Konfigurieren der 802.1X-Authentifizierung auf Catalyst Wireless Controllern der Serie 9800

Inhalt

Einleitung

In diesem Dokument wird die Einrichtung eines WLAN mit 802.1X-Sicherheit auf einem Cisco Catalyst Wireless Controller der Serie 9800 beschrieben.

Voraussetzungen

Anforderungen

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

- 802.1x

Verwendete Komponenten

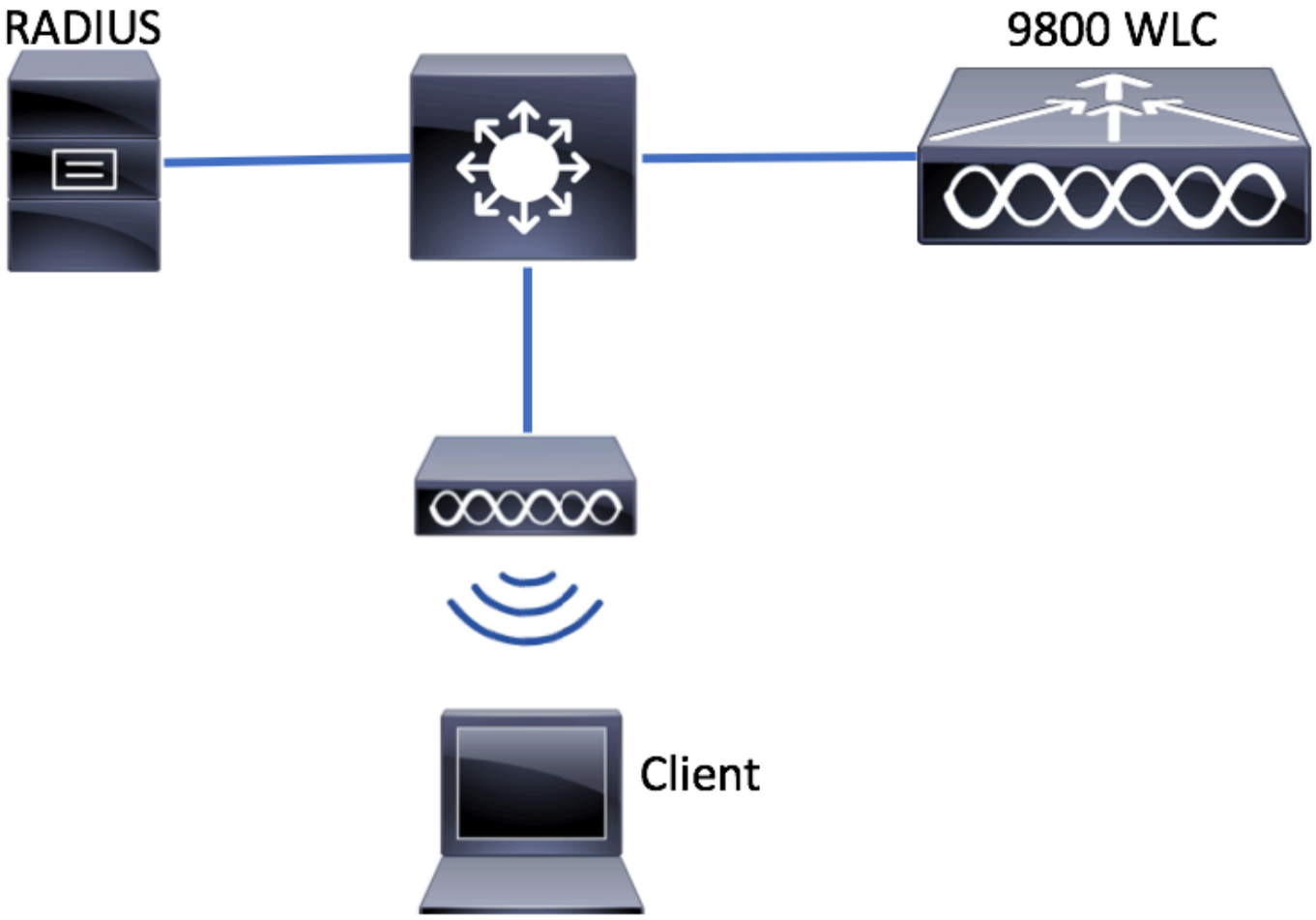
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst Wireless Controller der Serie 9800 (Catalyst 9800-CL)
- Cisco IOS® XE Gibraltar 17.3.x
- 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.

Konfigurieren

Netzwerkdiagramm



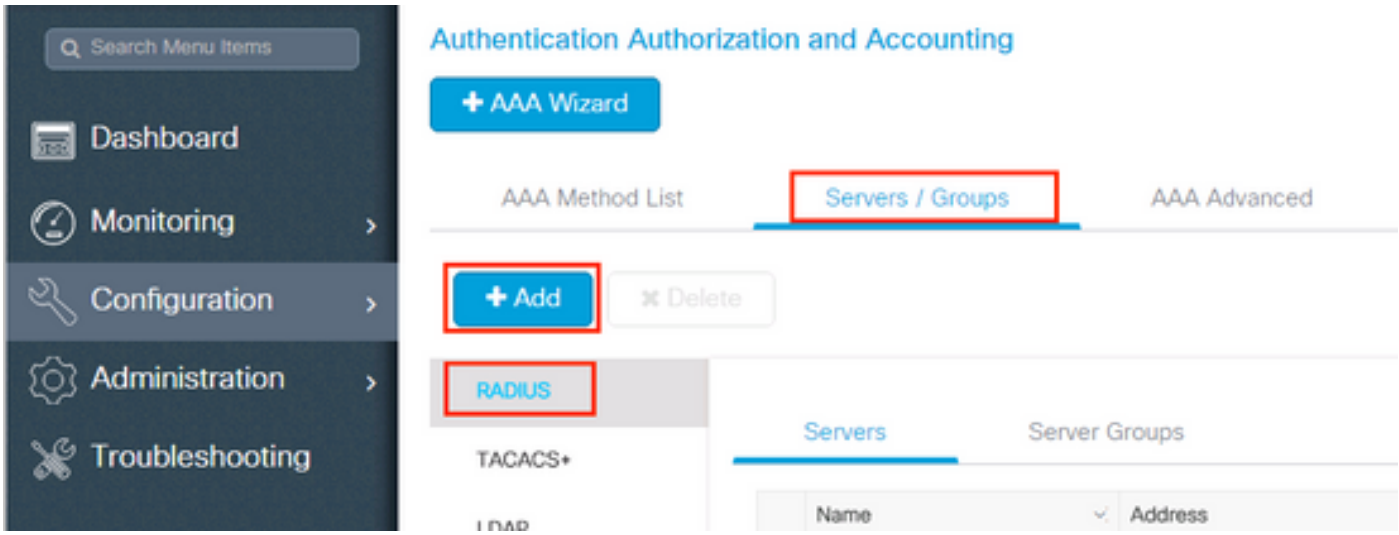
WLC-Konfiguration

AAA-Konfiguration auf 9800 WLCs

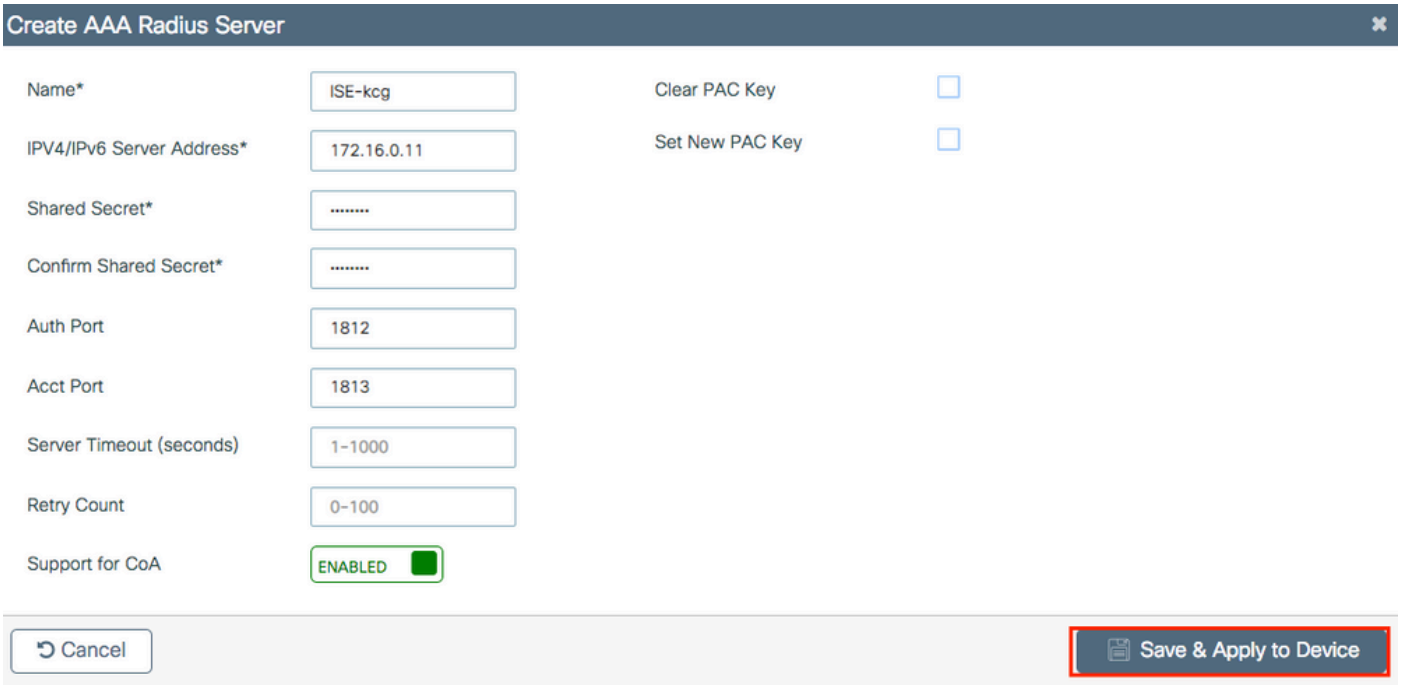
GUI:

