Konfigurieren der dynamischen VLAN-Zuordnung mit ISE und dem Catalyst 9800 Wireless LAN Controller

Inhalt

[Einleitung](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Dynamische VLAN-Zuweisung mit RADIUS-Server](#)
[Konfigurieren](#)
[Netzwerkdiagramm](#)
[Konfigurationsschritte](#)
[Cisco ISE-Konfiguration](#)
[Schritt 1: Konfigurieren des Catalyst WLC als AAA-Client auf dem Cisco ISE-Server](#)
[Schritt 2: Konfigurieren interner Benutzer für die Cisco ISE](#)
[Schritt 3: Konfigurieren der RADIUS (IETF)-Attribute für die dynamische VLAN-Zuweisung](#)
[Switch für mehrere VLANs konfigurieren](#)
[Catalyst 9800 WLC-Konfiguration](#)
[Schritt 1: Konfigurieren des WLC mit den Details des Authentifizierungsservers](#)
[Schritt 2: Konfigurieren der VLANs](#)
[Schritt 3: Konfigurieren der WLANs (SSID)](#)
[Schritt 4: Konfigurieren des Richtlinienprofils](#)
[Schritt 5: Konfigurieren der Richtlinien-Tag](#)
[Schritt 6: Zuweisen der Policy-Tag zu einem AP](#)
[Überprüfung](#)
[Fehlerbehebung](#)
[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt das Konzept der dynamischen VLAN-Zuweisung und die Konfiguration des Catalyst 9800 Wireless LAN Controller (WLC) und der Cisco Identity Service Engine (ISE) für die Zuweisung von WLANs (WLAN), um dies für die Wireless Clients zu erreichen.

Anforderungen

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

- Grundkenntnisse der WLC- und Lightweight Access Points (LAPs)
- über funktionale Kenntnisse des AAA-Servers wie ISE verfügen.

- Verschaffen Sie sich fundierte Kenntnisse über Wireless-Netzwerke und Wireless-Sicherheitsfragen.
- über funktionale Kenntnisse der dynamischen VLAN-Zuweisung verfügen.
- Grundkenntnisse der Steuerung und Bereitstellung für Wireless Access Points (CAPWAP)

Verwendete Komponenten

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

- Cisco Catalyst 9800 WLC (Catalyst 9800-CL) mit Firmware-Version 16.12.4a
- Cisco LAP der Serie 2800 im lokalen Modus
- Systemeigene Windows 10-Komponente.
- Cisco Identity Service Engine (ISE), die Version 2.7 ausführt.
- Cisco Switch der Serie 3850 mit Firmware-Version 16.9.6.

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.

Hintergrundinformationen

Dynamische VLAN-Zuweisung mit RADIUS-Server

In den meisten WLAN-Systemen (Wireless Local Area Network) verfügt jedes WLAN über eine statische Richtlinie, die für alle Clients gilt, die einem Service Set Identifier (SSID) zugeordnet sind. Diese Methode ist zwar leistungsstark, bietet jedoch Einschränkungen, da Clients verschiedene SSIDs zuordnen müssen, um unterschiedliche QoS- und Sicherheitsrichtlinien zu erben.

Die Cisco WLAN-Lösung unterstützt jedoch Identitätsnetzwerke. Auf diese Weise kann das Netzwerk eine einzelne SSID ankündigen, und bestimmte Benutzer können je nach Benutzeranmeldeinformationen unterschiedliche QoS- oder Sicherheitsrichtlinien erben.

Die dynamische VLAN-Zuweisung ist eine dieser Funktionen, die einen Wireless-Benutzer anhand der vom Benutzer angegebenen Anmeldeinformationen in ein bestimmtes VLAN versetzt. Die Aufgabe, Benutzer einem bestimmten VLAN zuzuweisen, wird von einem RADIUS-Authentifizierungsserver wie der Cisco ISE übernommen. Dies kann beispielsweise verwendet werden, um dem Wireless-Host zu ermöglichen, im selben VLAN zu bleiben, wie er sich innerhalb eines Campus-Netzwerks bewegt.

Wenn ein Client versucht, eine Verbindung zu einer LAP herzustellen, die bei einem Controller registriert ist, übergibt der WLC die Anmeldeinformationen des Benutzers zur Validierung an den RADIUS-Server. Nach erfolgreicher Authentifizierung übergibt der RADIUS-Server bestimmte IETF-Attribute (Internet Engineering Task Force) an den Benutzer. Diese RADIUS-Attribute legen die VLAN-ID fest, die dem Wireless-Client zugewiesen werden muss. Die SSID des Clients ist unerheblich, da der Benutzer immer dieser vordefinierten VLAN-ID zugewiesen wird.

Die für die VLAN-ID-Zuweisung verwendeten RADIUS-Benutzerattribute sind:

- IETF 64 (Tunnel Type) (Tunnel-Typ) - Legen Sie diesen Wert auf VLAN fest.
- IETF 65 (Tunnel Medium Type) (Tunnel-Medientyp): Legen Sie diesen Wert auf 802 fest.
- IETF 81 (Tunnel Private Group ID) (IETF 81 (Tunnel Private Group ID)): Legen Sie diese VLAN-ID fest.

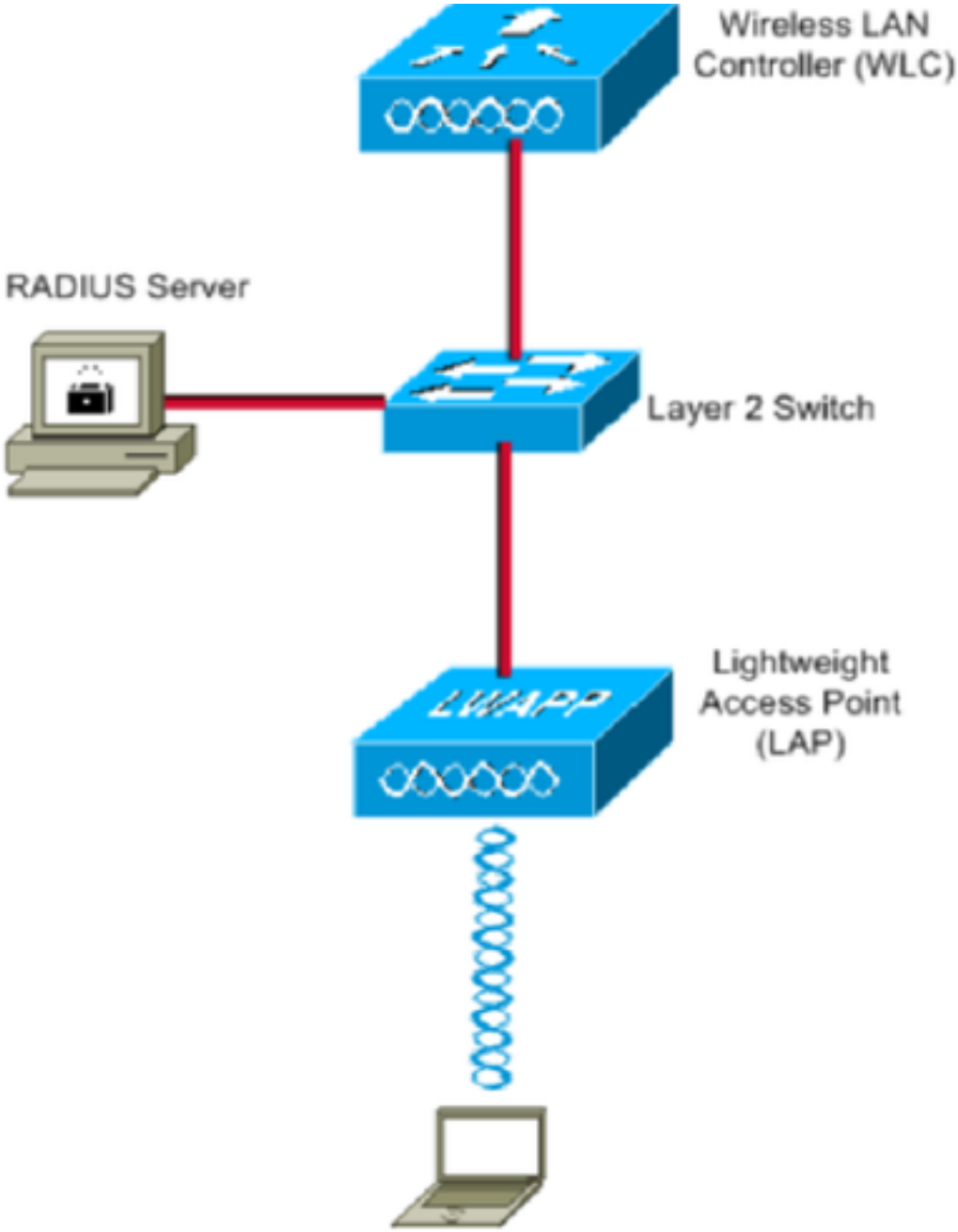
Die VLAN-ID beträgt 12 Bit und hat einen Wert zwischen 1 und 4094 (einschließlich). Da die Tunnel-Private-Group-ID vom Typ string ist, wie in RFC2868 für die Verwendung mit IEEE 802.1X definiert, wird der VLAN-ID-Integer-Wert als Zeichenfolge codiert. Wenn diese Tunnelattribute gesendet werden, müssen Sie sie im Feld Tag eingeben.

Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Dies sind die Konfigurationsdetails der in diesem Diagramm verwendeten Komponenten:

- Die IP-Adresse des Cisco ISE-Servers (RADIUS) lautet 10.10.1.24.
- Die Management-Schnittstellenadresse des WLC lautet 10.10.1.17.
- Der interne DHCP-Server des Controllers wird verwendet, um die IP-Adresse Wireless-Clients zuzuweisen.
- In diesem Dokument wird 802.1x mit PEAP als Sicherheitsmechanismus verwendet.
- VLAN102 wird in dieser Konfiguration verwendet. Der Benutzername jonathga-102 wird so konfiguriert, dass er vom RADIUS-Server in das VLAN102 eingegeben wird.

Konfigurationsschritte

Diese Konfiguration ist in drei Kategorien unterteilt:

- Cisco ISE-Konfiguration.
- Konfigurieren des Switches für mehrere VLANs

- Catalyst 9800 WLC-Konfiguration

Cisco ISE-Konfiguration

Für diese Konfiguration sind folgende Schritte erforderlich:

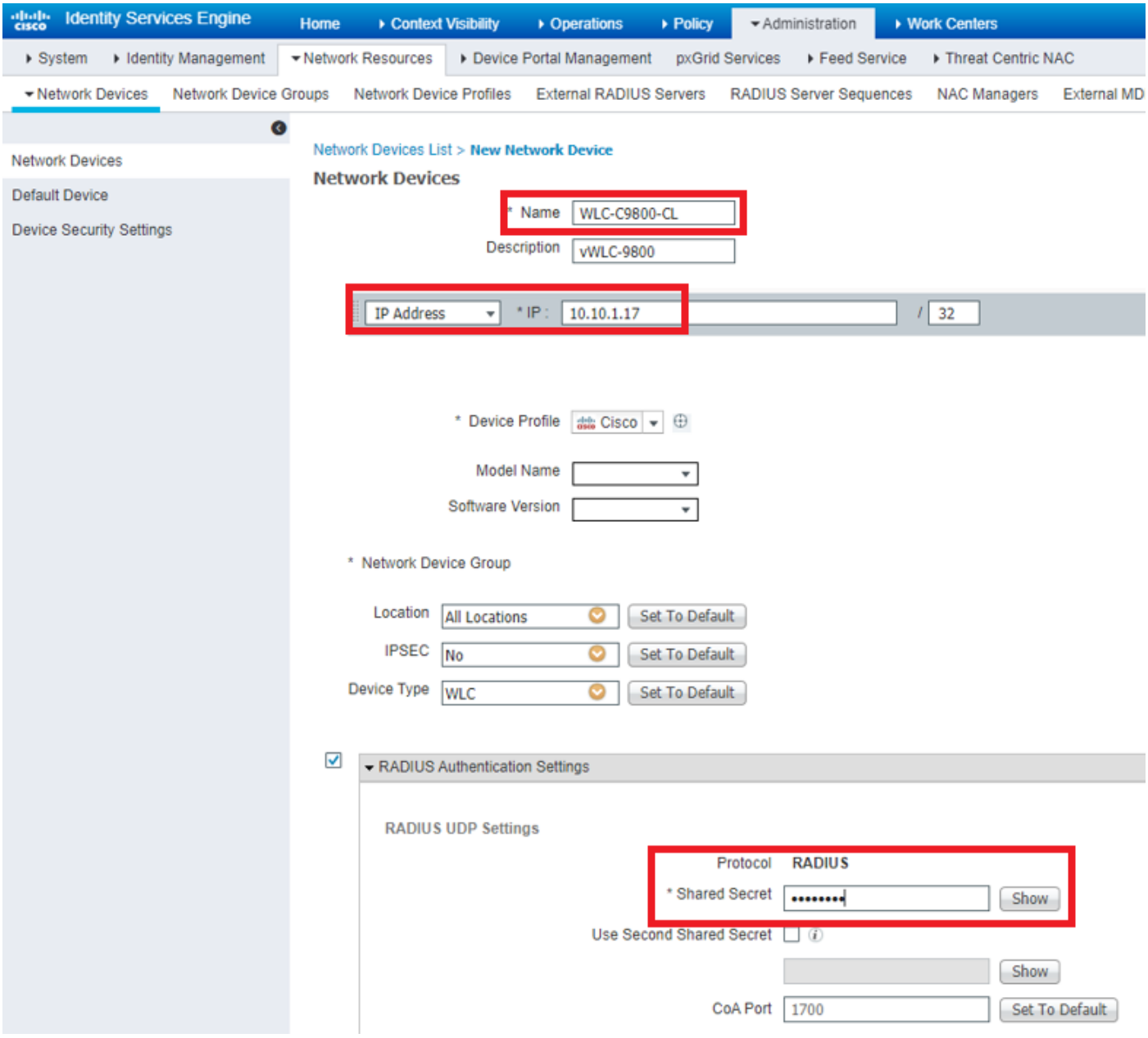
- Konfigurieren Sie den Catalyst WLC als AAA-Client auf dem Cisco ISE-Server.
- Konfigurieren Sie interne Benutzer auf der Cisco ISE.
- Konfigurieren Sie die RADIUS (IETF)-Attribute, die für die dynamische VLAN-Zuweisung auf der Cisco ISE verwendet werden.

Schritt 1: Konfigurieren des Catalyst WLC als AAA-Client auf dem Cisco ISE-Server

In diesem Verfahren wird erläutert, wie der WLC als AAA-Client auf dem ISE-Server hinzugefügt wird, sodass der WLC die Benutzeranmeldeinformationen an die ISE übergeben kann.

