FlexConnect WLAN mit 802.1x AAA-Überschreibung auf Catalyst Wireless Controllern der Serie 9800

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie einen elastischen Wireless LAN-Controller (9800 WLC) mit FlexConnect-Modus-Access Points (APs) und ein lokal geswitchtes 802.1x Wireless Local Area Network (WLAN) mit Virtual Local Area Network (VLAN) Authentication, Authorization and Accounting (AAA) Override einrichten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- 9800 WLC-Konfigurationsmodus
- FlexConnect

Verwendete Komponenten

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

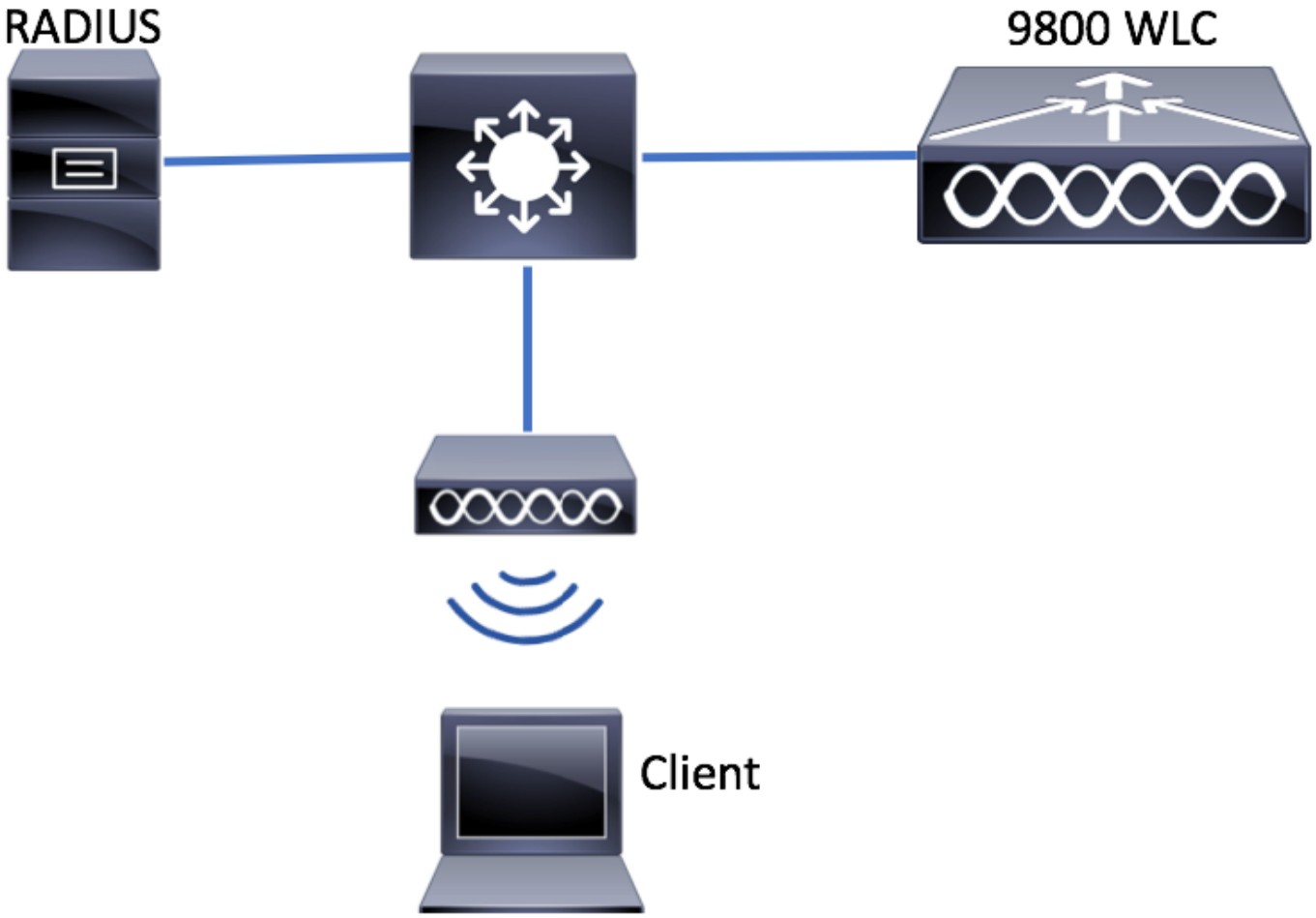
Hardwareversionen:

- 9800 WLC v16,10

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.

Konfigurieren

Netzwerkdiagramm



Konfiguration

AAA-Konfiguration auf dem 9800 WLC

Sie können die Anweisungen unter folgendem Link befolgen:

AAA-Konfiguration auf dem 9800 WLC

WLAN-Konfiguration

Sie können die Anweisungen unter folgendem Link befolgen:

[WLAN-Konfiguration]

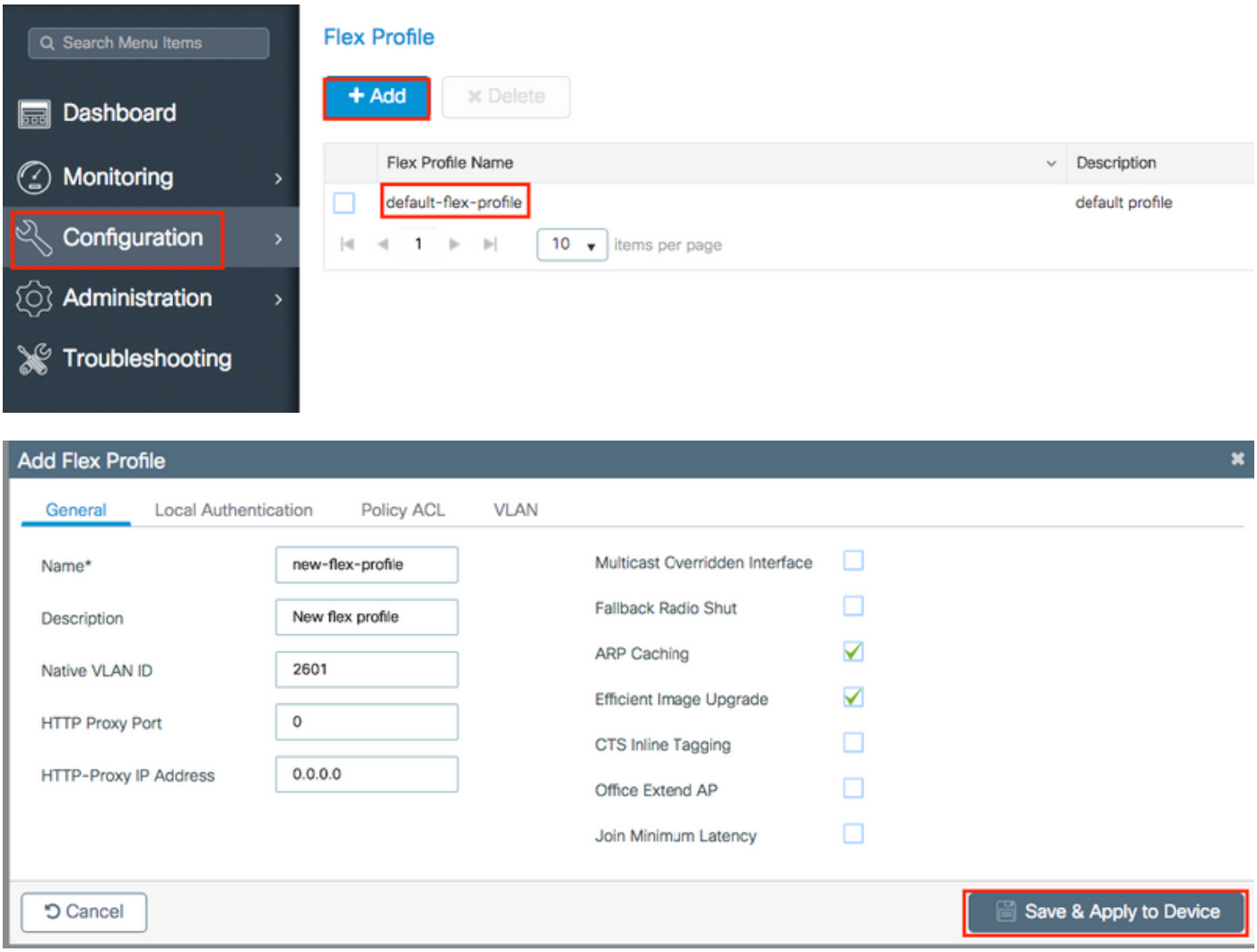
Festlegen von APs als FlexConnect-Modus

Anders als bei der AireOS-Konfiguration ist es auf dem 9800 WLC nicht möglich, den lokalen Access Point- oder Flexconnect-Modus direkt vom Access Point aus zu konfigurieren. Befolgen Sie diese Schritte, um einen Access Point im FlexConnect-Modus zu konfigurieren.

