Konfigurieren der 9800 WLC-Integration mit Aruba ClearPass - Dot1x & Bereitstellung von FlexConnect für Zweigstellen

Inhalt

Einleitung

In diesem Dokument wird die Integration des Catalyst 9800 Wireless Controllers mit Aruba ClearPass Policy Manager (CPPM) und Microsoft Active Directory (AD) beschrieben, um Wireless-Clients in einer Flexconnect-Bereitstellung eine 802.1x-Authentifizierung bereitzustellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie diese Themen kennen und dass sie konfiguriert und verifiziert wurden:

- Catalyst Wireless Controller 9800
- Aruba ClearPass Server (erfordert Plattformlizenz, Zugriffslizenz, Onboard-Lizenz)
- Betriebliches Windows AD
- Optionale Zertifizierungsstelle (Certificate Authority, CA)
- Betriebs-DHCP-Server
- Operativer DNS-Server (für die Zertifikatsperrlisten-Validierung erforderlich)
- ESXi
- Alle relevanten Komponenten werden mit NTP synchronisiert und auf korrekte Zeit überprüft (für die Zertifikatsvalidierung erforderlich).
- Kenntnisse der Themen: C9800-Bereitstellung und neues KonfigurationsmodellFlexConnect-Betrieb auf C9800 802.1x-Authentifizierung

Verwendete Komponenten

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

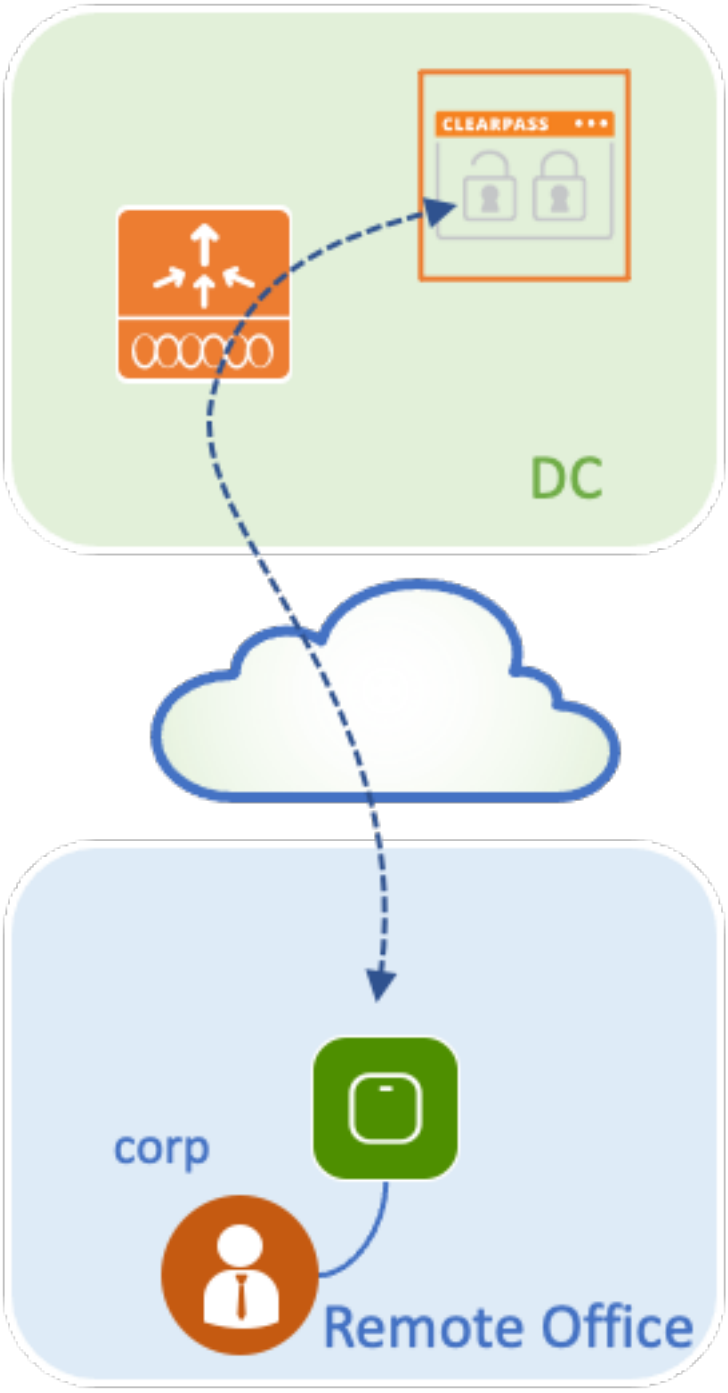
- C9800-L-C Cisco IOS-XE 17.3.3
- C9130AX, 4800 APs
- Aruba ClearPass, Patch 6-8-0-109592 und 6.8-3
- MS Windows-Server Active Directory (GP konfiguriert für die automatisierte, computerbasierte Zertifikatausstellung an verwaltete Endpunkte)DHCP-Server mit Option 43 und Option 60DNS-ServerNTP-Server zur Zeitsynchronisierung aller KomponentenCA

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.

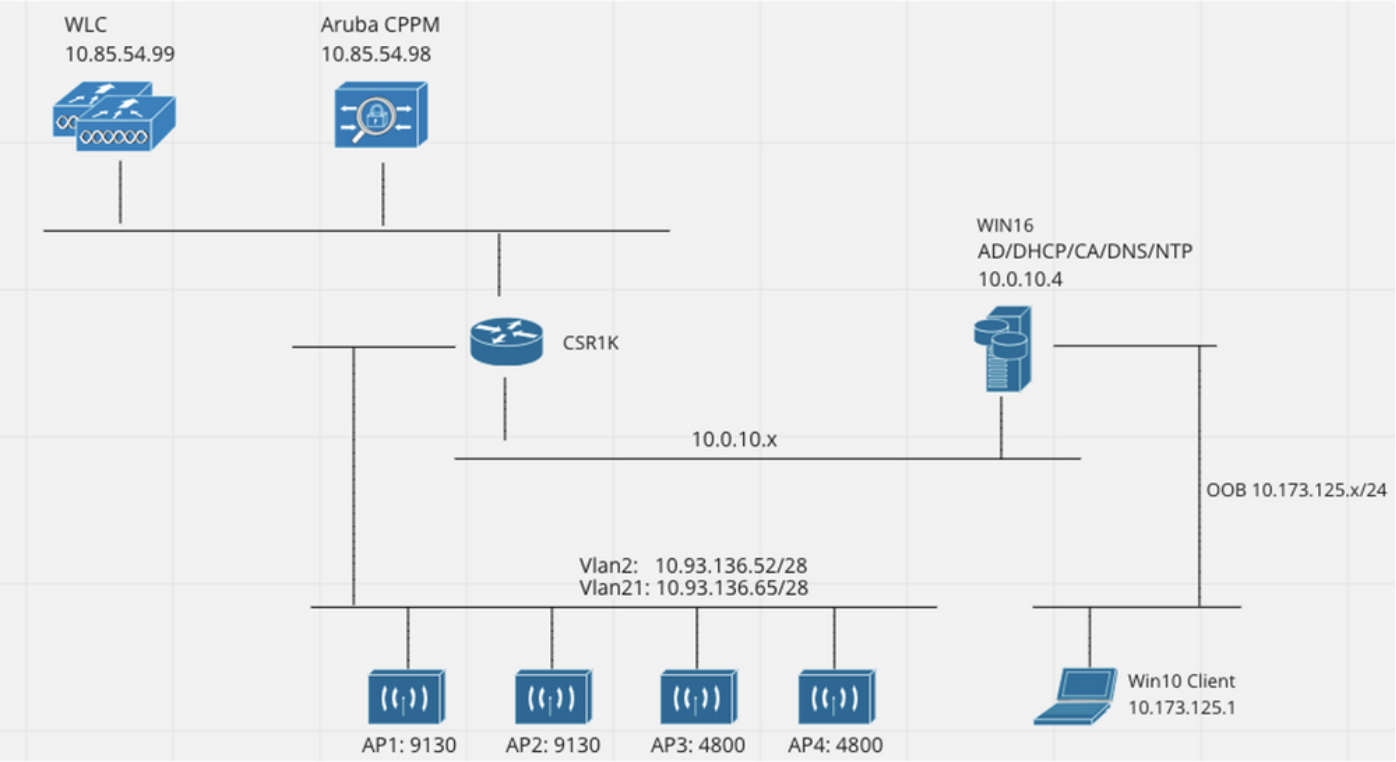
Hintergrundinformationen

Datenverkehrsfluss

In einer typischen Unternehmensbereitstellung mit mehreren Zweigstellen ist jede Zweigstelle so eingerichtet, dass sie den Mitarbeitern des Unternehmens einen 1-fach-Zugriff ermöglicht. In diesem Konfigurationsbeispiel wird PEAP verwendet, um Unternehmensbenutzern über eine im zentralen Rechenzentrum (DC) bereitgestellte ClearPass-Instanz einen 802.1x-Zugriff bereitzustellen. Systemzertifikate werden zusammen mit der Überprüfung der Anmeldeinformationen von Mitarbeitern auf einem Microsoft AD-Server verwendet.

