MAC-Authentifizierungs-SSID auf Catalyst 9800 Wireless Controllern konfigurieren

Inhalt

Einleitung

In diesem Dokument wird die Einrichtung eines Wireless Local Area Network (WLAN) mit MAC-Authentifizierungssicherheit auf dem Cisco Catalyst 9800 WLC beschrieben.

Voraussetzungen

Anforderung

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

- MAC-Adresse
- Wireless Controller der Cisco Catalyst 9800-Serie
- Identity Service Engine (ISE)

Verwendete Komponenten

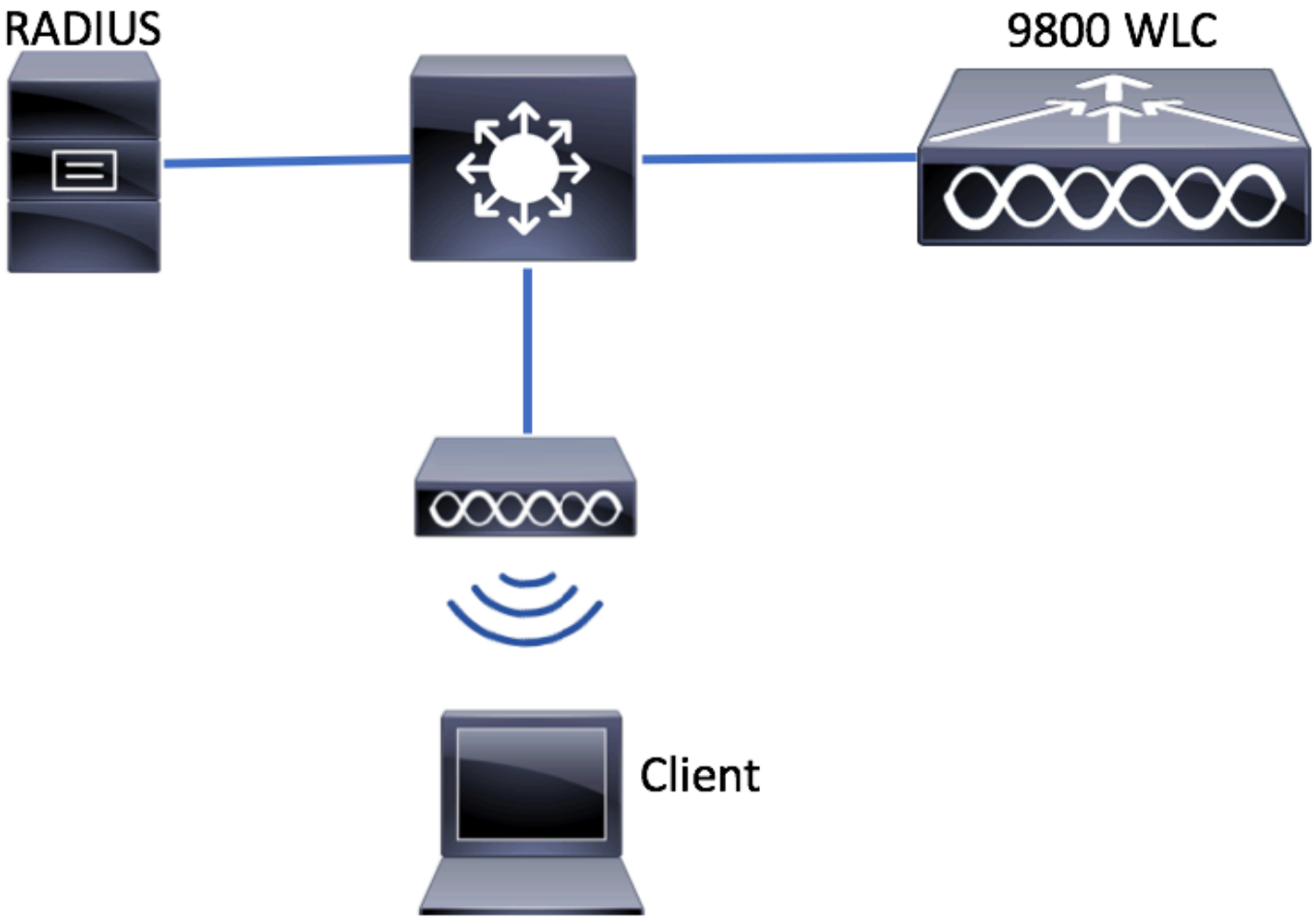
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco IOS® XE Gibraltar v16.12
- ISE 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 verstehen.

Konfigurieren

Netzwerkdiagramm



AAA-Konfiguration auf dem 9800 WLC

Clients mit externem Server authentifizieren

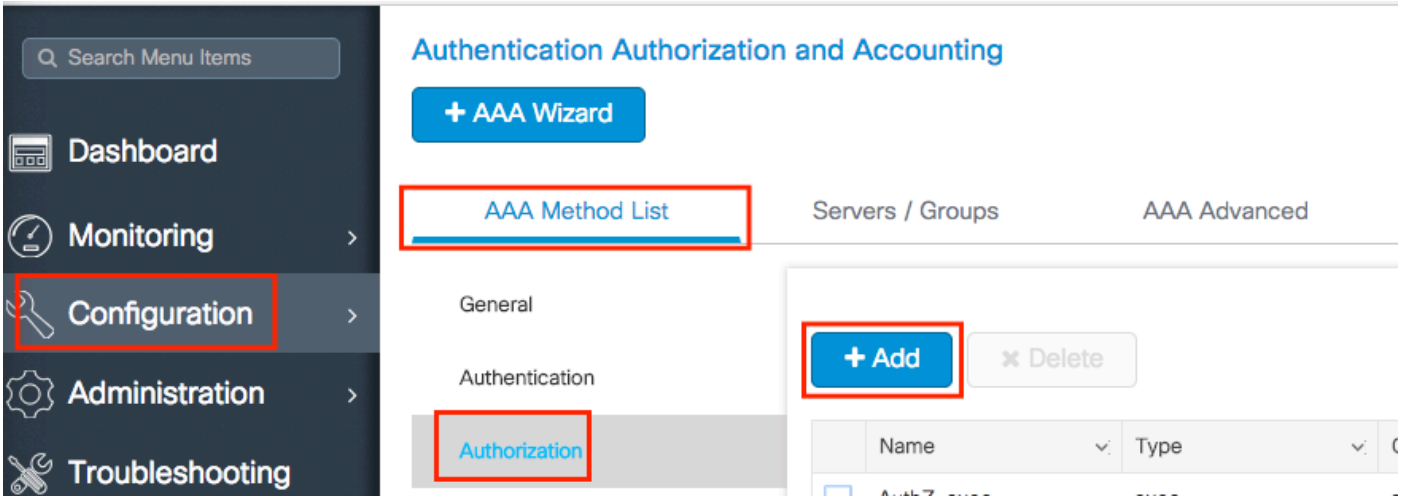
GUI:

