Konfigurieren der Catalyst 9800 Wireless Controller AP-Autorisierungsliste

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der Authentifizierungsrichtlinie für den Catalyst 9800 Wireless LAN Controller Access Point (AP) beschrieben.

Hintergrundinformationen

Um einen Access Point (AP) zu autorisieren, muss die Ethernet-MAC-Adresse des AP für die lokale Datenbank mit dem Wireless LAN Controller 9800 oder für einen externen RADIUS-Server (Remote Authentication Dial-In User Service) autorisiert werden.

Diese Funktion stellt sicher, dass nur autorisierte Access Points (APs) einem Catalyst 9800 Wireless LAN-Controller beitreten können. In diesem Dokument wird nicht auf vernetzte (1500-Serie) APs eingegangen, die einen MAC-Filtereintrag benötigen, um mit dem Controller verbunden zu werden, jedoch nicht den typischen AP-Autorisierungsfluss verfolgen (siehe Referenzen).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- 9800 WLC
- Zugriff auf die Wireless Controller über eine Kommandozeile (CLI)

Verwendete Komponenten

9800 WLC v16.12

AP 1810 W

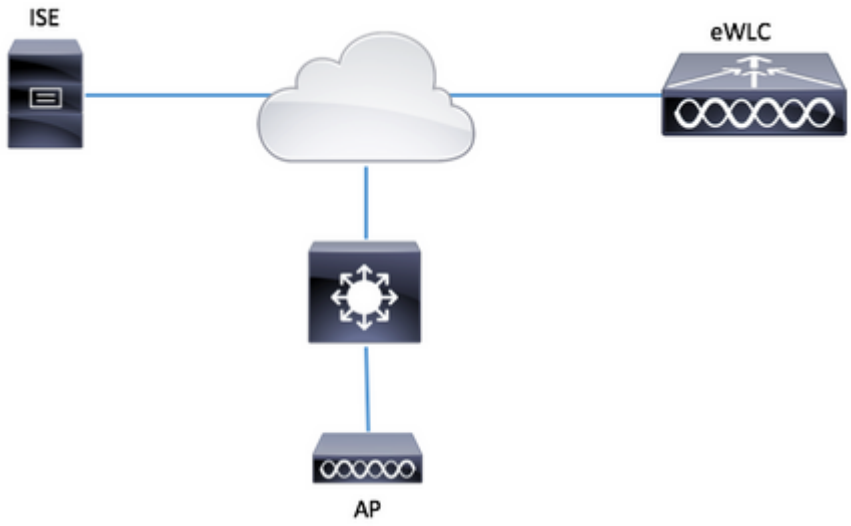
AP 1700

Identity Service Engine (ISE) Version 2.2

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 kennen.

Konfigurieren

Netzwerkdiagramm



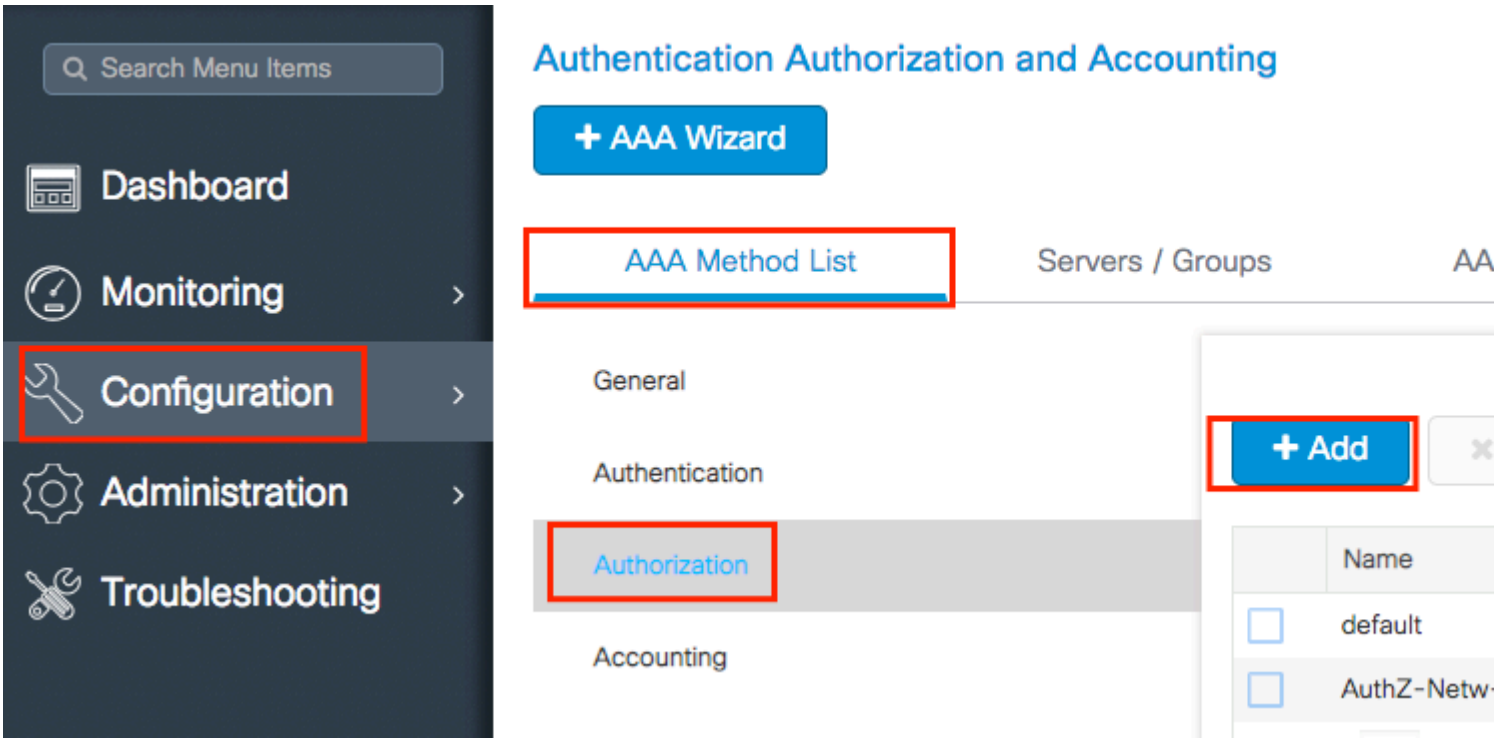
Konfigurationen

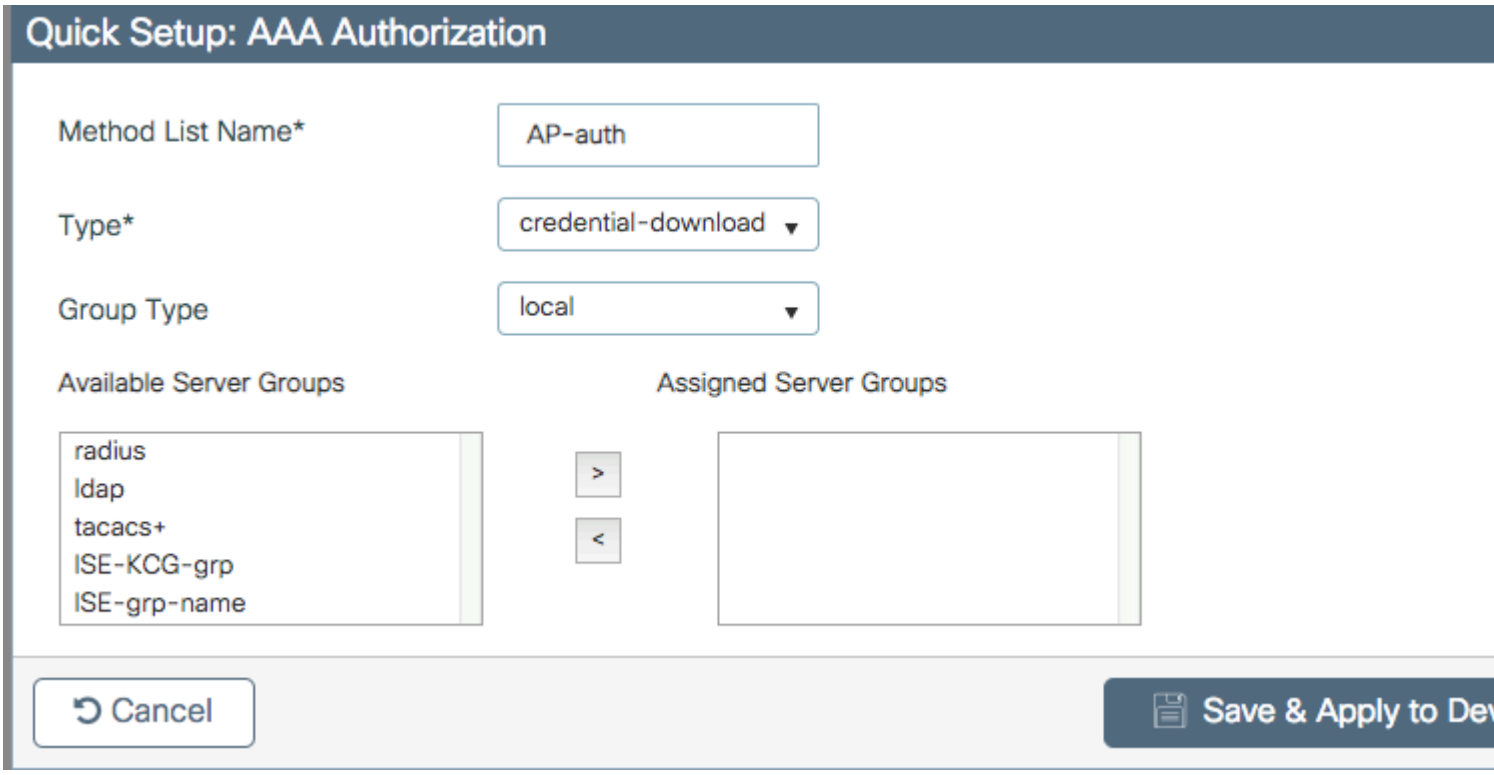
MAC AP-Autorisierungsliste - Lokal

Die MAC-Adresse der autorisierten Access Points wird lokal im 9800 WLC gespeichert.

Schritt 1: Erstellen Sie eine Liste mit lokalen Methoden zum Herunterladen von Autorisierungsanmeldeinformationen.

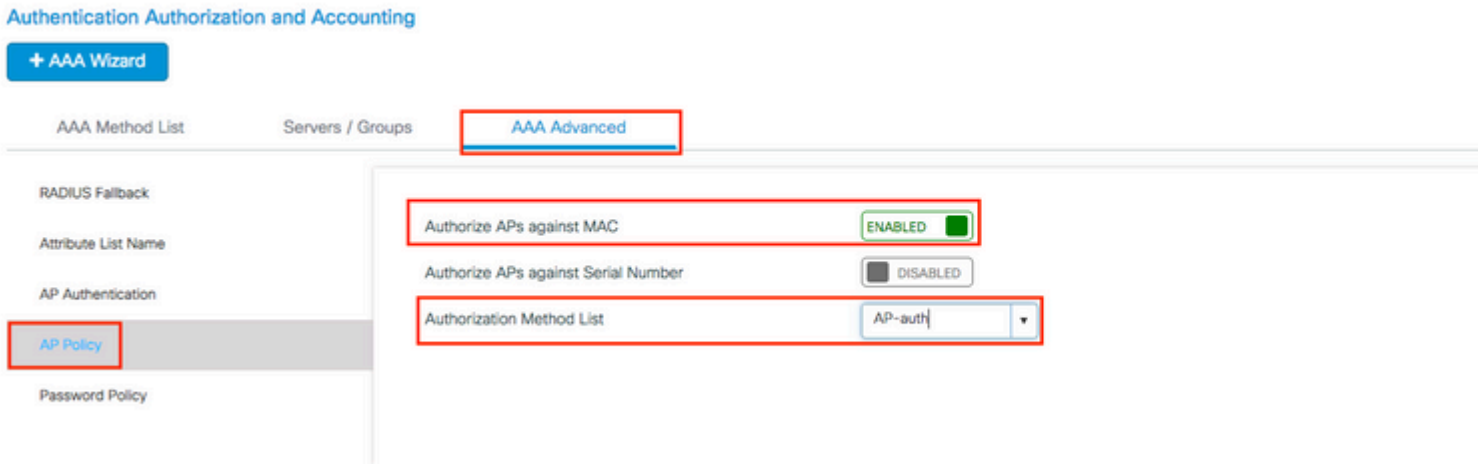
Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authorization > + Add.**