Schritt 1: Deklarieren des RADIUS-Servers Navigieren Sie zu **Configuration > Security > AAA > Servers /**

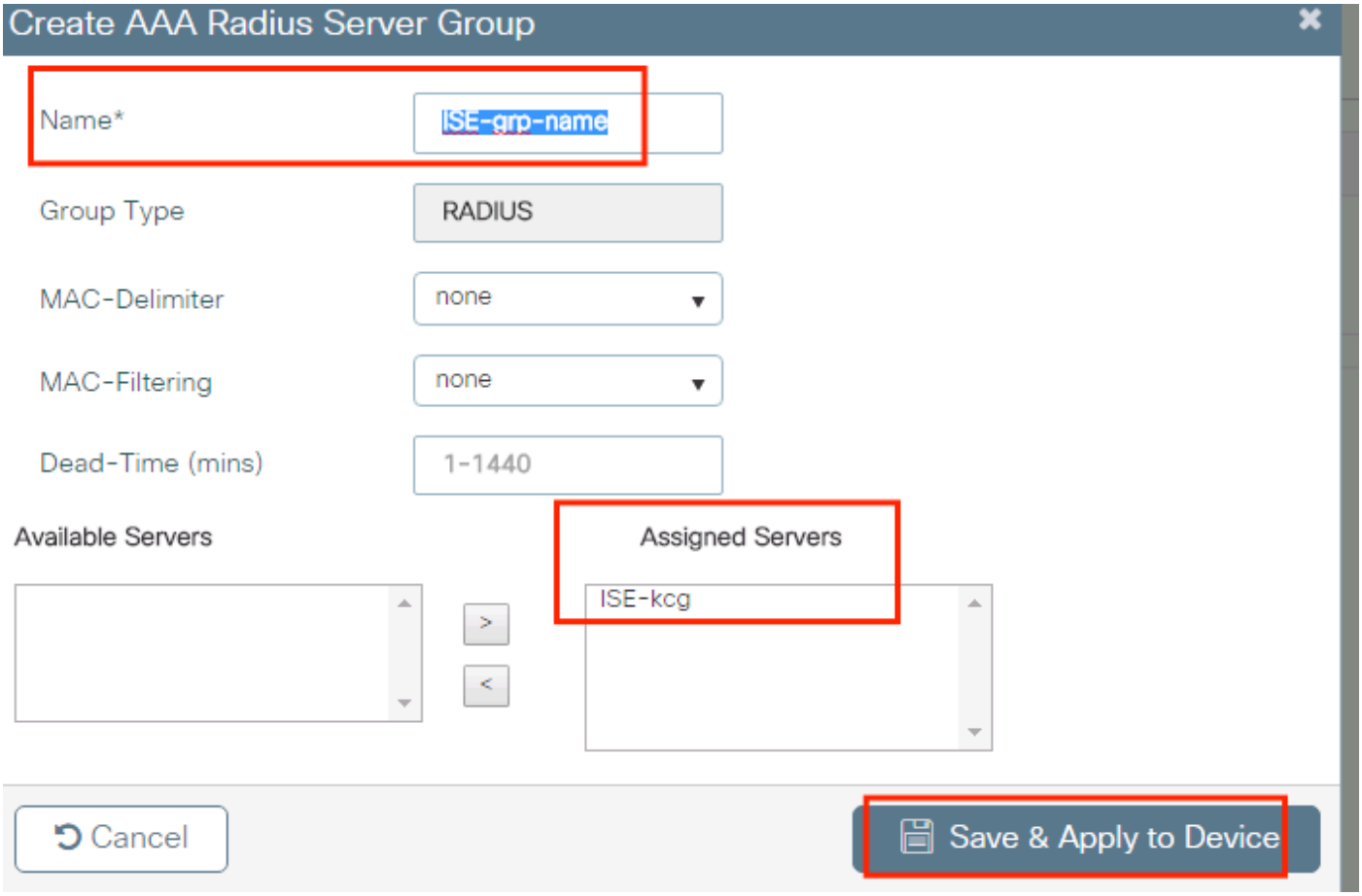
Groups > RADIUS > Servers > + Add und geben Sie die RADIUS-Serverinformationen ein.



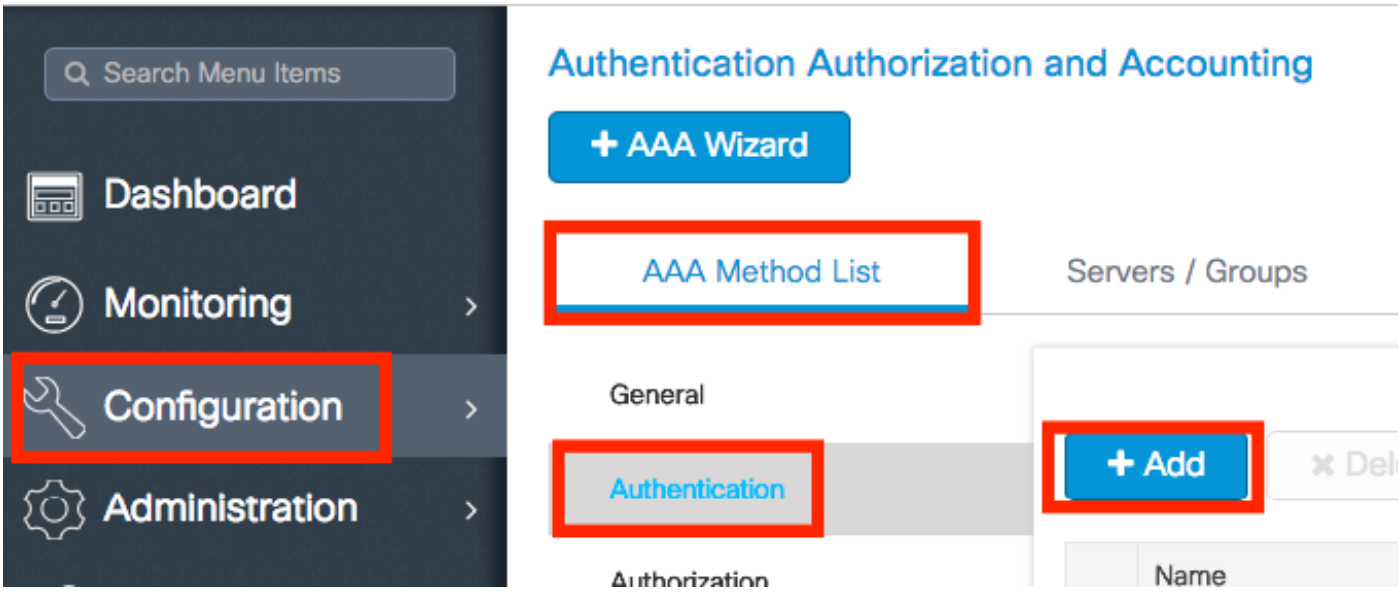
Stellen Sie sicher, dass **Support für CoA** aktiviert ist, wenn Sie beabsichtigen, Central Web Authentication (oder andere Sicherheitsfunktionen, die eine Autorisierungsänderung erfordern) in Zukunft zu verwenden.