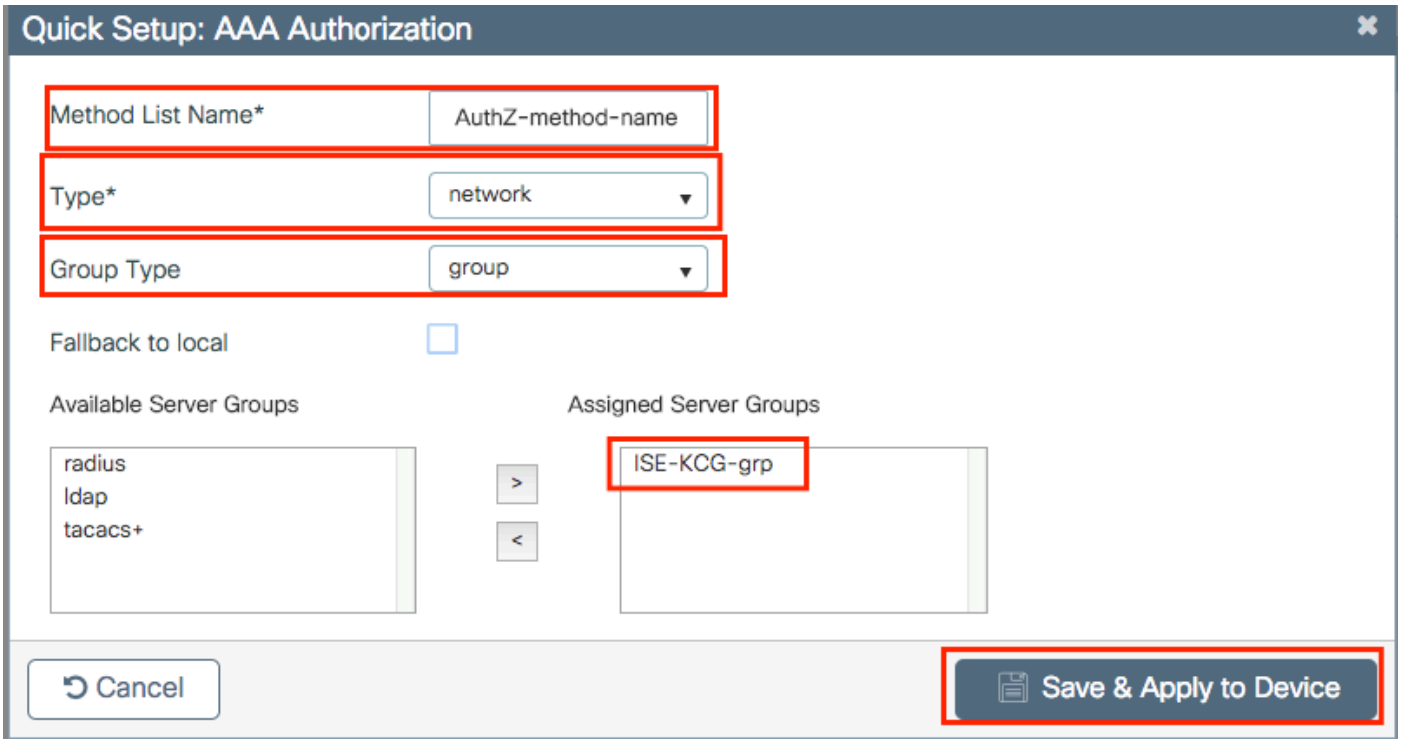
Lesen Sie die Schritte 1-3 im Abschnitt "AAA-Konfiguration für 9800-WLCs" über diesen Link:

AAA-Konfiguration des WLC der Serie 9800

Schritt 4: Erstellen Sie eine Methode für das Autorisierungsnetzwerk.

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





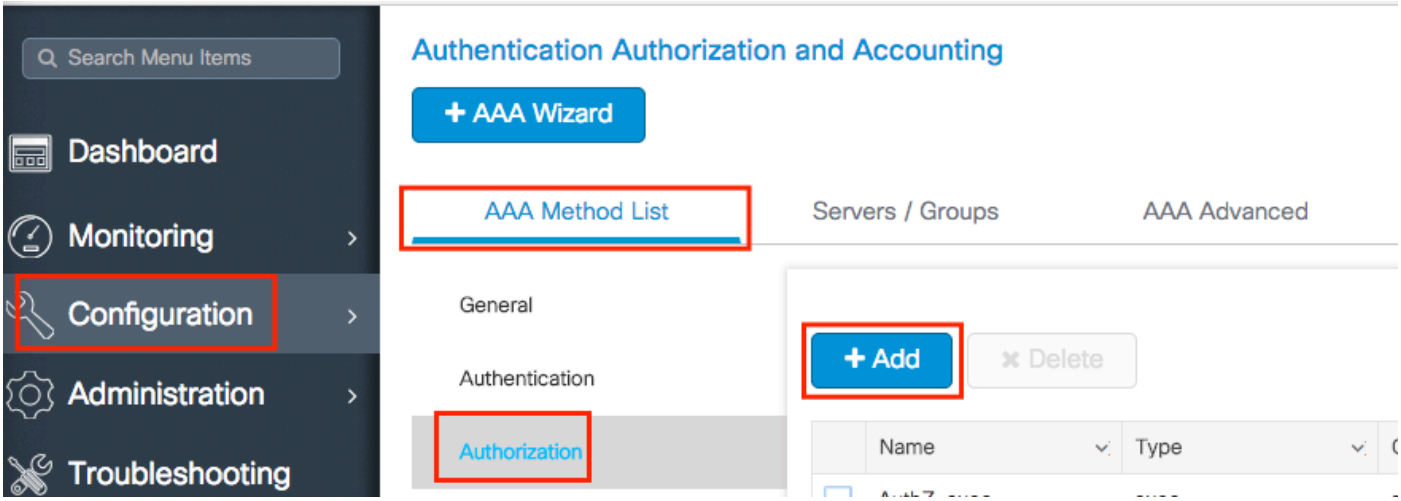
CLI:

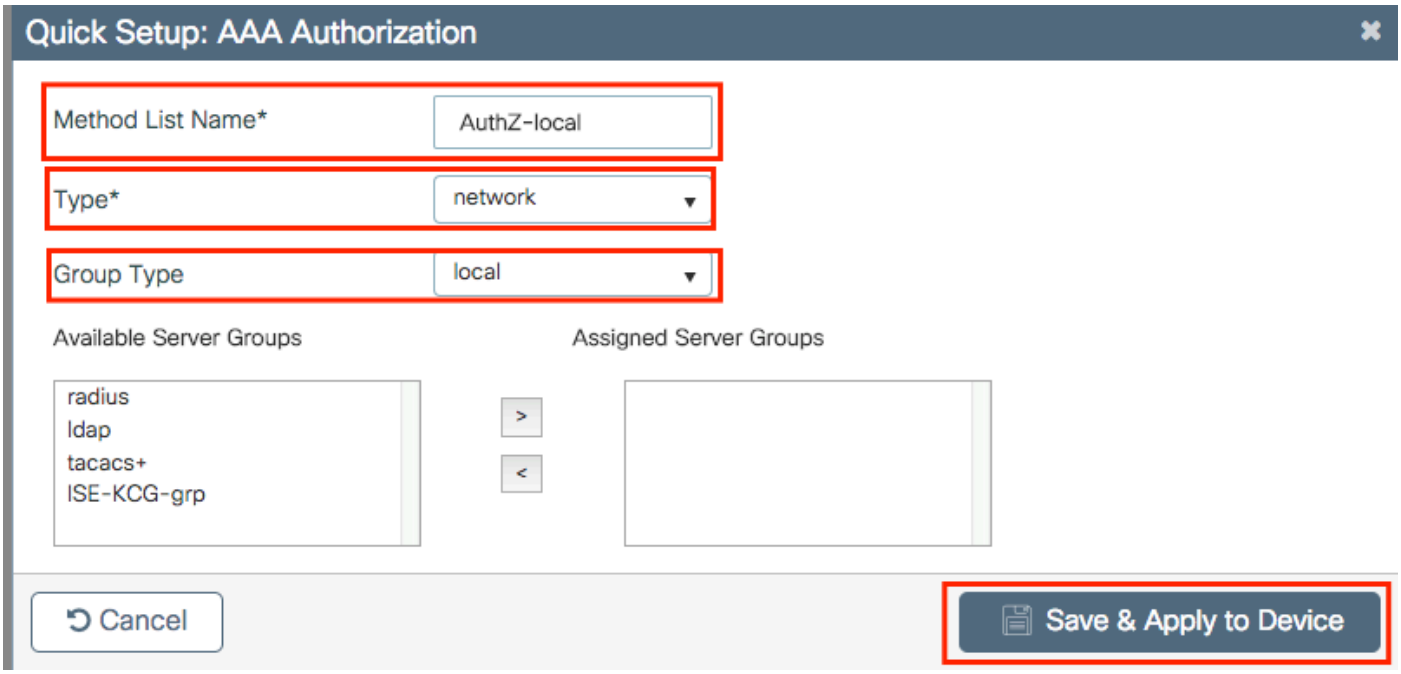
```
# config t
# aaa new-model

# 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 network <AuthZ-method-name> group <radius-grp-name>
```