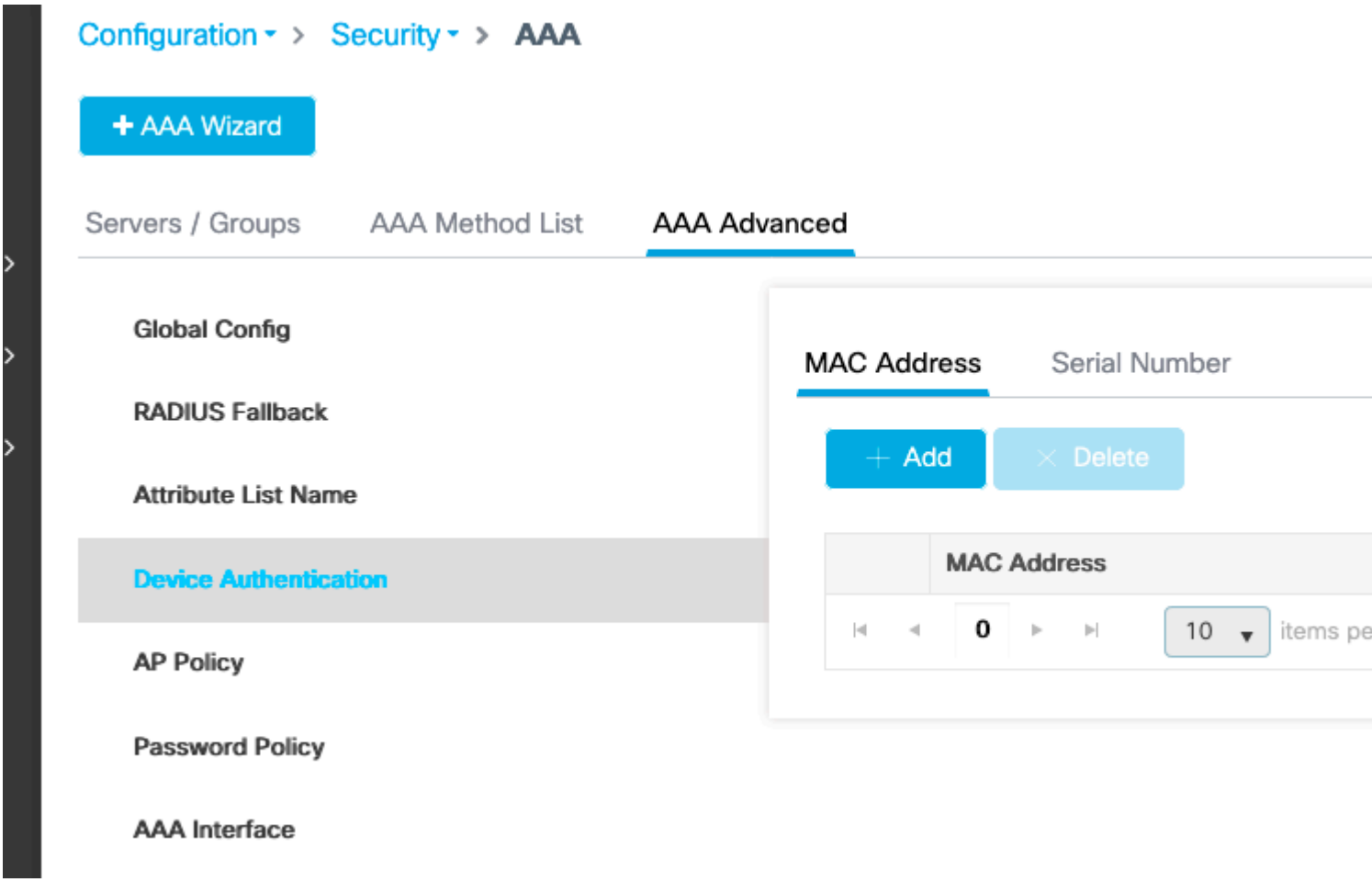
Schritt 2: Aktivieren Sie die AP-MAC-Autorisierung.

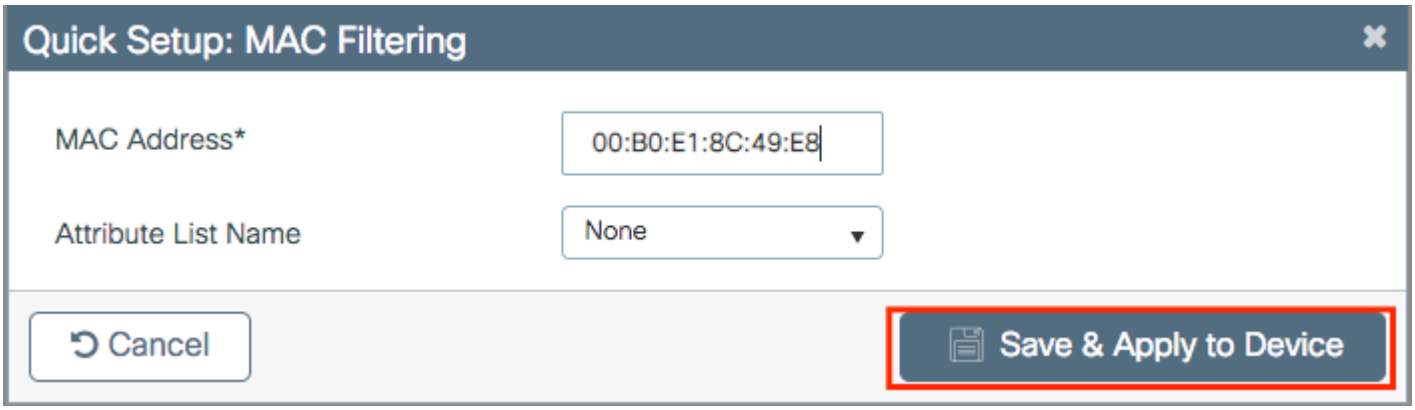
Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA Advanced > AP-Richtlinie.** Aktivieren Sie **die Autorisierung von APs für MAC**, und wählen Sie die in Schritt 1 erstellte **Liste** der **Autorisierungsmethoden aus**.



Schritt 3: Fügen Sie die MAC-Adresse des AP-Ethernets hinzu.

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA Advanced > Geräteauthentifizierung > MAC-Adresse > + Hinzufügen**





Hinweis: Die MAC-Adresse des AP-Ethernets muss in einem der folgenden Formate, wenn diese in Version 16.12 in die Webbenutzeroberfläche eingegeben wurden (xx:xx:xx:xx:xx:xx:xx (oder) xxxx.xxxx.xxxx (oder) xx-xx-xx-xx-xx). In Version 17.3 müssen sie das Format xxxxxxxxxxxx ohne Trennzeichen haben. Das CLI-Format ist immer xxxxxxxxxx in jeder beliebigen Version (in Version 16.12 werden die Trennzeichen in der Konfiguration von der Webbenutzeroberfläche entfernt). Die Cisco Bug-ID CSCvv43870 ermöglicht die Verwendung beliebiger Formate in der CLI oder der Webbenutzeroberfläche in späteren Versionen.

CLI:

```
# config t
# aaa new-model
# aaa authorization credential-download <AP-auth> local

# ap auth-list authorize-mac
# ap auth-list method-list <AP-auth>

# username <aaaabbbbcccc> mac
```

MAC AP-Autorisierungsliste - Externer RADIUS-Server

9800 WLC-Konfiguration

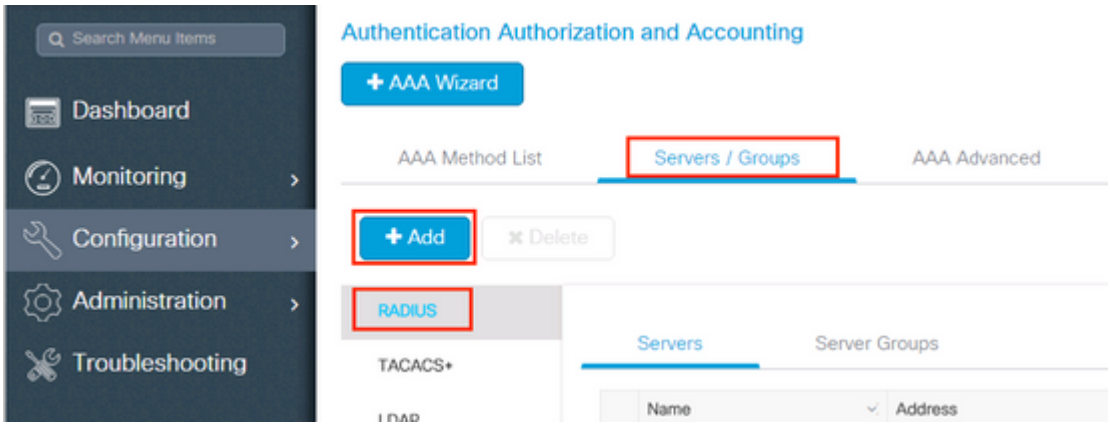
Die MAC-Adresse der autorisierten Access Points wird auf einem externen RADIUS-Server gespeichert, in diesem Beispiel ISE.

Auf der ISE können Sie die MAC-Adresse der Access Points entweder als Benutzername/Kennwort oder als Endpunkte registrieren. Entlang der Schritte werden Sie angewiesen, wie Sie die eine oder die andere Art zu verwenden.

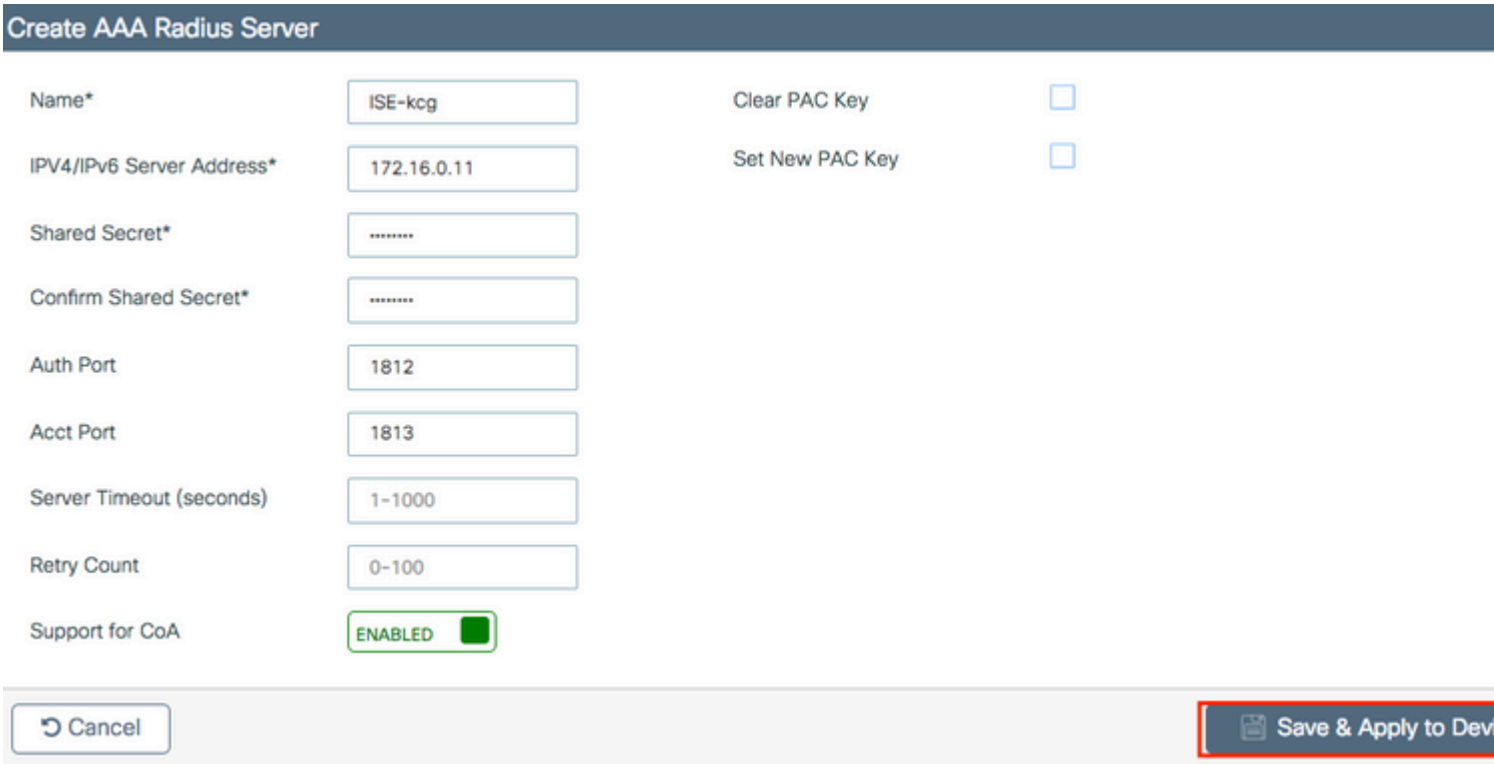
GUI:

Schritt 1: Deklarieren des RADIUS-Servers

Navigieren Sie zu **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add (Konfiguration > Sicherheit > AAA > Server/Gruppen > RADIUS > Server > + Hinzufügen),** und geben Sie die RADIUS-Serverinformationen ein.