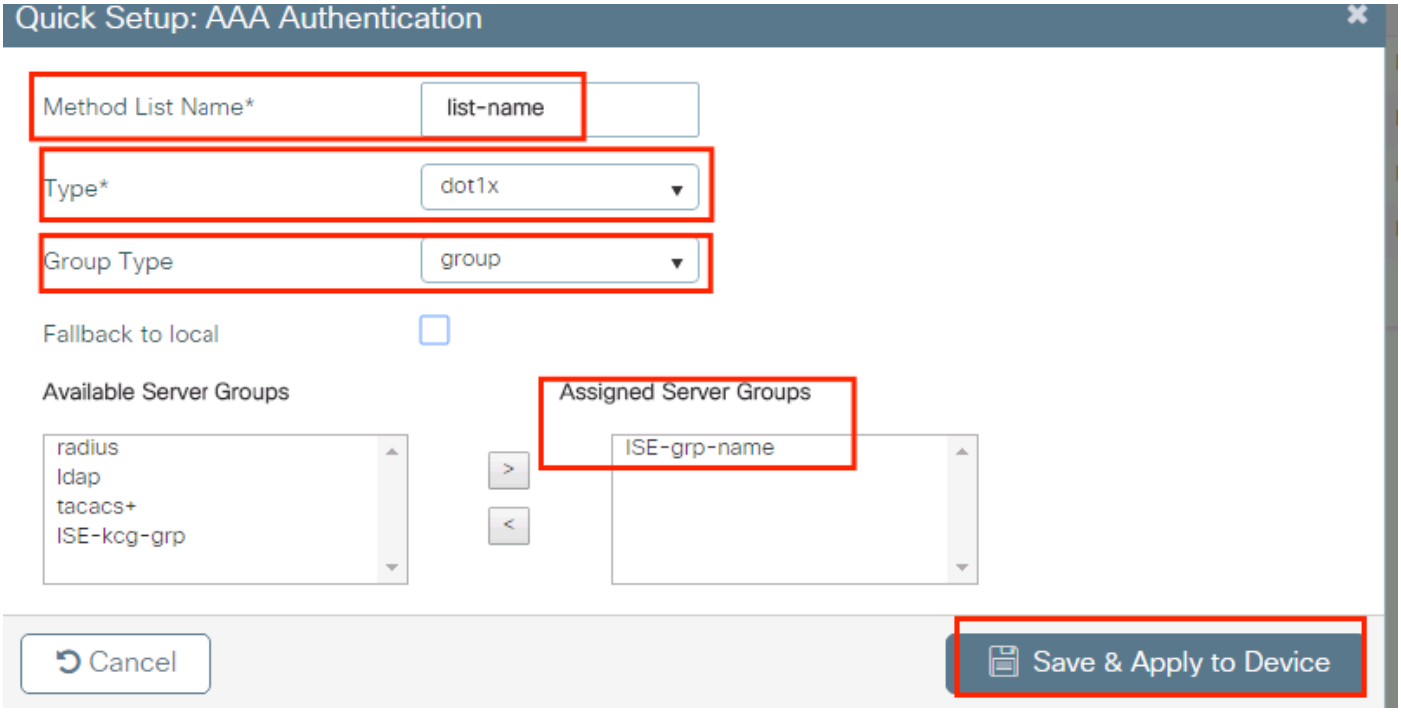
Schritt 2: Hinzufügen des RADIUS-Servers zu einer RADIUS-Gruppe Navigieren Sie zu **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.** Geben Sie Ihrer Gruppe einen Namen, und verschieben Sie den Server, den Sie zuvor in der Liste **Assigned Servers**.



Schritt 3: Erstellen einer Liste von Authentifizierungsmethoden Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.



Geben Sie die Informationen ein:



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 authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

Hinweis zur AAA Dead-Server-Erkennung

Nachdem Sie den RADIUS-Server konfiguriert haben, können Sie überprüfen, ob er als "ALIVE" gilt:

```
#show aaa servers | s WNCD Platform State from WNCD (1) : current UP Platform State from WNCD (2) : current UP Platform State from WNCD (3) : current UP Platform State from WNCD (4) : current UP ...
```

Sie können die **dead criteria**, sowie die **deadtime** auf Ihrem WLC, insbesondere wenn Sie mehrere RADIUS-Server verwenden.

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

> **Hinweis**: **dead criteria** ist das Kriterium, anhand dessen ein RADIUS-Server als ausgefallen markiert wird. Die Kommission wird um die Beantwortung folgender Fragen ersucht: 1. Ein

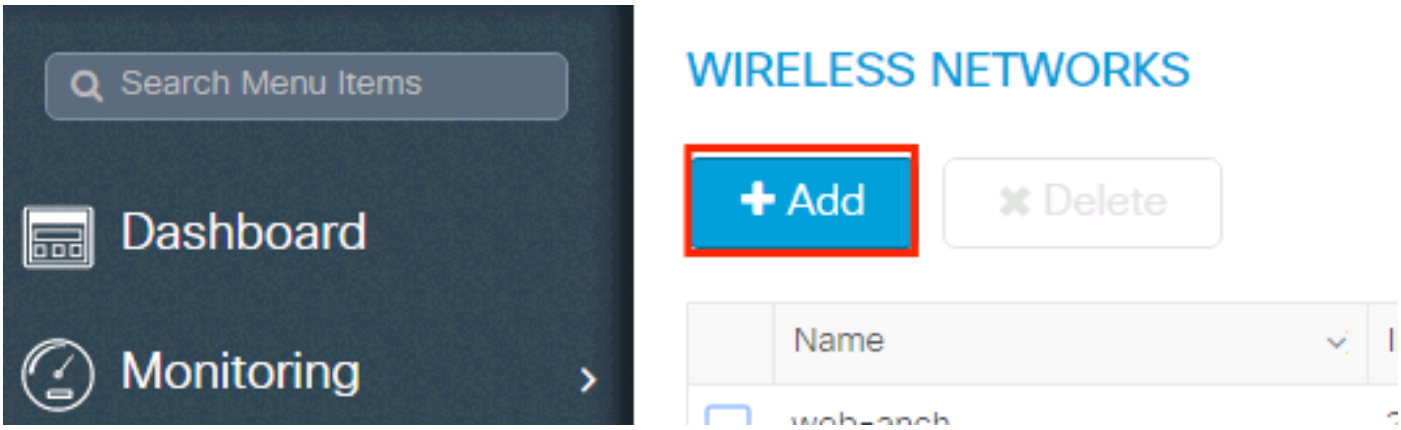
Timeout (in Sekunden), das die Zeitspanne von dem Zeitpunkt, zu dem der Controller das letzte Mal ein gültiges Paket vom RADIUS-Server empfangen hat, bis zu dem Zeitpunkt, zu dem der Server als ausgefallen markiert ist, angibt. 2. Ein Zähler, der die Anzahl aufeinander folgender Zeitüberschreitungen angibt, die auf dem Controller auftreten müssen, bevor der RADIUS-Server als ausgefallen markiert wird.

Hinweis: **deadtime** gibt die Zeitdauer (in Minuten) an, die der Server in den "Dead"-Status versetzt wird, nachdem "Dead Criteria" ihn als "Dead" markiert hat. Nach Ablauf der Deadtime markiert der Controller den Server als UP (ALIVE) und benachrichtigt die registrierten Clients über die Statusänderung. Ist der Server nach dem Status als UP noch nicht erreichbar und ist das Dead-Kriterium erfüllt, so wird der Server für das Deadtime-Intervall erneut als Dead markiert.