Führen Sie diese Schritte aus:

1. Navigieren Sie in der ISE-GUI zu **Administration > Network Resources > Network Devices**und wählen Sie **Add**.
2. Schließen Sie die Konfiguration mit der IP-Adresse für die WLC-Verwaltung und dem gemeinsamen geheimen RADIUS-Schlüssel zwischen WLC und ISE ab, wie im Bild gezeigt:

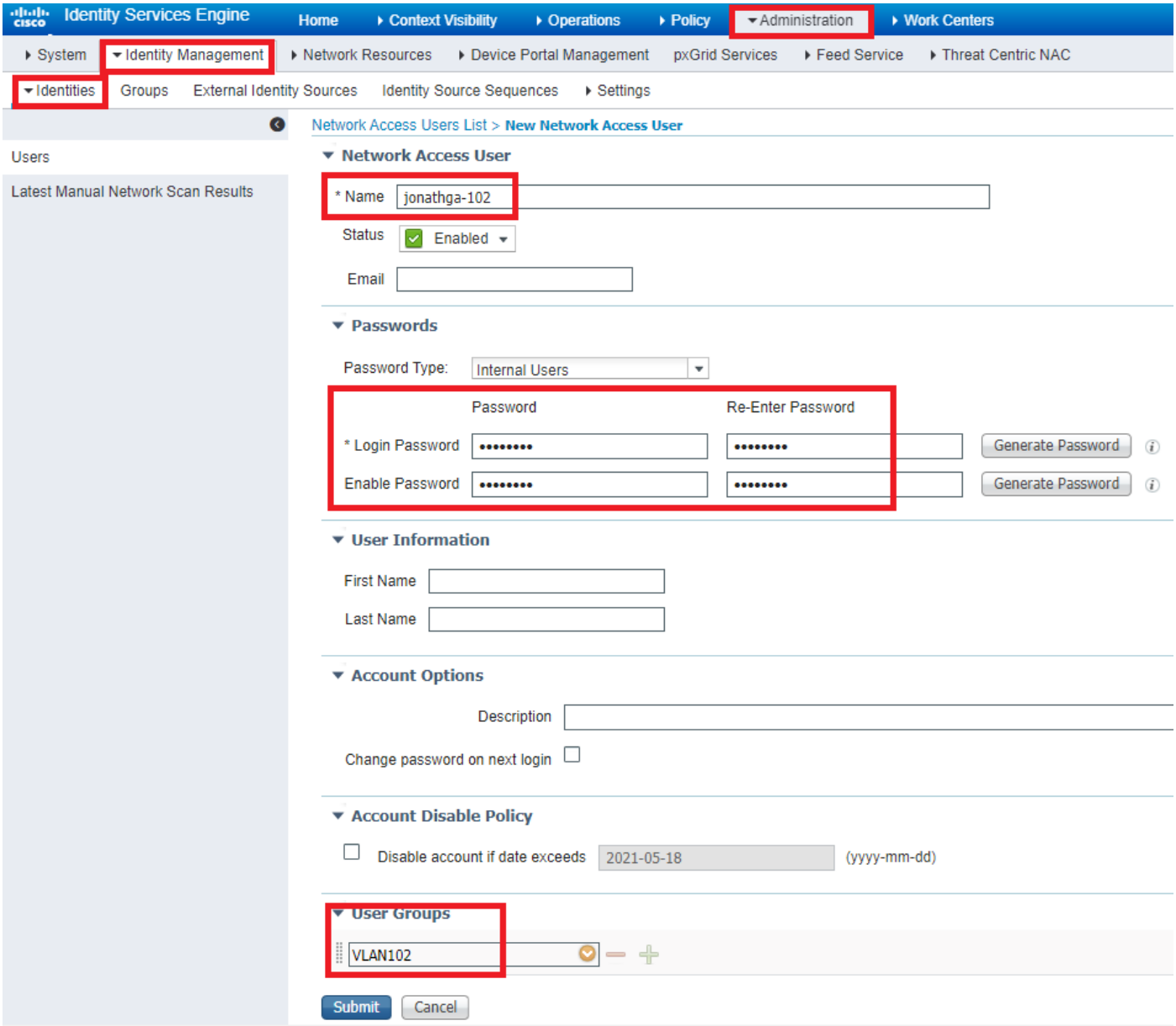


Schritt 2: Konfigurieren interner Benutzer für die Cisco ISE

In diesem Verfahren wird erläutert, wie Sie die Benutzer zur internen Benutzerdatenbank der Cisco ISE hinzufügen.

Führen Sie diese Schritte aus:

1. Navigieren Sie in der ISE-GUI zu **Administration > Identity Management > Identities** und wählen Sie **Add**.
2. Schließen Sie die Konfiguration mit Benutzername, Kennwort und Benutzergruppe wie im Bild gezeigt ab:

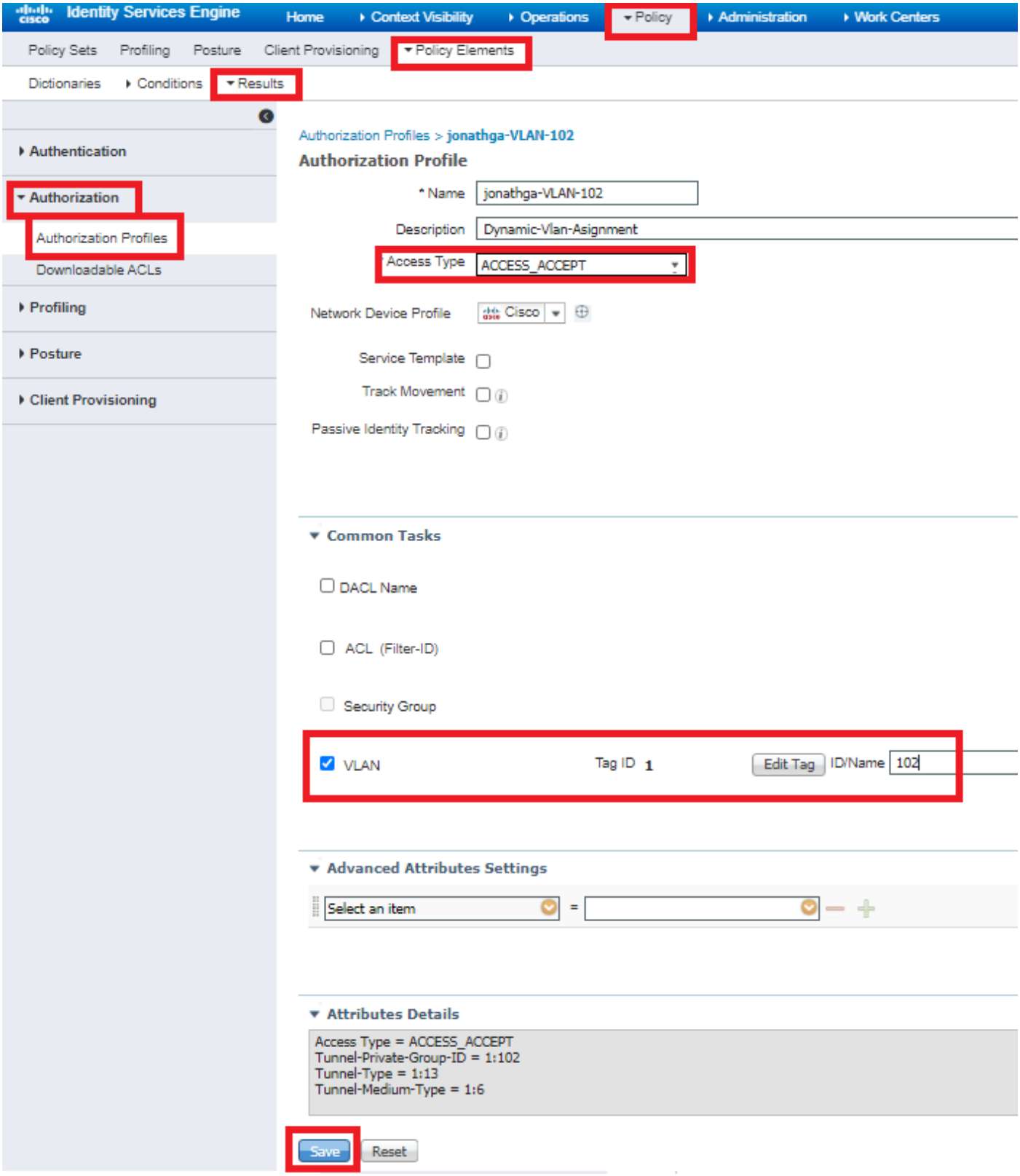


Schritt 3: Konfigurieren der RADIUS (IETF)-Attribute für die dynamische VLAN-Zuweisung

In diesem Verfahren wird erläutert, wie Sie ein Autorisierungsprofil und eine Authentifizierungsrichtlinie für Wireless-Benutzer erstellen.

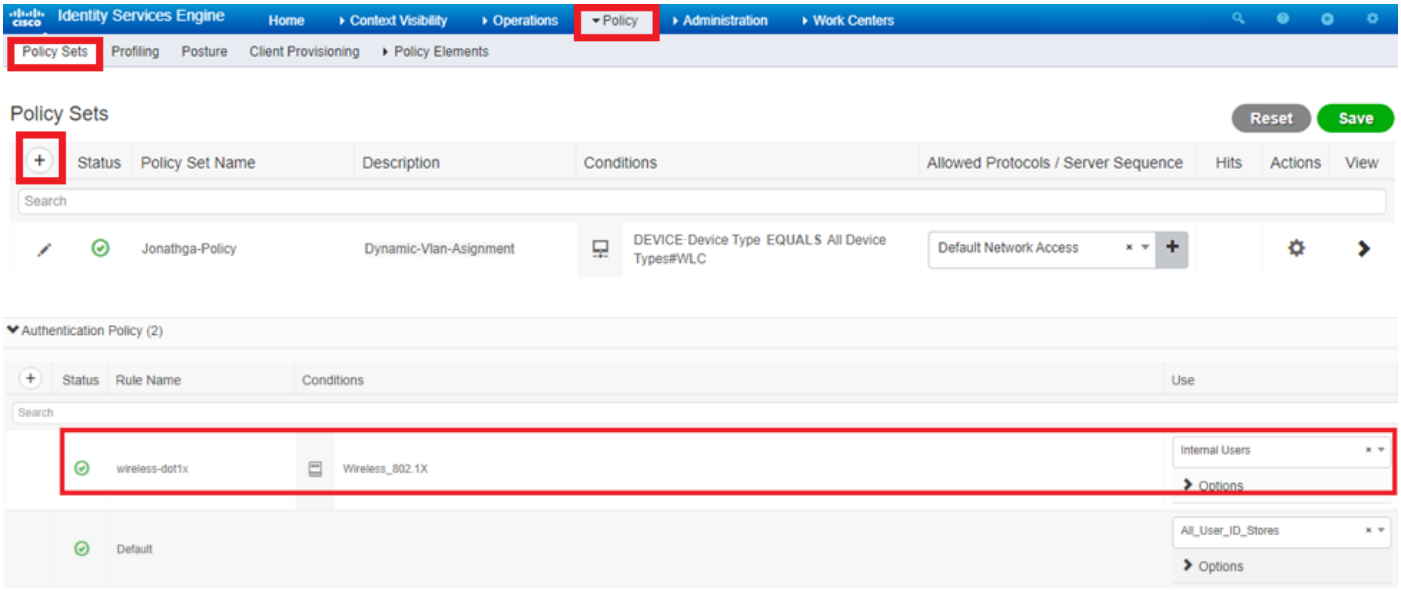
Führen Sie diese Schritte aus:

1. Navigieren Sie in der ISE-GUI zu **Policy > Policy Elements > Results > Authorization > Authorization profiles** und wählen Sie **Add** um ein neues Profil zu erstellen.
2. Vervollständigen Sie die Konfiguration des Autorisierungsprofils mit VLAN-Informationen für die entsprechende Gruppe. Dieses Bild zeigt **jonathga-VLAN-102** Gruppenkonfigurationseinstellungen.



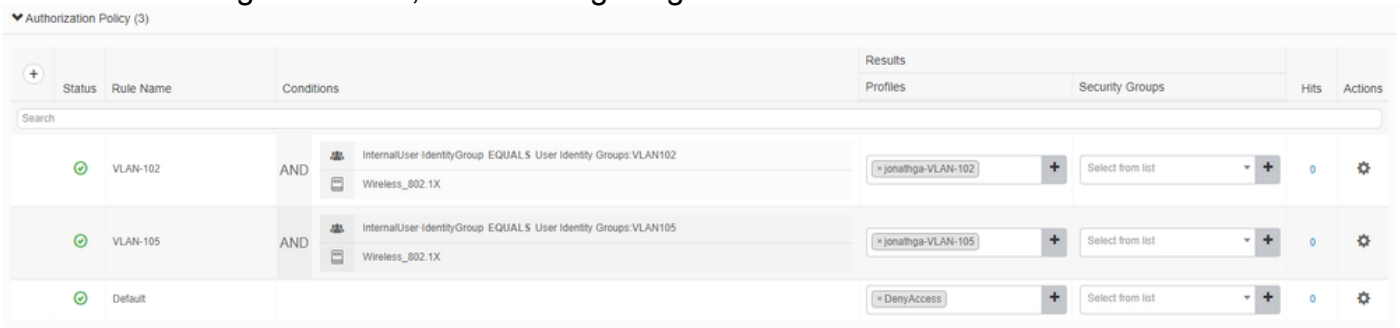
Nach der Konfiguration der Autorisierungsprofile muss eine Authentifizierungsrichtlinie für Wireless-Benutzer erstellt werden. Sie können eine neue **Custom** Richtlinien erstellen oder ändern **Default** Policy-Set. In diesem Beispiel wird ein benutzerdefiniertes Profil erstellt.

3. Navigieren zu **Policy > Policy Sets** und wählen Sie **Add** So erstellen Sie eine neue Richtlinie, wie im Bild gezeigt:



Jetzt müssen Sie Autorisierungsrichtlinien für Benutzer erstellen, um ein entsprechendes Autorisierungsprofil basierend auf der Gruppenmitgliedschaft zuzuweisen.

5. Öffnen Sie **Authorization policy** -Abschnitt erstellen und Richtlinien erstellen, um diese Anforderung zu erfüllen, wie im Bild gezeigt:



Switch für mehrere VLANs konfigurieren

Um mehrere VLANs über den Switch zu ermöglichen, müssen Sie die folgenden Befehle ausführen, um den mit dem Controller verbundenen Switch-Port zu konfigurieren:

```
Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation dot1q
```

> **Anmerkung:** Standardmäßig lassen die meisten Switches alle auf diesem Switch erstellten VLANs über den Trunk-Port zu. Wenn ein kabelgebundenes Netzwerk mit dem Switch verbunden ist, kann diese Konfiguration auf den Switch-Port angewendet werden, der mit dem kabelgebundenen Netzwerk verbunden ist. Dies ermöglicht die Kommunikation zwischen den gleichen VLANs im kabelgebundenen und Wireless-Netzwerk.

