Lokale Authentifizierung im FlexConnect-Modus konfigurieren

Inhalt

- Einleitung
  - Hintergrundinformationen
    - FlexConnect - Überblick und Anforderungen
    - Betriebsmodi
    - Schnelles und sicheres Roaming
    - FlexConnect High Scale-Modus
    - Unterstützung für Wi-Fi 7 FlexConnect
    - Ausfallsicherheit bei FlexConnect
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Konfigurieren
  - Netzwerkdiagramm
  - AAA-Server konfigurieren
  - Konfiguration des FlexConnect-Modus am Remote-Standort
  - Konfiguration eines 802.1x-WLAN mit lokaler Authentifizierung über einen externen RADIUS-Server
  - Konfigurieren der ISE
  - Konfiguration des PSK-WLAN mit lokaler Authentifizierung
- Überprüfung
- Fehlerbehebung
  - Standalone-Szenario
- Zugehörige Informationen

Einleitung

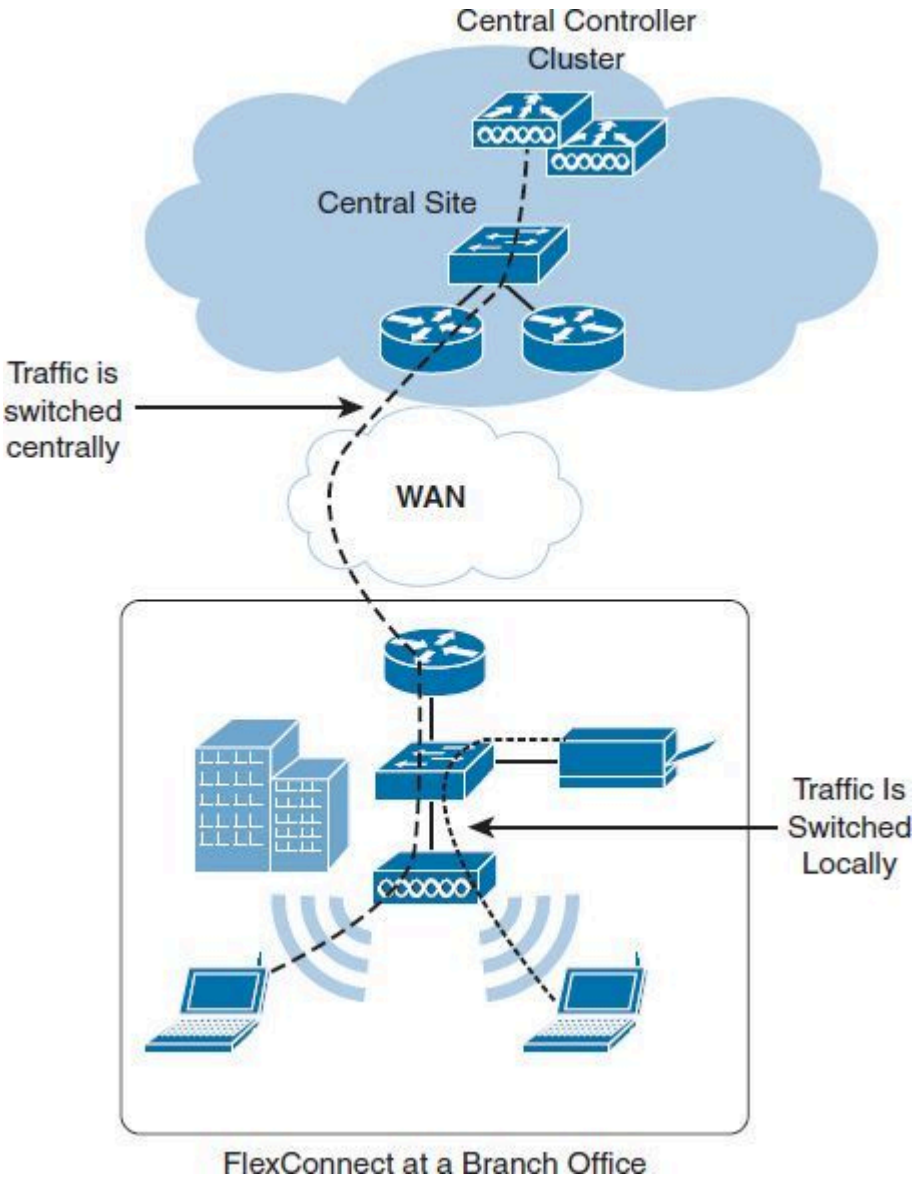
In diesem Dokument wird die Funktionsweise der lokalen FlexConnect-Authentifizierung und ihre Konfiguration mit dem Cisco Catalyst Wireless Controller (WLC) der Serie 9800 beschrieben.

Hintergrundinformationen

FlexConnect - Überblick und Anforderungen

FlexConnect ermöglicht es Access Points (APs) in Außen- oder Zweigstellen, eine Verbindung zu einem zentralen Controller herzustellen, während der Wireless-Datenverkehr lokal verarbeitet werden kann. Im Gegensatz zu herkömmlichen zentralisierten Wireless-Bereitstellungen, bei denen der gesamte Wireless-Datenverkehr mithilfe von CAPWAP (Control and Provisioning of Wireless Access Points) an den Controller getunnelt wird - ermöglicht FlexConnect das lokale Switching und die direkte Verarbeitung des Datenverkehrs durch den Access Point der Außenstelle. Durch diese lokale Umschaltung verfügt der Access Point über eine gewisse Autonomie, sodass wichtige Dienste wie Sicherheit, Roaming und Quality of Service (QoS) unabhängig vom Controller funktionieren.

FlexConnect wurde zwar primär für das Switching von lokalem Datenverkehr entwickelt, bietet jedoch auch die Flexibilität, bei Bedarf bestimmte SSIDs (Service Set Identifier) zentral zu schalten. Wenn beispielsweise bestimmter Datenverkehr eine zentrale Firewall durchläuft, können diese SSIDs für zentrales Switching über CAPWAP an den Controller zurückgesendet werden. Dank dieser doppelten Funktionalität unterstützt ein einzelner FlexConnect-WAP gleichzeitig sowohl lokal als auch zentral geschaltete WLANs (Wireless Local Area Network).



FlexConnect at a Branch Office

Betriebsmodi

Die FlexConnect APs können in zwei Modi betrieben werden: verbundenen Modus und Standalone-Modus.

- Im verbundenen Modus hält der AP über den CAPWAP-Steuerungskanal eine aktive Verbindung zum Controller aufrecht.
- Der Standalone-Modus ist ein Fallback-Status, der auftritt, wenn die Verbindung zwischen dem Access Point und dem Controller unterbrochen wird.

Unter normalen Bedingungen funktionieren FlexConnect-APs im verbundenen Modus, in dem der Controller wichtige Services wie zentrale Authentifizierung, Client-Profilerstellung und Radio Resource Management (RRM) verwaltet. Während davon ausgegangen wird, dass der Access Point die meiste Zeit in diesem Modus verbleibt, schaltet er automatisch in den Standalone-Modus um, wenn die Kommunikation mit dem Controller unterbrochen wird. Im Standalone-Modus bleibt der Access Point betriebsbereit und schaltet lokal den Datenverkehr um, sodass die Clients weiterhin verbunden bleiben. Die APs authentifizieren Clients unabhängig voneinander, ohne Authentifizierungsanforderungen an einen zentralen Controller weiterzuleiten. Bestimmte controllerabhängige Services wie RRM und zentralisierte Client-Authentifizierung stehen jedoch vorübergehend nicht zur Verfügung.

Wenn z. B. ein WAN-Ausfall (Wide Area Network) die Verbindung zwischen dem Access Point und dem Controller unterbricht, der Internetzugriff jedoch aktiv bleibt, wechselt der Access Point in den Standalone-Modus und verarbeitet den lokal übermittelten Datenverkehr ohne Unterbrechung weiter. Bestehende Clients bleiben verbunden, aber neue Clients, die eine zentrale Authentifizierung benötigen, können dem Netzwerk nicht beitreten - es sei denn, es ist eine lokale Authentifizierung konfiguriert. Die FlexConnect-APs können so eingerichtet werden, dass bei WAN-Ausfällen eine lokale Authentifizierung durchgeführt wird. Dadurch wird sichergestellt, dass der Dienst auch dann fortgesetzt wird, wenn der Controller nicht erreichbar ist.

Im Standalone-Modus sind diese Funktionen für den AP nicht verfügbar:

- Client-Webauthentifizierung
- Gastauthentifizierung (Portal-Umleitung)
- Alle zentral geschalteten SSIDs
- RRM

- IPv6 Layer-3-Mobilität
- Native Profilerstellung
- Richtlinienklassifizierung
- Service Discovery Gateway
- Konfigurations-Updates

Eine vollständige Liste der Funktionen und WLAN-Konfigurationen, die im Standalone-Modus (lokale Authentifizierung) unterstützt werden, finden Sie in der Funktionsmatrix: Funktionsübersicht für Cisco Wireless Access Points

Ein gängiges FlexConnect-Ausfallszenario beinhaltet einen vollständigen Verlust oder eine erhebliche Verschlechterung des WAN, wodurch der CAPWAP-Steuerungskanal unterbrochen wird. Wenn der WAP aufgrund von WAN-Problemen die Verbindung zum Controller verliert, schaltet er sofort in den Standalone-Modus um.

Das Hauptziel bei einem WAN-Ausfall besteht darin, die Kommunikation mit dem Controller so schnell wie möglich wiederherzustellen, um den vollen Funktionsumfang wieder herzustellen.

Wenn ein FlexConnect-WAP aufgrund eines WAN-Fehlers in den Standalone-Modus wechselt, bleiben aktive Clients verbunden und können nahtlos zwischen WAPs innerhalb des FlexConnect-Domänen-/Standort-Tags wechseln. Beim Roaming zwischen verschiedenen FlexConnect-Standort-Tags kann jedoch eine vollständige Neuauthentifizierung erforderlich sein. Neue Clients, die versuchen, dem lokal geschalteten WLAN beizutreten, können sich jedoch nicht authentifizieren, da der AAA-Server (Authentication, Authorization und Accounting Server) am zentralen Standort nicht erreichbar ist.

Schnelles und sicheres Roaming

Die EAP-Authentifizierung (Extensible Authentication Protocol) führt zu einer höheren Latenz im Vergleich zur PSK-Authentifizierung (Pre-Shared Key), da EAP-Frames mit dem AAA-Server ausgetauscht werden. Bei schnellem sicherem Roaming erfolgt die vollständige 802.1X/EAP-Authentifizierung eines Clients jedoch nur während der ersten Verbindung mit dem Netzwerk. Beim nachfolgenden Roaming zu benachbarten APs wird der EAP-Austausch umgangen, sodass nur der Vier-Wege-Handshake übrig bleibt, der wesentlich schneller ist, da der AAA-Server nicht involviert ist. In dieser Tabelle werden die verschiedenen Methoden für schnelles und sicheres Roaming beschrieben, die der 9800 WLC sowohl im lokalen Modus als auch in FlexConnect-Bereitstellungen unterstützt.

Funktion	Lokaler Modus	FlexConnect (Connected Mode; Zentrale Authentifizierung)	FlexConnect (verbundener Modus - lokale Authentifizierung)	FlexConnect (Standalone)
Zwischenspeicherung von Kurzschlüsseln (Sticky Key Caching, SKC)	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Opportunistic Key Caching (OKC)	Unterstützt	Unterstützt	Unterstützt	Unterstützt (bis die Client-Sitzung abläuft)
Cisco Centralized Key Management (CCKM)	Unterstützt	Unterstützt	Unterstützt	Nicht unterstützt
FT-802.11r/Adaptive 11r (schneller Umstieg) (über Funk)	Unterstützt	Unterstützt	Unterstützt	Unterstützt (bis die Client-Sitzung abläuft)
FT-802.11r/Adaptive 11r (schneller Übergang) (über die DS)	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt

Im Standalone-Modus hängt schnelles Roaming davon ab, ob zwischengespeichertes Schlüsselmaterial gültig bleibt. Wenn der zwischengespeicherte PMK (Pairwise Master Key) bzw. die Sitzung abläuft, kann der Access Point erst nach der Wiederherstellung der Controller-Konnektivität neue vom Controller abgeleitete Schlüsselinformationen abrufen.

FlexConnect High Scale-Modus

Ab Cisco IOS XE 17.8.1 wurde die Kapazität des Flex Site-Standorts auf 300 APs und 3.000 802.1x-Clients erweitert.

Durch die PMK-Propagierung können die APs am selben FlexConnect-Standort PMK-Informationen austauschen, sodass beim Roaming kein vollständiger EAP-Austausch erforderlich ist. Die PMK-Propagierung ist nicht standardmäßig aktiviert.

Verwenden Sie diese Befehle, um die PMK-Propagierung zu überprüfen und PMK zu aktivieren:

- Wireless-Statistiken anzeigen pmk-Übertragung
- pmk propagieren

Unterstützung für Wi-Fi 7 FlexConnect

Diese Tabelle fasst die FlexConnect-Funktionen zusammen, die von der CW917x Wi-Fi 7 AP-Familie unterstützt werden.

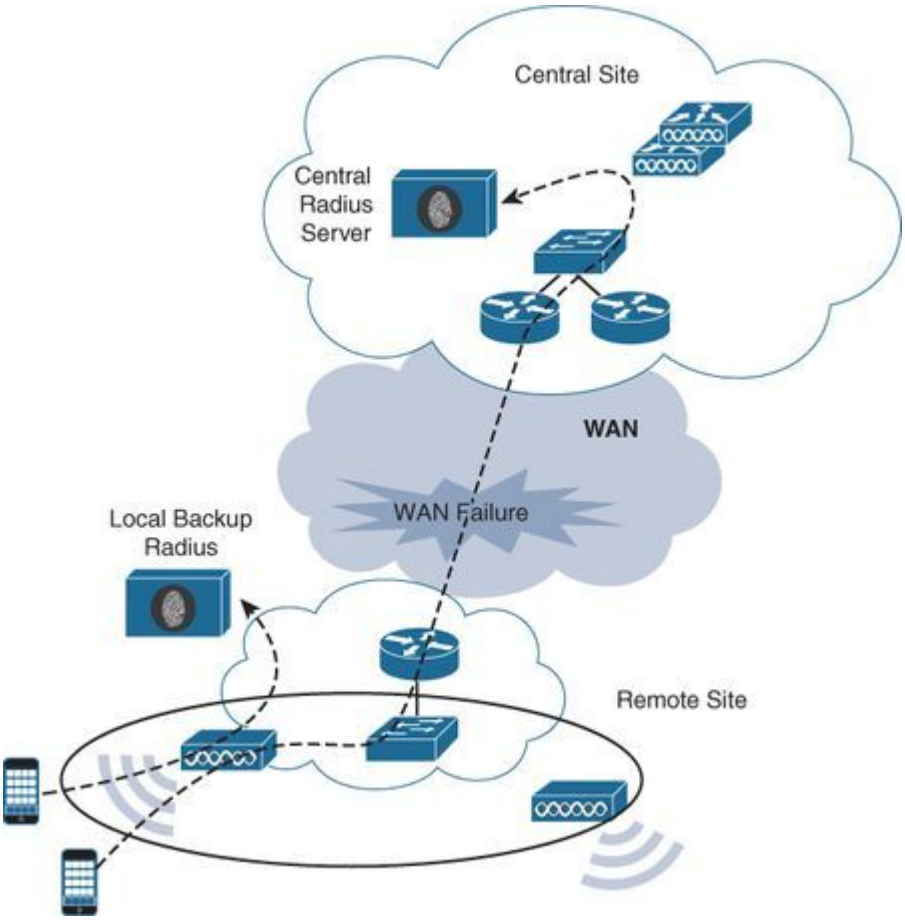
Funktion	Support
Lokales Switching	Unterstützt
Zentrales Switching	Unterstützt
WLAN-VLAN-Zuordnung	Unterstützt
Lokale Authentifizierung mit externem RADIUS	Unterstützt
WPA3-Enterprise	Unterstützt
FT-802.11r Fast-Roaming	Unterstützt
Multi Link Operation (MLO)	Unterstützt
Lokale Authentifizierung mit internem RADIUS	Nicht unterstützt
WPA3-Enterprise-192	Nicht unterstützt

Ausfallsicherheit bei FlexConnect

1. In einer N+1-Konfiguration für Ausfallsicherheit nutzen mehrere aktive Controller einen gemeinsamen Backup-Controller, der bei einem Ausfall eines aktiven Controllers die Leitung übernimmt. Wenn ein primärer Controller offline geht, wechseln die FlexConnect APs sofort in den Standalone-Modus und suchen nach dem Backup-Controller. Während dieser Trennperiode werden zentral geschaltete Clients von den APs getrennt. Sobald die APs den Backup-Controller lokalisiert und mit diesem synchronisiert haben, werden die Clients, die Zugriff auf zentral geschaltete SSIDs benötigen, erneut verbunden. Lokal geswitchte Clients bleiben derweil unbeeinträchtigt und arbeiten weiter, ohne dass die Service-Unterbrechung bemerkt wird.
2. Stellen Sie am Remote-Standort einen AAA-Backup-Server bereit, auf den die FlexConnect-

Gruppe zugreifen kann. Bei aktivierter lokaler Authentifizierung wird dieser RADIUS-Backup-Server nur verwendet, wenn die Access Points in den Standalone-Modus wechseln. Er bleibt inaktiv, während sich die Access Points im verbundenen Modus befinden. Wenn FlexConnect-APs den lokalen Backup-AAA-Server für die Authentifizierung verwenden, werden die Authentifizierungsschlüssel auf alle APs in der FlexConnect-Gruppe verteilt, genau wie bei einem zentralisierten AAA-Server. So wird sichergestellt, dass neue Clients auch bei Verwendung des Backup-RADIUS-Servers nahtlos zwischen APs wechseln können, ohne dass eine erneute Authentifizierung erforderlich ist.

3. Jede in der Funktionsmatrix für Cisco Wireless Access Points vorhandene Methode, die die lokale Authentifizierung ermöglicht.