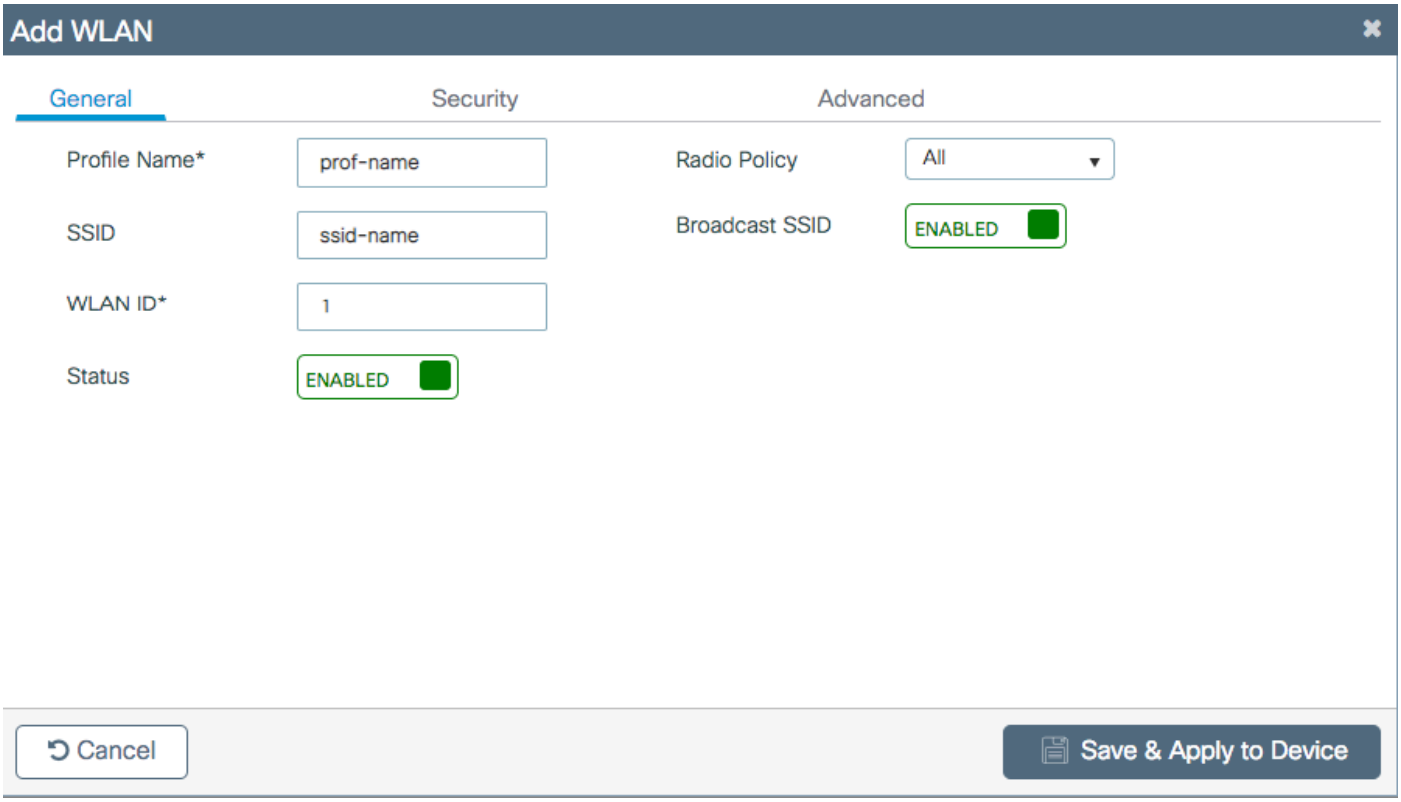
WLAN-Profilkonfiguration

GUI:

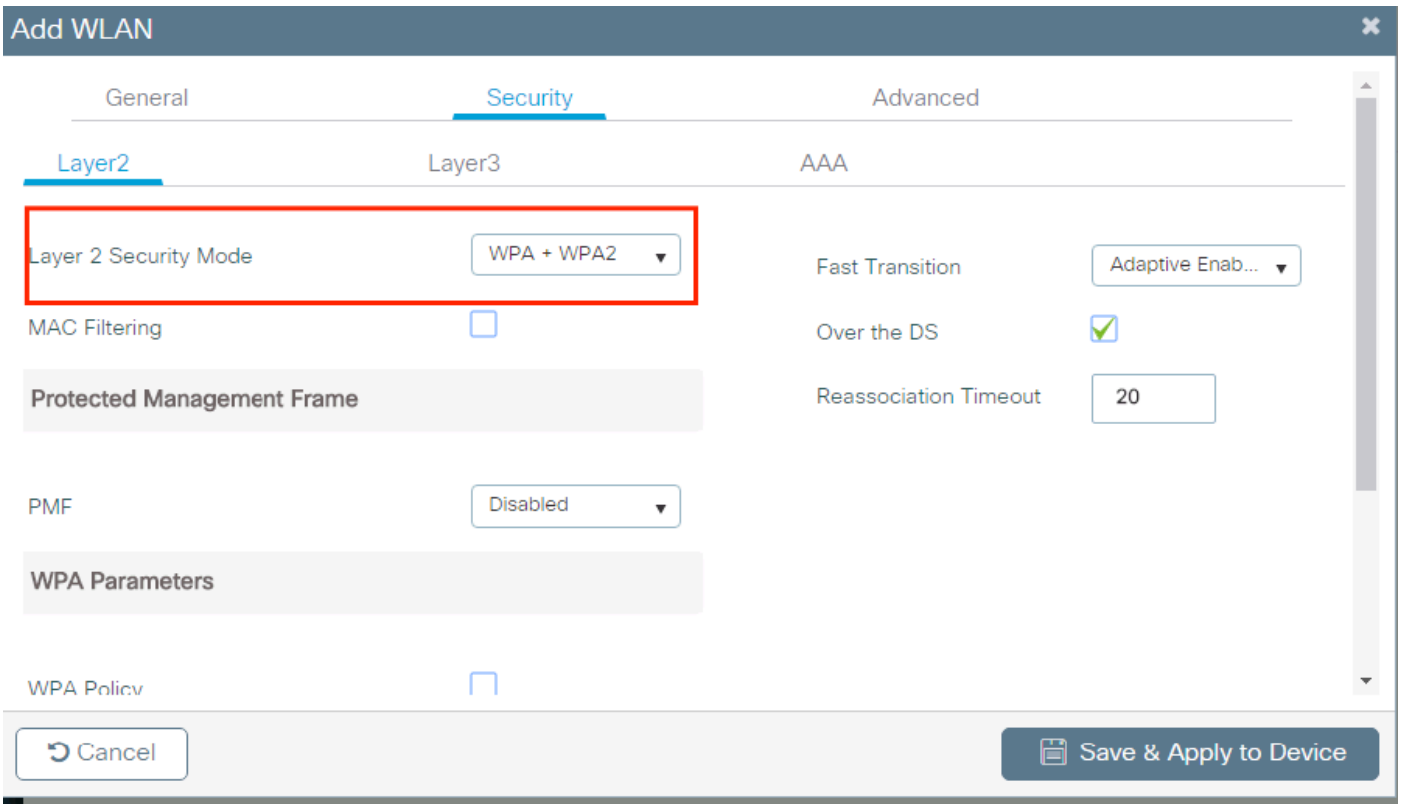
Schritt 1: WLAN erstellen. Navigieren Sie zu **Configuration > Wireless > WLANs > + Add,** und konfigurieren Sie das Netzwerk nach Bedarf.

