Bereitstellungsleitfaden für Flex 7500 Wireless Branch Controller

Inhalt

Einführung

Dieses Dokument beschreibt die Bereitstellung eines Cisco Flex 7500 Wireless Branch Controller. Ziel dieses Dokuments ist es,

- Erläutern Sie die verschiedenen Netzwerkelemente der Cisco FlexConnect-Lösung sowie deren Kommunikationsfluss.
- Stellen Sie allgemeine Richtlinien für die Bereitstellung der Cisco FlexConnect Wireless-Zweigstellenlösung bereit.
- Erläutern Sie die Softwarefunktionen in der Codeversion 7.2.103.0, die die Informationsdatenbank zum Produkt unterstützen.

Hinweis: Vor 7.2 hieß FlexConnect Hybrid REAP (HREAP). Jetzt heißt es FlexConnect.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Produktübersicht

Abbildung 1: Cisco Flex 7500

Der Cisco Flex Cloud Controller der Serie 7500 ist ein hochskalierbarer Zweigstellen-Controller für Wireless-Bereitstellungen mit mehreren Standorten. Der Cisco Flex Controller der Serie 7500 wird in der Private Cloud bereitgestellt und ermöglicht die Bereitstellung von Wireless-Services in

verteilten Zweigstellen mit zentralisierter Kontrolle zur Senkung der Gesamtbetriebskosten.

Die Cisco Flex 7500-Serie (Abbildung 1) kann Wireless-Access Points in bis zu 500 Zweigstellen verwalten und ermöglicht IT-Managern die Konfiguration, Verwaltung und Fehlerbehebung für bis zu 3.000 Access Points (APs) und 30.000 Clients vom Rechenzentrum aus. Der Cisco Flex-Controller der Serie 7500 unterstützt sicheren Gastzugriff, Erkennung von nicht autorisierten Access Points zur Einhaltung von PCI-Standards (Payment Card Industry) und Wi-Fi-Sprach- und Videofunktionen in Zweigstellen (lokal geschaltet).

In dieser Tabelle werden die Unterschiede bei der Skalierbarkeit zwischen dem Flex 7500-, WiSM2- und dem WLC 5500-Controller hervorgehoben:

Skalierbarkeit	Flex 7500	WiSM2	WLC 5500
Access Points gesamt	6,000	1000	500
Gesamtanzahl an Clients	64,000	15,000	7,000
Max. FlexConnect-Gruppen	2000	100	100
Max. APs pro FlexConnect-Gruppe	100	25	25
Max. AP-Gruppen	6000	1000	500

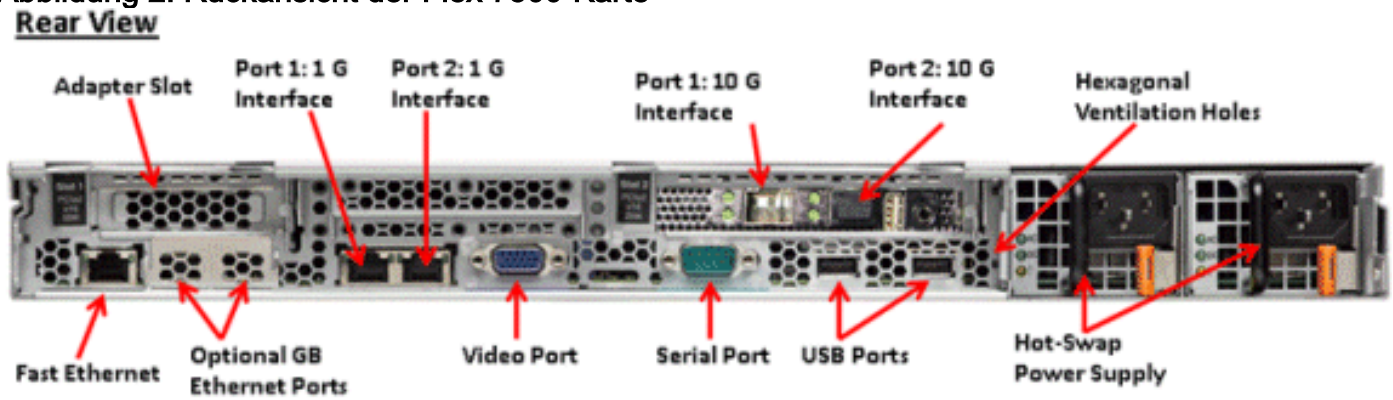
Produktspezifikationen

Datenblatt

Weitere Informationen finden Sie unter http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps11635/data_sheet_c78-650053.html.

Plattformfunktionen

Abbildung 2: Rückansicht der Flex 7500-Karte



Netzwerkschnittstellen-Ports

Schnittstellen-Ports	Verwendung
Fast Ethernet	Integrated Management Module (IMM)

Port 1: 1 G	WLC-Service-Port
Port 2: 1 G	Redundanter WLC-Port (RP)
Port 1: 10 G	WLC-Verwaltungsschnittstelle
Port 2: 10 G	WLC Backup Management Interface Port (Port-Ausfall)
Optionale GbE-Ports	–

Hinweis:

- Die LAG-Unterstützung für 2 x 10-G-Schnittstellen ermöglicht den Betrieb von Aktiv-Aktiv-Verbindungen mit einer schnellen Failover-Link-Redundanz. Eine zusätzliche aktive 10G-Verbindung mit der LAG ändert den Wireless-Durchsatz des Controllers nicht.
- 2 x 10-G-Schnittstellen
- 2x10G-Schnittstellen unterstützen nur optische Kabel mit der SFP-Produktnummer SFP-10G-SR.
- SFP-Produkt auf Switch-Seite # X2-10GB-SR

MAC-Systemadressen

Port 1: 10 G (Management-Schnittstelle)	MAC-Adresse System/Base
Port 2: 10 G (Backup Management Interface)	MAC-Basisadresse + 5
Port 1: 1G (Service-Port)	MAC-Basisadresse + 1
Port 2: 1 G (redundanter Port)	MAC-Basisadresse + 3

Serielle Konsolenumleitung

Der WLC 7500 aktiviert standardmäßig die Konsolenumleitung mit einer Baudrate von 9600, wodurch Vt100 Terminal ohne Flusssteuerung simuliert wird.

Bestandsdaten

Abbildung 3: WLC 7500-Konsole

```
(Cisco Controller) >show inventory

Burned-in MAC Address.............................. E4:1F:13:65:DB:6C
Maximum number of APs supported.................... 2000
NAME: "Chassis"    , DESCR: "Cisco Wireless Controller"
PID: AIR-CT7510-K9,  VID: V01,  SN: KQZZXWL
```

Die Tabelle der Desktop Management Interface (DMI) enthält Serverhardware- und BIOS-Informationen.

Der WLC 7500 zeigt BIOS-Version, PID/VID und Seriennummer als Teil des Inventars an.

Hochfahren des Flex 7500

Die Cisco Boot Loader-Optionen für die Softwarewartung sind mit den vorhandenen Controller-Plattformen von Cisco identisch.