Clients authentifizieren sich auf einem lokalen AAA-Backup-Server, wenn der zentrale AAA-Server aufgrund eines WAN-Fehlers nicht mehr verfügbar ist.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

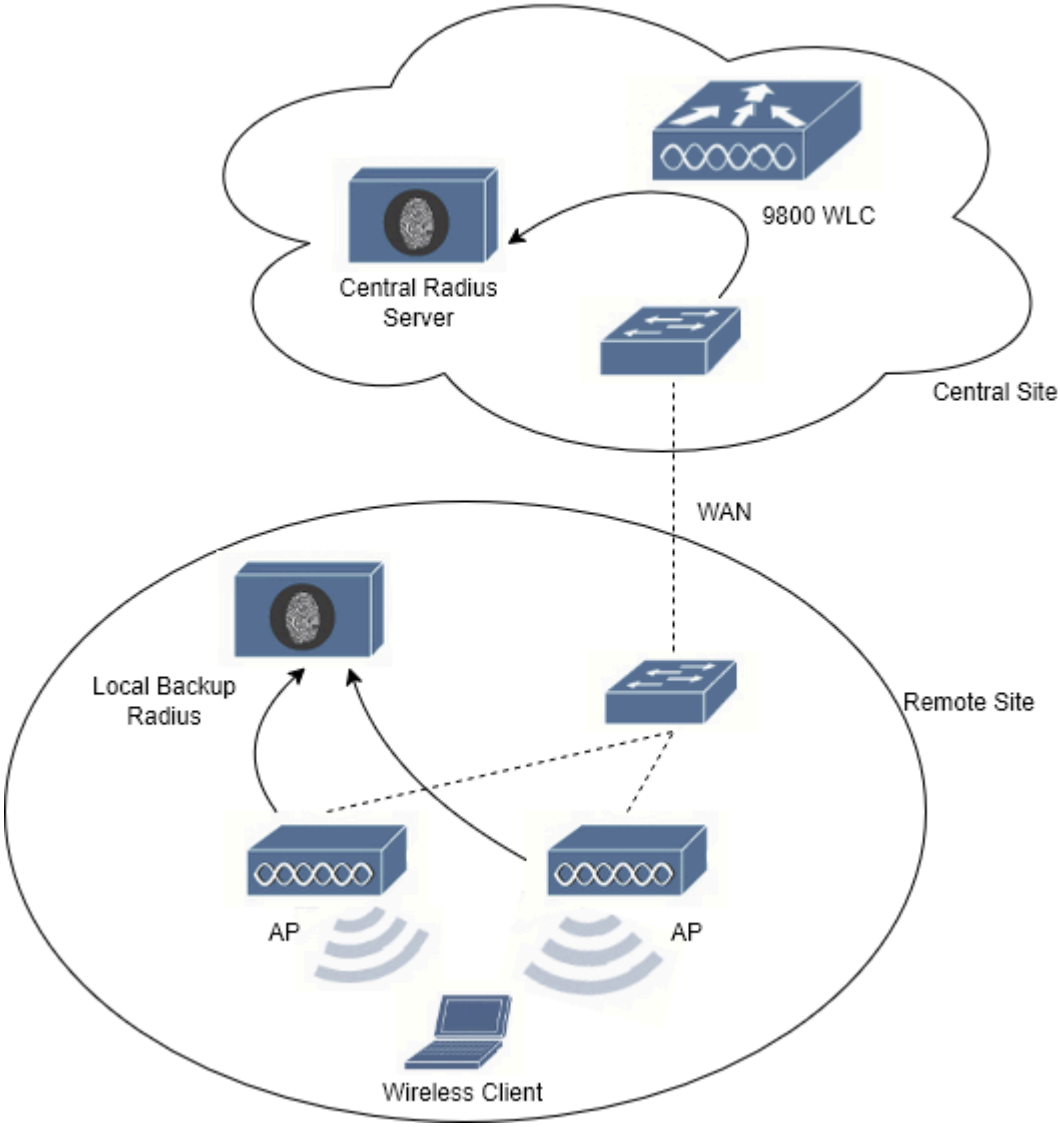
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst Wireless Controller C9800-CL für die Cloud mit Cisco IOS® XE Dublin 17.18.3
- Catalyst CW9164I-ROW Access Point v17.18.3.18
- Aironet® AIR-AP2802I-E-K9 Access Point v17.18.3.18
- 2 x Identity Services Engine v3.2.0.542

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 kennen.

Konfigurieren

Netzwerkdiagramm



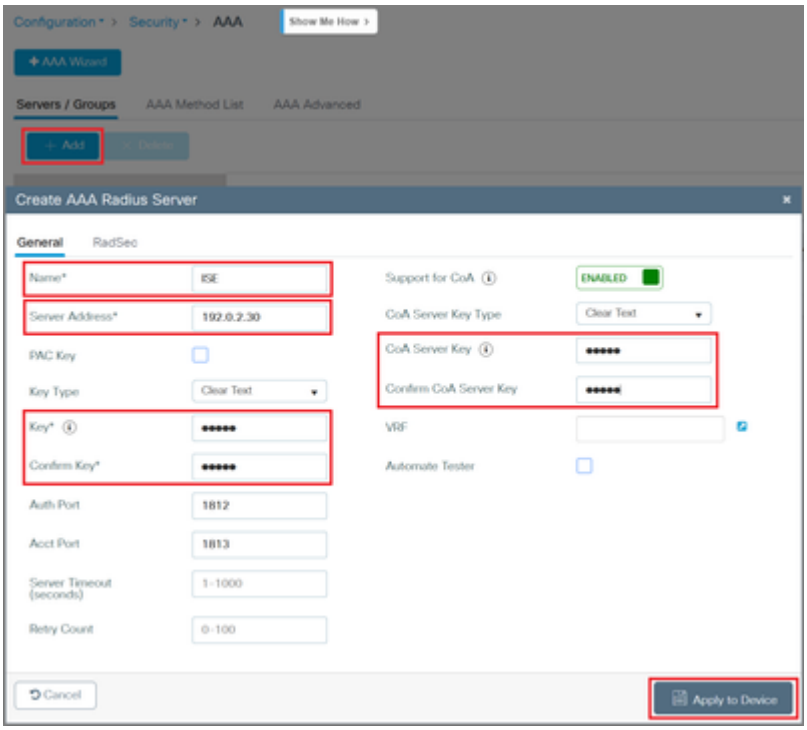
Netzwerkdiagramm

AAA-Server konfigurieren

Schritt 1: Um ein 802.1x-WLAN zu konfigurieren, müssen Sie die AAA-Servergruppe auf dem 9800 WLC erstellen.

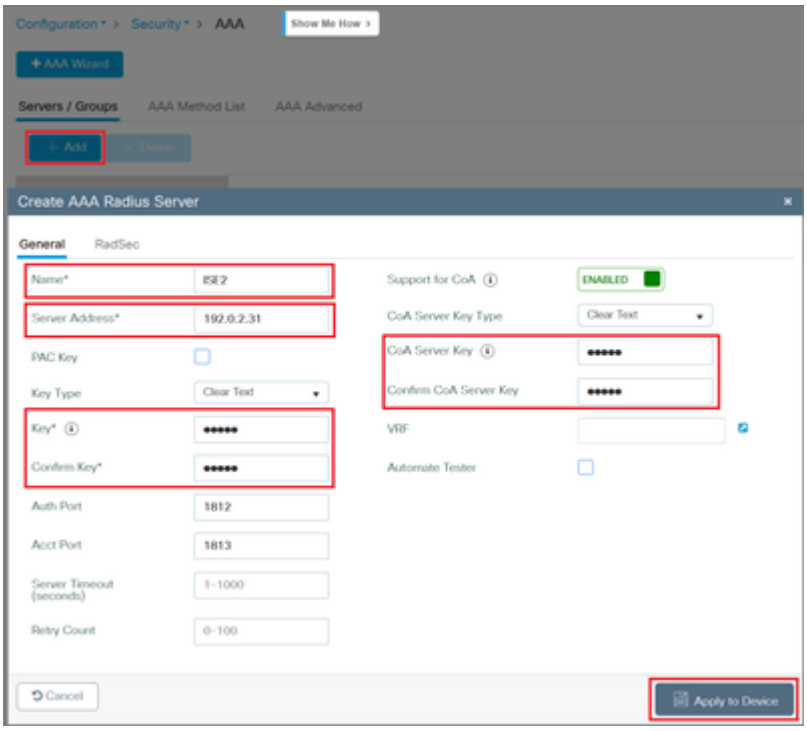
Erstellen Sie für jeden Standort einen AAA-Server - den Server am zentralen Standort und den Server am Remote-Standort.

Navigieren Sie zu Konfiguration > Sicherheit > AAA > Server/Gruppen > Server, und wählen Sie +Hinzufügen. Geben Sie einen Namen für den Server, seine IP-Adresse, den Schlüssel (und den Bestätigungsschlüssel) ein, aktivieren Sie die Unterstützung für CoA (Autorisationsänderung), und geben Sie den CoA-Serverschlüssel (und bestätigen Sie den CoA-Serverschlüssel) ein. Die Schlüssel müssen identisch sein.



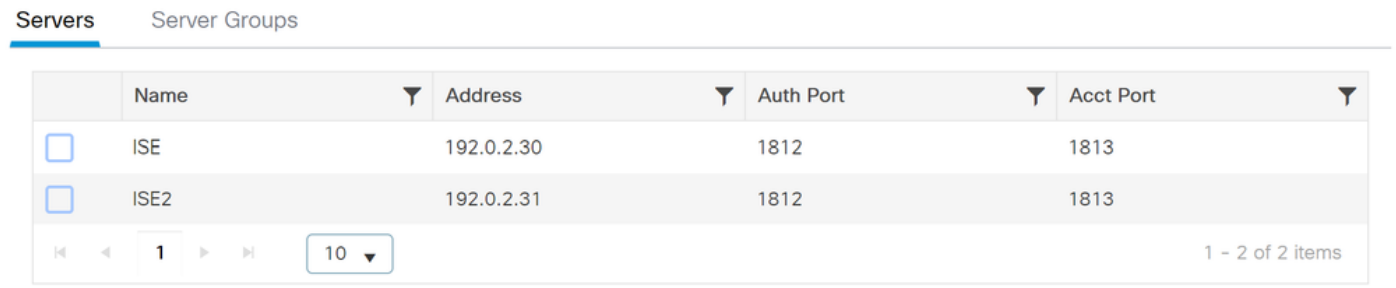
Klicken Sie auf Auf Gerät anwenden.

Schritt 2: Erstellen Sie den anderen AAA-Server:

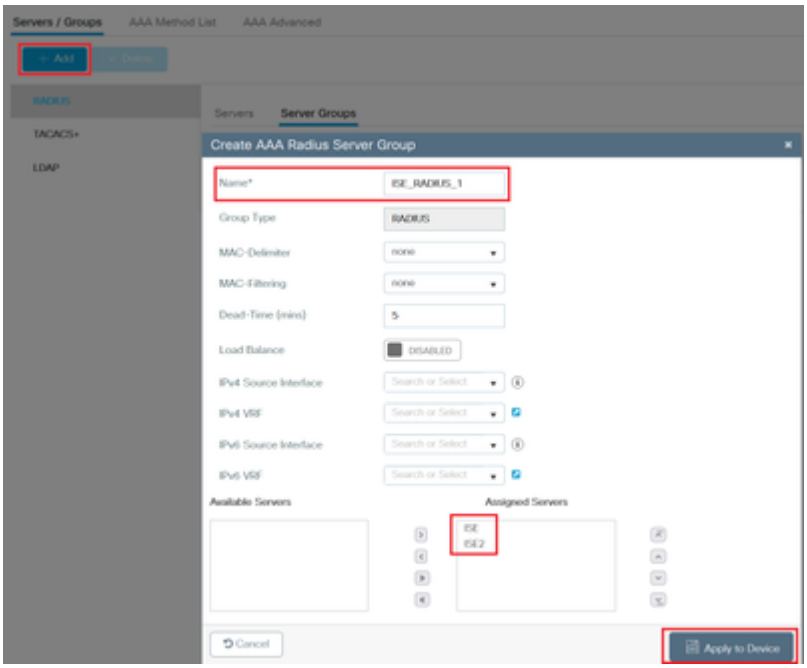


Klicken Sie auf Auf Gerät anwenden.

Ihre AAA-Server sind jetzt konfiguriert:

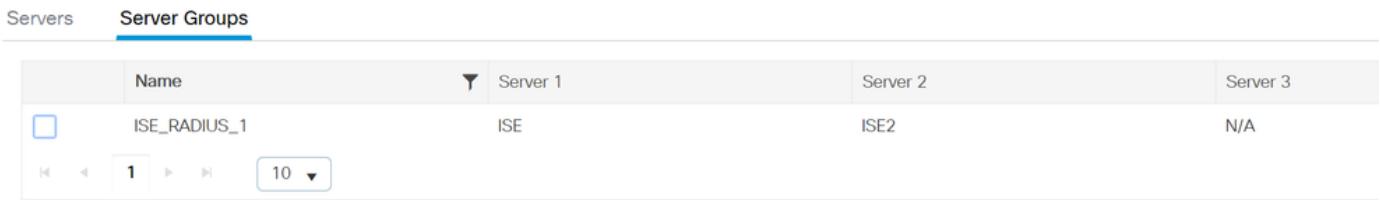


Schritt 3: Navigieren Sie zu Konfiguration > Sicherheit > AAA > Server/Gruppen > Servergruppen, und wählen Sie +Hinzufügen. Geben Sie dem Gruppenserver einen Namen, und wählen Sie die zuvor erstellten AAA-Server in der Spalte Zugewiesene Server aus:



Klicken Sie auf Auf Gerät anwenden.

Anschließend wird die konfigurierte AAA-Servergruppe angezeigt:



CLI:

```
aaa new-model
```

```
!
radius server ISE
address ipv4 192.0.2.30 auth-port 1812 acct-port 1813
key keystring
!
radius server ISE2
address ipv4 192.0.2.31 auth-port 1812 acct-port 1813
key keystring
!
aaa server radius dynamic-author
client 192.0.2.30 server-key keystring
client 192.0.2.31 server-key keystring
!
aaa group server radius ISE_RADIUS_1
server name ISE
server name ISE2
deadtime 5
```

Konfiguration des FlexConnect-Modus am Remote-Standort

Schritt 1: Im ersten Schritt wird FlexConnect am Remote-Standort konfiguriert.

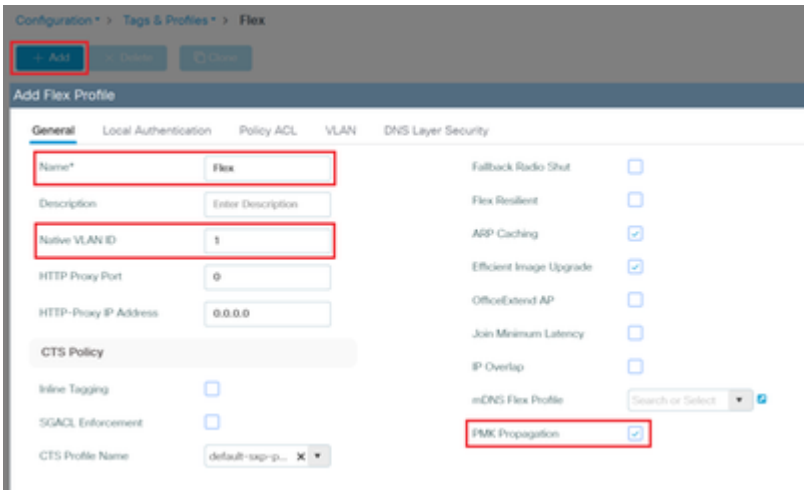
Ändern Sie mit diesem Leitfaden den Modus Ihrer APs in Flex: Verstehen Sie FlexConnect auf dem Catalyst 9800 Wireless Controller.

Die APs in diesem Leitfaden/in dieser Übung verwenden dasselbe Flex Profile-System.

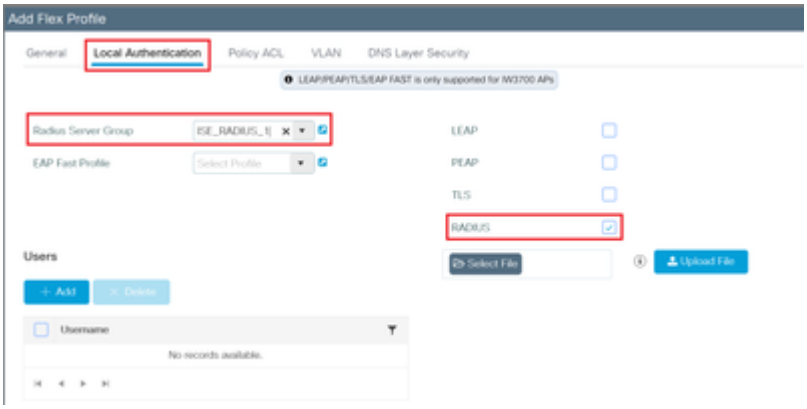
Schritt 2: Navigieren Sie zu Konfiguration > Tags & Profile > Flex.

Erstellen Sie mit +Hinzufügen einen neuen Flex Profile-Namen. Geben Sie auf der Registerkarte Allgemein einen Namen für das Profil ein, geben Sie die ID des nativen VLANs (Virtual Local Area Network) ein, und aktivieren Sie die PMK-Propagierung.

Aktivieren Sie die PMK-Propagierung, um ein nahtloses Wireless-Client-Roaming zu ermöglichen, indem Sie PMK-Informationen für den Access Point an einem einzigen Standort freigeben.