Clients lokal authentifizieren

Erstellen Sie ein lokales Autorisierungsnetzwerk.

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





CLI:

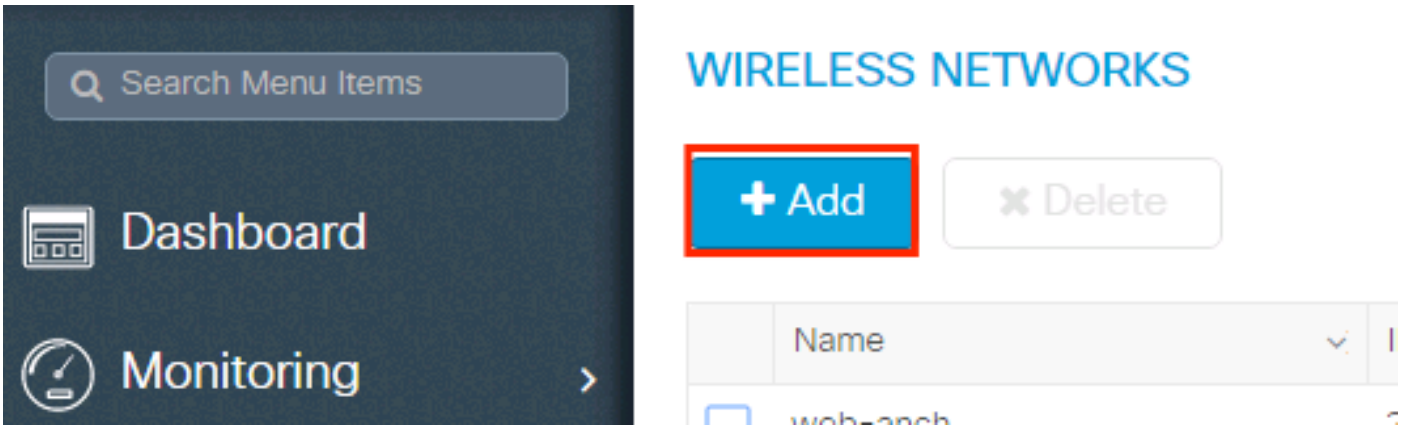
```
# config t
# aaa new-model
# aaa authorization network AuthZ-local local
```

WLAN-Konfiguration

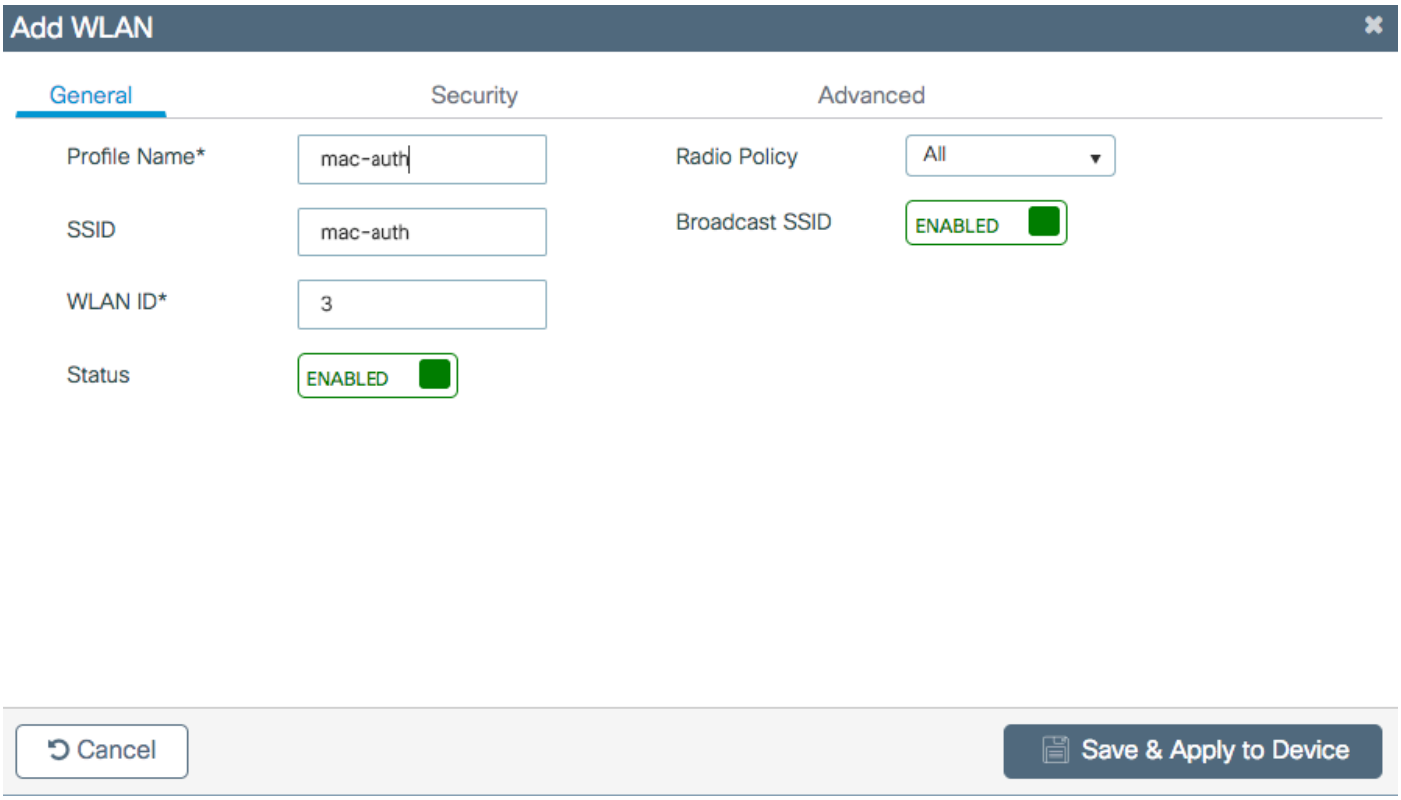
GUI:

Schritt 1: WLAN erstellen.

