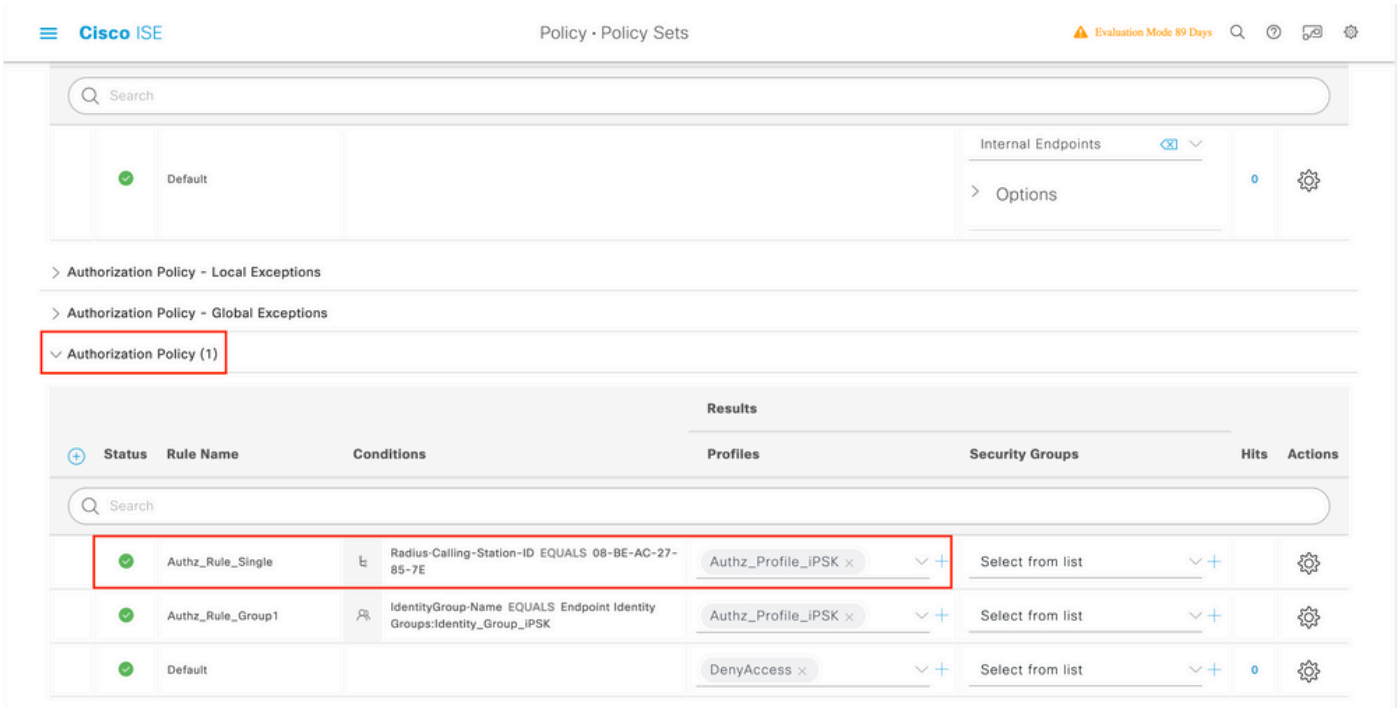
wobei das **Ergebnis** das **Autorisierungsprofil** ist, das zuvor erstellt wurde. Vergewissern Sie sich, dass die **Standardregel** unten beibehalten wird und auf **DenyAccess** zeigt.