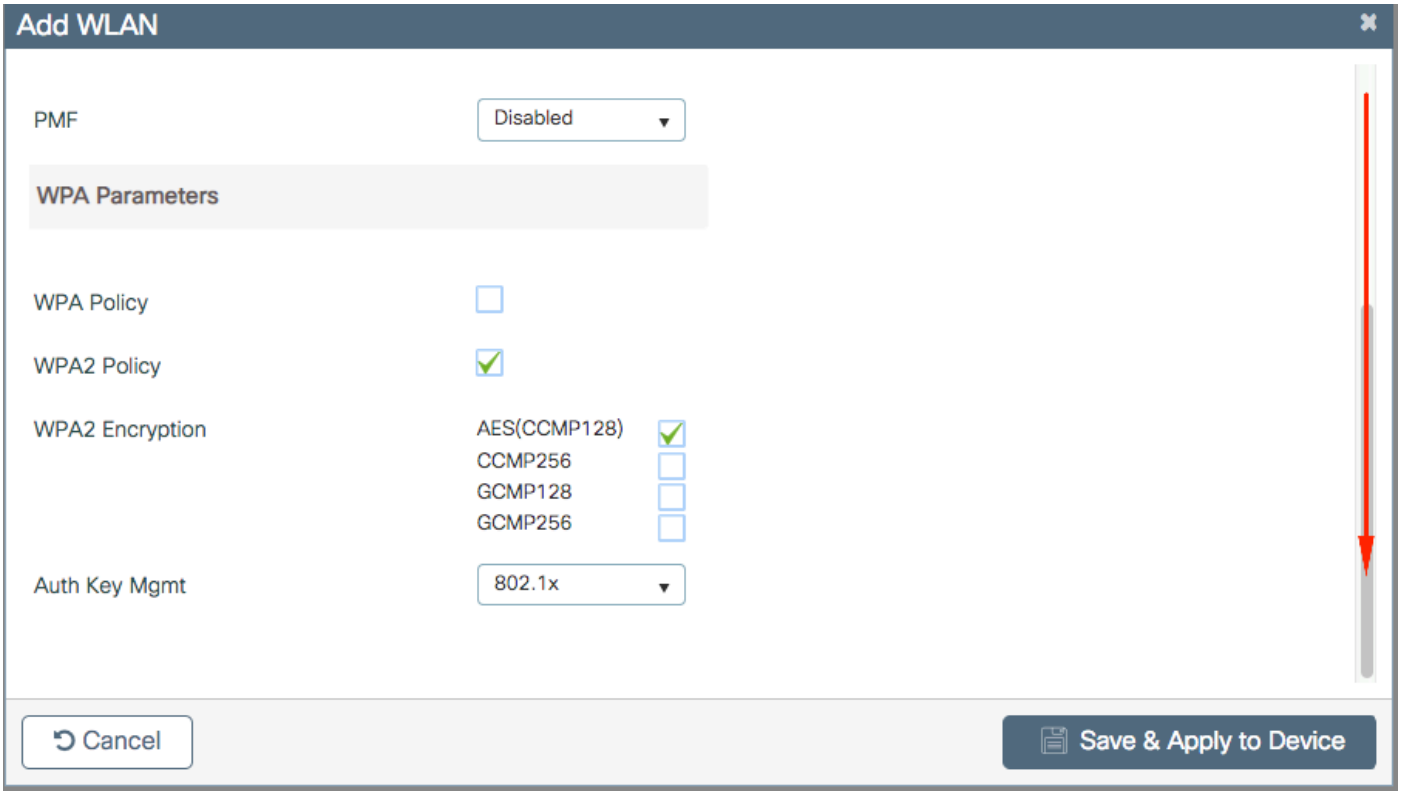


Schritt 2: Geben Sie die WLAN-Informationen ein

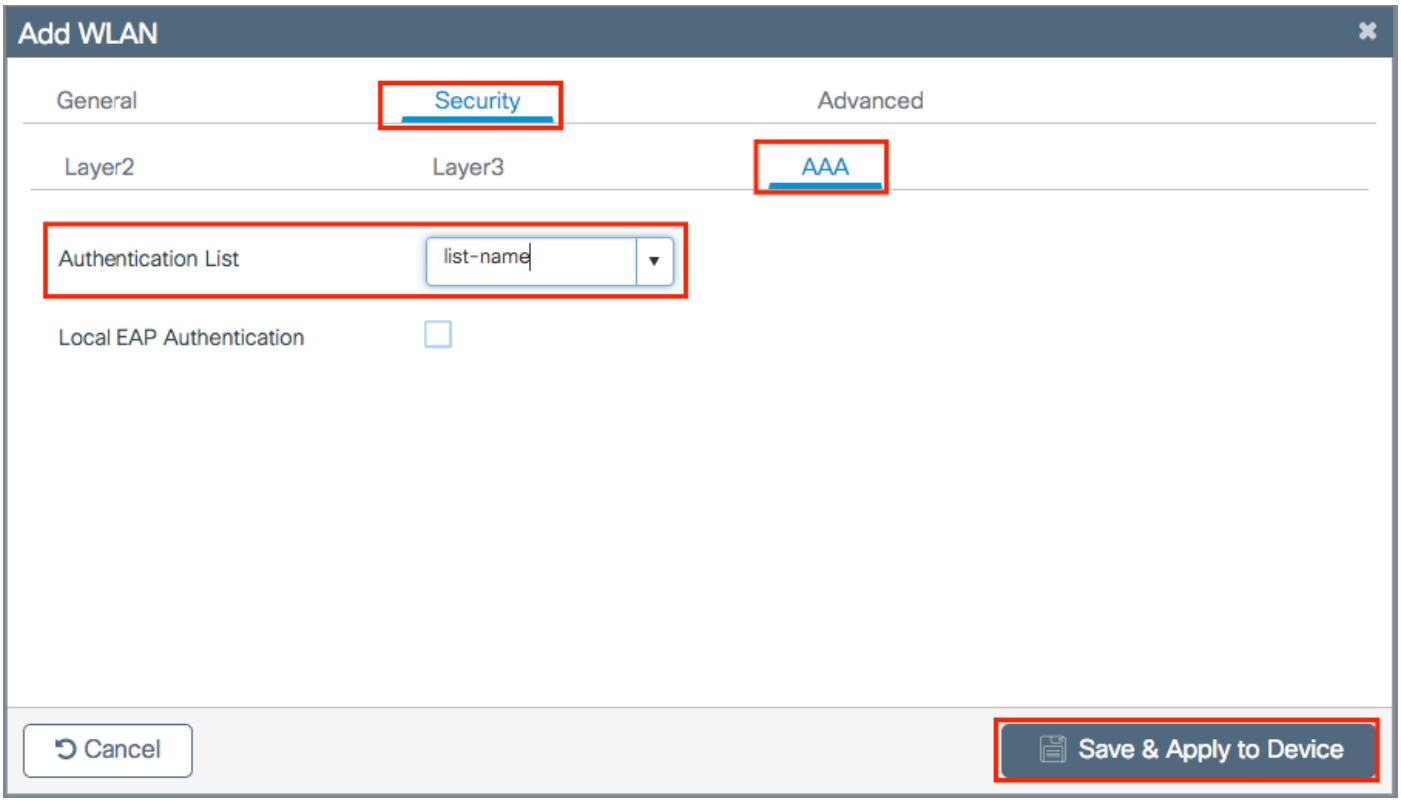


Schritt 3: Navigieren Sie zum und wählen Sie die erforderliche Sicherheitsmethode aus. In diesem Fall **WPA2 + 802.1x**.





Schritt 4: Über die **Security > AAA** die unter Schritt 3 erstellte Authentifizierungsmethode im Abschnitt AAA Configuration on 9800 WLC auswählen.



CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
# no shutdown
```

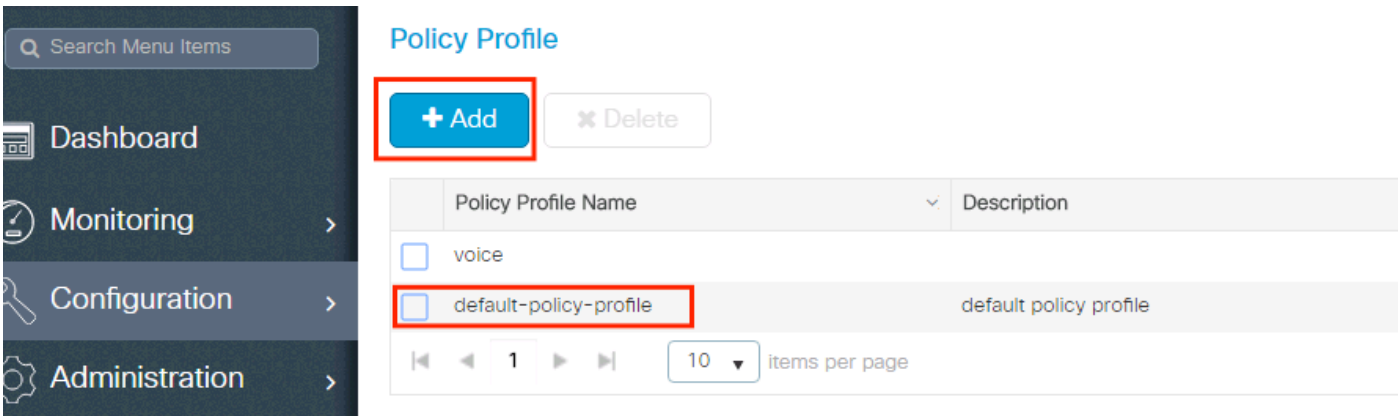
Richtlinienprofilkonfiguration

In einem Richtlinienprofil können Sie neben anderen Einstellungen (wie Zugriffskontrolllisten [ACLs], Quality of Service [QoS], Mobility Anchor, Timer usw.) festlegen, welchem VLAN die Clients zugewiesen werden sollen.

Sie können entweder Ihr Standardrichtlinienprofil verwenden oder ein neues Profil erstellen.

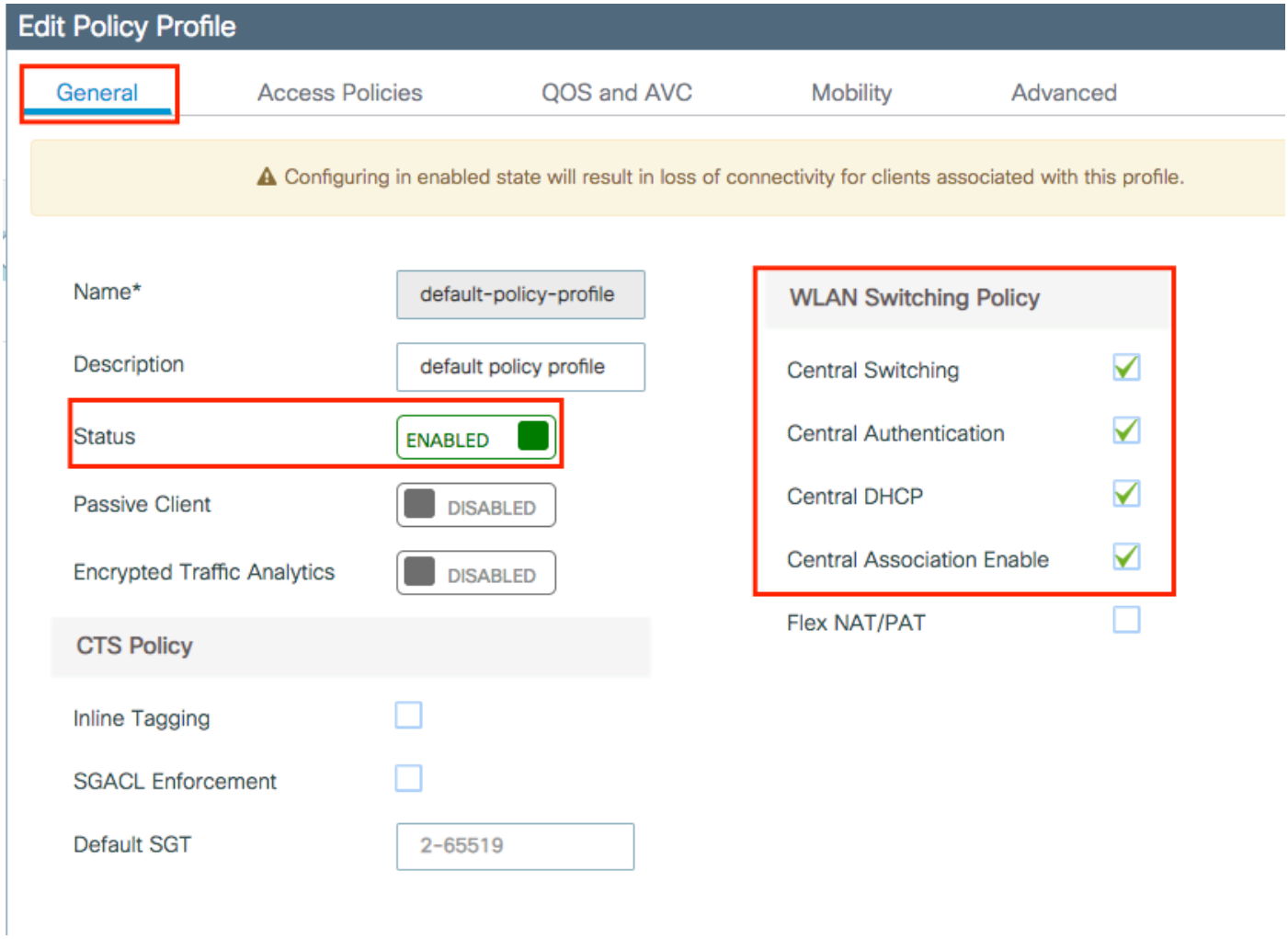
GUI:

Navigieren Sie zu **Configuration > Tags & Profiles > Policy Profile,** und konfigurieren Sie entweder Ihr **Standard-Richtlinienprofil** oder erstellen Sie ein neues.

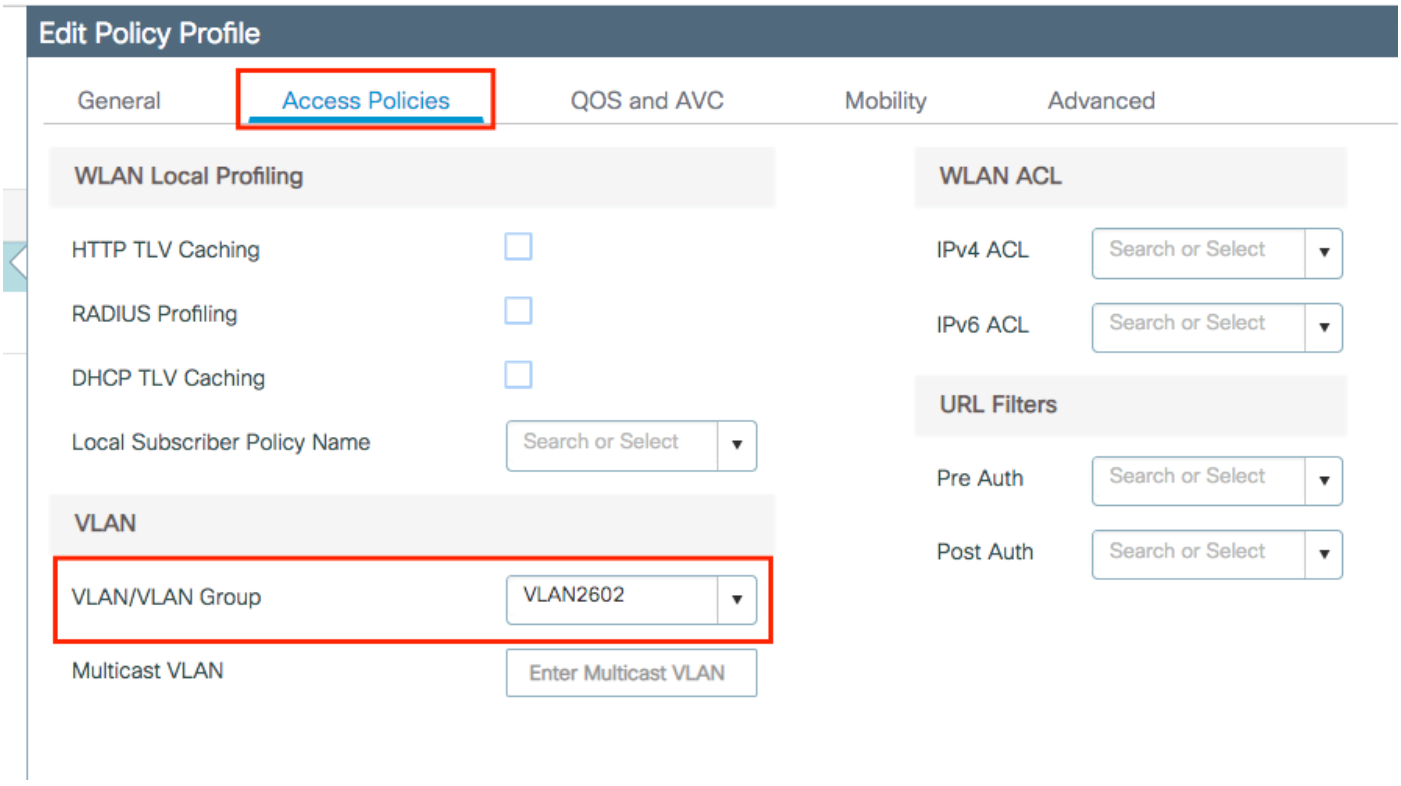


Stellen Sie sicher, dass das Profil aktiviert ist.

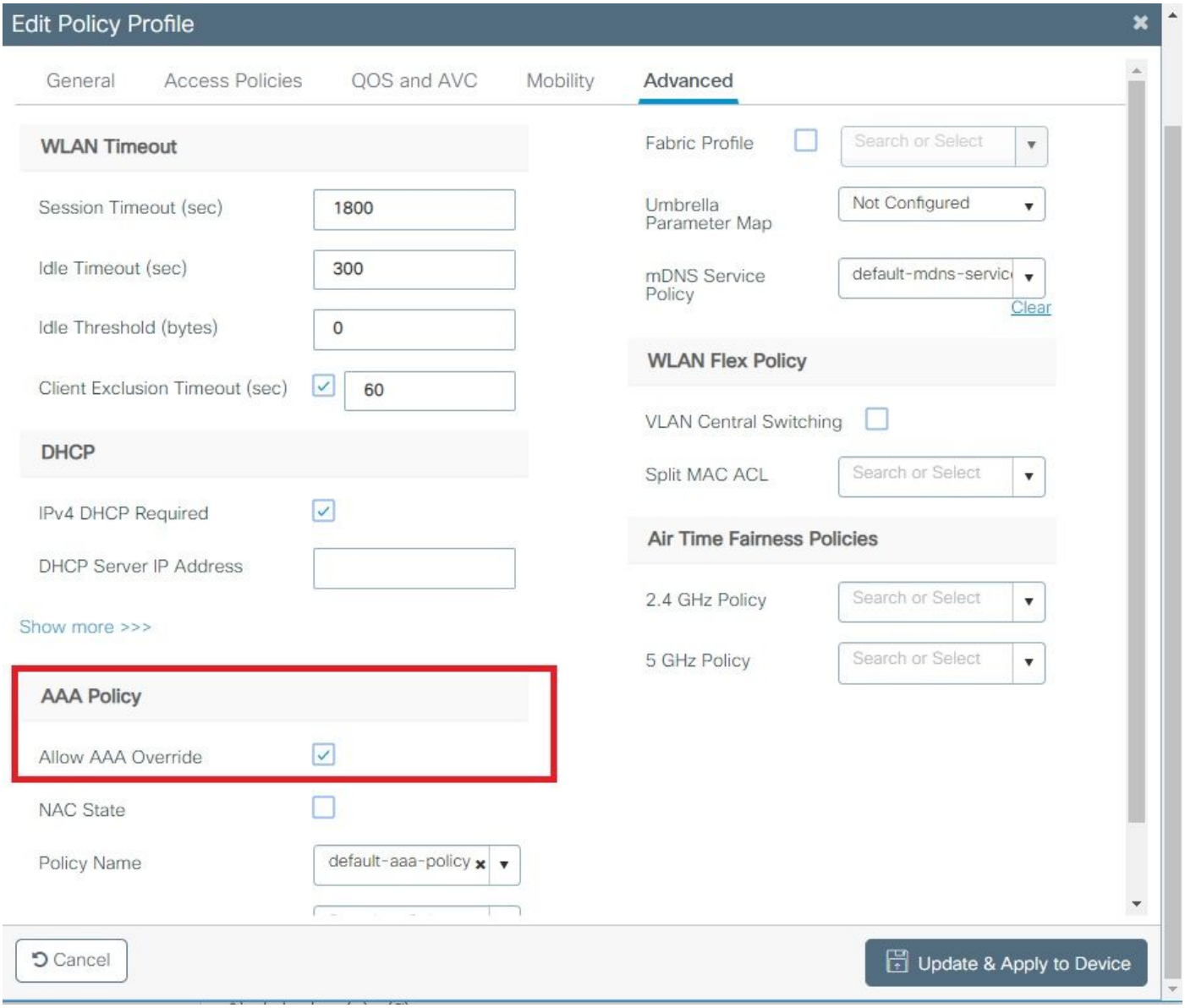
Wenn sich Ihr Access Point (AP) im lokalen Modus befindet, stellen Sie außerdem sicher, dass im Richtlinienprofil **Central Switching** und **Central Authentication** aktiviert sind.



Wählen Sie auf der Registerkarte "**Access Policies**" (**Zugriffsrichtlinien)** das VLAN aus, dem die Clients zugewiesen werden müssen.



Wenn im Feld "Access-Accept" ISE-Rückgabeattribute (z. B. "VLAN Assignment") vorhanden sein sollen, aktivieren Sie AAA override im **Advanced** Registerkarte:



CLI:

```
# config
# wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> #
no shutdown
```

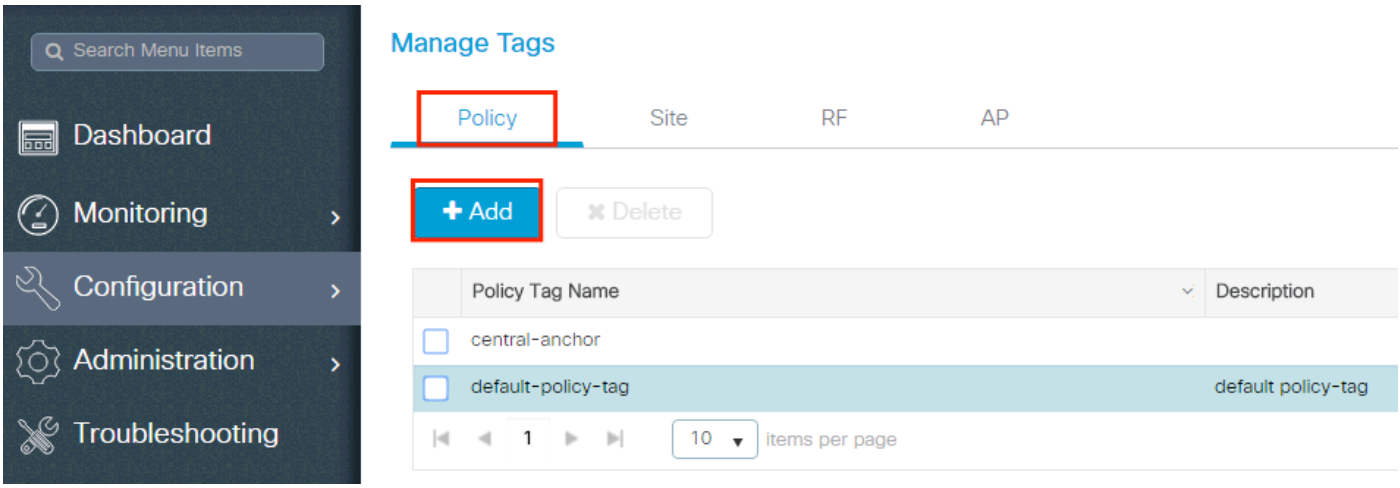
Richtlinien-Tag-Konfiguration

Das Policy Tag (Richtlinien-Tag) dient zum Verknüpfen der SSID mit dem Richtlinienprofil. Sie können entweder ein neues Richtlinien-Tag erstellen oder das Standard-Richtlinien-Tag verwenden.

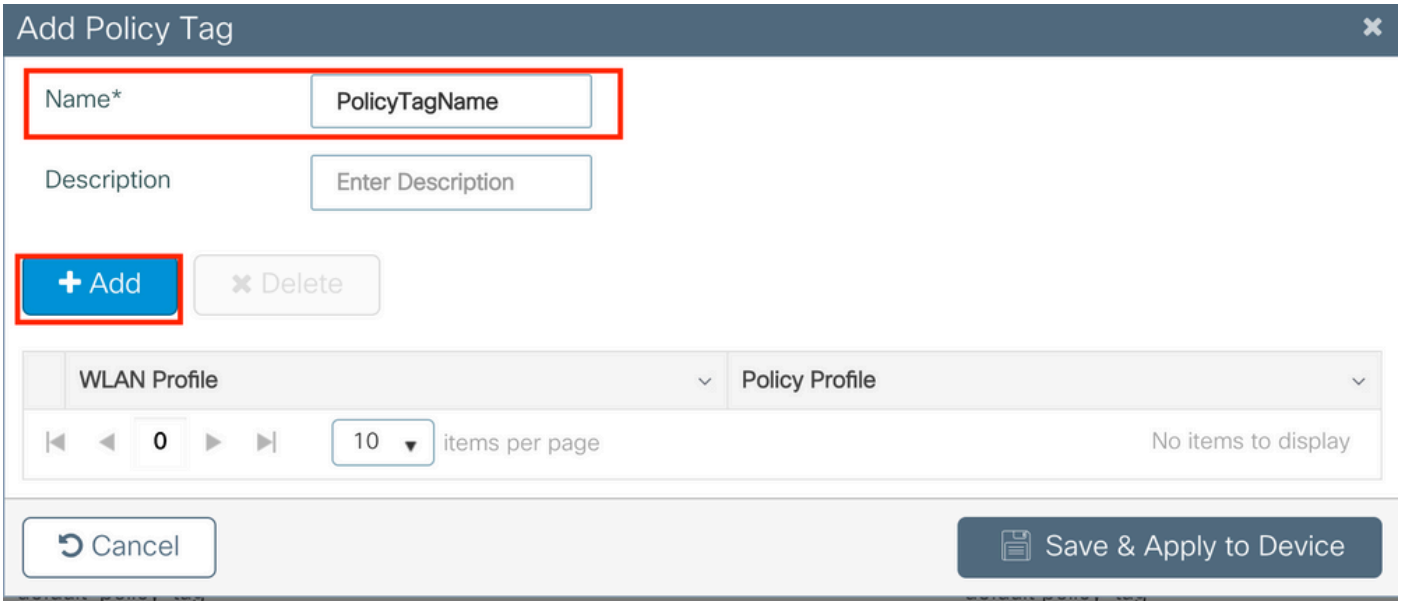
> **Hinweis**: Das default-policy-Tag ordnet dem default-policy-Profil automatisch alle SSIDs mit einer WLAN-ID zwischen 1 und 16 zu. Sie kann weder geändert noch gelöscht werden. Wenn Sie über ein WLAN mit der ID 17 oder höher verfügen, kann das default-policy-tag nicht verwendet werden.

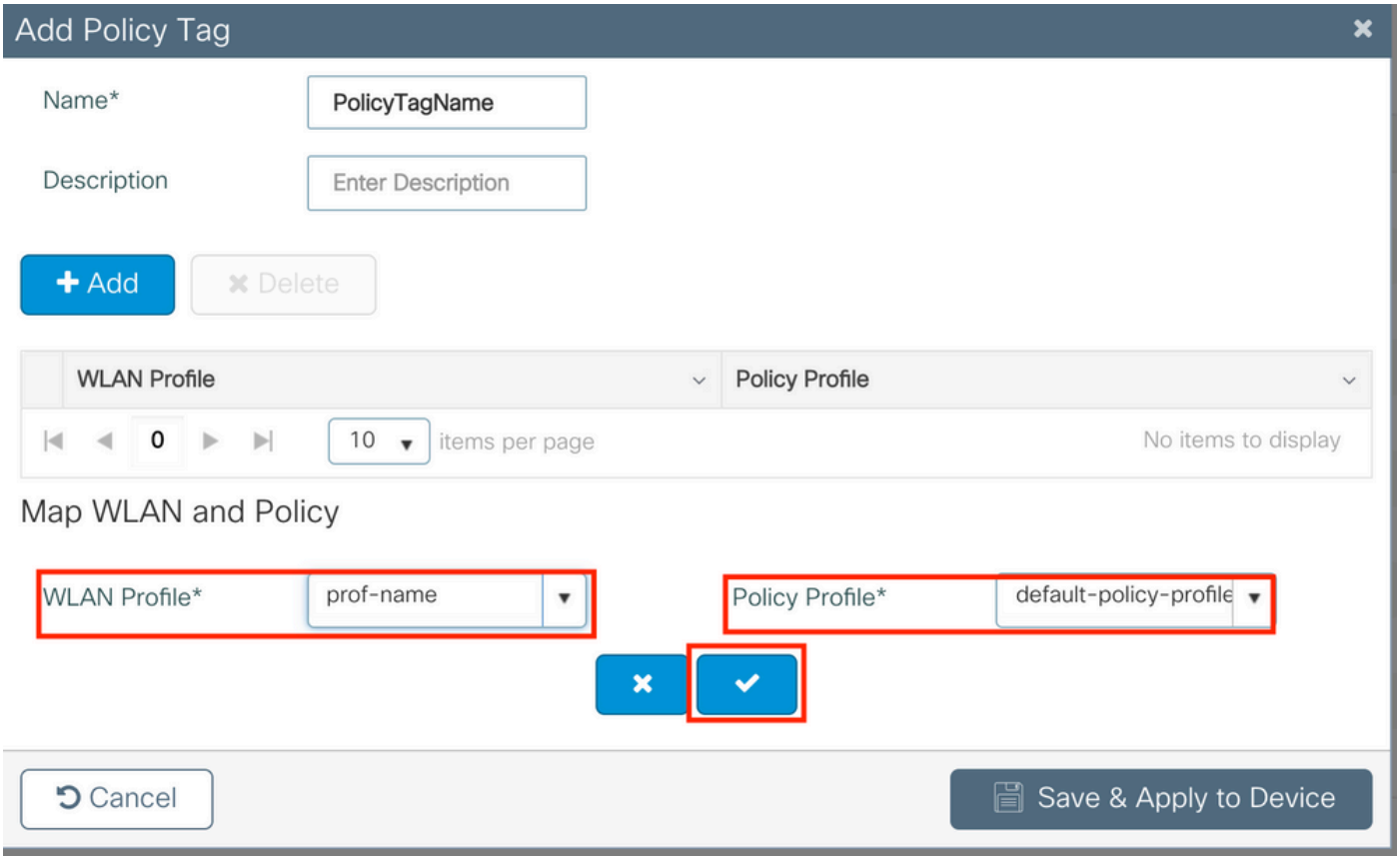
GUI:

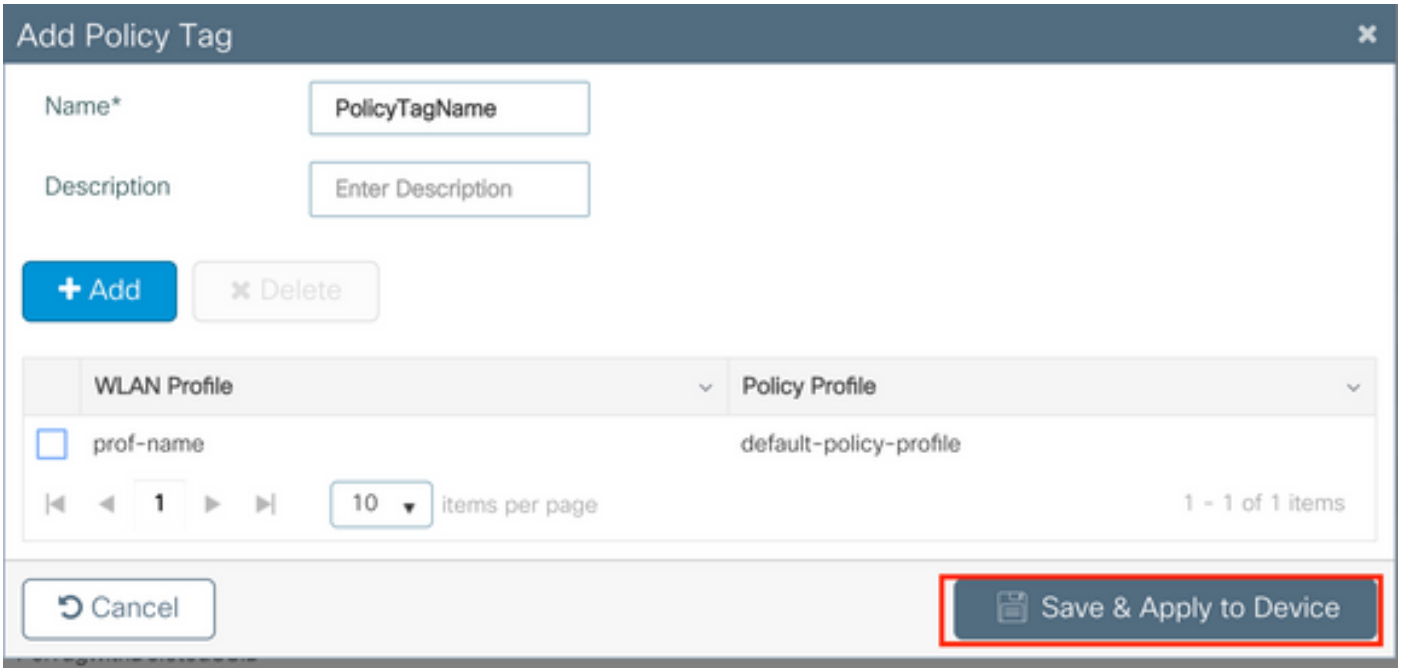
Navigieren Sie zu **Configugation > Tags & Profiles > Tags > Policy** und fügen Sie ggf. ein neues hinzu.