Abbildung 4: Bestellung hochfahren

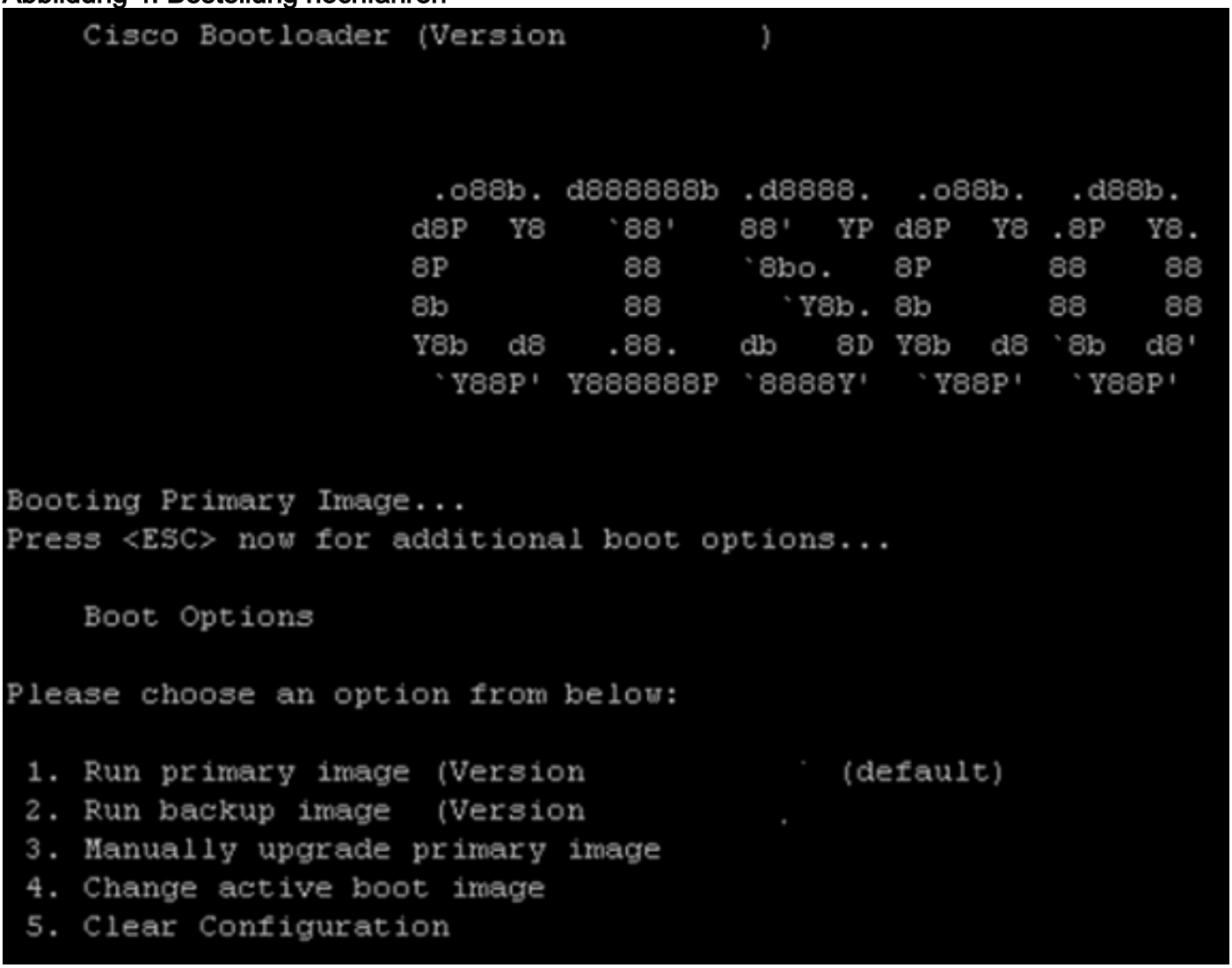


Abbildung 5: WLC-Konfigurationsassistent

```
Would you like to terminate autoinstall? [yes]:

System Name [Cisco_65:db:6c] (31 characters max):
AUTO-INSTALL: process terminated -- no configuration loaded

Enter Administrative User Name (24 characters max): admin
Default values (admin or Cisco or its variants) in password is not allowed.
Enter Administrative Password (24 characters max): *******
Re-enter Administrative Password                  : *******

Management Interface IP Address: 172.20.227.174
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 172.20.227.161
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: 172.20.227.161

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: mobility

Network Name (SSID): DataCenter

Configure DHCP Bridging Mode [yes][NO]: NO

Allow Static IP Addresses [YES][no]: Yes

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: 09/02/10
Enter the time in HH:MM:SS format: 11:50:00

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

Management Port 1: 10G

Hinweis: Die Flex 7500-Startsequenz ist äquivalent und konsistent mit vorhandenen Controller-Plattformen. Für das erstmalige Booten ist eine WLC-Konfiguration mit dem Assistenten erforderlich.

Flex 7500-Lizenzierung

AP Base Count Licensing

SKUs für die AP-Basisanzahl

300
500
1000
2000
3000
6000

AP-Upgrade-Lizenzierung

AP-Upgrade-SKUs
100
250
500
1000

Mit Ausnahme der Basis- und Upgrade-Anzahl ähnelt das gesamte Lizenzierungsverfahren für Bestellung, Installation und Anzeige dem vorhandenen WLC 5508 von Cisco.

Weitere Informationen finden Sie im WLC 7.3-Konfigurationsleitfaden, der das gesamte Lizenzierungsverfahren behandelt.

Unterstützung für Softwareversionen

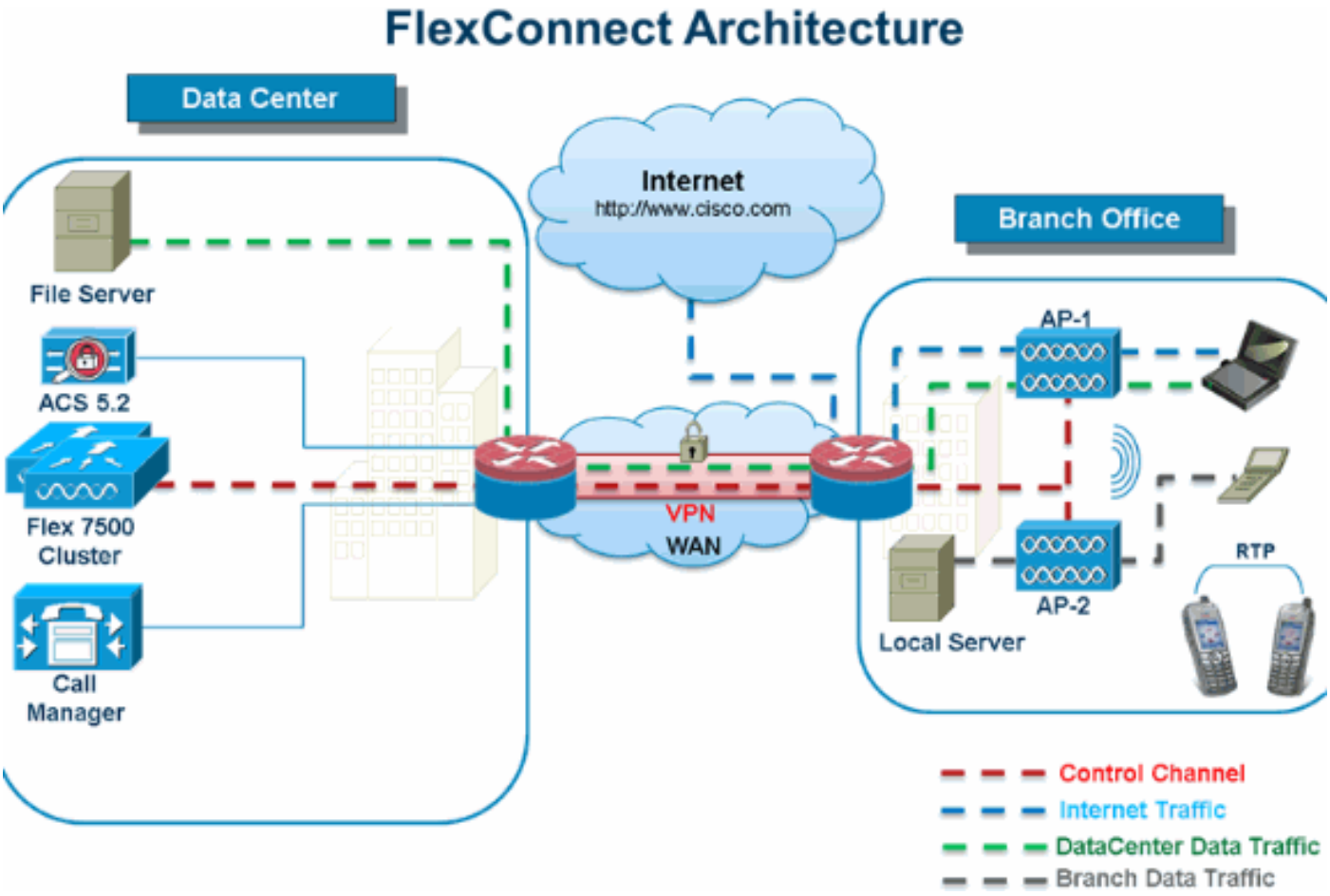
Der Flex 7500 unterstützt nur den WLC-Code der Version 7.0.116.x und höher.

Unterstützte Access Points

Access Points 1040, 1130, 1140, 1550, 3500, 3600, 2600, 1250, 1260, 1240, OEAP 600, ISR 891 und ISR R 881 wird von Flex 7500 unterstützt.

FlexConnect-Architektur

Abbildung 6: Typische Wireless-Zweigstellentopologie



FlexConnect ist eine Wireless-Lösung für Bereitstellungen in Zweigstellen und Zweigstellen. Sie wird auch als Hybrid-REAP-Lösung bezeichnet, wird jedoch in diesem Dokument als FlexConnect bezeichnet.

Die FlexConnect-Lösung bietet Kunden folgende Vorteile:

- Zentralisieren Sie die Steuerung und das Management des Datenverkehrs der Access Points vom Rechenzentrum aus.Kontrolldatenverkehr wird in Abbildung 6 durch rote Bindestriche gekennzeichnet.
- Verteilung des Client-Datenverkehrs in jeder ZweigstelleDatenverkehr wird in Abbildung 6 durch blaue, grüne und violette Bindestriche gekennzeichnet.Jeder Datenverkehrsfluss geht so effizient wie möglich an sein endgültiges Ziel.

Vorteile der Zentralisierung des Kontrollverkehrs über Access Points

- Zentrale Oberfläche für Überwachung und Fehlerbehebung
- Einfache Verwaltung
- Sicherer und nahtloser mobiler Zugriff auf Rechenzentrumsressourcen
- Weniger Platzbedarf in Zweigstellen
- Einsparungen bei Betriebskosten

Vorteile der Verteilung von Client-Datenverkehr

- Keine Betriebsausfallzeiten (Ausfallsicherheit) bei vollständigen WAN-Verbindungsausfällen oder Nichtverfügbarkeit des Controllers

- Ausfallsicherheit der Mobilität in Zweigstellen bei Ausfällen von WAN-Verbindungen
- Verbesserte Skalierbarkeit in Zweigstellen Unterstützt Zweigstellengrößen, die auf bis zu 100 APs und 5.000 m² skaliert werden können. Fuß pro AP).

Die Cisco FlexConnect-Lösung unterstützt auch den zentralen Client-Datenverkehr, sollte jedoch auf den Gastdatenverkehr beschränkt sein. In der folgenden Tabelle werden die Einschränkungen für WLAN-L2-Sicherheitstypen nur für Nicht-Gast-Clients beschrieben, deren Datenverkehr ebenfalls zentral im Rechenzentrum geschaltet wird.

L2-Sicherheitsunterstützung für zentral geswitchte Nicht-Gastbenutzer

WLAN L2-Sicherheit	Typ	Ergebnis
None	–	Zulässig
WPA + WPA2	802.1x	Zulässig
	CCKM	Zulässig
	802.1x + CCKM	Zulässig
	PSK	Zulässig
802.1x	WEP	Zulässig
Statisches WEP	WEP	Zulässig
WEP + 802.1x	WEP	Zulässig
CKIP		Zulässig

Hinweis: Diese Authentifizierungsbeschränkungen gelten nicht für Clients, deren Datenverkehr in der Zweigstelle verteilt ist.

L3-Sicherheitsunterstützung für zentrale und lokal verteilte Benutzer

WLAN L3-Sicherheit	Typ	Ergebnis
Webauthentifizierung	Intern	Zulässig
	Extern	Zulässig
	Benutzerdefiniert	Zulässig
Web-Passthrough	Intern	Zulässig
	Extern	Zulässig
	Benutzerdefiniert	Zulässig
Bedingte Webumleitung	Extern	Zulässig
Splash Page-Webumleitung	Extern	Zulässig

Weitere Informationen zur Bereitstellung externer Webauthentifizierungen für FlexConnect finden Sie im Flexconnect External WebAuth Deployment Guide.

Weitere Informationen zu HREAP/FlexConnect AP-Zuständen und Optionen für das Switching von Datenverkehr finden Sie unter Konfigurieren von FlexConnect.

FlexConnect-Betriebsmodi

FlexConnect-Modus	Beschreibung

Verbunden	Ein FlexConnect befindet sich im Connected Mode, wenn die CAPWAP-Kontrollebene wieder zum Controller hochgefahren und betriebsbereit ist, was bedeutet, dass die WAN-Verbindung nicht ausfällt.
Standalone	Der Standalone-Modus wird als Betriebsstatus festgelegt, in den FlexConnect eingeht, wenn die Verbindung zum Controller nicht mehr besteht. FlexConnect-APs im Standalone-Modus funktionieren auch bei Stromausfall und WLC- oder WAN-Ausfall mit der zuletzt bekannten Konfiguration weiter.

Weitere Informationen zur FlexConnect-Betriebstheorie finden Sie im H-Reap/FlexConnect Design and Deployment Guide.

WAN-Anforderungen

FlexConnect-APs werden in der Außenstelle bereitgestellt und über eine WAN-Verbindung vom Rechenzentrum aus verwaltet. Es wird dringend empfohlen, die minimale Bandbreitenbeschränkung bei einer Round-Trip-Latenz von höchstens 300 ms für Datenbereitstellungen und 100 ms für Daten- und Sprachbereitstellungen auf 12,8 Kbit/s pro AP zu belassen. Die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) muss mindestens 500 Byte betragen.

Bereitstellungsart	WAN-Bandbreite (mindestens)	WAN-RTT-Latenz (max.)	Max. APs pro Zweigstelle	Max. Anzahl Clients pro Zweigstelle
Daten	64 Kbit/s	300 ms	5	25
Daten + Sprache	128 Kbit/s	100 ms	5	25
Überwachung	64 Kbit/s	2 Sek.	5	–
Daten	640 Kbit/s	300 ms	50	1000
Daten + Sprache	1,44 Mbit/s	100 ms	50	1000
Überwachung	640 Kbit/s	2 Sek.	50	–

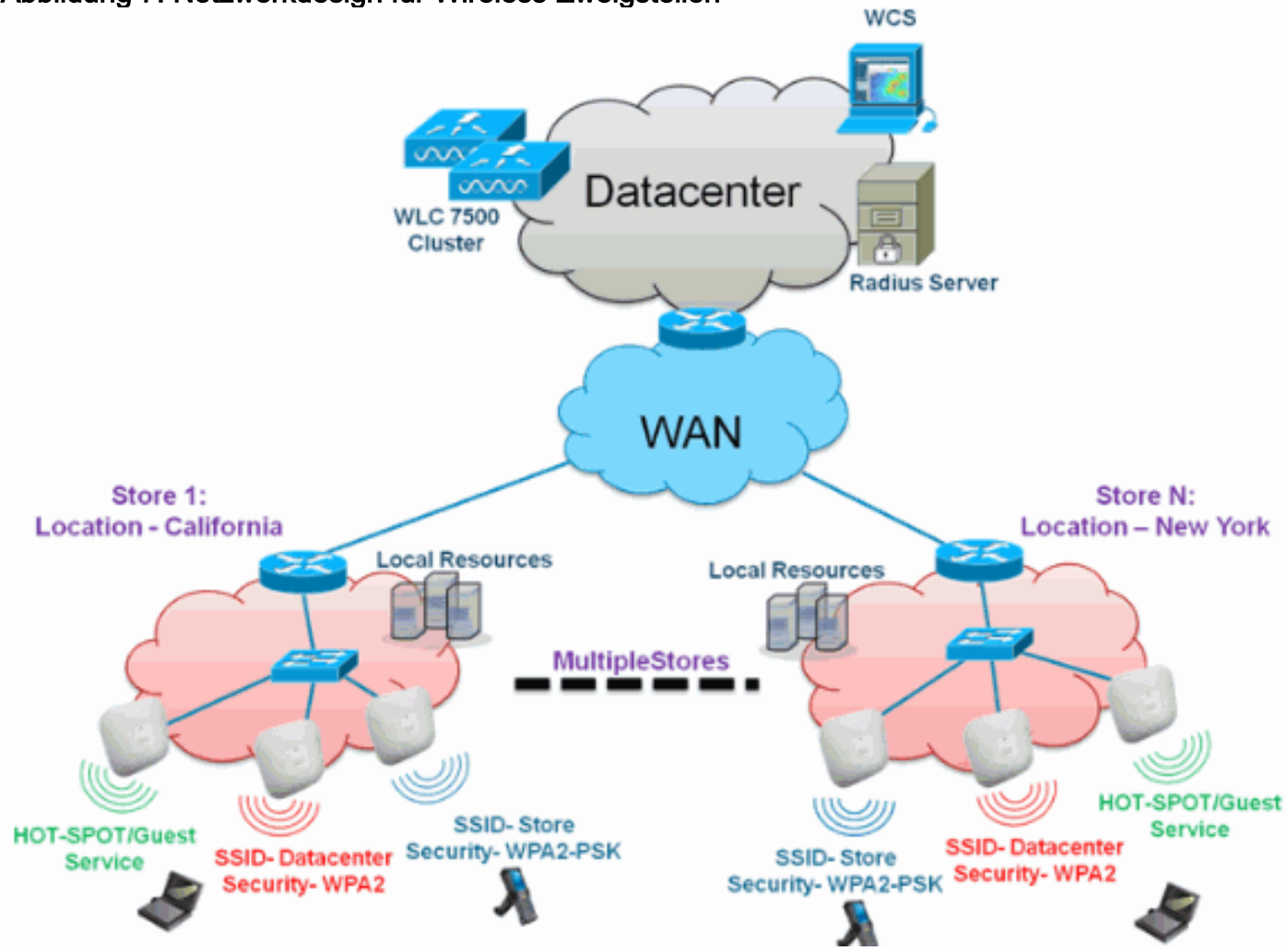
Netzwerkdesign für Wireless-Zweigstellen