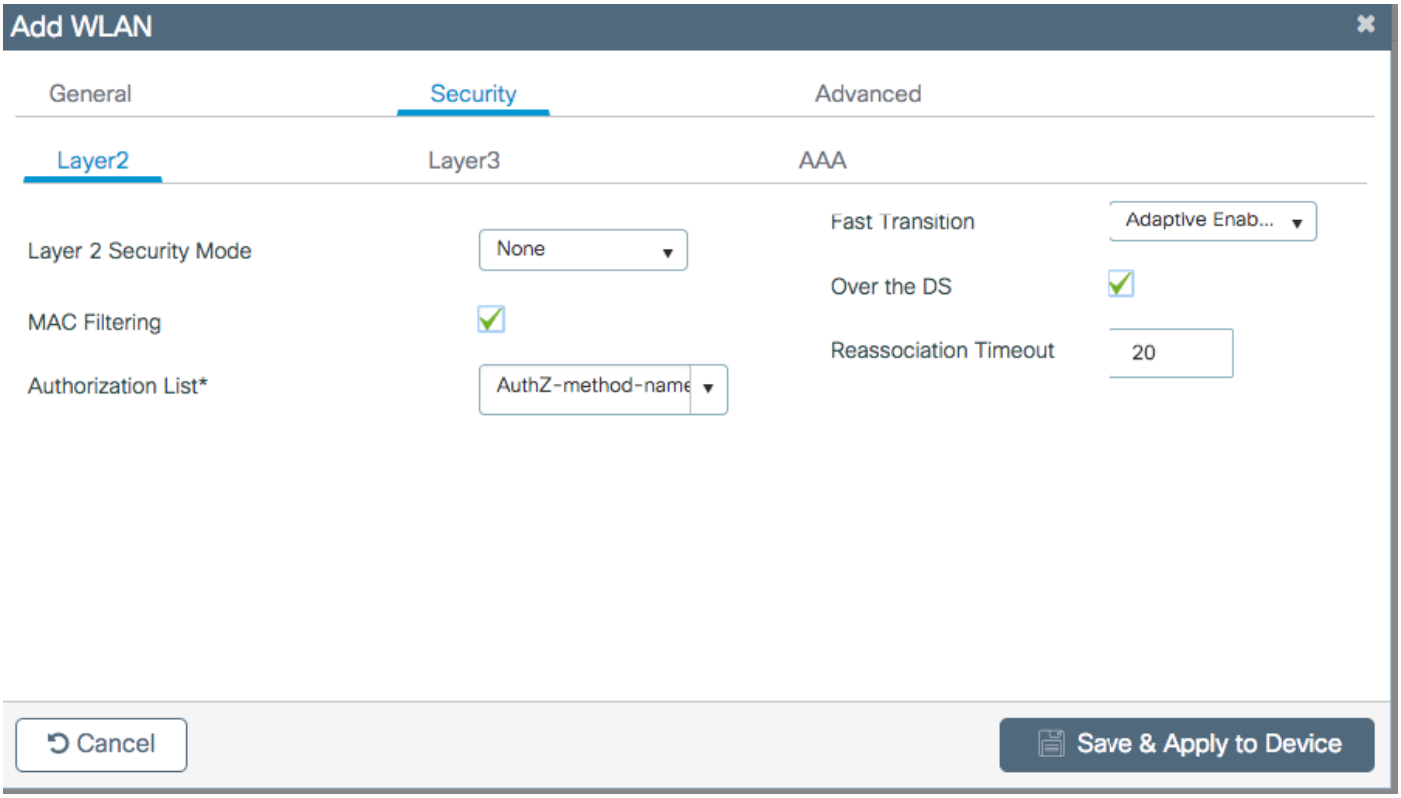
Navigieren Sie zu Configuration > Wireless > WLANs > + Add und konfigurieren Sie das Netzwerk nach Bedarf.



Schritt 2: Geben Sie die WLAN-Informationen ein.



Schritt 3: Navigieren Sie zum Security und deaktivieren Layer 2 Security Mode und aktivieren MAC Filtering. Von Authorization List, wählen Sie die Autorisierungsmethode aus, die im vorherigen Schritt erstellt wurde. Klicken Sie anschließend auf Save & Apply to Device.



CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# mac-filtering <authZ-network-method>
# no security wpa akm dot1x
# no security wpa wpa2 ciphers aes
# no shutdown
```

Richtlinienprofilkonfiguration

Sie müssen aktivieren, aaa-override im Richtlinienprofil, um sicherzustellen, dass die MAC-Filterung pro SSID einwandfrei funktioniert.

Richtlinienprofil-Konfiguration auf dem 9800 WLC

Richtlinien-Tag-Konfiguration

Richtlinien-Tag für 9800 WLC

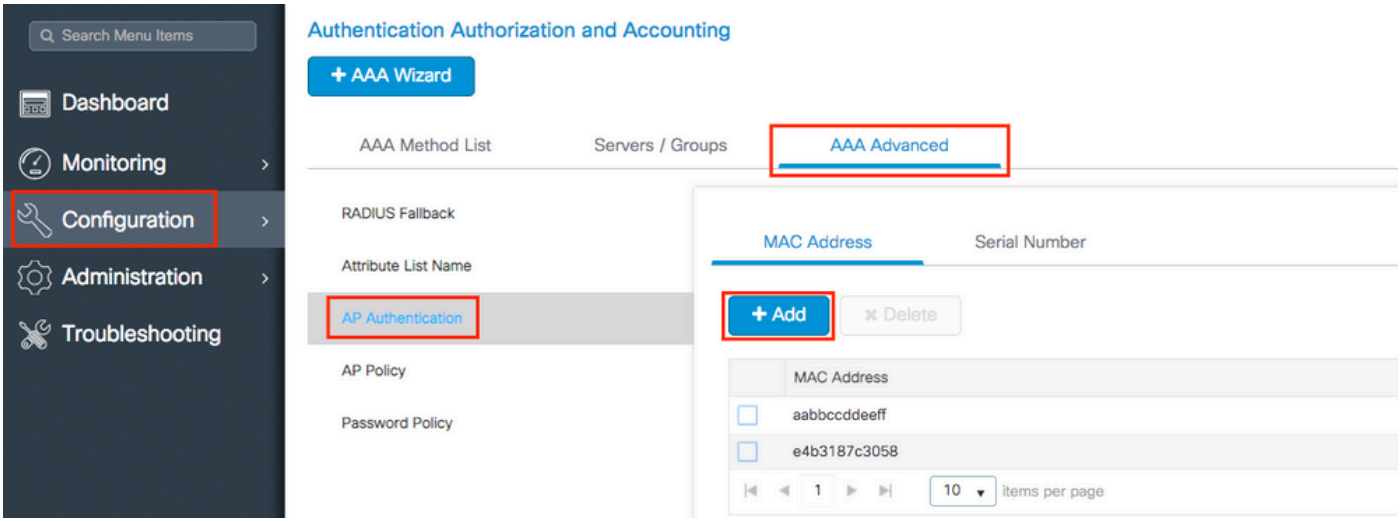
Richtlinien-Tag-Zuweisung

Zuweisen von Richtlinien-Tags für den 9800 WLC

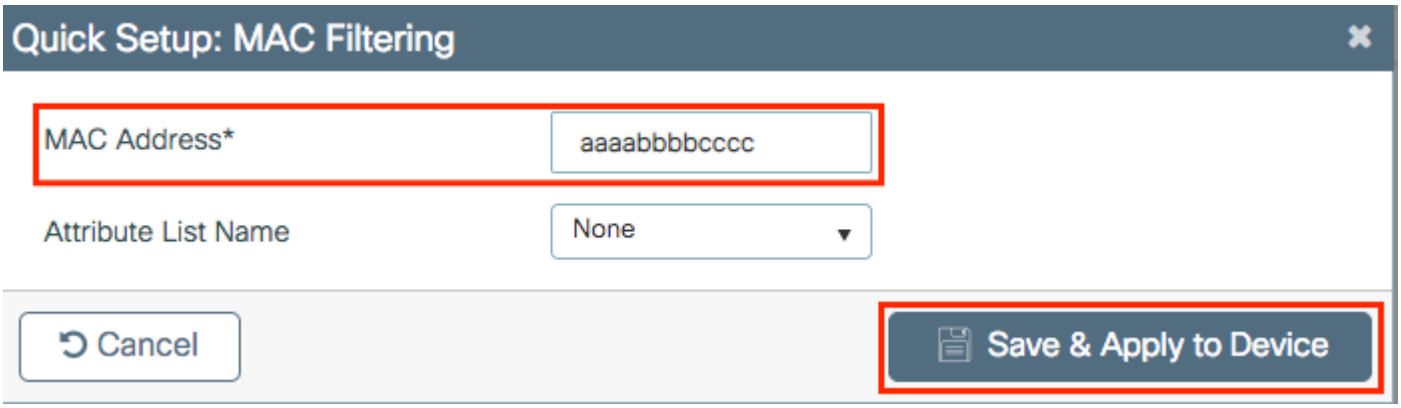
Registrieren der zulässigen MAC-Adresse

Lokale Registrierung der MAC-Adresse auf dem WLC für die lokale Authentifizierung

Navigieren Sie zu Configuration > Security > AAA > AAA Advanced > AP Authentication > + Add.



Schreiben Sie die MAC-Adresse in Kleinbuchstaben ohne Trennzeichen, und klicken Sie auf Save & Apply to Device.



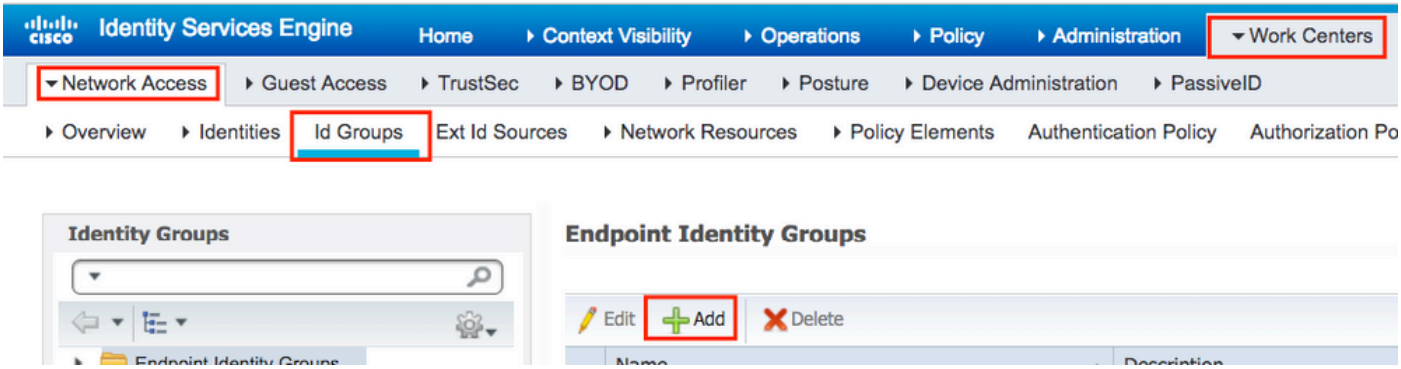
> **Hinweis**: In früheren Versionen als 17.3 hat die Webbenutzeroberfläche jedes eingegebene MAC-Format in das in der Abbildung dargestellte Format ohne Trennzeichen geändert. In 17.3 und höher respektiert die Web-Benutzeroberfläche das eingegebene Design, und es ist daher wichtig, keine Trennlinie einzugeben. Enhancement Bug Die Cisco Bug-ID CSCv43870 verfolgt die Unterstützung verschiedener Formate für die MAC-Authentifizierung.

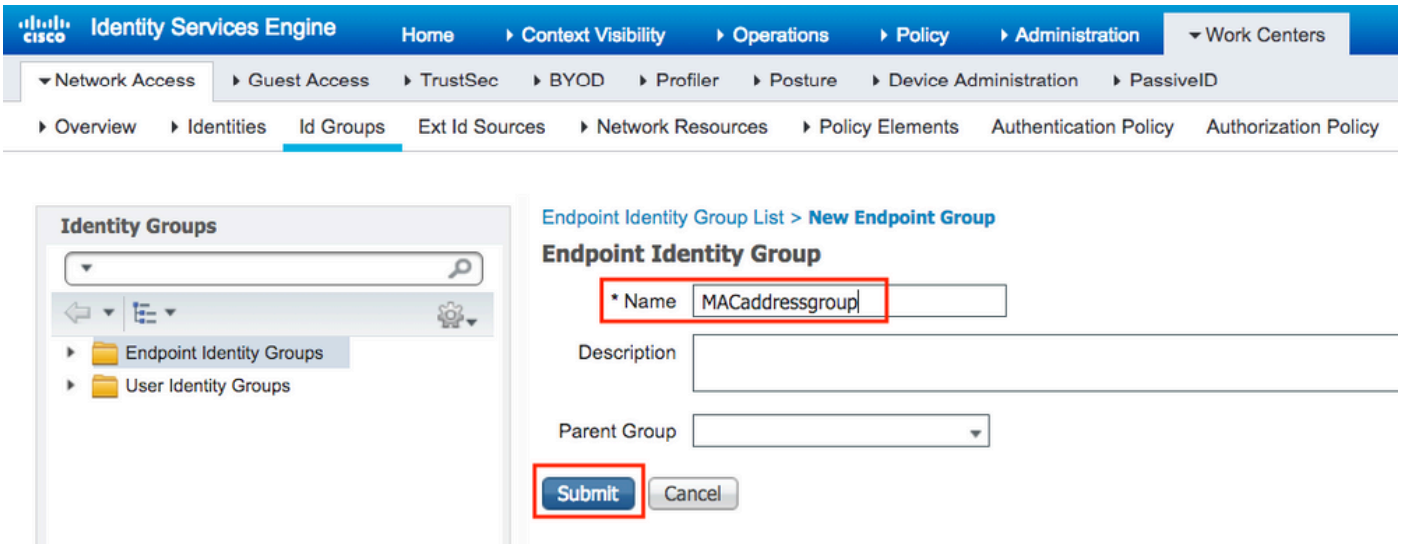
CLI:

```
# config t
# username <aabbccddeeff> mac
```

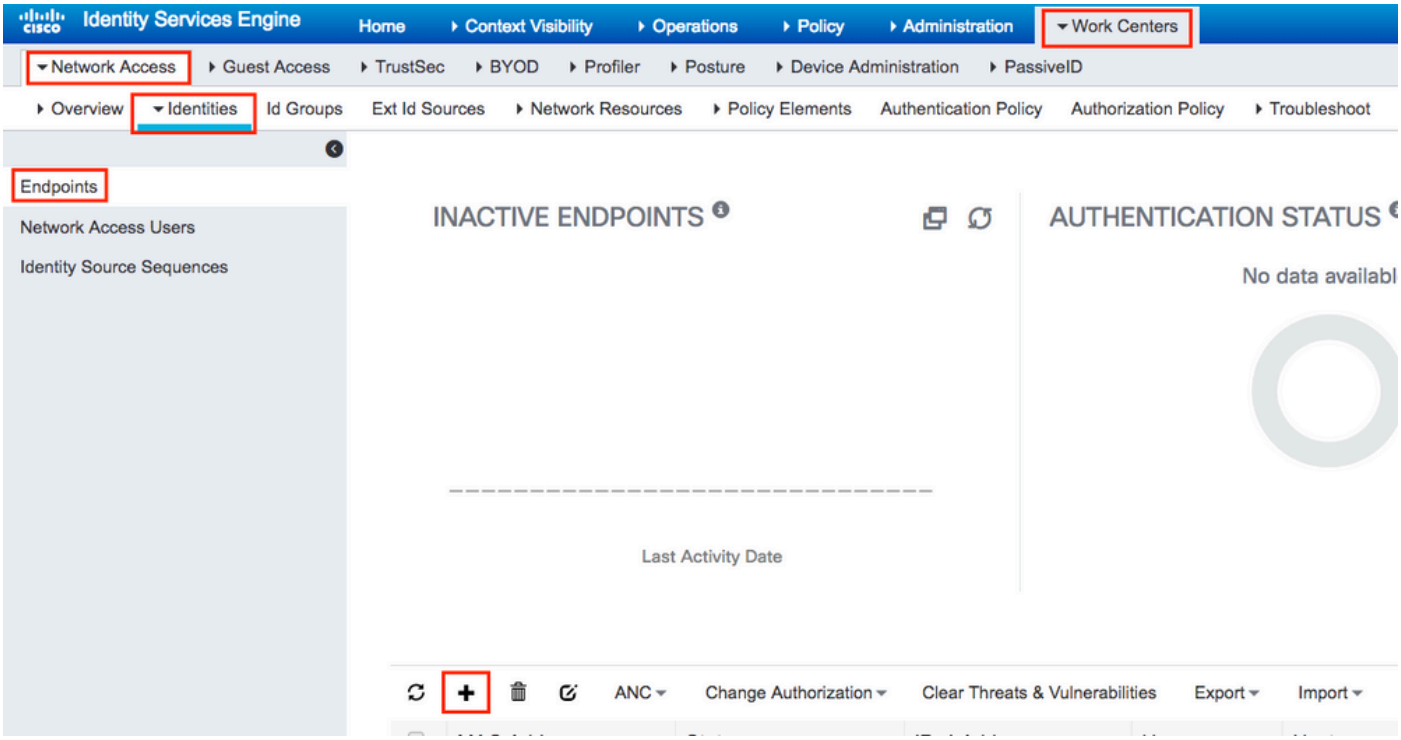
Geben Sie die MAC-Adresse in die ISE-Endpunktdatenbank ein.

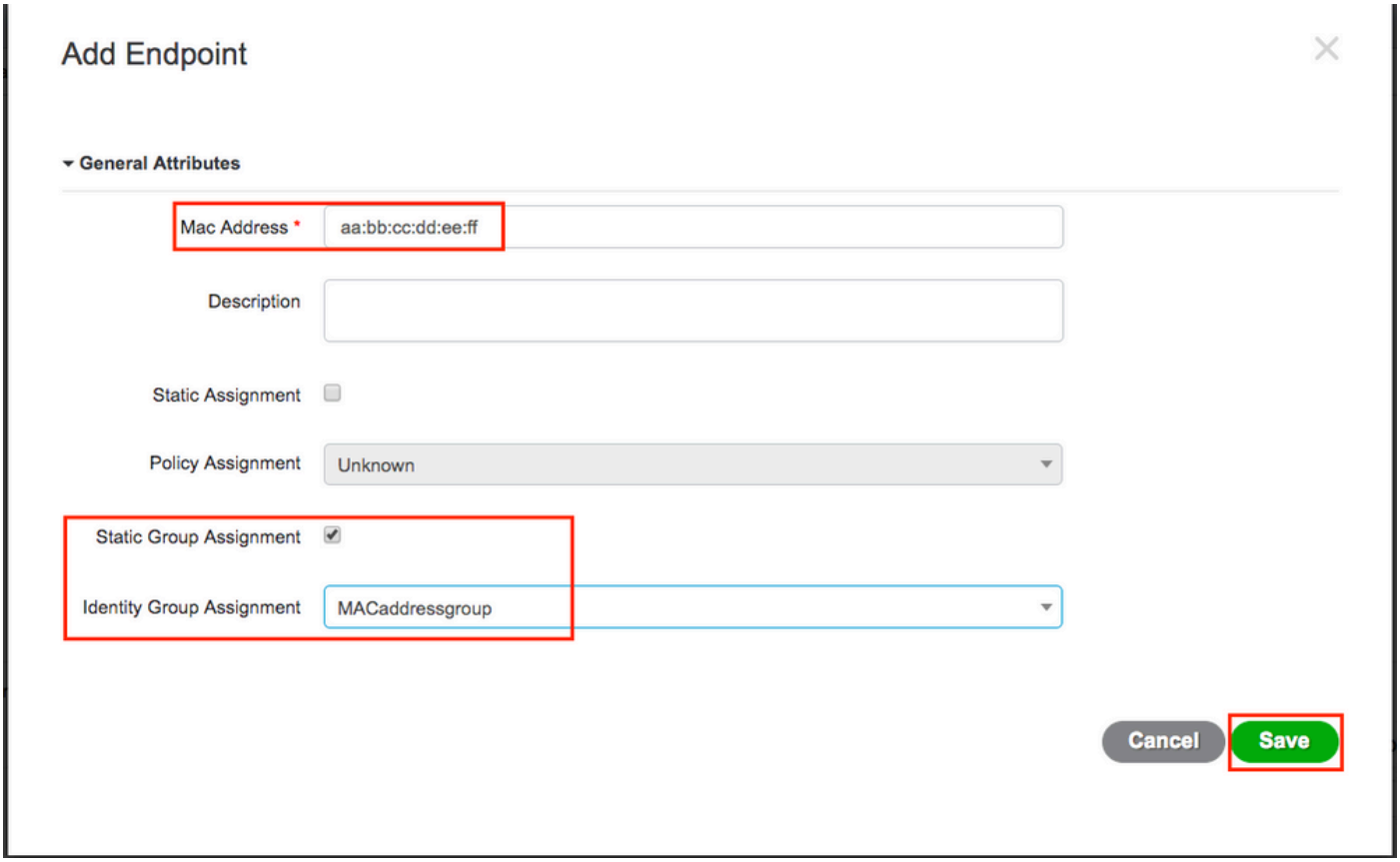
Schritt 1: (Optional) Erstellen Sie eine neue Endpunktgruppe.
Navigieren Sie zu Work Centers > Network Access > Id Groups > Endpoint Identity Groups > + Add.





Schritt 2: Navigieren Sie zu Work Centers > Network Access > Identities > Endpoints > +Add.





ISE-Konfiguration

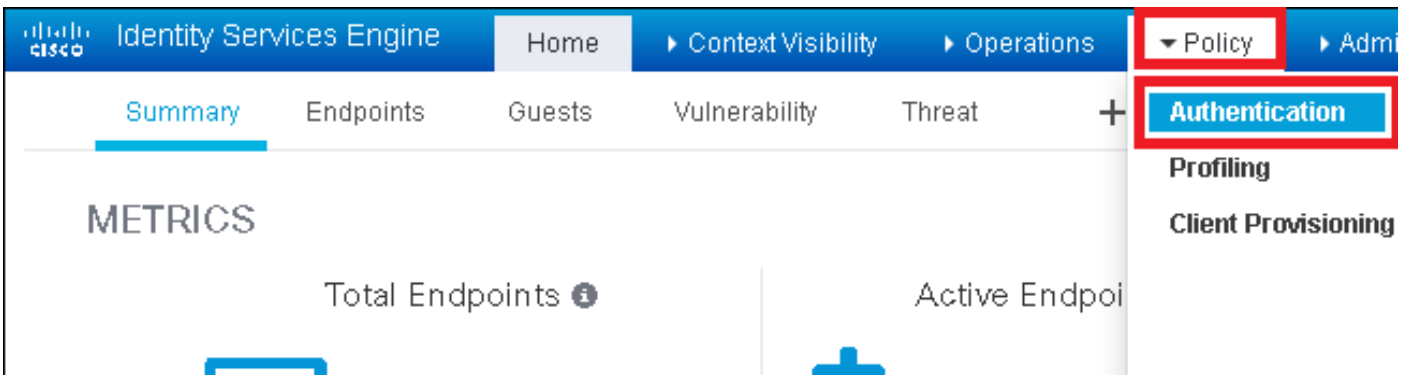
Hinzufügen von 9800 WLC zu ISE.

Lesen Sie die Anweisungen unter diesem Link: Declare WLC to ISE (WLC zur ISE erklären).

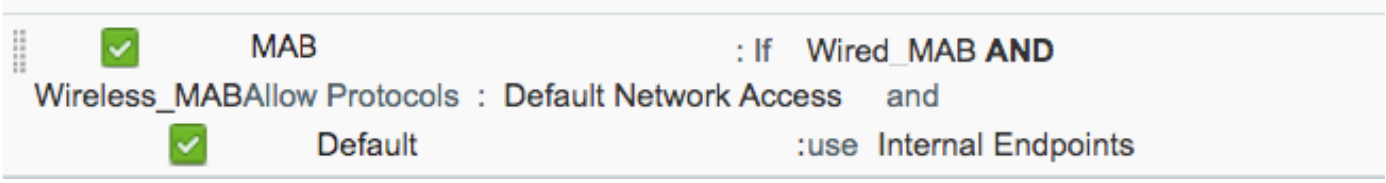
Erstellen einer Authentifizierungsregel

Authentifizierungsregeln werden verwendet, um zu überprüfen, ob die Anmeldeinformationen der Benutzer richtig sind (überprüfen Sie, ob der Benutzer wirklich der ist, für den er sich ausgibt), und um die Authentifizierungsmethoden einzuschränken, die von ihm verwendet werden dürfen.

Schritt 1: Navigieren Sie zu Policy > Authentication wie im Bild dargestellt.
Bestätigen Sie, dass die Standard-MAB-Regel auf Ihrer ISE vorhanden ist.



Schritt 2: Überprüfen Sie, ob die Standardauthentifizierungsregel für MAB bereits vorhanden ist:

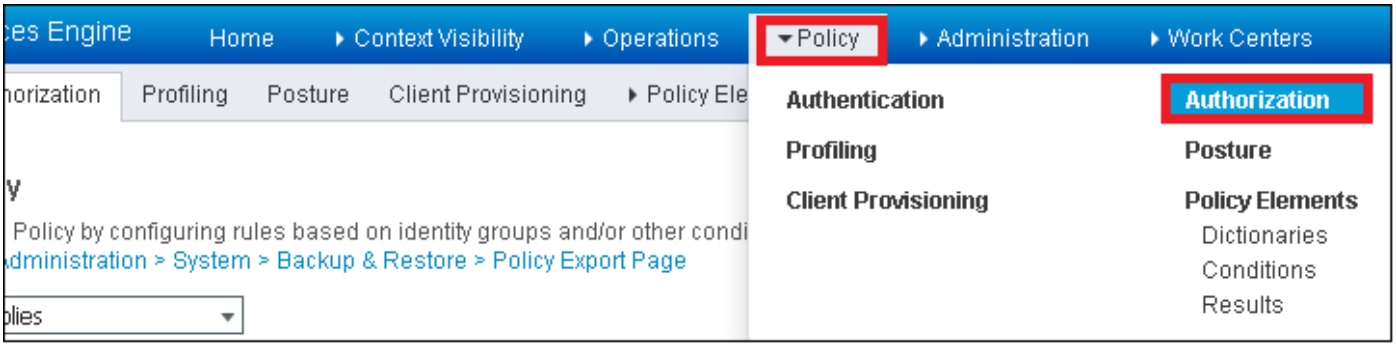


Wenn nicht, können Sie ein neues hinzufügen, indem Sie auf Insert new row above.

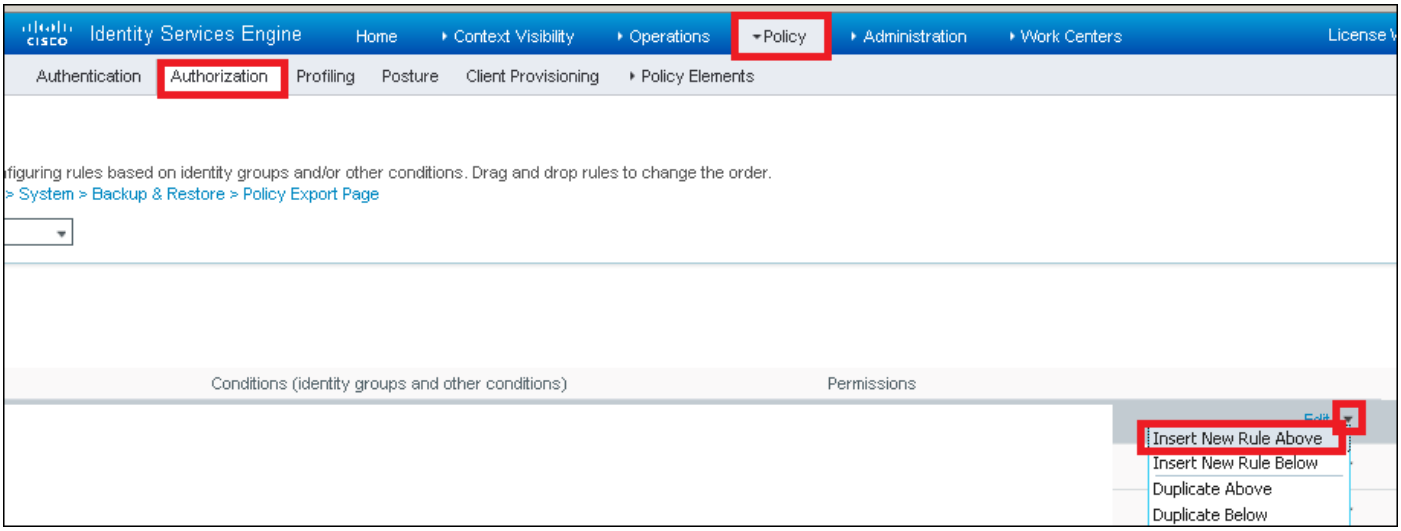
Erstellung von Autorisierungsregeln

Die Autorisierungsregel bestimmt, welche Berechtigungen (welches Autorisierungsprofil) auf den Client angewendet werden.

Schritt 1: Navigieren Sie zu Policy > Authorization wie im Bild dargestellt.

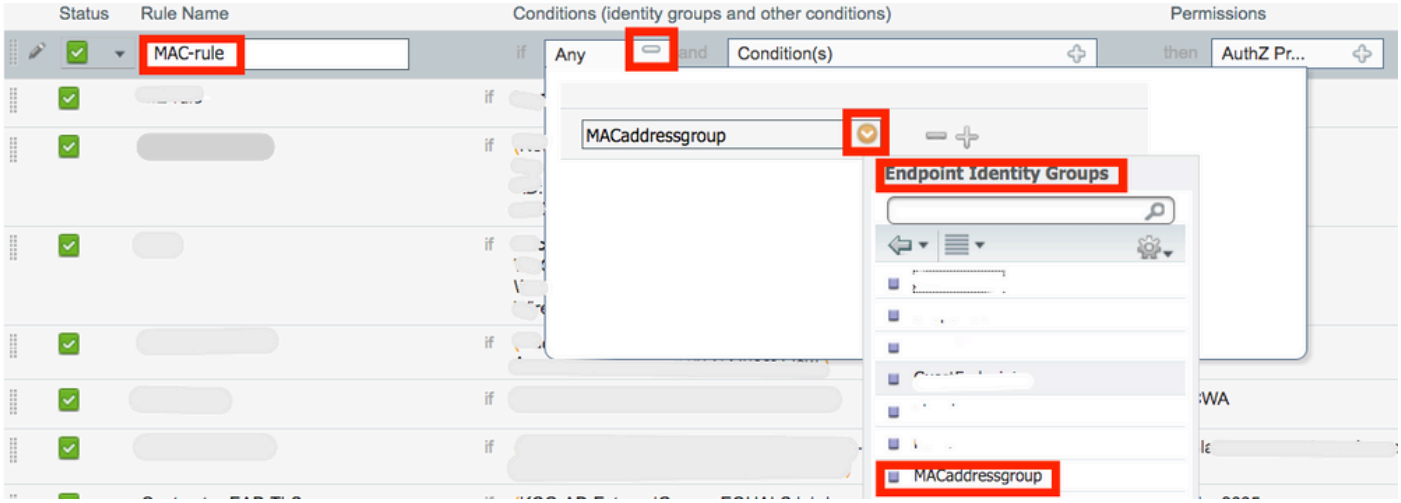


Schritt 2: Fügt eine neue Regel wie im Bild dargestellt ein.

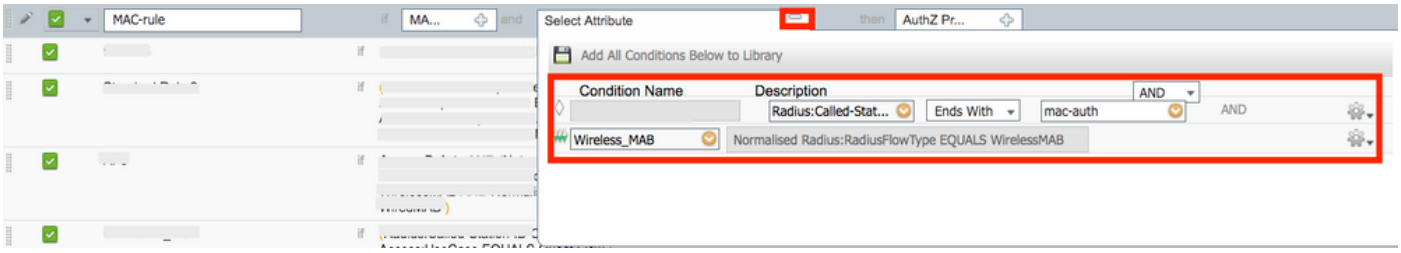


Schritt 3: Geben Sie die Werte ein.

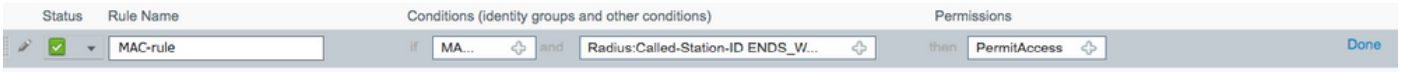
Wählen Sie zunächst einen Namen für die Regel und die Identitätsgruppe aus, in der der Endpunkt gespeichert ist (**MACaddressgroup**), wie im Bild dargestellt.



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 er Wireless-MAB verwendet, und seine angerufene Stations-ID (der Name der SSID) endet mit mac-auth wie im Bild dargestellt.



Wählen Sie abschließend das zugewiesene Autorisierungsprofil aus. In diesem Fall PermitAccess für die Clients, die diese Regel getroffen haben. Klicken Sie auf Done und speichere sie.



Überprüfung

Sie können diese Befehle verwenden, um die aktuelle Konfiguration zu überprüfen:

```
# show wlan { summary | id | name | all }
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Fehlerbehebung

Der WLC 9800 bietet IMMER-EIN-Ablaufverfolgungsfunktionen. So wird sichergestellt, dass alle verbindungsbezogenen Fehler, Warnungen und Benachrichtigungen auf Client-Ebene ständig protokolliert werden und Sie nach einem Vorfall oder Fehler Protokolle anzeigen können.

> **Hinweis**: Obwohl es von der Menge der generierten Protokolle abhängt, können Sie einige Stunden bis mehrere Tage zurückgehen.

Um die Traces anzuzeigen, die 9800 WLC standardmäßig gesammelt hat, können Sie sich über SSH/Telnet mit dem 9800 WLC verbinden und diese Schritte lesen (stellen Sie sicher, dass Sie die Sitzung in einer Textdatei protokollieren).

Schritt 1: Überprüfen Sie die aktuelle Zeit des Controllers, damit Sie die Protokolle von der Zeit bis zum Auftreten des Problems verfolgen können.

```
# show clock
```

Schritt 2: Erfassen Sie die Syslogs aus dem Controller-Puffer oder dem externen Syslog gemäß der Systemkonfiguration. Dadurch erhalten Sie eine Kurzübersicht über den Status und Fehler des Systems, sofern vorhanden.

```
# show logging
```

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

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

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

> **Hinweis:** Wenn eine Bedingung aufgeführt wird, bedeutet dies, dass die Ablaufverfolgungen für alle Prozesse, bei denen die aktivierten Bedingungen auftreten (MAC-Adresse, IP-Adresse usw.) protokolliert werden. Dadurch erhöht sich die Anzahl der Protokolle. Daher wird empfohlen, alle Bedingungen zu löschen, wenn gerade kein Debugging aktiv ist.

Schritt 4: Wenn die zu testende MAC-Adresse in Schritt 3. nicht als Bedingung aufgeführt wurde,

sammeln Sie die Nachverfolgungen auf permanenter Benachrichtigungsebene für die spezifische MAC-Adresse.

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

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 bereitstellen, um den Auslöser für das zu untersuchende Problem zu ermitteln, können Sie das bedingte 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). Lesen Sie diese Schritte, um das bedingte Debuggen zu aktivieren.

Schritt 5: Stellen Sie sicher, dass keine Debugbedingungen 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>}
```

> **Anmerkung:** Um mehrere Clients gleichzeitig zu überwachen, führen Sie debug wireless mac aus. -Befehl pro MAC-Adresse aus.

> **Hinweis**: Die Ausgabe der Client-Aktivität wird in der Terminal-Sitzung nicht angezeigt, 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>
```

Wenn die Überwachungszeit 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 die ra trace .log auf einen externen Server oder zeigen die Ausgabe direkt auf dem Bildschirm an.

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/ra-FILENAME.txt
```

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, sammeln Sie die internen Protokolle, die eine ausführlichere Ansicht der Protokolle auf Debugebene darstellen. Sie müssen den Client nicht noch einmal debuggen, da Sie sich nur noch ausführlicher mit Debug-Protokollen befassen, 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-internal-<FILENAME>.txt
```

> **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 Traces zu analysieren.

Sie können die ra-internal-FILENAME.txt auf einen externen Server oder zeigen die Ausgabe direkt auf dem Bildschirm an.

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.

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.