Benutzeroberfläche

Schritt 1: Konfigurieren eines Flex-Profils

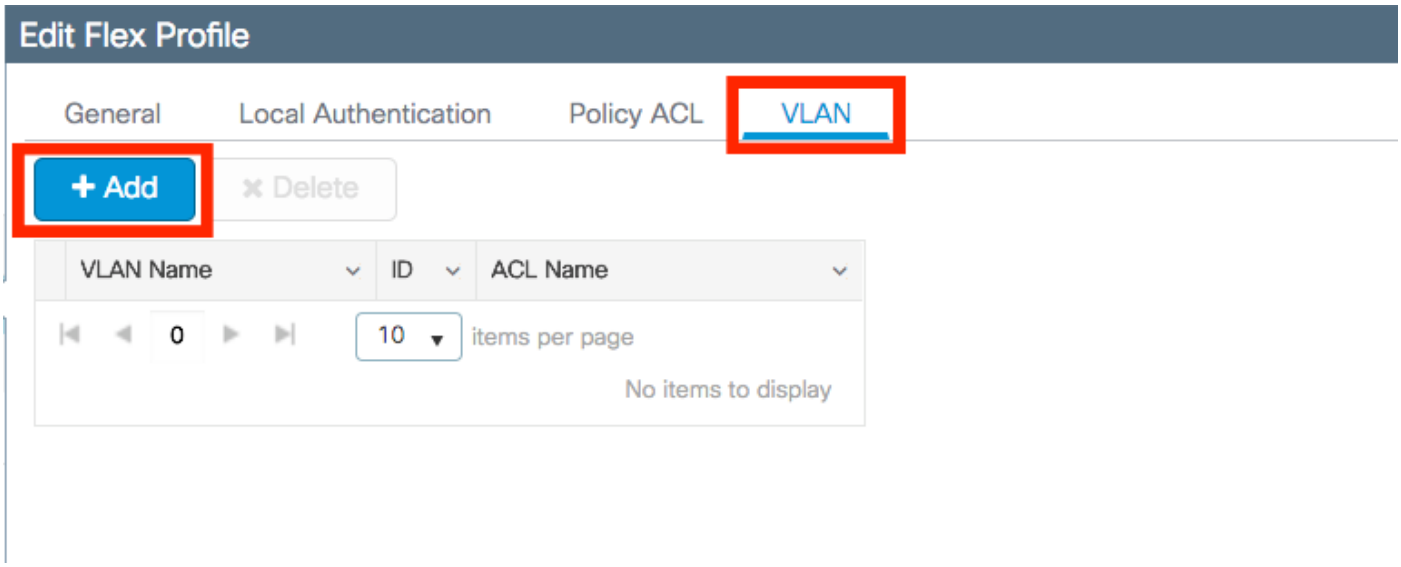
Navigieren zu **Konfiguration > Tags & Profile > Flex** und ändern Sie entweder das **default-flex-Profil** oder klicken Sie auf **+Add**, um ein neues Profil zu erstellen.



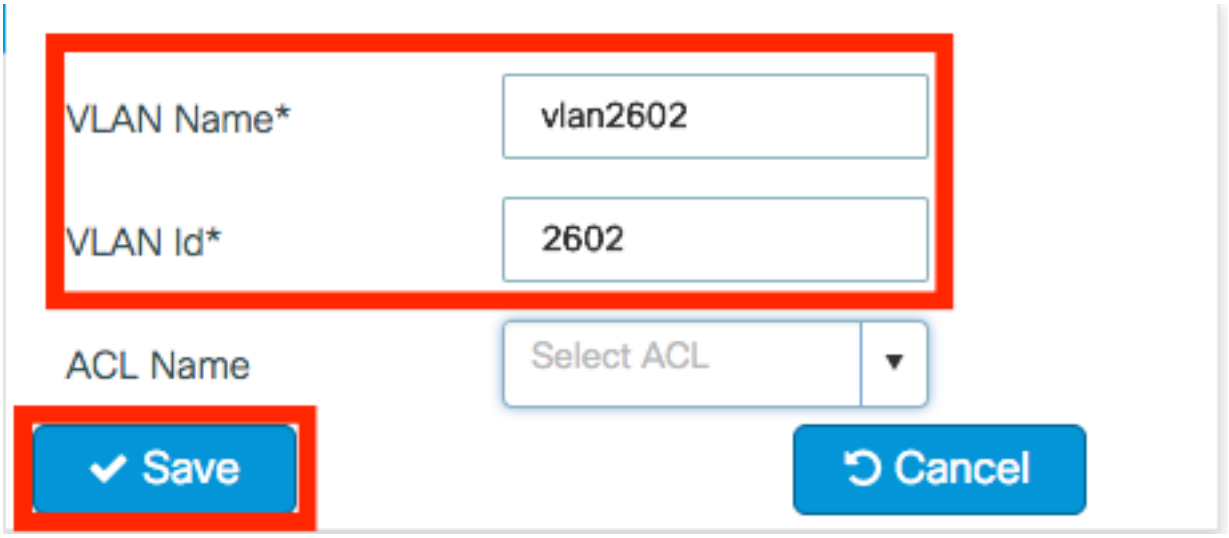
Schritt 2: Fügen Sie die erforderlichen VLANs hinzu (sowohl die Standard-WLANs als auch die von der ISE gesendeten VLANs).

> **Hinweis**: In Schritt 3 des Abschnitts **"Policy Profile Configuration"** wählen Sie das Standard-VLAN aus, das der SSID zugewiesen wurde. Wenn Sie in diesem Schritt einen VLAN-Namen verwenden, stellen Sie sicher, dass Sie in der Flex Profile-Konfiguration den gleichen VLAN-Namen verwenden. Andernfalls können Clients keine Verbindung zum

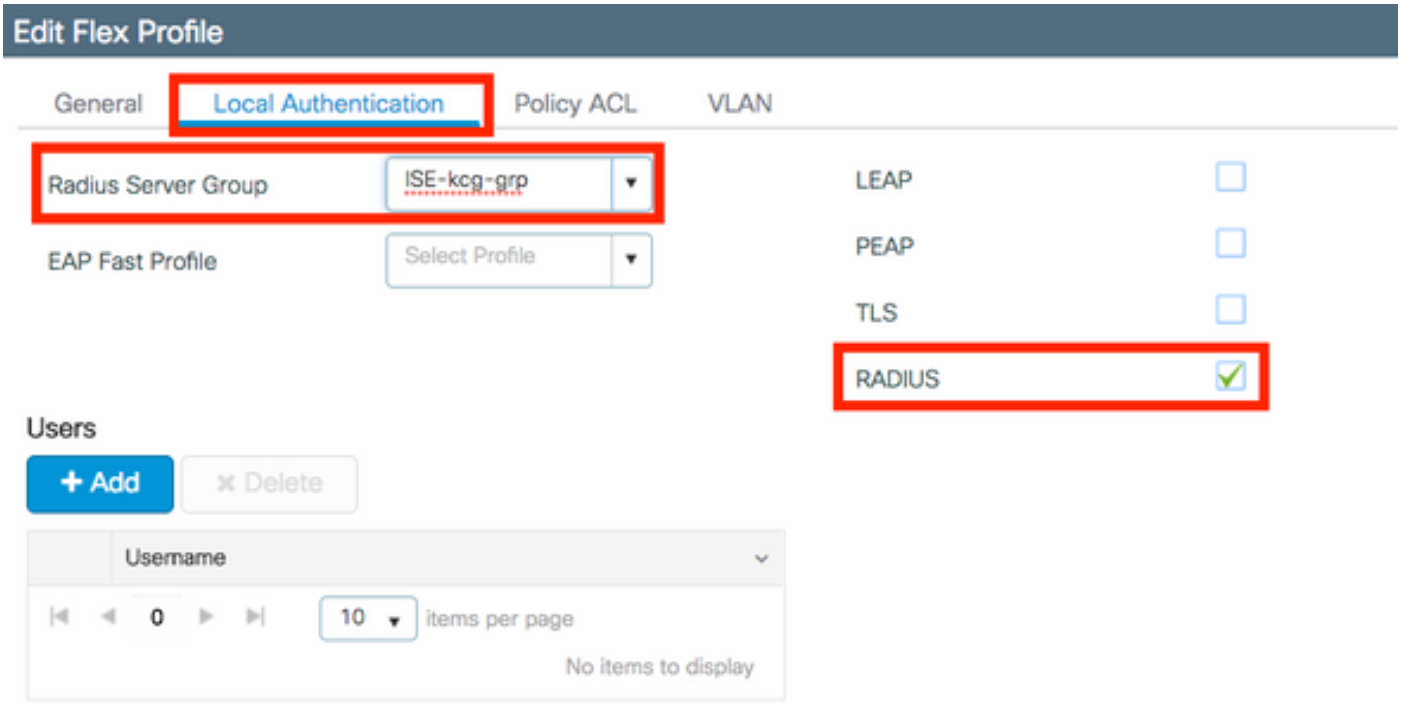
WLAN herstellen.



Sie können optional spezifische ACLs pro VLAN hinzufügen.