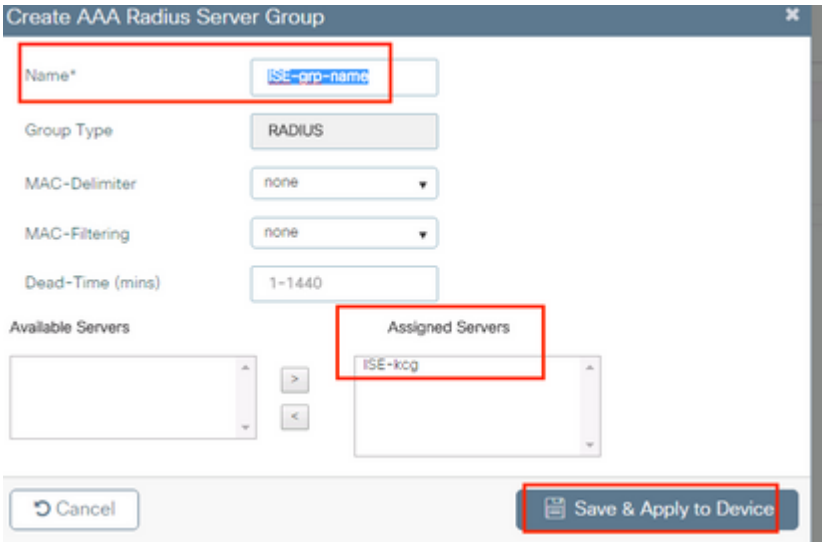
Stellen Sie sicher, dass die Unterstützung für CoA aktiviert ist, wenn Sie zukünftig Central Web Authentication (oder irgendeine Art der Sicherheit, die CoA erfordert) verwenden möchten.



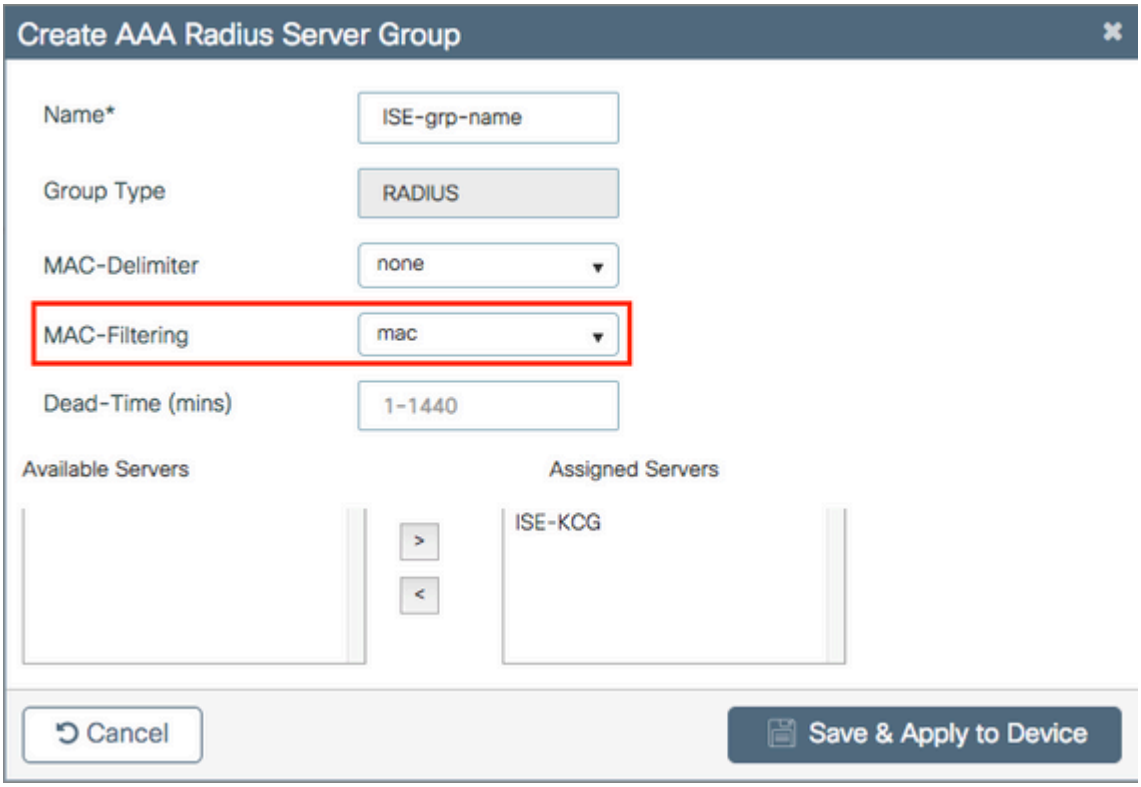
Schritt 2: Hinzufügen eines RADIUS-Servers zu einer RADIUS-Gruppe

Navigieren Sie zu **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.**

Damit die ISE die MAC-Adresse des Access Points authentifiziert, wenn Benutzernamen keine MAC-Filterung zulassen.

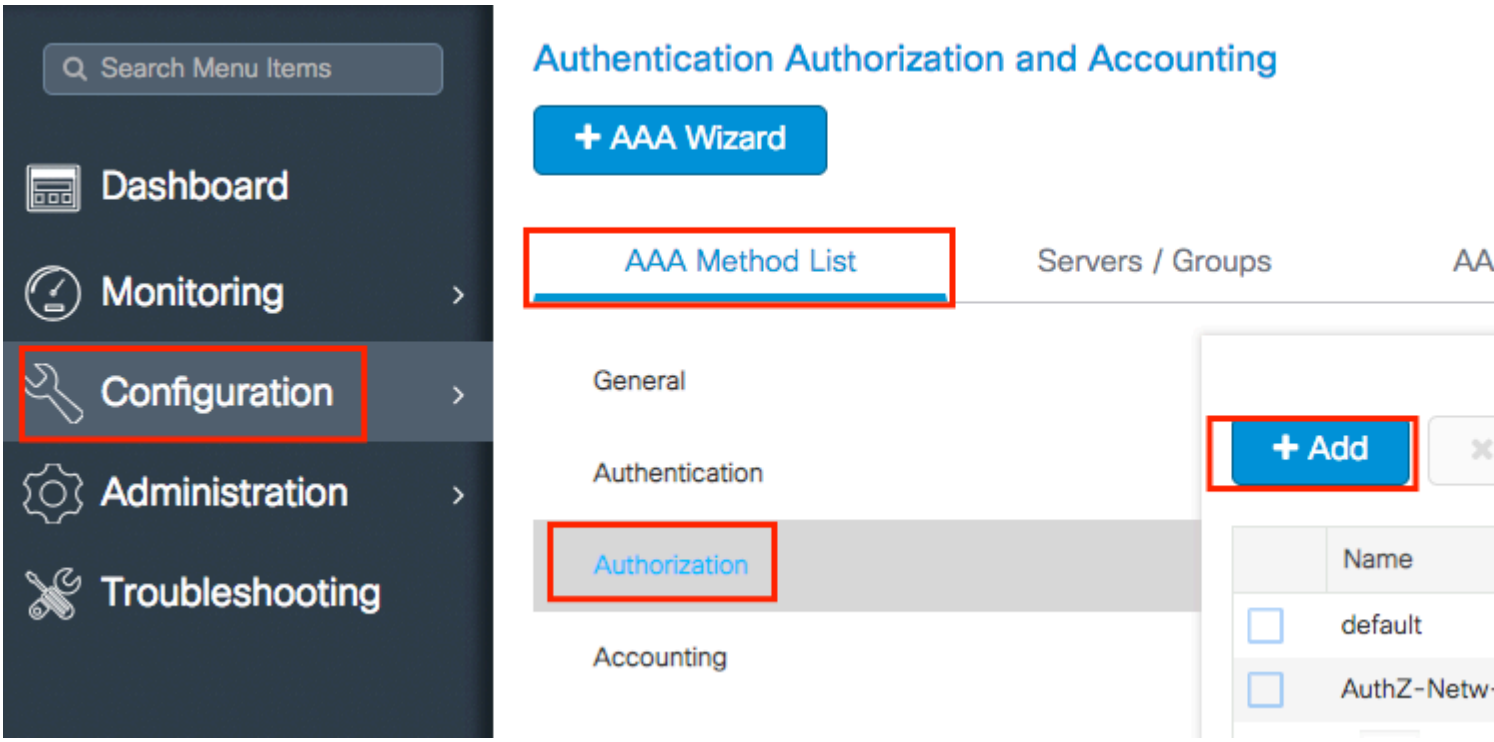


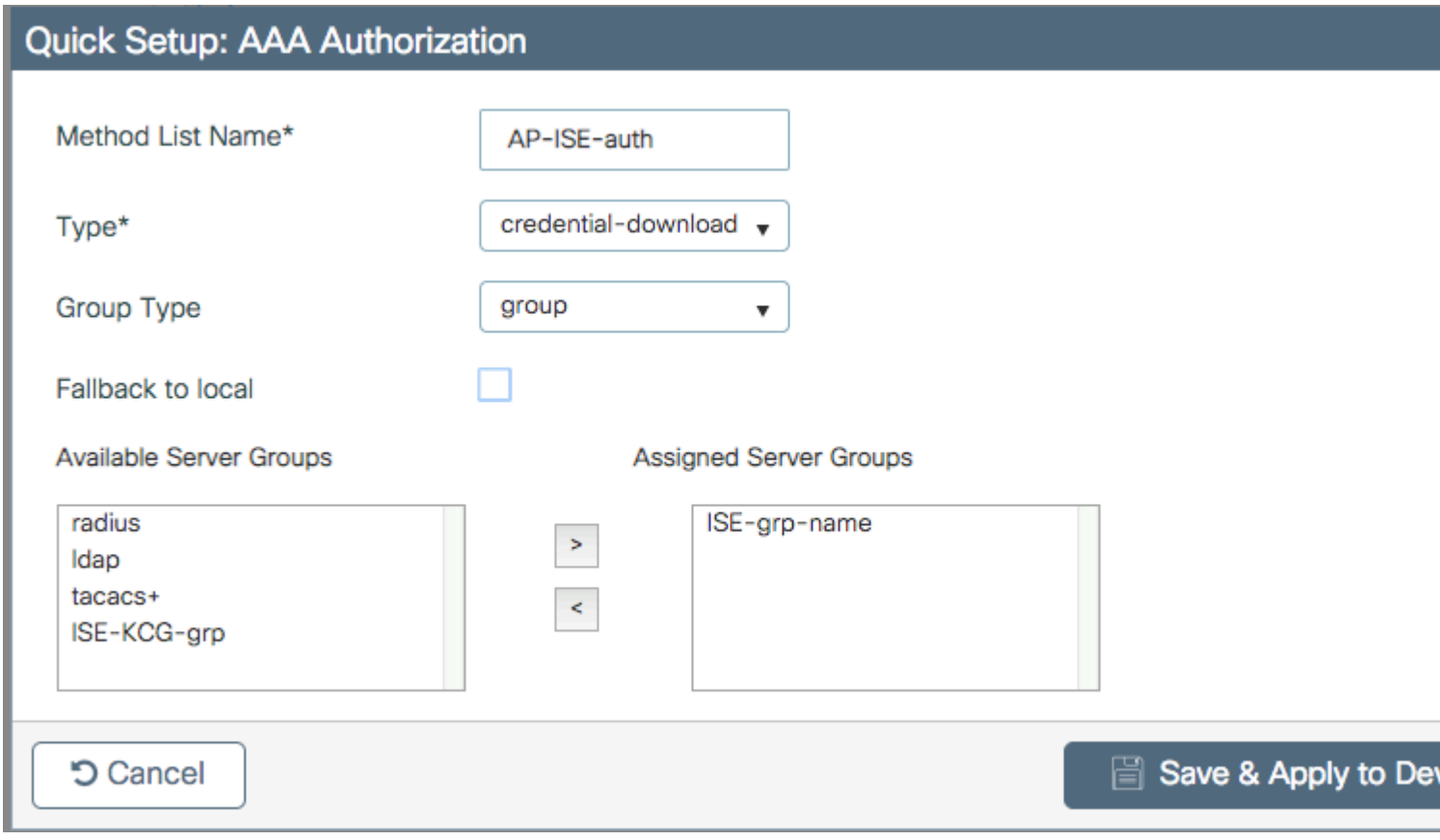
Damit die ISE die AP-MAC-Adresse authentifiziert, wenn Endpunkte die MAC-Filterung in mac ändern.