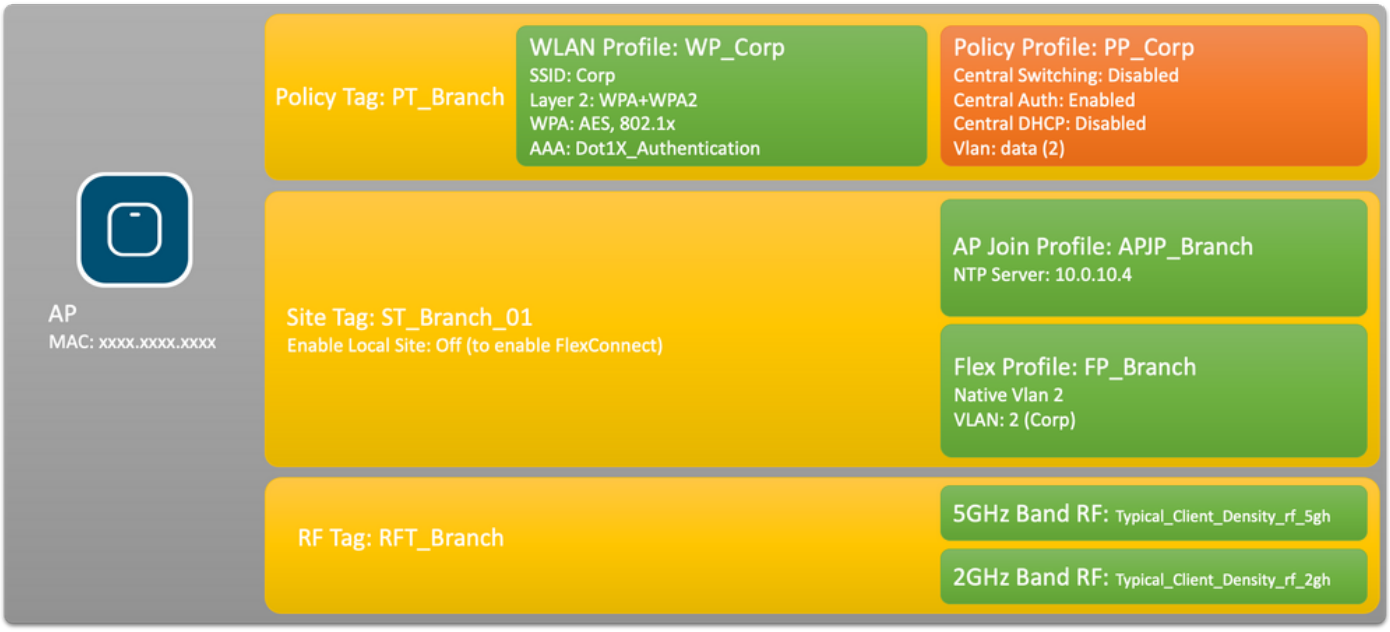


Netzwerkdiagramm



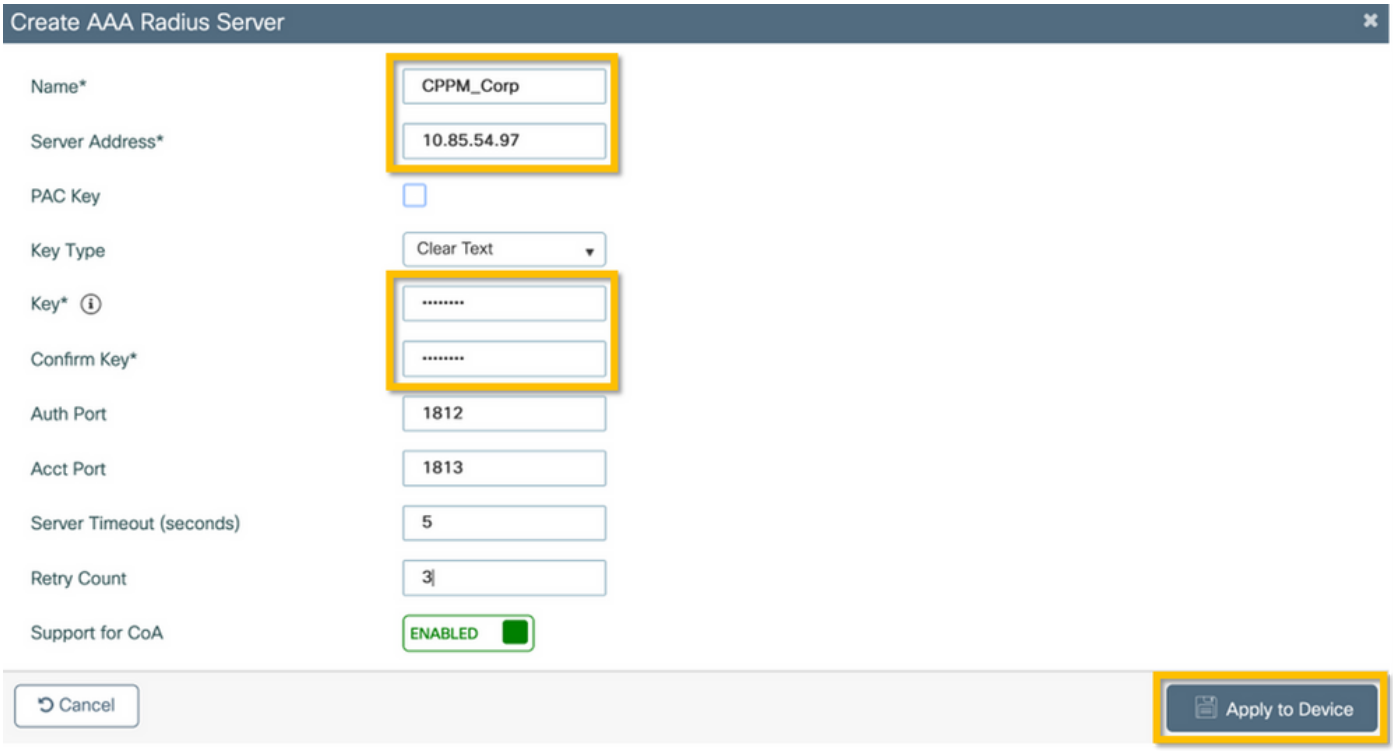
Konfigurieren des Catalyst 9800 Wireless Controllers

In diesem Konfigurationsbeispiel wird das neue Konfigurationsmodell auf dem C9800 verwendet, um die erforderlichen Profile und Tags zu erstellen, um dot1x Corporate Access für Zweigstellen bereitzustellen. Die resultierende Konfiguration ist im Diagramm zusammengefasst.

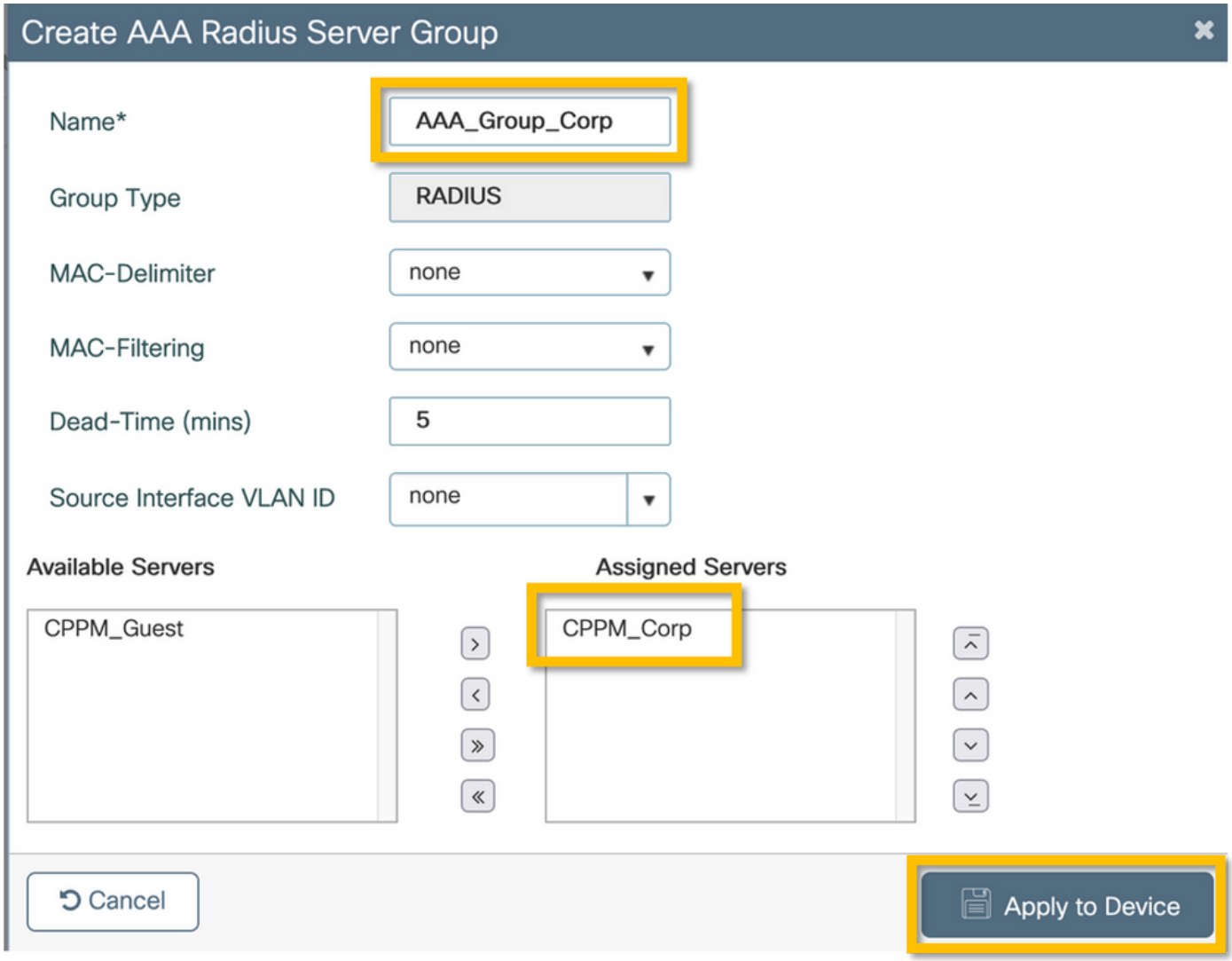


C9800 - Konfigurieren der AAA-Parameter für dot1x

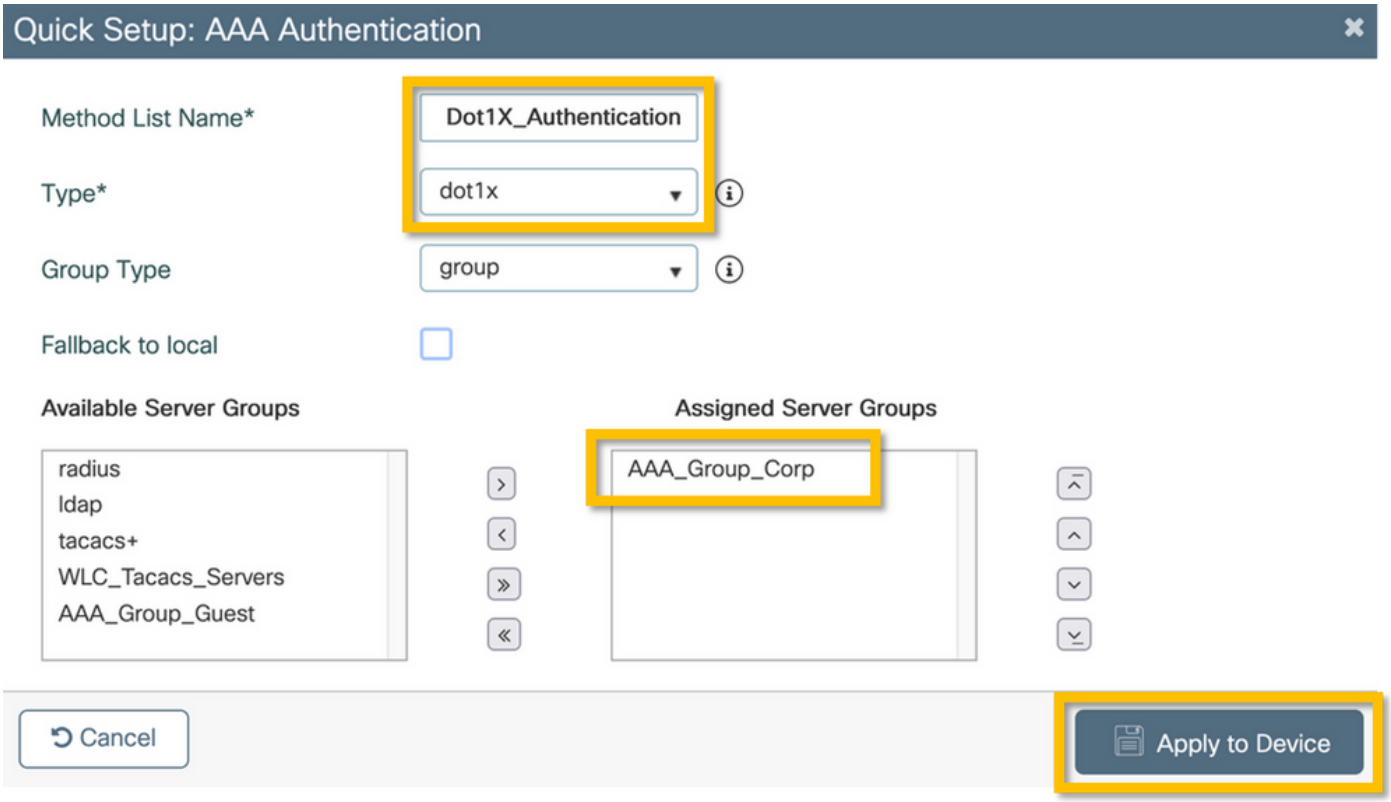
Schritt 1: Fügen Sie den Corp-Server des Aruba ClearPass Policy Manager zur 9800 WLC-Konfiguration hinzu. Navigieren Sie zu **Konfiguration > Sicherheit > AAA > Server/Gruppen > RADIUS > Server.** Klicken Sie auf **+Hinzufügen,** und geben Sie die RADIUS-Serverinformationen ein. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden,** wie in diesem Bild dargestellt.