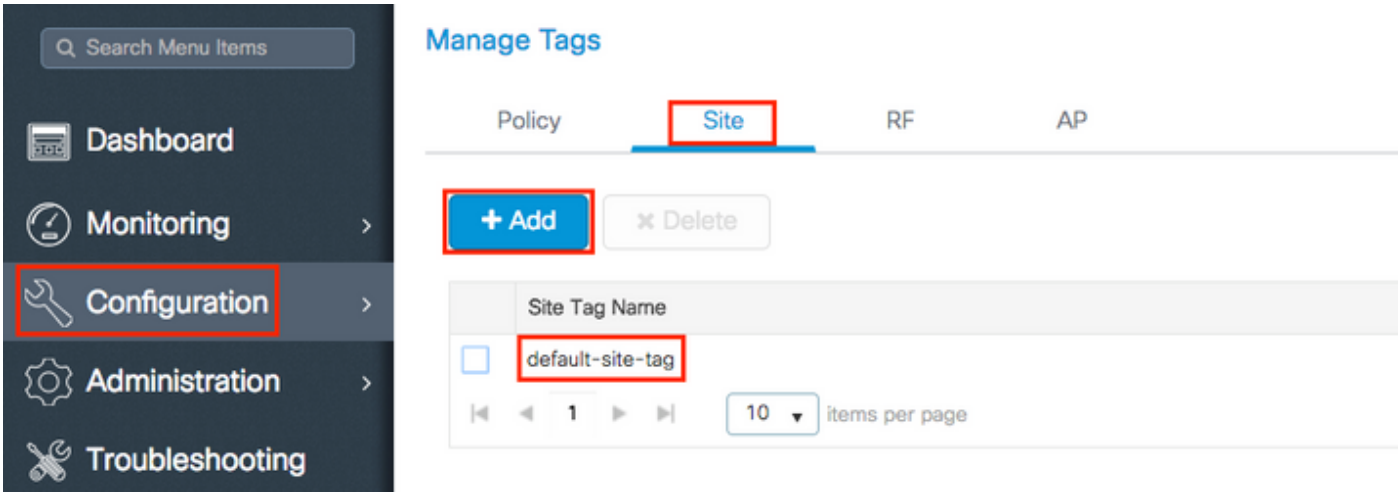


Weisen Sie optional eine Radius-Servergruppe zu, damit die FlexConnect-APs eine lokale Authentifizierung durchführen können.



Schritt 3: Konfigurieren einer Site-Tag-Nummer

Navigieren Sie zu **Konfiguration > Tags & Profile > Tags > Site.** Ändern Sie entweder das **Standard-Site-Tag** (das Tag, das standardmäßig allen APs zugewiesen ist), oder erstellen Sie ein neues Tag (Klicken **+Hinzufügen**, um ein neues zu erstellen).

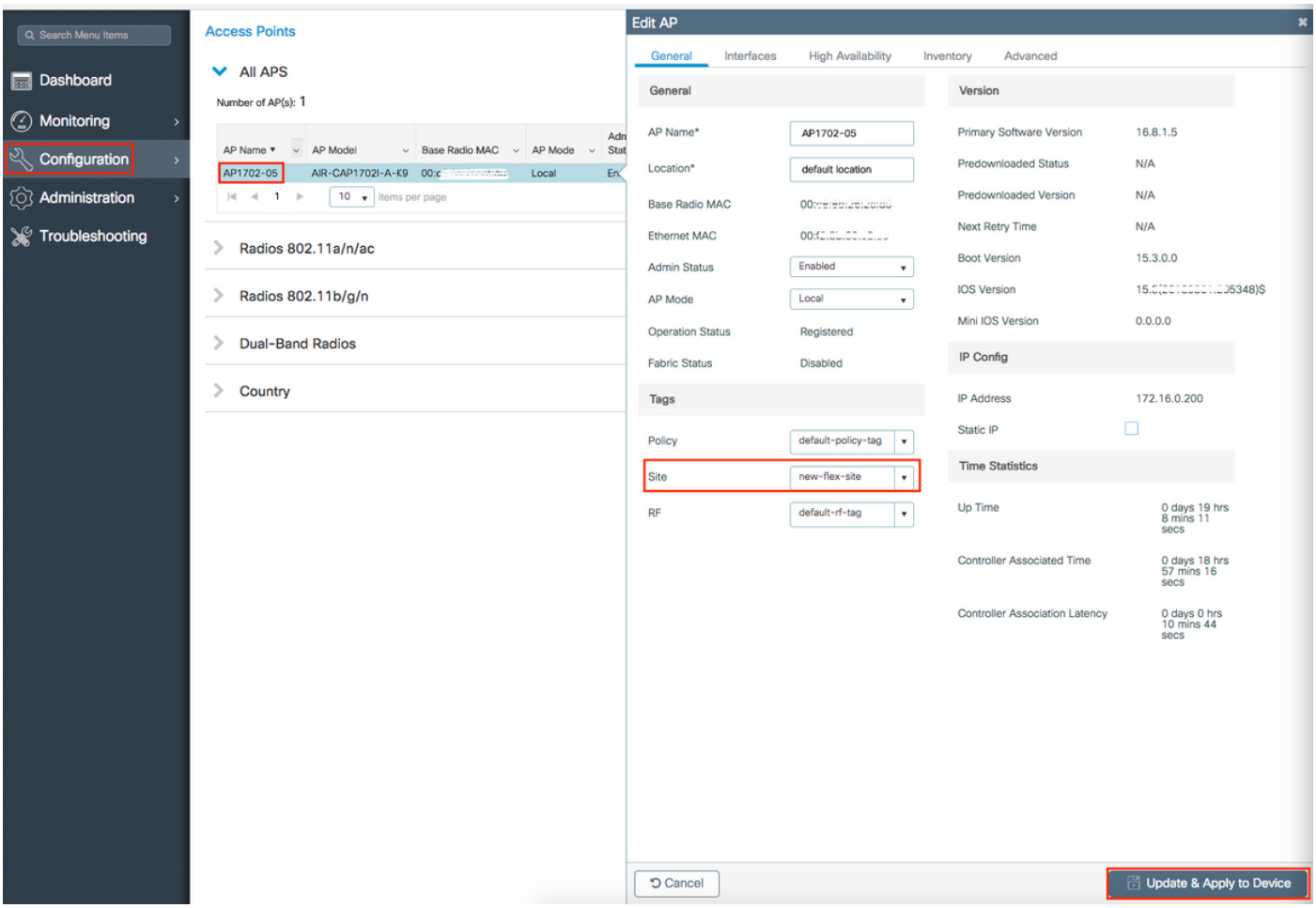


Stellen Sie sicher, dass Sie die Option **Lokalen Standort aktivieren** deaktivieren, da die Option **Flex Profile** nicht verfügbar ist.

Hinweis: Jeder Access Point, der eine Site-Tag-Nummer erhält, bei der **Lokalen Standort aktivieren** aktiviert ist, wird als lokaler Modus konfiguriert. Ebenso wird jeder Access Point, der eine Site-Tag-Nummer erhält, bei der die **lokale Site aktivieren** deaktiviert ist, als Flexconnect-Modus konfiguriert.

Schritt 4: Legen Sie eine AP-Zuordnung zum 9800 WLC fest, und weisen Sie das in Schritt 2 konfigurierte Site-Tag zu.

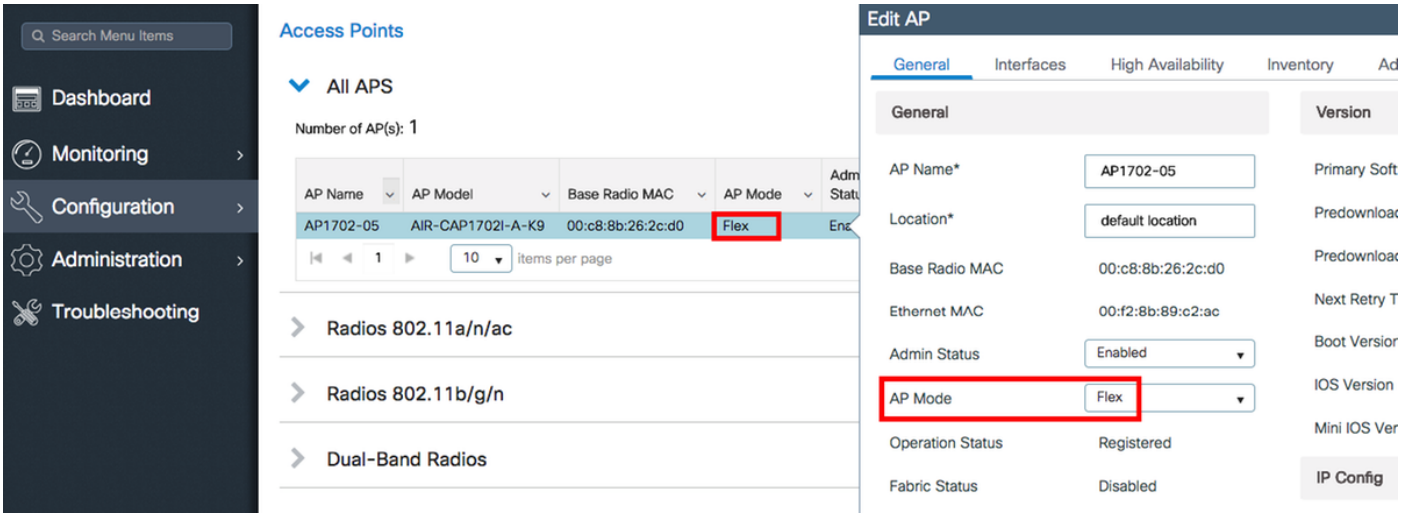
Navigieren Sie zu **Configuration > Wireless > Access Points > AP name,** und legen Sie die Site-Tag-Nummer fest. Klicken Sie anschließend auf **Aktualisieren und auf Gerät anwenden**, um die Änderung festzulegen.



Hinweis: Beachten Sie, dass nach dem Ändern des Tags auf einem Access Point die

Verknüpfung zum 9800 WLC verloren geht und sich innerhalb von etwa einer Minute wieder anmeldet.

Schritt 5: Sobald der Access Point wieder zurück ist, stellen Sie fest, dass der AP-Modus "Flex" ist.