Schritt 3: Erstellen Sie eine Liste der Autorisierungsanmeldeinformationen-Downloadmethoden.

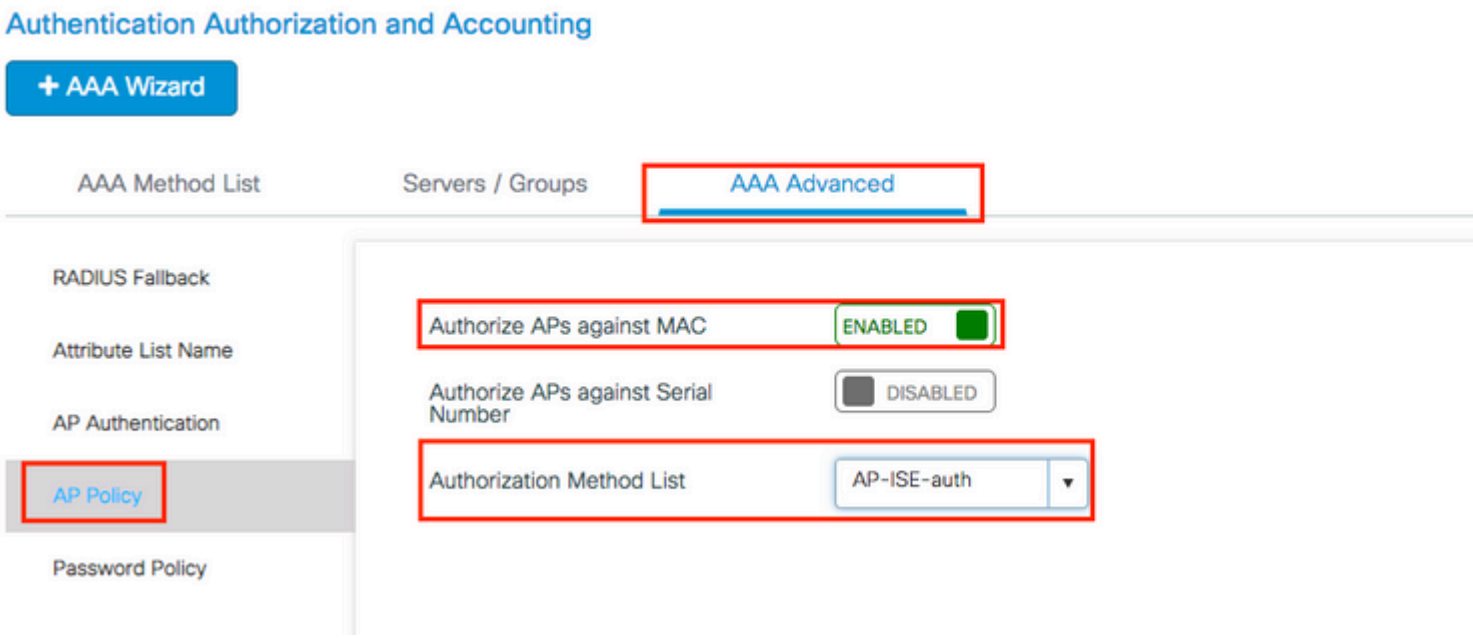
Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authorization > + Add.**





Schritt 4: Aktivieren Sie die AP-MAC-Autorisierung.

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA Advanced > AP-Richtlinie.** Aktivieren Sie die **Autorisierung von APs für MAC**, und wählen Sie die in Schritt 3 erstellte **Liste** der **Autorisierungsmethoden aus**.



CLI:

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authorization credential-download <AP-auth> group <radius-grp-name>
# ap auth-list authorize-mac
# ap auth-list method-list <AP-ISE-auth>
```

ISE-Konfiguration

Schritt 1: So fügen Sie der ISE den 9800 WLC hinzu:

9800 WLC auf der ISE angeben

Legen Sie fest, dass die MAC-Adresse der Access Points anhand der Authentifizierung konfiguriert werden soll. Führen Sie hierzu die folgenden Schritte aus:

Konfigurieren von USE zur Authentifizierung von MAC-Adressen als Endpunkte

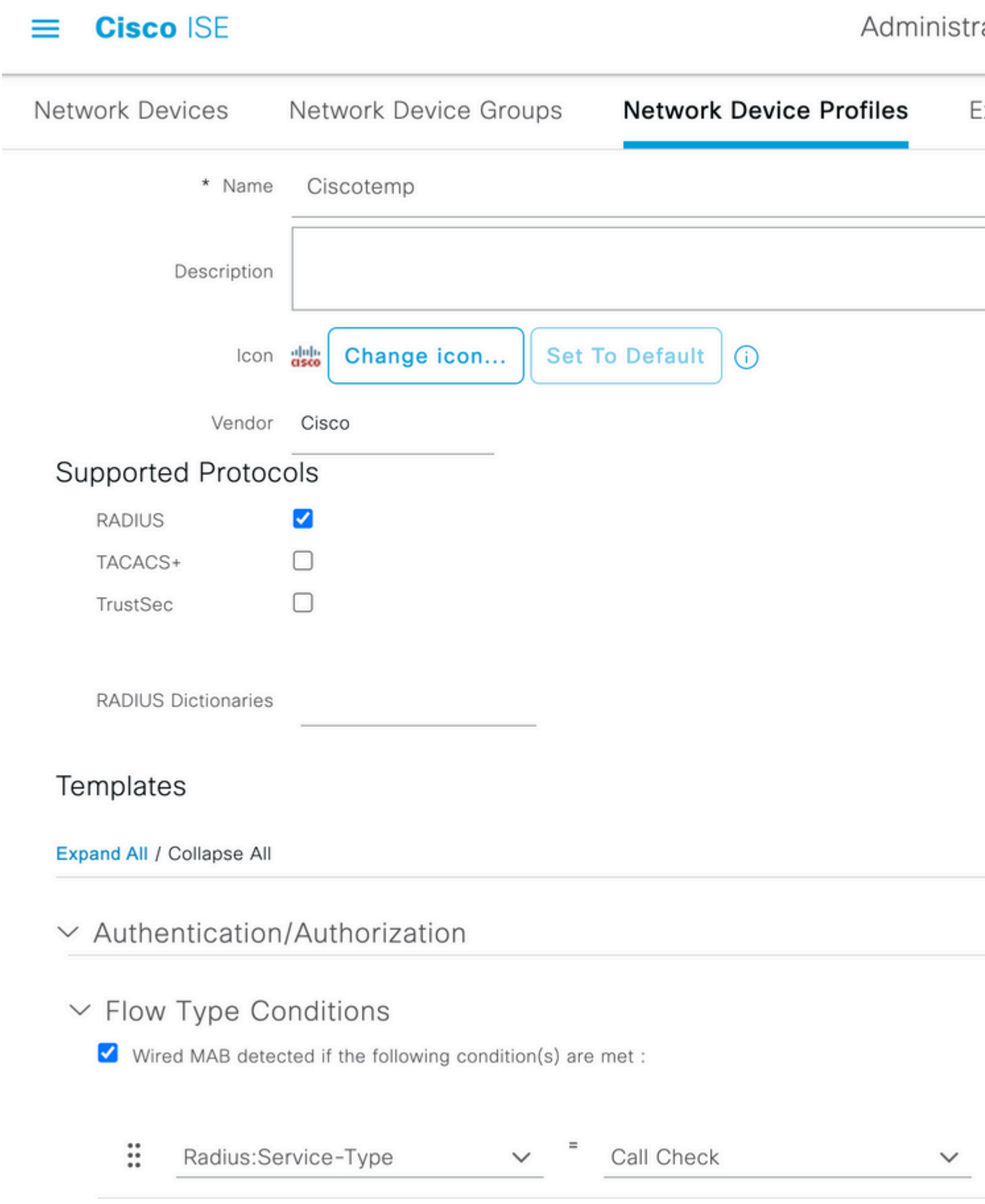
Konfigurieren der ISE zur Authentifizierung der MAC-Adresse als Benutzername/Kennwort

Konfigurieren der ISE zur Authentifizierung der MAC-Adresse als Endpunkte

Schritt 2. (Optional) Erstellen einer Identitätsgruppe für Access Points

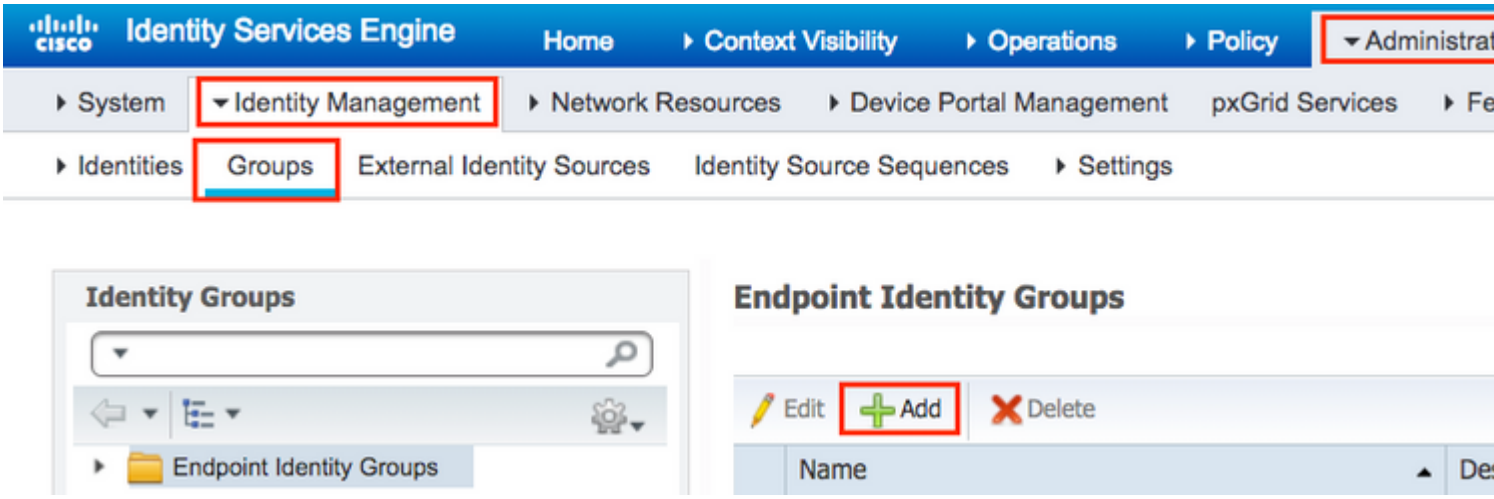
Da der 9800 das NAS-Port-Type-Attribut nicht mit AP-Autorisierung sendet, hat Cisco einen Fehler IDCSCvy74904.) erkennt die ISE eine AP-Autorisierung nicht als MAB-Workflow und daher ist es nicht möglich, einen AP zu authentifizieren, wenn die MAC-Adresse des AP in der Endpunktliste platziert wird, es sei denn, Sie ändern die MAB-Workflows so, dass das NAS-PORT-Attribut auf der ISE nicht erforderlich ist.

Navigieren Sie zu **Administrator > Network device profile,** und erstellen Sie ein neues Geräteprofil. Aktivieren Sie RADIUS, und fügen Sie service-type=call-check für Wired MAB hinzu. Den Rest können Sie aus dem ursprünglichen Cisco Profil kopieren. Es soll keine Bedingung für den "nas-port-type" für den Wired MAB geben.

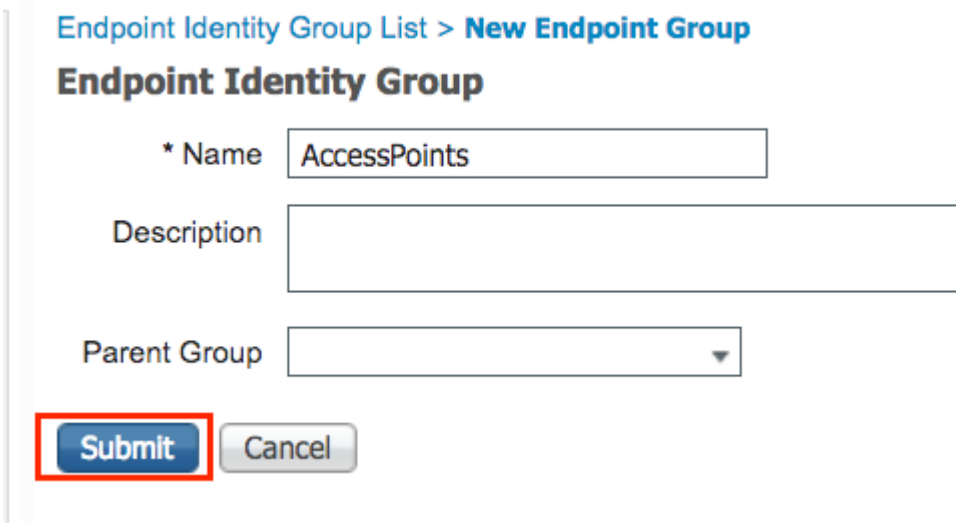


Kehren Sie zum Eintrag für das Netzwerkgerät für den 9800 zurück, und legen Sie dessen Profil auf das neu erstellte Geräteprofil fest.

Navigieren Sie zu **Administration > Identity Management > Groups > Endpoint Identity Groups > + Add.**

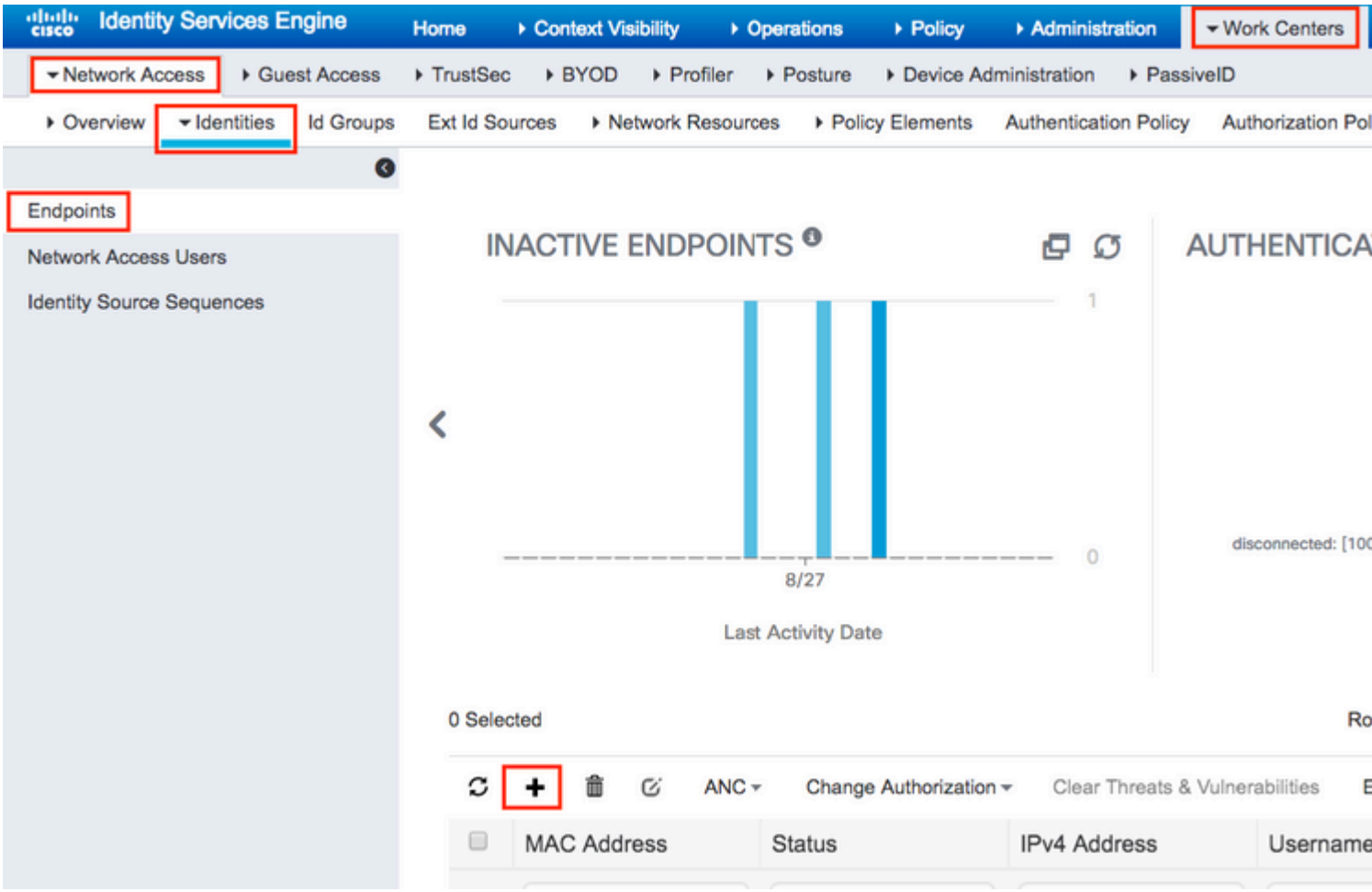


Wählen Sie einen Namen aus, und klicken Sie auf **Senden.**

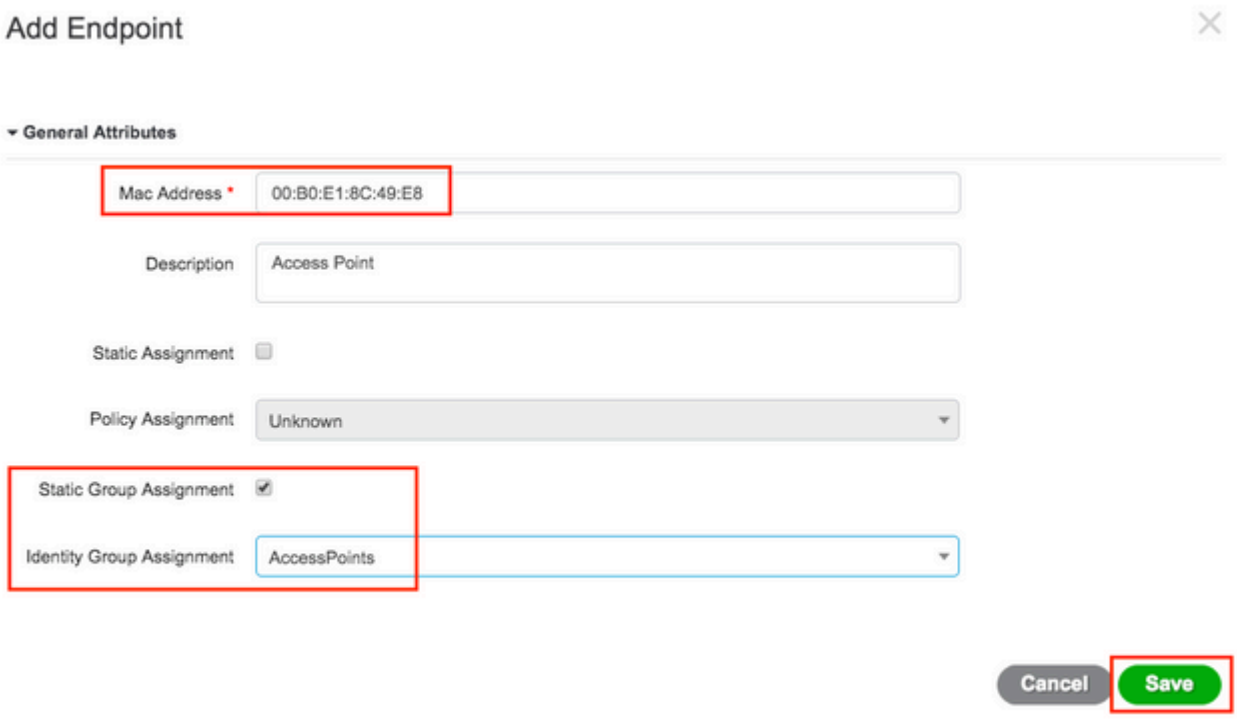


Schritt 3: Fügen Sie die MAC-Adresse des AP-Ethernets der Endgerätidentitätsgruppe hinzu.

Navigieren Sie zu **Work Centers > Network Access > Identities > Endpoints > +**



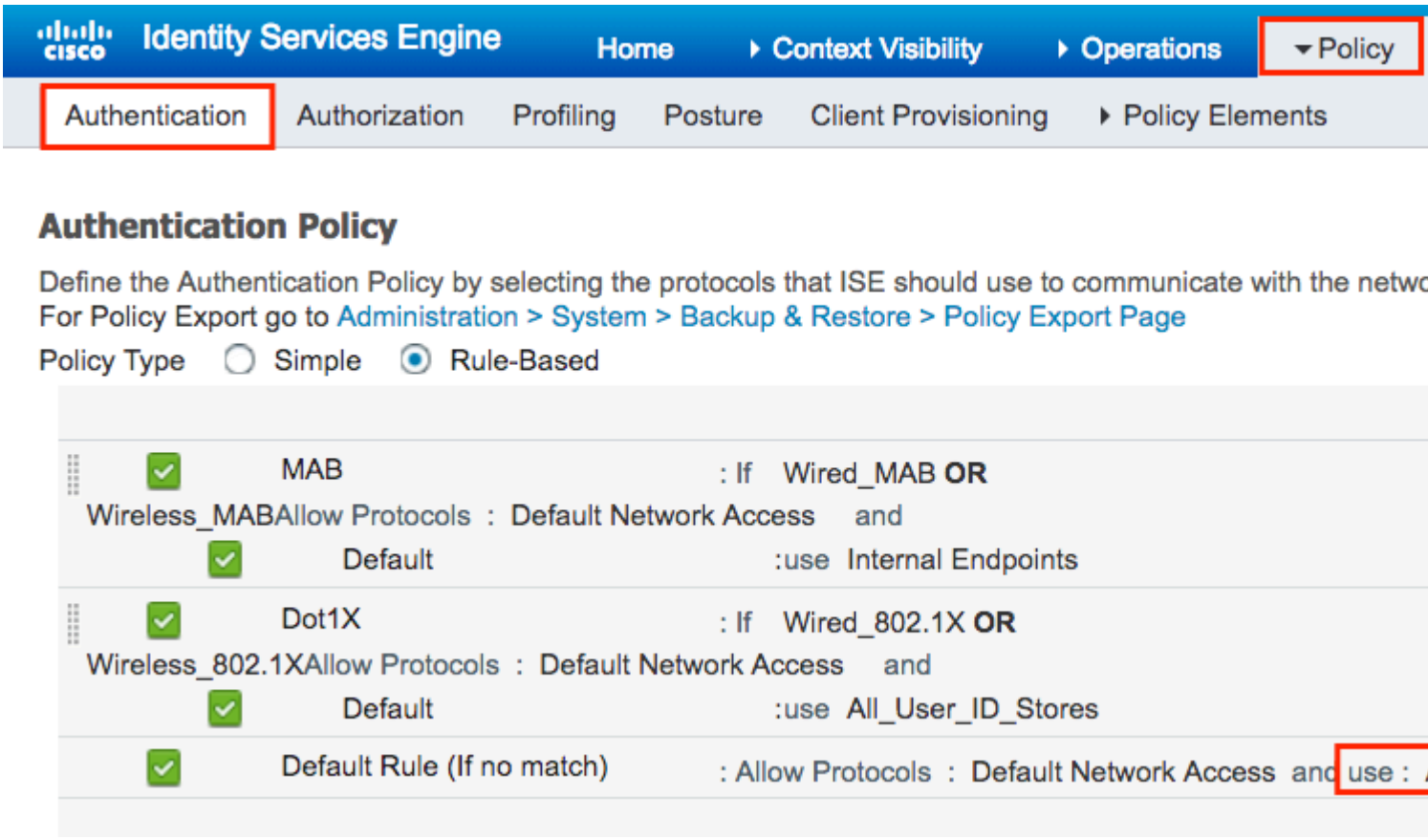
Geben Sie die erforderlichen Informationen ein.



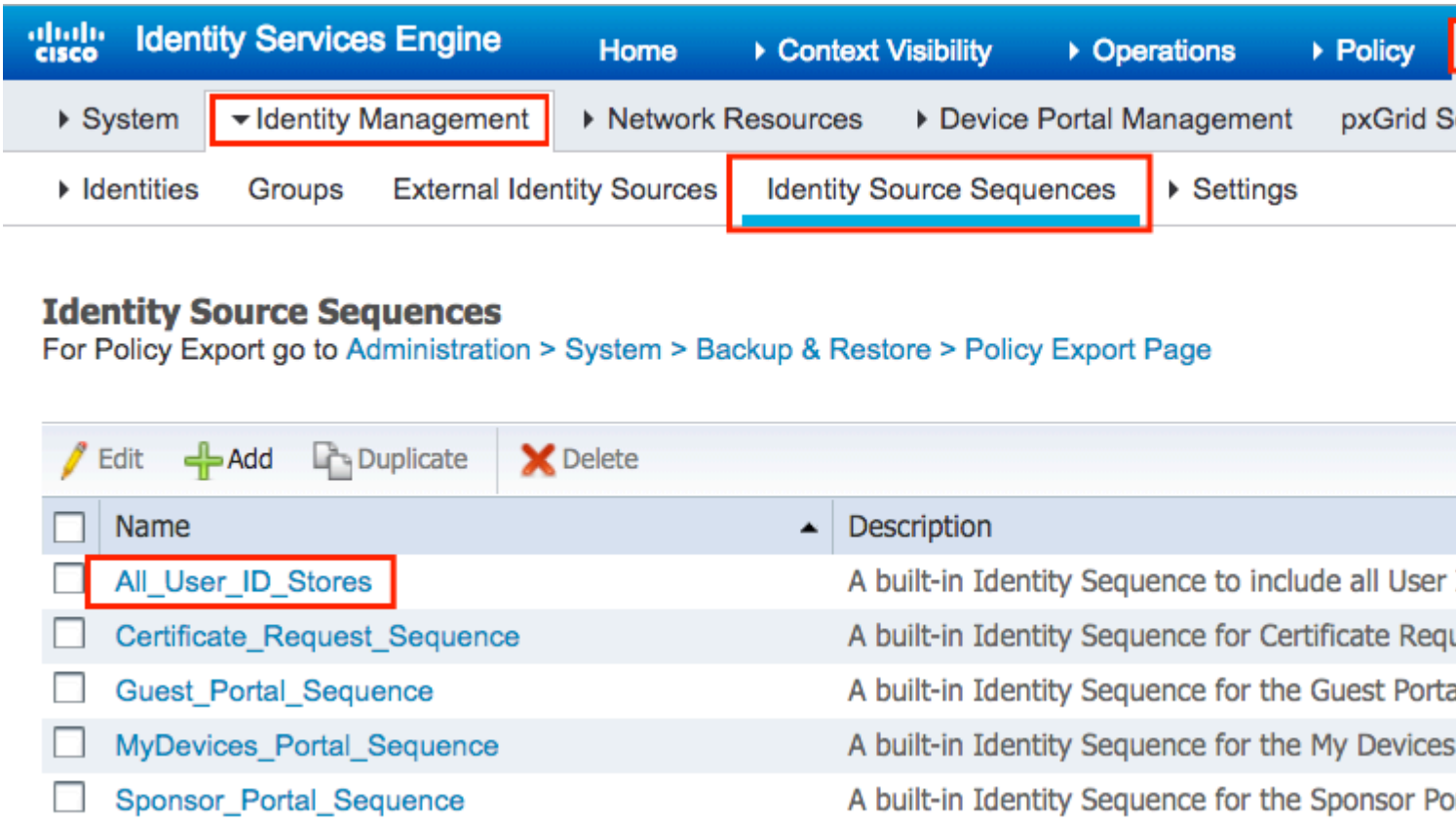
Schritt 4: Überprüfen Sie, ob der in der Standardauthentifizierungsregel verwendete Identitätsspeicher die

internen Endpunkte enthält.

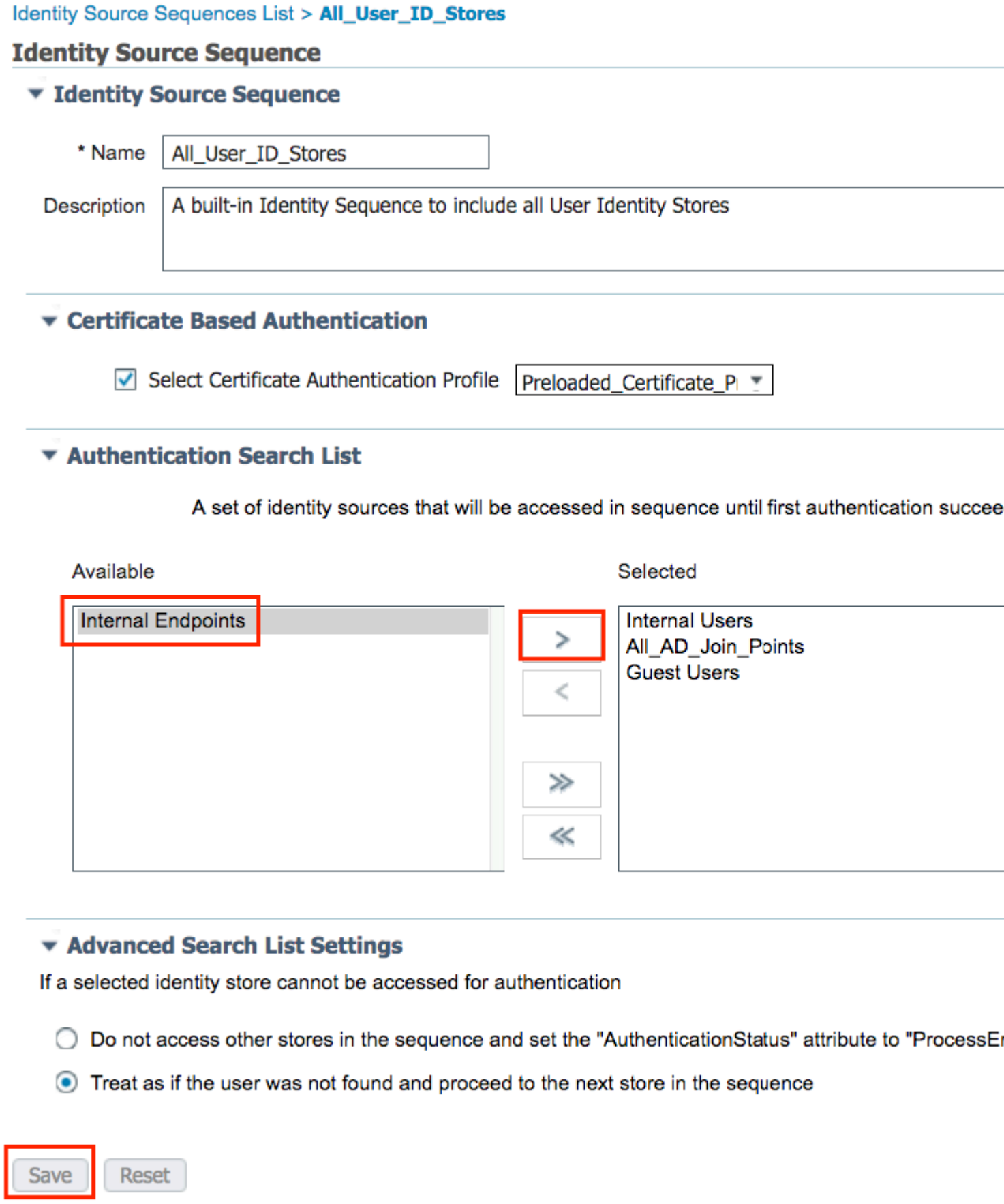
A. Navigieren Sie zu **Richtlinie > Authentifizierung,** und notieren Sie sich den Identitätsspeicher.



B. Navigieren Sie zu **Administration > Identity Management > Identity Source Sequences > Identity Name.**



C. Stellen Sie sicher, dass interne Endpunkte dazu gehören, und fügen Sie sie gegebenenfalls hinzu.



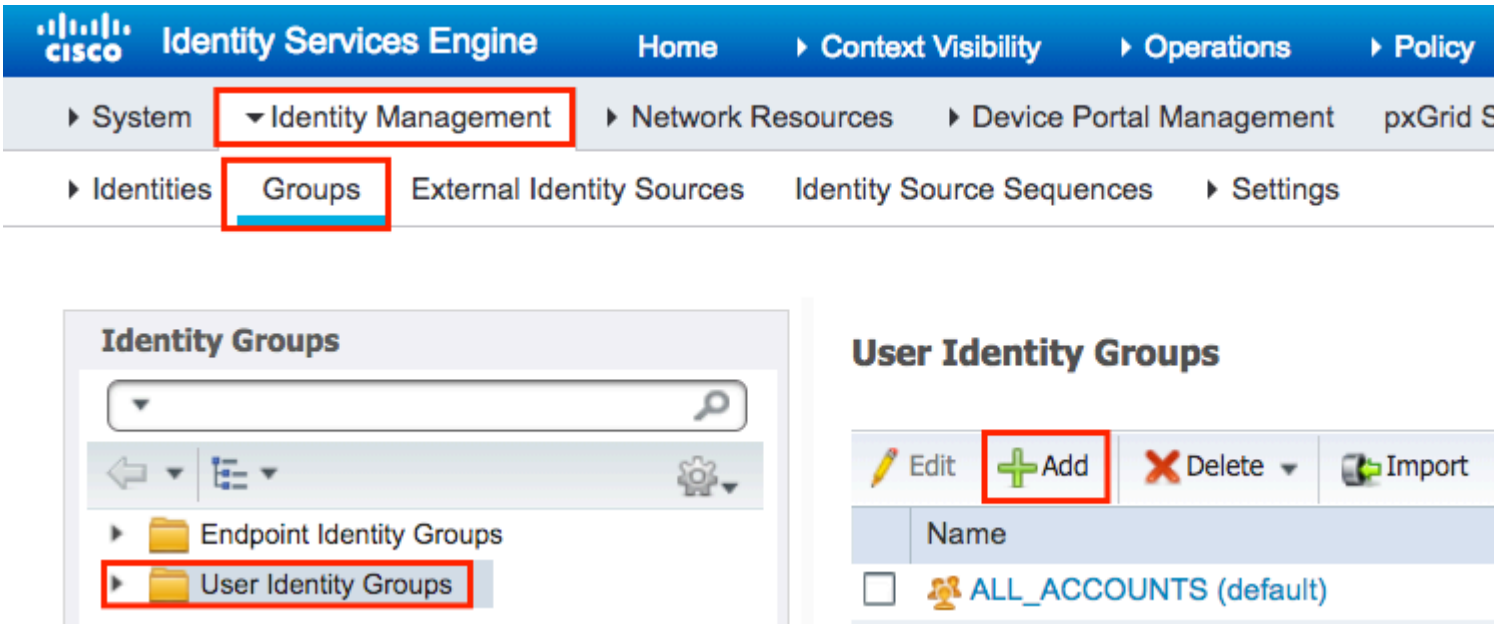
Konfigurieren der ISE zur Authentifizierung der MAC-Adresse als Benutzername/Kennwort