Schritt 2: Definieren Sie eine AAA-Servergruppe für Unternehmensbenutzer. Navigieren Sie zu **Konfiguration > Sicherheit > AAA > Server/Gruppen > RADIUS > Gruppen,** und klicken Sie auf **+Hinzufügen,** geben Sie den Namen der RADIUS-Servergruppe ein, und weisen Sie die RADIUS-Serverinformationen zu. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.

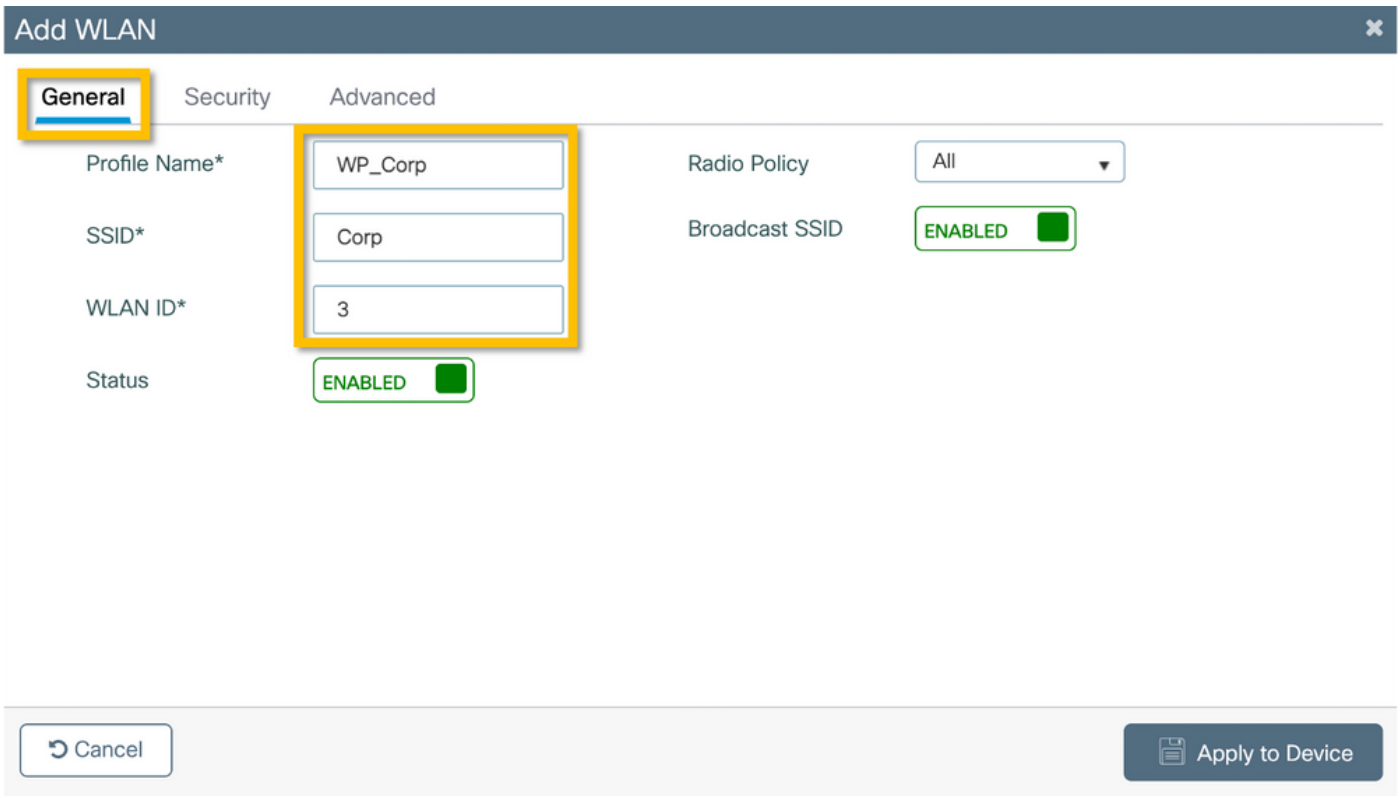


Schritt 3: Definieren Sie die dot1x-Authentifizierungsmethodenliste für Unternehmensbenutzer. Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authentication,** und klicken Sie auf **+Add**. Wählen Sie **Type dot1x** aus dem Dropdown-Menü aus. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.

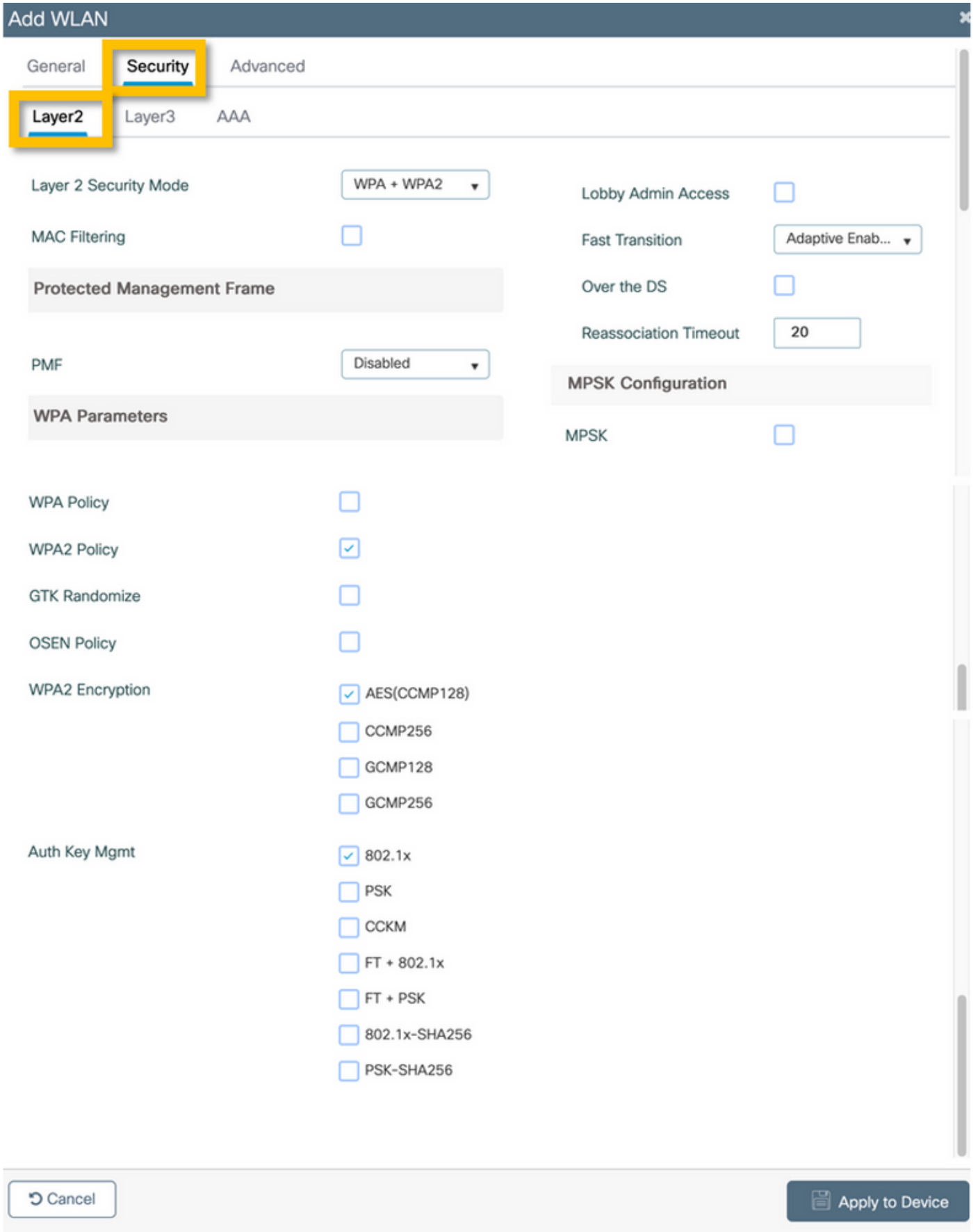


C9800 - Konfigurieren des WLAN-Profils der Firma

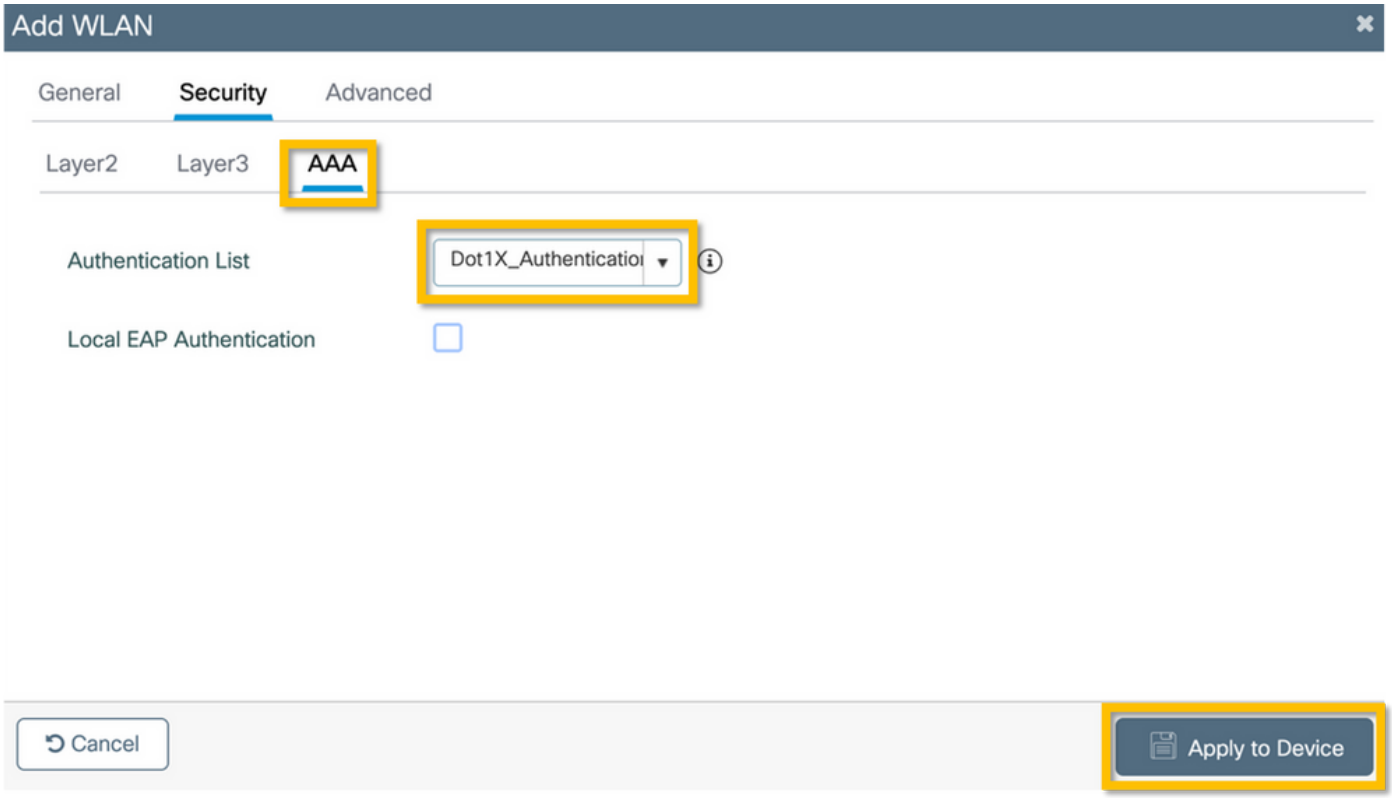
Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Wireless,** und klicken Sie auf **+Hinzufügen**. Geben Sie einen Profilnamen, die SSID "Corp" und eine WLAN-ID ein, die noch nicht verwendet wird.