CLI

```
# config t
# wireless profile flex new-flex-profile
# arp-caching
# description "New flex profile"
# native-vlan-id 2601

# config t
# wireless tag site new-flex-site
# flex-profile new-flex-profile
# no local-site
# site-tag new-flex-site

# config t
# ap <eth-mac-address>
# site-tag new-flex-site
Associating site-tag will cause associated AP to reconnect
# exit

#show ap name <ap-name> config general | inc AP Mode
AP Mode                                         : FlexConnect
```

Switch-Konfiguration

Konfigurieren Sie die Switch-Schnittstelle, mit der der Access Point verbunden ist.

```
# config t
# interface <int-id>
# switchport trunk native vlan 2601
# switchport mode trunk
# spanning-tree portfast trunk
# end
```

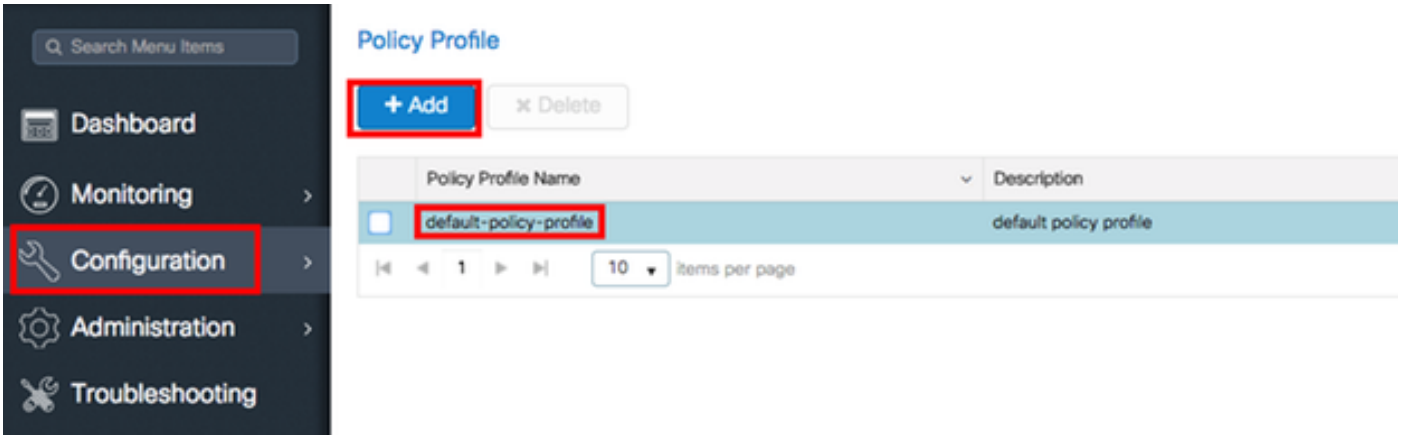
Richtlinienprofil-Konfiguration

In einem Richtlinienprofil können Sie festlegen, welches VLAN die Clients zuweist, unter anderem Einstellungen (z. B. Zugriffssteuerungsliste [ACLs], Quality of Service [QoS], Mobility Anchor, Timer usw.).

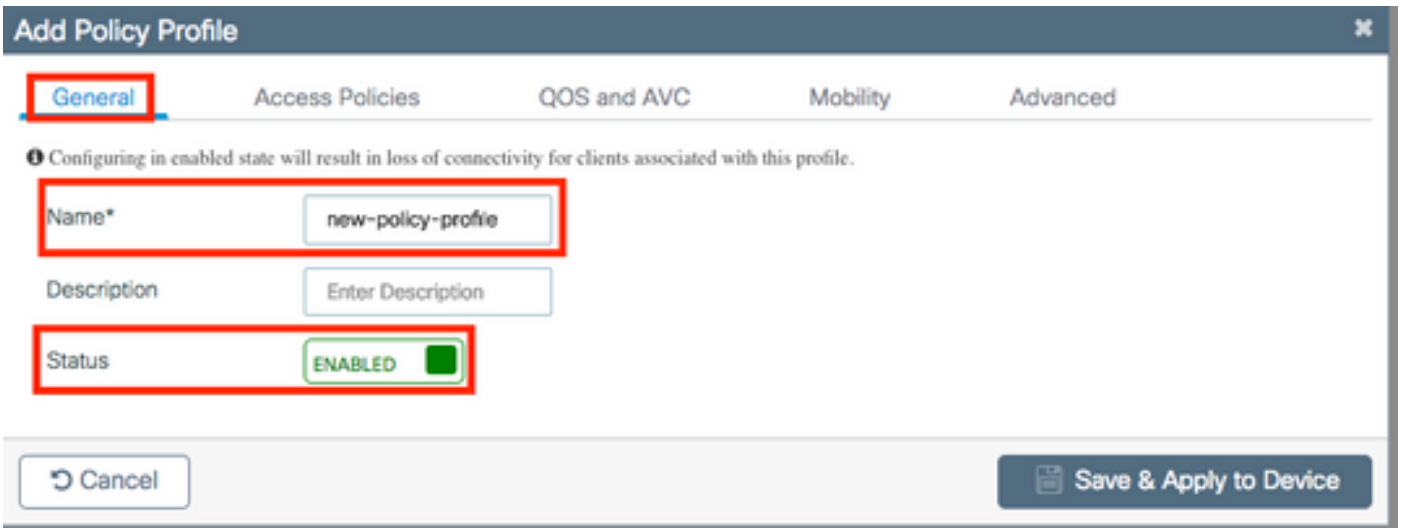
Benutzeroberfläche

Schritt 1: Konfigurieren Sie das Richtlinienprofil, das dem WLAN zugewiesen werden soll.

Navigieren Sie zu **Configuration > Tags & Profiles > Policy,** und erstellen Sie entweder eine neue oder ändern Sie das **Standardrichtlinienprofil.**



Schritt 2: Weisen Sie dem Richtlinienprofil auf der **Registerkarte Allgemein** einen Namen zu**,** und ändern Sie seinen Status in **ENABLED.**

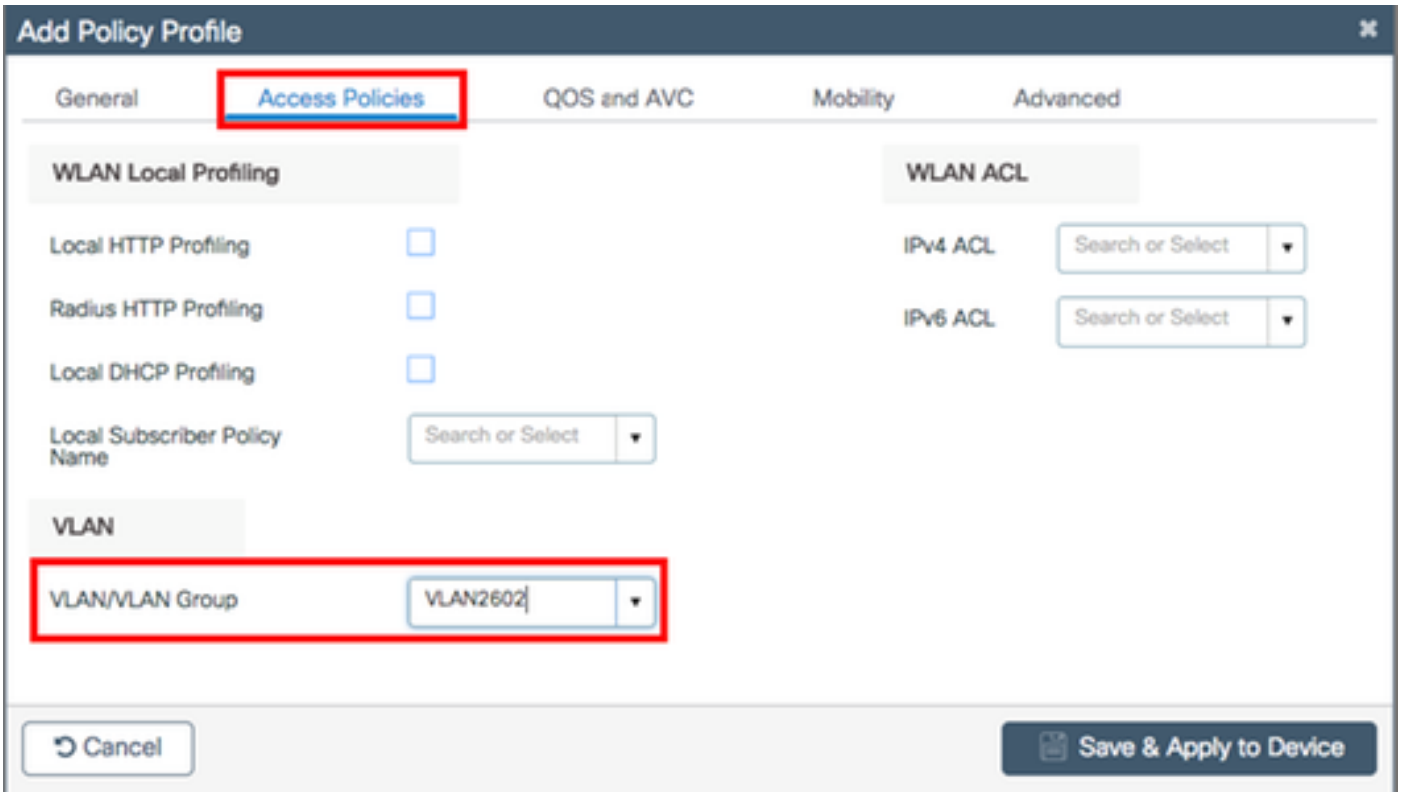


Schritt 3: Weisen Sie auf der Registerkarte **Access Policies (Zugriffsrichtlinien**) das VLAN zu, dem die Wireless-Clients zugewiesen sind, wenn sie standardmäßig eine Verbindung zu diesem WLAN herstellen.