Diese Methode wird nicht empfohlen, da sie niedrigere Kennwortrichtlinien erfordert, damit dasselbe Kennwort wie der Benutzername zulässig ist.

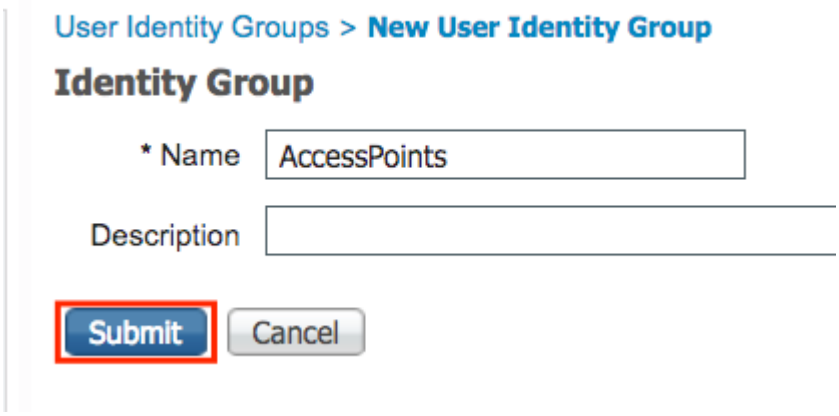
Es kann jedoch eine Problemumgehung sein, falls Sie Ihr Netzwerkgeräteprofil nicht ändern können.

Schritt 2. (Optional) Erstellen einer Identitätsgruppe für Access Points

Navigieren Sie zu **Administration > Identity Management > Groups > User Identity Groups > + Add.**

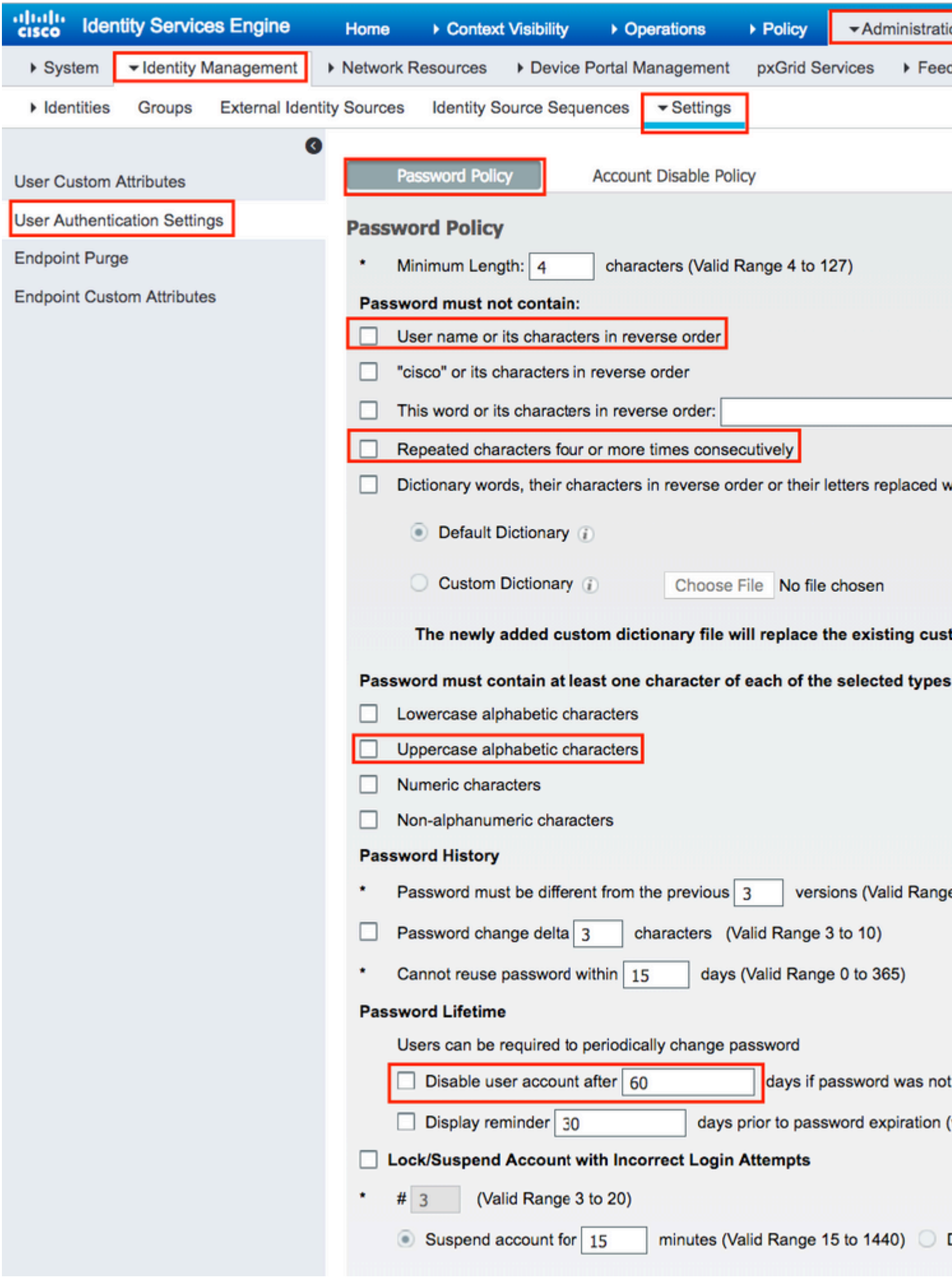


Wählen Sie einen Namen aus, und klicken Sie auf **Senden.**



Schritt 3: Vergewissern Sie sich, dass Sie mit Ihrer aktuellen Kennwortrichtlinie eine MAC-Adresse als Benutzername und Kennwort hinzufügen können.

Navigieren Sie zu **Administration > Identity Management > Settings > User Authentication Settings > Password Policy,** und stellen Sie sicher, dass mindestens diese Optionen deaktiviert sind:

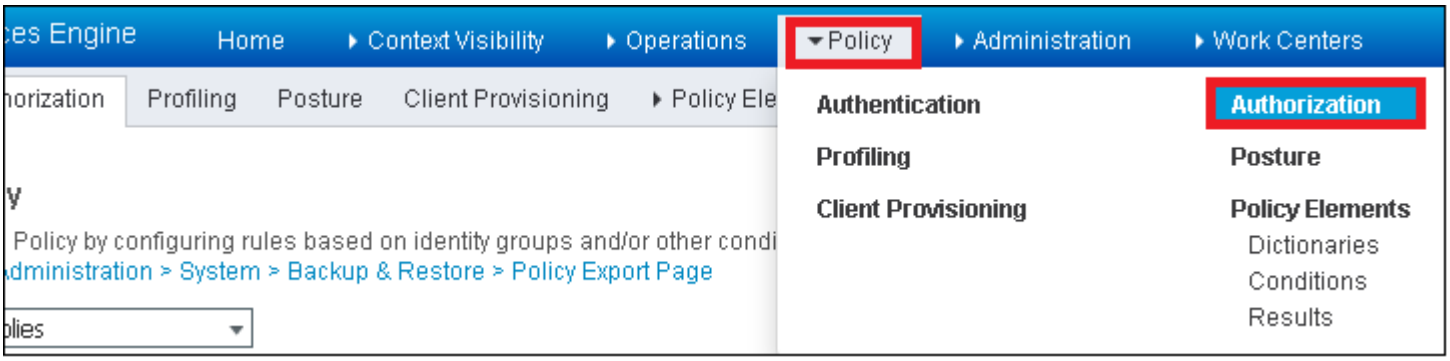


Hinweis: Sie können die Option **Benutzerkonto nach** XX **Tagen deaktivieren, wenn das Kennwort nicht geändert**

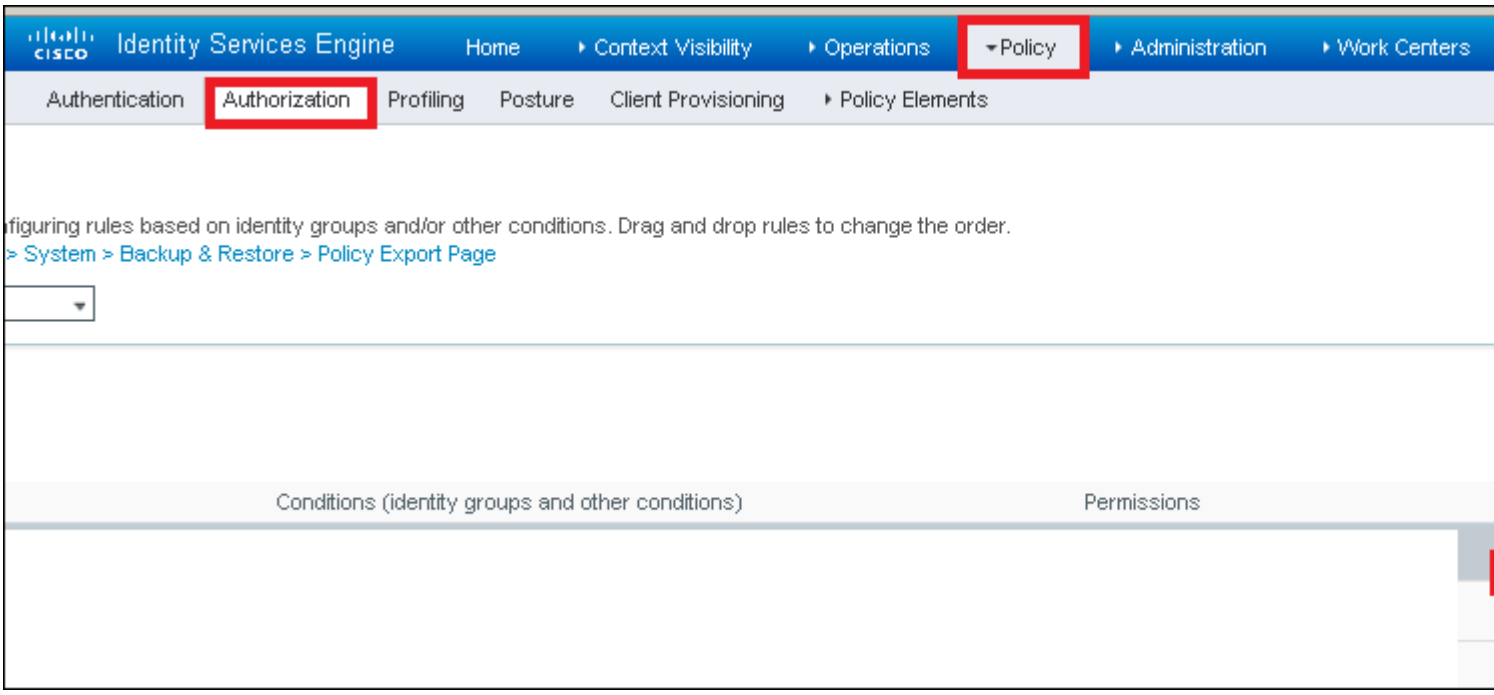
-Passwortfeld muss die Ethernet-MAC-Adresse des APs sein, nur Kleinbuchstaben und keine Trennzeichen.

Autorisierungsrichtlinie zur Authentifizierung von APs

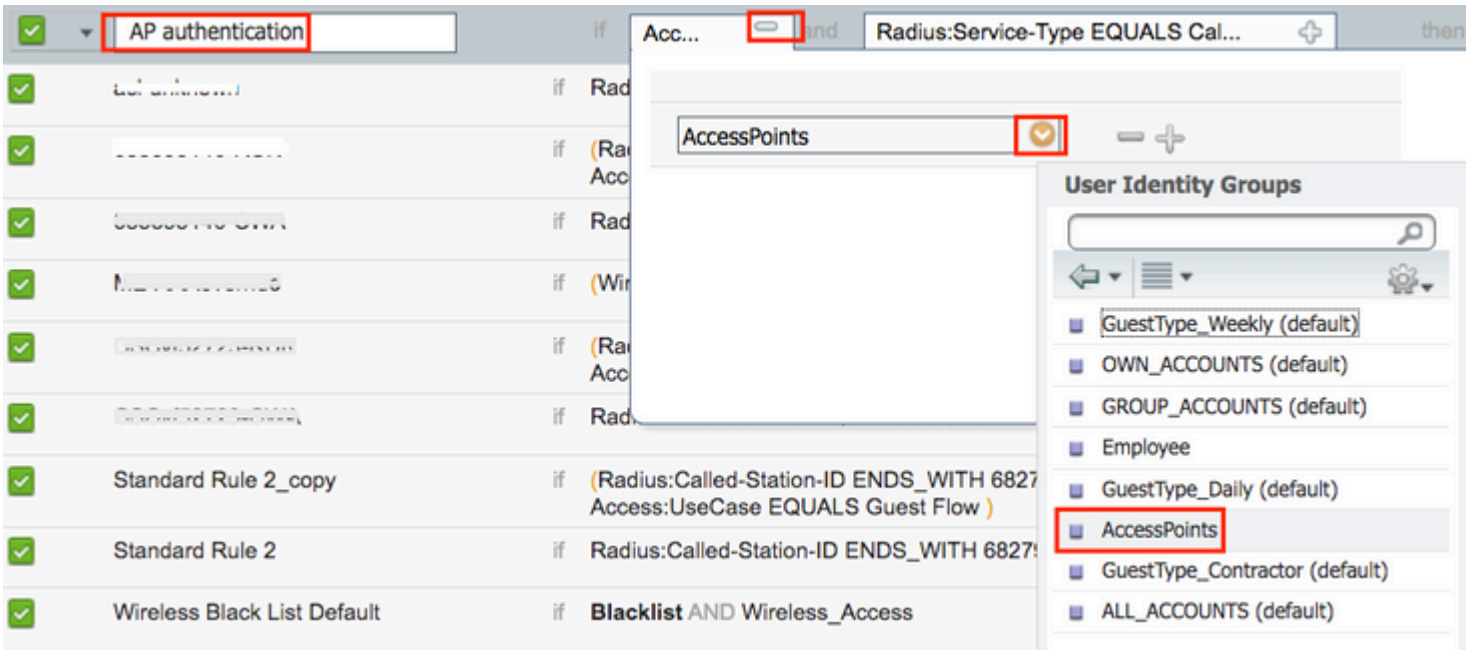
Navigieren Sie wie im Bild dargestellt **zuRichtlinie > Autorisierung**.



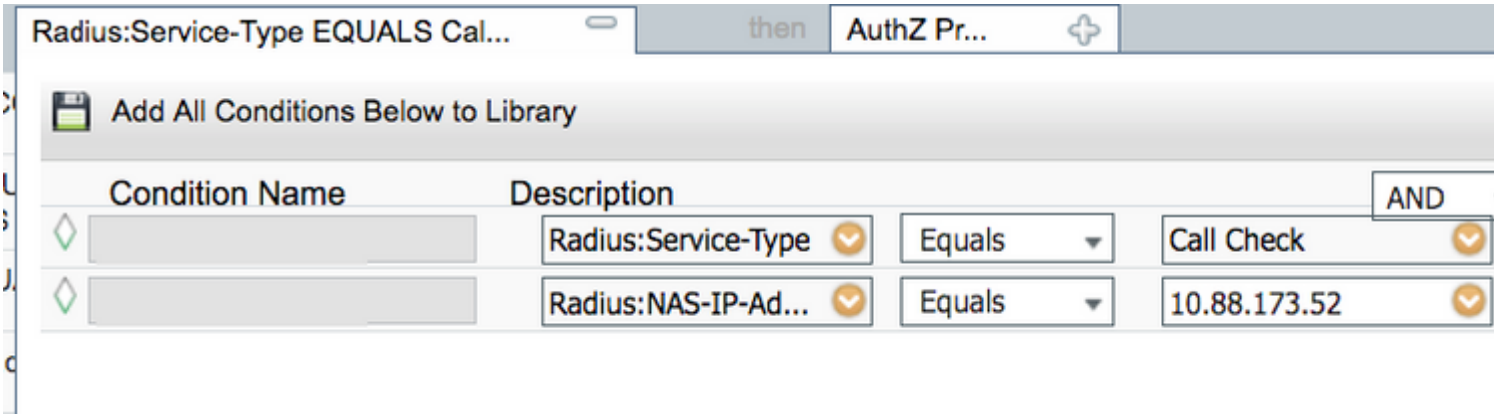
Fügt eine neue Regel wie im Bild dargestellt ein.



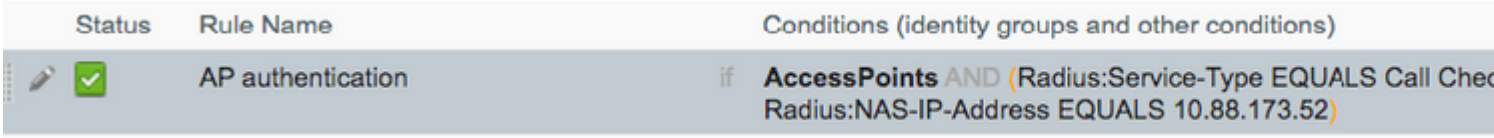
Wählen Sie zunächst einen Namen für die Regel und die Identitätsgruppe aus, in der der Access Point gespeichert ist (AccessPoints). Wählen Sie **Benutzeridentitätsgruppen** aus, wenn Sie die MAC-Adresse als Benutzername und Kennwort authentifizieren möchten, oder **Endpunkt-Identitätsgruppen,** wenn Sie die AP-MAC-Adresse als Endpunkte authentifizieren möchten.



Wählen Sie anschließend andere Bedingungen für den Autorisierungsprozess aus, um in diese Regel zu fallen. In diesem Beispiel greift der Autorisierungsprozess auf diese Regel zu, wenn der Diensttyp "Anrufprüfung" verwendet wird und die Authentifizierungsanforderung von der IP-Adresse 10.88.173.52 stammt.



Wählen Sie anschließend das Autorisierungsprofil aus, das den Clients zugewiesen ist, die diese Regel aufgerufen haben, klicken Sie aufWeiter, und speichern Sie es, wie im Bild dargestellt.



Hinweis: APs, die dem Controller bereits beigetreten sind, verlieren ihre Zuordnung nicht. Wenn sie jedoch nach der Aktivierung der Autorisierungsliste die Kommunikation mit dem Controller verlieren und versuchen, sich wieder anzuschließen, durchlaufen sie den Authentifizierungsprozess. Wenn ihre MAC-Adressen nicht lokal oder im RADIUS-Server aufgeführt werden, können sie keine Verbindung zum Controller herstellen.

Überprüfung

Überprüfen Sie, ob der 9800 WLC eine Liste zur Authentifizierung von APs aktiviert hat.

<#root>

 # show ap auth-list