Schritt 2: Navigieren Sie zur Registerkarte **Security (Sicherheit)** und zur Unterregisterkarte **Layer** 2. Die Standardparameter für dieses Konfigurationsbeispiel müssen nicht geändert werden.

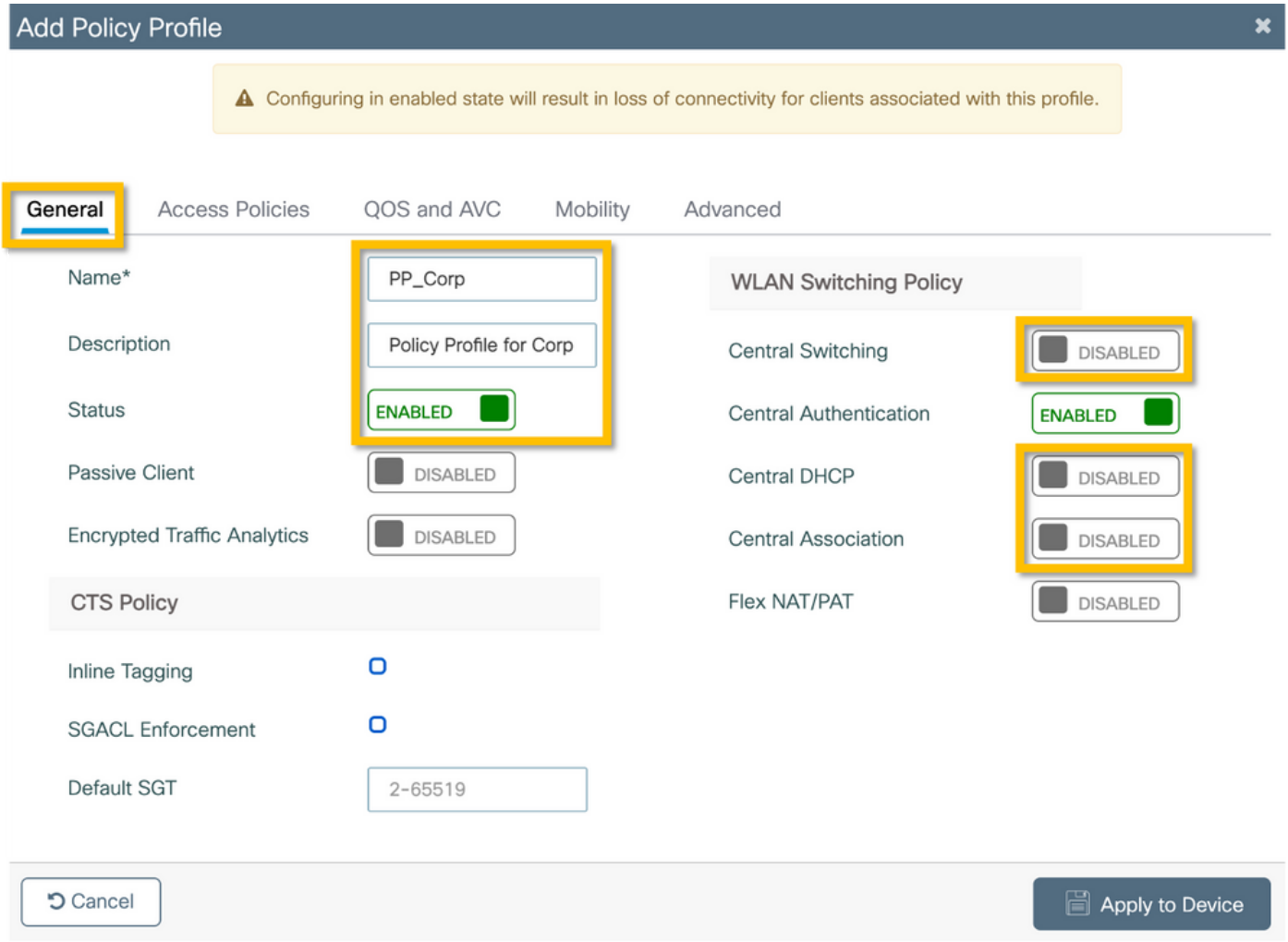


Schritt 3: Navigieren Sie zur Unterregisterkarte **AAA**, und wählen Sie die zuvor konfigurierte Liste der Authentifizierungsmethoden aus. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.

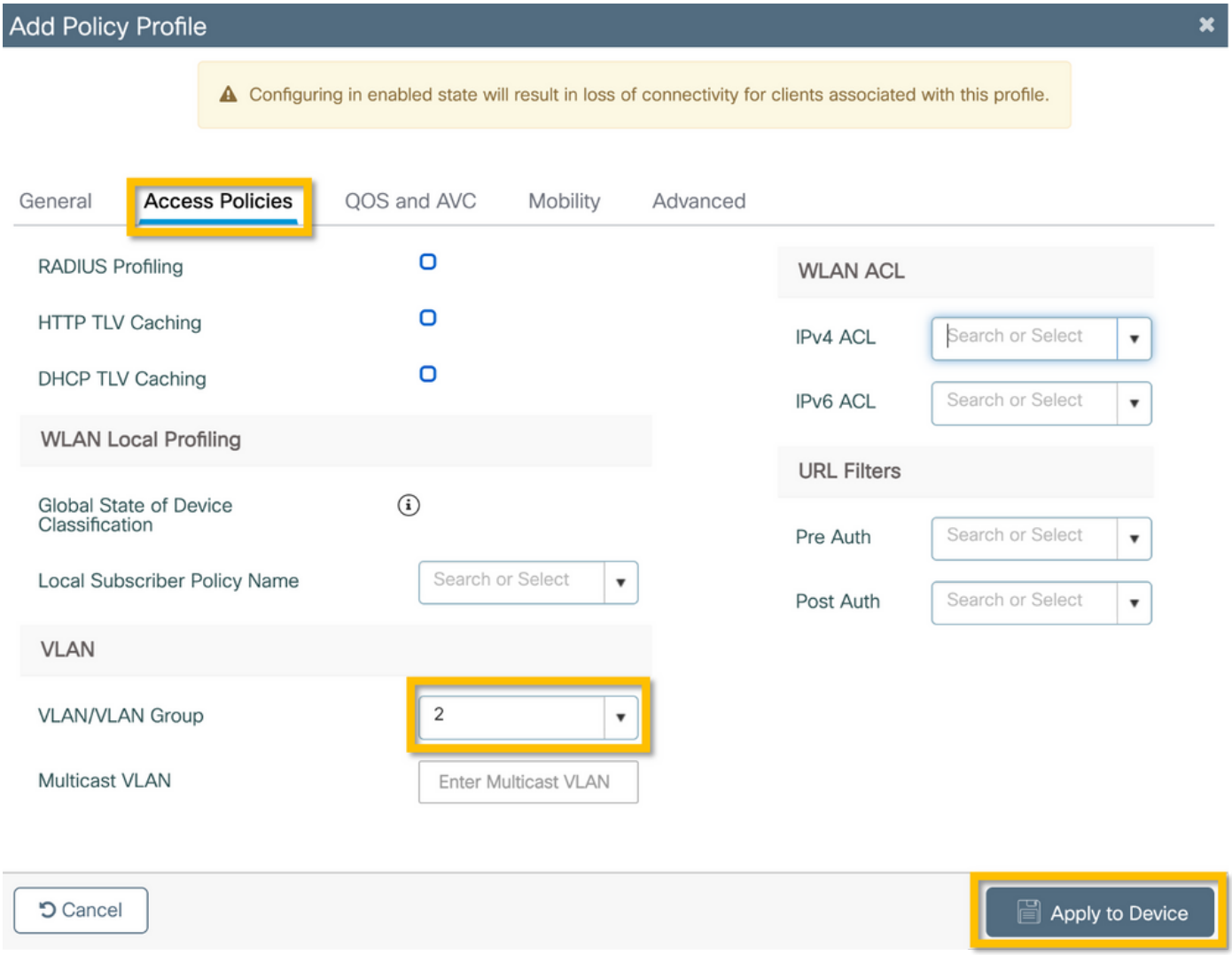


C9800 - Konfigurieren des Richtlinienprofils

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Richtlinie,** und klicken Sie auf **+Hinzufügen**, und geben Sie einen Namen und eine Beschreibung für das Richtlinienprofil ein. Aktivieren Sie die Richtlinie, und deaktivieren Sie das zentrale Switching, DHCP und die Verknüpfung, da der Datenverkehr der Unternehmensbenutzer lokal am Access Point geswitcht wird, wie im Bild gezeigt.