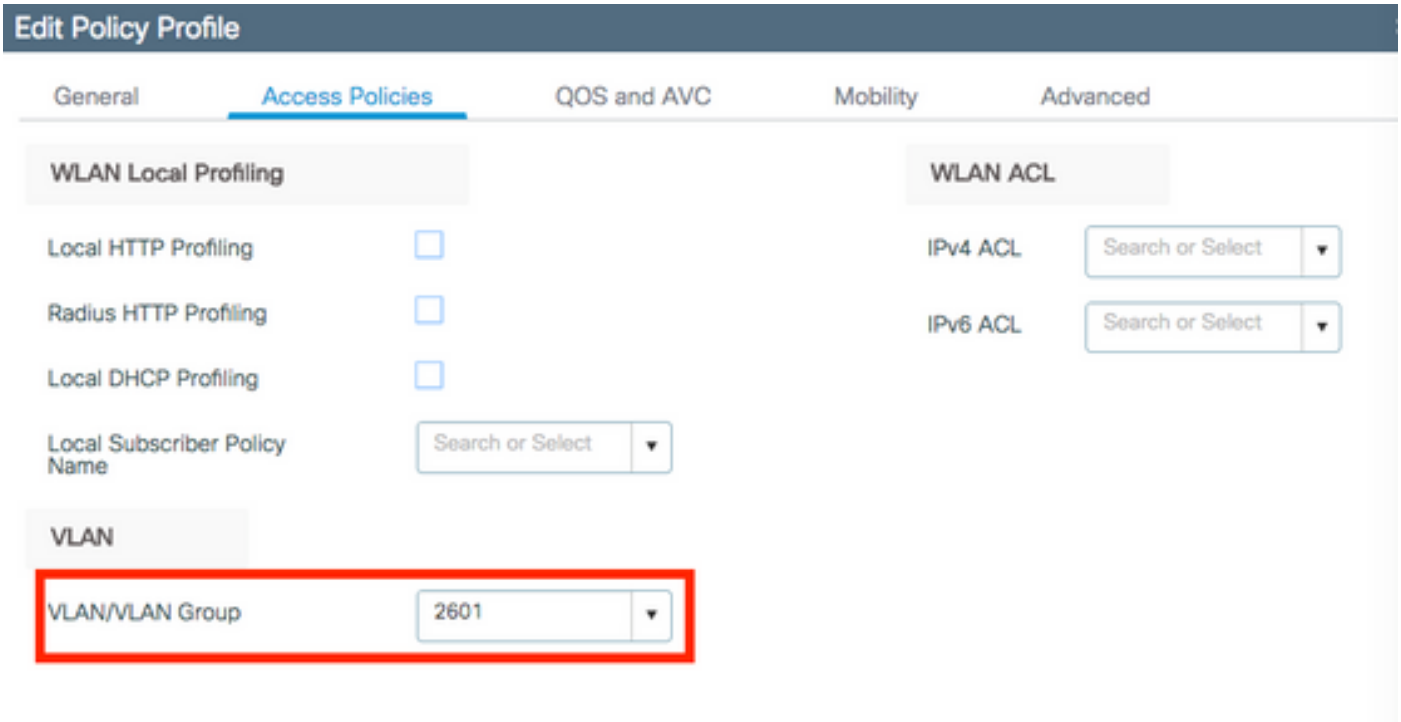
Sie können entweder einen VLAN-Namen aus dem Dropdown-Menü auswählen oder eine VLAN-ID manuell eingeben.

Hinweis: Wenn Sie einen VLAN-Namen aus dem Dropdown-Menü auswählen, müssen Sie

sicherstellen, dass dieser dem VLAN-Namen entspricht, der in Schritt 2 aus Abschnitt **AP als FlexConnect-Modus festlegen** wird.

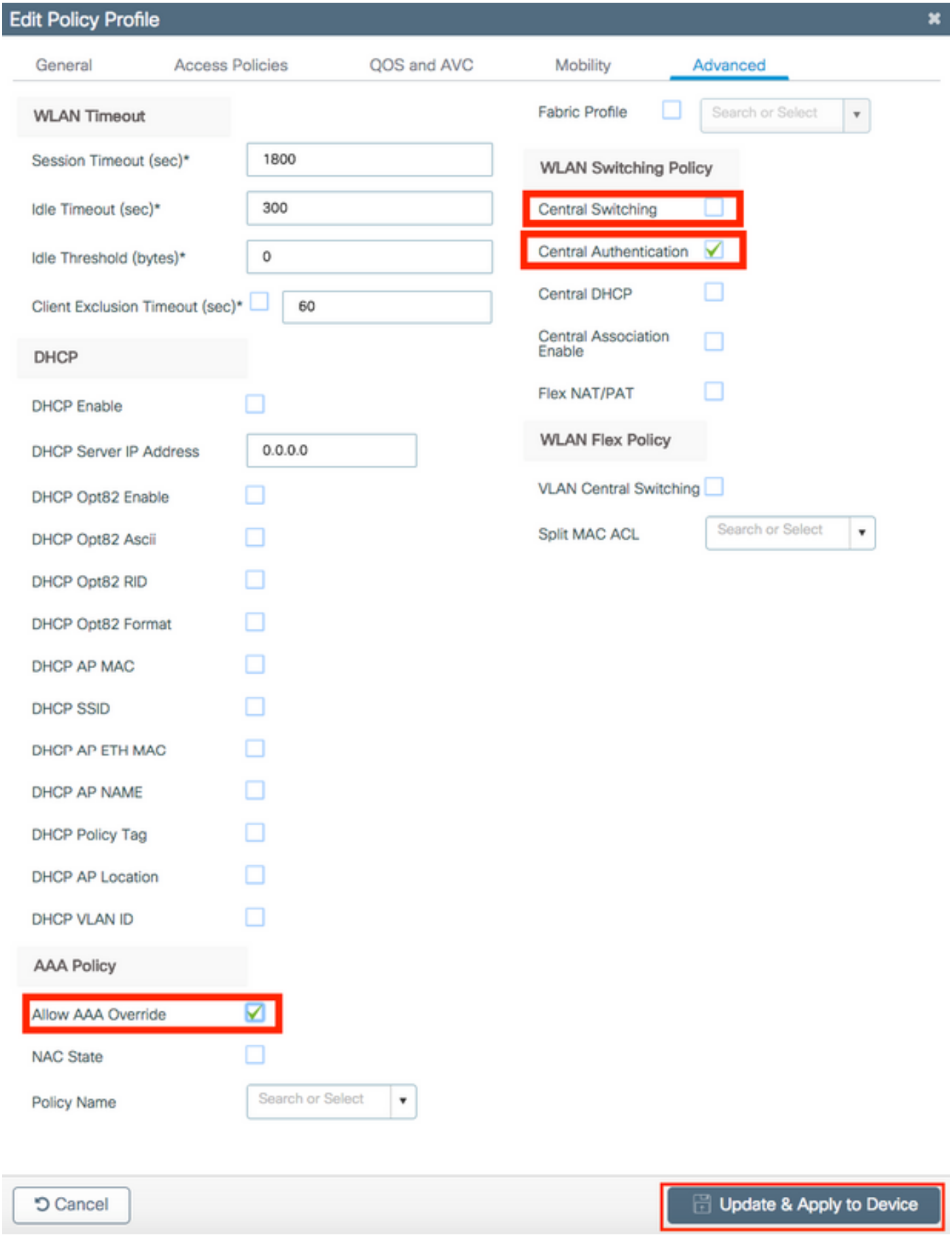


oder



Schritt 4: Navigieren Sie zur **Registerkarte Erweitert**, und aktivieren Sie die **Option Zentrale Authentifizierung aktivieren** und **AAA-**Überschreibungsoptionen **zulassen. Central Switching** muss deaktiviert werden.

Zentrale Authentifizierung muss aktiviert werden, wenn der Authentifizierungsprozess zentral vom 9800 WLC ausgeführt werden soll. Deaktivieren Sie die Funktion, wenn die FlexConnect-APs die Wireless-Clients authentifizieren möchten.