Catalyst 9800 WLC-Konfiguration

Für diese Konfiguration sind folgende Schritte erforderlich:

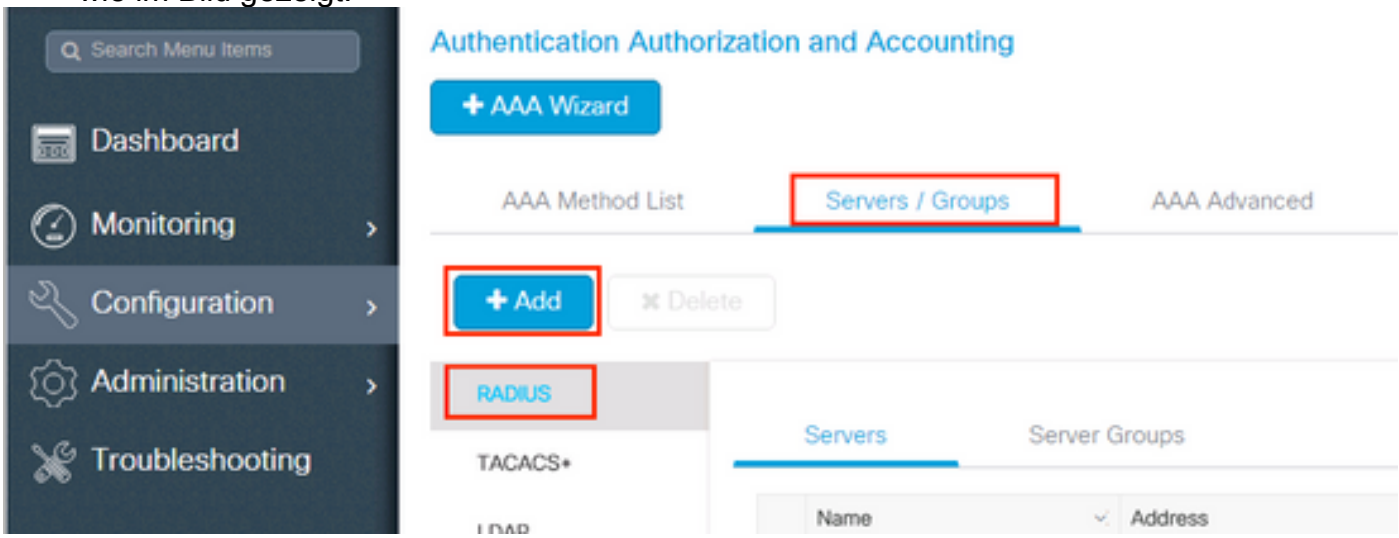
- Konfigurieren Sie den WLC mit den Details des Authentifizierungsservers.
- Konfigurieren der VLANs
- Konfigurieren der WLANs (SSID)
- Konfigurieren Sie das Richtlinienprofil.
- Konfigurieren Sie das Richtlinien-Tag.
- Weisen Sie einem Access Point den Policy-Tag zu.

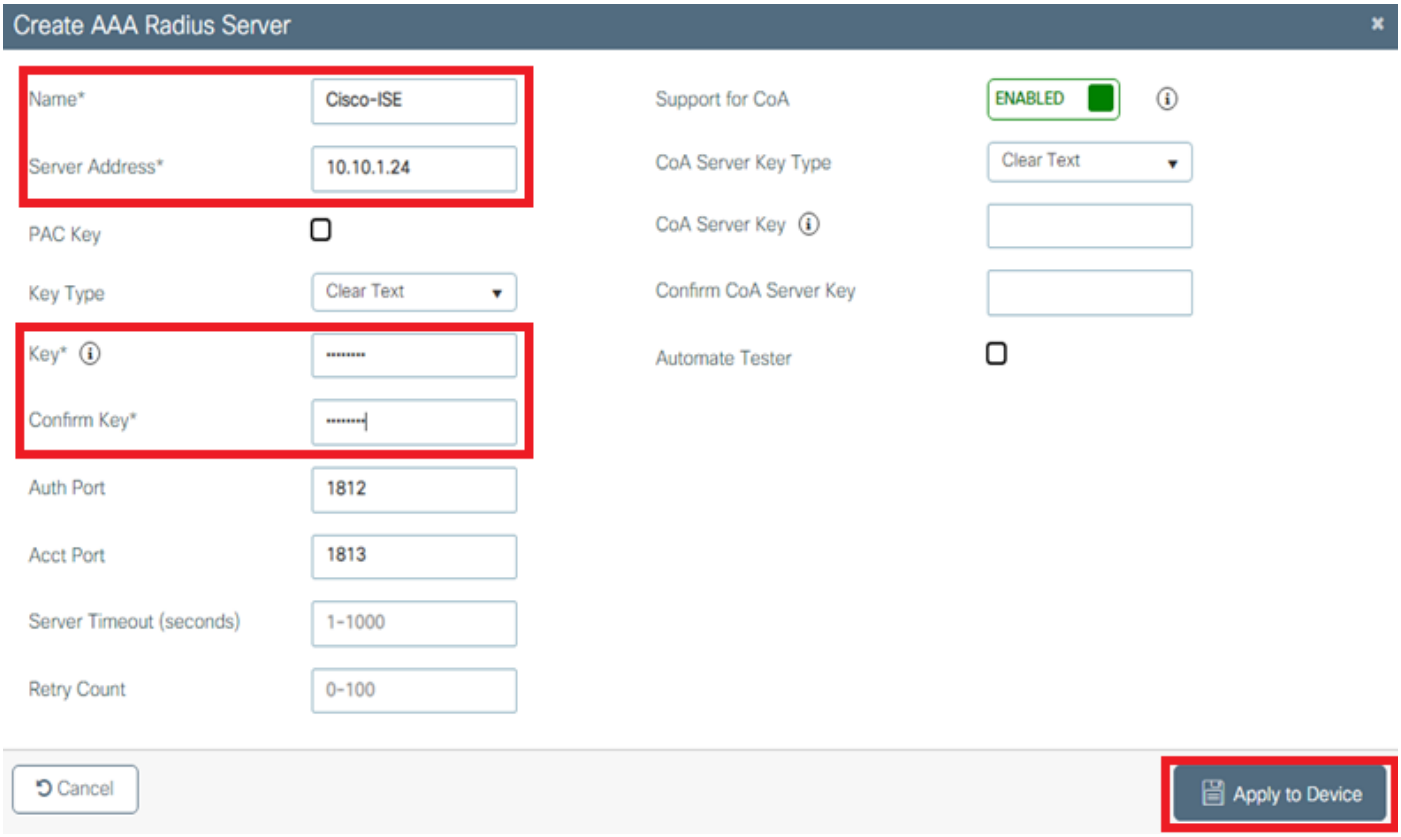
Schritt 1: Konfigurieren des WLC mit den Details des Authentifizierungsservers

Der WLC muss so konfiguriert werden, dass er mit dem RADIUS-Server kommunizieren kann, um die Clients zu authentifizieren.

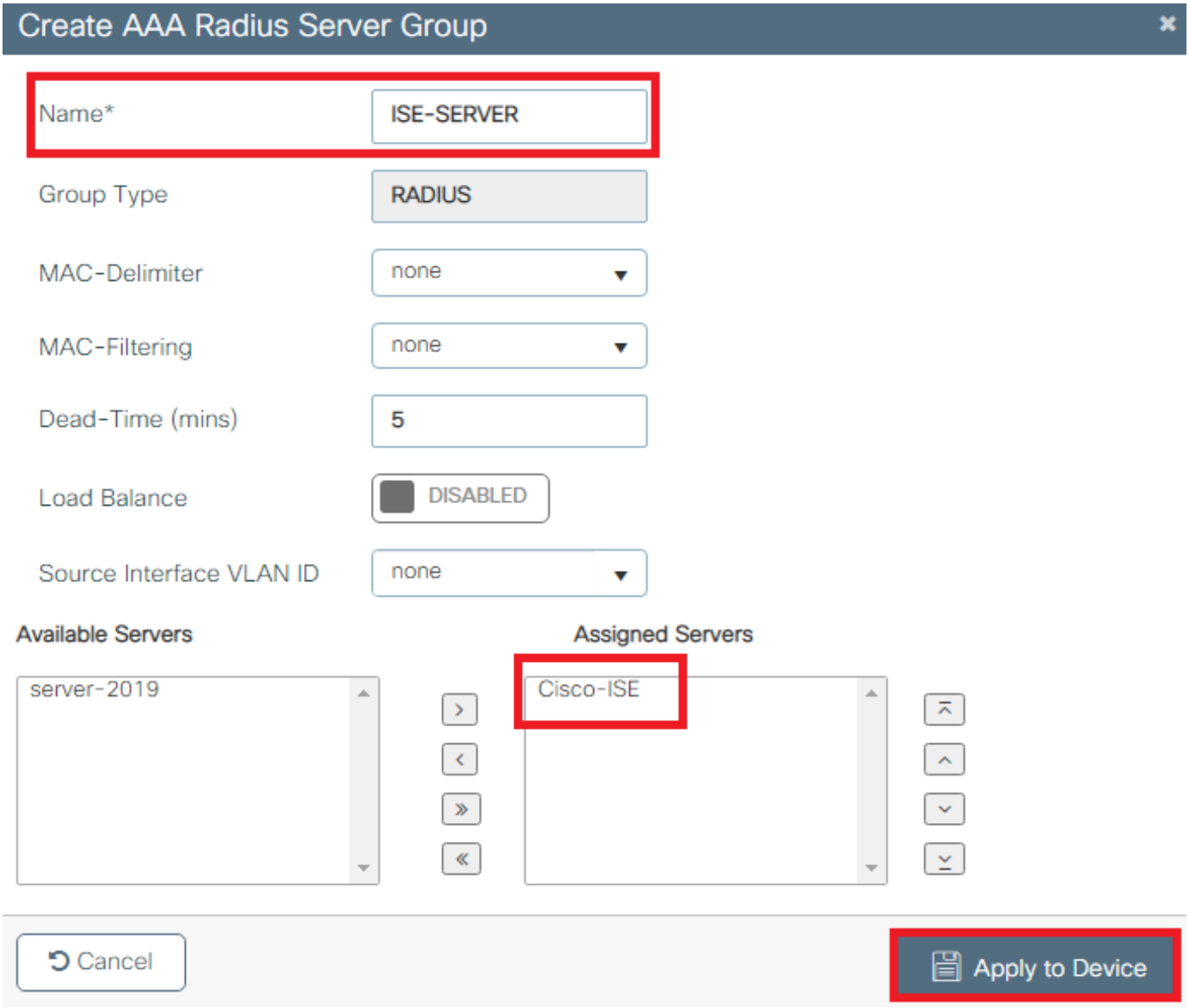
Führen Sie diese Schritte aus:

1. Navigieren Sie in der Benutzeroberfläche des Controllers zu **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** und geben Sie die RADIUS-Serverinformationen ein, wie im Bild gezeigt:

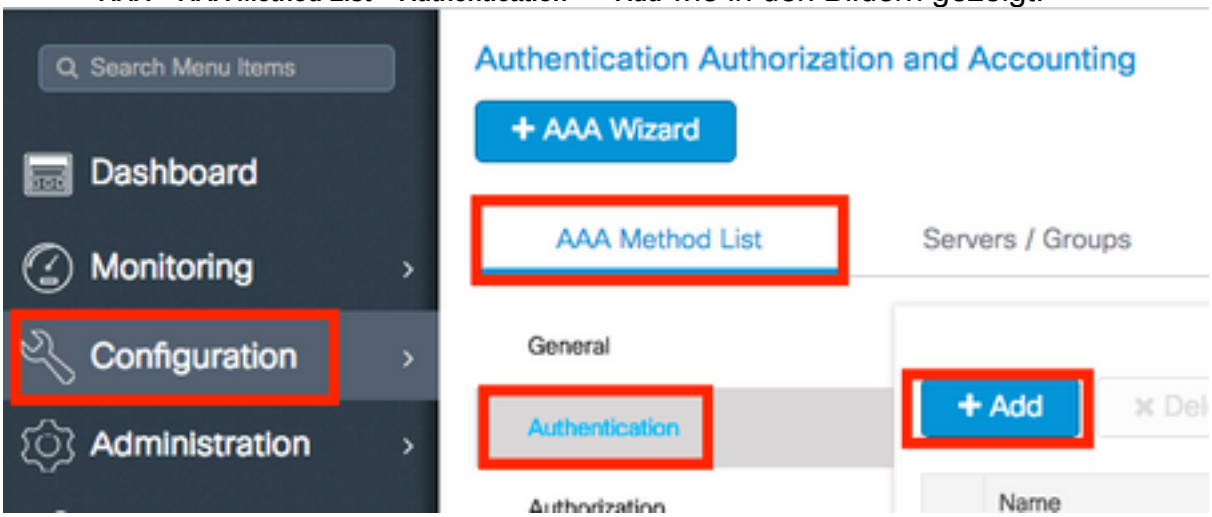


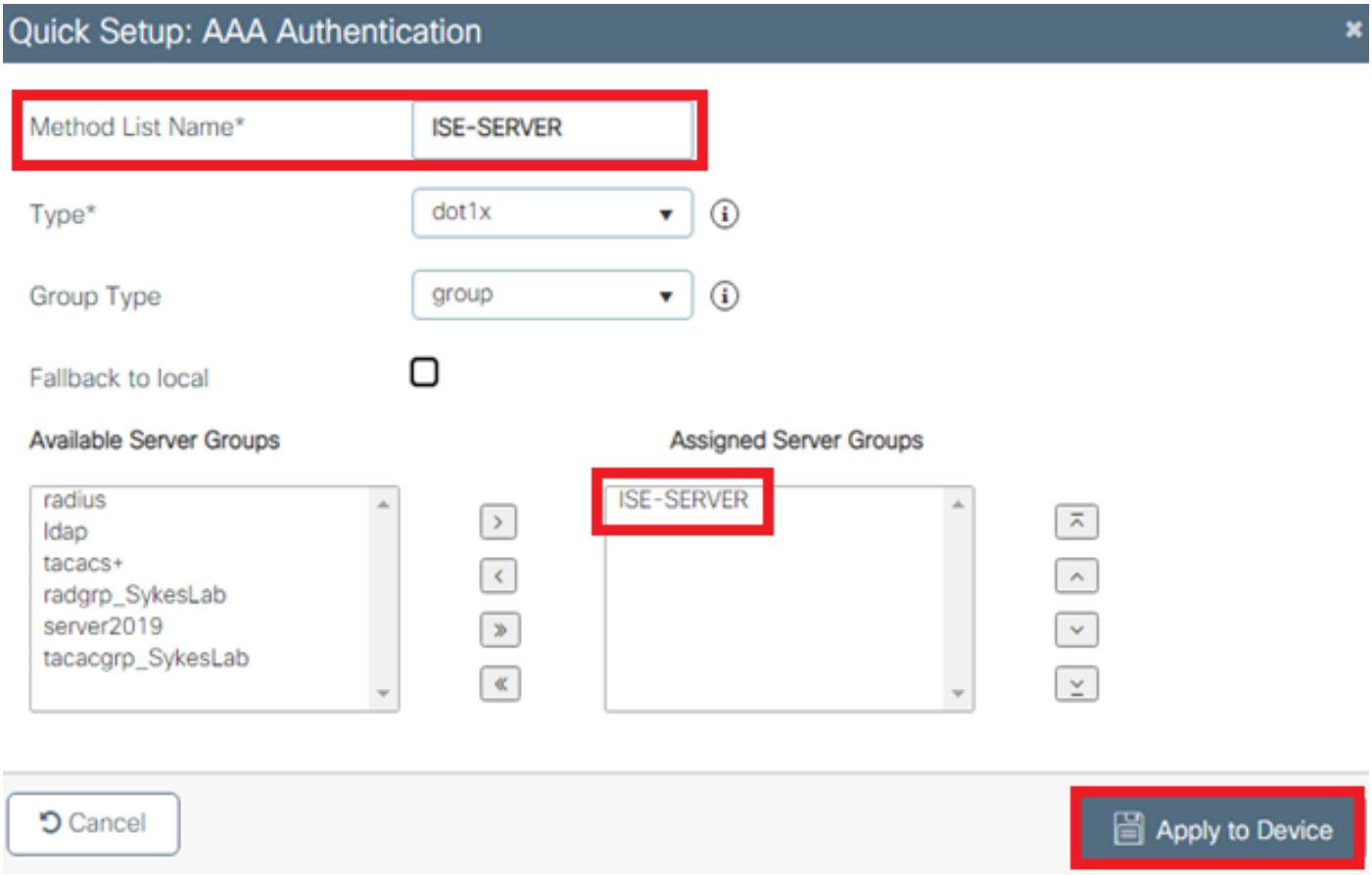


2. Um den RADIUS-Server einer RADIUS-Gruppe hinzuzufügen, navigieren Sie zu **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** wie im Bild gezeigt:



3. Um eine Authentifizierungsmethodenliste zu erstellen, navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authentication > + Add** wie in den Bildern gezeigt:



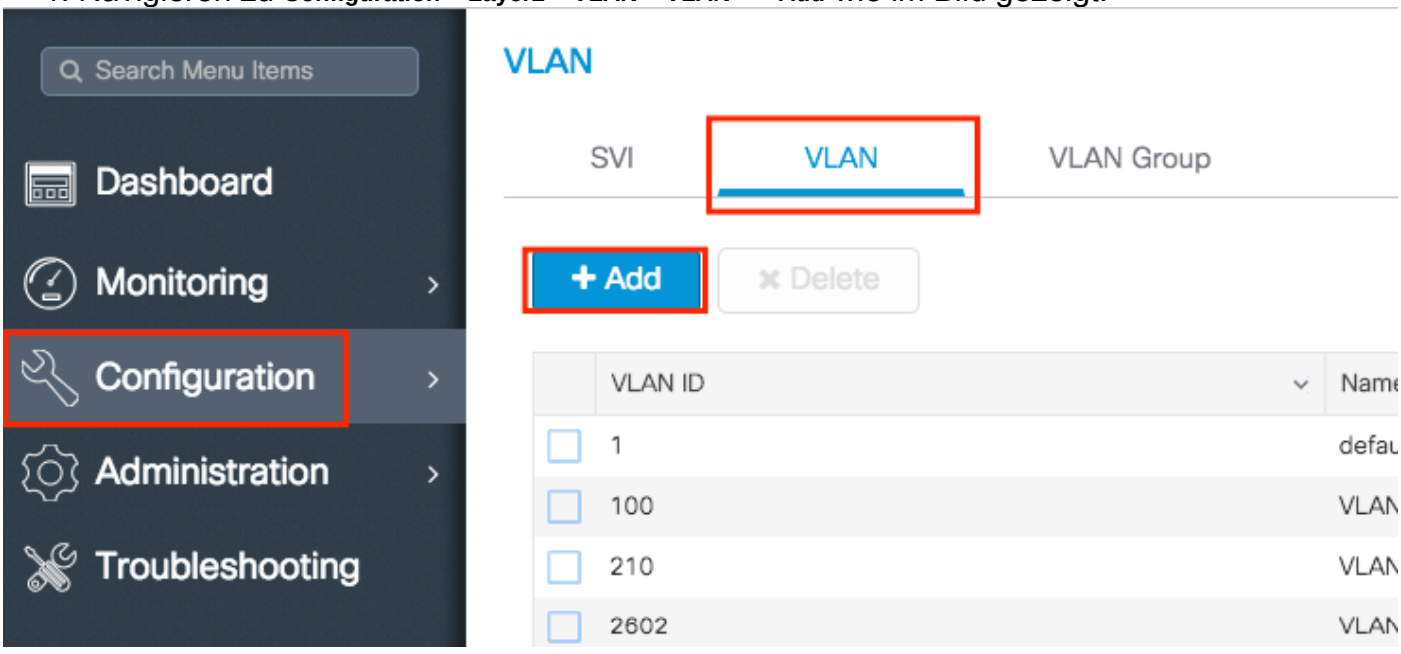


Schritt 2: Konfigurieren der VLANs

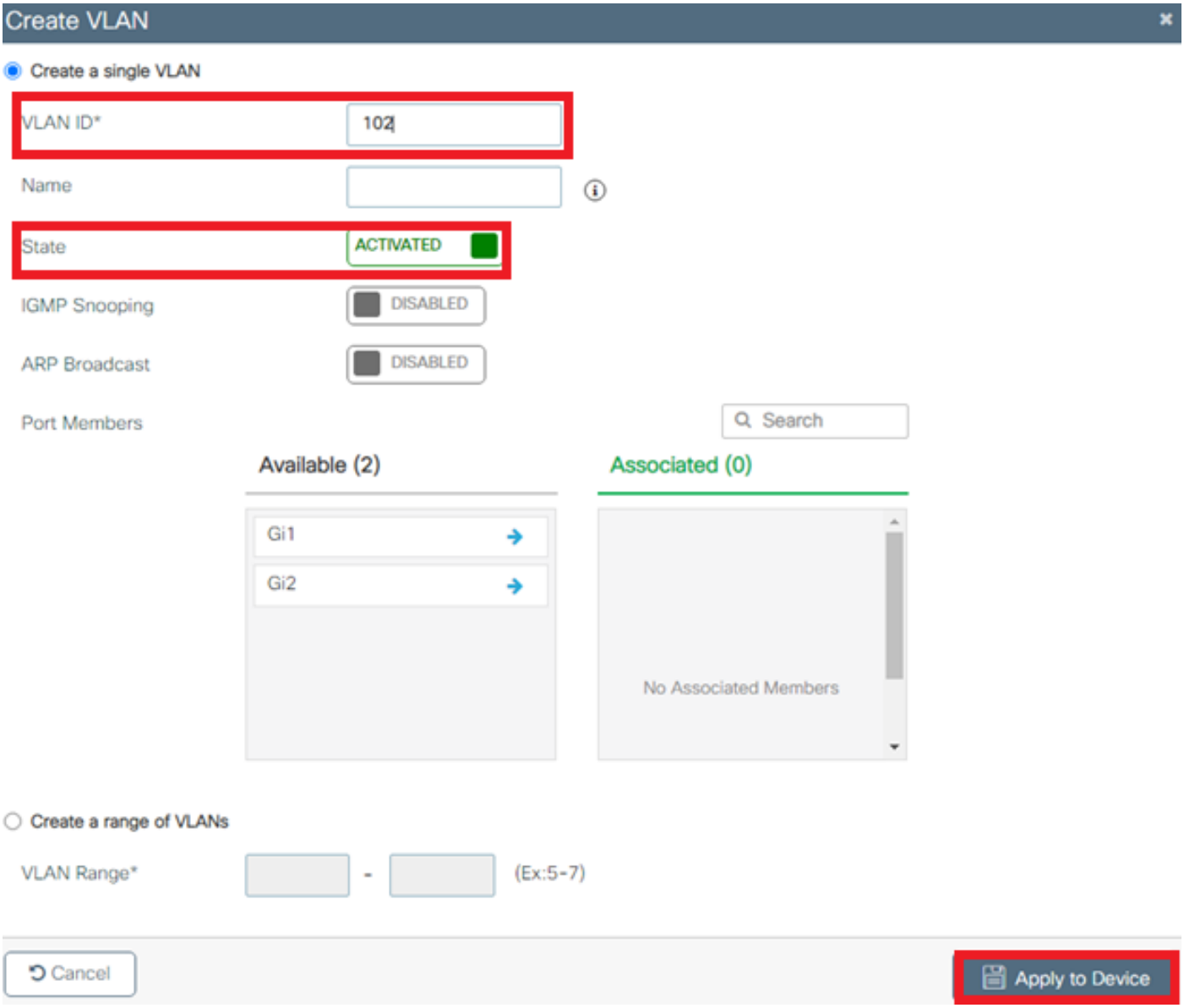
In diesem Verfahren wird die Konfiguration von VLANs auf dem Catalyst 9800 WLC erläutert. Wie bereits in diesem Dokument erläutert, muss die im Tunnel-Private-Group-ID-Attribut des RADIUS-Servers angegebene VLAN-ID auch im WLC vorhanden sein.

Im Beispiel wird der Benutzer jonathga-102 mit dem **Tunnel-Private-Group ID of 102 (VLAN =102)** auf dem RADIUS-Server.

1. Navigieren zu **Configuration > Layer2 > VLAN > VLAN > + Add** wie im Bild gezeigt:



2. Geben Sie die erforderlichen Informationen ein, wie im Bild gezeigt:



Anmerkung: Wenn Sie keinen Namen angeben, wird dem VLAN automatisch der Name VLANXXXX zugewiesen, wobei XXXX für die VLAN-ID steht.

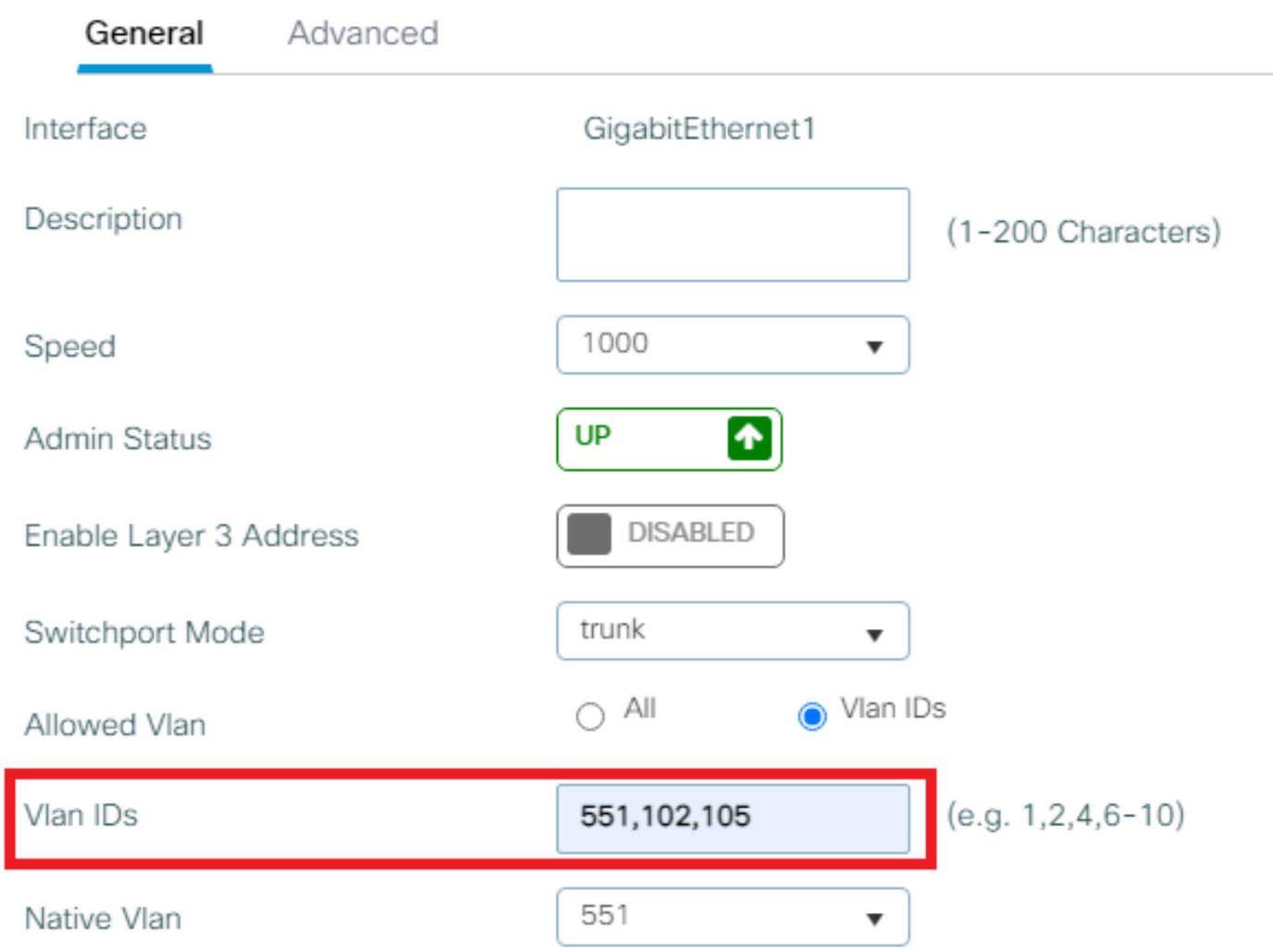
Wiederholen Sie die Schritte 1 und 2 für alle erforderlichen VLANs. Danach können Sie mit Schritt 3 fortfahren.