Der Rest dieses Dokuments beschreibt die Richtlinien und Best Practices für die Implementierung sicherer verteilter Zweigstellennetzwerke. Die FlexConnect-Architektur wird für Wireless-Zweigstellennetzwerke empfohlen, die diese Designanforderungen erfüllen.

Primäre Designanforderungen

- Zweigstellengröße, die auf bis zu 100 APs und 5.000 Quadratmeter skalierbar ist Fuß pro AP)
- Zentrale Verwaltung und Fehlerbehebung
- Keine Betriebsausfallzeiten
- Client-basierte Segmentierung des Datenverkehrs
- Nahtlose und sichere Wireless-Verbindungen zu Unternehmensressourcen
- PCI-konform
- Gastsupport

Abbildung 7: Netzwerkdesign für Wireless-Zweigstellen



Übersicht

Kunden in Zweigstellen sehen es zunehmend schwieriger und teurer, skalierbare und sichere Netzwerkservices mit vollem Funktionsumfang über geografische Standorte hinweg bereitzustellen. Um Kunden zu unterstützen, setzt Cisco auf die Flex 7500-Plattform, um diese Herausforderungen zu meistern.

Die Flex 7500-Lösung virtualisiert die komplexen Prozesse für Sicherheit, Management, Konfiguration und Fehlerbehebung im Rechenzentrum und erweitert diese Services anschließend transparent auf die einzelnen Zweigstellen. Bereitstellungen mit Flex 7500 sind für die IT einfacher einzurichten, zu verwalten und vor allem zu skalieren.

Vorteile

- Erhöhte Skalierbarkeit durch Unterstützung von 6000 APs

- Erhöhte Ausfallsicherheit durch FlexConnect-Fehlertoleranz
- Erhöhung der Segmentierung des Datenverkehrs mit FlexConnect (Central und Local Switching)
- Einfache Verwaltung durch Replizierung von Ladendesigns mithilfe von AP-Gruppen und FlexConnect-Gruppen

Funktionen für Außenstellen-Netzwerkdesign

Die übrigen Abschnitte im Handbuch enthalten nützliche Funktionen und Empfehlungen zur Umsetzung des Netzwerkdesigns, wie in Abbildung 7 dargestellt.

Funktionen:

Hauptfunktionen	Highlights
AP-Gruppen	Einfache Betriebs-/Verwaltungsmöglichkeiten bei der Verwaltung mehrerer Zweigstellen Bietet außerdem die Flexibilität, Konfigurationen für ähnliche Zweigstellen zu replizieren.
FlexConnect-Gruppen	FlexConnect-Gruppen bieten die Funktionen "Lokaler Backup-Radius", "CCKM/OKC Fast Roaming" und "Lokale Authentifizierung".
Fehlertoleranz	Verbessert die Ausfallsicherheit in Wireless-Zweigstellen und verhindert Ausfallzeiten.
ELM (Enhanced Local Mode für Adaptive wIPS)	Bereitstellung von adaptiven wIPS-Funktionen für Clients ohne Beeinträchtigung der Client-Leistung
Client-Limit pro WLAN	Beschränkung der Gesamtzahl von Gastclients im Zweigstellennetzwerk.
AP-Pre-Image-Download	Reduziert Ausfallzeiten durch Upgrades in Zweigstellen.
Automatisches Konvertieren von APs in FlexConnect	Funktion zum automatischen Konvertieren von APs in FlexConnect für Ihre Zweigstelle.
Gastzugriff	Mit FlexConnect können Sie die bestehende Cisco Gastzugriffs-Architektur fortsetzen.

IPv6-Unterstützungs-Matrix

Funktionen	Zentral Switched		Lokal gewechselt	
	5500/WiSM-2	Flex 7500	5500/WiSM-2	Flex 7500
IPv6 (Client-Mobilität)	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
IPv6 RA Guard	Unterstützt	Unterstützt	Unterstützt	Unterstützt
IPv6 DHCP Guard	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
IPv6 Source Guard	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Beschränkung der RA-Drosselung/Rate	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
IPv6-ACL	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
IPv6-Client-Transparenz	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Caching von IPv6 Neighbor Discovery	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
IPv6-Bridging	Unterstützt	Nicht unterstützt	Unterstützt	Unterstützt

Funktionsmatrix

Eine Funktionsmatrix zur FlexConnect-Funktion finden Sie in der FlexConnect-Funktionsmatrix.

AP-Gruppen

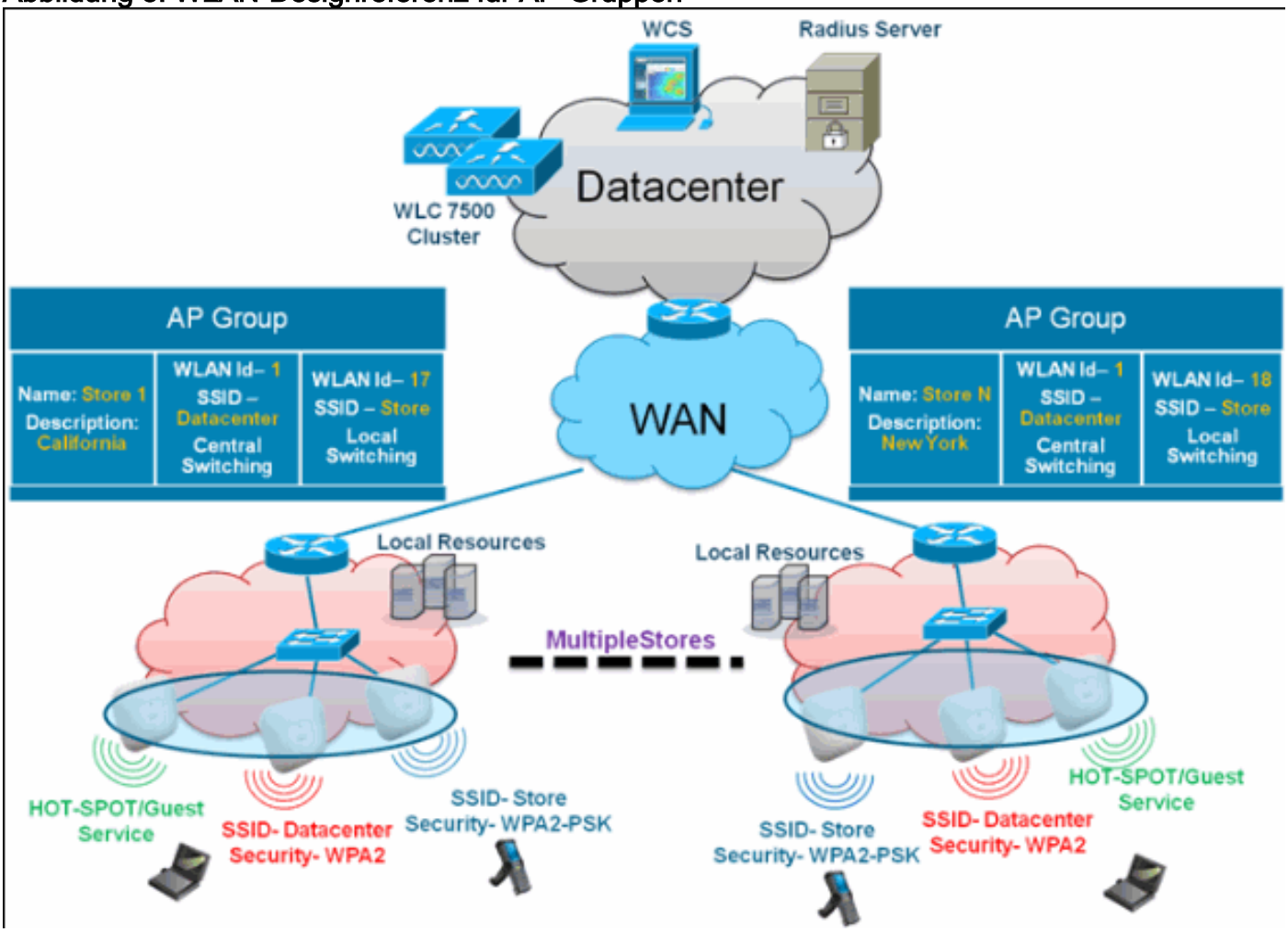
Nachdem Sie WLANs auf dem Controller erstellt haben, können Sie diese selektiv (mithilfe von Access Point-Gruppen) an verschiedene Access Points veröffentlichen, um Ihr Wireless-Netzwerk besser zu verwalten. In einer typischen Bereitstellung werden alle Benutzer in einem WLAN einer einzigen Schnittstelle auf dem Controller zugeordnet. Aus diesem Grund befinden sich alle diesem WLAN zugeordneten Benutzer im gleichen Subnetz oder VLAN. Sie können die Last jedoch auf mehrere Schnittstellen oder auf eine Benutzergruppe verteilen, indem Sie Zugangspunktgruppen erstellen, z. B. für einzelne Abteilungen (z. B. Marketing, Technik oder Betrieb). Darüber hinaus können diese Access Point-Gruppen in separaten VLANs konfiguriert werden, um die Netzwerkadministration zu vereinfachen.

In diesem Dokument werden AP-Gruppen verwendet, um die Netzwerkverwaltung zu vereinfachen, wenn mehrere Geschäfte an verschiedenen geografischen Standorten verwaltet

werden. Um den Betrieb zu vereinfachen, erstellt das Dokument pro Geschäft eine AP-Gruppe, um diese Anforderungen zu erfüllen:

- Das zentral geswitchte SSID-**Rechenzentrum** für den Administratorzugriff durch den Local Store Manager ist in allen Geschäften verfügbar.
- Lokal gewechselter SSID-**Store** mit unterschiedlichen WPA2-PSK-Schlüsseln in allen Geschäften für Handheld-Scanner.

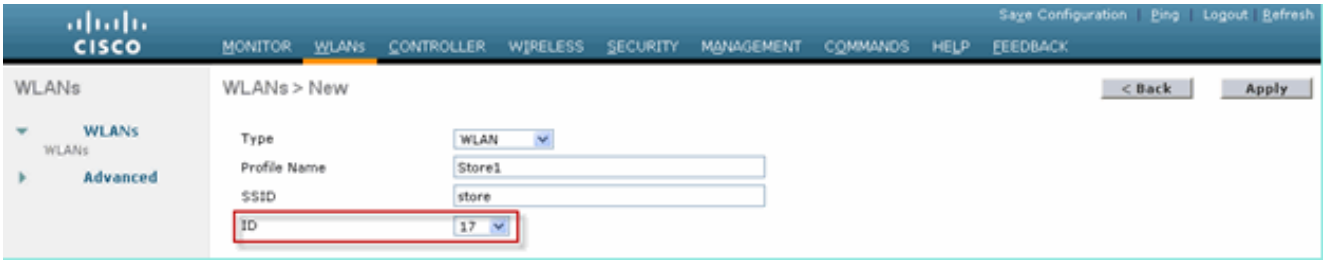
Abbildung 8: WLAN-Designreferenz für AP-Gruppen



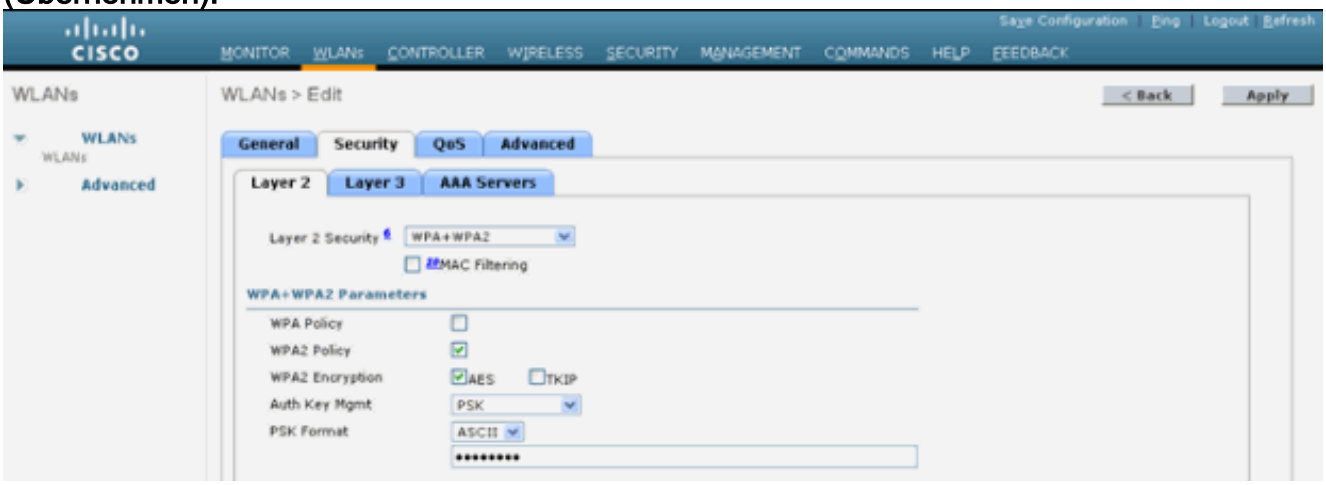
Konfigurationen von WLC

Führen Sie diese Schritte aus:

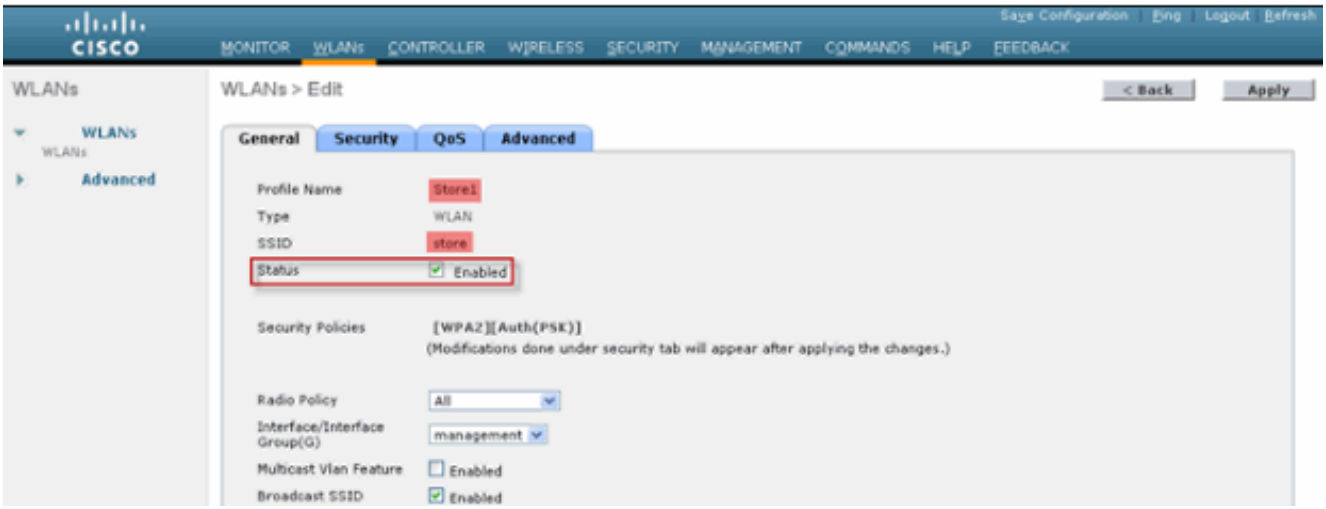
1. Geben Sie auf der Seite WLANs > New (WLANs > Neu) **Store1** im Feld Profilname ein, geben Sie **store** in das Feld SSID ein, und wählen Sie **17** aus der ID-Dropdown-Liste aus.**Hinweis:** Die WLAN-IDs 1-16 sind Teil der Standardgruppe und können nicht gelöscht werden. Um unsere Anforderung zu erfüllen, für jeden Speicher denselben SSID-Speicher mit einem anderen WPA2-PSK zu verwenden, müssen Sie die WLAN-ID 17 und höher verwenden, da diese nicht zur Standardgruppe gehören und auf jeden Speicher beschränkt werden
können.



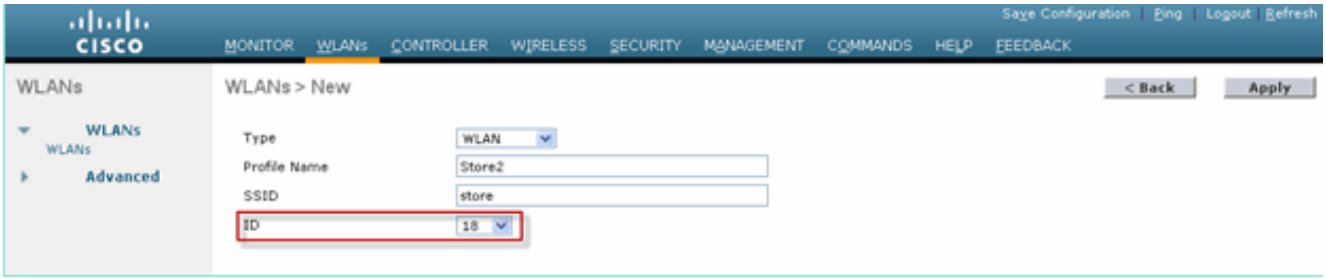
2. Wählen Sie unter WLAN > Security (WLAN > Sicherheit) **PSK** aus der Dropdown-Liste Auth Key Mgmt (Auth-Schlüsselverwaltung) aus, wählen Sie **ASCII** aus der Dropdown-Liste PSK Format (PSK-Format) aus, und klicken Sie auf **Apply (Übernehmen).**

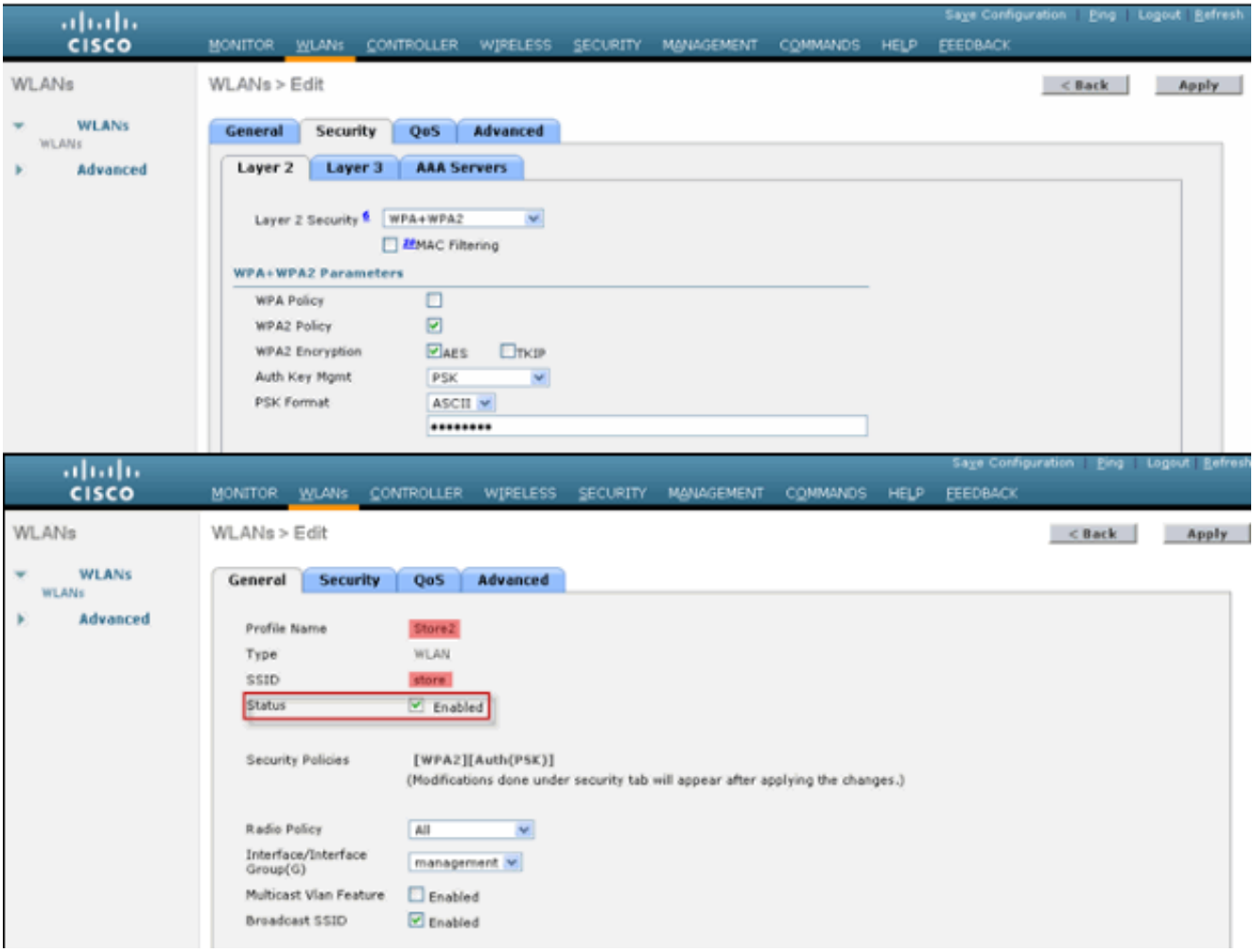


3. Klicken Sie auf **WLAN > General**, überprüfen Sie die Änderung der Sicherheitsrichtlinien, und aktivieren Sie das Kontrollkästchen **Status**, um das WLAN zu aktivieren.



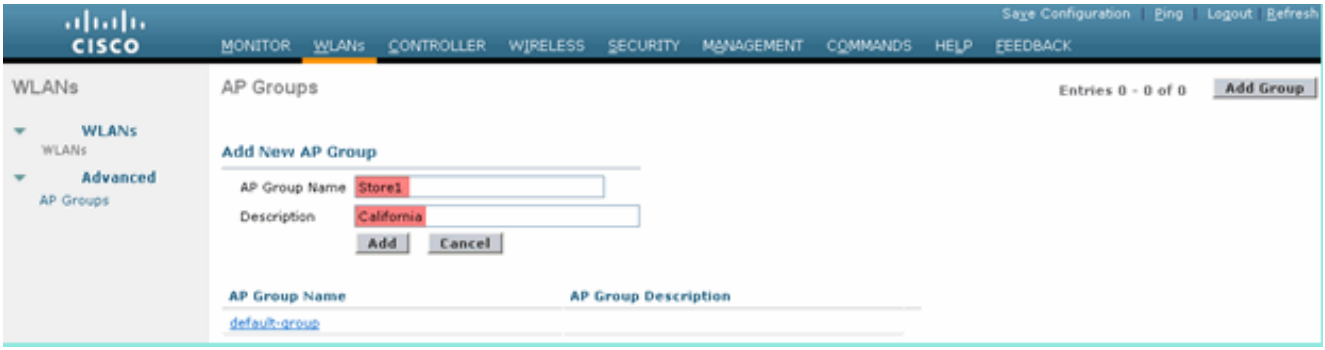
4. Wiederholen Sie die Schritte 1, 2 und 3 für den neuen WLAN-Profil-**Store2** mit SSID-**Speicher** und ID 18.



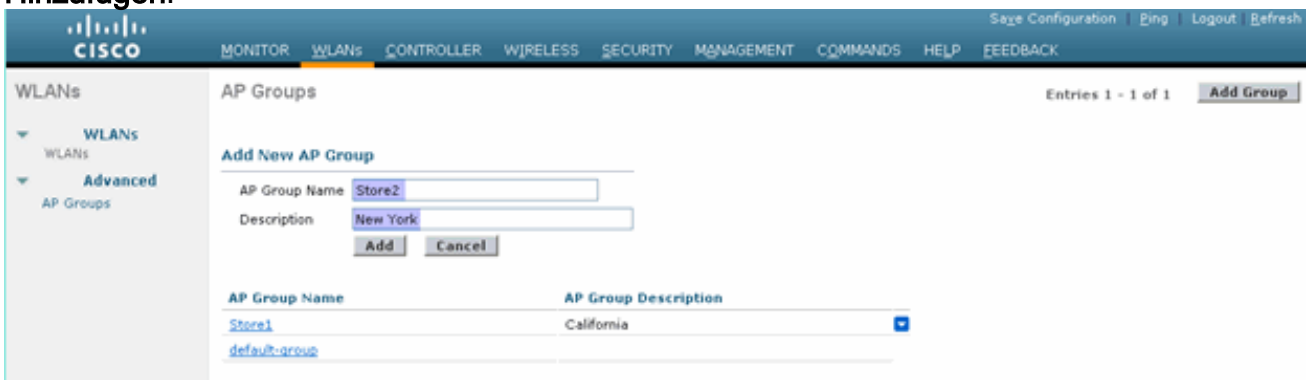