CLI

```
# config t
# wireless profile policy new-policy-profile # central association # vlan <vlan-id or vlan-name>
```

```
# no shutdown
```

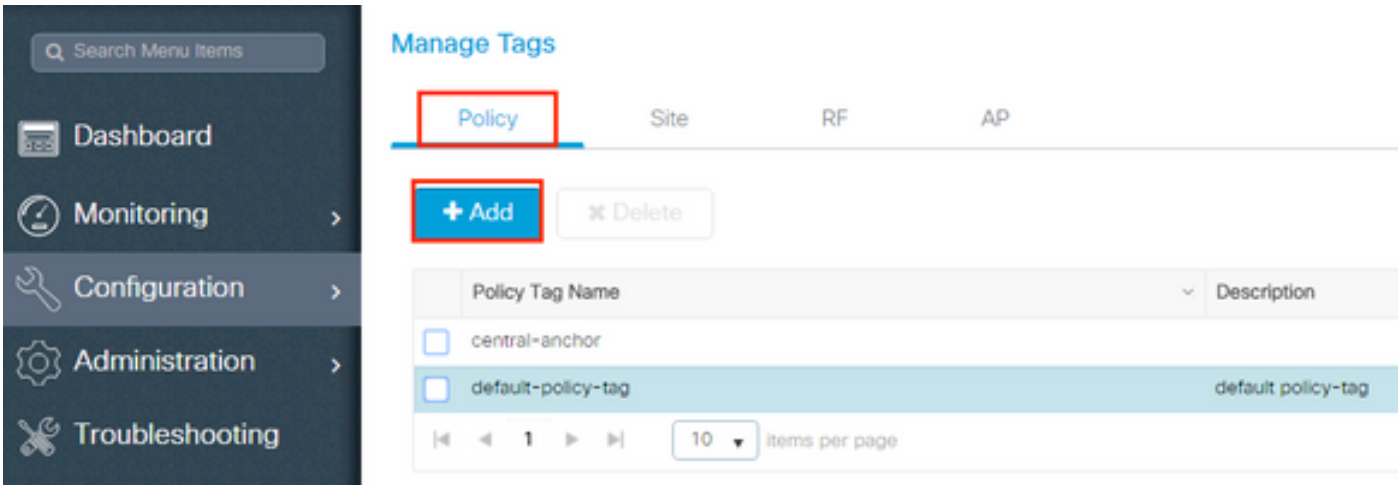
Richtlinien-Tag-Konfiguration

Policy-Tag wird verwendet, um die SSID mit dem Richtlinienprofil zu verknüpfen. Sie können entweder eine neue Policy-Tag-Nummer erstellen oder das Standard-Policy-Tag verwenden.

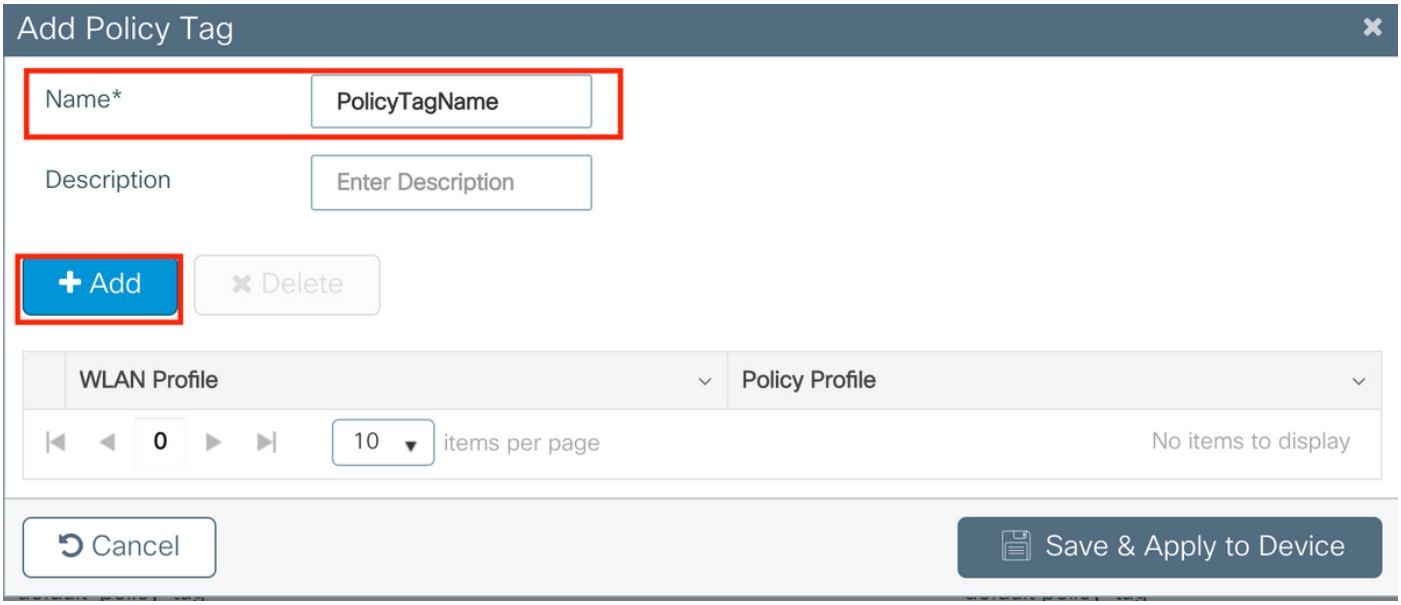
> **Hinweis**: Das Standard-Policy-Tag ordnet alle SSID mit einer WLAN-ID zwischen 1 und 16 automatisch dem Standard-Richtlinienprofil zu. Sie kann weder geändert noch gelöscht werden. Wenn Sie ein WLAN mit der ID 17 oder höher haben, kann das Standard-Policy-Tag nicht verwendet werden.

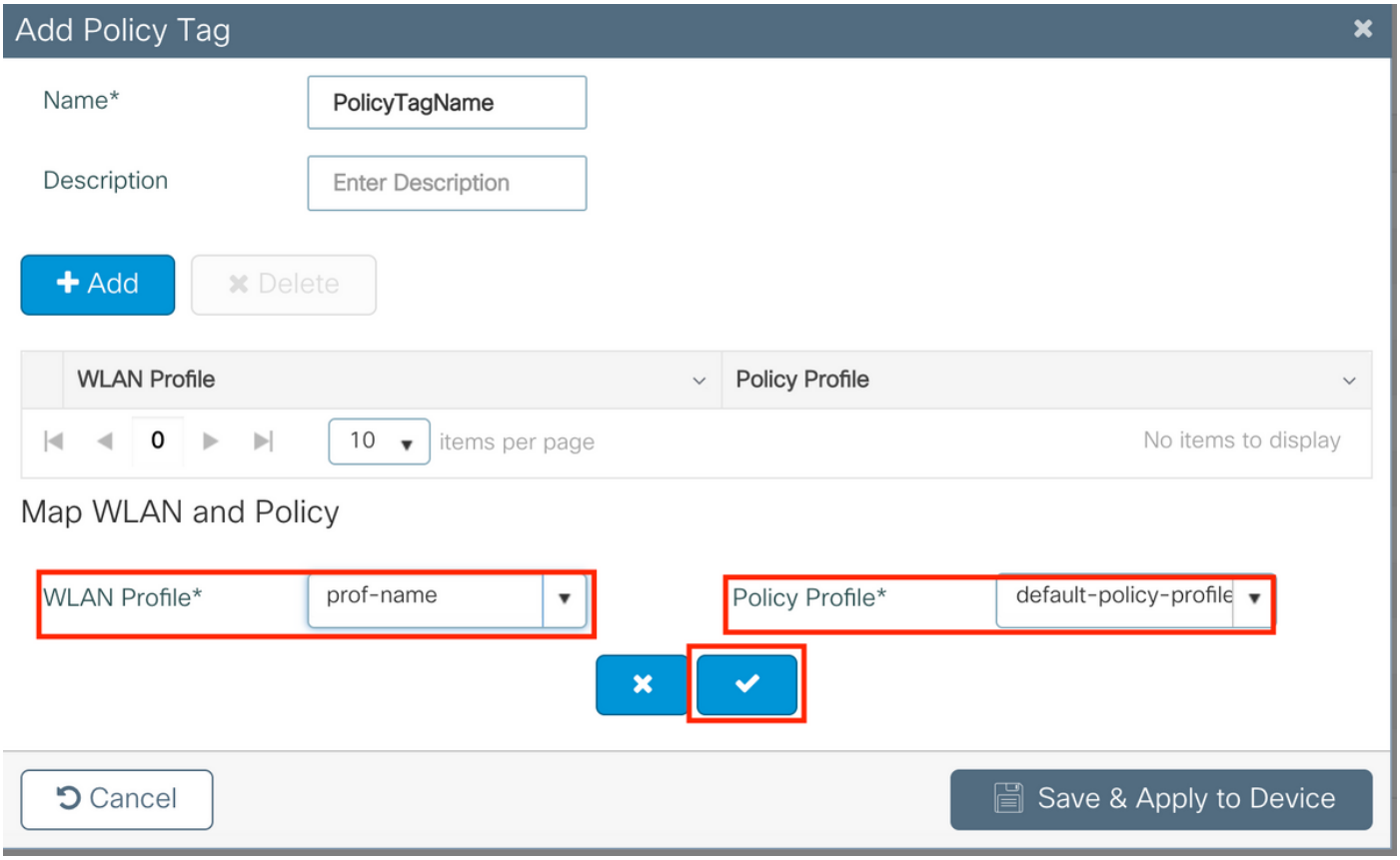
Benutzeroberfläche:

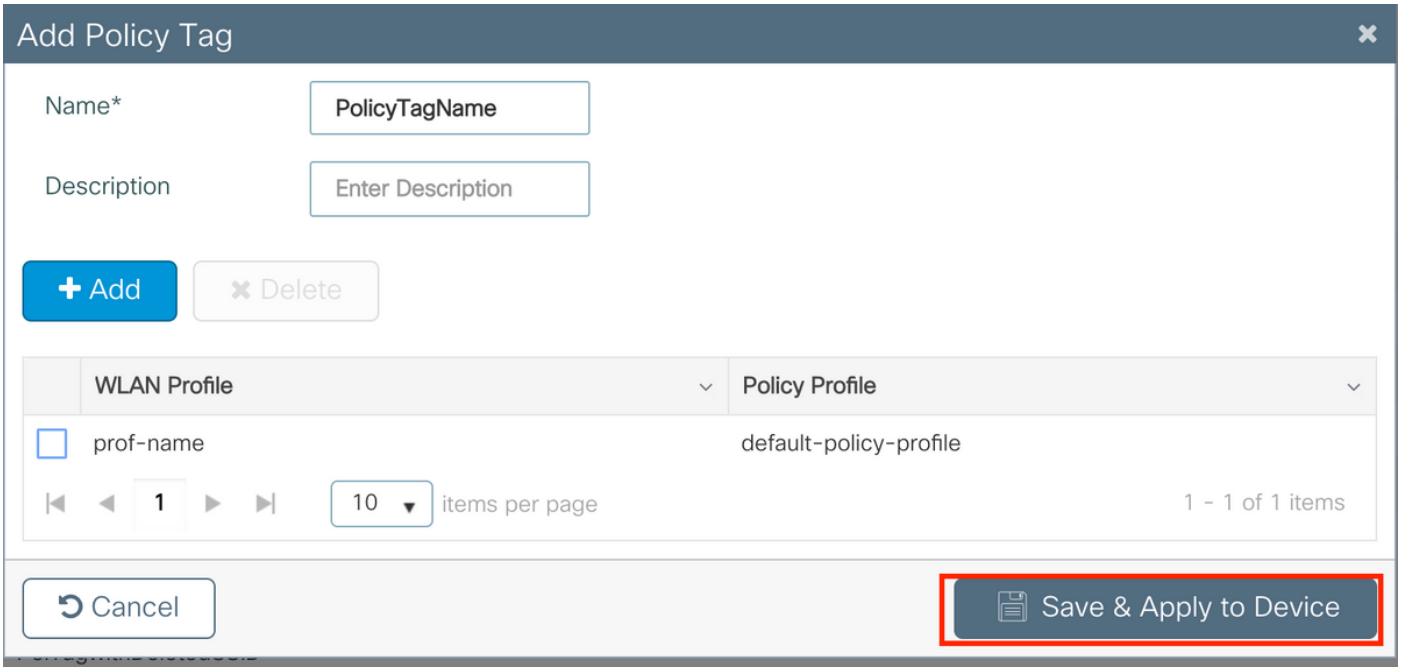
Navigieren Sie zu **Konfiguration > Tags & Profile > Tags > Richtlinien,** und fügen Sie bei Bedarf eine neue hinzu.



Verknüpfen Sie Ihr WLAN-Profil mit dem gewünschten Richtlinienprofil.







CLI:

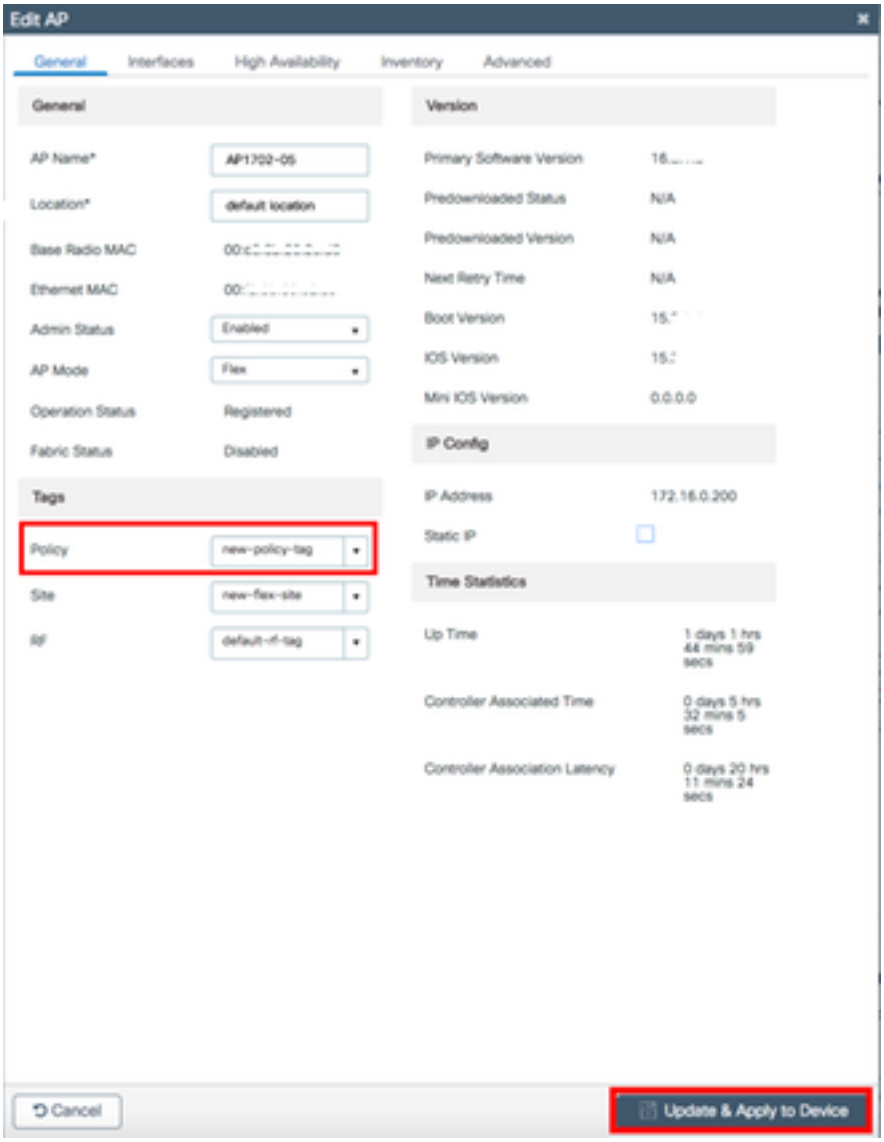
```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

Zuweisung von Richtlinien-Tags

Zuweisen des Policy-Tags zum AP

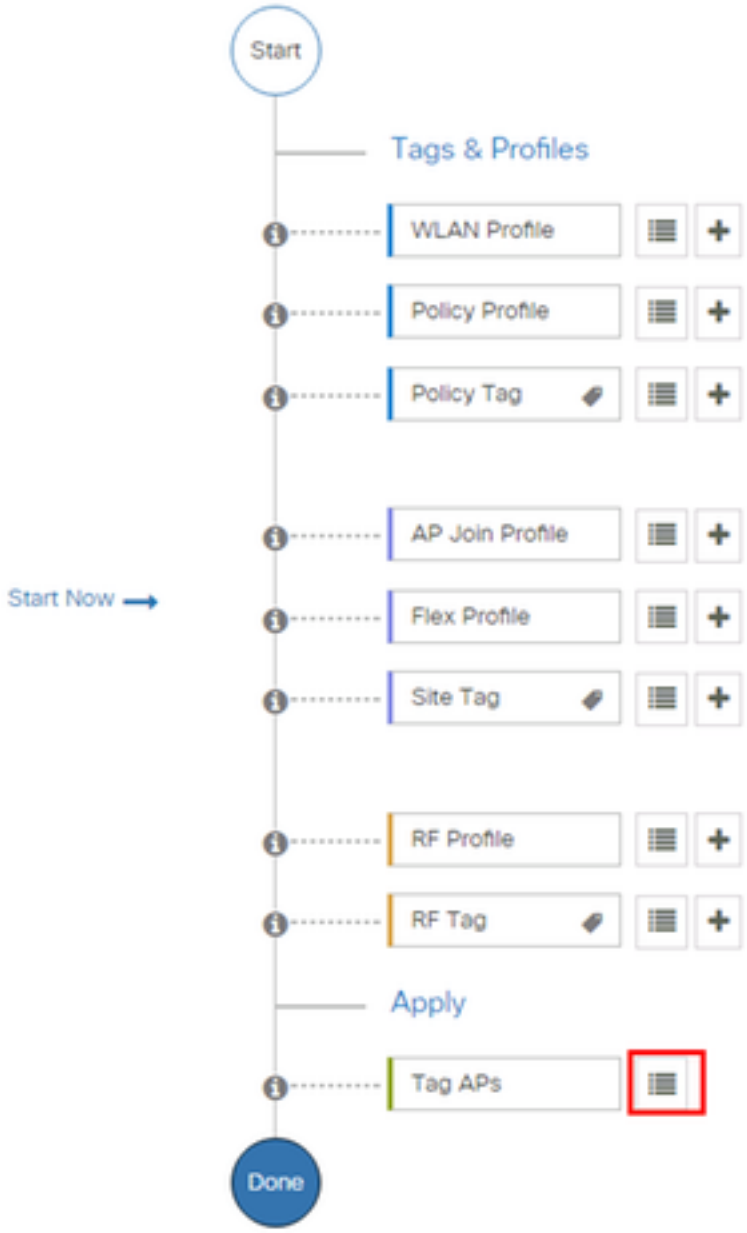
Benutzeroberfläche

Um das Tag einem Access Point zuzuweisen, navigieren Sie zu **Configuration > Wireless > Access Points > AP Name > General Tags,** nehmen Sie die gewünschte Zuordnung vor und klicken Sie dann auf **Update & Apply to Device (Aktualisieren und auf Gerät anwenden).**

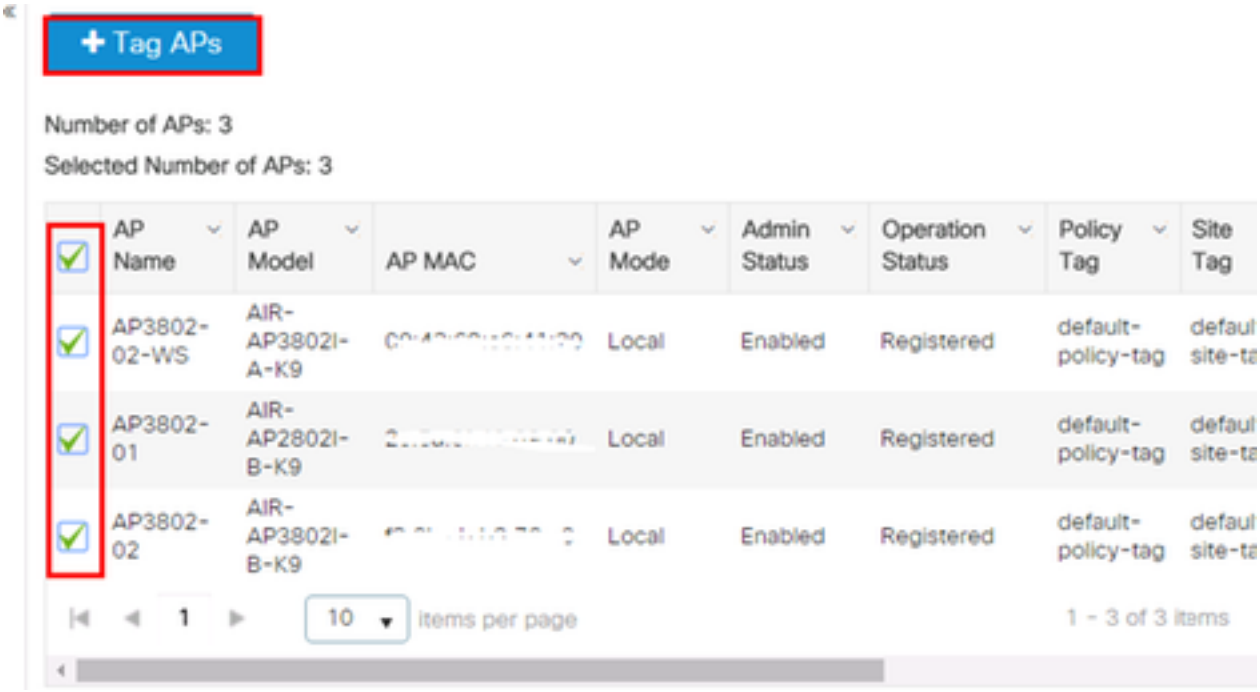


> **Hinweis**: Beachten Sie, dass nach dem Ändern des Richtlinien-Tags eines Access Points die Verbindung zum 9800-WLC unterbrochen und innerhalb von etwa einer Minute wieder aufgenommen wird.

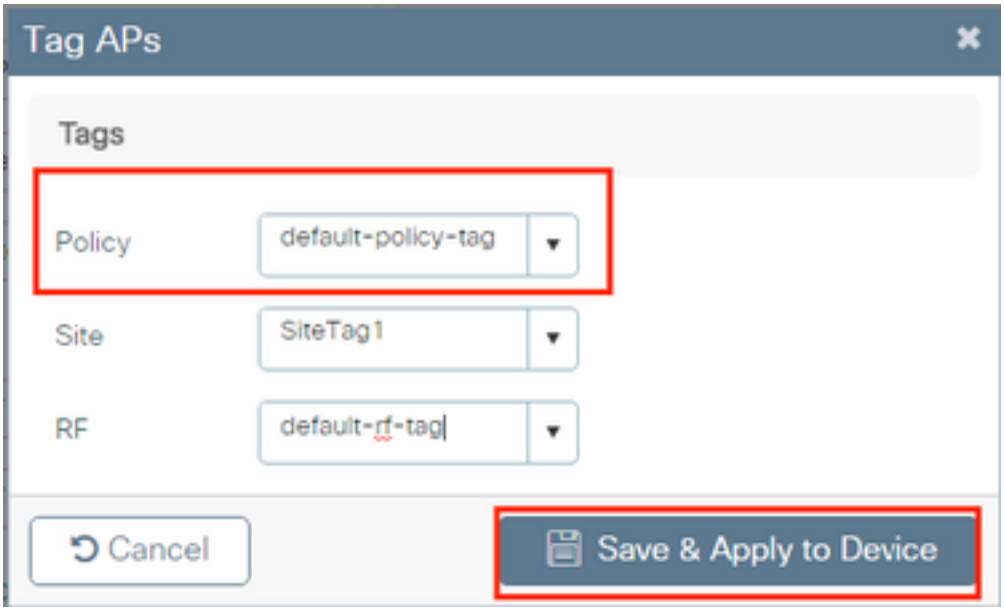
Um mehrere APs mit derselben Policy-Tag zu versehen, navigieren Sie zu **Configuration > Wireless Setup > Start Now > Apply.**



Wählen Sie die APs aus, denen Sie das Tag zuweisen möchten, und klicken Sie auf **+ Tag APs.**



Wählen Sie das gewünschte Tag aus, und klicken Sie auf **Save & Apply (Speichern und anwenden).**



CLI