3. Überprüfen Sie, ob die VLANs in Ihren Datenschnittstellen zulässig sind. Wenn ein Port-Channel verwendet wird, navigieren Sie zu **Configuration > Interface > Logical > PortChannel name > General**. Wenn die Konfiguration als **Allowed VLAN = All** die Konfiguration abgeschlossen ist. Wenn Sie Folgendes sehen: **Allowed VLAN = VLANs IDs**, fügen Sie die erforderlichen VLANs hinzu, und wählen Sie anschließend **Update & Apply to Device**.Wenn kein Port-Channel verwendet wird, navigieren Sie zu **Configuration > Interface > Ethernet > Interface Name > General**. Wenn die Konfiguration als **Allowed VLAN = All** die Konfiguration abgeschlossen ist. Wenn Sie Folgendes sehen: **Allowed VLAN = VLANs IDs**, fügen Sie die erforderlichen VLANs hinzu, und wählen Sie anschließend **Update & Apply to Device**.

Diese Abbildungen zeigen die Konfiguration für die Schnittstelleneinrichtung, wenn Sie Alle oder bestimmte VLAN-IDs verwenden.

General Advanced

Interface	GigabitEthernet3
Description	(1-200 Characters)
Admin Status	UP
Port Fast	disable
Enable Layer 3 Address	DISABLED
Switchport Mode	trunk
Allowed Vlan	All / Vlan IDs
Native Vlan	

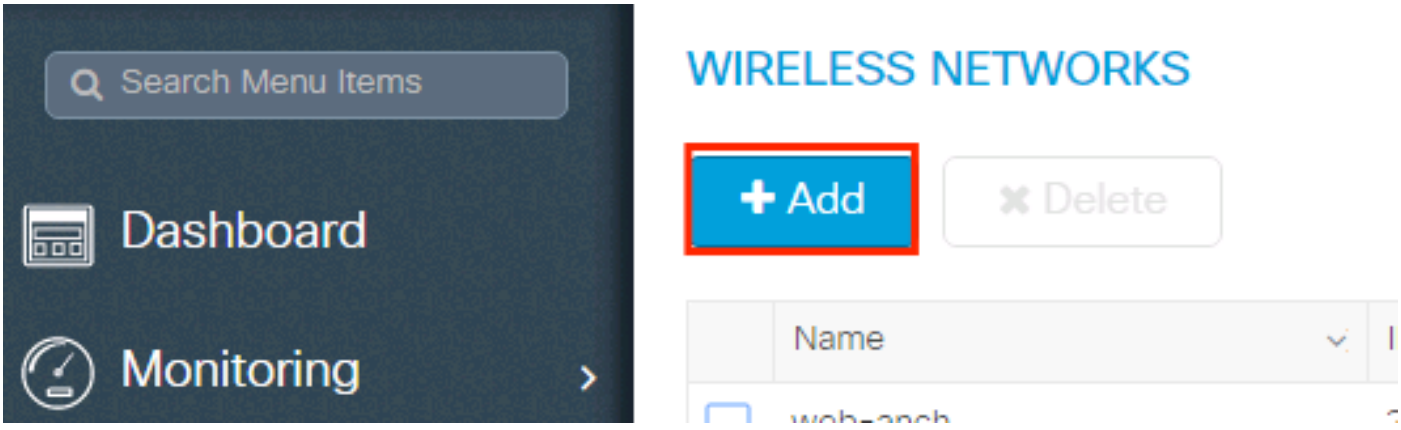


Schritt 3: Konfigurieren der WLANs (SSID)

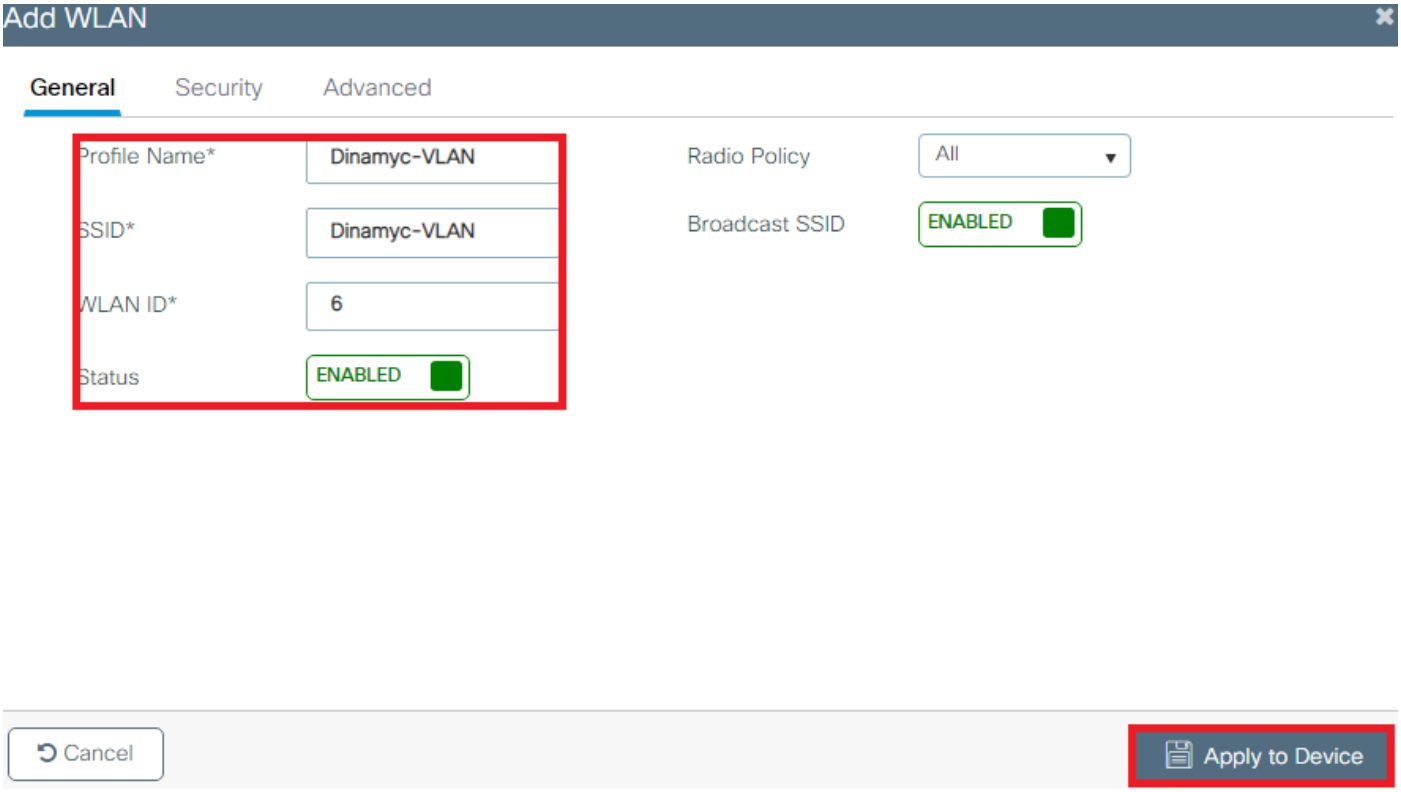
In diesem Verfahren wird erläutert, wie die WLANs im WLC konfiguriert werden.

Führen Sie diese Schritte aus:

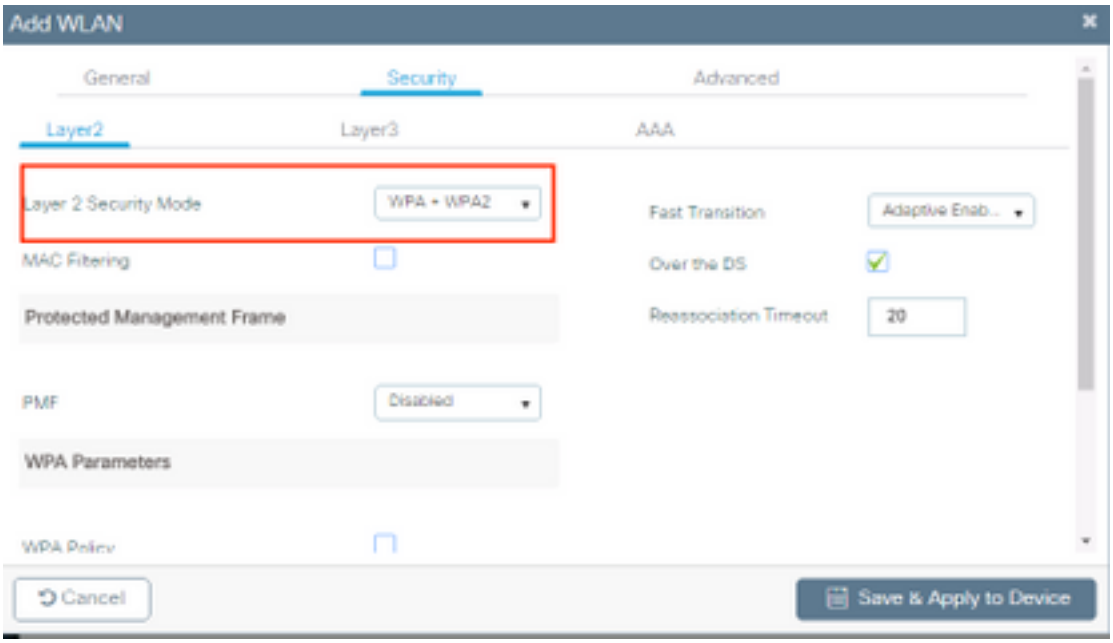
1. So erstellen Sie das WLAN. Navigieren zu **Configuration > Wireless > WLANs > + Add** und konfigurieren Sie das Netzwerk nach Bedarf, wie im Bild gezeigt:

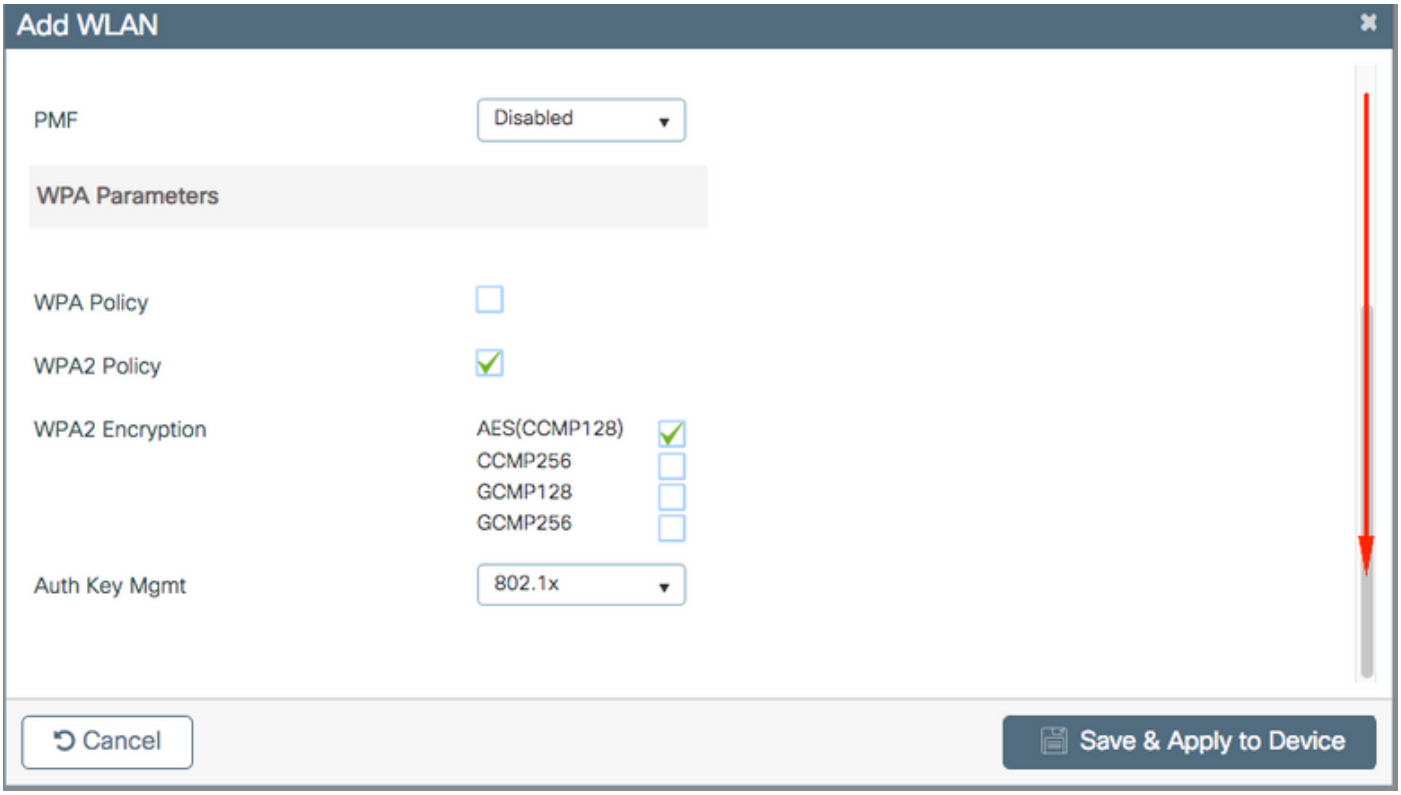


2. Geben Sie die WLAN-Informationen ein, wie im Bild gezeigt:

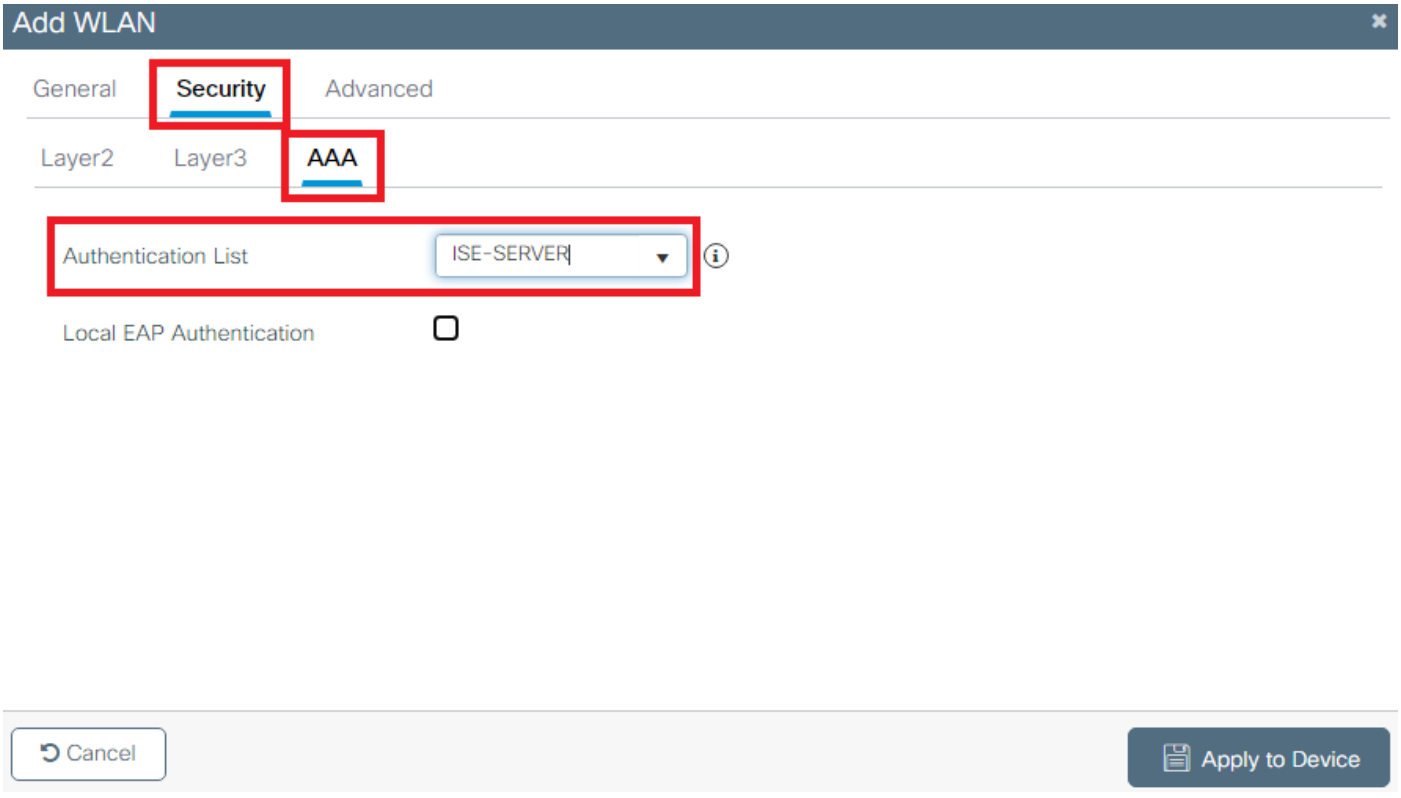


3. Navigieren zu **Security** und wählen Sie die gewünschte Sicherheitsmethode aus. In diesem Fall ist WPA2 + 802.1x wie in den Bildern gezeigt:





Von**Security > AAA** auf, wählen Sie die in Schritt 3 erstellte Authentifizierungsmethode aus. **Configure the WLC with the Details of the Authentication Server** wie im Bild gezeigt:



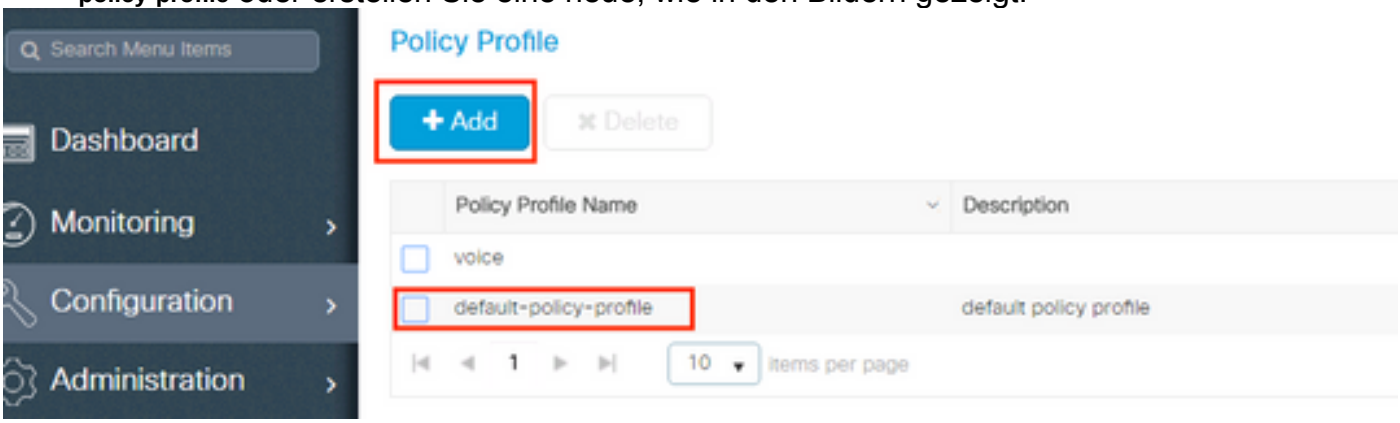
Schritt 4: Konfigurieren des Richtlinienprofils

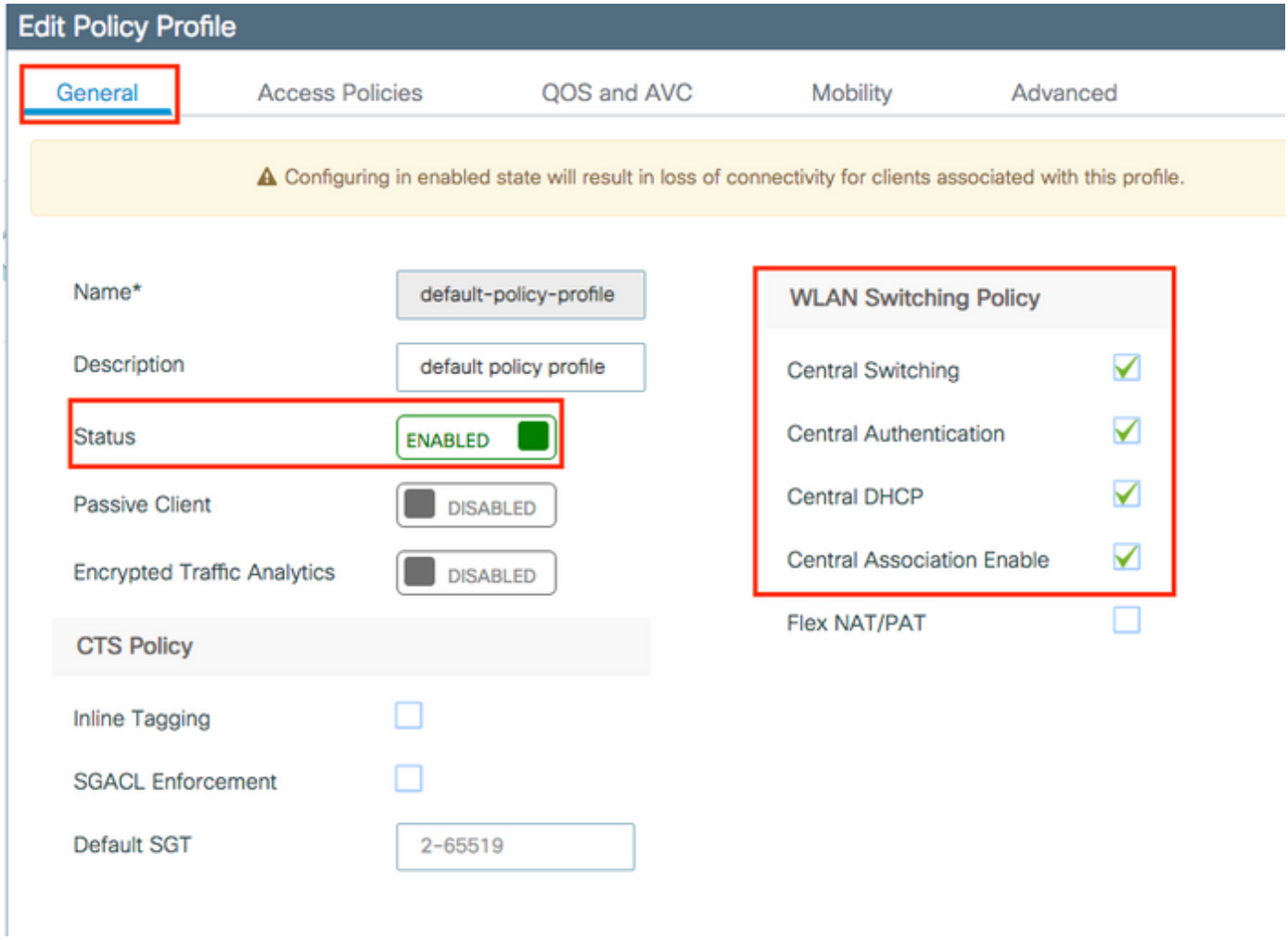
In diesem Verfahren wird erläutert, wie das Richtlinienprofil im WLC konfiguriert wird.

Führen Sie diese Schritte aus:

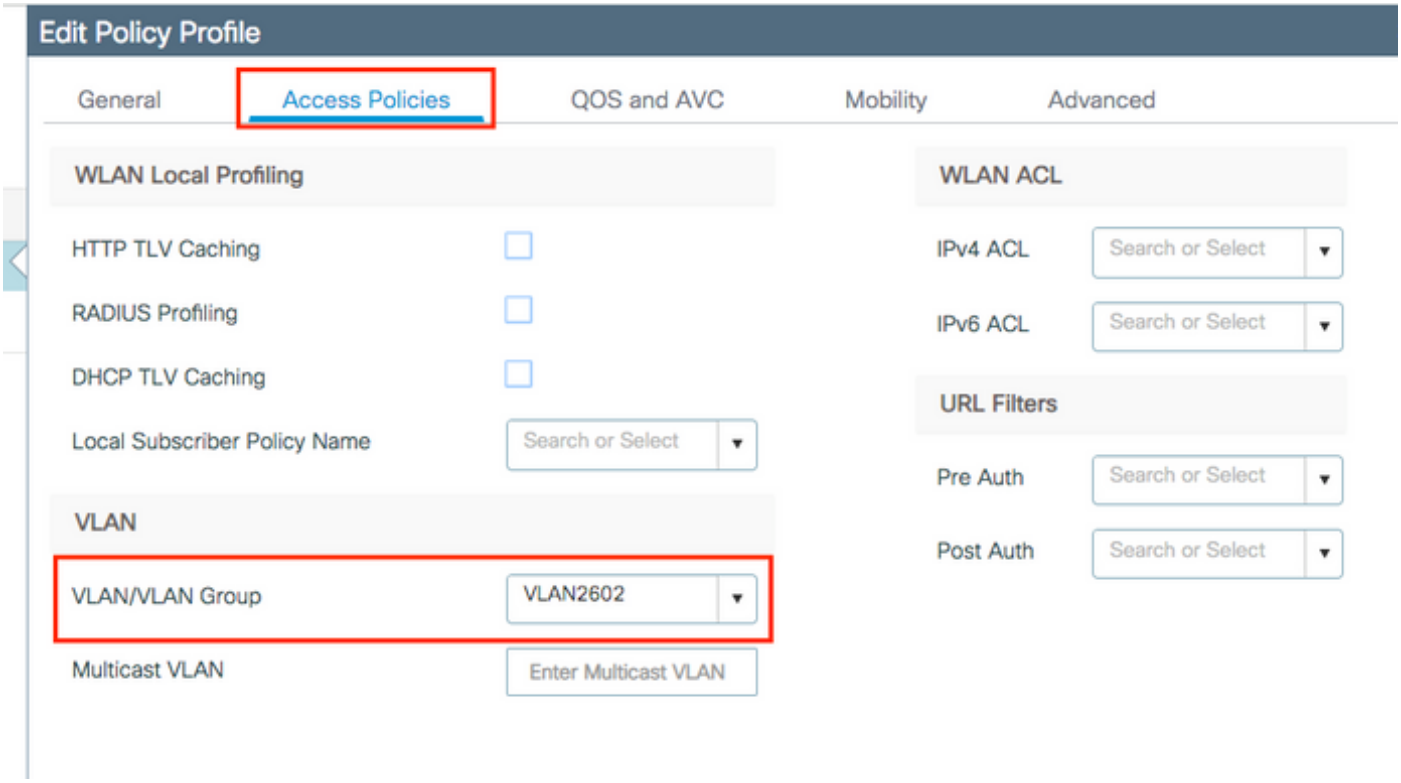
1. Navigieren zu **Configuration > Tags & Profiles > Policy Profile** und konfigurieren Sie entweder **default-**

policy-profile oder erstellen Sie eine neue, wie in den Bildern gezeigt:



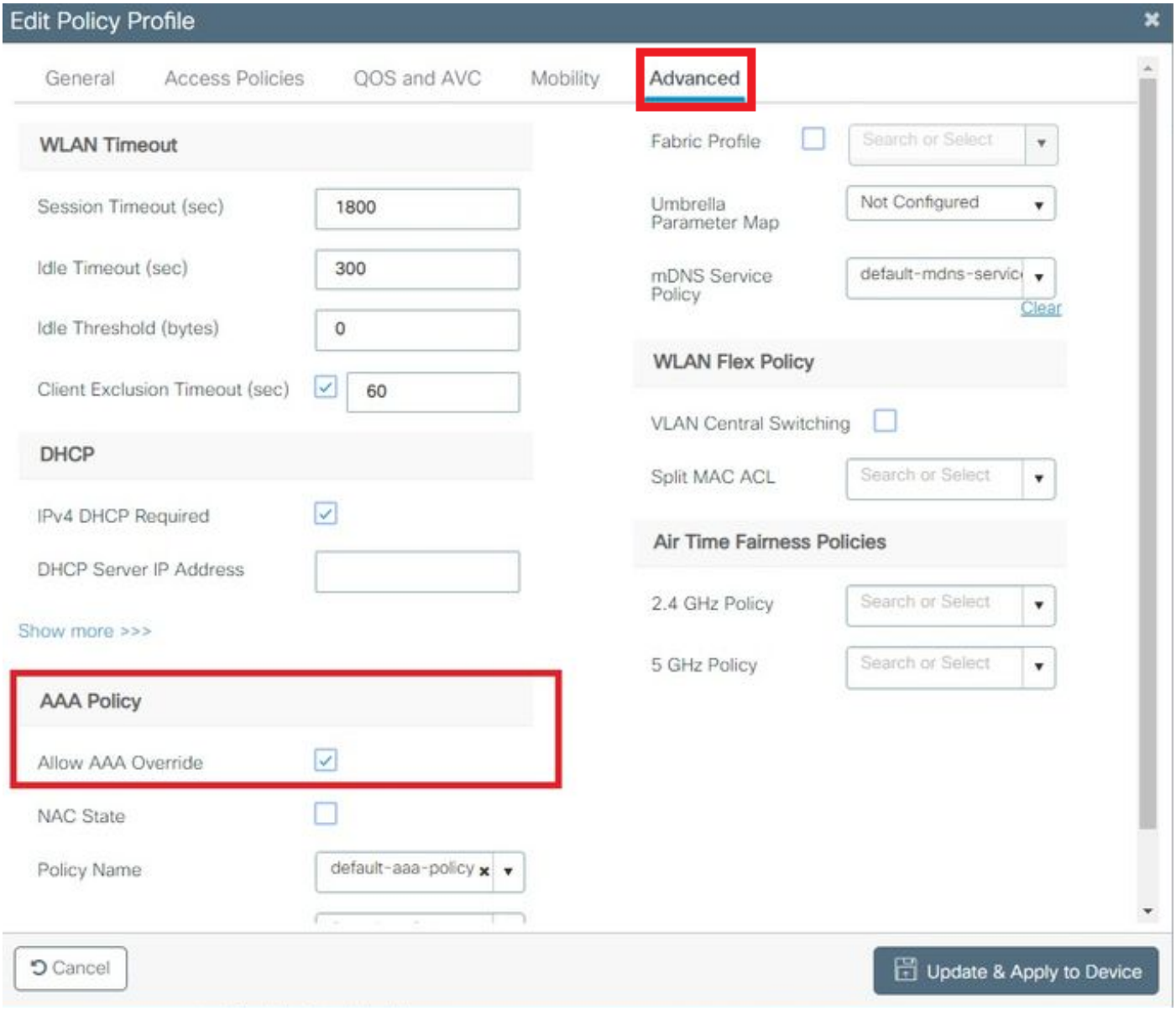


2. Von der **Access Policies** Registerkarte weisen Sie das VLAN zu, dem die Wireless-Clients zugewiesen sind, wenn sie standardmäßig eine Verbindung zu diesem WLAN herstellen, wie im Bild gezeigt:



Anmerkung: Im angegebenen Beispiel ist es Aufgabe des RADIUS-Servers, nach erfolgreicher Authentifizierung einem bestimmten VLAN einen Wireless-Client zuzuweisen. Daher kann das im Richtlinienprofil konfigurierte VLAN ein Black-Hole-VLAN sein. Der RADIUS-Server überschreibt diese Zuordnung und weist den Benutzer, der über dieses WLAN erfolgt, dem VLAN zu, das im Feld "Tunnel-Group-Private-ID" des RADIUS-Servers angegeben ist.