```
Authorize APs against MAC : Disabled
Authorize APs against Serial Num : Enabled
Authorization Method List : <auth-list-name>
```

Radius-Konfiguration überprüfen:

<#root>

#

show run aaa

Fehlerbehebung

Der WLC 9800 bietet IMMER-EIN-Ablaufverfolgungsfunktionen. Dadurch wird sichergestellt, dass alle mit dem AP-Beitritt zusammenhängenden Fehler, Warnungen und Meldungen auf Benachrichtigungsebene ständig protokolliert werden und Sie nach einem Vorfall oder Ausfall Protokolle anzeigen können.

Hinweis: Die Anzahl der generierten Protokolle variiert von einigen Stunden bis zu mehreren Tagen.

Um die Traces anzuzeigen, die der 9800 WLC standardmäßig erfasst, können Sie über SSH/Telnet eine Verbindung zum 9800 WLC herstellen (stellen Sie sicher, dass Sie die Sitzung in einer Textdatei protokollieren).

Schritt 1: Überprüfen Sie die aktuelle Uhrzeit des Controllers, damit Sie die Protokolle bis zum Auftreten des Problems nachverfolgen können.

```
# show clock
```

Schritt 2: Erfassen Sie die Syslogs aus dem Controller-Puffer oder dem externen Syslog gemäß der Systemkonfiguration. Dadurch erhalten Sie einen schnellen Überblick über den Systemzustand und eventuelle Fehler.