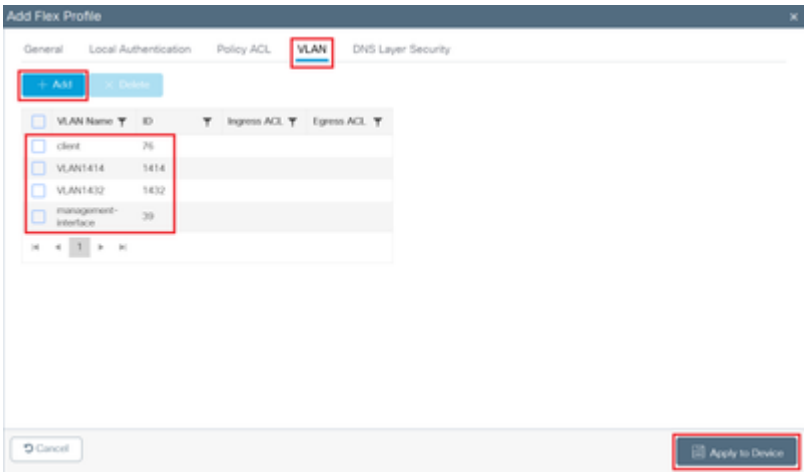


Schritt 3: Wählen Sie für 802.1x WLAN auf der Registerkarte Lokale Authentifizierung die Radius-Servergruppe aus, und aktivieren Sie RADIUS:



Tipp: Bei einem PSK-WLAN müssen Sie auf dieser Registerkarte keine Informationen hinzufügen.

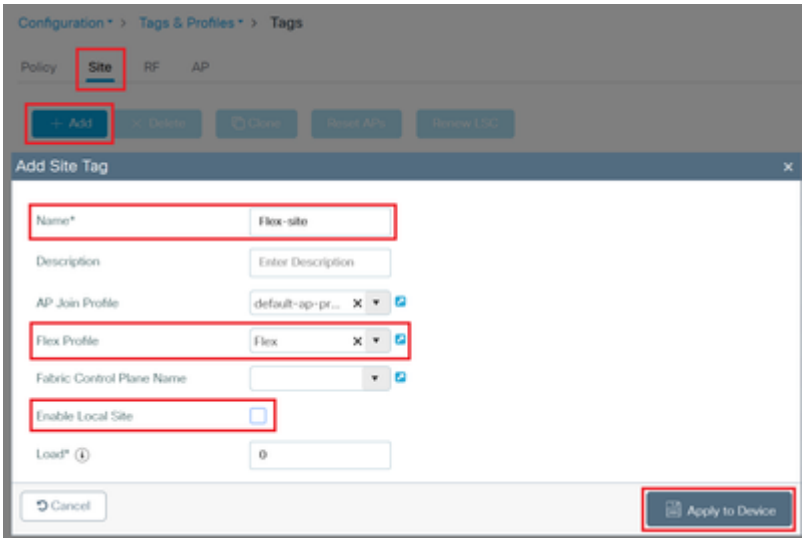
Schritt 4: Auf der Registerkarte VLAN fügen Sie alle VLANs hinzu, die von Clients, APs und RADIUS-Server verwendet werden. Achten Sie darauf, dass jeder VLAN-Name der richtigen VLAN-ID entspricht:



Klicken Sie am Ende auf Aktualisieren und auf Gerät anwenden.

Schritt 5: Navigieren Sie zu Konfiguration > Tags & Profile > Tags > Site, und wählen Sie +Hinzufügen.

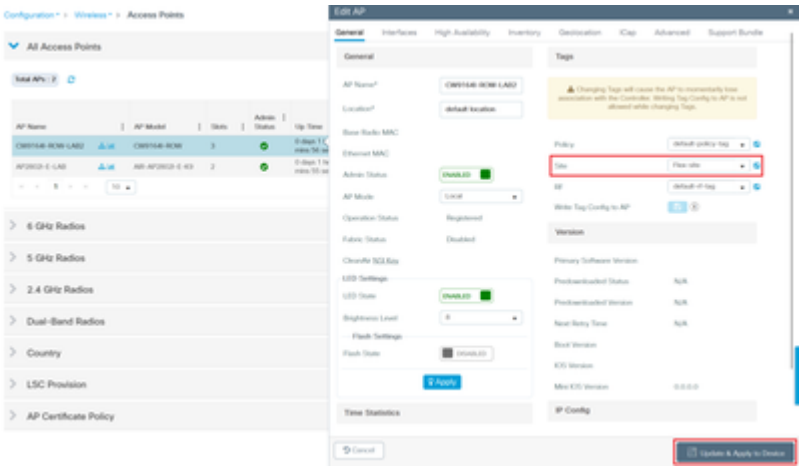
Erstellen Sie das Site-Tag mit dem zuvor erstellten Flex Profile. Geben Sie ihm einen Namen, wählen Sie das richtige Flex Profile aus, und deaktivieren Sie Enable Local Site. Stellen Sie sicher, dass das Zugangsprofil der richtige ist.



Klicken Sie auf Auf Gerät anwenden.

Schritt 6: Navigieren Sie zu Konfiguration > Wireless > Access Points.

Wählen Sie Ihren AP aus, und ändern Sie unter Allgemein > Tags die Site-Tag-Nummer zu der zuvor konfigurierten Tag-Nummer:



Klicken Sie auf Aktualisieren und auf Gerät anwenden.

Der Access Point wird vom WLC getrennt und im Flex AP-Modus wieder verbunden.

Wenn der Access Point erneut beitritt, können Sie auf derselben Seite den Access Point-Modus in der Spalte "Access Point-Modus" überprüfen.

Wenn Sie den Access Point auswählen, wird das neue Site-Tag angezeigt:



CLI:

```
wireless profile flex Flex
ip http client proxy 0.0.0.0 0
local-auth radius-server-group ISE_RADIUS_1
vlan-name client
vlan-id 76
vlan-name VLAN1414
vlan-id 1414
vlan-name VLAN1432
vlan-id 1432
vlan-name management-interface
vlan-id 39
pmk propagate
!
wireless tag site Flex-site
ap-profile default-ap-profile
no local-site
flex-profile Flex
```

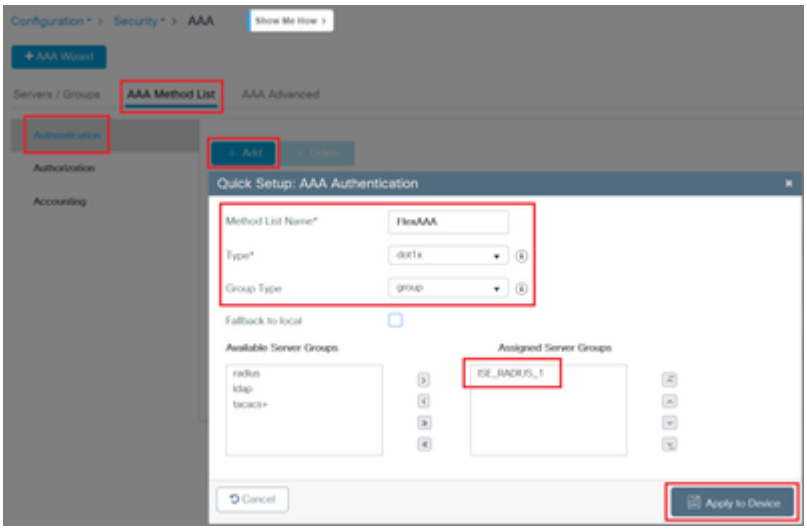
```
!
ap h.h.h (AP Radio MAC address)
policy-tag default-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

Konfiguration eines 802.1x-WLAN mit lokaler Authentifizierung über einen externen RADIUS-Server

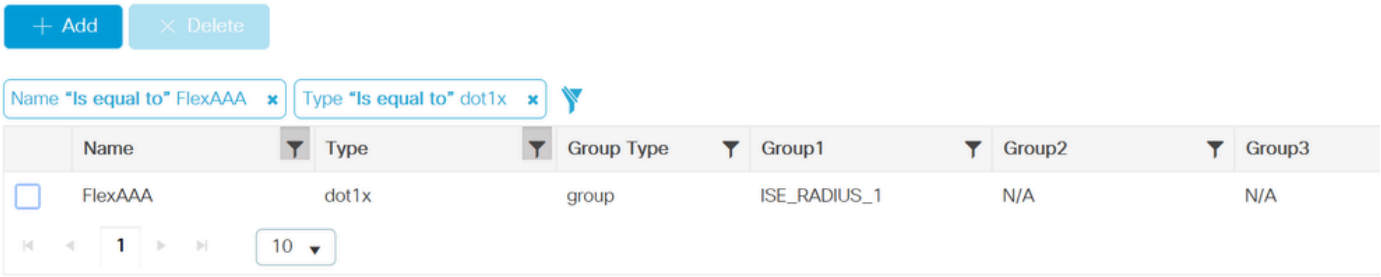
Schritt 1: Erstellen Sie die Liste der Authentifizierungsmethoden.

Navigieren Sie zu Configuration > Security > AAA (Konfiguration > Sicherheit > AAA) auf der Registerkarte AAA Method List (AAA-Methodenliste > Authentifizierung).

Wählen Sie +Hinzufügen, geben Sie einen Namen für den Namen der Methodenliste ein, wählen Sie dot1x als Typ aus, wählen Sie Gruppe als Gruppentyp aus, und weisen Sie die AAA-Servergruppe in der Spalte Zugewiesene Servergruppen zu:



Nun wird die erstellte AAA-Methodenliste angezeigt:



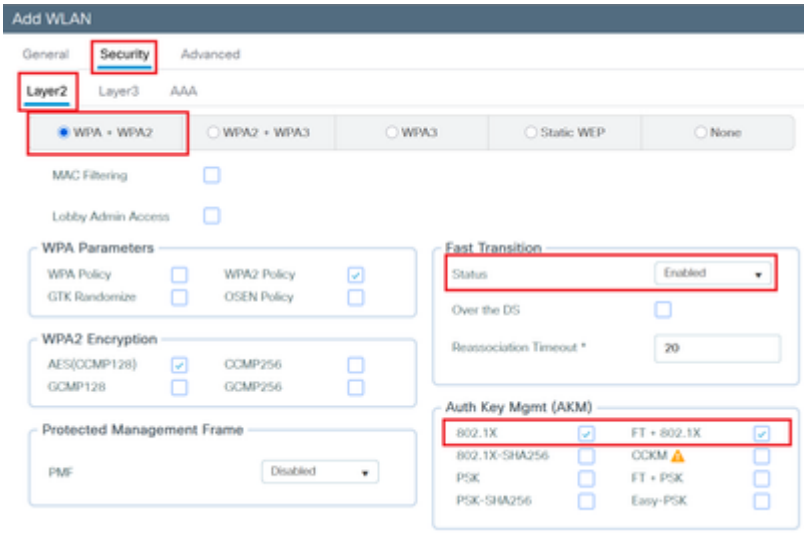
Schritt 2: Erstellen Sie das WLAN.

Navigieren Sie zu Configuration > Tags & Profiles > WLANs, und wählen Sie +Add.

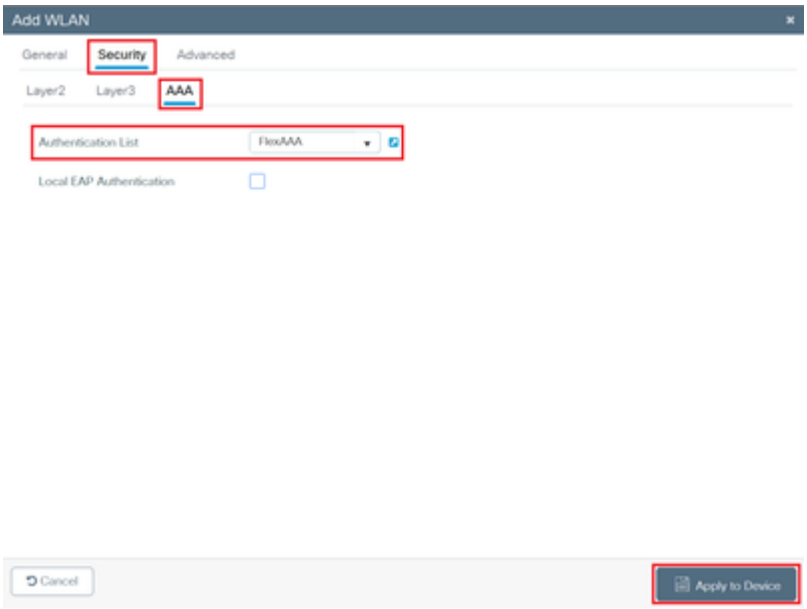
Erstellen Sie unter General einen Namen für den Profilnamen, die SSID und den Aktivierungsstatus:



Schritt 3: Navigieren Sie zu Sicherheit > Layer 2 Registerkarte, wählen Sie WPA+WPA2 (Wi-Fi Protected Access), Fast Transition as Enabled (Schneller Übergang als aktiviert), Auth Key Mgmt 802.1X und FT+802.1X aus:



Schritt 4: Navigieren Sie zur Registerkarte Security > AAA, und wählen Sie im Dropdown-Menü Authentication List (Authentifizierungsliste) die zuvor erstellte Liste aus:



Klicken Sie auf Aktualisieren und auf Gerät anwenden.

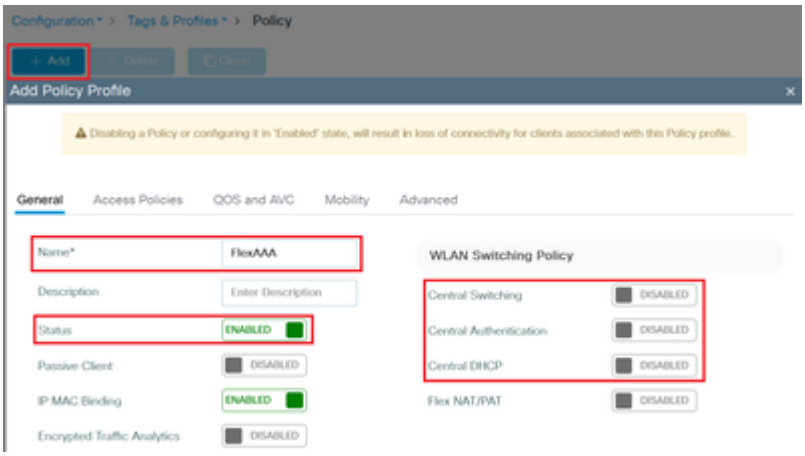
Anschließend wird das erstellte WLAN angezeigt:



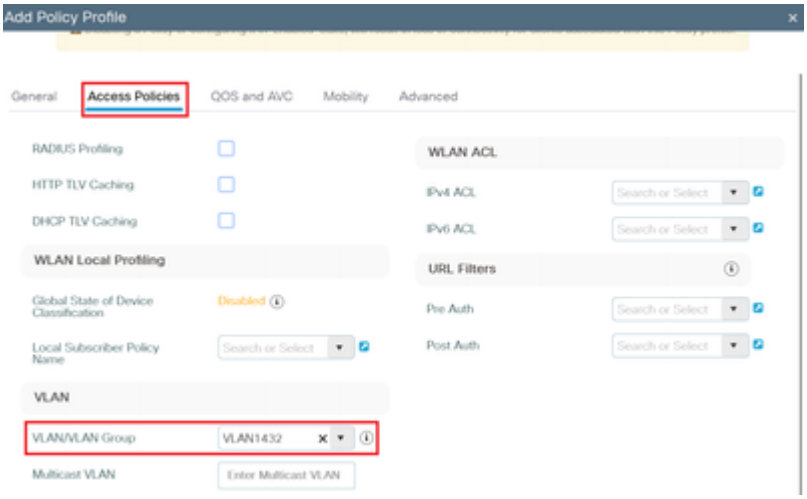
Schritt 5: Erstellen Sie das Richtlinienprofil.

Navigieren Sie zu Konfiguration > Tags und Profile > Richtlinie.

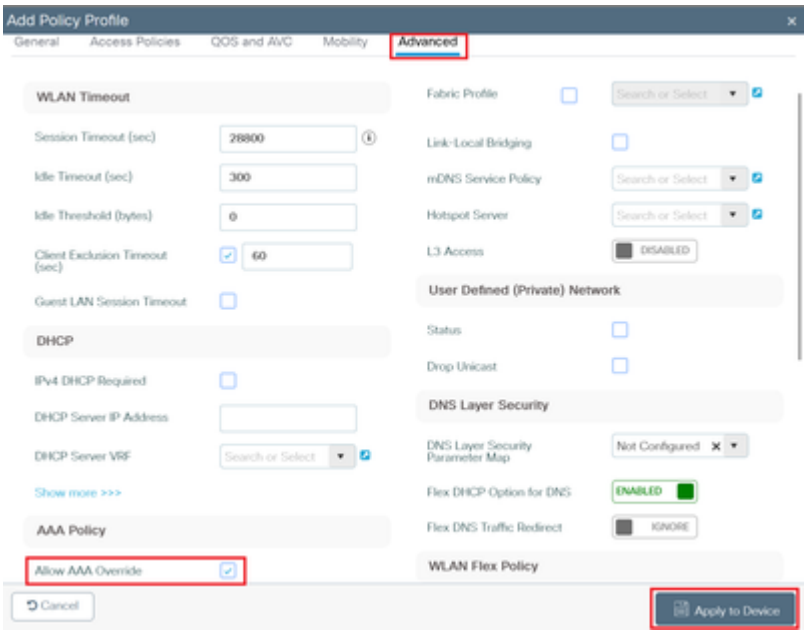
Wählen Sie +Hinzufügen und geben Sie auf der Registerkarte Allgemein einen Namen für das Richtlinienprofil ein, aktivieren Sie den Status, und deaktivieren Sie das zentrale Switching, die zentrale Authentifizierung und das zentrale DHCP (Dynamic Host Configuration Protocol):



Schritt 6. Navigieren Sie zur Registerkarte Access Policies (Zugriffsrichtlinien), und wählen Sie das VLAN aus:

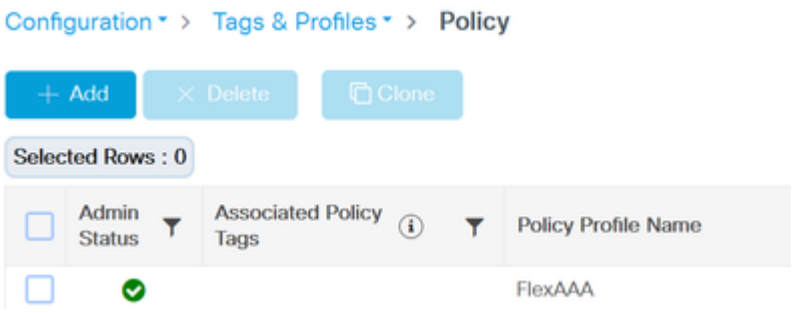


Schritt 7: Navigieren Sie zur Registerkarte Erweitert, aktivieren Sie AAA-Außerkraftsetzung zulassen.:



Klicken Sie auf Aktualisieren und auf Gerät anwenden.

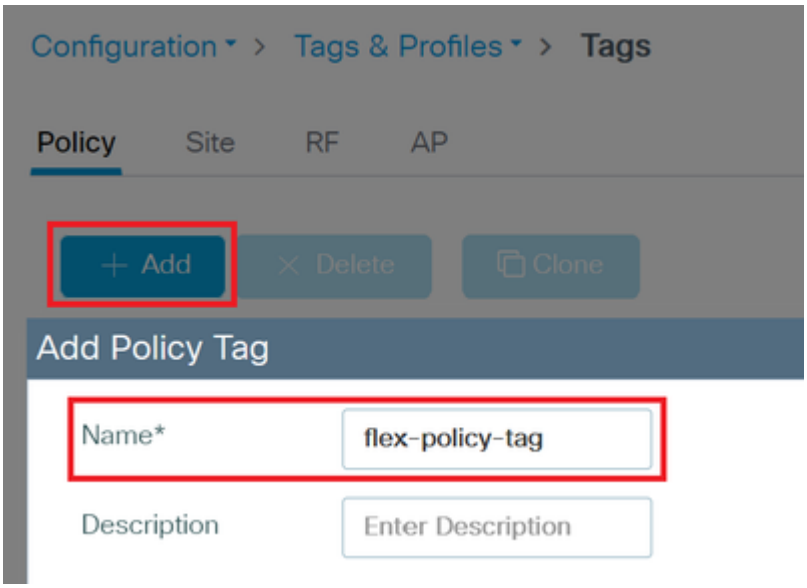
Das Richtlinienprofil wird in der Liste angezeigt:



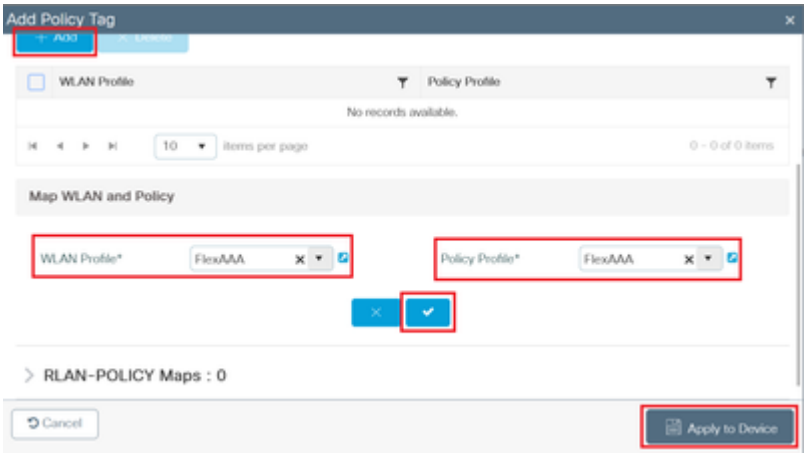
Schritt 8: Policy-Tag erstellen

Navigieren Sie zu Konfiguration > Tags & Profile > Tags.

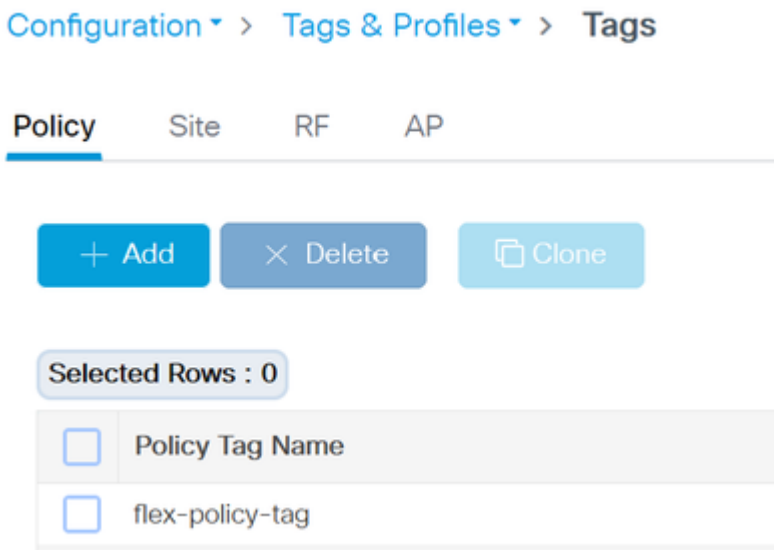
Wählen Sie auf der Registerkarte Policy (Richtlinie) +Add (Hinzufügen). Geben Sie einen Namen für das Policy-Tag ein:



Blättern Sie nach unten, und wählen Sie +Hinzufügen unter WLAN-POLICY Maps aus. Wählen Sie im WLAN Profile (WLAN-Profil) das zuvor erstellte WLAN aus dem Dropdown-Menü aus. Wählen Sie im Dropdown-Menü Policy Profile (Richtlinienprofil) das zuvor erstellte Richtlinienprofil aus. Klicken Sie auf die Schaltfläche zum Aktivieren und dann auf Auf Gerät anwenden:

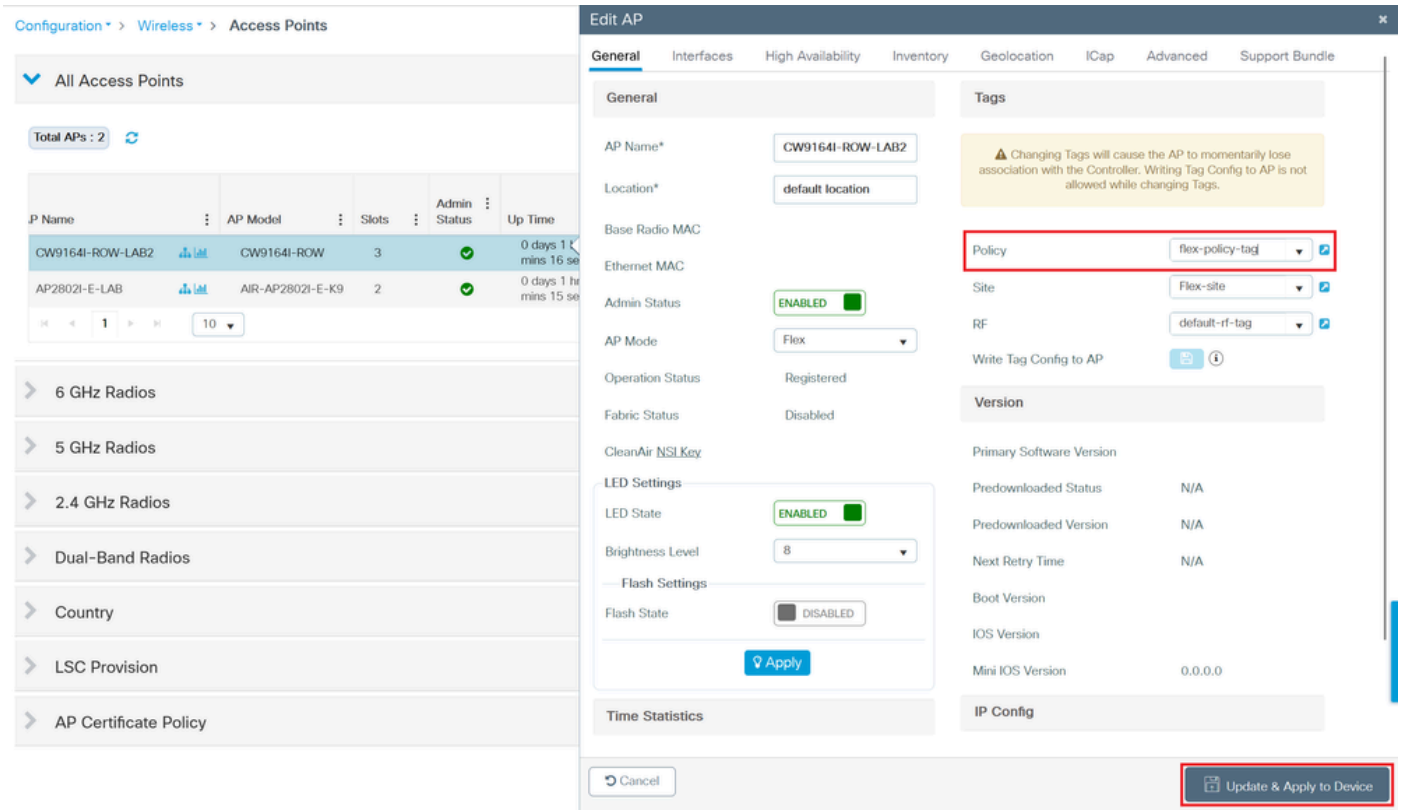


Das Policy-Tag wird in der Liste angezeigt:



Schritt 9: Weisen Sie dem AP-Tag das Policy-Tag zu.

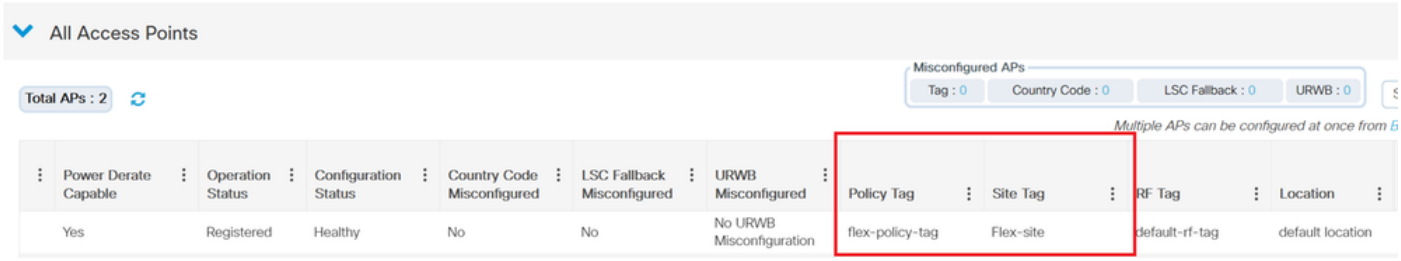
Navigieren Sie zu Konfiguration > Wireless > Access Points. Wählen Sie den Access Point aus, um das Tag zu ändern.



Klicken Sie auf Aktualisieren und auf Gerät anwenden.

Der Access Point trennt sich und tritt mit dem neuen Policy-Tag wieder ein.

Wenn der Access Point wieder hinzugefügt wird, können Sie die Liste der Access Points überprüfen, überprüfen, ob sich der Access Point im Flex-Modus befindet, und die zugewiesenen Tags überprüfen:



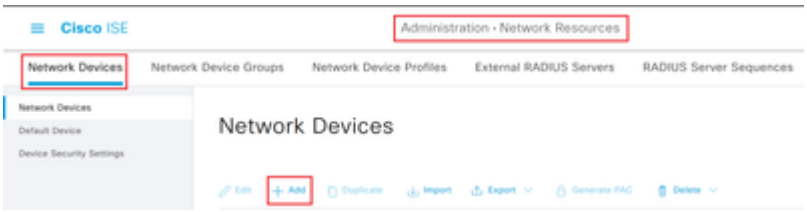
CLI:

```
aaa authentication dot1x FlexAAA group ISE_RADIUS_1
!
wlan FlexAAA 4 FlexAAA
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa akm ft dot1x
security dot1x authentication-list FlexAAA
no shutdown
!
wireless profile policy FlexAAA
aaa-override
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

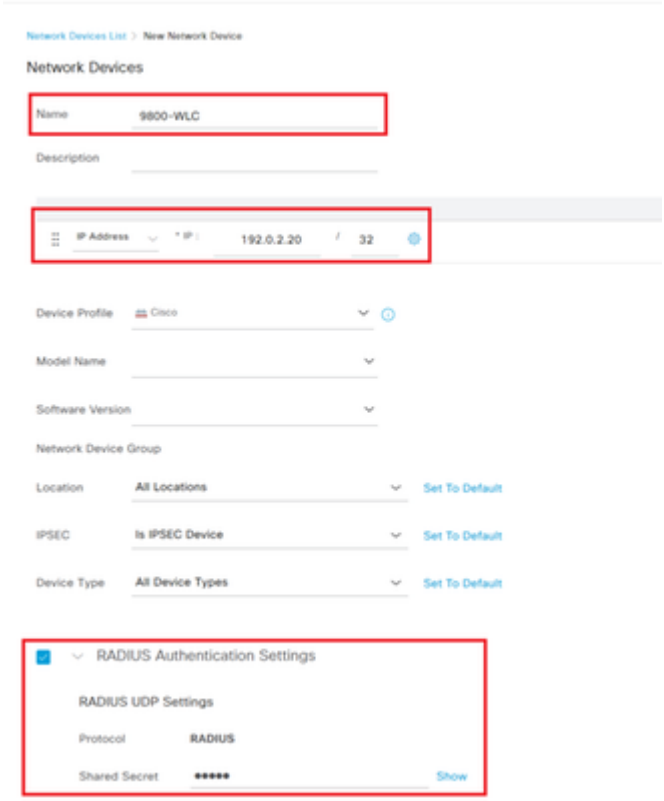
Konfigurieren der ISE

Jetzt müssen Sie die ISE so konfigurieren, dass Clients authentifiziert werden können, wenn sie sich in der lokalen Authentifizierung befinden.

Schritt 1:Navigieren Sie zu Administration > Network Resources > Network Devices. Wählen Sie +Hinzufügen.



Schritt 2: Hinzufügen des 9800 WLC Geben Sie ihm einen Namen, fügen Sie seine IP-Adresse hinzu, aktivieren Sie die RADIUS-Authentifizierungseinstellungen, und fügen Sie den Schlüssel für den gemeinsamen geheimen Schlüssel hinzu. Dieser Schlüssel muss mit dem Schlüssel identisch sein, den Sie zuvor beim Erstellen der AAA-Server auf dem 9800 WLC konfiguriert haben.



Klicken Sie unten rechts auf Speichern.

Schritt 3: Wir müssen die APs zur Liste der Netzwerkgeräte hinzufügen, damit sie als AAA-Authentifizierer/Forwarder agieren können, wenn der Remote-Standort die WAN-Verbindung verliert (und wenn die APs in den Standalone-Modus wechseln).

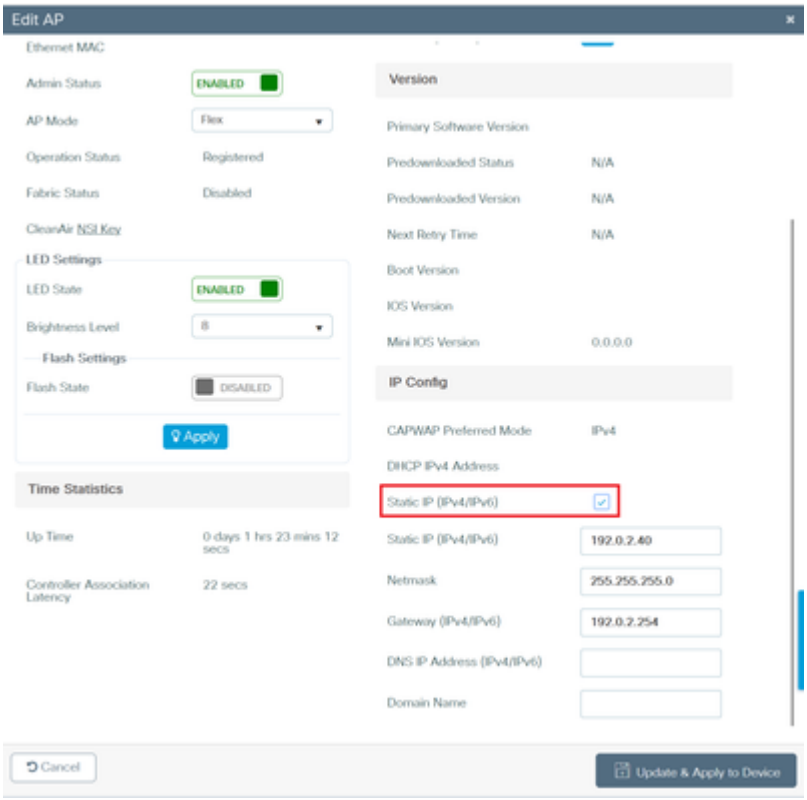
Navigieren Sie in der GUI des 9800 WLC zu Configuration > Wireless > Access Points, und notieren Sie sich die einzelnen AP-IP-Adressen.

Anmerkung: Konfigurieren Sie die IP-Adresse jedes Flex AP auf "Statisch". Wenn die APs

---

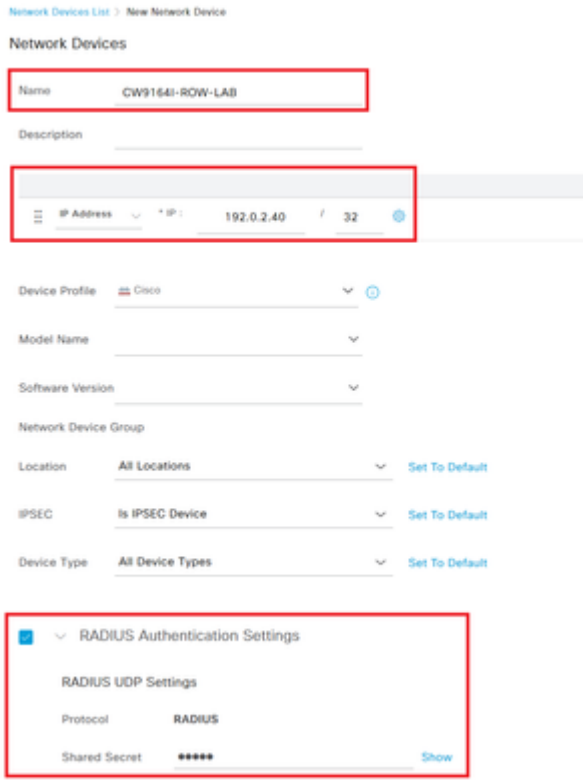
die Verbindung zum 9800 WLC verlieren und wieder herstellen, können sie eine andere IP-Adresse von DHCP verwenden und damit die Kommunikation mit der ISE verlieren.