3. Von der **Advance** aktivieren, aktivieren Sie **Allow AAA Override** Aktivieren Sie das Kontrollkästchen, um die WLC-Konfiguration zu überschreiben, wenn der RADIUS-Server die Attribute zurückgibt, die erforderlich sind, um den Client wie im Bild gezeigt im richtigen VLAN zu platzieren:

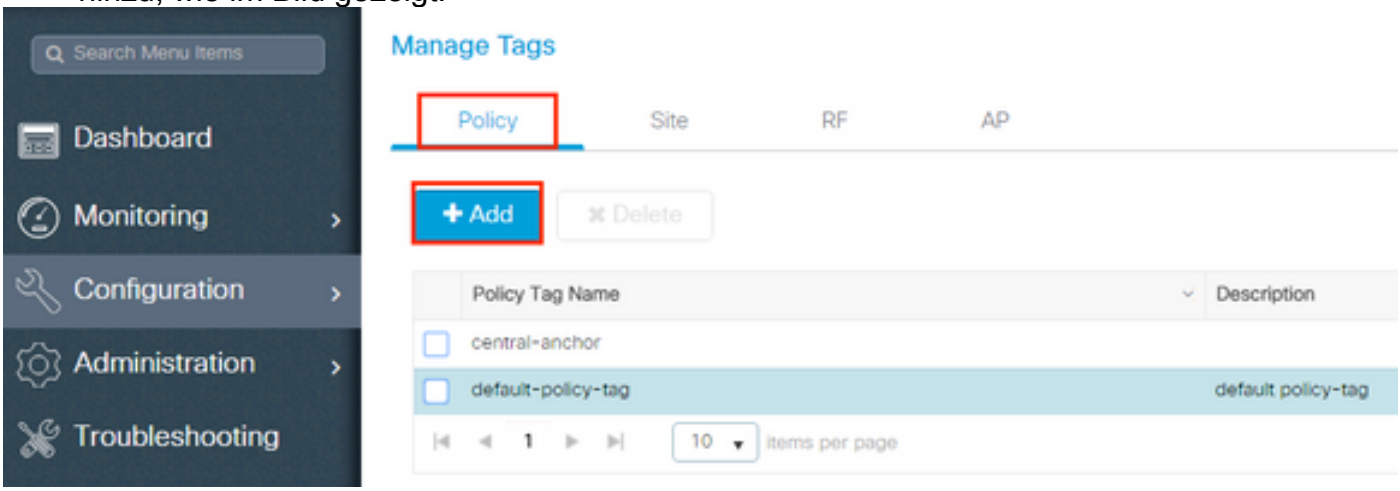


Schritt 5: Konfigurieren der Richtlinien-Tag

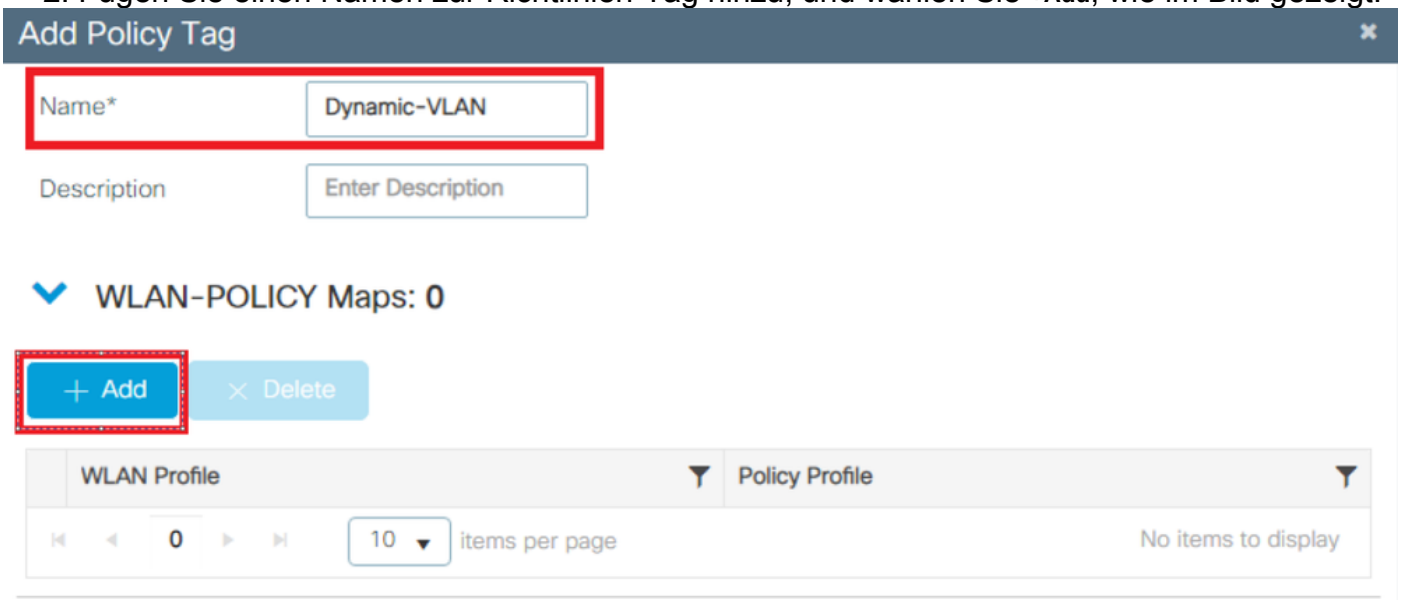
In diesem Verfahren wird erläutert, wie das Policy-Tag im WLC konfiguriert wird.

Führen Sie diese Schritte aus:

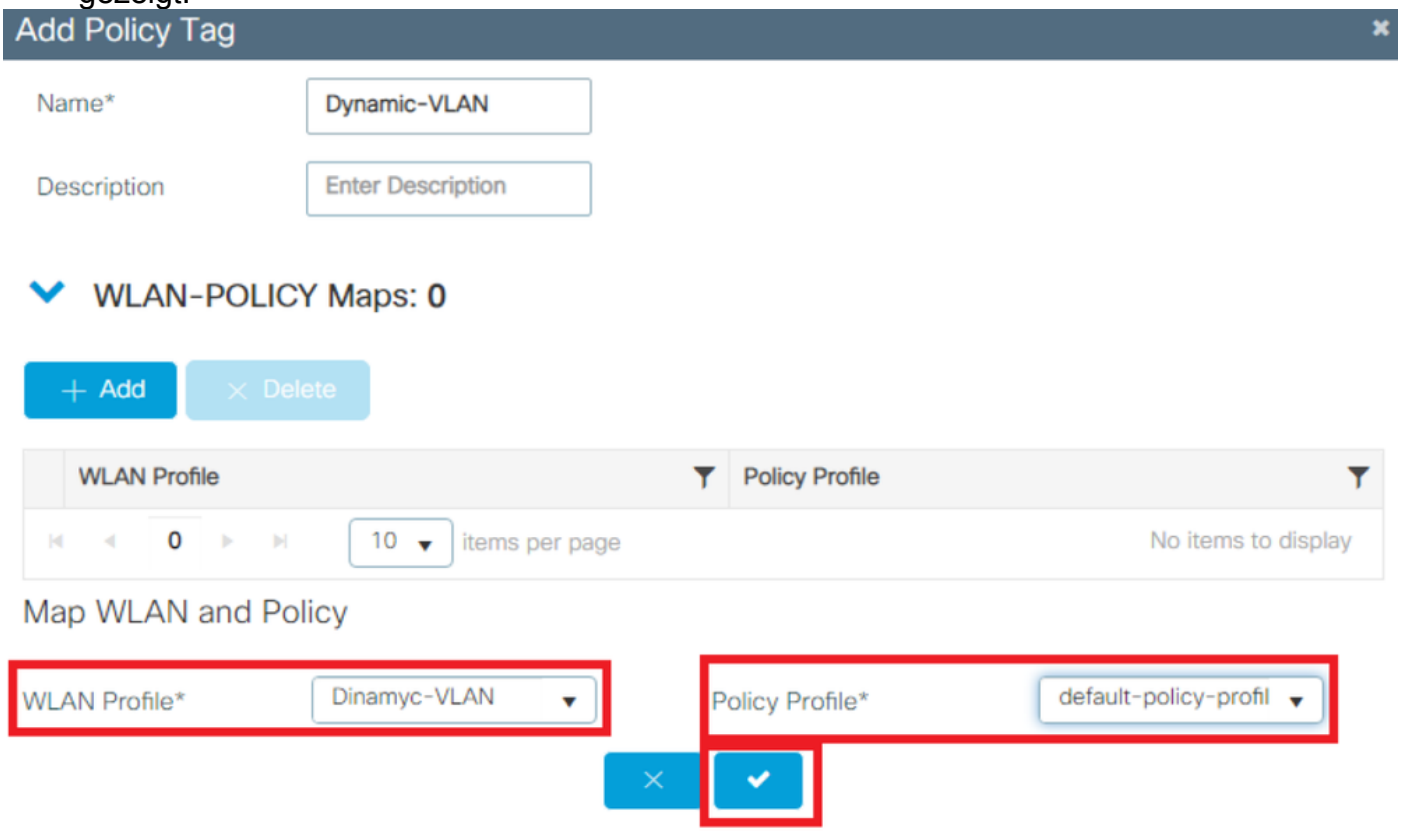
1. Navigieren zu **Configuration > Tags & Profiles > Tags > Policy** und fügen Sie bei Bedarf eine neue hinzu, wie im Bild gezeigt:

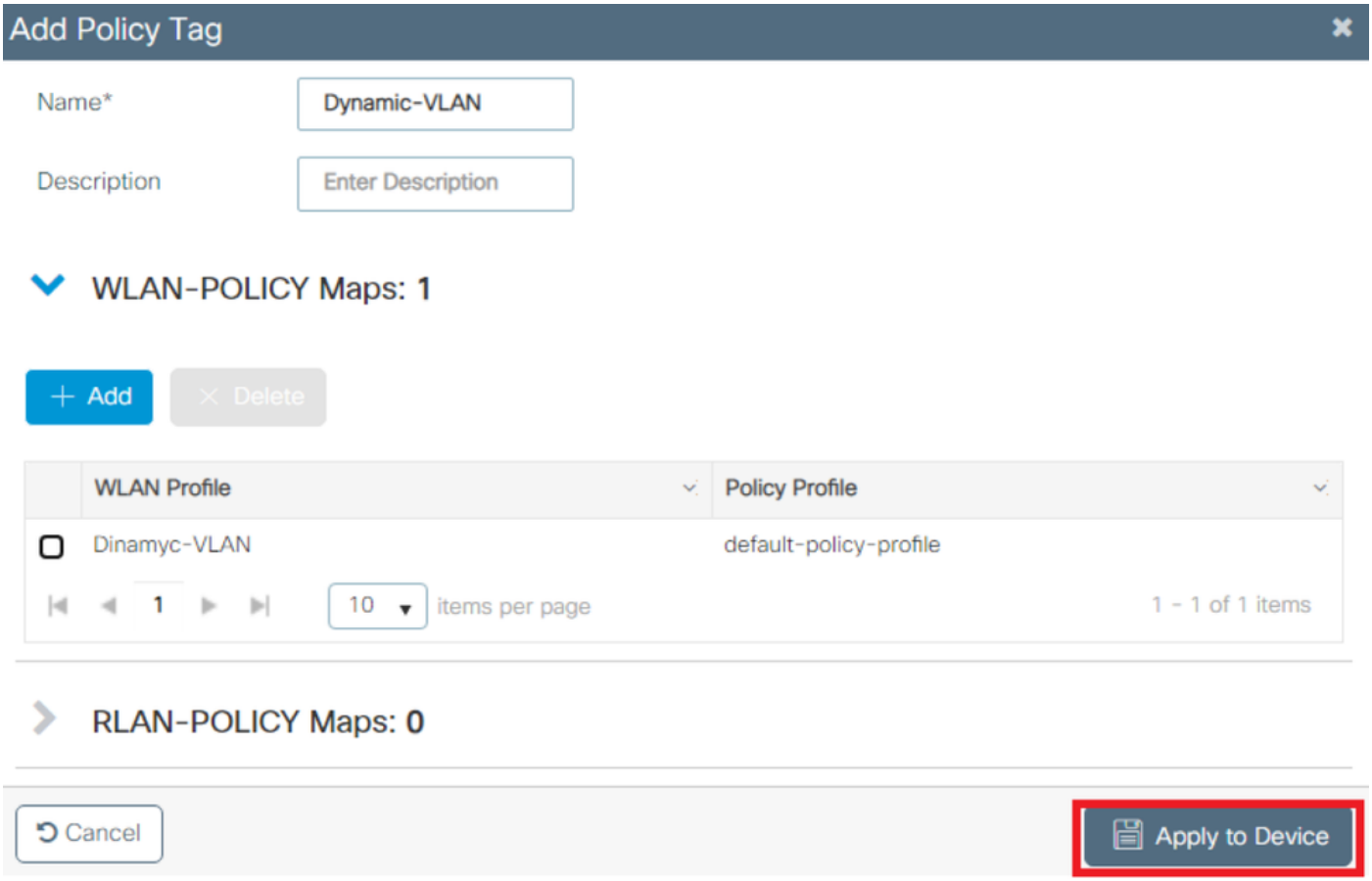


2. Fügen Sie einen Namen zur Richtlinien-Tag hinzu, und wählen Sie **+Add**, wie im Bild gezeigt:



3. Verknüpfen Sie Ihr WLAN-Profil mit dem gewünschten Richtlinienprofil, wie in den Bildern gezeigt:



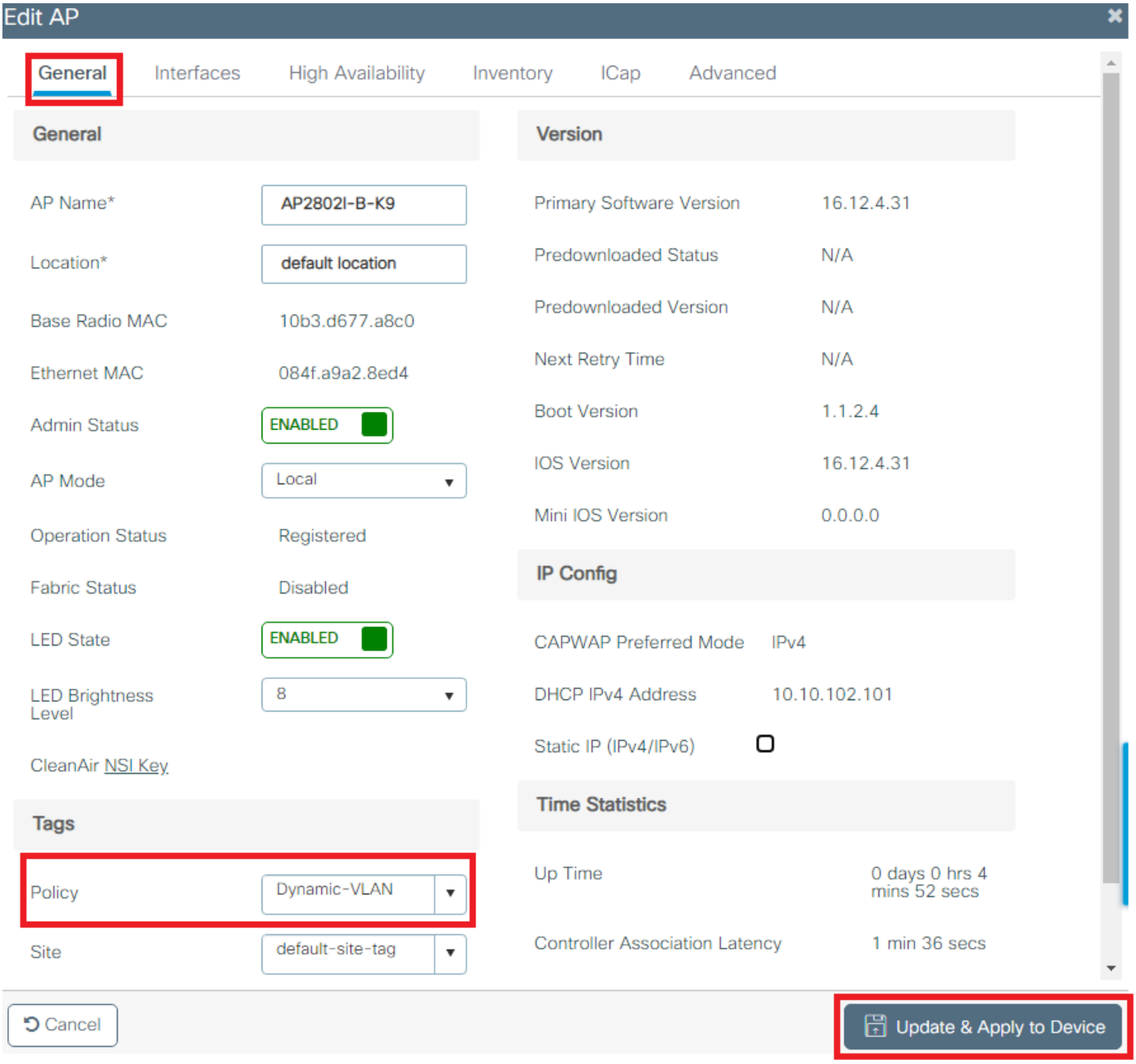


Schritt 6: Zuweisen der Policy-Tag zu einem AP

In diesem Verfahren wird erläutert, wie das Policy-Tag im WLC konfiguriert wird.

Führen Sie diese Schritte aus:

1. Navigieren zu **Configuration > Wireless > Access Points > AP Name > General Tags** und weisen Sie die entsprechende Richtlinien-Tag zu, und wählen Sie dann **Update & Apply to Device** wie im Bild gezeigt:



Vorsicht: Beachten Sie, dass die Richtlinienkennzeichnung eines Access Points beim Ändern die Zuordnung zum WLC verwirft und wieder verbunden wird.

Überprüfung

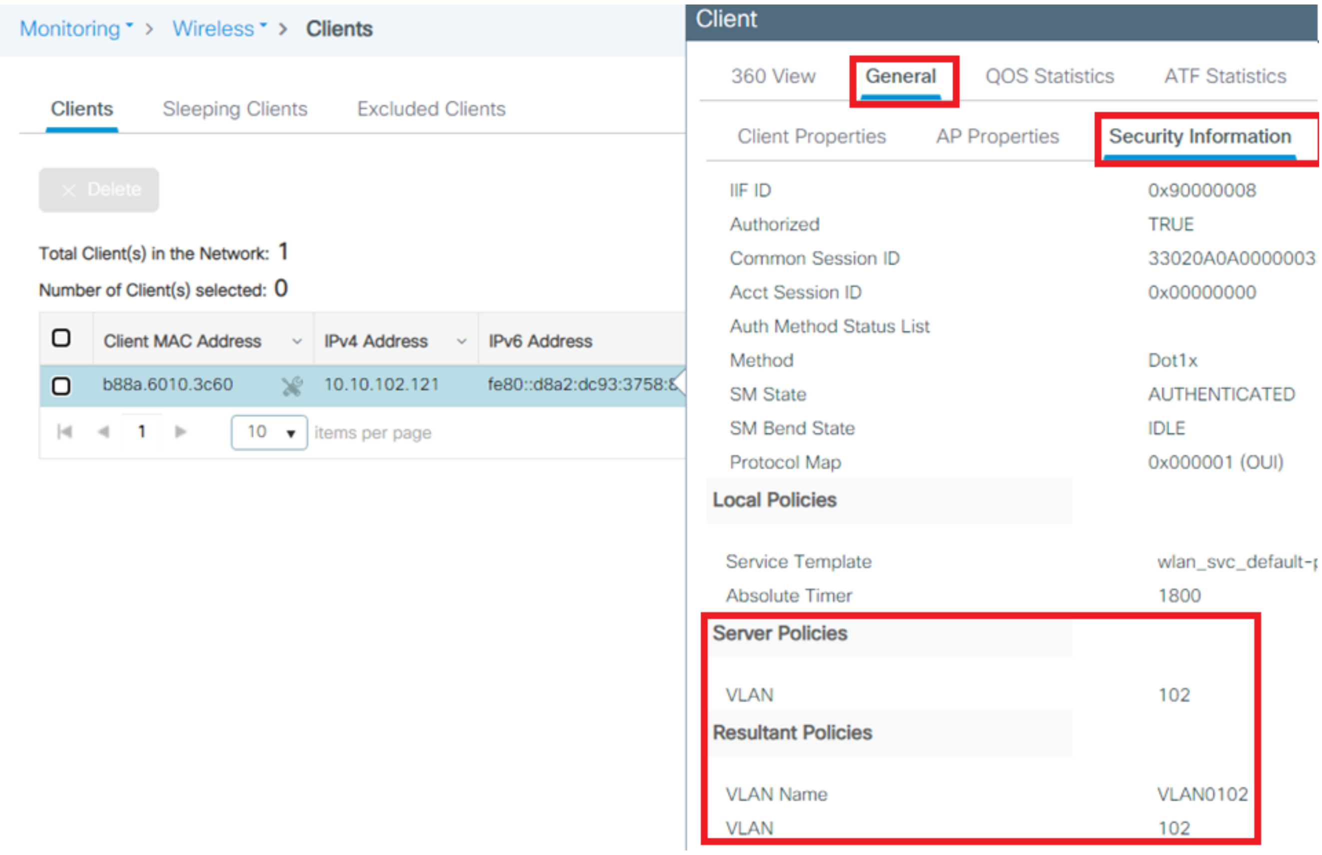
Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Testen Sie die Verbindung mit Windows 10 und der systemeigenen Komponente. Wenn Sie nach einem Benutzernamen und Kennwort gefragt werden, geben Sie die Informationen des Benutzers ein, der einem VLAN auf der ISE zugeordnet ist.

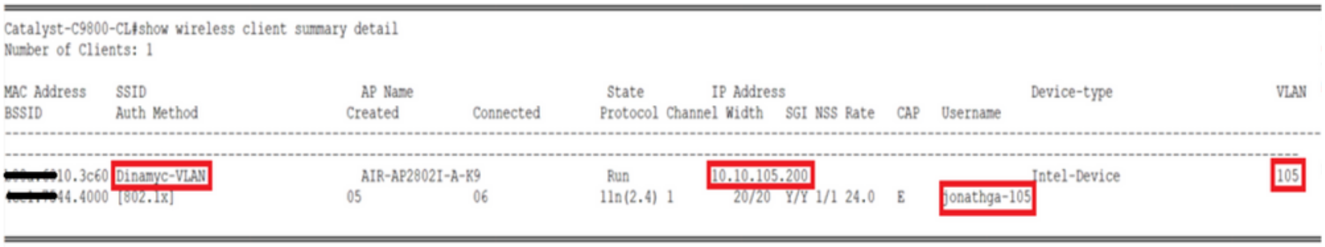
Beachten Sie im vorherigen Beispiel, dass jonathga-102 dem VLAN102 zugewiesen ist, wie im RADIUS-Server angegeben. In diesem Beispiel wird dieser Benutzername verwendet, um eine Authentifizierung zu erhalten und einem VLAN vom RADIUS-Server zuzuweisen:

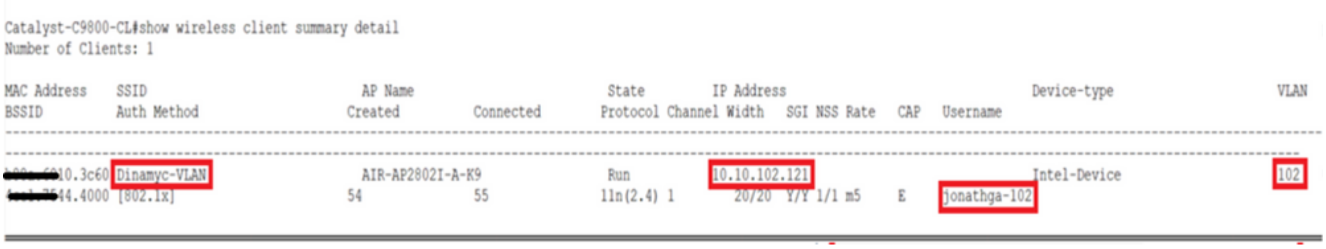
Nach Abschluss der Authentifizierung müssen Sie überprüfen, ob der Client gemäß den gesendeten RADIUS-Attributen dem richtigen VLAN zugewiesen ist. Gehen Sie wie folgt vor, um diese Aufgabe durchzuführen:

1. Navigieren Sie in der Benutzeroberfläche des Controllers zu **Monitoring > Wireless > Clients > Select the client MAC address > General > Security Information** und suchen Sie das VLAN-Feld, wie in der Abbildung gezeigt:



In diesem Fenster können Sie feststellen, dass dieser Client gemäß den auf dem RADIUS-Server konfigurierten RADIUS-Attributen VLAN102 zugewiesen ist.Über die CLI können Sie **show wireless client summary detail** So zeigen Sie die gleichen Informationen an wie im Bild:





2. Es ist möglich, **Radioactive traces** um die erfolgreiche Übertragung der RADIUS-Attribute auf den WLC sicherzustellen. Führen Sie dazu die folgenden Schritte aus: Navigieren Sie in der Benutzeroberfläche des Controllers zu **Troubleshooting > Radioactive Trace > +Add.**Geben Sie die MAC-Adresse des Wireless-Clients ein.Auswählen **Start.**Verbinden Sie den Client mit dem

WLAN.Navigieren zu **Stop > Generate > Choose 10 minutes > Apply to Device > Select the trace file to download the log**.

Dieser Teil der Ablaufverfolgungsausgabe gewährleistet die erfolgreiche Übertragung von RADIUS-Attributen:

```
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Received from id
1812/60 10.10.1.24:0, Access-Accept, len 352
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  authenticator e5 5e
58 fa da 0a c7 55 - 53 55 7d 43 97 5a 8b 17
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  User-Name
[1]     13  "jonathga-102"
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  State
[24]    40  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Class
[25]    54  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Tunnel-Type
       [64]     6  VLAN                    [13]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Tunnel-Medium-Type
[65]     6  ALL_802               [6]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  EAP-Message
[79]     6  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Message-
Authenticator[80]    18  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Tunnel-Private-
Group-Id[81]     6  "102"
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  EAP-Key-Name
 [102]   67  *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:   MS-MPPE-Send-Key
[16]    52  *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:   MS-MPPE-Recv-Key
[17]    52  *
2021/03/21 22:22:45.238 {wncd_x_R0-0}{1}: [eap-auth] [25253]: (info): SUCCESS for EAP method
name: PEAP on handle 0x0C000008

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:            username   0 "jonathga-102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:               class   0 43 41 43 53 3a 33 33 30 32 30 41 30 41 30 30 30 30 30 30 33 35 35 36
45 32 32 31 36 42 3a 49 53 45 2d 32 2f 33 39 33 33 36 36 38 37 32 2f 31 31 32 36 34 30  ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:         tunnel-type   1 13 [vlan] ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute :
tunnel-medium-type   1 6 [ALL_802] ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:tunnel-private-group-id   1 "102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:             timeout   0 1800 (0x708) ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [25253]: (info):
[0000.0000.0000:unknown] AAA override is enabled under policy profile
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Benutzerhandbuch