```
# show logging
```

Schritt 3: Überprüfen Sie, ob Debug-Bedingungen aktiviert sind.

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Trace Configs:


Packet Infra debugs:

Ip Address                                              Port
------------------------------------------------------|----------
```

> **Hinweis**: Wenn eine Bedingung aufgelistet ist, bedeutet dies, dass die Traces für alle Prozesse, bei denen die aktivierten Bedingungen (MAC-Adresse, IP-Adresse usw.) auftreten, auf Debugging-Ebene protokolliert werden. Dies würde das Protokollvolumen erhöhen. Daher wird empfohlen, alle Bedingungen zu löschen, wenn gerade kein Debugging aktiv ist

---

Schritt 4: Angenommen, die zu testende MAC-Adresse wurde in Schritt 3 nicht als Bedingung aufgeführt. Sammeln Sie die stets verfügbaren Traces auf Benachrichtigungsebene für die jeweilige MAC-Adresse.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<
```

Sie können entweder den Inhalt der Sitzung anzeigen oder die Datei auf einen externen TFTP-Server kopieren.

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Bedingtes Debugging und Radio Active Tracing

Wenn die stets verfügbaren Ablaufverfolgungen nicht genügend Informationen liefern, um den Auslöser für das zu untersuchende Problem zu bestimmen, können Sie bedingtes Debuggen aktivieren und die Radio Active (RA)-Ablaufverfolgung erfassen, die Ablaufverfolgungen auf Debugebene für alle Prozesse bereitstellt, die mit der angegebenen Bedingung interagieren (in diesem Fall Client-MAC-Adresse).

Schritt 5: Stellen Sie sicher, dass keine Debug-Bedingungen aktiviert sind.

```
# clear platform condition all
```

Schritt 6: Aktivieren Sie die Debug-Bedingung für die MAC-Adresse des Wireless-Clients, die Sie überwachen möchten.

Mit diesen Befehlen wird die angegebene MAC-Adresse 30 Minuten (1800 Sekunden) lang überwacht. Sie können diese Zeit optional auf bis zu 2085978494 Sekunden erhöhen.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Hinweis: Um mehr als einen Client gleichzeitig zu überwachen, führen Sie den Befehl â€ždebug wireless mac <aaaa.bbbb.cccc>â€œ für jede MAC-Adresse aus.

Hinweis: Sie sehen die Ausgabe der Client-Aktivität in der Terminalsitzung nicht, da alles intern gepuffert wird, um später angezeigt zu werden.

Schritt 7. Reproduzieren Sie das Problem oder Verhalten, das Sie überwachen möchten.

Schritt 8: Stoppen Sie die Debugs, wenn das Problem reproduziert wird, bevor die standardmäßige oder konfigurierte Monitoring-Zeit abgelaufen ist.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Sobald die Monitoring-Zeit abgelaufen ist oder das Wireless-Debugging beendet wurde, generiert der 9800 WLC eine lokale Datei mit dem Namen:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Schritt 9. Rufen Sie die Datei mit der MAC-Adressaktivität ab. Sie können entweder die Datei â€žra trace.logâ€œ auf einen externen Server kopieren oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Überprüfen Sie den Namen der RA-Tracing-Datei

```
# dir bootflash: | inc ra_trace
```

Datei auf externen Server kopieren:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d
```

Inhalt anzeigen:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Schritt 10. Wenn die Ursache immer noch nicht offensichtlich ist, rufen Sie die internen Protokolle ab, die eine ausführlichere Ansicht der Protokolle auf Debug-Ebene darstellen. Sie müssen den Client nicht noch einmal debuggen, da wir uns nur die Debug-Protokolle genauer ansehen, die bereits gesammelt und intern gespeichert wurden.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra
```

> **Hinweis**: Diese Befehlsausgabe gibt Traces für alle Protokollierungsebenen für alle Prozesse zurück und ist sehr umfangreich. Wenden Sie sich an das Cisco TAC, um diese Nachverfolgungen zu analysieren.

Sie können entweder die Datei â€žra-internal-FILENAME.txtâ€œ auf einen externen Server kopieren oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Datei auf externen Server kopieren:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Inhalt anzeigen:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Schritt 11. Entfernen Sie die Debug-Bedingungen.

```
# clear platform condition all
```

> **Hinweis**: Stellen Sie sicher, dass Sie die Debug-Bedingungen immer nach einer Fehlerbehebungssitzung entfernen.

Referenzen

Verbindung von Mesh-APs mit 9800 WLC

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.