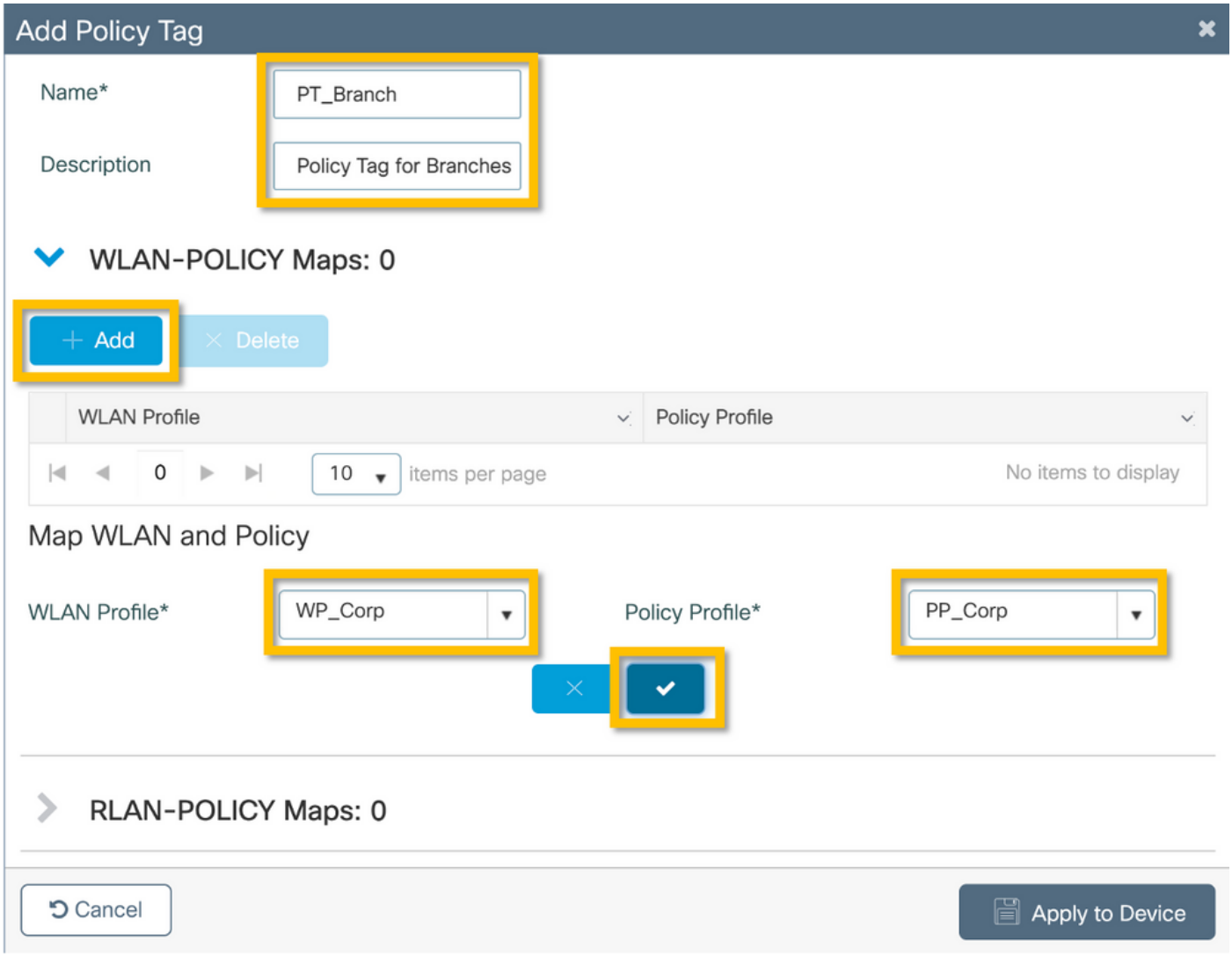
Schritt 2: Navigieren Sie zur Registerkarte **Zugriffsrichtlinien**, und geben Sie die ID des VLANs, das in der Außenstelle für den Datenverkehr der Benutzer des Unternehmens verwendet werden soll, manuell ein. Dieses VLAN muss nicht auf dem C9800 selbst konfiguriert werden. Sie muss im Flex Profile-Tool konfiguriert werden (siehe Details weiter unten). Wählen Sie keinen VLAN-Namen aus der Dropdown-Liste aus (siehe Cisco Bug-ID CSCvn48234). für weitere Informationen). Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.



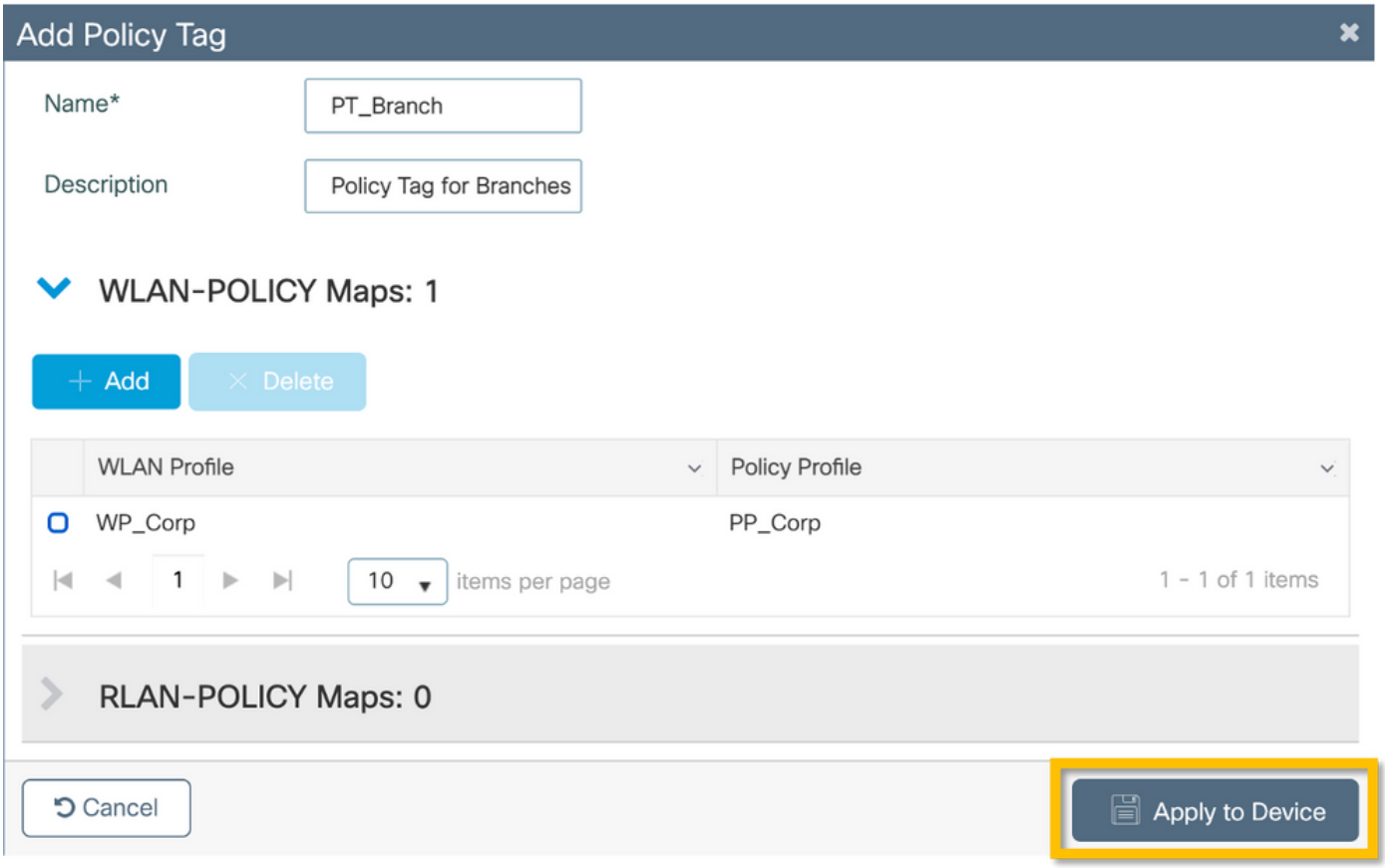
C9800 - Konfigurieren des Richtlinien-Tags

Nachdem das WLAN-Profil (WP_Corp) und das Richtlinienprofil (PP_Corp) erstellt wurden, muss wiederum ein Richtlinien-Tag erstellt werden, um diese WLAN- und Richtlinienprofile miteinander zu verbinden. Dieses Richtlinien-Tag wird auf Access Points angewendet. Weisen Sie diesen Policy Tag Access Points zu, um diese zu konfigurieren und die ausgewählten SSIDs zu aktivieren.

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Tags**, wählen Sie die Registerkarte **Policy** aus, und klicken Sie auf **+Hinzufügen**. Geben Sie den Namen und die Beschreibung der Policy Tag-Nummer ein. Klicken Sie auf **+Hinzufügen** unter **WLAN-POLICY Maps**. Wählen Sie das WLAN-Profil und das Richtlinienprofil aus, die Sie zuvor erstellt haben, und klicken Sie dann auf das Kontrollkästchen, wie in diesem Bild gezeigt.



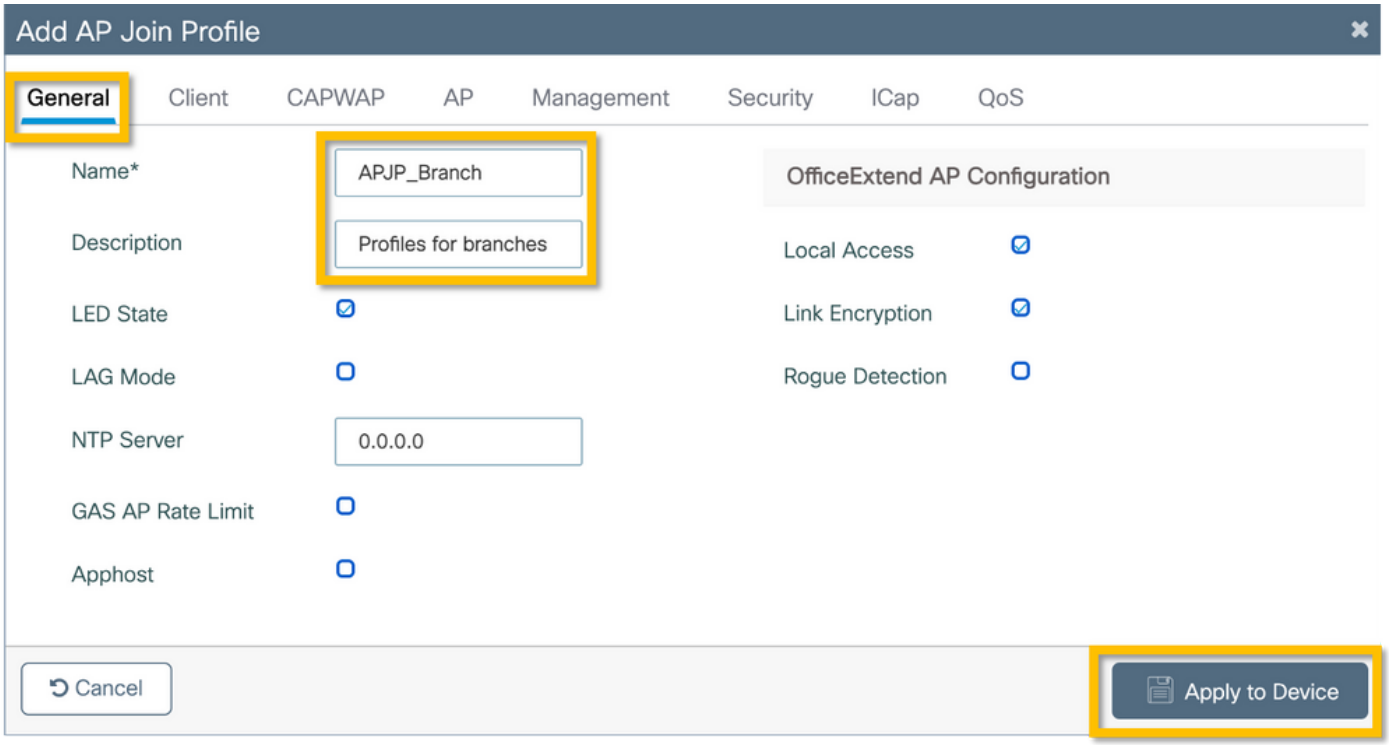
Schritt 2: Überprüfen Sie, und klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in dieser Abbildung dargestellt.



C9800 - AP-Beitrittsprofil

AP-Join-Profile und Flex-Profile müssen konfiguriert und Access Points mit Site-Tags zugewiesen werden. Für jede Außenstelle muss eine andere Site-Tag-Nummer verwendet werden, um den schnellen Übergang (802.11r Fast Transition, FT) innerhalb einer Außenstelle zu unterstützen. Die Verteilung der Client-PMK auf die Access Points dieser Außenstelle ist jedoch zu begrenzen. Es ist wichtig, dieselbe Site-Tag nicht für mehrere Außenstelle zu verwenden. Konfigurieren eines Zugangsprofils für den Access Point Sie können ein einzelnes Zugangsprofil verwenden, wenn alle Zweige ähnlich sind, oder mehrere Profile erstellen, wenn einige der konfigurierten Parameter unterschiedlich sein müssen.