5. Erstellen und aktivieren Sie das WLAN-Profil mit Profile Name **DataCenter**, SSID **DataCenter** und ID 1.**Hinweis:** Bei der Erstellung sind WLAN-IDs von 1 bis 16 automatisch Teil der default-ap-Gruppe.
6. Überprüfen Sie unter WLAN den Status der WLAN-IDs 1, 17 und 18.

7. Klicken Sie auf **WLAN > Erweitert > AP-Gruppe > Gruppe hinzufügen**.
8. Fügen Sie AP Group Name **Store1**, wie WLAN Profile **Store1** und Description as Location des Speichers hinzu. In diesem Beispiel wird Kalifornien als Speicherort des Geschäfts verwendet.
9. Klicken Sie abschließend auf **Hinzufügen**.

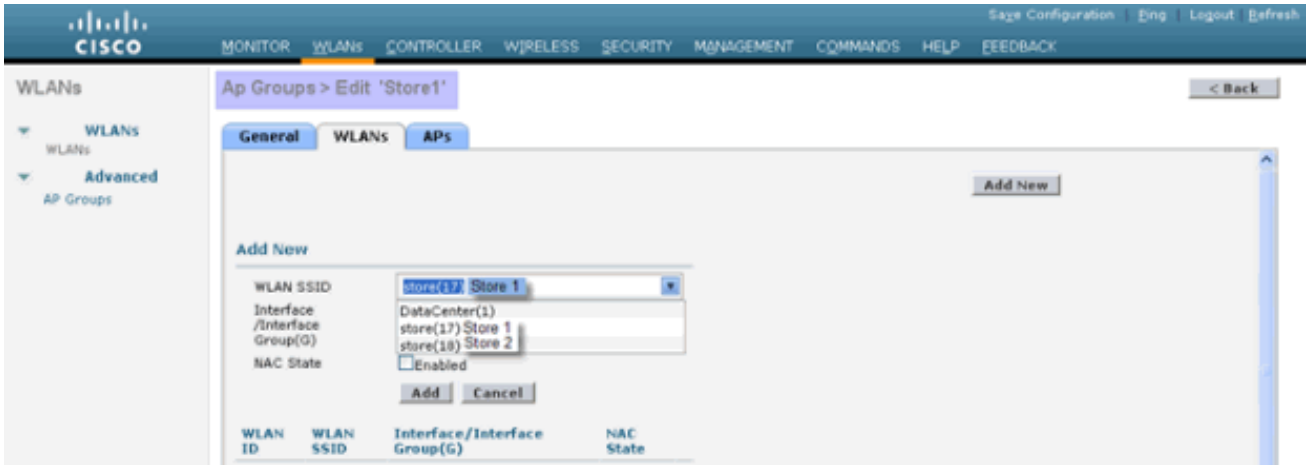


10. Klicken Sie auf **Gruppe hinzufügen**, und erstellen Sie AP Group Name **Store2** und Beschreibung New York.
11. Klicken Sie auf **Hinzufügen**.

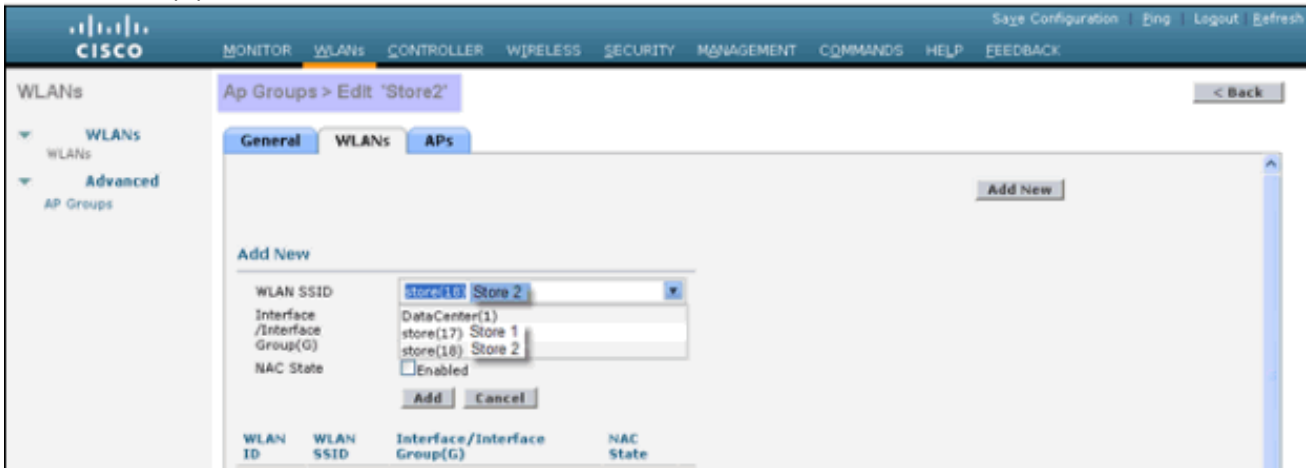


12. Überprüfen Sie die Gruppenerstellung, indem Sie auf **WLAN > Erweitert > AP Groups** klicken.

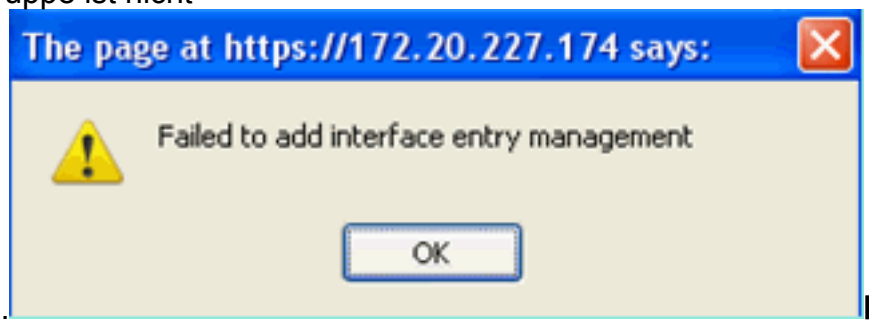
13. Klicken Sie auf AP Group Name **Store1**, um das WLAN hinzuzufügen oder zu bearbeiten.
14. Klicken Sie auf **Neu hinzufügen**, um das WLAN auszuwählen.
15. Wählen Sie unter WLAN im Dropdown-Menü WLAN SSID (WLAN-SSID) die Option **WLAN ID 17 store (17)** aus.
16. Klicken Sie auf **Hinzufügen**, nachdem die WLAN-ID 17 ausgewählt wurde.
17. Wiederholen Sie die Schritte 14-16 für die WLAN-ID 1 DataCenter(1). Dieser Schritt ist optional und nur erforderlich, wenn Sie den Zugriff auf die Remote-Ressource zulassen möchten.



18. Wechseln Sie zurück zum Bildschirm **WLAN > Advanced > AP Groups**.
19. Klicken Sie auf AP Group Name **Store2**, um WLAN hinzuzufügen oder zu bearbeiten.
20. Klicken Sie auf **Neu hinzufügen**, um das WLAN auszuwählen.
21. Wählen Sie unter WLAN im Dropdown-Menü WLAN SSID die Option **WLAN ID 18 store(18)** aus.
22. Klicken Sie auf **Hinzufügen**, nachdem die WLAN-ID 18 ausgewählt wurde.
23. Wiederholen Sie die Schritte 14-16 für die WLAN-ID 1 DataCenter(1).



Hinweis: Das Hinzufügen mehrerer WLAN-Profile mit derselben SSID unter einer einzigen WAP-Gruppe ist nicht



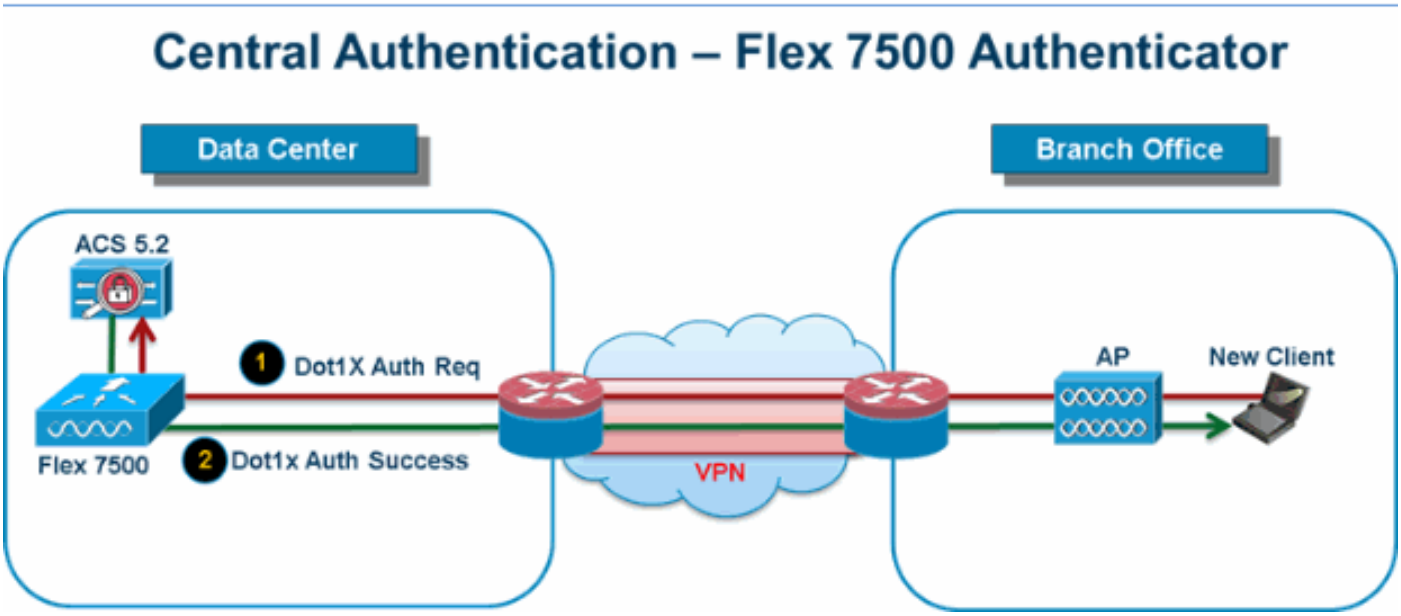
zulässig. **Hinweis:** Das Hinzufügen von APs zur AP-Gruppe ist in diesem Dokument nicht enthalten. Es ist jedoch für Clients erforderlich, um auf Netzwerkdienste zuzugreifen.

Zusammenfassung

- AP-Gruppen vereinfachen die Netzwerkverwaltung.
- Einfache Fehlerbehebung mit detaillierter Detaillierung für jede Außenstelle
- Erhöhte Flexibilität

FlexConnect-Gruppen

Abbildung 9: Zentrale Dot1X-Authentifizierung (Flex 7500 fungiert als Authentifizierer)



In den meisten typischen Zweigstellenbereitstellungen ist leicht vorherzusehen, dass die Client-802.1X-Authentifizierung zentral im Rechenzentrum erfolgt, wie in Abbildung 9 gezeigt. Da das oben beschriebene Szenario vollkommen gültig ist, wirft es folgende Bedenken auf:

- Wie können Wireless-Clients 802.1X-Authentifizierung durchführen und auf Rechenzentrumsdienste zugreifen, wenn Flex 7500 ausfällt?
- Wie können Wireless-Clients eine 802.1X-Authentifizierung durchführen, wenn die WAN-Verbindung zwischen Zweigstelle und Rechenzentrum ausfällt?
- Können bei WAN-Ausfällen Auswirkungen auf die Außenstellenmobilität auftreten?
- Bietet die FlexConnect-Lösung keine Ausfallzeiten in der Zweigstelle?

Die FlexConnect Group ist in erster Linie auf diese Herausforderungen ausgelegt und sollte daher entwickelt werden. Darüber hinaus wird die Organisation jeder Zweigstelle vereinfacht, da alle FlexConnect Access Points jeder Zweigstelle Teil einer einzigen FlexConnect-Gruppe sind.

Hinweis: FlexConnect-Gruppen entsprechen nicht AP-Gruppen.

Primäre Ziele von FlexConnect-Gruppen

Backup RADIUS-Server-Failover

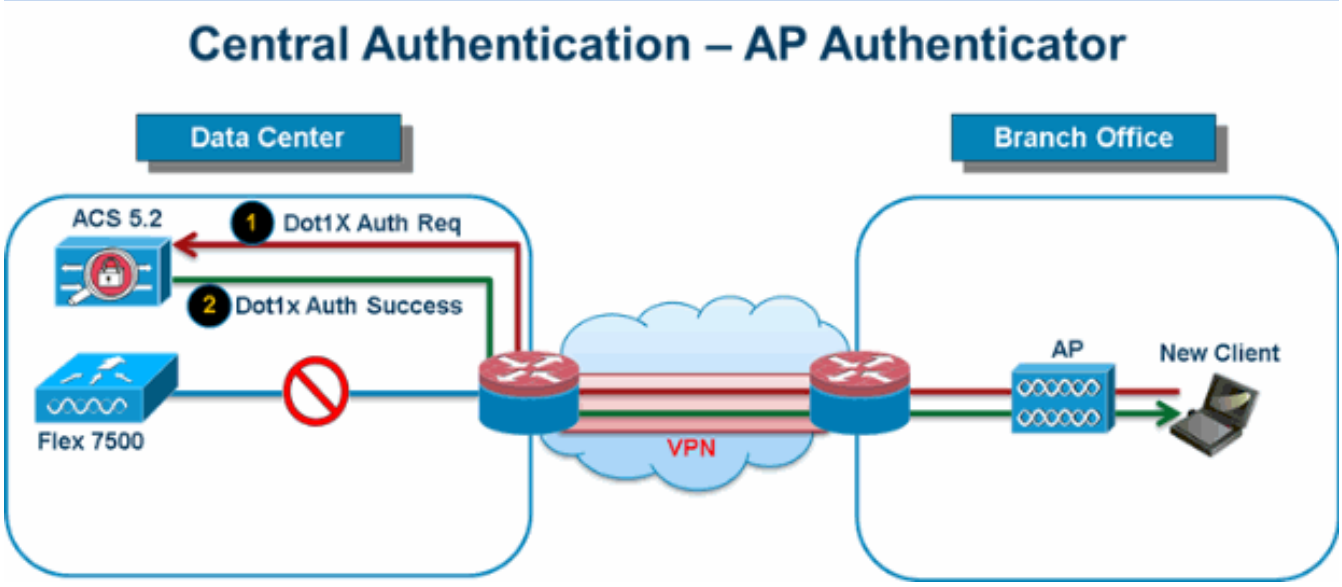
- Sie können den Controller so konfigurieren, dass ein FlexConnect Access Point im Standalone-Modus eine vollständige 802.1X-Authentifizierung für einen Backup-RADIUS-Server durchführen kann. Um die Ausfallsicherheit der Zweigstelle zu erhöhen, können Administratoren einen primären Backup-RADIUS-Server oder einen primären und sekundären Backup-RADIUS-Server konfigurieren. Diese Server werden nur verwendet, wenn der FlexConnect Access Point nicht mit dem Controller verbunden ist.

Hinweis: Backup RADIUS Accounting wird nicht unterstützt.

Lokale Authentifizierung

- Vor der Codeversion 7.0.98.0 wurde die lokale Authentifizierung nur dann unterstützt, wenn sich FlexConnect im Standalone-Modus befindet, um sicherzustellen, dass die Client-Konnektivität während eines WAN-Verbindungsausfalls nicht beeinträchtigt wird. Mit der Version 7.0.116.0 wird diese Funktion jetzt auch dann unterstützt, wenn sich die FlexConnect

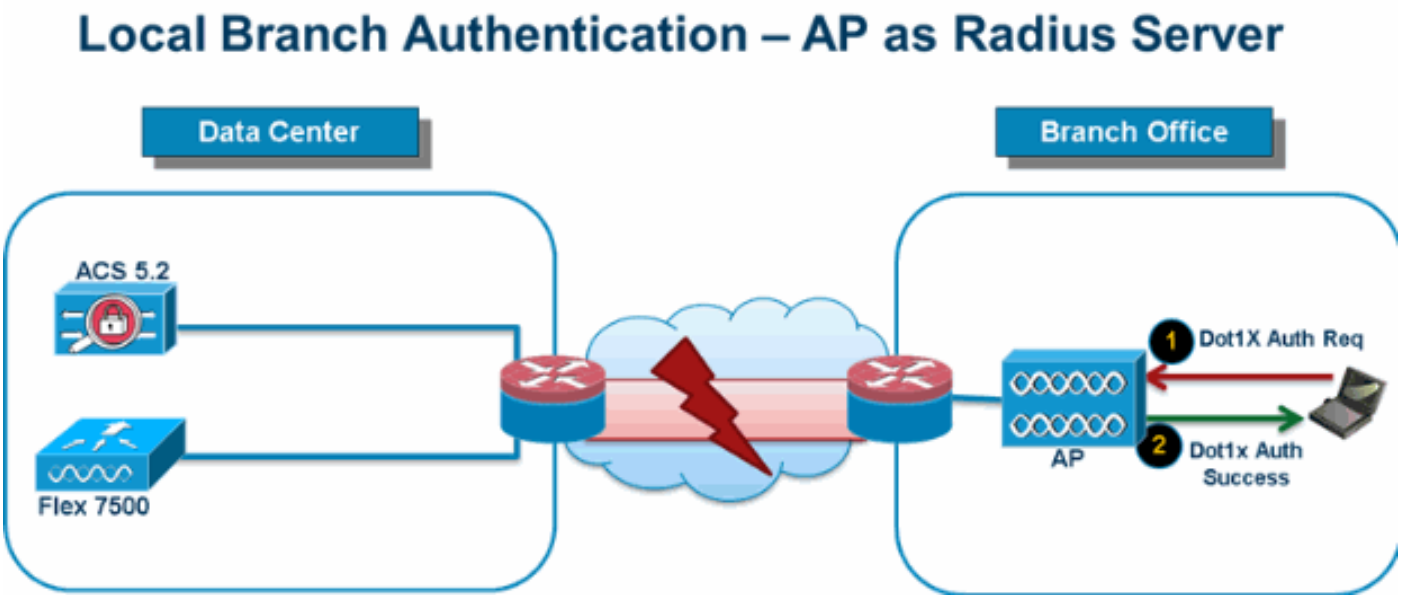
Access Points im Connected Mode befinden.**Abbildung 10: Zentrale Dot1X-Authentifizierung (FlexConnect-APs fungieren als Authentifizierer)**



Wie in Abbildung 10 gezeigt, können Zweigstellen-Clients weiterhin eine 802.1X-Authentifizierung durchführen, wenn die Verbindungen der FlexConnect Branch-APs mit Flex 7500 unterbrochen werden. Solange der RADIUS/ACS-Server von der Zweigstelle aus erreichbar ist, authentifizieren Wireless-Clients weiterhin Wireless-Services und greifen auf diese zu. Mit anderen Worten: Wenn sich der RADIUS/ACS in der Zweigstelle befindet, authentifizieren sich die Clients und greifen auf Wireless-Services auch während eines WAN-Ausfalls zu.**Hinweis:** Diese Funktion kann in Verbindung mit der FlexConnect-Backup-RADIUS-Serverfunktion verwendet werden. Wenn eine FlexConnect-Gruppe sowohl mit einem Backup-RADIUS-Server als auch mit einer lokalen Authentifizierung konfiguriert ist, versucht der FlexConnect-Access Point immer, Clients zuerst mithilfe des primären Backup-RADIUS-Servers zu authentifizieren, gefolgt vom sekundären Backup-RADIUS-Server (wenn der primäre Access Point nicht erreichbar ist) und schließlich dem lokalen EAP-Server auf dem FlexConnect-Access Point selbst (wenn der primäre und sekundäre Access Point nicht erreichbar sind).

Lokaler EAP (Continuous Local Authentication)

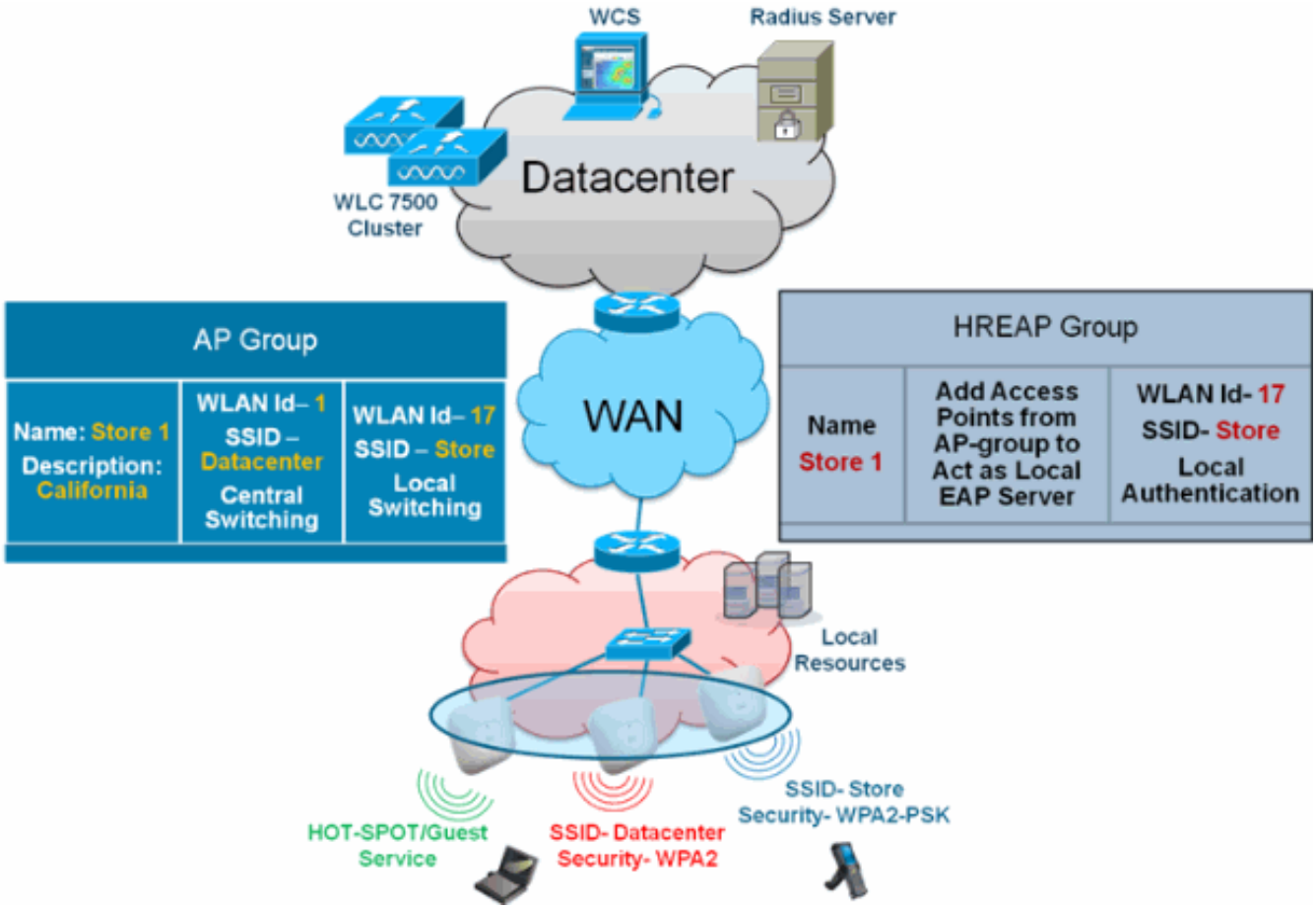
Abbildung 11: Dot1X-Authentifizierung (FlexConnect-APs agieren als Local-EAP-Server)



- Sie können den Controller so konfigurieren, dass ein FlexConnect AP im Standalone- oder Connected-Modus LEAP- oder EAP-FAST-Authentifizierung für bis zu 100 statisch konfigurierte Benutzer ausführen kann. Der Controller sendet die statische Liste der Benutzernamen und Kennwörter an jeden FlexConnect-Access Point der jeweiligen FlexConnect-Gruppe, wenn dieser dem Controller beitritt. Jeder Access Point in der Gruppe authentifiziert nur seine eigenen zugeordneten Clients.