Aktivieren Sie Static IP (IPv4/IPv6). Klicken Sie auf Aktualisieren und auf Gerät anwenden:



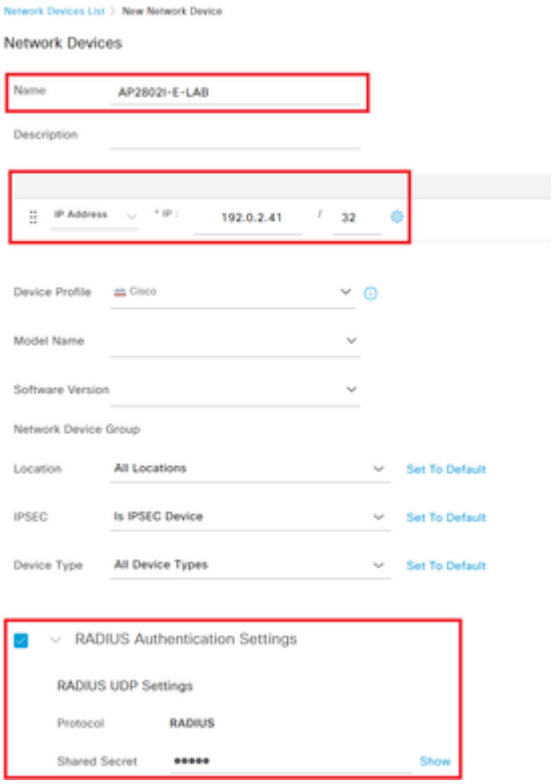
Schritt 4: Navigieren Sie auf der ISE zu Administration > Network Resources > Network Devices (Verwaltung > Netzwerkressourcen > Netzwerkgeräte). Wählen Sie +Hinzufügen.

Fügen Sie Ihre APs als Netzwerkgeräte hinzu, dieselbe Konfiguration wie beim 9800 WLC:



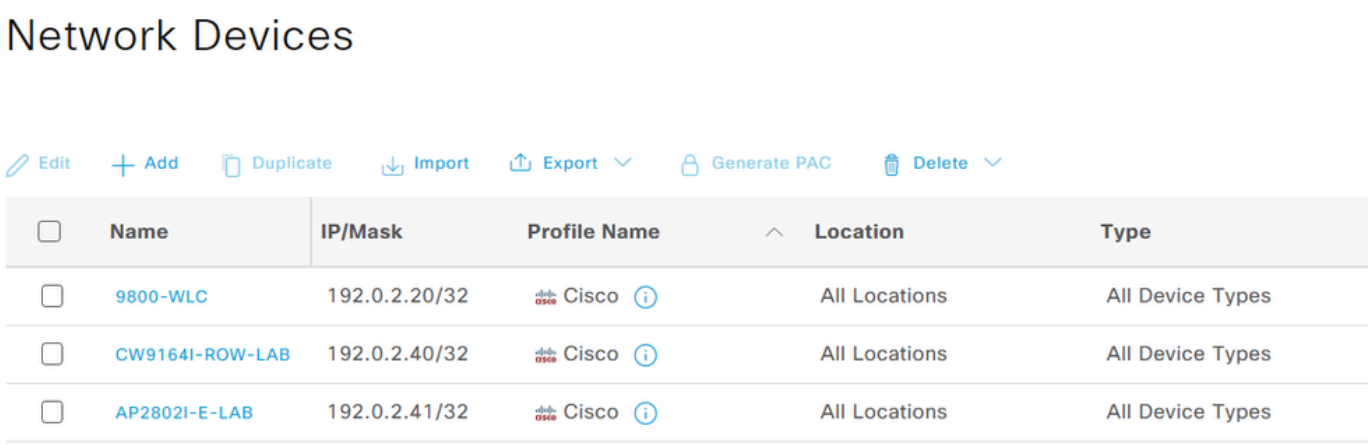
Klicken Sie unten rechts auf Speichern.

Für den zweiten AP:



Klicken Sie unten rechts auf Speichern.

Die folgende Liste der Netzwerkgeräte wird angezeigt:

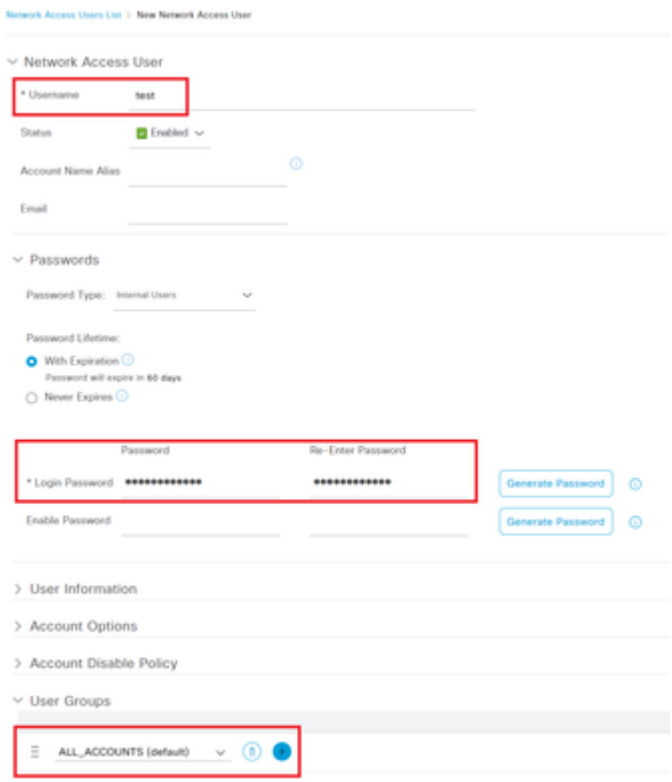


Wenn sich Ihre APs in zusammenhängenden IP-Bereichen befinden, können Sie die Maskenfunktion verwenden, um einen einzelnen Eintrag zu konfigurieren, der den gemeinsamen geheimen Schlüssel für eine ganze Gruppe (wenn nicht für alle) von APs definiert. Es ist nicht erforderlich, in der ISE ein Netzwerkgerät pro WAP zu konfigurieren. Beachten Sie jedoch, dass Sie durch die Verwendung von Platzhaltern und Masken Raum für ein nicht autorisiertes Gerät lassen, um als Forwarder für die ISE zu fungieren.

Schritt 5: Navigieren Sie zu Administration > Identity Management > Identities (Verwaltung > Identitätsverwaltung > Identitäten), auf der Registerkarte Users (Benutzer), und erstellen Sie einen Benutzer für die 802.1x-Authentifizierung. Auswählen +Hinzufügen:

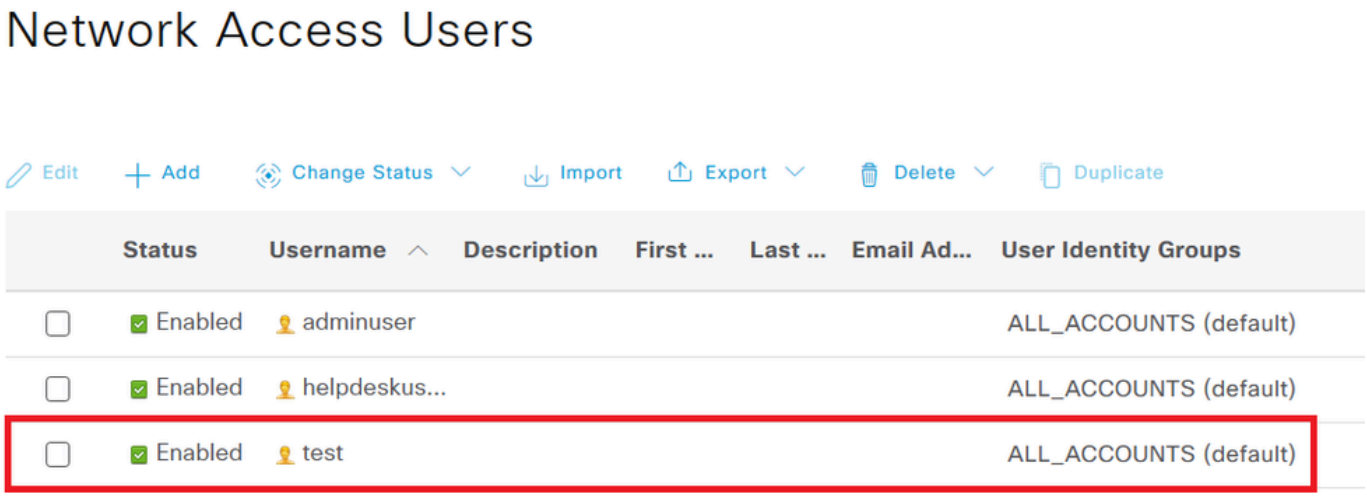


Erstellen Sie einen Benutzernamen und das Kennwort (und geben Sie dasselbe Kennwort unter Kennwort erneut eingeben ein), und wählen Sie im Dropdown-Menü "Benutzergruppen" die Option ALL_ACCOUNTS (Standard) aus:

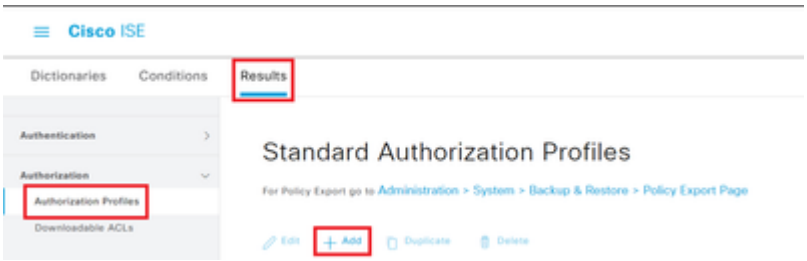


Klicken Sie unten rechts auf Senden.

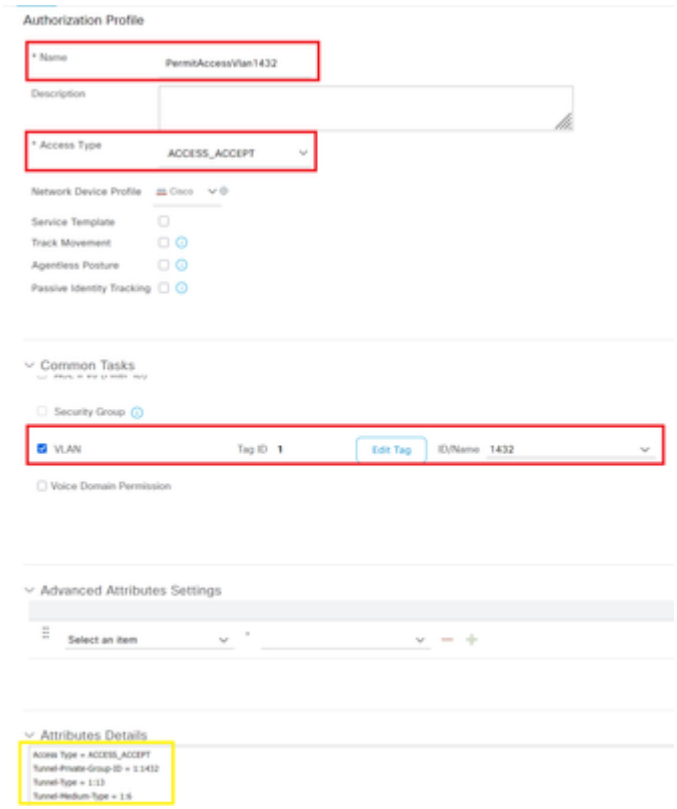
Der Benutzer wird in der Liste der Netzwerkzugriffsbenutzer angezeigt:



Schritt 6: Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse. Wählen Sie auf der Registerkarte Autorisierung > Autorisierungsprofile die Option +Hinzufügen aus.



Erstellen Sie das Autorisierungsprofil für das VLAN, dem die lokalen Authentifizierungsclients zugewiesen sind:

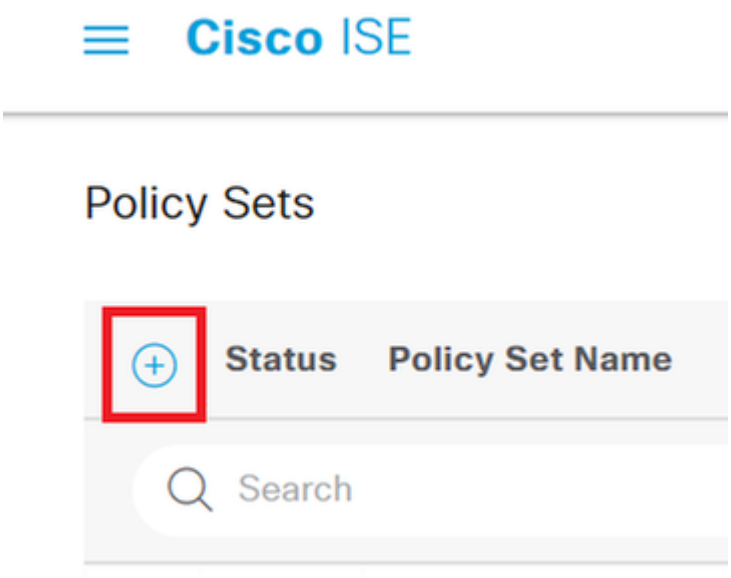


Klicken Sie unten rechts auf Senden.

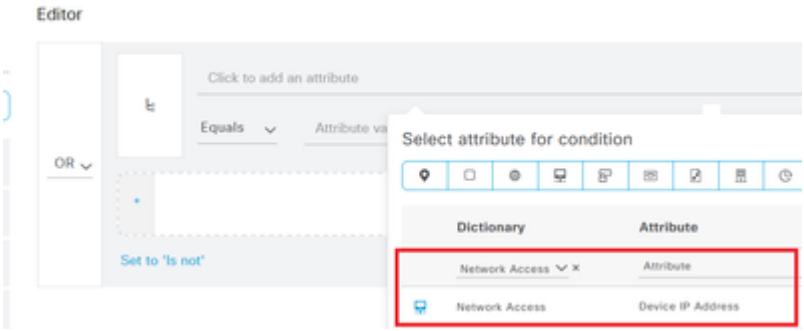
Die von der ISE an die WLC/APs gesendeten Attributdetails werden in einem erfolgreichen Szenario angezeigt.

Schritt 7: Navigieren Sie zu Richtlinie > Richtliniensätze. Erstellen Sie einen neuen Policy Set.

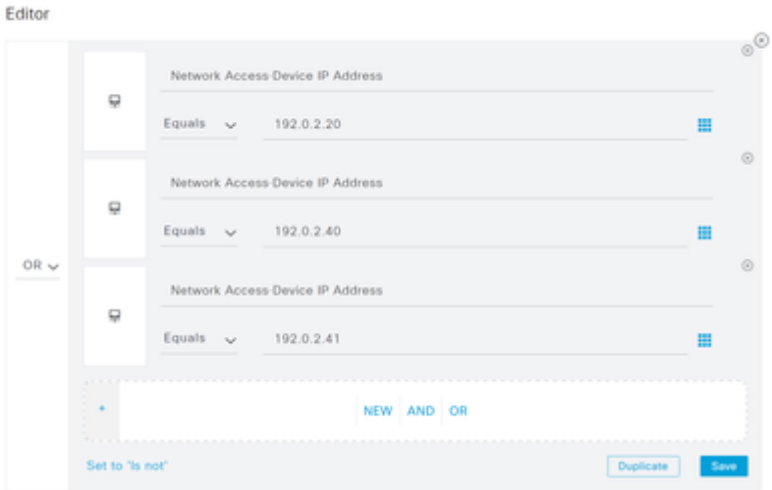
Klicken Sie auf das Zeichen +:



Geben Sie dem Richtliniensatz einen Namen. Fügen Sie in der Spalte Bedingungen die OR-Regel hinzu, und fügen Sie das Wörterbuch Netzwerkzugriff hinzu. Wählen Sie unter Attribute Geräte-IP-Adresse die Option Gleich:

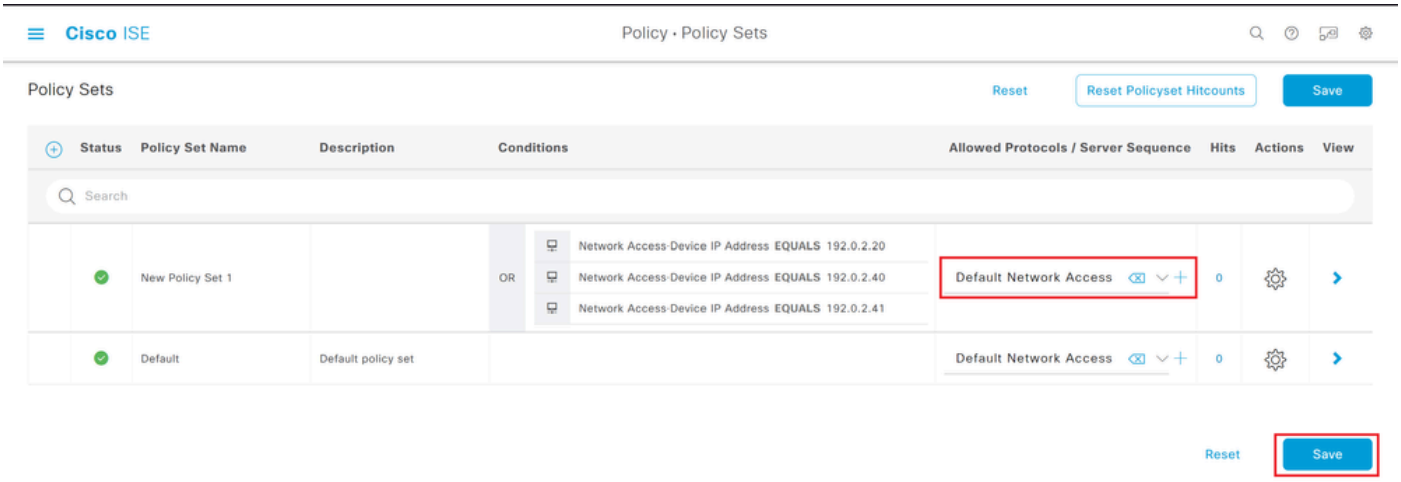


Fügen Sie den 9800 WLC und die IP-Adressen der APs hinzu:

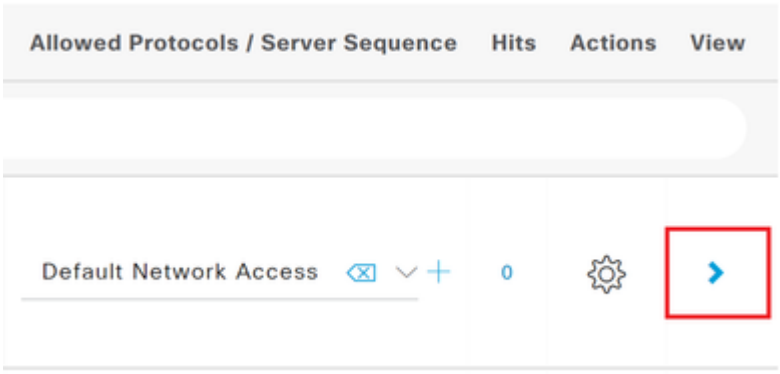


Klicken Sie unten rechts auf Verwenden.