```
# config t
# ap <ethernet-mac-addr>
# policy-tag <policy-tag-name>
# end
```

ISE-Konfiguration

Für die ISE v1.2-Konfiguration überprüfen Sie diesen Link:

ISE-Konfiguration

Überprüfen

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

```
# 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 ON-Ablaufverfolgungsfunktionen. Dadurch wird sichergestellt, dass alle Client-Verbindungsfehler, Fehler- und Warnstufen-Meldungen kontinuierlich protokolliert werden und dass Sie Protokolle nach einem Vorfall oder einem Fehler anzeigen können.

> **Hinweis**: Je nach Menge der generierten Protokolle können Sie mehrere Stunden bis mehrere Tage zurücklegen.

Um die Spuren anzuzeigen, die der 9800-WLC standardmäßig erfasst hat, können Sie über SSH/Telnet eine Verbindung zum 9800-WLC herstellen und die folgenden Schritte ausführen (Stellen Sie sicher, dass Sie die Sitzung in einer Textdatei protokollieren).

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

```
# show clock
```

Schritt 2: Erfassen Sie Syslogs aus dem Puffer des Controllers oder aus dem externen Syslog, wie von der Systemkonfiguration vorgegeben. Dies bietet einen schnellen Überblick über den Systemstatus und etwaige Fehler.

```
# show logging
```

Schritt 3: Überprüfen Sie, ob Debugbedingungen 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 aufgelistet wird, bedeutet dies, dass die Ablaufverfolgungen für alle Prozesse, die mit den aktivierten Bedingungen konfrontiert sind (MAC-Adresse, IP-Adresse usw.) bis zum Debug-Level protokolliert werden. Dadurch würde sich die Protokollmenge erhöhen. Daher wird empfohlen, alle Bedingungen zu löschen, wenn das Debuggen nicht aktiv ist.

Schritt 4: Unter der Annahme, dass die MAC-Adresse nicht als Bedingung in Schritt 3 aufgeführt war, sammeln Sie die stets verfügbaren Pegel-Traces 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 Debuggen und Radio Active Tracing

Wenn Ihnen die stets verfügbaren Ablaufverfolgungen nicht genügend Informationen liefern, um den Auslöser für das zu untersuchende Problem zu bestimmen, können Sie das bedingte Debuggen aktivieren und 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). Führen Sie die folgenden Schritte aus, um bedingtes Debuggen zu aktivieren.

Schritt 5: Stellen Sie sicher, dass keine Debugbedingungen aktiviert sind.

```
# clear platform condition all
```

Schritt 6: Aktivieren Sie die Debugbedingung für die MAC-Adresse des Wireless-Clients, die überwacht werden soll.

Diese Befehle beginnen, die angegebene MAC-Adresse für 30 Minuten (1800 Sekunden) zu überwachen. Optional können Sie diese Zeit auf bis zu 2085978494 Sekunden erhöhen.

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

Hinweis: Um mehrere Clients gleichzeitig zu überwachen, führen Sie den Befehl debug wireless mac **<**aaa.bbbb.cccc**>** pro MAC-Adresse aus.

Hinweis: Die Ausgabe der Clientaktivität in der Terminalsitzung wird nicht angezeigt, da alles intern gepuffert wird, um später angezeigt zu werden.

Schritt 7: Reproduzieren Sie das zu überwachende Problem oder Verhalten.

Schritt 8: Beenden Sie das Debuggen, wenn das Problem reproduziert wird, bevor die Standard- oder konfigurierte Überwachungszeit aktiv ist.

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

Wenn die Überwachungszeit abgelaufen ist oder die Wireless-Debugging-Funktion beendet wurde, generiert der 9800 WLC eine lokale Datei mit dem Namen:

ra_trace_MAC_aaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year_year.log

Schritt 9: Erfassen Sie die Datei der MAC-Adressenaktivität. Sie können die Datei ra trace.log auf einen externen Server kopieren oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Überprüfen Sie den Namen der RA Traces-Datei.

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

Kopieren Sie die Datei auf einen externen Server:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://a.b.c.d/ra-FILENAME.txt
```

Inhalte 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 Debug-Level-Protokolle darstellen. Sie müssen den Client nicht erneut debuggen, da wir nur noch die Debug-Protokolle genauer betrachten, 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 ziemlich umfangreich. Wenden Sie sich an das Cisco TAC, um bei der Analyse dieser Ablaufverfolgungen zu helfen.

Sie können die Datei ra-internal-FILENAME.txt auf einen externen Server kopieren oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Kopieren Sie die Datei auf einen externen Server:

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

Inhalte anzeigen:

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

Schritt 11: Entfernen Sie die Debugbedingungen.

```
# clear platform condition all
```

Hinweis: Stellen Sie sicher, dass Sie die Debugbedingungen immer nach einer Fehlerbehebungssitzung entfernen.