- Diese Funktion eignet sich ideal für Kunden, die von einem autonomen Access Point-Netzwerk zu einem Lightweight FlexConnect Access Point-Netzwerk migrieren und nicht daran interessiert sind, eine große Benutzerdatenbank zu pflegen oder ein anderes Hardwaregerät hinzuzufügen, um die im autonomen Access Point verfügbare RADIUS-Serverfunktionalität zu ersetzen.
- Wie in Abbildung 11 gezeigt, können FlexConnect-APs automatisch als Local-EAP-Server fungieren, wenn der RADIUS/ACS-Server im Rechenzentrum nicht erreichbar ist, um die Dot1X-Authentifizierung für Clients in Wireless-Zweigstellen durchzuführen.

CCKM/OKC Fast Roaming

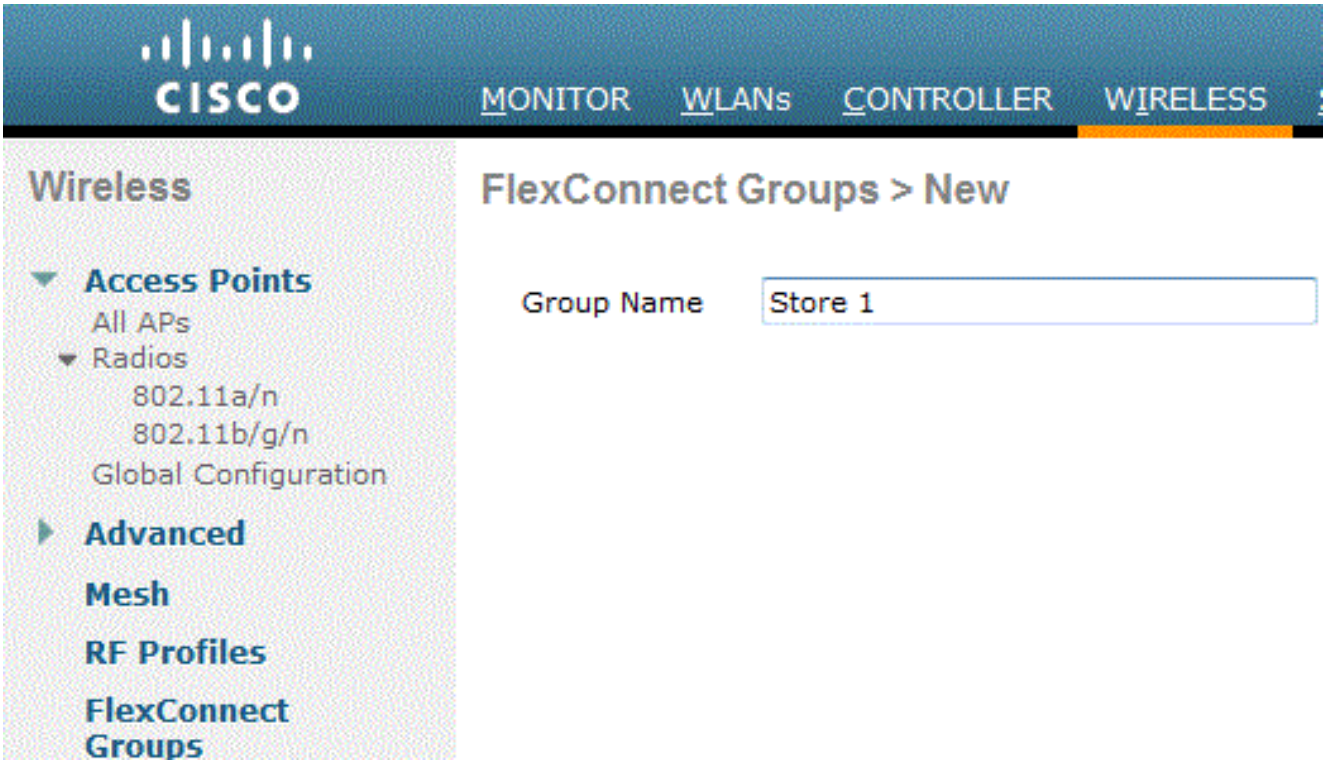
- FlexConnect-Gruppen sind für schnelles CCKM/OKC-Roaming erforderlich, um mit FlexConnect Access Points arbeiten zu können. Ein schnelles Roaming wird durch Zwischenspeichern einer Ableitung des Master-Schlüssels aus einer vollständigen EAP-Authentifizierung erreicht, sodass ein einfacher und sicherer Schlüsselaustausch möglich ist, wenn ein Wireless-Client mit einem anderen Access Point wechselt. Diese Funktion verhindert, dass eine vollständige RADIUS EAP-Authentifizierung ausgeführt werden muss, wenn der Client von einem Access Point zu einem anderen wechselt. Die FlexConnect-Access Points müssen die CCKM/OKC-Cache-Informationen für alle Clients abrufen, die möglicherweise zugeordnet werden, damit diese schnell verarbeitet werden können, anstatt sie an den Controller zurückzusenden. Wenn Sie beispielsweise einen Controller mit 300 Access Points und 100 Clients haben, die eine Verbindung herstellen können, ist das Senden des CCKM/OKC-Cache für alle 100 Clients nicht praktikabel. Wenn Sie eine FlexConnect-Gruppe mit einer begrenzten Anzahl von Access Points erstellen (z. B. eine Gruppe für vier Access Points in einer Außenstelle), wechseln die Clients nur zwischen diesen vier Access Points, und der CCKM/OKC-Cache wird nur dann auf diese vier Access Points verteilt, wenn die Clients einem von ihnen zugeordnet sind.
- Diese Funktion stellt zusammen mit Backup Radius und lokaler Authentifizierung (Local-EAP) sicher, dass **keine Ausfallzeiten** für Ihre Zweigstellen auftreten.**Hinweis:** CCKM/OKC Fast Roaming zwischen FlexConnect- und Nicht-FlexConnect-Access Points wird nicht unterstützt.**Abbildung 12: Wireless-Netzwerkdesign-Referenz mit FlexConnect-Gruppen**



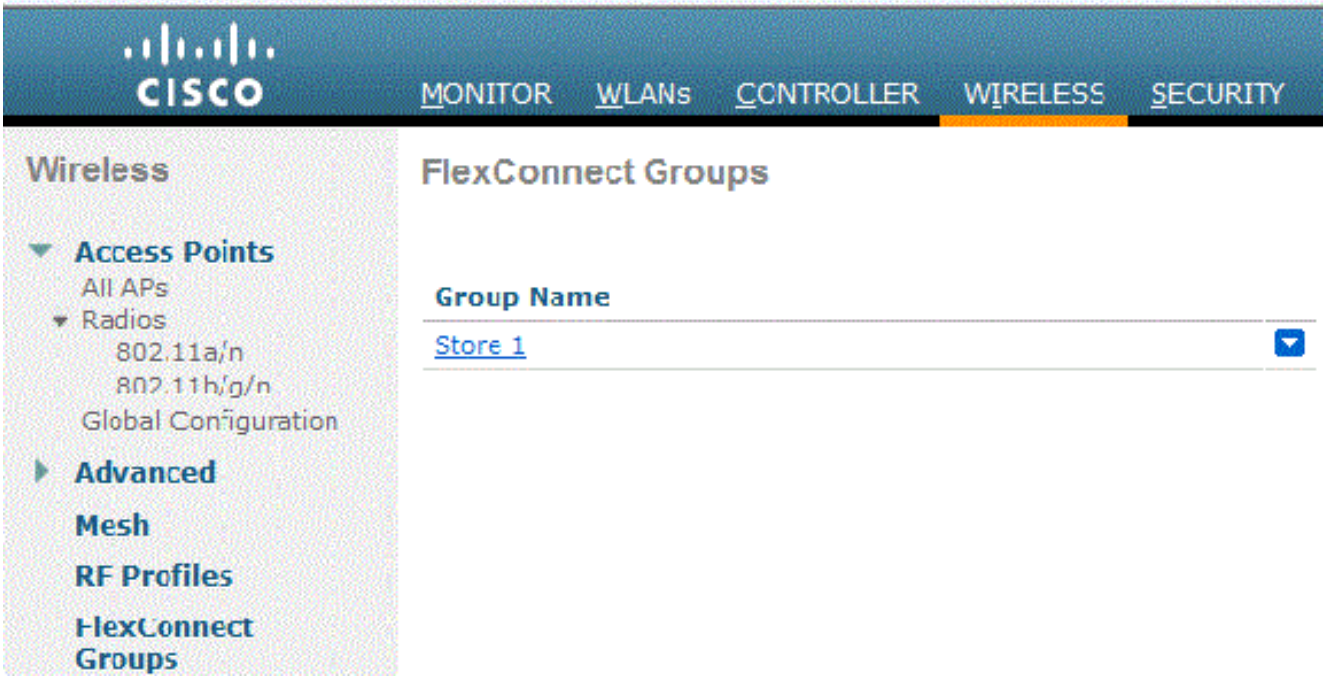
Konfiguration der FlexConnect-Gruppe vom WLC

Führen Sie die Schritte in diesem Abschnitt aus, um FlexConnect-Gruppen für die Unterstützung der lokalen Authentifizierung mithilfe von LEAP zu konfigurieren, wenn sich FlexConnect entweder im Connected- oder im Standalone-Modus befindet. Das Konfigurationsbeispiel in Abbildung 12 veranschaulicht die objektiven Unterschiede und die 1:1-Zuordnung zwischen der AP-Gruppe und der FlexConnect-Gruppe.

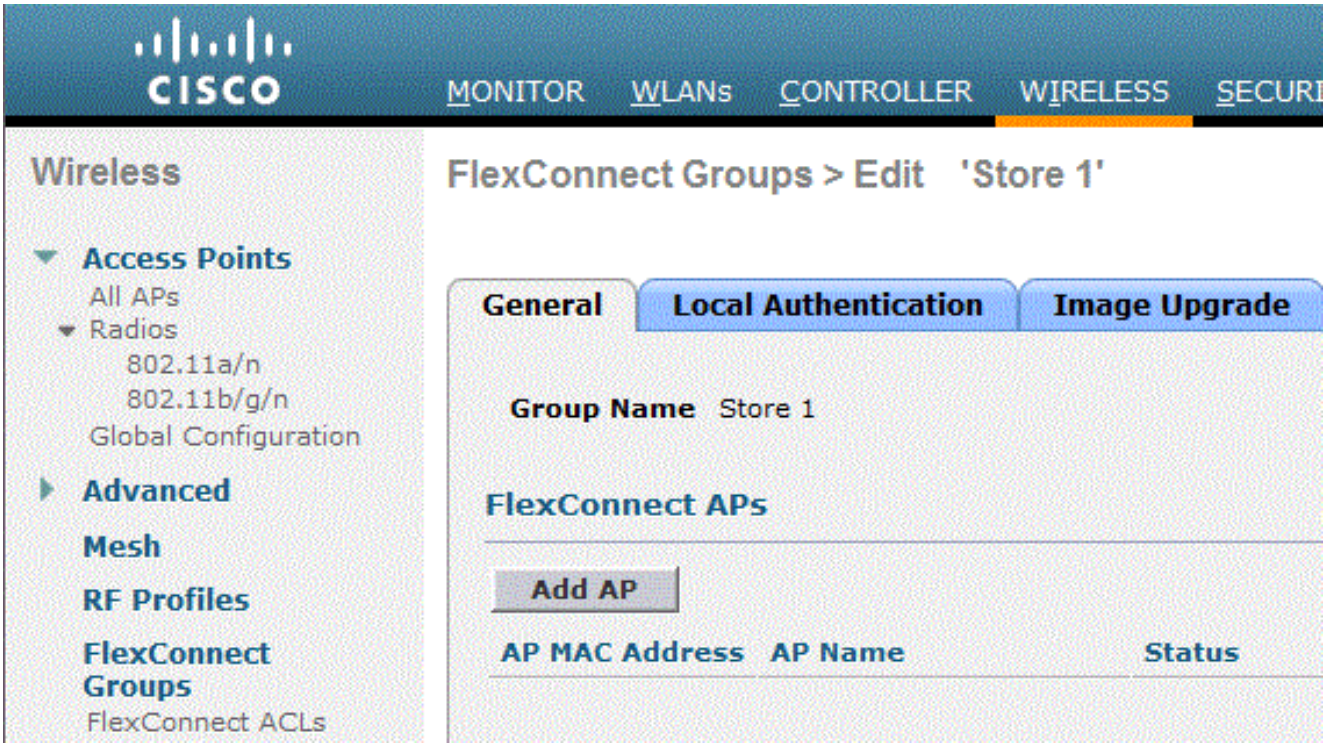
1. Klicken Sie unter Wireless > FlexConnect Groups **auf Neu**.
2. Zuweisen des Group Name Store 1, ähnlich der Beispielkonfiguration, wie in Abbildung 12 gezeigt.
3. Klicken Sie auf **Übernehmen**, wenn der Gruppenname festgelegt ist.



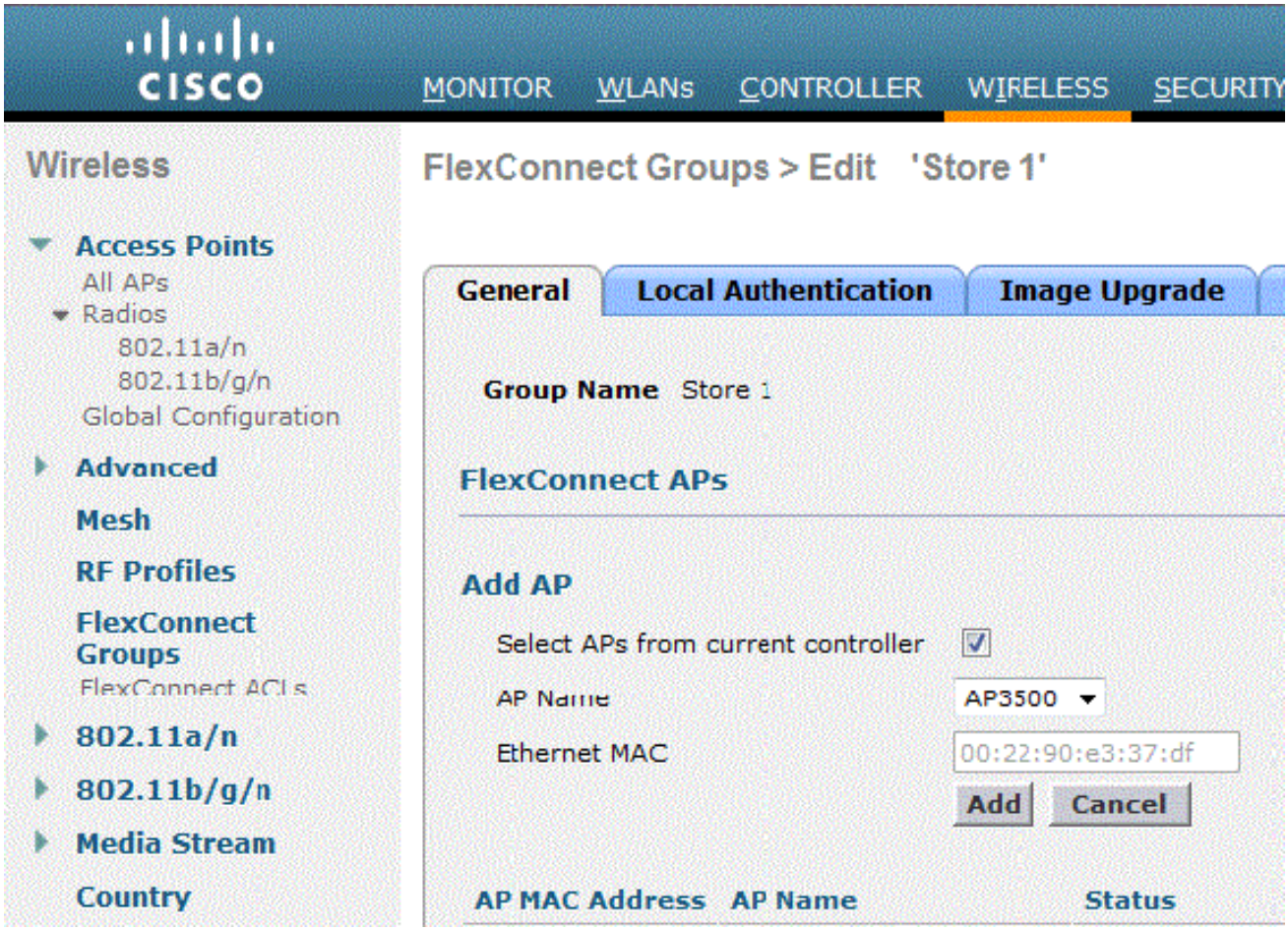
4. Klicken Sie auf den Group Name **Store 1**, den Sie gerade zur weiteren Konfiguration erstellt haben.



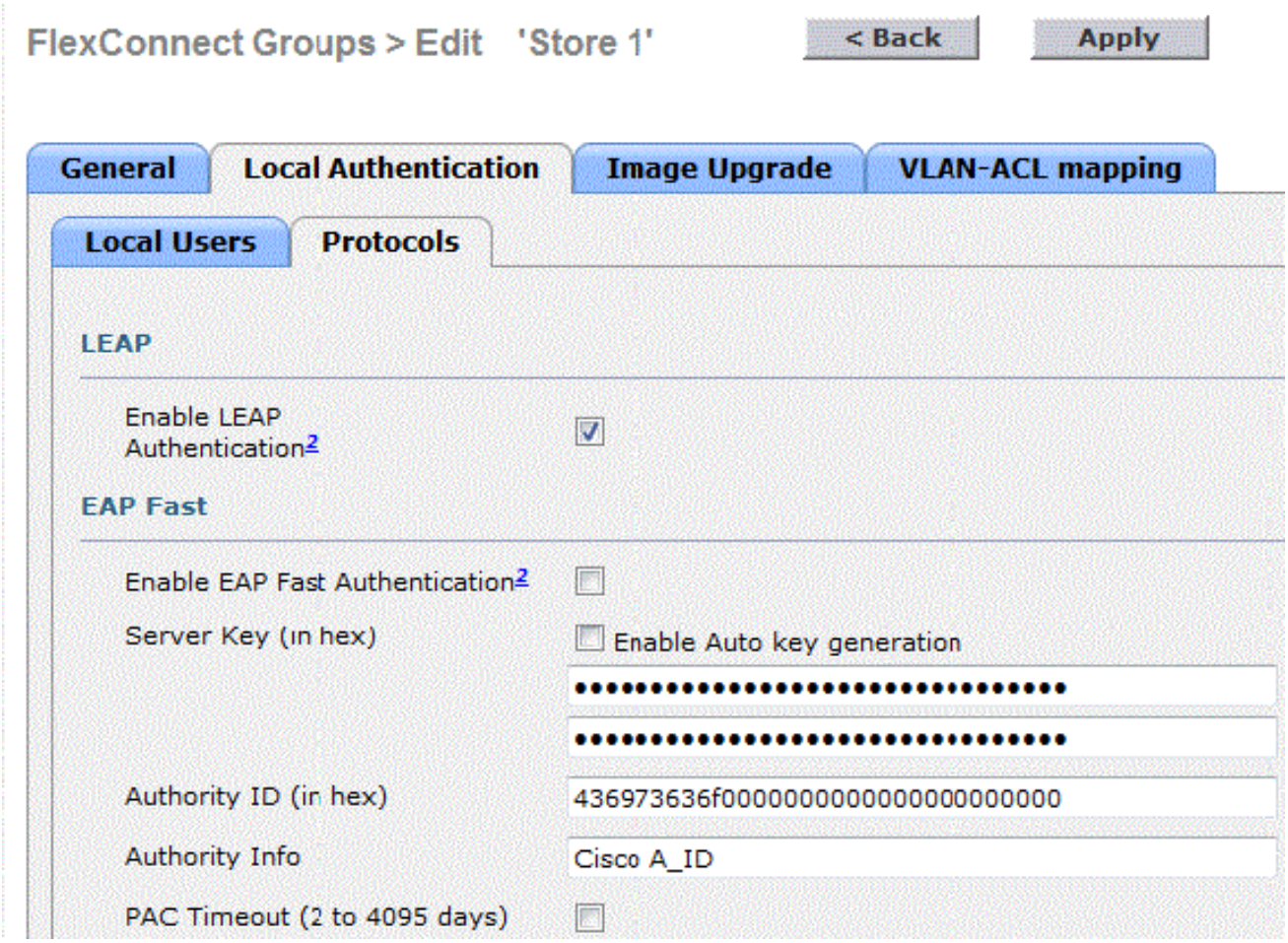
5. Klicken Sie auf **AP hinzufügen**.



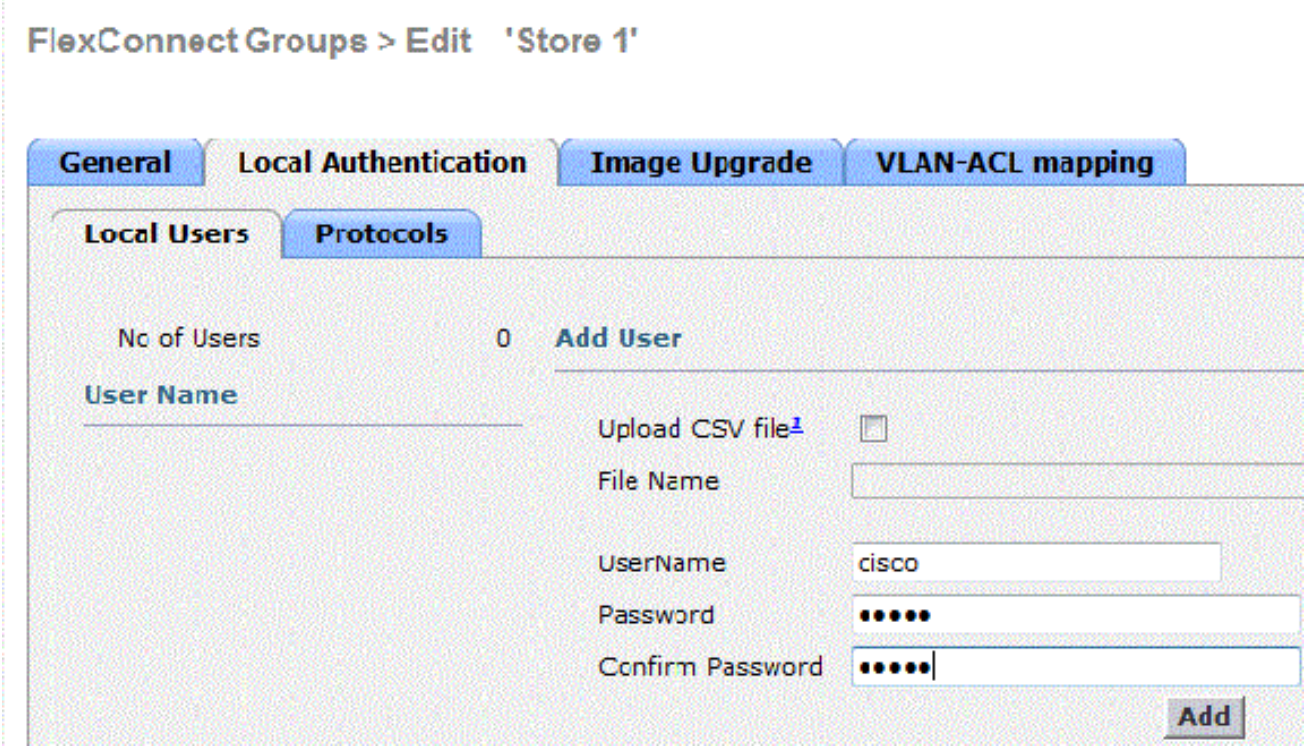
6. Aktivieren Sie das Kontrollkästchen **Lokale Authentifizierung aktivieren**, um die lokale Authentifizierung zu aktivieren, wenn sich der Access Point im Standalone-Modus befindet.**Hinweis:** Schritt 20 zeigt, wie die lokale Authentifizierung für AP im Connected Mode aktiviert wird.
7. Aktivieren Sie das Kontrollkästchen **Access Points aus aktuellem Controller auswählen**, um das Dropdown-Menü "AP Name" zu aktivieren.
8. Wählen Sie den Access Point aus dem Dropdown-Menü aus, der Teil dieser FlexConnect-Gruppe sein muss.
9. Klicken Sie auf **Hinzufügen**, nachdem der Access Point aus dem Dropdown-Menü ausgewählt wurde.
10. Wiederholen Sie die Schritte 7 und 8, um alle APs dieser FlexConnect-Gruppe hinzuzufügen, die ebenfalls Teil des AP-Group Store 1 sind. In Abbildung 12 wird die 1:1-Zuordnung zwischen der AP-Gruppe und der FlexConnect-Gruppe erläutert.Wenn Sie eine AP-Gruppe pro Speicher erstellt haben (Abbildung 8), sollten im Idealfall alle APs dieser AP-Gruppe zu dieser FlexConnect-Gruppe gehören (Abbildung 12). Die Aufrechterhaltung des 1:1-Verhältnisses zwischen der AP-Gruppe und der FlexConnect-Gruppe vereinfacht die
Netzwerkverwaltung.



11. Klicken Sie auf **Lokale Authentifizierung > Protokolle** und aktivieren Sie das Kontrollkästchen **LEAP-Authentifizierung aktivieren**.
12. Klicken Sie nach dem Festlegen des Kontrollkästchens auf **Übernehmen**.**Hinweis:** Wenn Sie über einen Backup-Controller verfügen, stellen Sie sicher, dass die FlexConnect-Gruppen identisch sind und die AP-MAC-Adresseinträge pro FlexConnect-Gruppe enthalten sind.

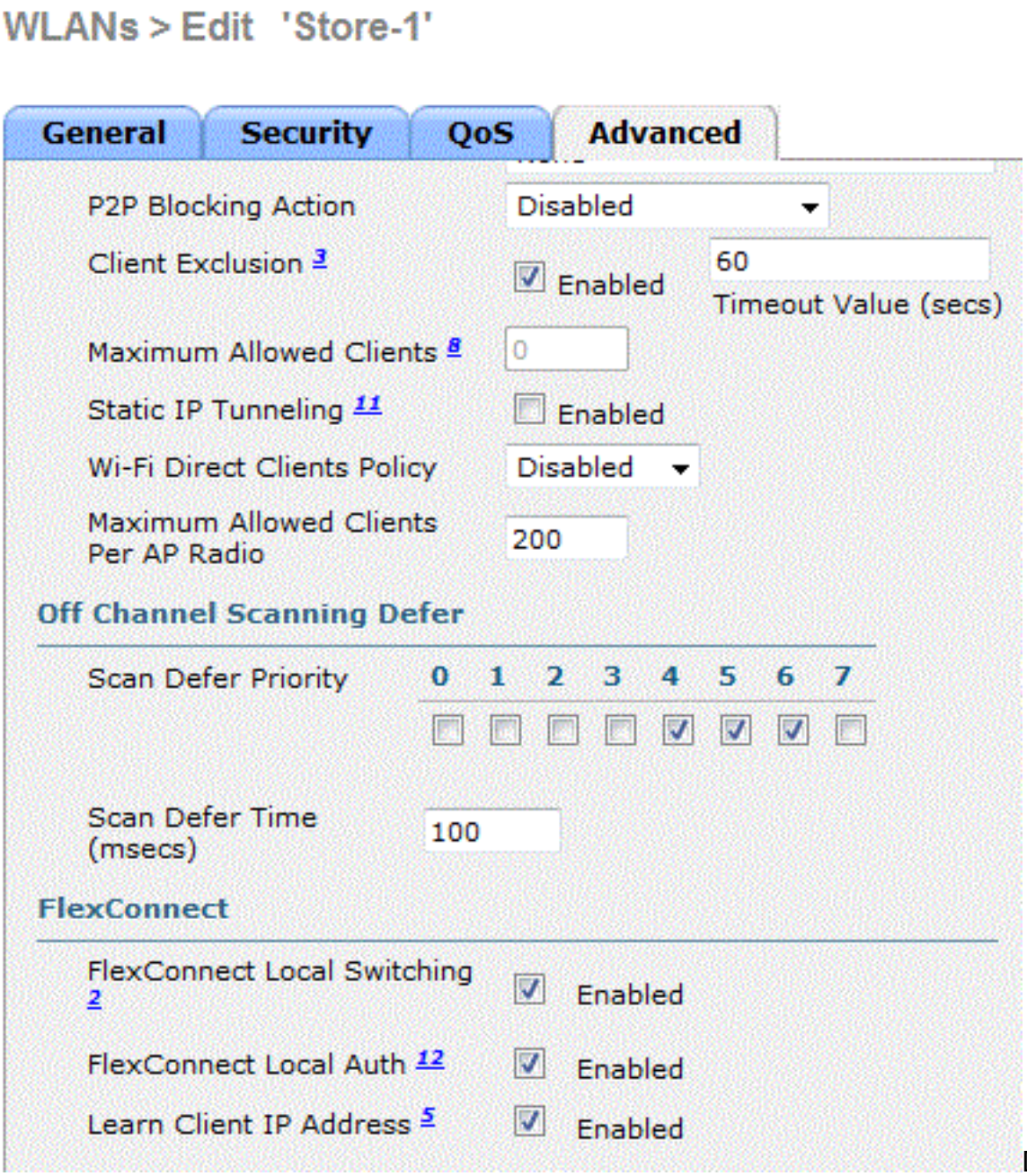


13. Klicken Sie unter Lokale Authentifizierung auf **Lokale Benutzer**.
14. Legen Sie die Felder Benutzername, Kennwort und Kennwort bestätigen fest, und klicken Sie dann auf **Hinzufügen**, um einen Benutzereintrag auf dem lokalen EAP-Server im AP zu erstellen.
15. Wiederholen Sie Schritt 13, bis Ihre lokale Benutzernamenliste erschöpft ist. Sie können nicht mehr als 100 Benutzer konfigurieren oder hinzufügen.
16. Klicken Sie nach Abschluss von Schritt 14 auf **Apply**, und die Anzahl der Benutzer wird überprüft.

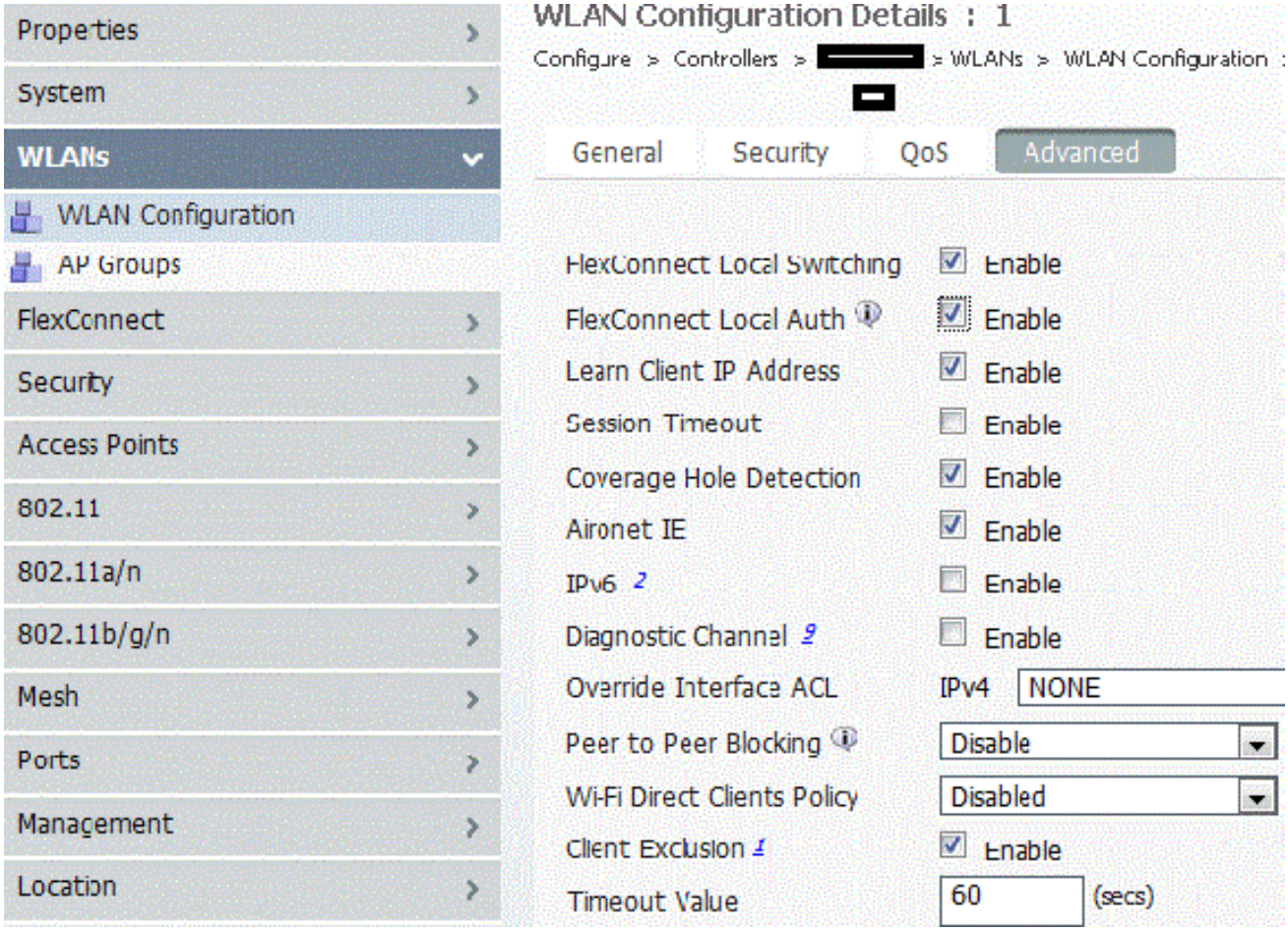


17. Klicken Sie im oberen Teilfenster auf **WLANs**.
18. Klicken Sie auf **WLAN-ID 17**. Diese wurde während der Erstellung der AP-Gruppe erstellt. Siehe Abbildung 8.

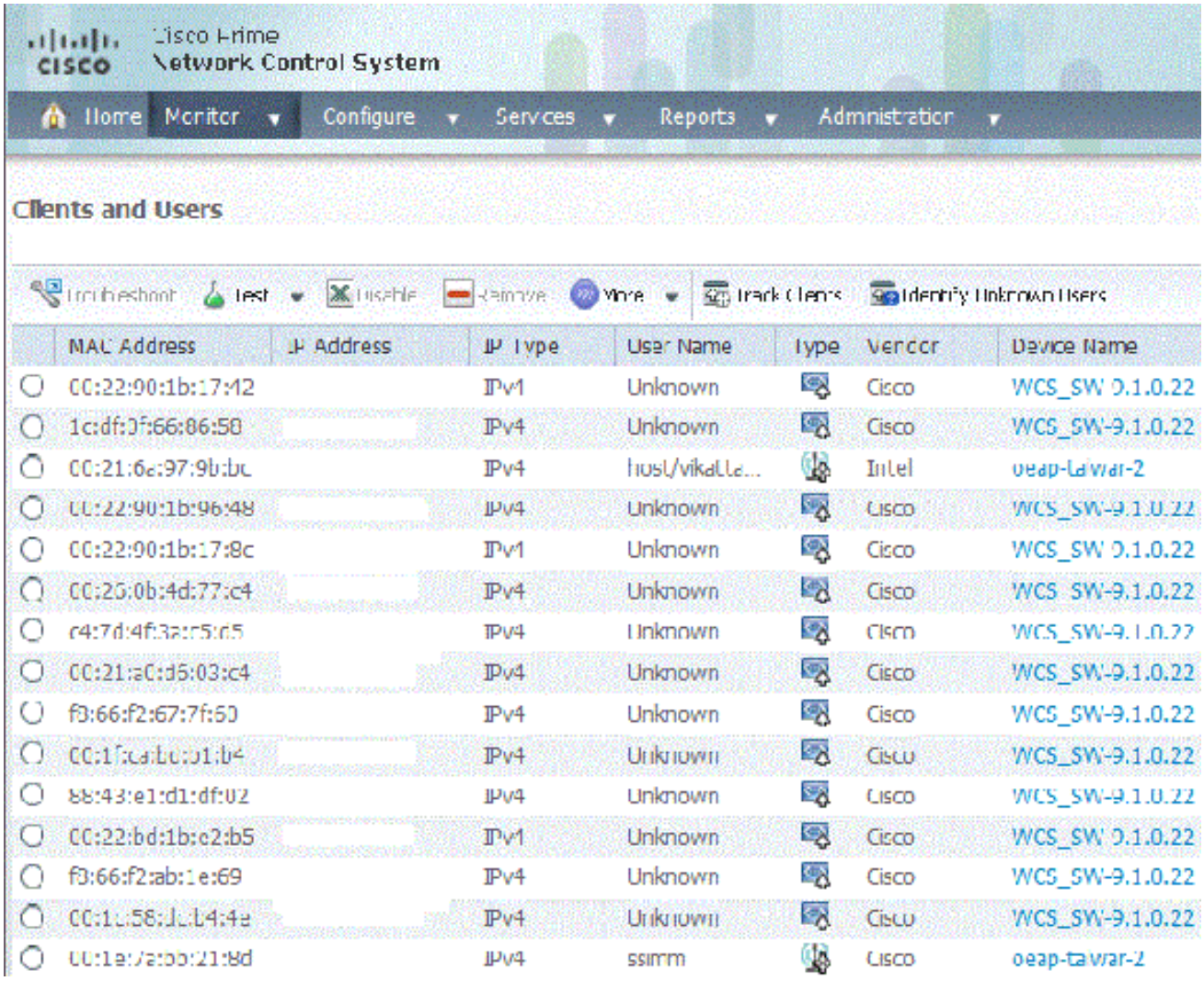
19. Klicken Sie unter WLAN > Edit for WLAN ID 17 (Für WLAN-ID bearbeiten) auf **Advanced (Erweitert)**.
20. Aktivieren Sie das Kontrollkästchen **FlexConnect Local Auth**, um die lokale Authentifizierung im Connected Mode zu aktivieren.**Hinweis:** Lokale Authentifizierung wird nur für FlexConnect mit lokalem Switching unterstützt.**Hinweis:** Erstellen Sie immer die FlexConnect-Gruppe, bevor Sie die lokale Authentifizierung unter WLAN aktivieren.

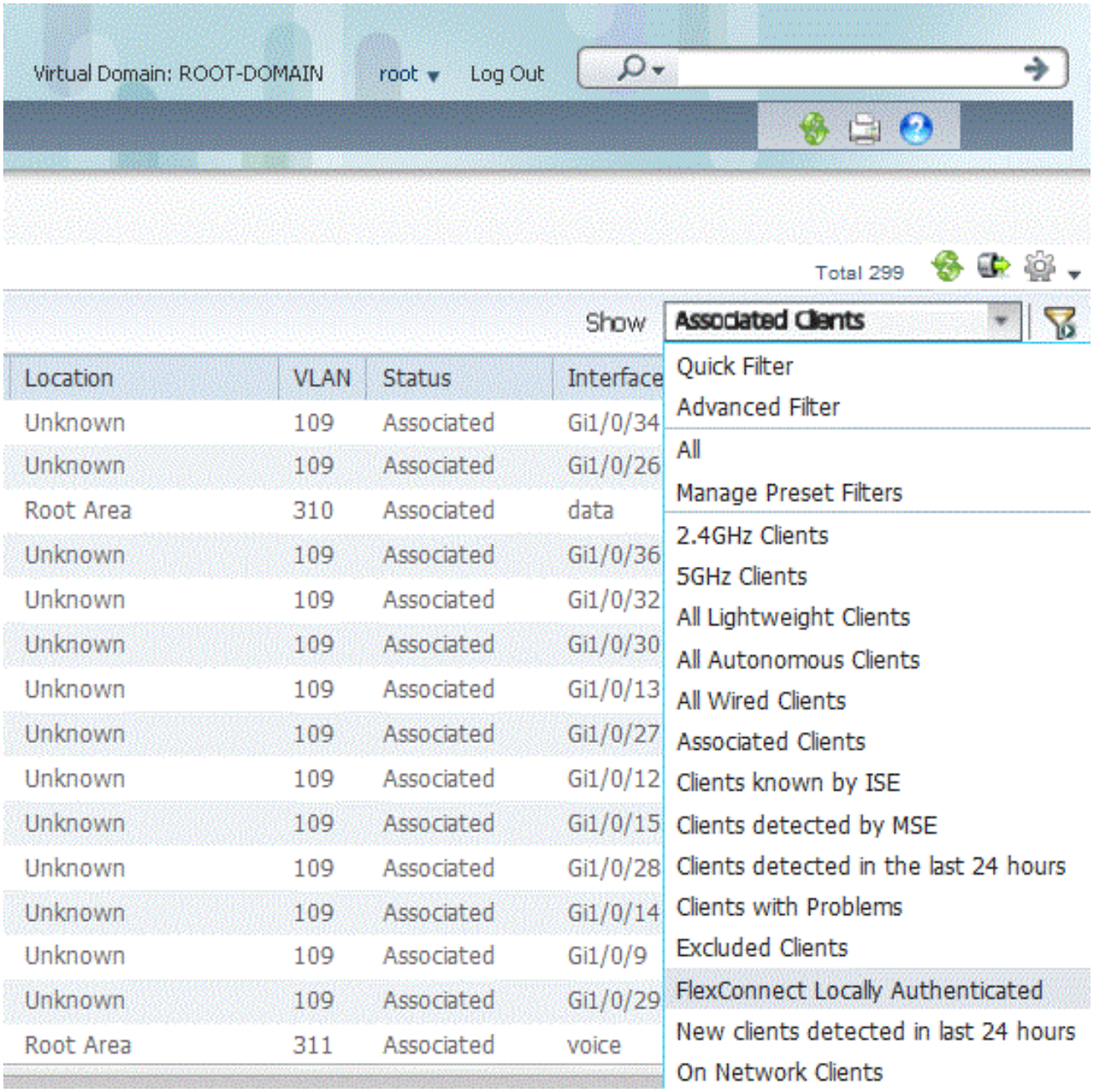


Das NCS stellt außerdem das Kontrollkästchen "FlexConnect Local Auth" bereit, um die lokale Authentifizierung im Connected Mode zu aktivieren, wie hier gezeigt:



Das NCS bietet auch eine Möglichkeit zum Filtern und Überwachen von lokal authentifizierten FlexConnect-Clients, wie hier gezeigt:


Cisco Prime
Network Control System
Home
Monitor
Configure
Services
Reports
Administration
Clients and Users
Troubleshoot
Test
Disable
Remove
More
Track Clients
Identify Unknown Users
MAC Address
IP Address
IP Type
User Name
Type
Vendor
Device Name
00:22:90:1b:17:12 IPv4 Unknown Cisco WCS_SW 9.1.0.22
1c:df:0f:66:86:58 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:21:6a:97:9b:bc IPv4 host/vikalla... Intel deap-tavar-2
00:22:90:1b:96:48 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:22:90:1b:17:8c IPv4 Unknown Cisco WCS_SW 9.1.0.22
00:25:0b:4d:77:c4 IPv4 Unknown Cisco WCS_SW-9.1.0.22
c4:7d:4f:3a:c5:c5 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:21:a0:d5:03:c4 IPv4 Unknown Cisco WCS_SW-9.1.0.22
f0:66:f2:67:7f:50 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:1f:ca:bc:b1:b4 IPv4 Unknown Cisco WCS_SW-9.1.0.22
88:43:e1:d1:df:02 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:22:bd:1b:e2:b5 IPv4 Unknown Cisco WCS_SW 9.1.0.22
f0:66:f2:ab:1e:69 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:1c:58:bc:b4:4a IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:1e:7a:bb:21:8d IPv4 ssimm Cisco deap-tavar-2



Verifizierung mit CLI

Der Client-Authentifizierungsstatus und der Switching-Modus können mithilfe dieser CLI im WLC schnell überprüft werden:

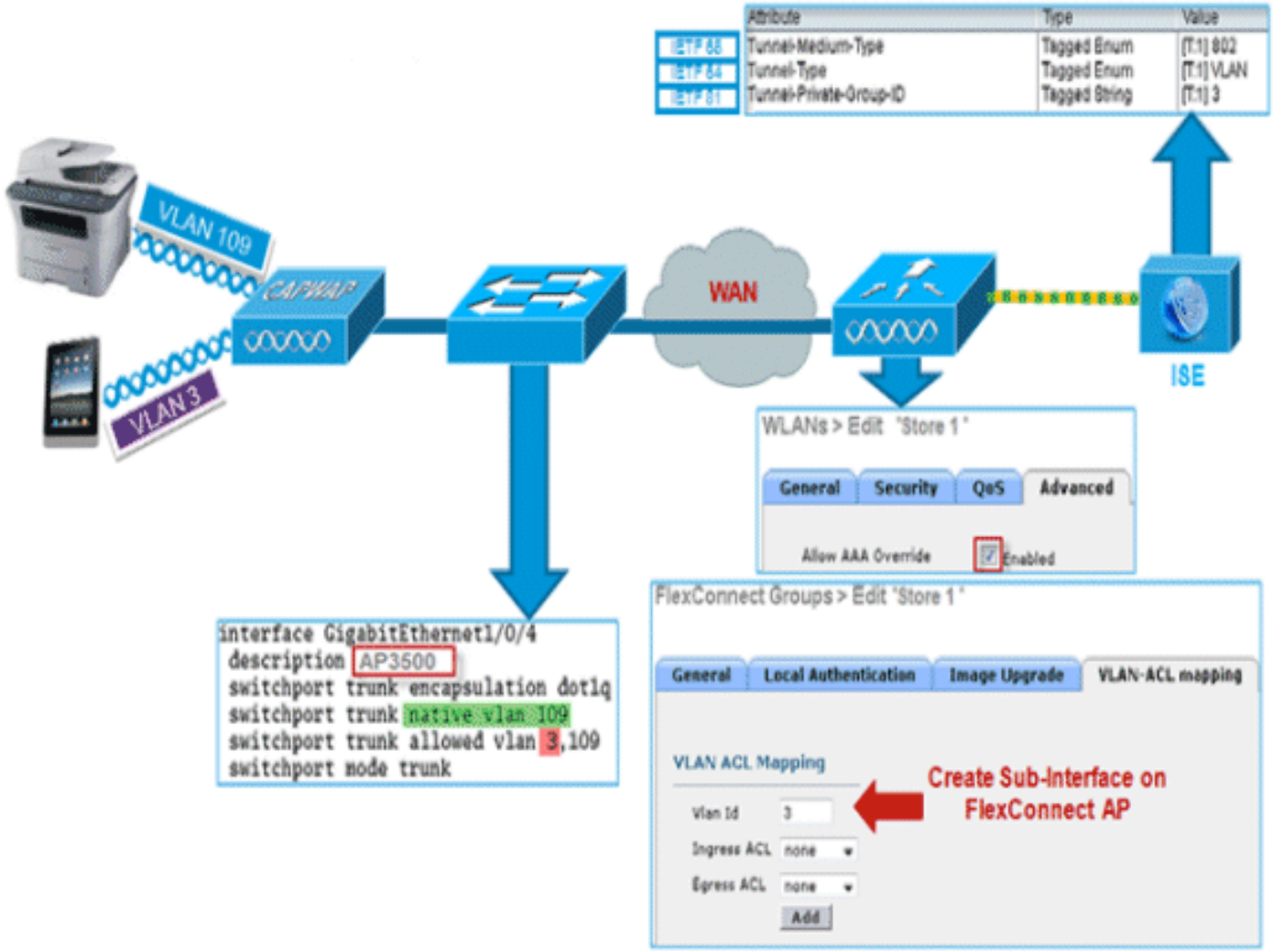
```
(Cisco Controller) >show client detail 00:24:d7:2b:7c:0c
Client MAC Address.............................. 00:24:d7:2b:7c:0c
Client Username ................................ N/A
AP MAC Address.................................. d0:57:4c:08:e6:70
Client State.................................... Associated
H-REAP Data Switching........................... Local
H-REAP Authentication.......................... Local
```

VLAN-Außerkraftsetzung bei FlexConnect

In der aktuellen FlexConnect-Architektur wird WLAN einem VLAN strikt zugeordnet, sodass der Client, der einem bestimmten WLAN auf FlexConnect AP zugeordnet ist, sich an ein VLAN halten

muss, das ihm zugeordnet ist. Diese Methode hat Einschränkungen, da Clients verschiedene SSIDs verknüpfen müssen, um verschiedene VLAN-basierte Richtlinien zu erben.

Ab Version 7.2 wird die AAA-Überschreibungen von VLANs in einzelnen WLANs unterstützt, die für lokales Switching konfiguriert sind. Um eine dynamische VLAN-Zuweisung zu ermöglichen, hätte der Access Point die Schnittstellen für das VLAN vorab erstellt, die auf einer Konfiguration basieren, bei der die vorhandene WLAN-VLAN-Zuordnung für einen einzelnen FlexConnect-Access-Point verwendet wird, oder die ACL-VLAN-Zuordnung in einer FlexConnect-Gruppe verwendet wird. Der WLC wird zum Vorerstellen der Subschnittstellen am Access Point verwendet.



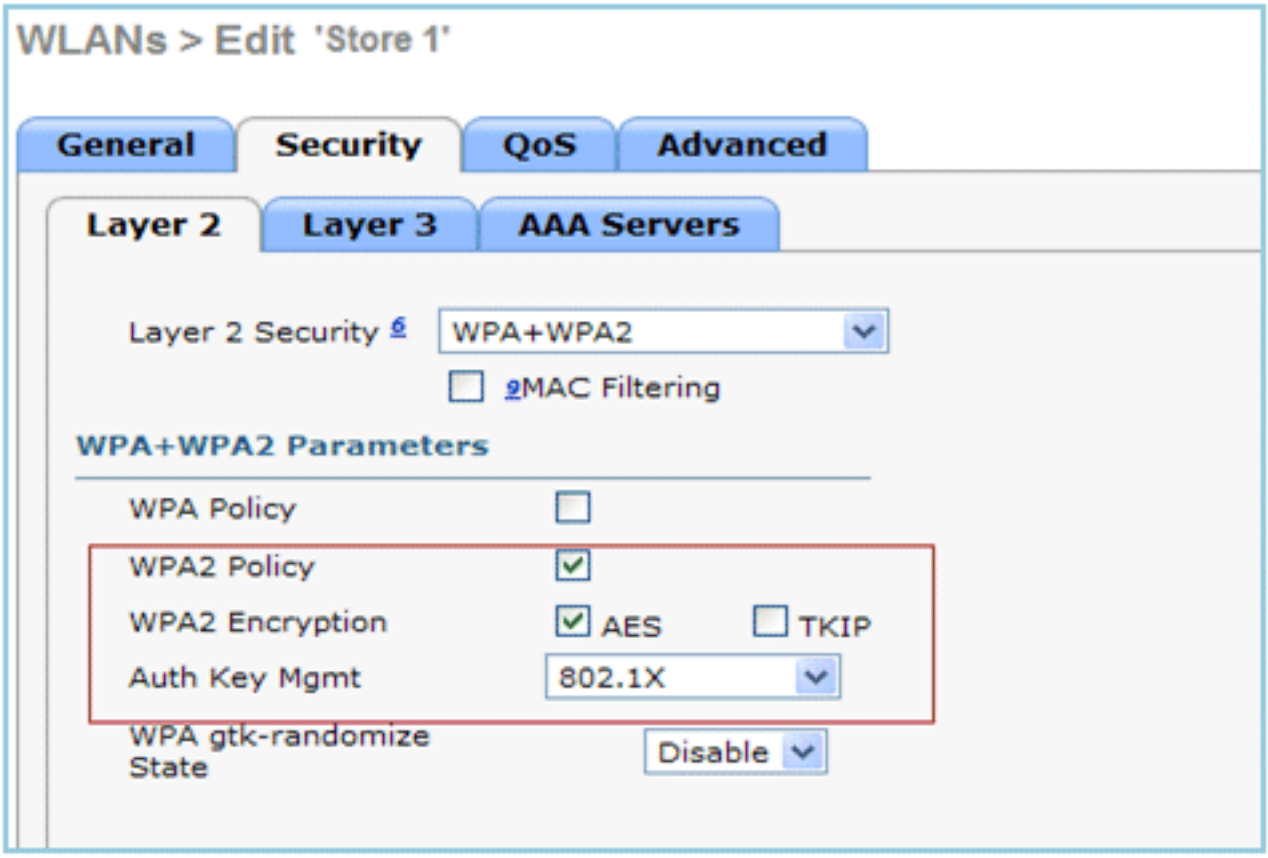
Zusammenfassung

- AAA-VLAN-Override wird von Version 7.2 für WLANs unterstützt, die für lokales Switching im zentralen und lokalen Authentifizierungsmodus konfiguriert sind.
- AAA-override sollte in WLAN aktiviert werden, das für lokales Switching konfiguriert ist.
- Der FlexConnect-Zugangspunkt muss über ein VLAN verfügen, das aus dem WLC vorerstellt wurde, um eine dynamische VLAN-Zuweisung zu ermöglichen.
- Wenn auf dem AP-Client keine VLANs vorhanden sind, die durch AAA-Überschreibungen zurückgegeben werden, wird eine IP-Adresse von der Standard-VLAN-Schnittstelle des Access Points abgerufen.

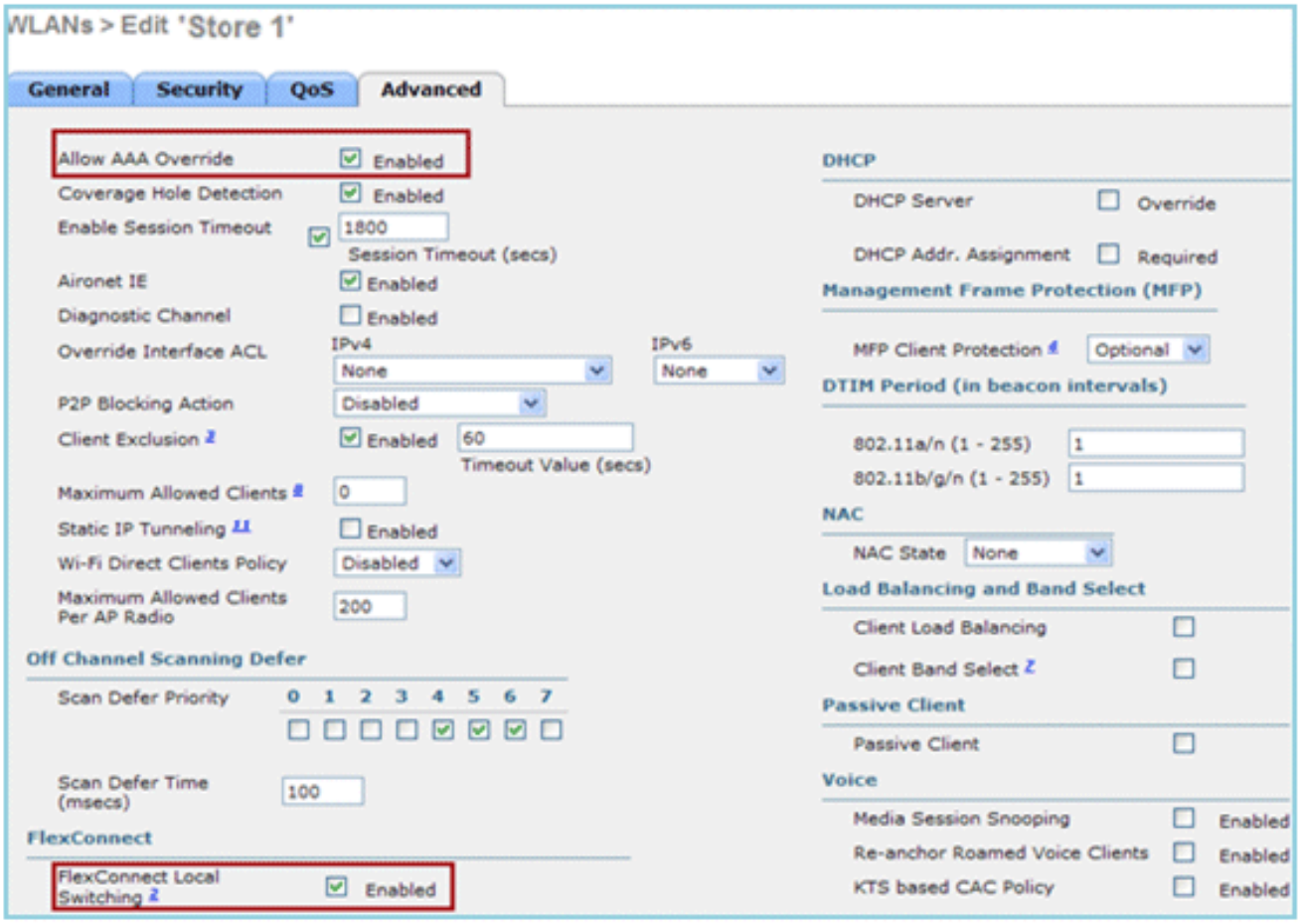
Vorgehensweise

Führen Sie diese Schritte aus:

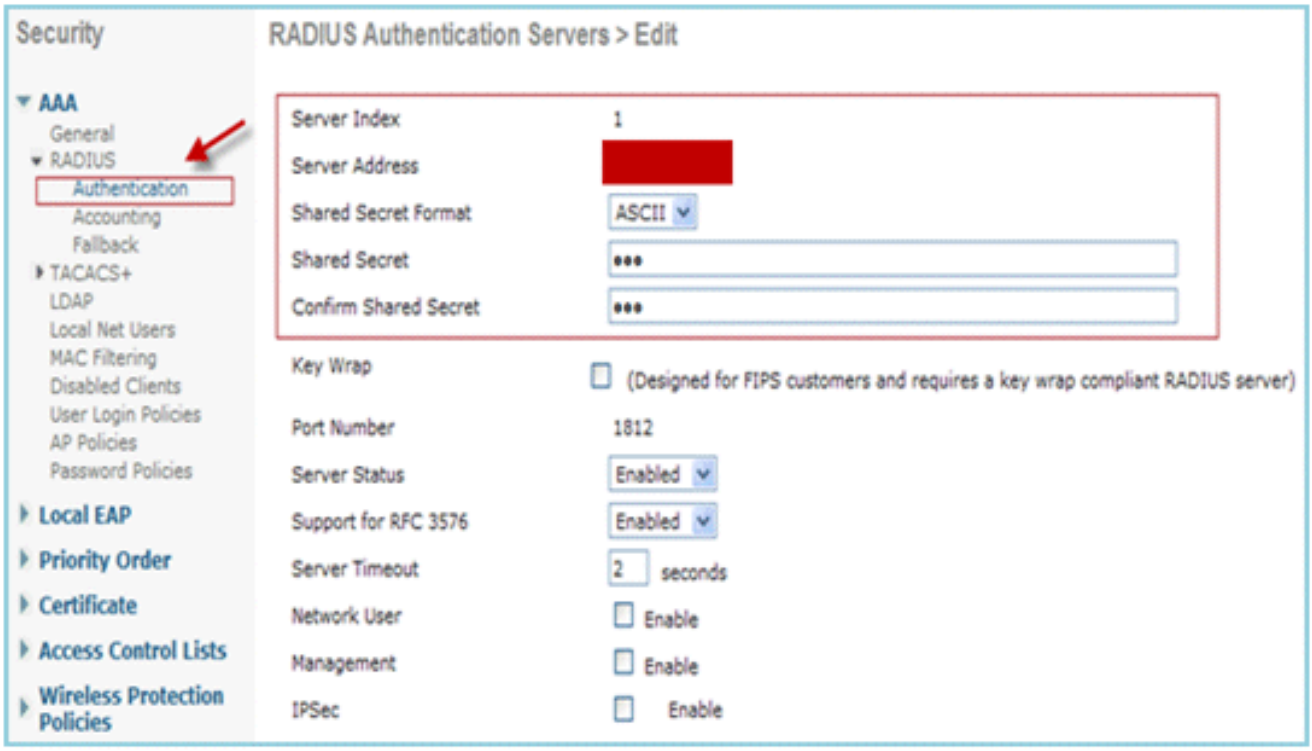
1. Erstellen Sie ein WLAN für die 802.1x-Authentifizierung.



2. Aktivieren Sie die Option AAA Override-Unterstützung für lokales Switching-WLAN im WLC. Navigieren Sie zur Registerkarte **WLAN GUI > WLAN > WLAN ID > Advance**.

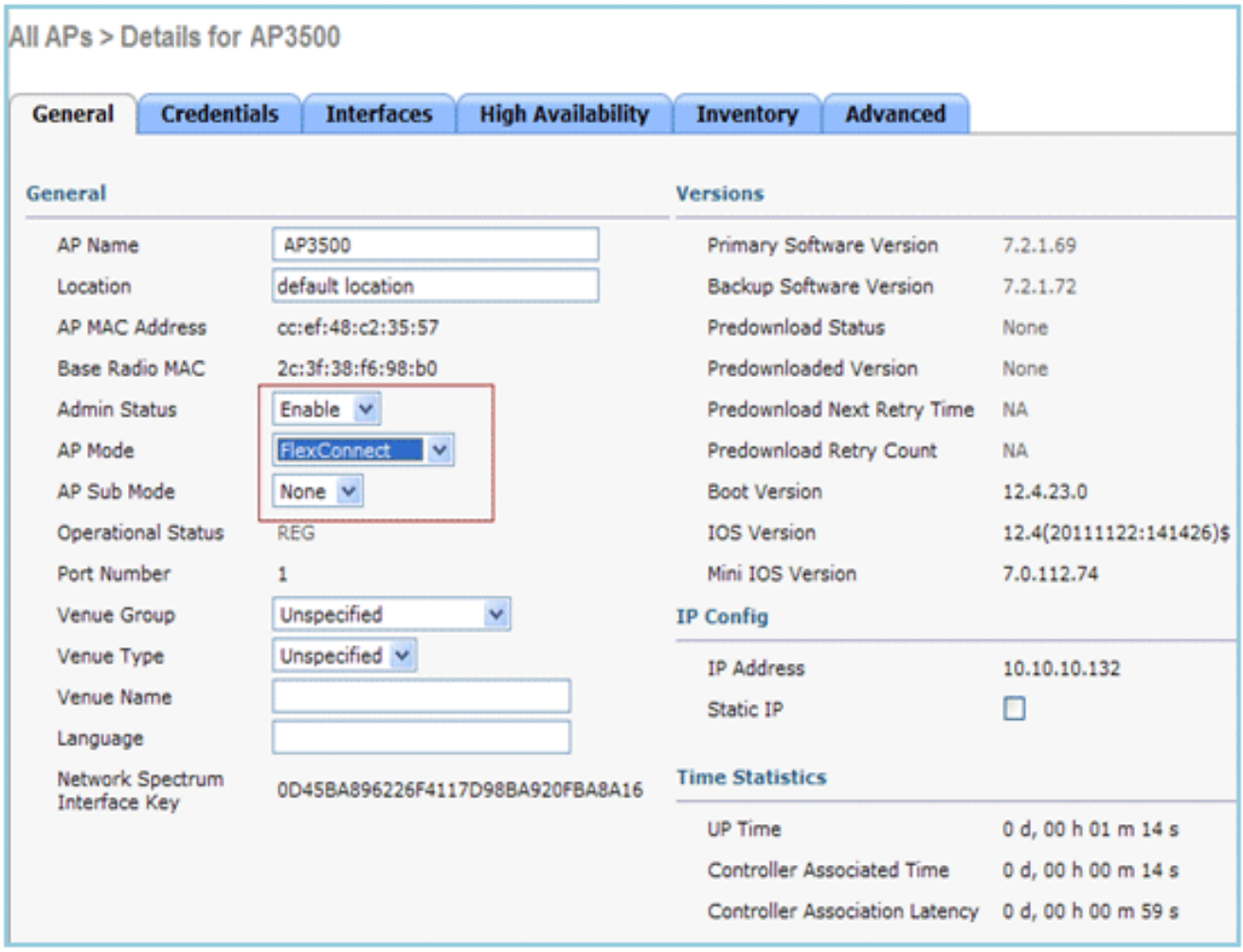


3. Fügen Sie die AAA-Serverdetails des Controllers für die 802.1x-Authentifizierung hinzu. Um den AAA-Server hinzuzufügen, navigieren Sie zu **WLC GUI > Security > AAA > Radius > Authentication > New.**

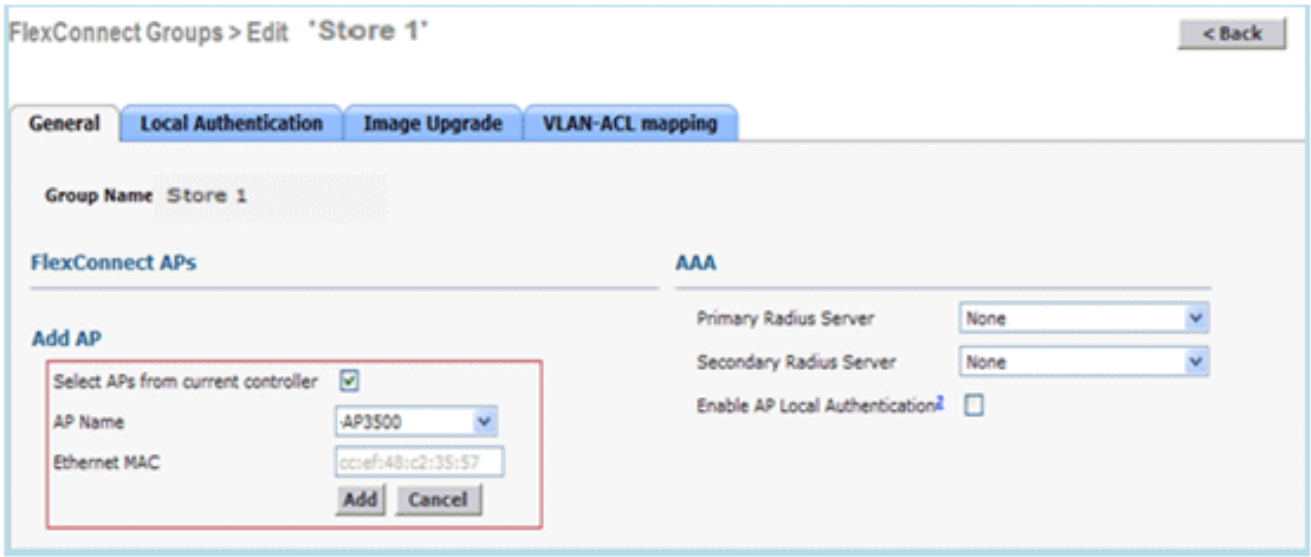


4. Der Access Point befindet sich standardmäßig im lokalen Modus, sodass der Modus in den FlexConnect-Modus umgeleitet wird. APs im lokalen Modus können in den FlexConnect-Modus konvertiert werden, indem Sie **Wireless > All APs (Alle APs)** aufrufen und auf den individuellen Access Point

klicken.



5. Fügen Sie die FlexConnect-APs der FlexConnect-Gruppe hinzu.Navigieren Sie unter **WLC GUI > Wireless > FlexConnect Groups > Wählen Sie FlexConnect Group > Registerkarte General (Allgemein) > Add AP aus.**

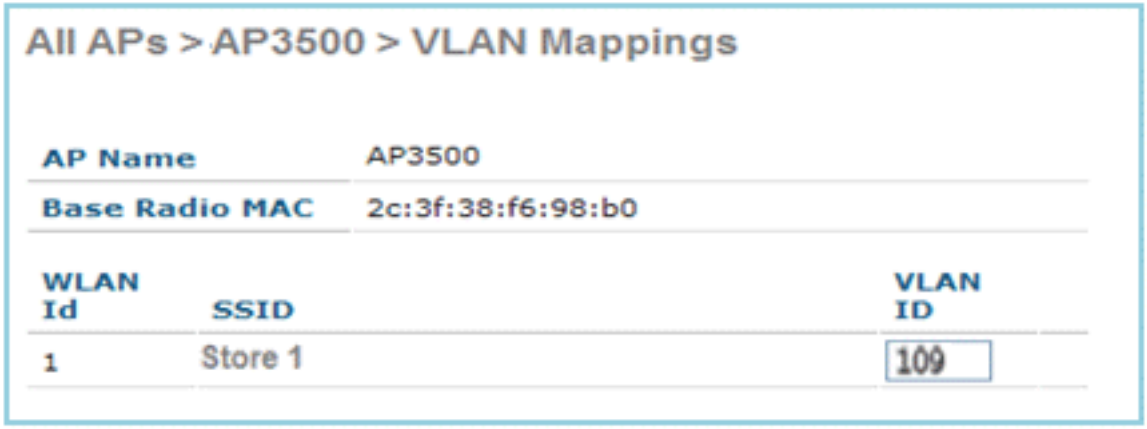


6. Der FlexConnect-AP sollte über einen Trunk-Port verbunden werden, und dem Trunk-Port sollte ein VLAN mit WLAN-Zuordnung und ein überschriebenes AAA-VLAN zugelassen

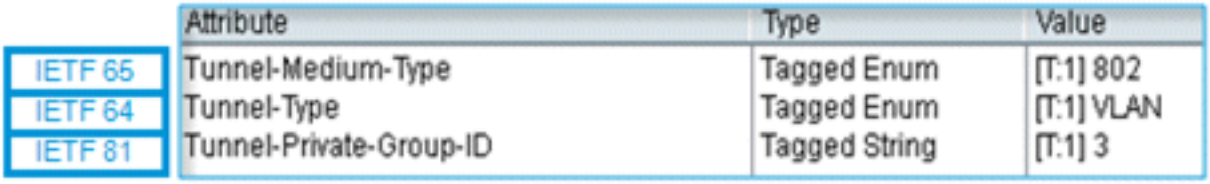
```
interface GigabitEthernet1/0/4
 description AP3500
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 109
 switchport trunk allowed vlan 3,109
 switchport mode trunk
```

werden. **Hinweis:** In dieser Konfiguration wird VLAN 109 für die WLAN-VLAN-Zuordnung und VLAN 3 für die AAA-Überschreibung verwendet.

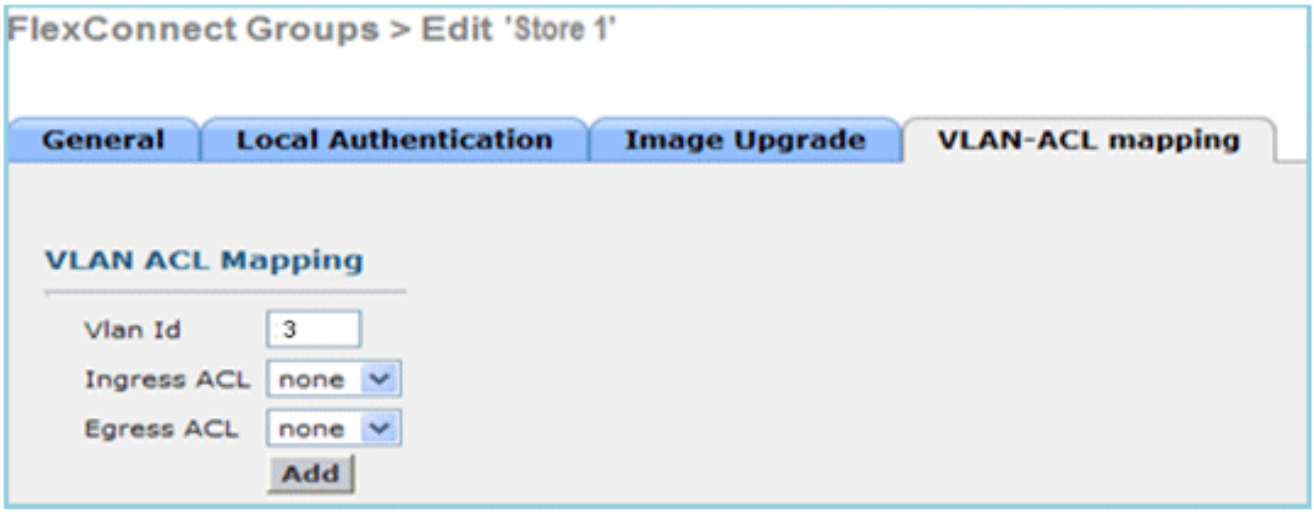
7. Konfigurieren der WLAN-VLAN-Zuordnung für den FlexConnect AP Basierend auf dieser Konfiguration verfügt der Access Point über die Schnittstellen für das VLAN. Wenn der WAP die VLAN-Konfiguration empfängt, werden entsprechende dot11- und Ethernet-Subschnittstellen erstellt und einer Bridge-Gruppe hinzugefügt. Verknüpfen Sie einen Client mit diesem WLAN, und wenn der Client eine Zuordnung vornimmt, wird sein VLAN (Standard, basierend auf der WLAN-VLAN-Zuordnung) zugewiesen.Navigieren Sie zu **WLAN GUI > Wireless > All APs >** klicken Sie auf die Registerkarte AP **> FlexConnect**, und klicken Sie dann auf **VLAN Mapping.**



8. Erstellen Sie einen Benutzer im AAA-Server, und konfigurieren Sie den Benutzer so, dass die VLAN-ID im IETF Radius-Attribut zurückgegeben wird.



9. Um eine dynamische VLAN-Zuweisung zu ermöglichen, verfügt der Access Point über die Schnittstellen für das dynamische VLAN, das anhand der Konfiguration mithilfe der vorhandenen WLAN-VLAN-Zuordnung für den einzelnen FlexConnect-AP oder mithilfe der ACL-VLAN-Zuordnung in der FlexConnect-Gruppe vorerstellt wurde.Um das AAA-VLAN auf dem FlexConnect AP zu konfigurieren, navigieren Sie zur **WLC-GUI > Wireless > FlexConnect Group >** klicken Sie auf die jeweilige FlexConnect-Gruppe **> VLAN-ACL-Zuordnung**, und geben Sie VLAN in das **VLAN-ID-Feld ein.**