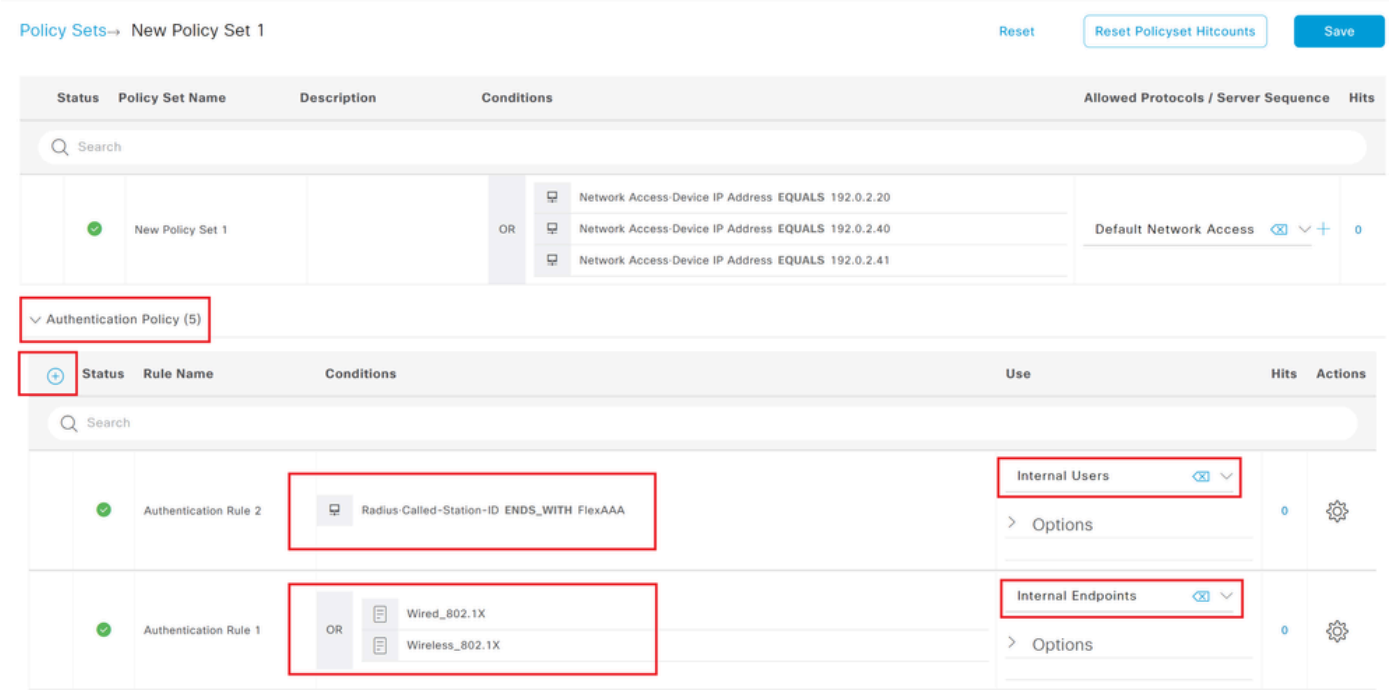
Schritt 8: Wählen Sie in der Spalte Zugelassene Protokolle die Option Standard-Netzwerkzugriff aus. Klicken Sie am Ende auf Speichern:



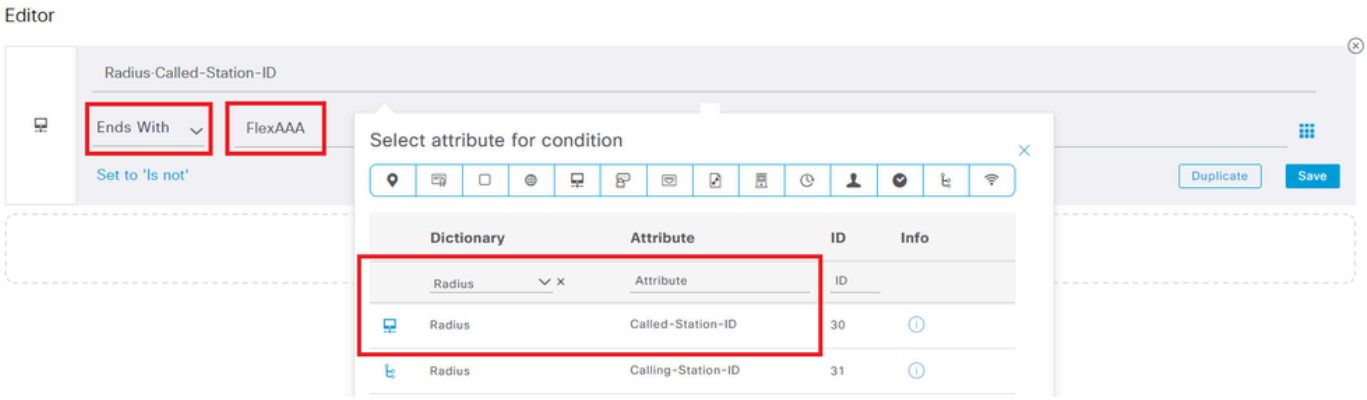
Schritt 9. Klicken Sie in der Spalte Ansicht auf das Pfeilzeichen:



Schritt 10. Erweitern Sie die Authentifizierungsrichtlinie, und erstellen Sie zwei neue Richtlinien: einen für den WLAN-Namen, den anderen für die 802.1X-Konfiguration:

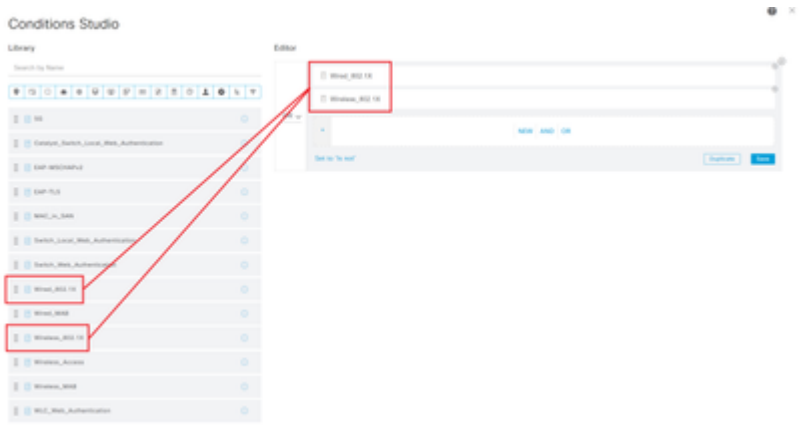


Erstellen Sie als WLAN-Namen die Bedingung mit dem Dictionary Radius und dem Attribut "Called-Station-ID". Wählen Sie Ends With (Endet mit) aus, und geben Sie den WLAN-Namen ein:



Klicken Sie unten rechts auf Verwenden. Wählen Sie für diese Richtlinie in der Spalte Verwendung die Option Interne Benutzer aus.

Schritt 11: Erstellen Sie für die 802.1X-Richtlinie die Bedingung mit der Wired_802.1X- und Wireless_802.1X-Bibliothek, die auf der ISE verfügbar ist. Sie können diese Elemente per Drag-and-Drop verschieben und die Bedingung auswählen ODER:



Klicken Sie unten rechts auf Verwenden. Wählen Sie für diese Richtlinie in der Spalte Verwendung die Option Interne Endpunkte aus.

Schritt 12: Blättern Sie nach unten zur Autorisierungsrichtlinie, und erstellen Sie eine neue Richtlinie. Geben Sie ihm einen Namen, und erstellen Sie dieselbe Bedingung wie die für den WLAN-Namen in der Authentifizierungsrichtlinie erstellte.

Wählen Sie in der Spalte Profile aus dem Dropdown-Menü das Profil PermitAccessVlan1432 aus:



Klicken Sie unten rechts auf Speichern.

Konfiguration des PSK-WLAN mit lokaler Authentifizierung

Schritt 1: Konfigurieren Sie die APs zunächst im Flex-Modus, wie im Abschnitt Konfigurieren des FlexConnect-Modus am Remote-Standort beschrieben.

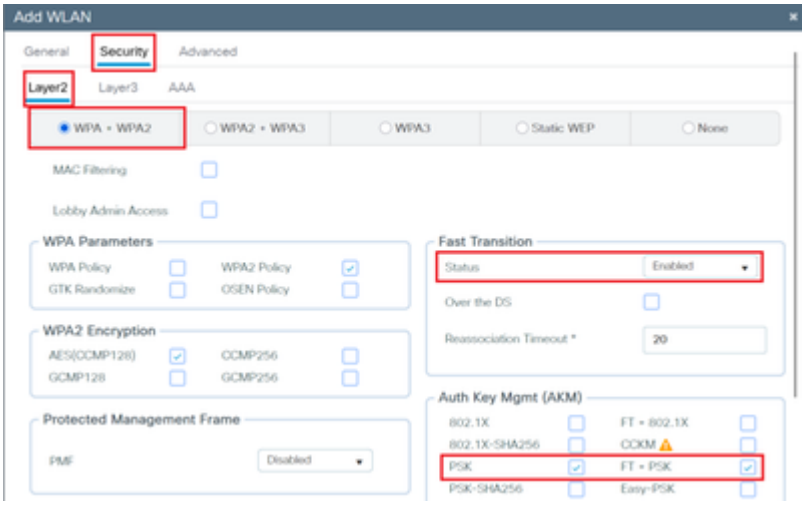
Schritt 2: Erstellen Sie das WLAN.

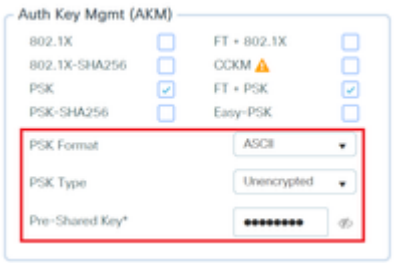
Navigieren Sie zu Configuration > Tags & Profiles > WLANs, und wählen Sie +Add.

Erstellen Sie unter General einen Namen für den Profilnamen, die SSID und den Aktivierungsstatus:



Schritt 3. Navigieren Sie zu Sicherheit > Layer 2 Registerkarte wählen Sie WPA+WPA2, Fast Transition as Enabled, Auth Key Mgmt PSK und FT+PSK, wählen Sie das PSK-Format und PSK-Typ, die Sie möchten, und geben Sie den Pre-Shared Key, den Ihre Clients verwenden sollen:





Klicken Sie auf Aktualisieren und auf Gerät anwenden.

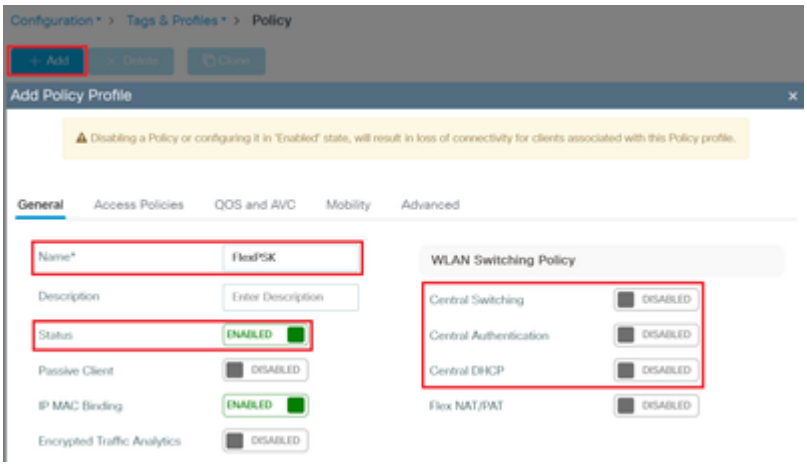
Sie können das erstellte WLAN sehen:



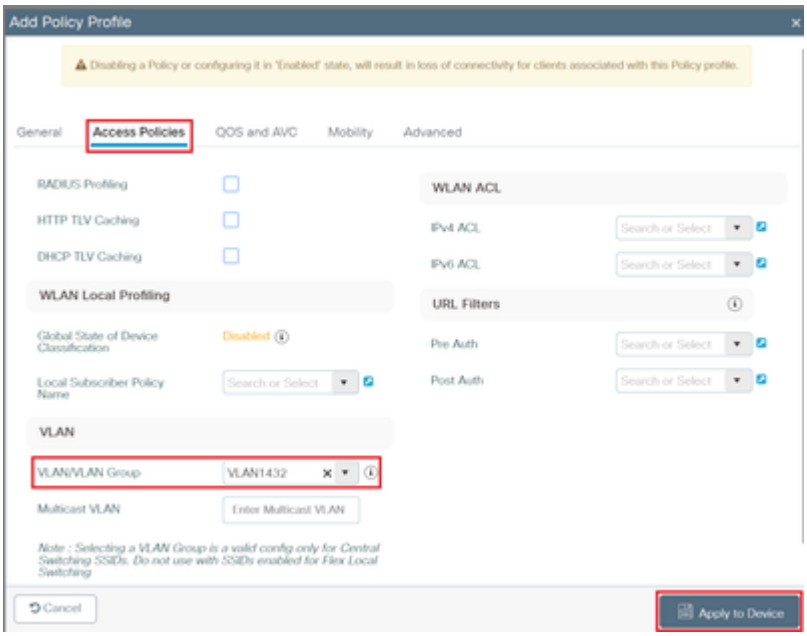
Schritt 4: Erstellen Sie das Richtlinienprofil.

Navigieren Sie zu Konfiguration > Tags und Profile > Richtlinie.

Wählen Sie +Hinzufügen und geben Sie auf der Registerkarte Allgemein einen Namen für das Richtlinienprofil ein, aktivieren Sie den Status, und deaktivieren Sie das zentrale Switching, die zentrale Authentifizierung und das zentrale DHCP:

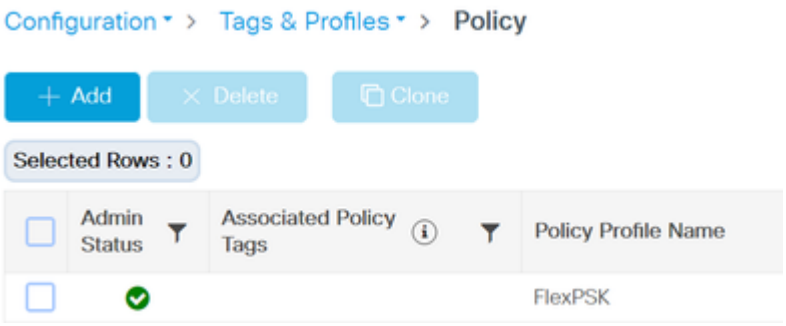


Schritt 5: Navigieren Sie zur Registerkarte Access Policies (Zugriffsrichtlinien), und wählen Sie das VLAN aus:



Klicken Sie auf Aktualisieren und auf Gerät anwenden.

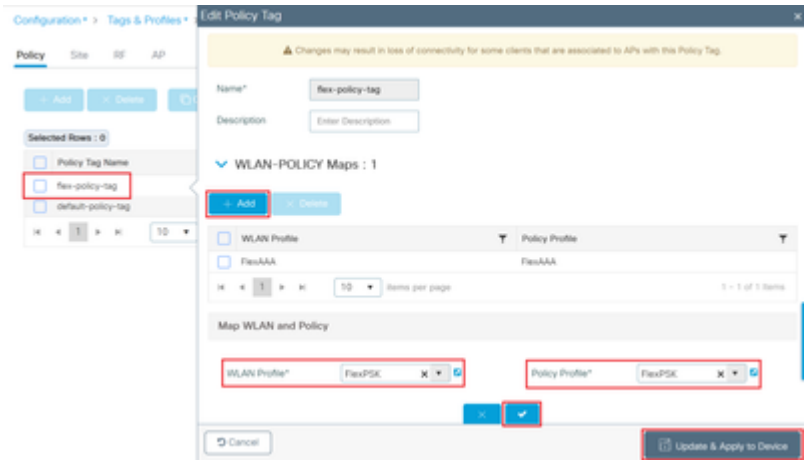
Das Richtlinienprofil wird in der Liste angezeigt:



Schritt 6: Sie können einen neuen Policy-Tag erstellen oder den vorhandenen bearbeiten.

Navigieren Sie zu Configuration > Tags & Profiles > Tags, um das vorhandene Policy-Tag zu bearbeiten. Wählen Sie das zu bearbeitende Tag aus.