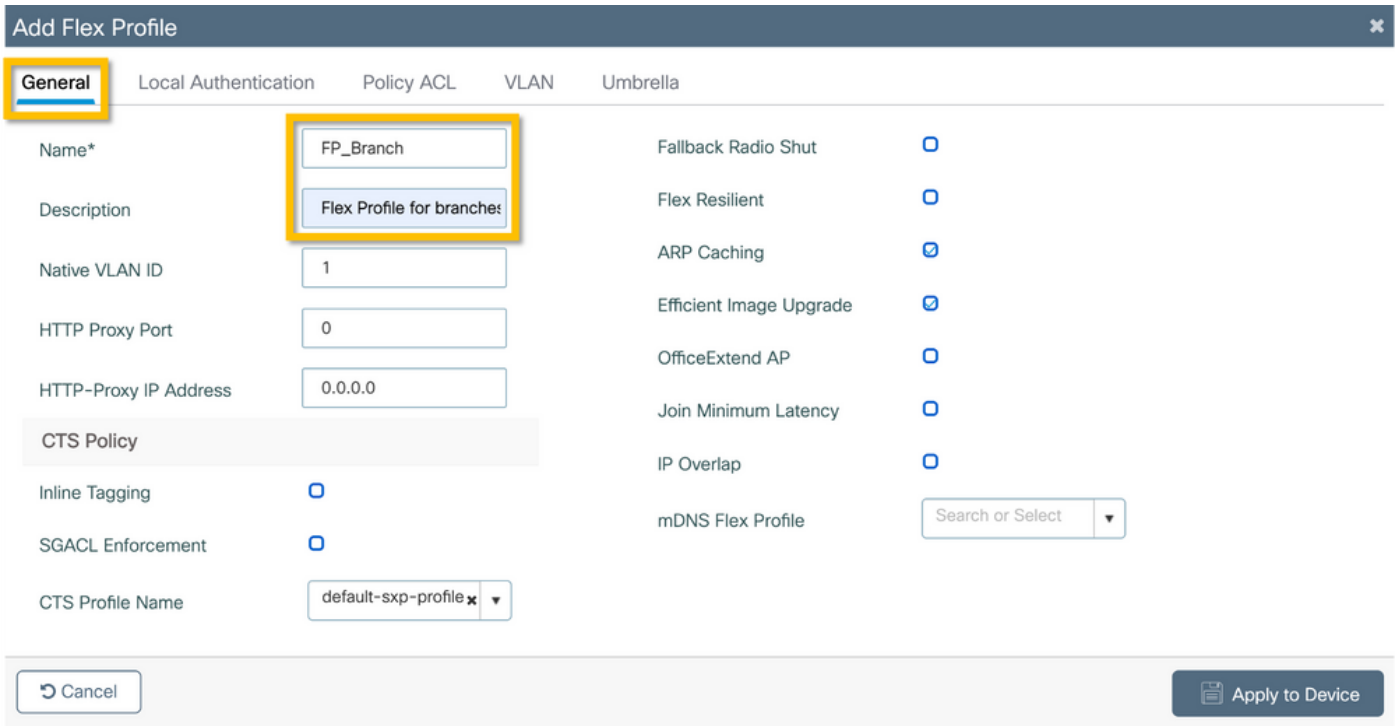
Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > AP Join,** und klicken Sie auf **+Add**. Geben Sie den Namen und die Beschreibung des AP Join-Profils ein. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.



C9800 - Flex Profile

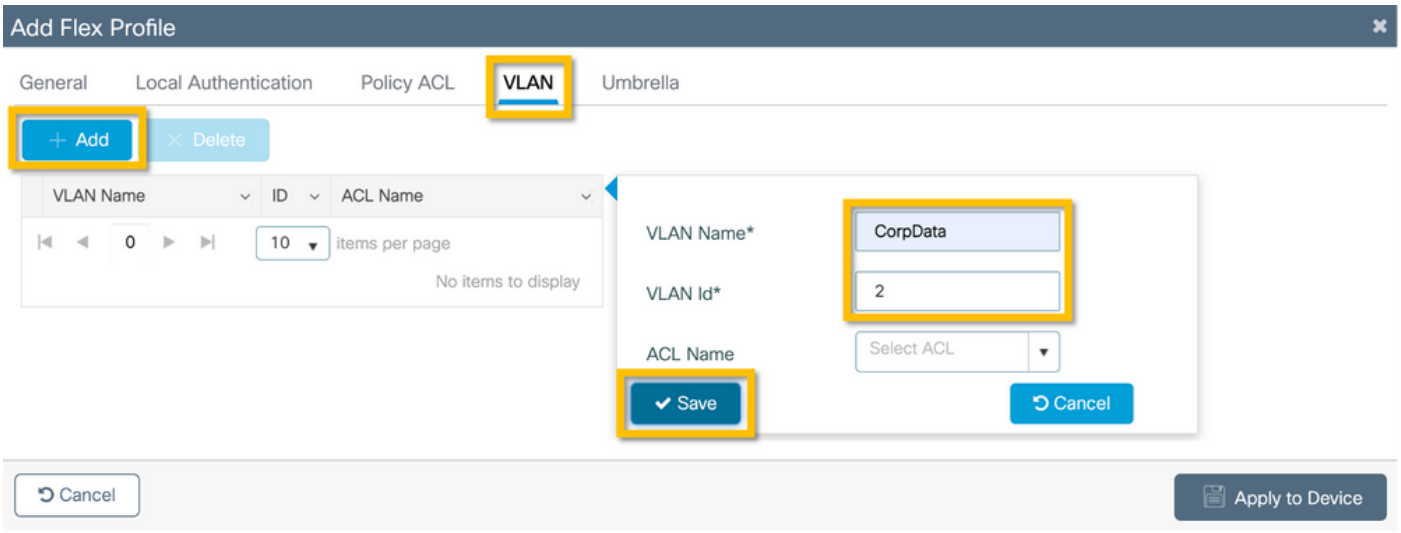
Konfigurieren Sie jetzt ein Flex Profile. Auch hier können Sie ein einziges Profil für alle Zweigstellen verwenden, wenn diese ähnlich sind, und die gleiche VLAN/SSID-Zuordnung haben. Sie können auch mehrere Profile erstellen, wenn einige der konfigurierten Parameter, z. B. die VLAN-Zuweisungen, unterschiedlich sind.

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Flex,** und klicken Sie auf **+Hinzufügen.** Geben Sie den Flex Profile-Namen und die entsprechende Beschreibung ein.

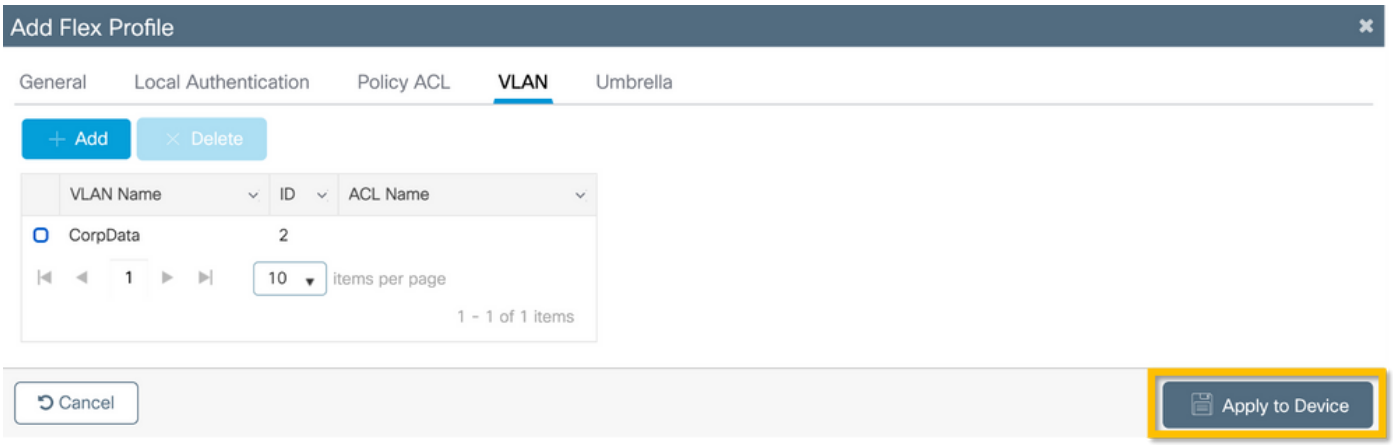


Schritt 2. Navigieren Sie zur Registerkarte **VLAN,** und klicken Sie auf **+Hinzufügen.** Geben Sie den VLAN-Namen und die ID des lokalen VLANs in der Außenstelle ein, die der Access Point zum lokalen Umschalten des Datenverkehrs des Unternehmens verwenden muss. Klicken Sie auf die

Schaltfläche **Speichern**, wie in diesem Bild dargestellt.



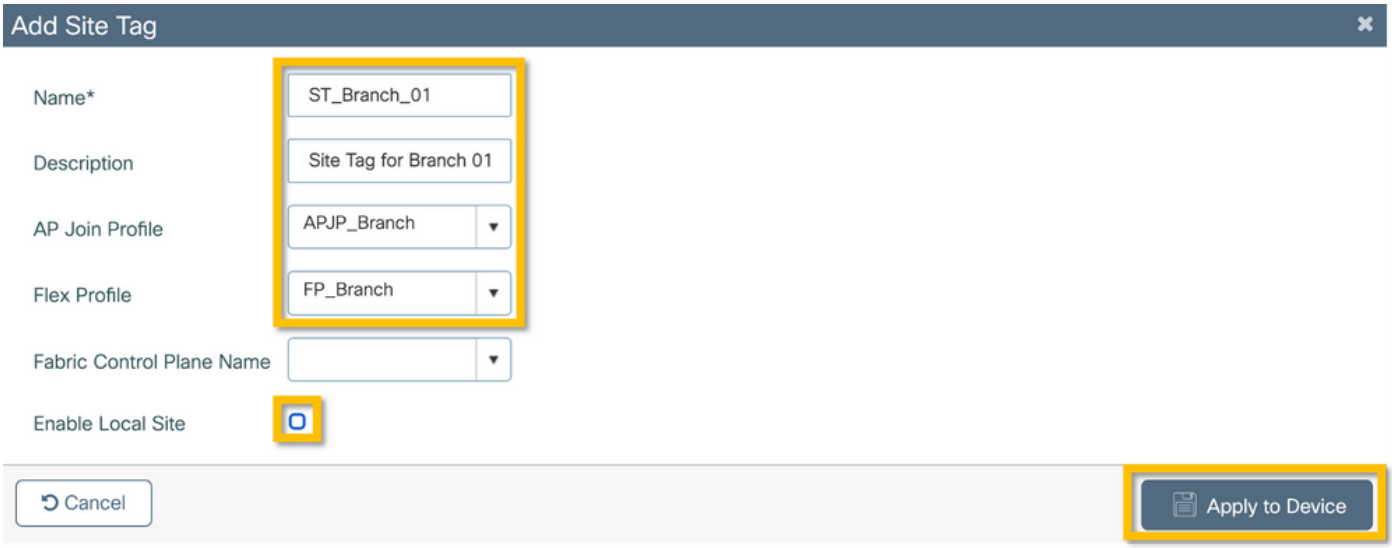
Schritt 3: Überprüfen Sie, und klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in dieser Abbildung dargestellt.