10. Verknüpfen Sie einen Client in diesem WLAN, und authentifizieren Sie ihn mithilfe des im AAA-Server konfigurierten Benutzernamens, um das AAA-VLAN zurückzugeben.
11. Der Client sollte eine IP-Adresse vom dynamischen VLAN erhalten, das über den AAA-Server zurückgegeben wird.
12. Klicken Sie zur Überprüfung auf die **WLC-GUI > Monitor > Client >** klicken Sie auf die jeweilige Client-MAC-Adresse, um die Client-Details zu überprüfen.

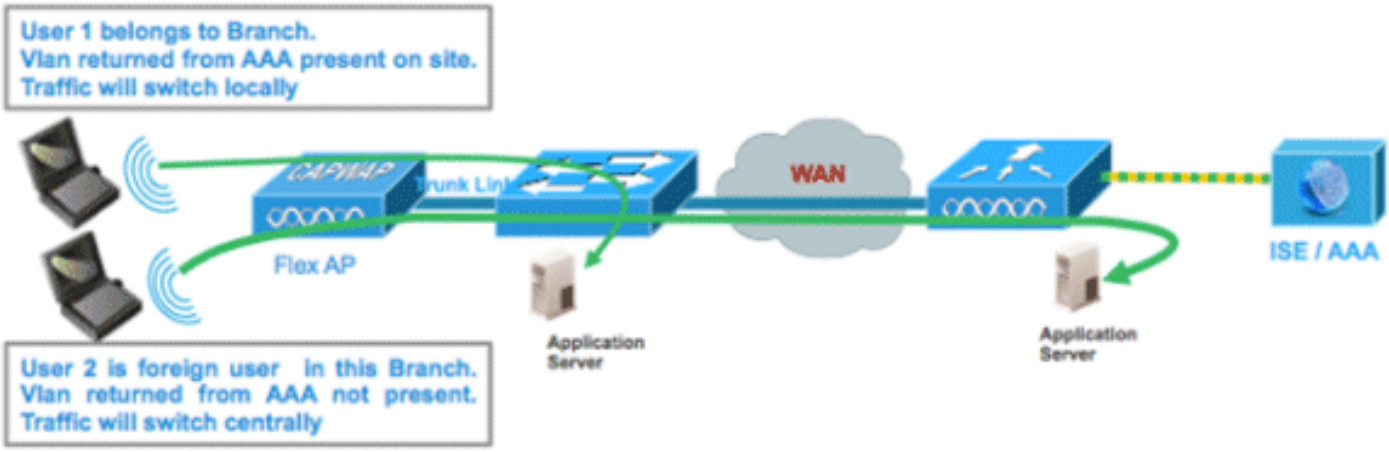
Einschränkungen

- **Cisco** Attribute für die **Luftqualität** werden nicht unterstützt, und die IETF-Attribut-VLAN-ID wird nur unterstützt.
- Es können maximal 16 VLANs pro AP-Konfiguration konfiguriert werden, entweder über die WLAN-VLAN-Zuordnung für einen einzelnen FlexConnect-AP oder mithilfe der ACL-VLAN-Zuordnung in der FlexConnect-Gruppe.

FlexConnect VLAN-basiertes zentrales Switching

In der Controller-Software Version 7.2 werden WLAN-Clients durch AAA-Überschreibung (dynamische VLAN-Zuweisung) für lokal geschaltete WLANs in das vom AAA-Server bereitgestellte VLAN verschoben. Wenn das vom AAA-Server bereitgestellte VLAN am AP nicht vorhanden ist, wird der Client einem WLAN zugeordneten VLAN für diesen WAP zugewiesen, und der Datenverkehr wird lokal in diesem VLAN geschaltet. Darüber hinaus kann der Datenverkehr für ein bestimmtes WLAN von FlexConnect-APs vor Version 7.3 abhängig von der WLAN-Konfiguration zentral oder lokal geschaltet werden.

Ab Version 7.3 kann der Datenverkehr von FlexConnect-APs abhängig von einem VLAN auf einem FlexConnect-AP zentral oder lokal geschaltet werden.



Zusammenfassung

Datenverkehrsfluss in WLANs, die für lokales Switching konfiguriert sind, wenn sich Flex-APs im Connected Mode befinden:

- Wenn das VLAN als eines der AAA-Attribute zurückgegeben wird und dieses VLAN nicht in der Flex AP-Datenbank vorhanden ist, wird der Datenverkehr zentral umgeleitet, und dem Client wird dieses VLAN/die Schnittstelle zugewiesen, das vom AAA-Server zurückgegeben wird, sofern das VLAN im WLC vorhanden ist.
- Wenn das VLAN als eines der AAA-Attribute zurückgegeben wird und dieses VLAN in der Flex AP-Datenbank nicht vorhanden ist, wird der Datenverkehr zentral umgeleitet. Wenn dieses VLAN auch nicht im WLC vorhanden ist, wird dem Client ein VLAN/Interface zugewiesen, das einem WLAN im WLC zugeordnet ist.
- Wenn das VLAN als eines der AAA-Attribute zurückgegeben wird und dieses VLAN in der FlexConnect AP-Datenbank vorhanden ist, wechselt der Datenverkehr lokal.
- Wenn das VLAN nicht vom AAA-Server zurückgegeben wird, wird dem Client ein WLAN-zugeordnetes VLAN für diesen FlexConnect-AP zugewiesen, und der Datenverkehr wechselt lokal.

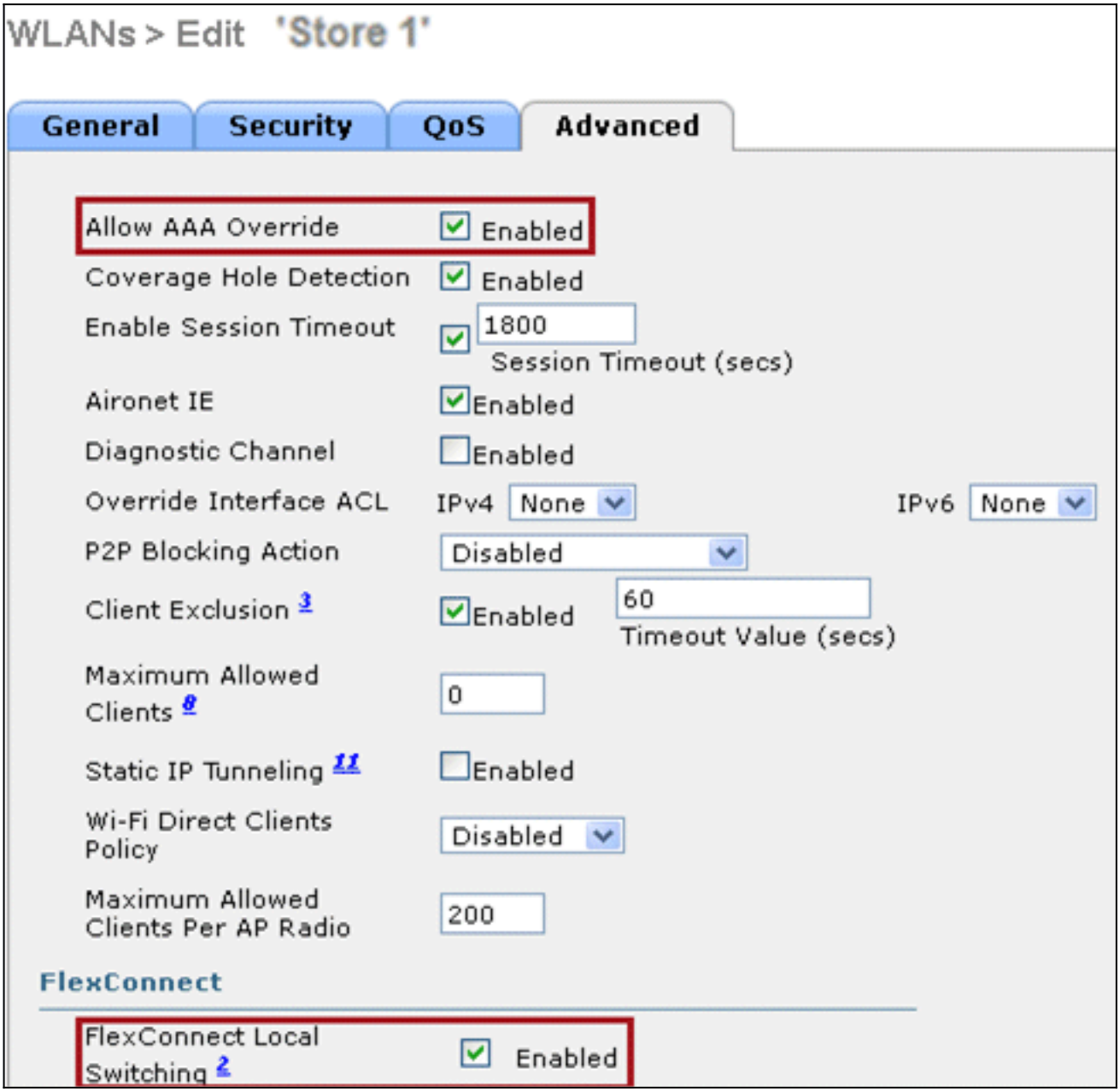
Datenverkehrsfluss in WLANs, die für lokales Switching konfiguriert sind, wenn sich Flex-APs im Standalone-Modus befinden:

- Wenn das von einem AAA-Server zurückgegebene VLAN nicht in der Flex AP-Datenbank vorhanden ist, wird dem Client das Standard-VLAN zugewiesen (d. h. ein WLAN-zugeordnetes VLAN auf Flex AP). Wenn der Access Point wieder eine Verbindung herstellt, wird dieser Client deauthentifiziert und der Datenverkehr zentral umgeleitet.
- Wenn das von einem AAA-Server zurückgegebene VLAN in der Flex AP-Datenbank vorhanden ist, wird der Client in ein zurückgegebenes VLAN gesetzt, und der Datenverkehr wechselt lokal.
- Wenn das VLAN nicht von einem AAA-Server zurückgegeben wird, wird dem Client ein WLAN-zugeordnetes VLAN für diesen FlexConnect-AP zugewiesen, und der Datenverkehr wechselt lokal.

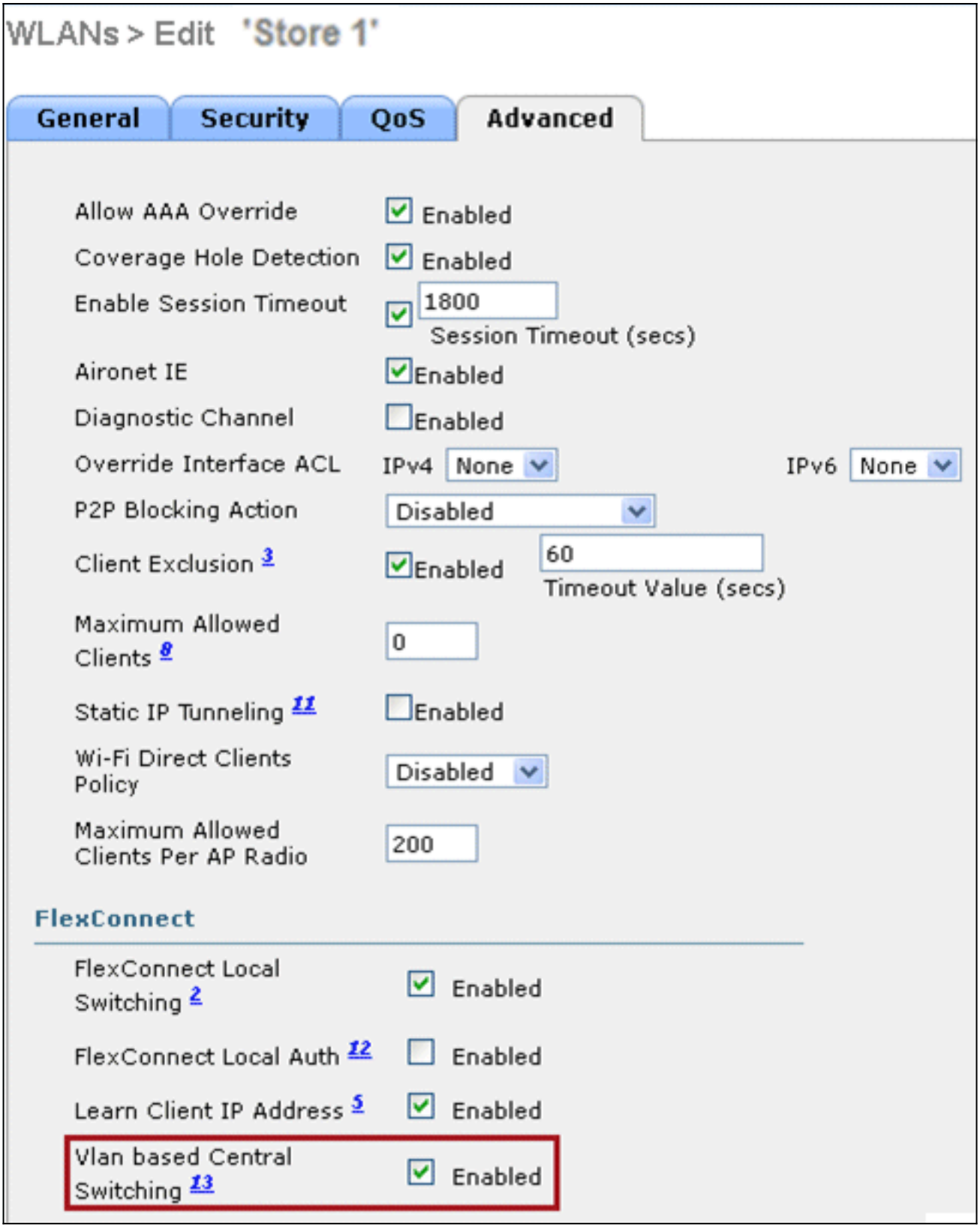
Vorgehensweise

Führen Sie diese Schritte aus:

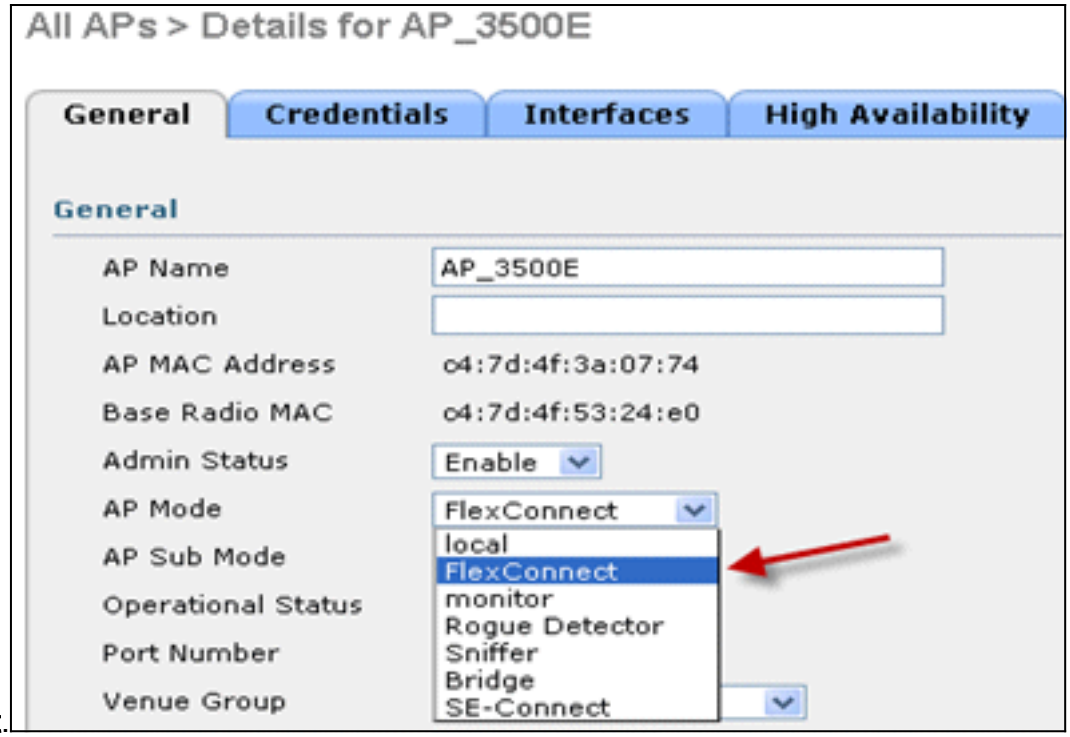
1. Konfigurieren Sie ein WLAN für das lokale Switching, und aktivieren Sie AAA override.



2. Aktivieren Sie **VLAN-basiertes Central Switching** im neu erstellten WLAN.

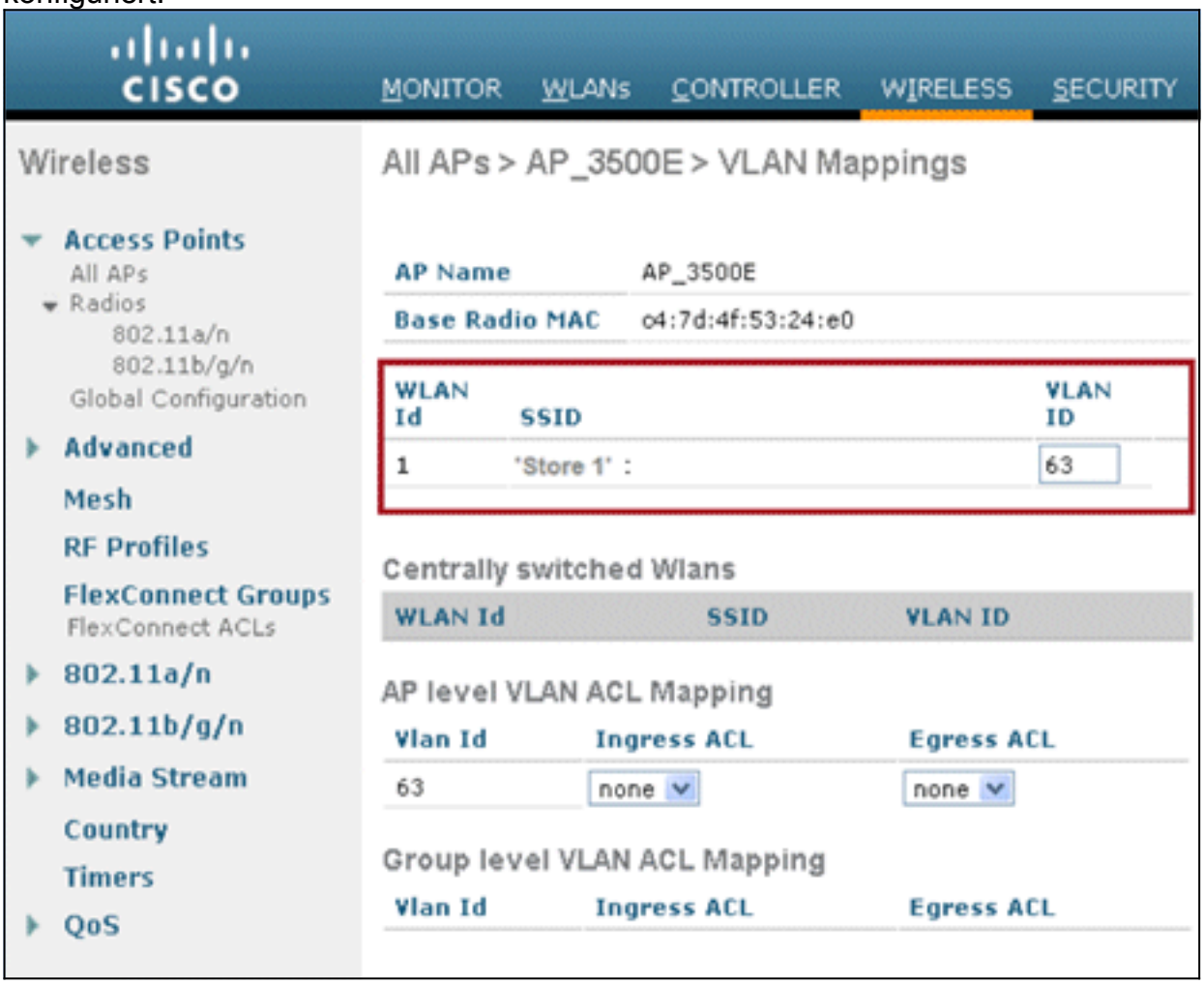


3. Legen Sie den AP-Modus auf **FlexConnect**



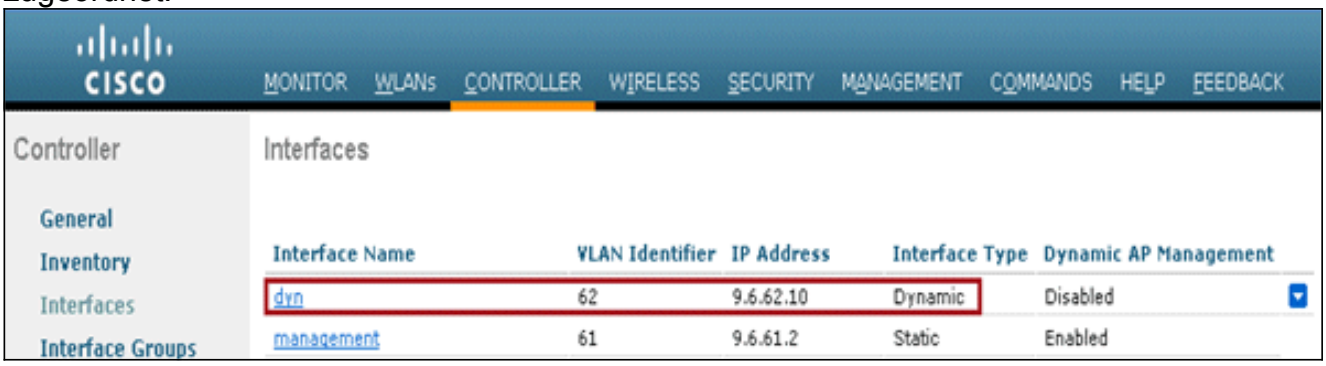
fest.

4. Stellen Sie sicher, dass der FlexConnect AP über eine Subschnittstelle in seiner Datenbank verfügt, entweder über die WLAN-VLAN-Zuordnung eines bestimmten Flex AP oder über die Konfiguration eines VLANs von einer Flex-Gruppe. In diesem Beispiel wird VLAN 63 in der WLAN-VLAN-Zuordnung auf Flex AP konfiguriert.

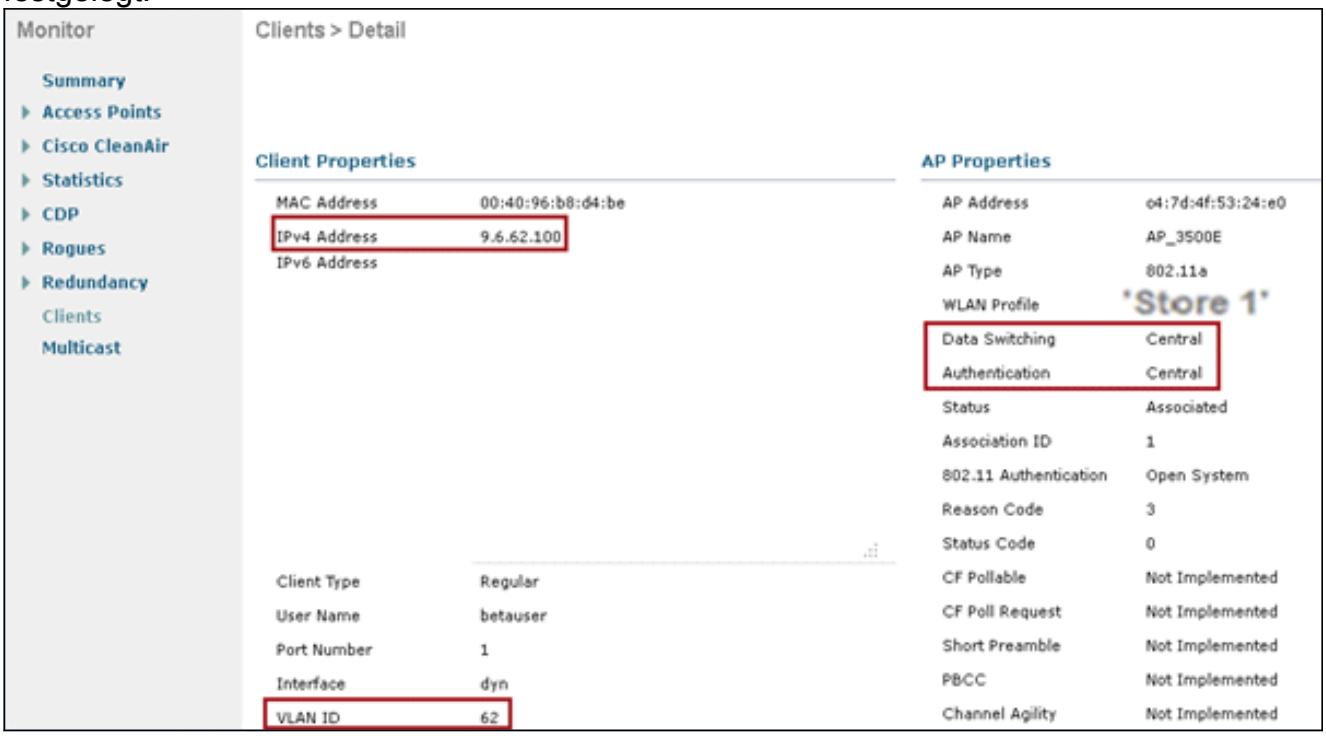


5. In diesem Beispiel wird VLAN 62 auf dem WLC als eine der dynamischen Schnittstellen konfiguriert und nicht dem WLAN auf dem WLC zugeordnet. Das WLAN auf dem WLC ist

dem Management-VLAN (d. h. VLAN 61) zugeordnet.

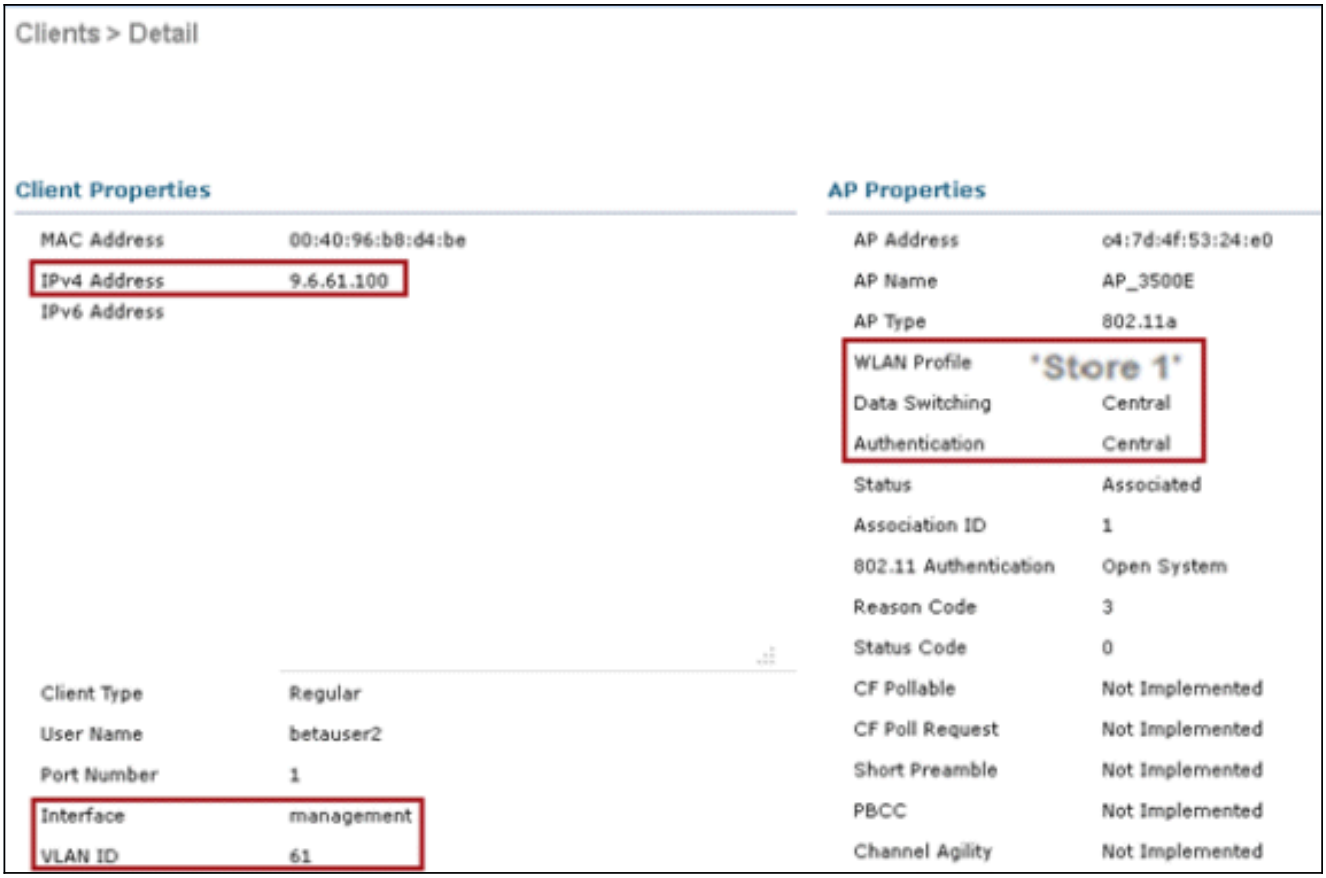


6. Verknüpfen Sie einen Client mit dem in Schritt 1 konfigurierten WLAN auf diesem Flex AP, und geben Sie VLAN 62 vom AAA-Server zurück. VLAN 62 ist auf diesem Flex AP nicht vorhanden, ist aber auf dem WLC als dynamische Schnittstelle vorhanden, sodass der Datenverkehr zentral umschaltet und dem Client VLAN 62 auf dem WLC zugewiesen wird. In der hier erfassten Ausgabe wurde dem Client das VLAN 62 zugewiesen, und Data Switching and Authentication (Daten-Switching und -Authentifizierung) wurde auf **Central** festgelegt.



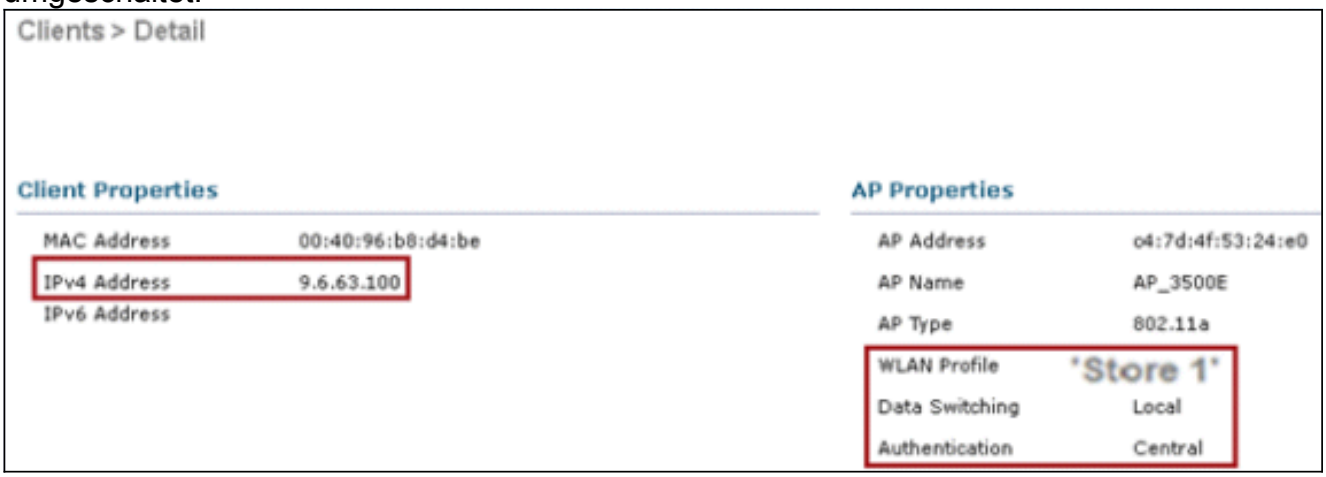
Hinweis: Beachten Sie, dass WLAN zwar für lokales Switching konfiguriert ist, das Data Switching-Feld für diesen Client jedoch Central ist, da ein VLAN vorhanden ist (d. h. VLAN 62, das vom AAA-Server zurückgegeben wird, nicht in der AP-Datenbank vorhanden ist).

7. Wenn ein anderer Benutzer demselben WAP auf diesem erstellten WLAN zugeordnet wird und ein VLAN vom AAA-Server zurückgegeben wird, der nicht im WLAN sowie im WLC vorhanden ist, wird der Datenverkehr zentral umgeschaltet und dem Client die WLAN-zugeordnete Schnittstelle im WLC zugewiesen (in diesem Beispiel VLAN 61), da das WLAN der Management-Schnittstelle zugeordnet ist, die für VLAN 61 konfiguriert ist.



Hinweis: Beachten Sie, dass das Feld "Data Switching" für diesen Client - obwohl WLAN für lokales Switching konfiguriert ist - auf der Grundlage eines VLANs "Central" (Zentrale Datenvermittlung) lautet. Das heißt, VLAN 61, das vom AAA-Server zurückgegeben wird, ist nicht in der AP-Datenbank vorhanden, aber auch nicht in der WLC-Datenbank vorhanden. Als Ergebnis wird dem Client ein Standard-VLAN/Interface zugewiesen, das dem WLAN zugeordnet ist. In diesem Beispiel ist das WLAN einer Verwaltungsschnittstelle (d. h. VLAN 61) zugeordnet, sodass der Client eine IP-Adresse von VLAN 61 erhalten hat.