Wählen Sie +Hinzufügen unter WLAN-POLICY Maps aus. Wählen Sie im WLAN Profile (WLAN-Profil) das zuvor erstellte WLAN aus dem Dropdown-Menü aus. Wählen Sie im Dropdown-Menü Policy Profile (Richtlinienprofil) das zuvor erstellte Richtlinienprofil aus. Klicken Sie auf die Schaltfläche zum Aktivieren und dann auf Auf Gerät anwenden:



Wenn die Richtlinie bereits auf dem Access Point zugewiesen ist, müssen Sie nichts weiter tun.

Falls nicht, weisen Sie das Policy Tag auf dem APs Tag zu. Navigieren Sie zu Konfiguration > Wireless > Access Points. Wählen Sie den Access Point aus, um das Policy-Tag zu ändern, und klicken Sie auf "Aktualisieren und auf Gerät anwenden".

Der Access Point trennt die Verbindungen und verbindet sich mit dem neuen Richtlinientag wieder.

Wenn der Access Point wieder hinzugefügt wird, können Sie die Liste der Access Points überprüfen und überprüfen, ob sich der Access Point im Flex-Modus befindet und über die richtigen zugewiesenen Tags verfügt.

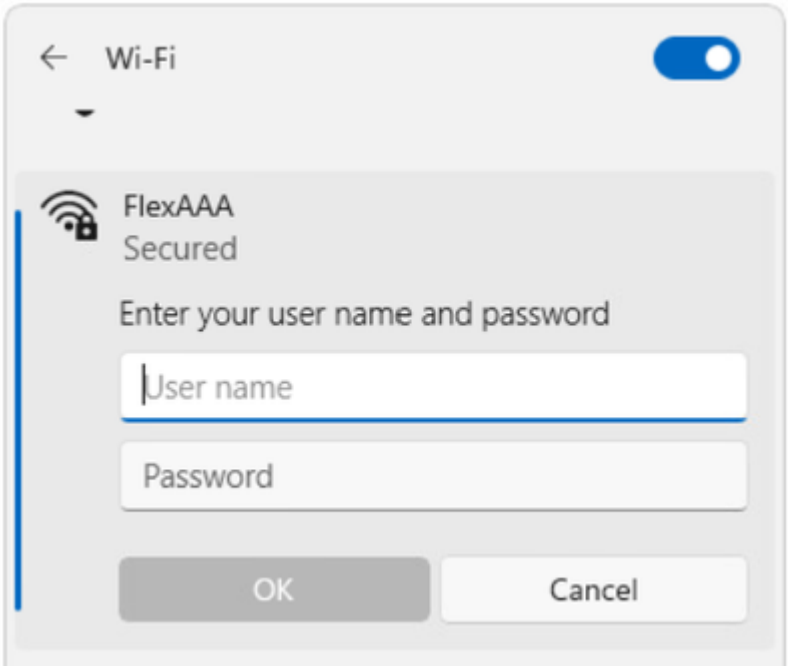
CLI:

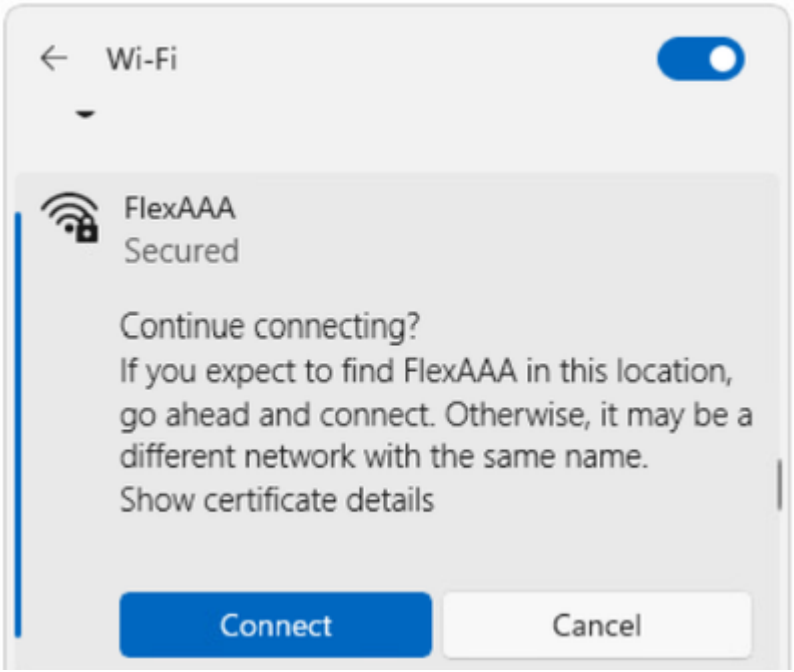
```
wlan FlexPSK 5 FlexPSK
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa psk set-key ascii 0 Password123
no security wpa akm dot1x
security wpa akm ft psk
security wpa akm psk
no shutdown
!
wireless profile policy FlexPSK
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
wlan FlexPSK policy FlexPSK
!
```

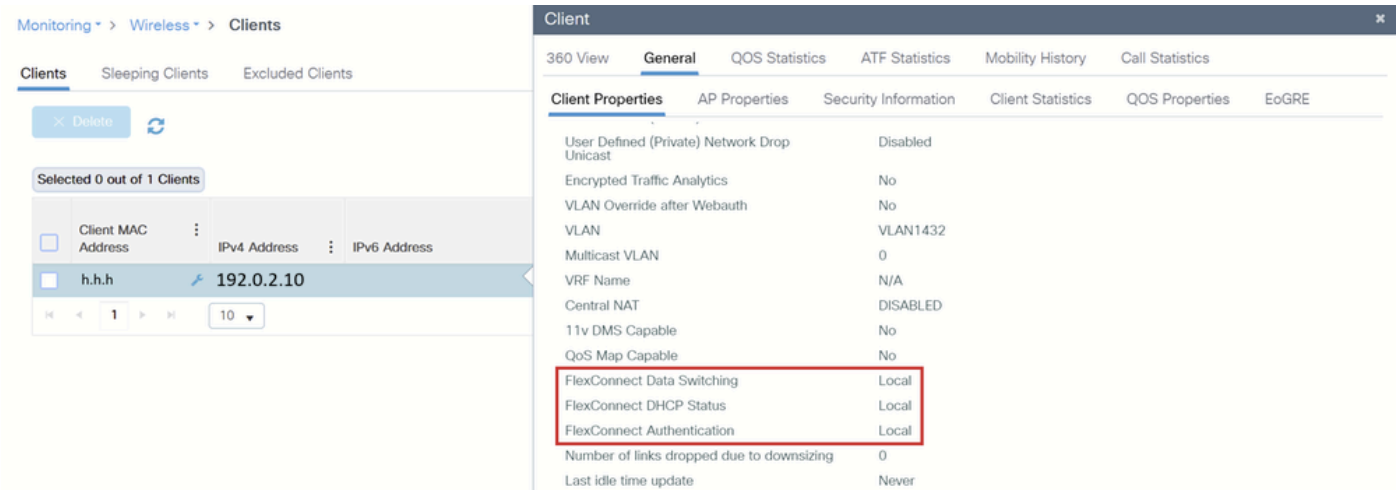
```
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

Überprüfung

Für 802.1x-WLAN:







CLI:

```
C9800-1#show wireless client mac-address h.h.h detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :192.0.2.10
Client IPv6 Addresses :
Client Username : test
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexAAA
Flex Profile : Flex
Wireless LAN Id: 4
WLAN Profile Name: FlexAAA
Wireless LAN Network Name (SSID): FlexAAA
BSSID :
Connected For : 134 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

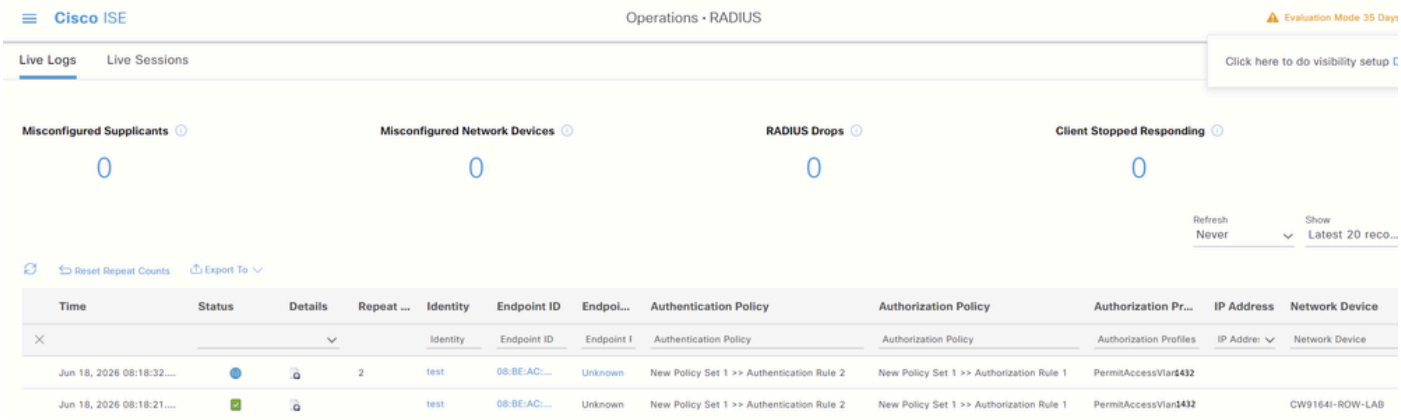
```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

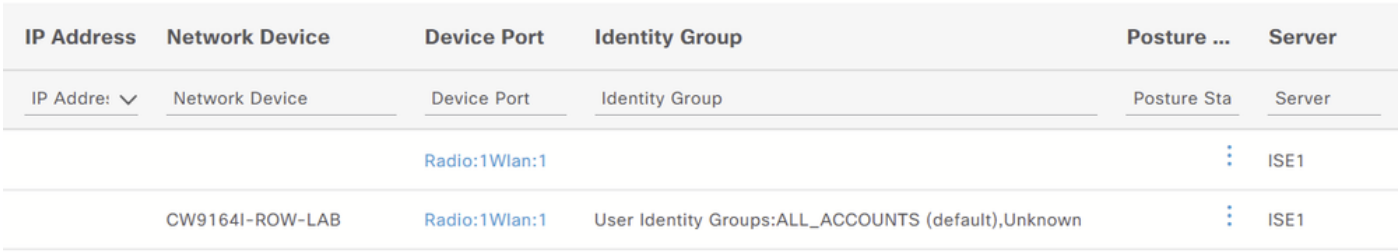
Über die AP-CLI:

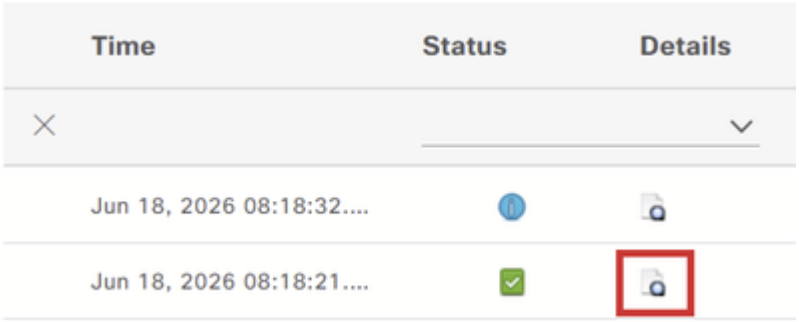
```
CW9164I-ROW-LAB#show dot11 clients

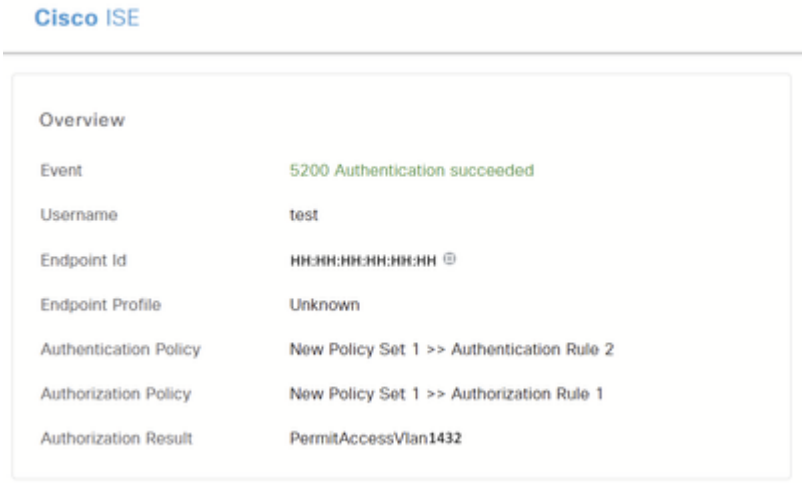
Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH          1       1  33   FlexAAA  -45 MCS9ISS           No          No
```

Auf der ISE


Cisco ISE
Operations · RADIUS
Evaluation Mode 35 Days
Live Logs
Live Sessions
Click here to do visibility setup
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
0
Refresh
Never
Show
Latest 20 reco...
Reset Repeat Counts
Export To
Time
Status
Details
Repeat ...
Identity
Endpoint ID
Endpoi...
Authentication Policy
Authorization Policy
Authorization Pr...
IP Address
Network Device
Jun 18, 2026 08:18:32....
2
test
08:BE:AC:...
Unknown
New Policy Set 1 >> Authentication Rule 2
New Policy Set 1 >> Authorization Rule 1
PermitAccessVlan1432
Jun 18, 2026 08:18:21....
test
08:BE:AC:...
Unknown
New Policy Set 1 >> Authentication Rule 2
New Policy Set 1 >> Authorization Rule 1
PermitAccessVlan1432
CW9164I-ROW-LAB

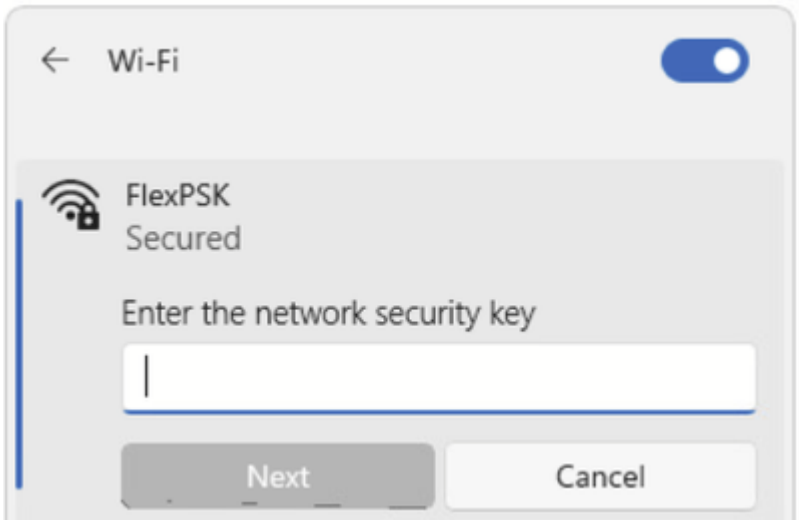

IP Address
Network Device
Device Port
Identity Group
Posture ...
Server
IP Addre:
Network Device
Device Port
Identity Group
Posture Sta
Server
Radio:1Wlan:1
ISE1
CW9164I-ROW-LAB
Radio:1Wlan:1
User Identity Groups:ALL_ACCOUNTS (default),Unknown
ISE1

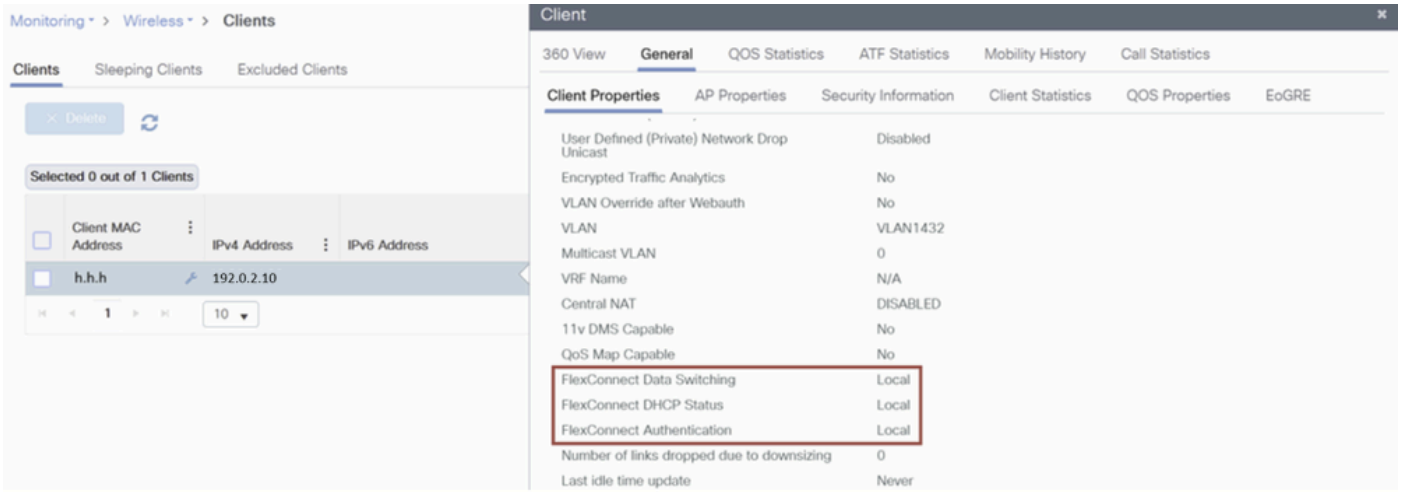

Time
Status
Details
Jun 18, 2026 08:18:32....
Jun 18, 2026 08:18:21....


Cisco ISE
Overview
Event
5200 Authentication succeeded
Username
test
Endpoint Id
HH:HH:HH:HH:HH:HH
Endpoint Profile
Unknown
Authentication Policy
New Policy Set 1 >> Authentication Rule 2
Authorization Policy
New Policy Set 1 >> Authorization Rule 1
Authorization Result
PermitAccessVlan1432

Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:ALL_ACCOUNTS (default),Unknown
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	CW9164I-ROW-LAB
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.0.2.40
NAS Port Id	Radio:1Wlan:1
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccessVlan1432
Response Time	64 milliseconds

Für das PSK-WLAN:





CLI:

```
C9800-1#show wireless client mac-address      h.h.h      detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 192.0.2.10
Client IPv6 Addresses :
Client Username: N/A
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexPSK
Flex Profile : Flex
Wireless LAN Id: 5
WLAN Profile Name: FlexPSK
Wireless LAN Network Name (SSID): FlexPSK
BSSID :
Connected For : 116 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

Auf AP-CLI:

```
CW9164I-ROW-LAB#show dot11 clients

Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
  xxxxxxxxxxxx          1       2  33   FlexPSK  -45 MCS9iSS          No         No
```

Fehlerbehebung

AP-Debugging und RA-Ablaufverfolgung mit synchronisierter MAC-Adresse des Clients aktivieren.