C9800 - Site-Tag

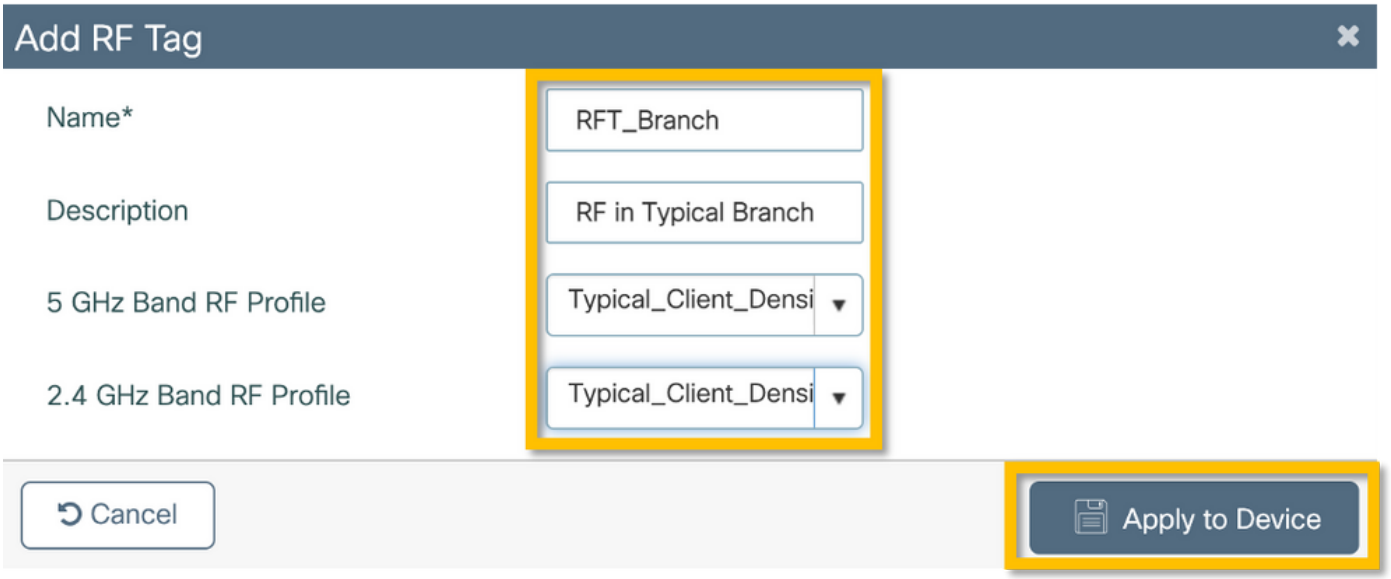
Site-Tags werden verwendet, um Join-Profile und Flex-Profile Access Points zuzuweisen. Wie bereits erwähnt, muss für jede Verzweigung ein anderes Site-Tag verwendet werden, um 802.11r Fast Transition (FT) innerhalb einer Verzweigung zu unterstützen. Die Verteilung der Client-PMK auf die Access Points dieser Verzweigung ist jedoch auf diese beschränkt. Es ist wichtig, denselben Site-Tag nicht über mehrere Verzweigungen hinweg zu verwenden.

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Tags**, wählen Sie die Registerkarte **Site aus**, und klicken Sie auf **+Hinzufügen**. Geben Sie einen Site-Tag-Namen und eine Beschreibung ein, wählen Sie das erstellte AP-Join-Profil aus, deaktivieren Sie das Kontrollkästchen **Lokalen Standort aktivieren,** und wählen Sie schließlich das zuvor erstellte Flex-Profil aus. Deaktivieren Sie das Kontrollkästchen **Lokalen Standort aktivieren,** um den Access Point von **Lokaler Modus** in **FlexConnect** zu ändern. Klicken Sie abschließend auf die Schaltfläche **Auf Gerät anwenden,** wie in diesem Bild dargestellt.



C9800 - RF-Tag

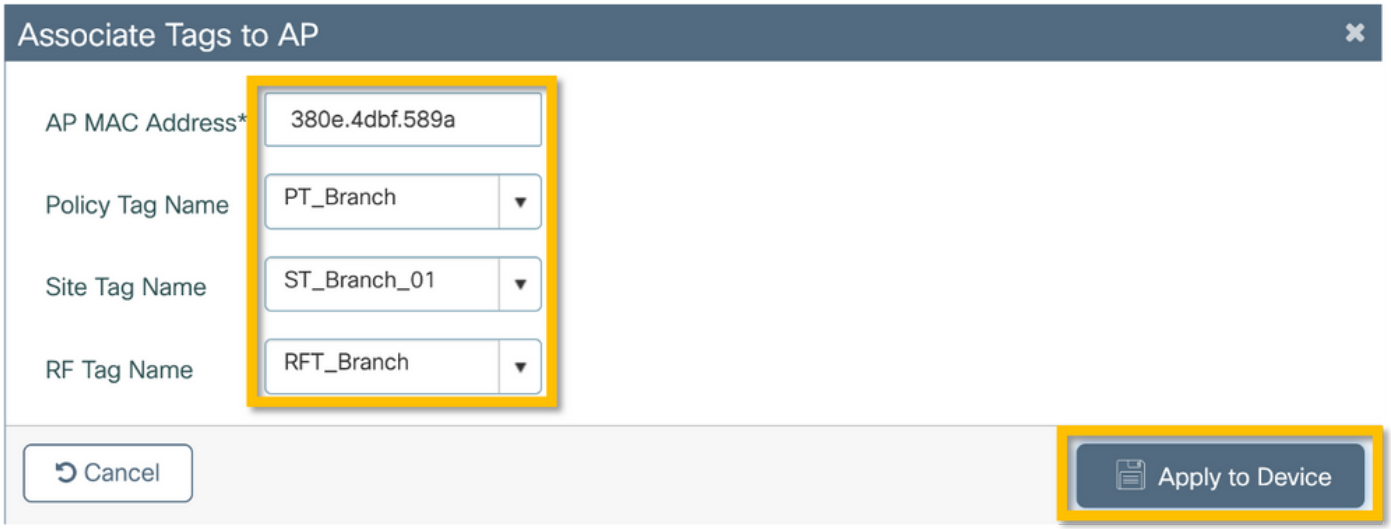
Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Tags,** wählen Sie die Registerkarte **RF,** und klicken Sie auf **+Hinzufügen.** Geben Sie einen Namen und eine Beschreibung für das RF-Tag ein.Wählen Sie die systemdefinierten **RF-Profile aus dem Dropdown-Menü aus**. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.



C9800 - Zuweisen von Tags zu AP

Nachdem die Tags erstellt wurden, die die verschiedenen Richtlinien und Profile enthalten, die für die Konfiguration der Access Points erforderlich sind, müssen diese den Access Points zugewiesen werden. In diesem Abschnitt wird gezeigt, wie ein statisches Tag, das einem Access Point manuell zugewiesen wird, basierend auf seiner Ethernet-MAC-Adresse ausgeführt wird. Für Produktivumgebungen wird empfohlen, den Cisco DNA Center AP PNP Workflow oder eine statische CSV-Upload-Methode zum Hochladen großer Mengen aus dem 9800 zu verwenden.

Schritt 1: Navigieren Sie zu **Konfigurieren > Tags & Profile > Tags**, wählen Sie die Registerkarte **AP** und dann die **Registerkarte Statisch aus**. Klicken Sie auf **+Hinzufügen**, geben Sie die AP-MAC-Adresse ein, und wählen Sie die zuvor definierte Policy-Tag-, Site-Tag- und RF-Tag-Nummer aus. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden,** wie in diesem Bild dargestellt.



Aruba CPPM konfigurieren

Aruba ClearPass Policy Manager Server - Erstkonfiguration

Aruba ClearPass wird über die OVF-Vorlage auf dem ESXi-Server mit folgenden Ressourcen bereitgestellt:

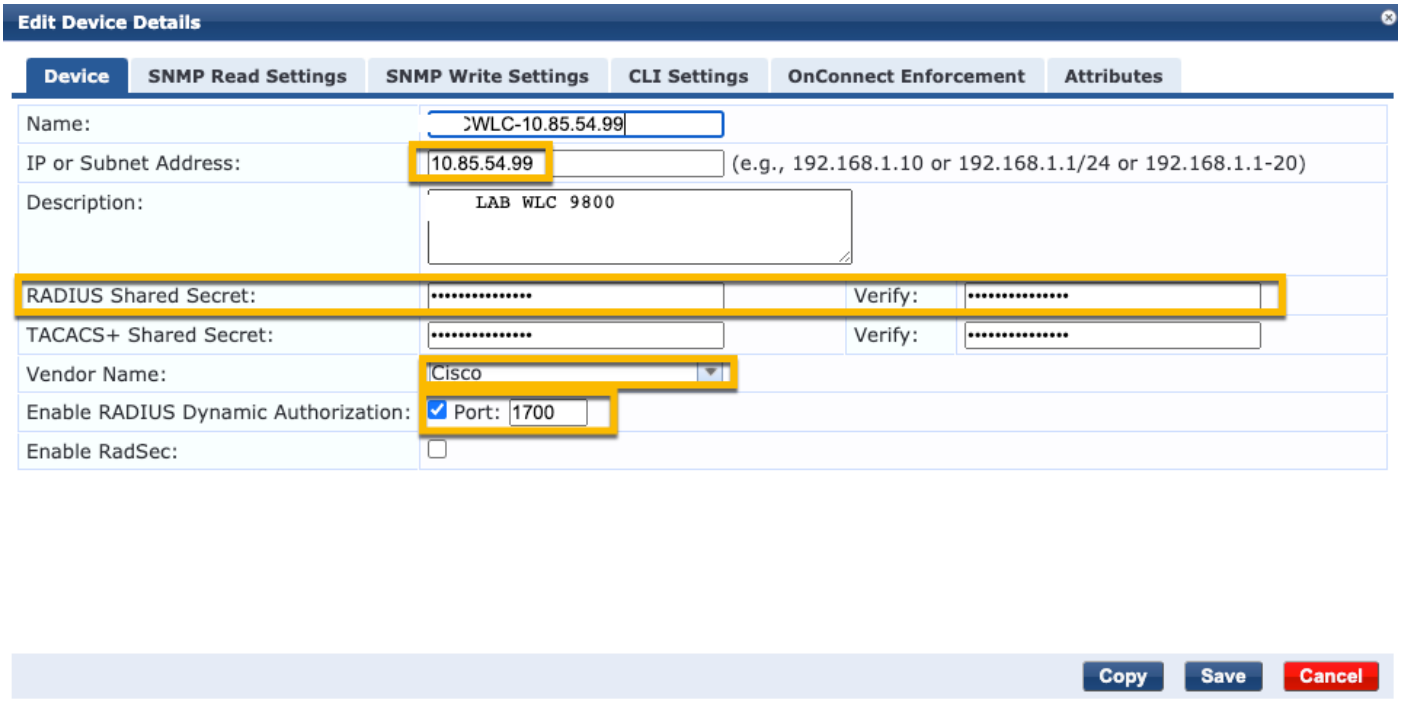
- 2 reservierte virtuelle CPUs
- 6 GB RAM
- 80 GB Festplatte (muss manuell nach der anfänglichen VM-Bereitstellung hinzugefügt werden, bevor der Computer eingeschaltet wird)