Wenn jeder Benutzer über ein anderes Kennwort verfügt, kann statt Endpunktgruppen und Regeln zu erstellen, die mit dieser Endpunktgruppe übereinstimmen, eine Regel mit dieser Bedingung erstellt werden:

```
Radius-Calling-Station-ID EQUALS <client_mac_addr>
```

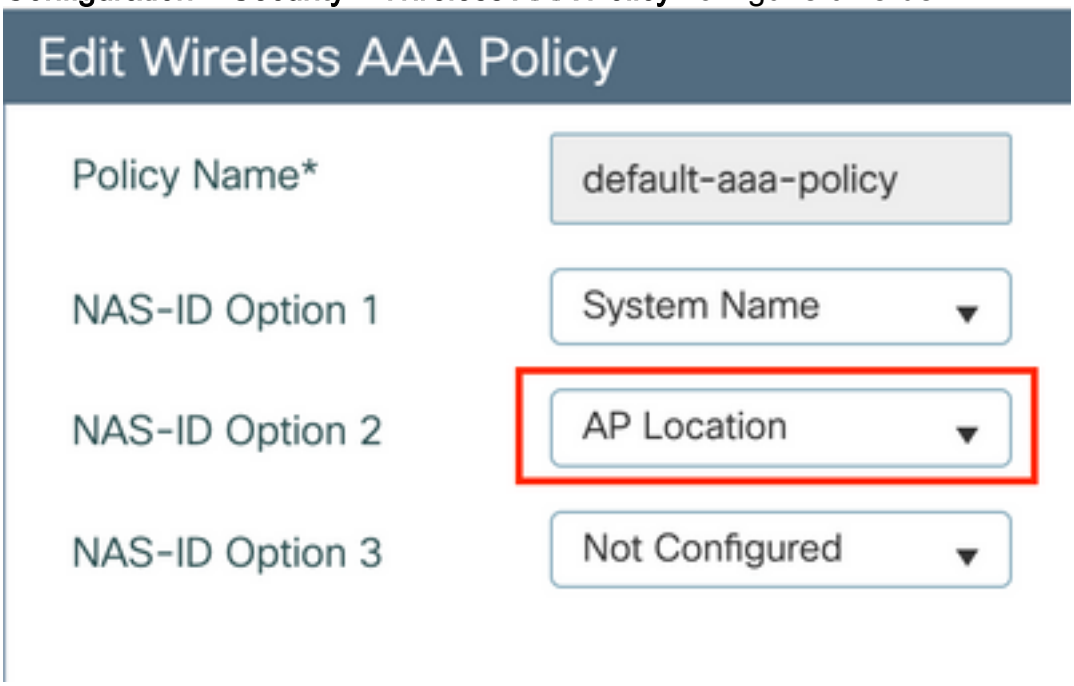
> **Anmerkung:** Das MAC-Adressen-Delimiter kann auf dem WLC unter **AAA > AAA Advanced > Global Config > Advanced Settings** konfiguriert werden. In diesem Beispiel wurde das Zeichen "-" verwendet.



Regeln für die Autorisierungsrichtlinie ermöglichen die Verwendung zahlreicher anderer Parameter, um das vom Benutzer verwendete Kennwort festzulegen. Zu den am häufigsten verwendeten Regeln gehören:

1. **Übereinstimmung basierend auf dem Benutzerstandort**

In diesem Szenario muss der WLC Informationen zum AP-Standort an die ISE senden. Dadurch können Benutzer an einem Standort ein Kennwort verwenden, während die Benutzer an einem anderen Standort ein anderes Kennwort verwenden. Dies kann unter **Configuration > Security > Wireless AAA Policy** konfiguriert werden:



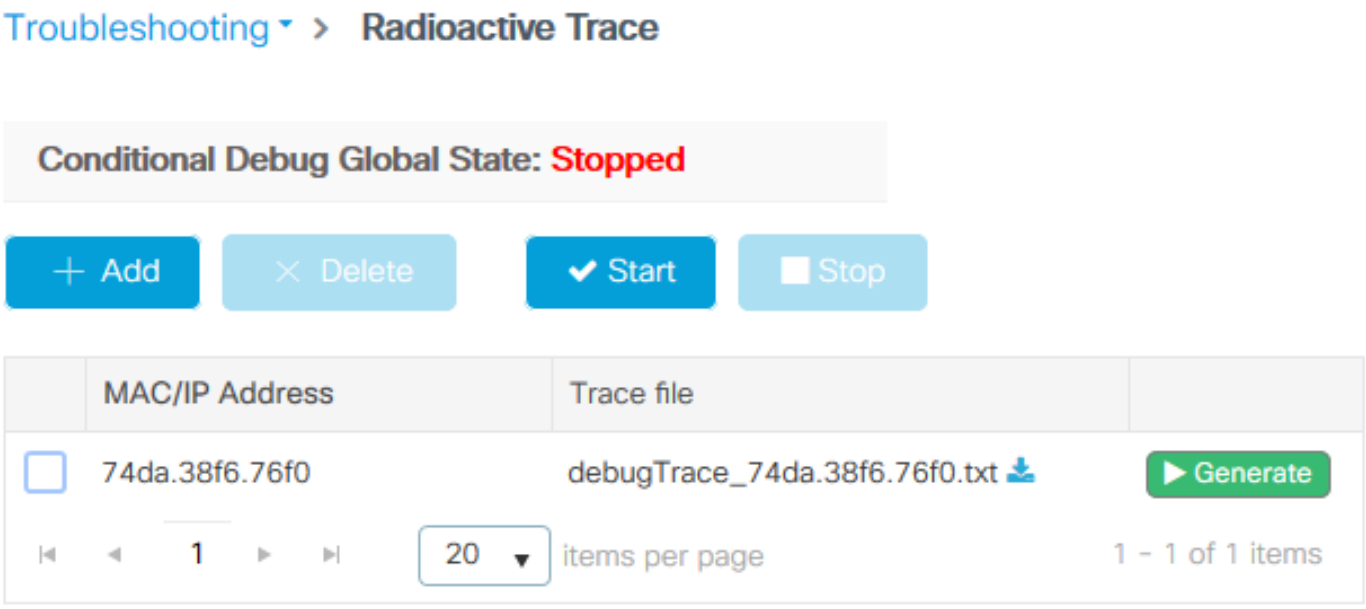
2. **Anpassung anhand der Erstellung von Geräteprofilen**
   In diesem Szenario muss der WLC so konfiguriert werden, dass ein globales Geräteprofil erstellt wird. Dadurch kann ein Administrator ein anderes Kennwort für Laptops und Telefone konfigurieren. Die globale Geräteklassifizierung kann aktiviert werden unter **Configuration > Wireless > Wireless Global**. Informationen zur Konfiguration der Erstellung von Geräteprofilen auf der ISE finden Sie im Designleitfaden zur ISE-Profilerstellung.

Da diese Autorisierung in der 802.11-Zuordnungsphase erfolgt, ist es nicht nur möglich, den Verschlüsselungsschlüssel zurückzugeben, sondern es können auch andere AAA-Attribute von der ISE wie ACL oder VLAN-ID zurückgegeben werden.