Aktivieren Sie auf dem Access Point die folgenden Debugging-Optionen:

debug-Flexconnect-Ereignis
debug flexconnect pmk
debug flexconnect dot11r
debug dot11 Client-Verwaltungsinformationen
debug dot11 client management kritisch
debug dot11 client management errors
debug dot11-Clientverwaltungsereignisse

Für 802.1x-WLAN:

AP-Debug-Protokolle mit erfolgreicher Authentifizierung:

Der Access Point übernimmt das 802.11-Statussystem und die lokale Schlüsselverwaltung.
Der WAP verarbeitet die Zuordnung und bereitet den Client auf die Authentifizierung vor.

```
[*06/19/2026 06:49:00.1836] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*06/19/2026 06:49:00.1890] wcp/flex_roam_st :: Flexconnect 11r enabled for client HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1908] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*06/19/2026 06:49:00.1909] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1931] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
```

Der WAP verarbeitet die Autorisierung, wendet die VLAN-Überschreibung an und verschiebt den Client in den FWD-Status (Forwarding).

```
[*06/19/2026 06:49:20.3601] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*06/19/2026 06:49:20.3601] CLSM[HH:HH:HH:HH:HH:HH]: WCP_EVENT_CLIENT_AUTHORIZE : Plumbing key info to
[*06/19/2026 06:49:20.3612] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*06/19/2026 06:49:20.3625] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*06/19/2026 06:49:20.3627] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Retrieved key for FT+FT_DOT1X algono: 8, vlanId: 1
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Local auth (Add) on radio 1 Vap 0 reported to WLC
[*06/19/2026 06:49:20.3701] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*06/19/2026 06:49:20.4313] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr1v0
[*06/19/2026 06:49:20.4317] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 1 Vap 0 IP 192.0.2.10 updatere
[*06/19/2026 06:49:20.4318] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

RA-Ablaufverfolgungsprotokolle für dieselbe erfolgreiche Authentifizierung:

Der RA Trace protokolliert die Orchestrierung der Sitzung durch den WLC. Der WLC validiert die Client-Identität und die Richtlinie.
WLC erkennt die FlexConnect-Zuordnung an.

```
2026/06/19 06:49:20.934325580 {wncd_x_R0-1}{1}: [client-orch-sm] [18318]: (note): MAC: hhhh.hhhh.hhhh H
2026/06/19 06:49:20.936543415 {wncd_x_R0-1}{1}: [dot1x] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040000
2026/06/19 06:49:20.936579730 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936600851 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936654791 {wncd_x_R0-1}{1}: [ewlc-infra-evq] [18318]: (note): Authentication Succes
2026/06/19 06:49:20.936769433 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

WLC überträgt die Richtlinie an den AP.

```
2026/06/19 06:49:20.937447786 {wncd_x_R0-1}{1}: [svm] [18318]: (info): [hhhh.hhhh.hhhh] Applied User Pr
2026/06/19 06:49:20.937451734 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: c
```

```
2026/06/19 06:49:20.937452534 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937455590 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: v
2026/06/19 06:49:20.937456177 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: m
2026/06/19 06:49:20.937458436 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: u
2026/06/19 06:49:20.937462127 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile:tu
2026/06/19 06:49:20.937462755 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937463426 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937464035 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
```

Autorisierung erfolgreich.

```
2026/06/19 06:49:20.937594042 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.937597878 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

Client-Parameter.
2026/06/19 06:49:20.939394217 {wncd_x_R0-1}{1}: [dot11] [18318]: (Hinweis): MAC: hhhh.hhh.hhh Client-Datenpfad-Eingabeparameter - ssid:FlexAAA,slot_id:1 bssid ifid: 0x0, radio_ifid: 0x90400008, wlan_ifid: 0xf0400004

WLC empfängt die IP über lokalen DHCP/ARP.
2026/06/19 06:49:21.001000218 {wncd_x_R0-1}{1}: [client-iplearn] [18318]: (Hinweis): MAC: hhhh.hhhh.hhh Client IP erfolgreich lernen. Methode: IP-Snooping: 192.0.2.10

Der Client ist vollständig verbunden.
2026/06/19 06:49:21.002363496 {wncd_x_R0-1}{1}: [errmsg] [18318]: (Info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/1: wncd: Eingabe des Benutzernamens (Test) verbunden mit SSID (FlexAAA) für Gerät mit MAC: hhhh.hhhh.hhh auf Kanal (48)
2026/06/19 06:49:21.002795009 {wncd_x_R0-1}{1}: [Client-Orch-State] [18318]: (Hinweis): MAC: hhhh.hhh.hhh Clientzustandsübergang: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

Standalone-Szenario

Verhalten bei Verbindungsverlust des AP-WLC und anschließender Wiederherstellung

Der AP wird mit dem WLC verbunden. Der Client führt eine erfolgreiche 802.1X-Authentifizierung durch, und der Access Point setzt den Client auf den FWD-Status (Forwarding) um.

Auf ISE RADIUS Live Logs wird die Client-Sitzung angezeigt.

```
[*07/06/2026 20:26:05.8590] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 0 Vap 0 IP 192.0.2.10 updatere
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD


CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```

Der AP erreicht den WLC nicht, erreicht seine Anzahl an erneuten Übertragungen nicht mehr und schaltet in den Standalone-Modus um. Vorhandene Clients bleiben lokal verbunden.

```
[*07/06/2026 20:28:47.0840] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=33, NumofPendingMsgs=4
[*07/06/2026 20:28:50.0860] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=34, NumofPendingMsgs=5
[*07/06/2026 20:28:53.0870] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:56.0990] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:59.1000] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:29:02.1010] Max retransmission count exceeded, going back to DISCOVER mode.
[*07/06/2026 20:29:02.1020] Flexconnect Switching to Standalone Mode!
[*07/06/2026 20:29:02.2170] CAPWAP State: DTLS Teardown
```

Der Client ist jedoch immer noch verbunden:

CW9164I-ROW-LAB2#show dot11 clients

Gesamtzahl der dot11-Clients: 1
Client-MAC-Steckplatz-ID WLAN-ID-AID WLAN-Name RSSI-Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 Nein Nein

Wenn der Client im Standalone-Modus zu einem anderen Access Point wechselt, schlägt der EAP-Handshake fehl, da der RADIUS-Server nicht erreichbar ist. Der Client wird deautorisiert und vom Access Point entfernt.

```
[*07/06/2026 20:34:44.7240] CLSM[HH:HH:HH:HH:HH:HH]: Session timeout
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-RETRANSMIT hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-TIMEOUT-FAILURE hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: Received UNAUTHORIZE for hh:hh:hh:h
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: recv'd UNAUTH with DISCONNECT REQUE
[*07/06/2026 20:36:15.2680] CLSM[HH:HH:HH:HH:HH:HH]: Client delete initiated with timeout of 10 seconds
[*07/06/2026 20:36:15.2770] CLSM[HH:HH:HH:HH:HH:HH]: Remove success from ClientIPTable on apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Not sending DELETE to cont, reason CLIENT_DEL_EAP_
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Deauthorize succeeded to radio intf apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: client moved from FWD to DELETE_PENDING
[*07/06/2026 20:36:15.2880] CLSM[HH:HH:HH:HH:HH:HH]: Send Deauth with reason 2 force 1 - Radio 0 Vap 0
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete timeout
```

```
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete client reassoc 0 succeeded to radio intf ap
```

AP sendet die Client-Sitzung an den RADIUS-Backup-Server.

Der AP stellt wieder Verbindung zum WLC her. Der Access Point wechselt zurück in den verbundenen Modus und synchronisiert die lokalen Client-Sitzungsinformationen mit dem WLC.

Die Client-Sitzung wechselt je nach Verbindungsstatus des Access Points zwischen dem primären und dem Backup-ISE-Knoten.

Der WAP und der Client werden auf dem WLC als verbunden angezeigt, und der Client hat keine Unterbrechungen oder Flapping-Ereignisse bemerkt, als die Verbindung zwischen dem WLC und dem WAP unterbrochen war.

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 0


Upon roaming back, the client undergoes local authentication. The AP processes the association and move

[*07/06/2026 20:48:49.2830] CLSM[HH:HH:HH:HH:HH:HH]: US Auth(b0) seq 2653 IF 23 slot 0 vap 0 len 30 sta
[*07/06/2026 20:48:49.2840] CLSM[HH:HH:HH:HH:HH:HH]: DS Auth len 30 slot 0 vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*07/06/2026 20:48:49.2920] CLSM[HH:HH:HH:HH:HH:HH]: US Reassoc Req(20) seq 2654 IF 23 slot 0 vap 0 len
[*07/06/2026 20:48:49.2930] CLSM[HH:HH:HH:HH:HH:HH]: AUTH TYPE RSNIE DOT1X
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: Populate client capability: cap_from_click=true, m
[*07/06/2026 20:48:49.2940] Flexconnect local_auth 1 local_assoc 1 frame subtype 32
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio id: 0, vap id: 0, max clients for this wlan:
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio state: 1, client state: 1, max_client_per_ra
[*07/06/2026 20:48:49.2940] Adding RM Capable IE - Len = 5, RRM[0] = 73, RRM[1] = c0
[*07/06/2026 20:48:49.2940] DS [re]Assoc 1 req_len=201 resp_len=146 11r_len=0 cckm 0 qos_flag 1 status
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: DS Reassoc Resp(30) IF 0 slot 0 vap 0 state AUTH,
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*07/06/2026 20:48:49.2950] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-n
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Driver Add Client success AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Added to ClientIPTable on apr0v0
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2980] wcp/flex_roam_st :: Flexconnect hapdev: client WCP_EVENT_CLIENT_ASSOC/REASS
[*07/06/2026 20:48:49.6360] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*07/06/2026 20:48:49.6360] wcp/flex_roam_st :: Flexconnect (AUTHORIZE) received PTK thru wcp_event
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect HH:HH:HH:HH:HH:HH client ACL , Qos Profile:
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-n
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client
```

```
[*07/06/2026 20:48:49.6370] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: check vlan override vlan 1432
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*07/06/2026 20:48:49.6390] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*07/06/2026 20:48:49.6900] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:48:49.6910] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD


CW9164I-ROW-LAB2#show dot11 clients

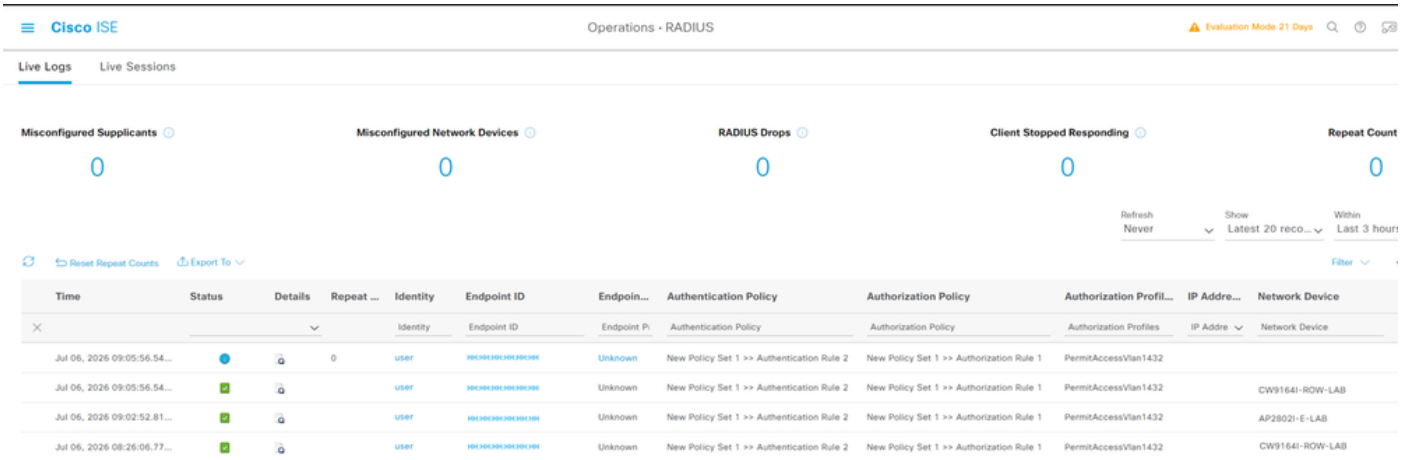
Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -39 M7 No No



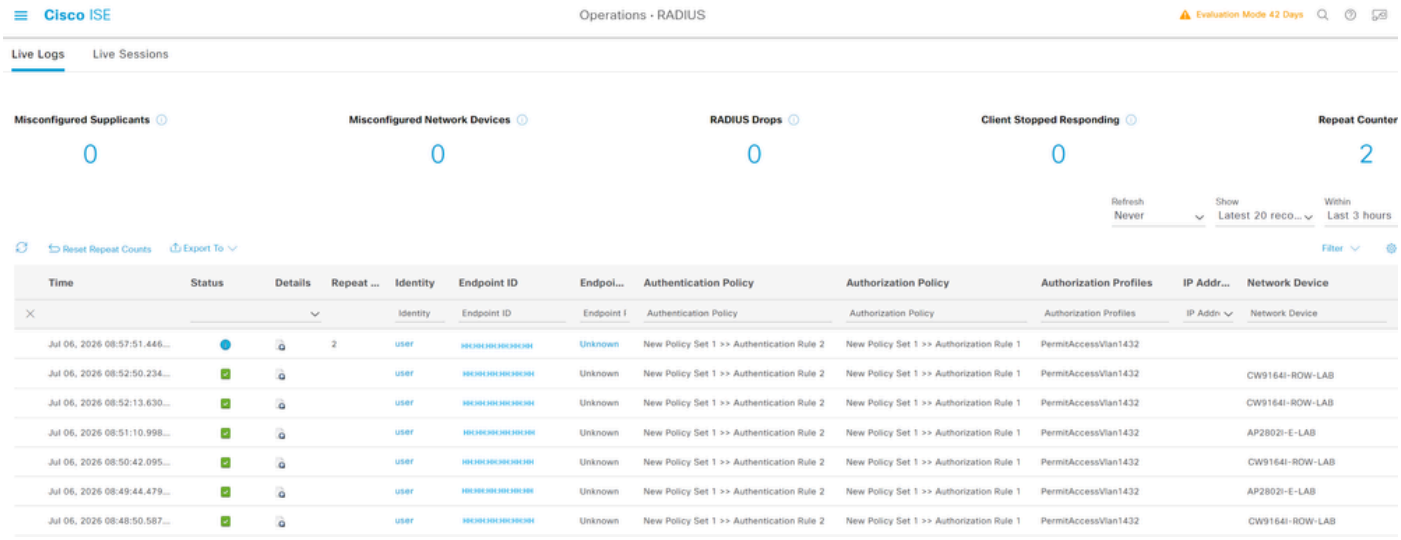

*07/06/2026 20:59:57.7690] Discovery Response from 192.0.2.20
[*07/06/2026 21:00:08.0080] CAPWAP State: DTLS Setup
[*07/06/2026 21:00:08.4820] CAPWAP State: Join
[*07/06/2026 21:00:09.3740] Sending Join request to 192.0.2.20 through port 5253, packet size 1376
[*07/06/2026 21:00:09.3780] Join Response from 192.0.2.20, packet size 1397
[*07/06/2026 21:00:09.4040] CAPWAP State: Image Data
[*07/06/2026 21:00:09.5020] CAPWAP State: Configure
[*07/06/2026 21:00:12.5510] CAPWAP State: Run
[*07/06/2026 21:00:12.6480] AP has joined controller C9800-1
[*07/06/2026 21:00:12.6490] Flexconnect Switching to Connected Mode!
[*07/06/2026 21:00:12.6520] CLSM[HH:HH:HH:HH:HH:HH]: AP_REAP_CLIENT_INFO_PAYLOAD Client MAC HH:HH:HH:HH
[*07/06/2026 21:00:12.6520] AssocTimeAtAP 1783371169 clientBitmap=0x13
[*07/06/2026 21:00:12.6520] CLSM[00:00:00:00:00:00]: Numbers of Local Switching clients to report : 1
[*07/06/2026 21:00:14.8270] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8270] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
[*07/06/2026 21:00:14.8280] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8280] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716


CW9164I-ROW-LAB2# show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```



Primäre ISE: Zeichnet die erste Sitzung (08:26:06) und die wieder aufgenommene Sitzung nach der Wiederherstellung der WLC-Verbindung (09:02:52) auf.



Backup-ISE: Erfasst die Sitzungsaktivität (08:48:50 - 08:57:51), während der Access Point im Standalone-Modus betrieben wurde.

In der ersten Sitzung wurde um 08:26:06 Uhr die Verbindung zum WLC getrennt, und der Access Point wechselte in den Standalone-Modus.

Die Sitzung 09:02:52 ist die erste Sitzung, nachdem der Access Point die Verbindung mit dem WLC wiederhergestellt hat.

Zugehörige Informationen

- CCNP Enterprise Wireless Design ENWLSD 300-425 und Implementierung ENWLSI 300-430 Offizieller Zertifizierungsleitfaden, 2. Ausgabe
- Software-Konfigurationsanleitung für Cisco Catalyst Wireless Controller der Serie 9800, Cisco IOS XE 17.8.x - Kapitel: FlexConnect
- Versionshinweise für Cisco Catalyst Wireless Controller der Serie 9800, Cisco IOS XE Cupertino Version 17.8.x
- Funktionsübersicht für Cisco Wireless Access Points
- Technischer Support und Downloads von Cisco

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.