Lizenzen anwenden

Wenden Sie die Plattformlizenz an über: **Administration > Server Manager > Licensing (Verwaltung > Server-Manager > Lizenzierung)**. **Zugriff** hinzufügen **und integrieren**

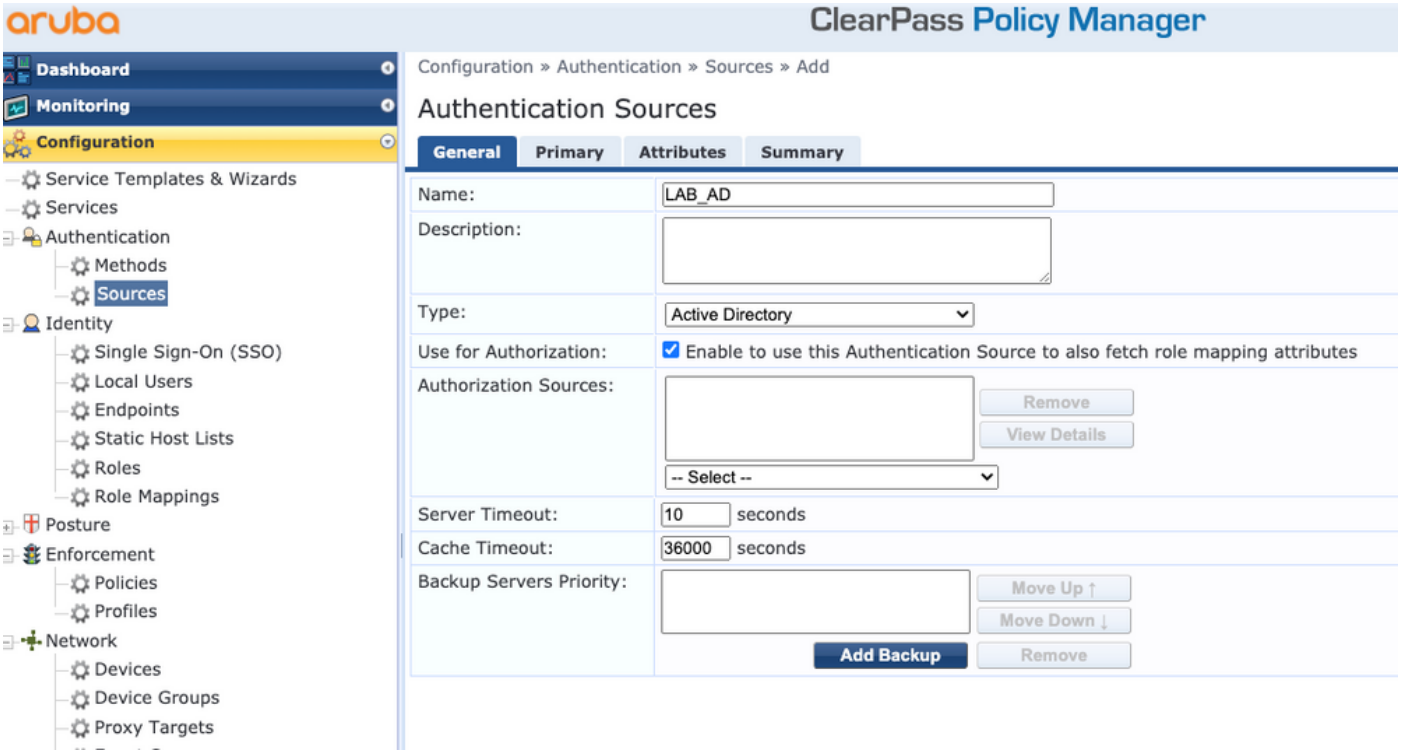
Hinzufügen des C9800 Wireless Controllers als Netzwerkgerät

Navigieren Sie zu **Konfiguration > Netzwerk > Geräte > Hinzufügen,** wie in dieser Abbildung dargestellt.



Konfigurieren von CPPM zur Verwendung von Windows AD als Authentifizierungsquelle

Navigieren Sie zu **Konfiguration > Authentifizierung > Quellen > Hinzufügen**. **Typ** auswählen: **Active Directory** aus dem Dropdown-Menü, wie in diesem Bild dargestellt.

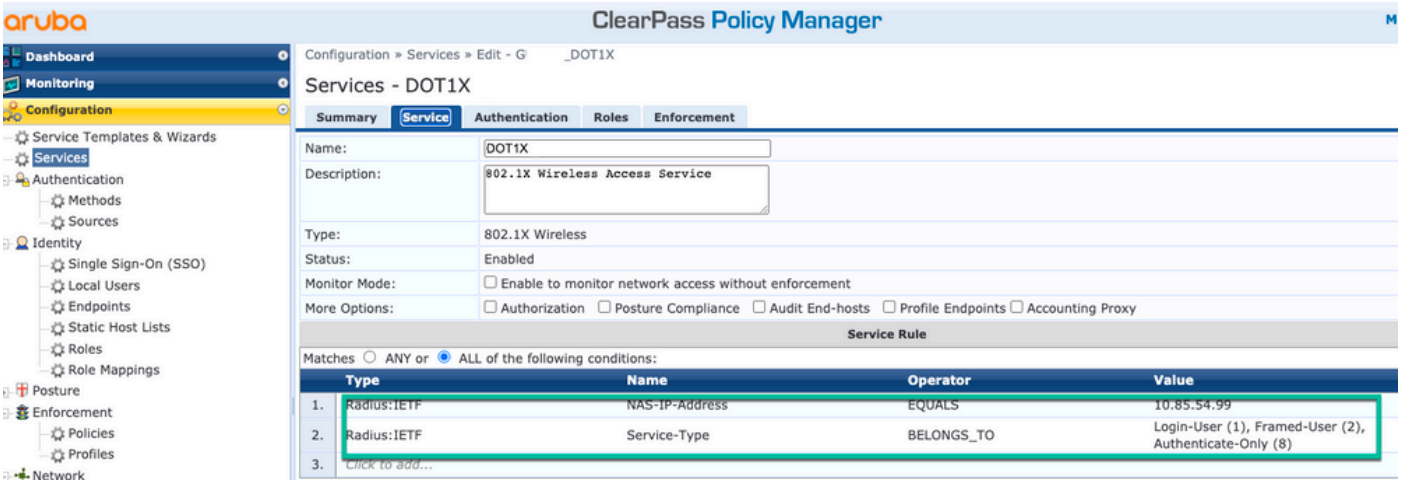


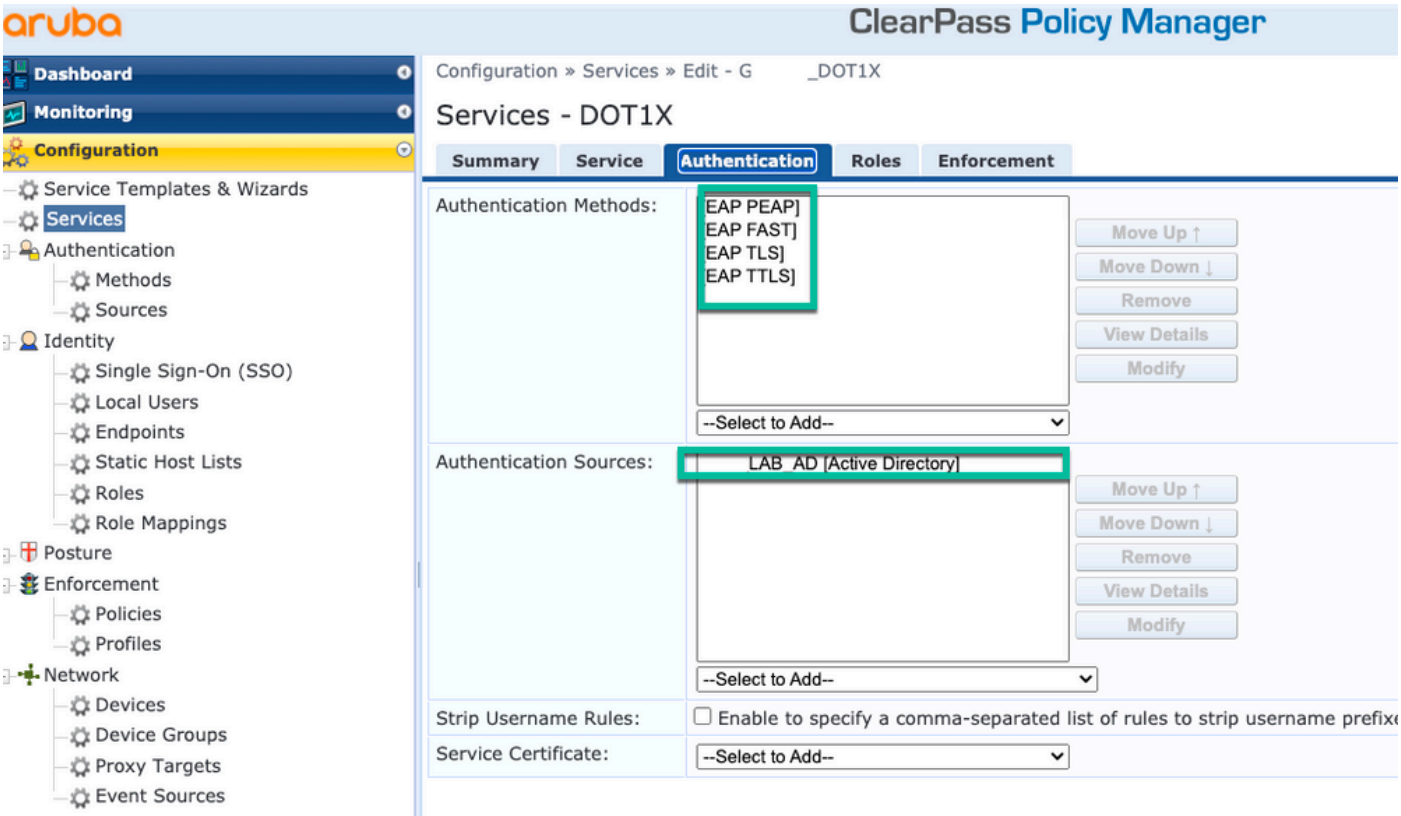
Konfigurieren von CPPM Do1X-Authentifizierungsdienst

Schritt 1: Erstellen Sie einen 'Dienst', der mit mehreren RADIUS-Attributen übereinstimmt:

- Radius:IETF | Name: NAS-IP-Adresse | GLEICH | <IP-ADDR>
- Radius:IETF | Name: Servicetyp | GLEICH | 1,2,8

Schritt 2: Für die Produktion wird empfohlen, den SSID-Namen anstelle von "NAS-IP-Adresse" abzugleichen, sodass eine Bedingung für eine Multi-WLC-Bereitstellung ausreicht.
Radius:Cisco:Cisco-AVPair | cisco-wlan-ssid | Dot1XSSID





Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

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

Zugehörige Informationen

- Cisco 9800 - Best Practices-Leitfaden zur Bereitstellung
- Catalyst Wireless Controller der Serie 9800 - Konfigurationsmodell
- FlexConnect auf Catalyst 9800 Wireless Controller verstehen
- **Technischer Support und Dokumentation für Cisco Systeme**

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.