Fehlerbehebung

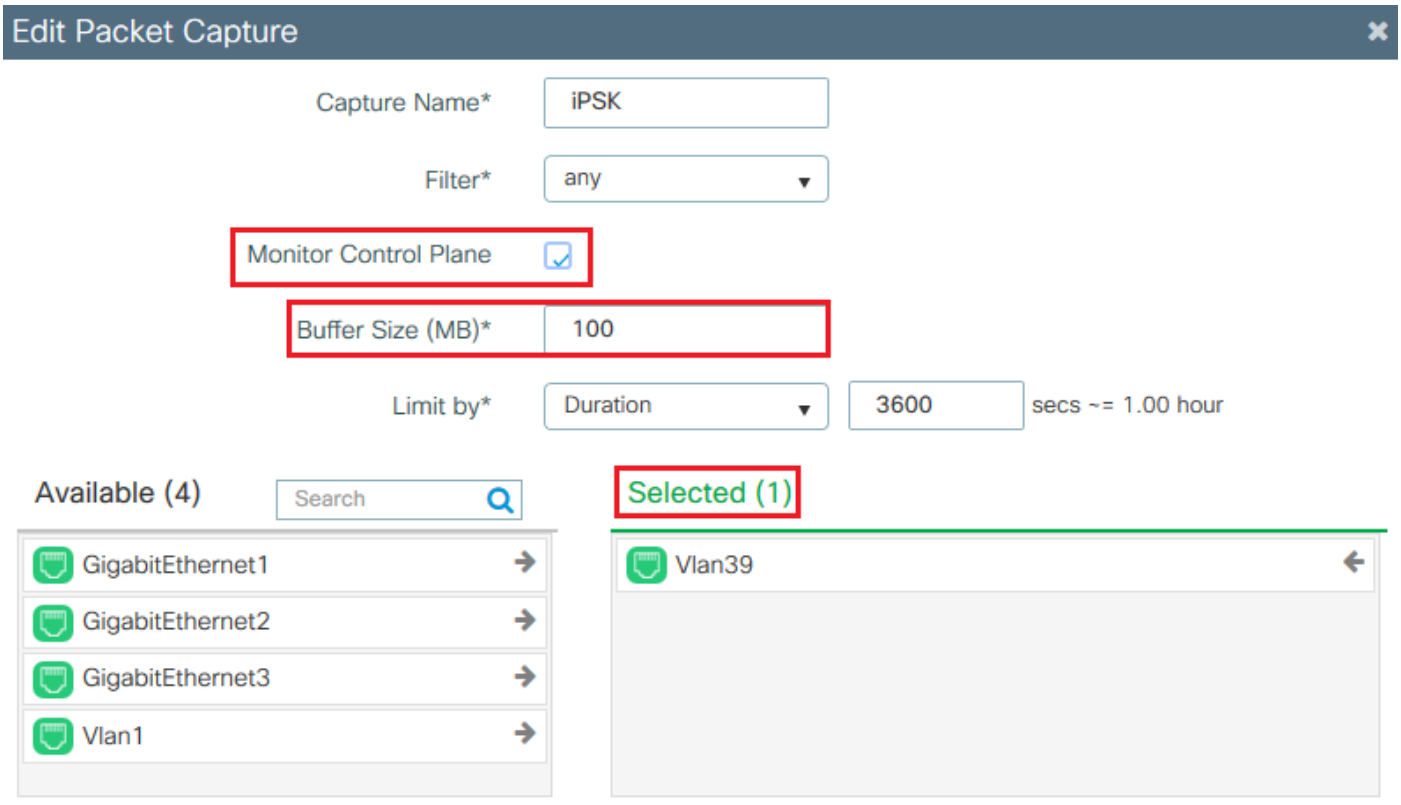
Fehlerbehebung am 9800 WLC

Auf dem WLC muss das Sammeln radioaktiver Spuren mehr als genug sein, um eine Mehrheit der Probleme zu identifizieren. Dies kann über die WLC-Webschnittstelle unter **Troubleshooting > Radioactive Trace** erfolgen. Fügen Sie die MAC-Adresse des Clients hinzu, drücken Sie **Start**, und versuchen Sie, das Problem zu reproduzieren. Klicken Sie auf **Generate (Generieren)**, um die Datei zu erstellen und herunterzuladen:



Wichtig: iPhones auf IOS 14- und Android 10-Smartphones verwenden bei der Verbindung mit dem Netzwerk eine randomisierte MAC-Adresse. Diese Funktion kann die iPSK-Konfiguration vollständig unterbrechen. Stellen Sie sicher, dass diese Funktion deaktiviert ist!

Reicht Radioactive Traces nicht aus, um das Problem zu identifizieren, können Paketerfassungen direkt auf dem WLC erfasst werden. Fügen Sie unter **Troubleshooting > Packet Capture** (Fehlerbehebung > Paketerfassung) einen Erfassungspunkt hinzu. Standardmäßig verwendet WLC eine Wireless-Management-Schnittstelle für die gesamte RADIUS-AAA-Kommunikation. Erhöhen Sie die Puffergröße auf 100 MB, wenn der WLC über eine hohe Anzahl an Clients verfügt:



Eine Paketerfassung eines erfolgreichen Authentifizierungs- und Abrechnungsversuchs ist in der

Abbildung unten dargestellt. Verwenden Sie diesen Wireshark-Filter, um alle relevanten Pakete für diesen Client herauszufiltern:

```
ip.addr==
```

wlc pcap.pcap

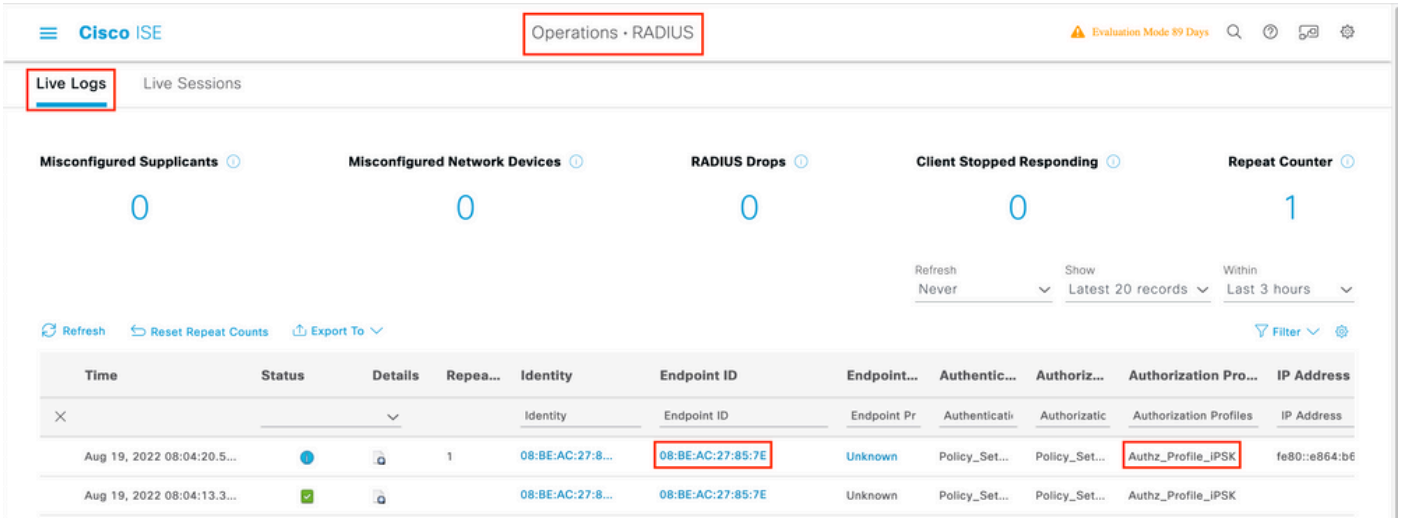
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.48.39.134 || eapol || bootp

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
1	0.000000	10.48.39.212	10.48.39.134	RADIUS	430	56240	1812	Access-Request id=123
2	0.014007	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123
3	0.000000	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123, Duplicate Response
4	5.944995	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	203	5247	5253	Key (Message 1 of 4)
5	0.005004	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	213	5253	5247	Key (Message 2 of 4)
6	0.001007	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	237	5247	5253	Key (Message 3 of 4)
7	0.004990	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	191	5253	5247	Key (Message 4 of 4)
8	4.318043	10.48.39.212	10.48.39.134	RADIUS	569	56240	1813	Accounting-Request id=124
9	0.013992	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124
10	0.000000	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124, Duplicate Response

Fehlerbehebung bei ISE

Das wichtigste Verfahren zur Fehlerbehebung bei der Cisco ISE ist die Seite **Live Logs** unter **Operations > RADIUS > Live Logs**. Sie können gefiltert werden, indem die MAC-Adresse des Clients in das Feld Endpunkt-ID eingegeben wird. Wenn Sie einen vollständigen ISE-Bericht öffnen, erhalten Sie weitere Details zum Fehlergrund. Stellen Sie sicher, dass der Client die richtige ISE-Richtlinie verwendet:



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.