Verknüpfen Sie Ihr WLAN-Profil mit dem gewünschten Richtlinienprofil.







CLI:

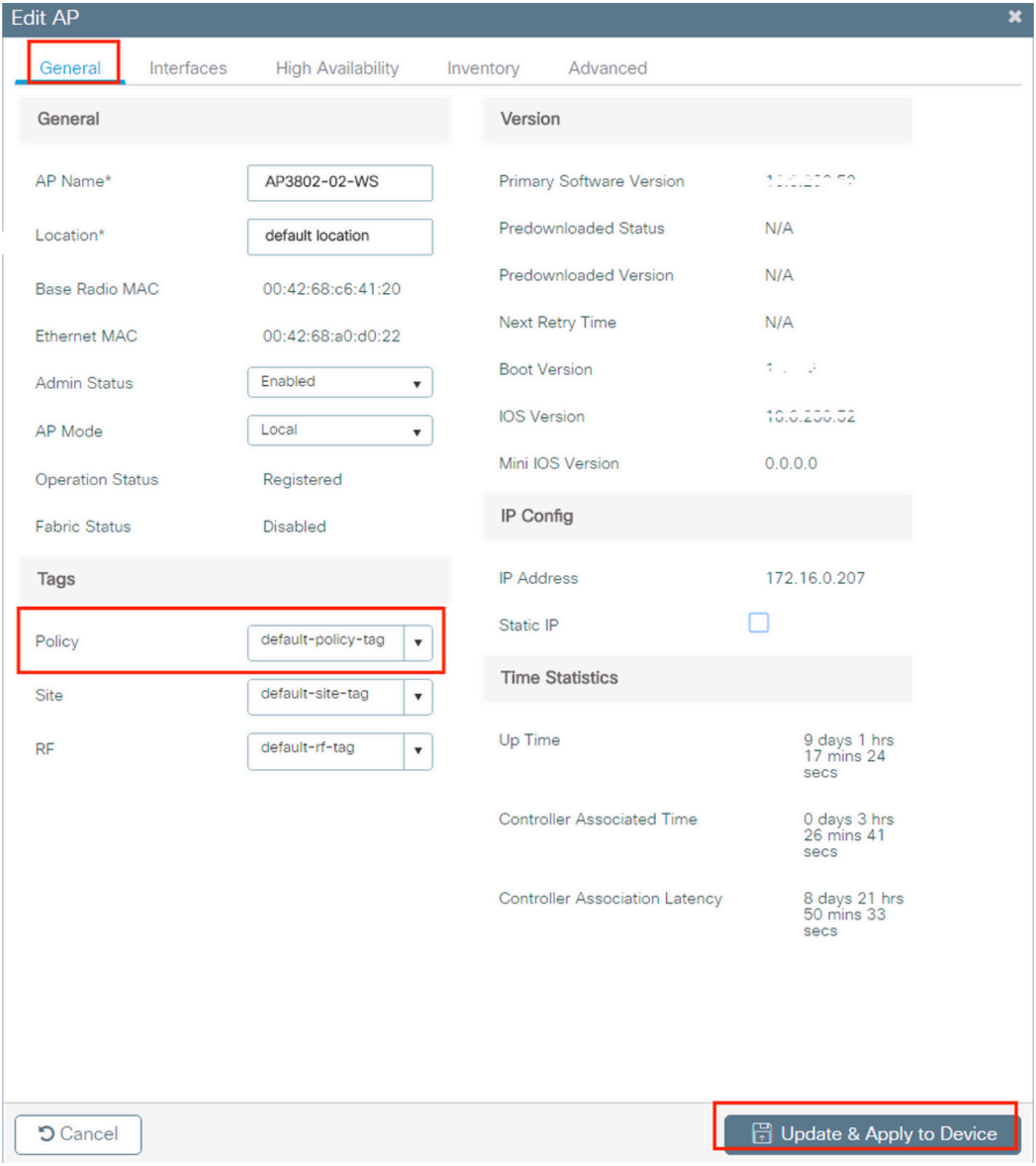
```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

Richtlinien-Tag-Zuweisung

Weisen Sie den erforderlichen APs das Richtlinien-Tag zu.

GUI:

Um das Tag einem AP zuzuweisen, navigieren Sie zu **Configuration > Wireless > Access Points > AP Name > General Tags**, die entsprechende Policy-Tag-Nummer zuzuweisen, und klicken Sie dann auf **Update & Apply to Device**.



Hinweis: Beachten Sie, dass bei einer Änderung des Richtlinien-Tags an einem Access Point dessen Verknüpfung mit dem 9800 WLC gelöscht wird und dieser dann einige Augenblicke später wieder hinzugefügt wird.

Um dieselbe Policy Tag mehreren APs zuzuweisen, navigieren Sie zu **Configuration > Wireless Setup > Advanced > Start Now > Apply**.

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.