8. Wenn ein anderer Benutzer diesem WLAN zugeordnet wird und das VLAN 63 vom AAA-Server zurückgegeben wird (der auf diesem Flex AP vorhanden ist), wird dem Client das VLAN 63 zugewiesen, und der Datenverkehr wird lokal umgeschaltet.



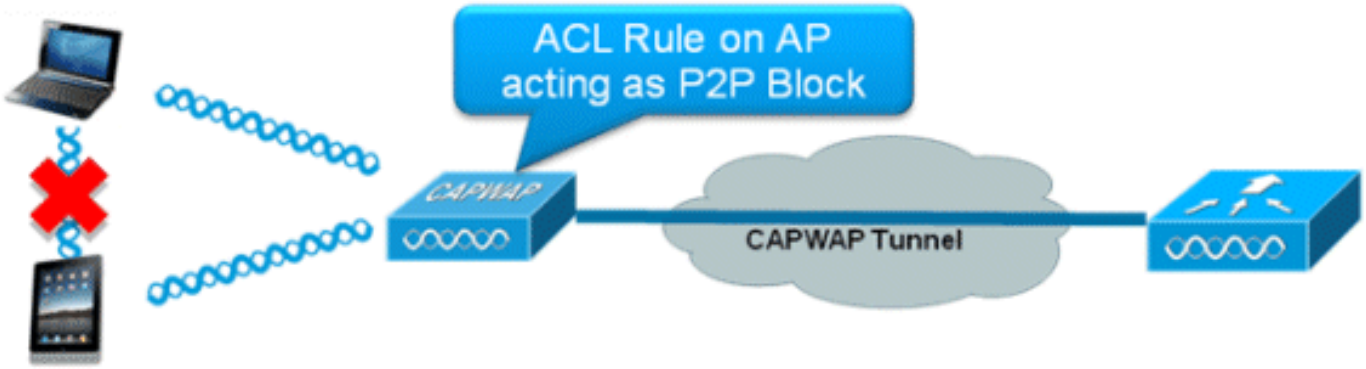
Einschränkungen

- VLAN Based Central Switching wird nur auf WLANs unterstützt, die für zentrale Authentifizierung und lokales Switching konfiguriert sind.

- Die AP-Subschnittstelle (d. h. die VLAN-Zuordnung) sollte auf dem FlexConnect AP konfiguriert werden.

FlexConnect ACL

Mit der Einführung von ACLs auf FlexConnect steht ein Mechanismus zur Verfügung, mit dem die Zugriffskontrolle auf dem FlexConnect-Access Point für den Schutz und die Integrität des lokal geswitchten Datenverkehrs vom Access Point gewährleistet werden kann. FlexConnect-ACLs werden auf dem WLC erstellt und sollten dann mit dem VLAN konfiguriert werden, das auf dem FlexConnect AP oder der FlexConnect-Gruppe vorhanden ist. Dabei sollte die VLAN-ACL-Zuordnung verwendet werden, die für AAA verwendet wird, um VLANs zu überschreiben. Diese werden dann an den Access Point weitergeleitet.



Zusammenfassung

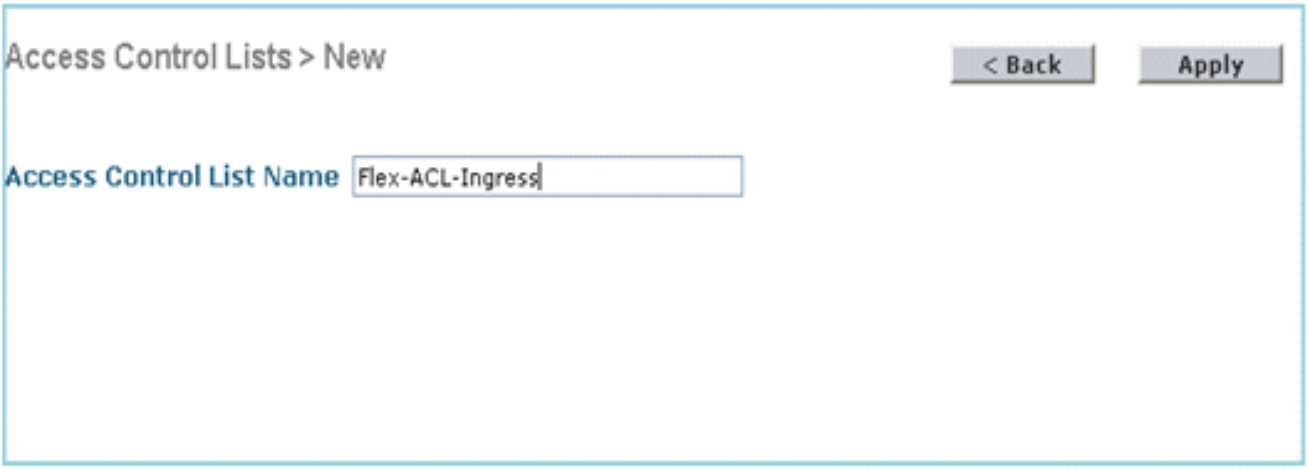
- Erstellen Sie FlexConnect-ACL auf dem Controller.
- Wenden Sie das Gleiche auf ein VLAN an, das auf dem FlexConnect AP unter Access Point-VLAN-ACL-Zuordnung vorhanden ist.
- Kann auf ein VLAN angewendet werden, das in der FlexConnect-Gruppe unter VLAN-ACL-Zuordnung vorhanden ist (wird in der Regel für über AAA abgelegte VLANs durchgeführt).
- Wählen Sie bei Anwendung der Zugriffskontrollliste auf das VLAN die anzuwendende Richtung aus: "Eingang", "Ausgang" oder "Eingang und Ausgang".

Vorgehensweise

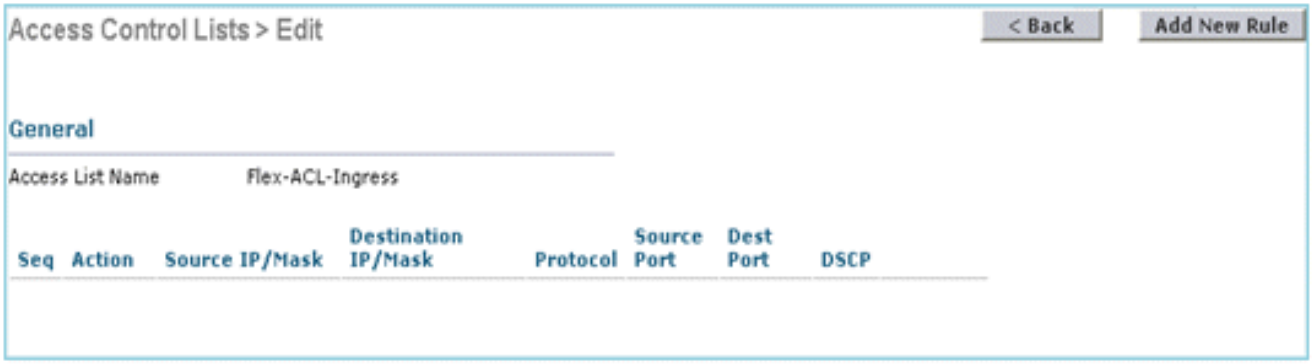
Führen Sie diese Schritte aus:

1. Erstellen Sie eine FlexConnect-ACL auf dem WLC. Navigieren Sie zu **WLC GUI > Security > Access Control List > FlexConnect ACLs**.

2. Klicken Sie auf **Neu**.
3. Konfigurieren Sie den ACL-Namen.



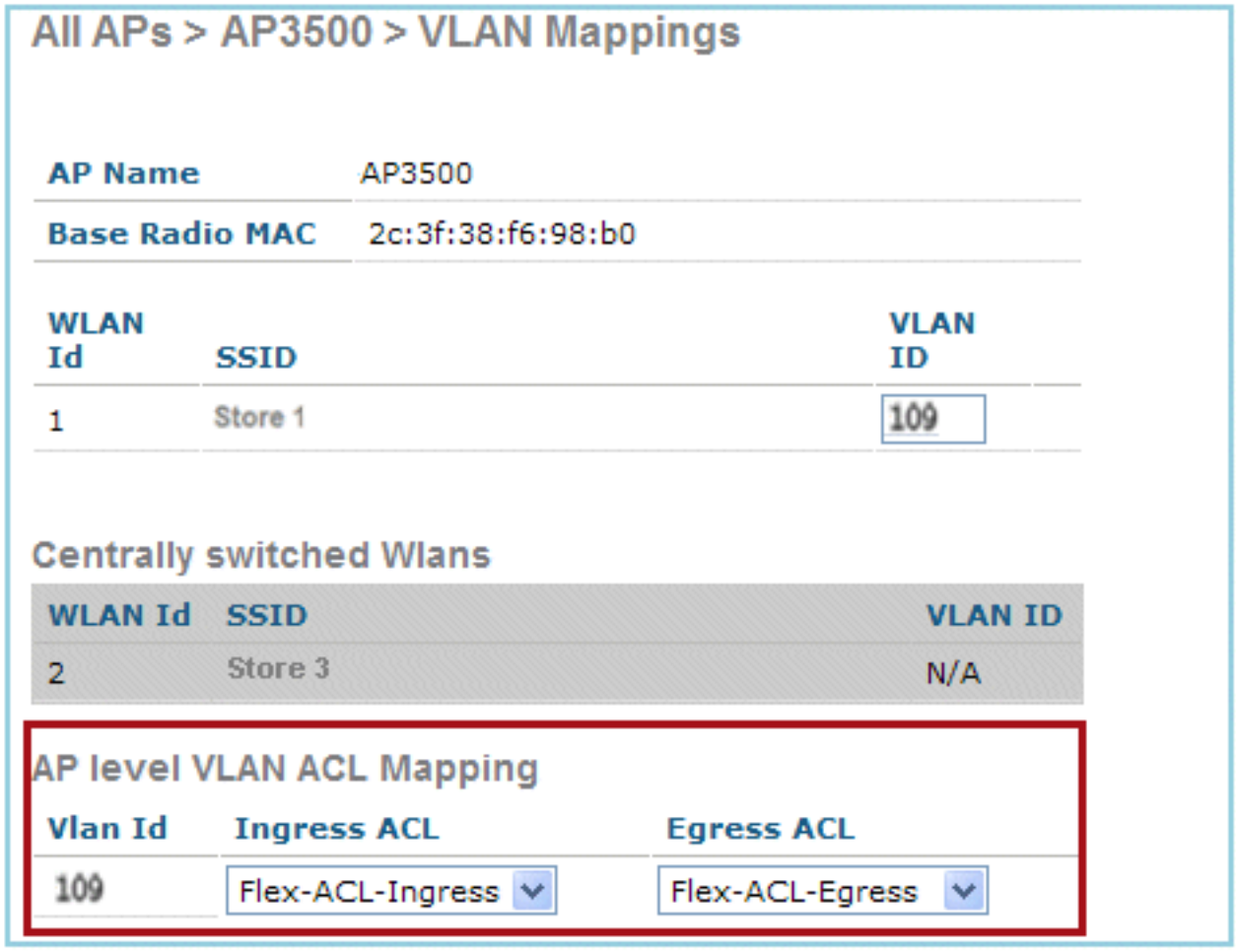
4. Klicken Sie auf **Apply** (Anwenden).
5. Erstellen Sie Regeln für jede ACL. Um Regeln zu erstellen, navigieren Sie zu **WLC GUI > Security > Access Control List > FlexConnect ACLs**, und klicken Sie auf die oben erstellte ACL.



6. Klicken Sie auf **Neue Regel hinzufügen**.

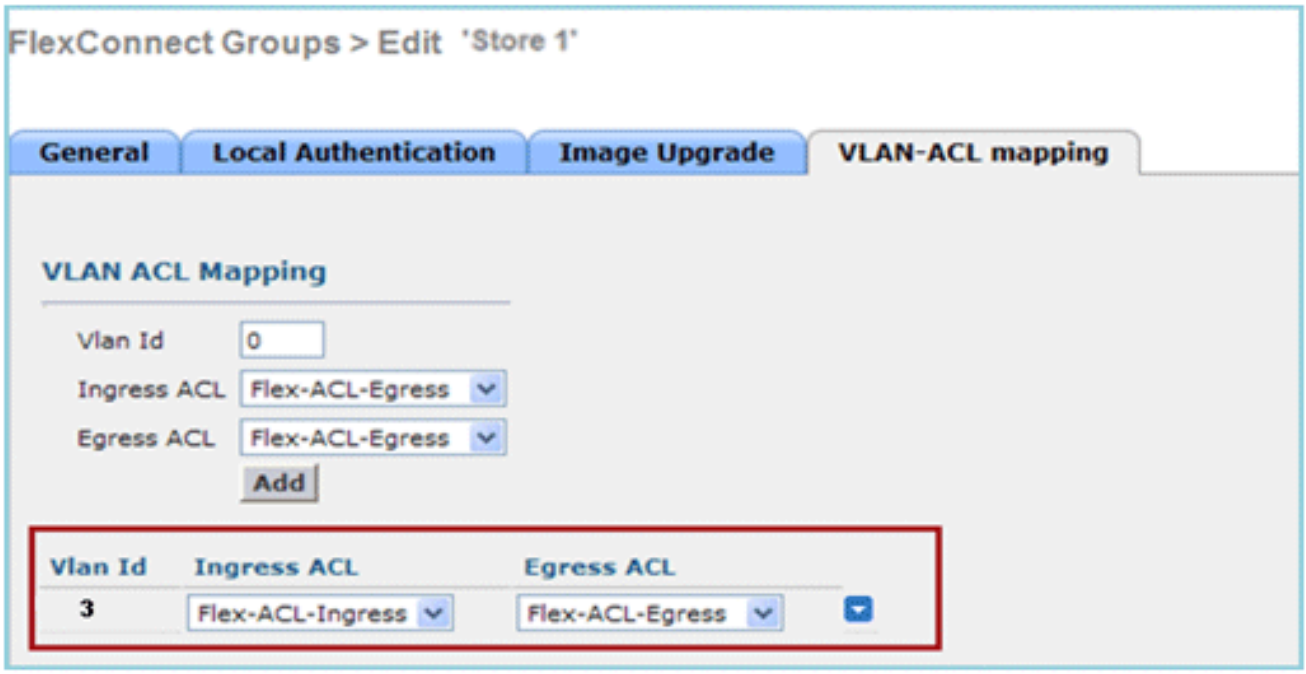
Hinweis: Konfigurieren Sie die Regeln entsprechend der Anforderung. Wenn am Ende keine Regel zugelassen ist, wird der gesamte Datenverkehr durch eine implizite Verweigerung blockiert.

7. Nachdem die FlexConnect-ACLs erstellt wurden, können sie für die WLAN-VLAN-Zuordnung unter einem einzelnen FlexConnect-AP zugeordnet oder für die VLAN-ACL-Zuordnung in der FlexConnect-Gruppe angewendet werden.
8. Zuordnen der oben konfigurierten FlexConnect-ACL auf AP-Ebene für einzelne VLANs unter VLAN-Zuordnungen für einzelne FlexConnect-APs Navigieren Sie zu **WLC-GUI > Wireless > All AP >** klicken Sie auf die **Registerkarte** AP **> FlexConnect > VLAN Mapping.**



9. FlexConnect ACL kann auch auf VLAN-ACL-Zuordnung in der FlexConnect-Gruppe angewendet werden. VLANs, die in der FlexConnect-Gruppe unter der VLAN-ACL-

Zuordnung erstellt wurden, werden hauptsächlich für die dynamische VLAN-Überschreibung verwendet.



Einschränkungen

- Auf dem WLC können maximal 512 FlexConnect-ACLs konfiguriert werden.
- Jede einzelne ACL kann mit 64 Regeln konfiguriert werden.
- Es können maximal 32 ACLs pro FlexConnect-Gruppe oder pro FlexConnect-AP zugeordnet werden.
- Zu jedem Zeitpunkt sind maximal 16 VLANs und 32 ACLs auf dem FlexConnect-Zugangspunkt verfügbar.

FlexConnect Split Tunneling

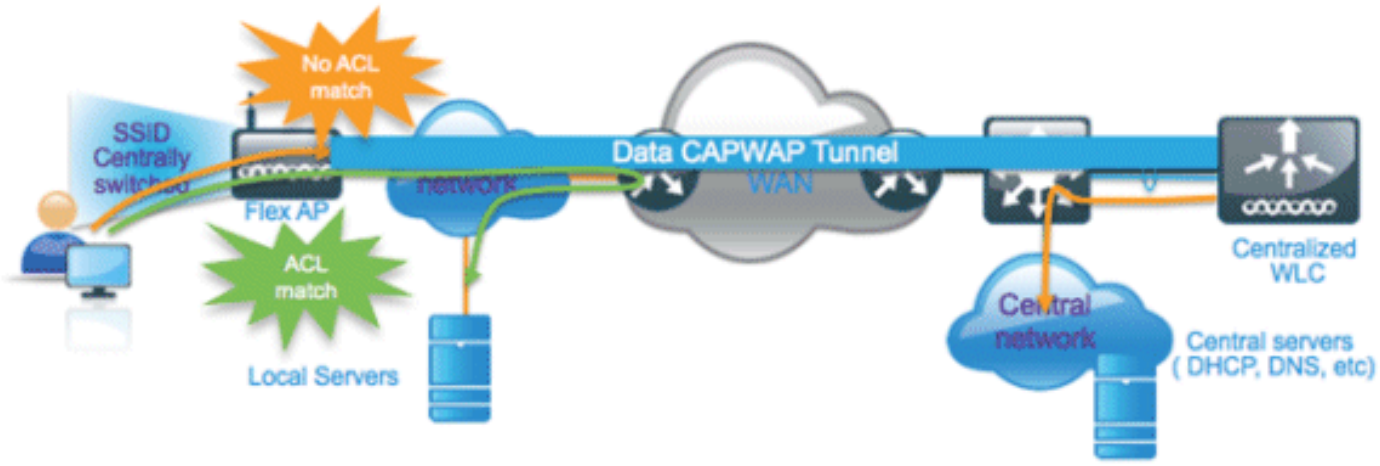
Wenn in WLC-Versionen vor 7.3 ein Client, der mit einem FlexConnect-AP verbunden ist, der einem zentral geswitchten WLAN zugeordnet ist, Datenverkehr an ein Gerät im lokalen Standort/Netzwerk senden muss, muss er Datenverkehr über CAPWAP an den WLC senden und dann denselben Datenverkehr über CAPWAP oder über eine Off-Band-Verbindung an den lokalen Standort zurückleiten.

Ab Version 7.3 führt **Split Tunneling** einen Mechanismus ein, mit dem der vom Client gesendete Datenverkehr anhand des Paketinhalts **mithilfe der Flex ACL** klassifiziert wird. Übereinstimmende Pakete werden lokal vom Flex AP umgeleitet, und die übrigen Pakete werden zentral über CAPWAP geschaltet.

Die Split Tunneling-Funktion ist ein zusätzlicher Vorteil für die OEAP-Konfiguration, bei der Clients auf einer Unternehmens-SSID direkt mit Geräten in einem lokalen Netzwerk kommunizieren können (Drucker, kabelgebundene Systeme auf einem Remote-LAN-Port oder Wireless-Geräte auf einem persönlichen SSID), ohne die WAN-Bandbreite zu beanspruchen, indem Pakete über CAPWAP gesendet werden. Split-Tunneling wird auf den OEAP 600-APs nicht unterstützt. Flex ACLs können mit Regeln erstellt werden, um alle Geräte am lokalen Standort/im lokalen Netzwerk zuzulassen. Wenn Pakete von einem Wireless-Client auf der Corporate SSID mit den auf dem OEAP konfigurierten Flex ACL-Regeln übereinstimmen, wird dieser Datenverkehr lokal geswitcht,

und der restliche Datenverkehr (d. h. impliziter Datenverkehr vom Typ "deny") wird zentral über CAPWAP umgeschaltet.

Bei der Split Tunneling-Lösung wird davon ausgegangen, dass das Subnetz/VLAN, das einem Client in der Zentrale zugeordnet ist, am lokalen Standort nicht vorhanden ist (d. h. Datenverkehr für Clients, die eine IP-Adresse aus dem Subnetz der Zentrale erhalten, kann nicht lokal umgeschaltet werden). Die Split Tunneling-Funktion ist so konzipiert, dass der Datenverkehr für Subnetze, die zum lokalen Standort gehören, lokal umgeleitet wird, um eine Bandbreitennutzung im WAN zu vermeiden. Datenverkehr, der den Flex ACL-Regeln entspricht, wird lokal geswitcht, und der NAT-Vorgang wird ausgeführt, wobei die Quell-IP-Adresse des Clients in die BVI-Schnittstellen-IP-Adresse des Flex AP geändert wird, die am lokalen Standort/Netzwerk routbar ist.



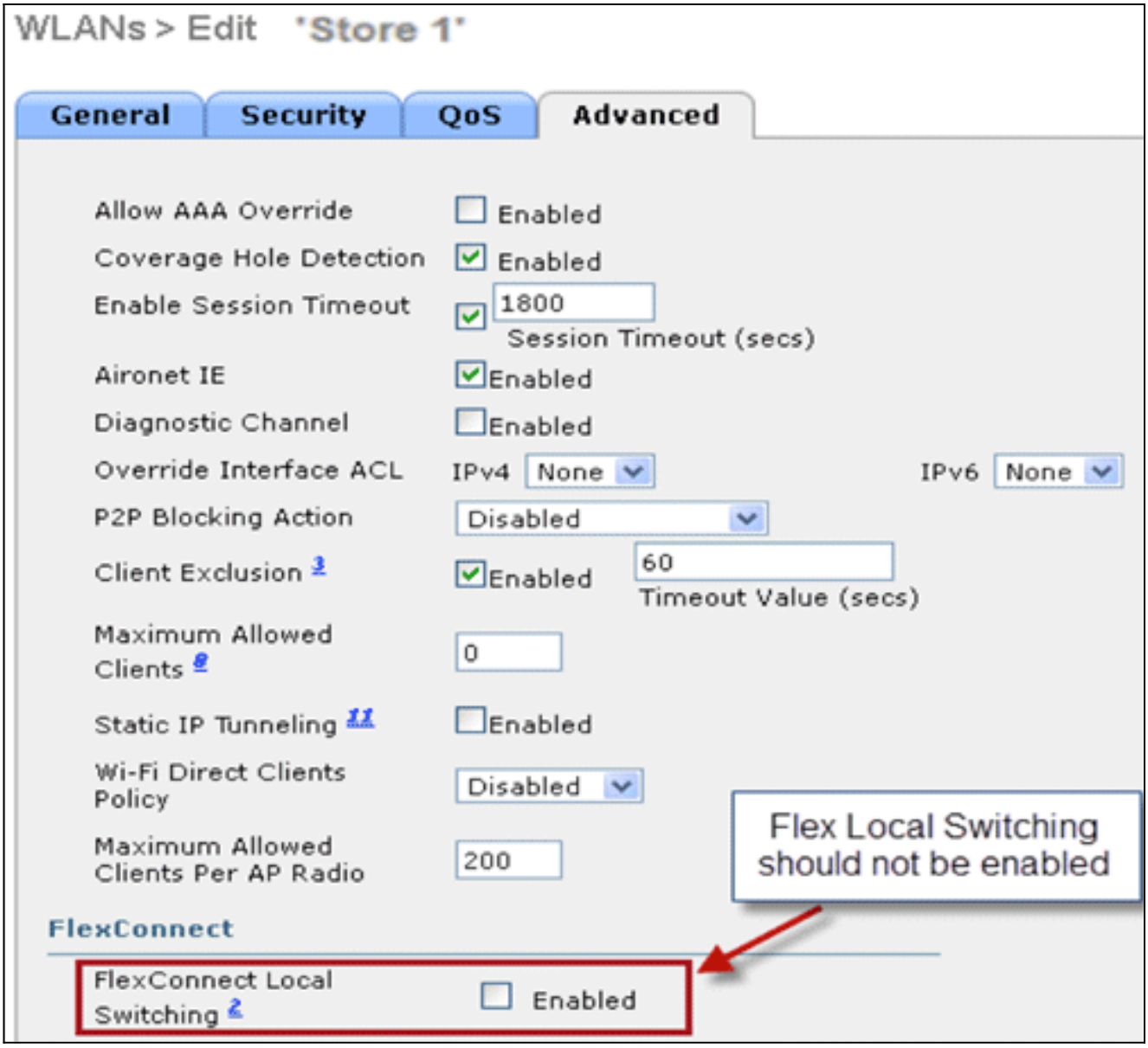
Zusammenfassung

- Die Split Tunneling-Funktion wird auf WLANs unterstützt, die für Central Switching konfiguriert sind und nur von Flex APs angekündigt werden.
- Der erforderliche DHCP sollte in WLANs aktiviert werden, die für Split Tunneling konfiguriert sind.
- Die Split Tunneling-Konfiguration wird pro WLAN angewendet, das für das zentrale Switching pro Flex AP oder für alle Flex APs in einer FlexConnect-Gruppe konfiguriert ist.

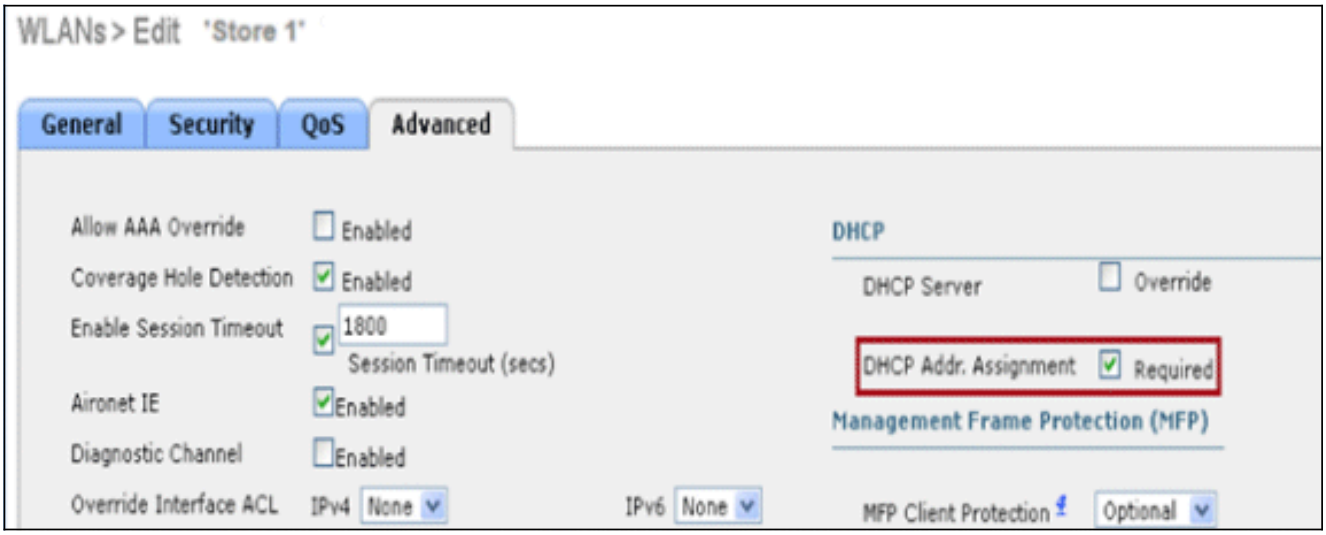
Vorgehensweise

Führen Sie diese Schritte aus:

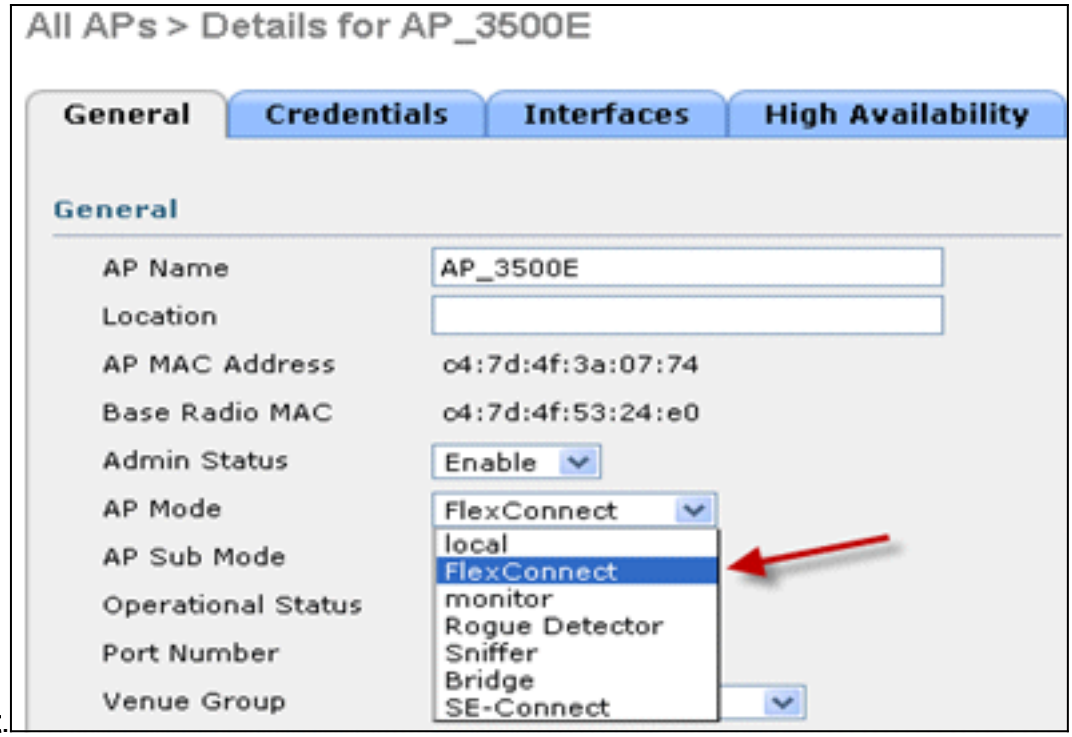
1. Konfigurieren eines WLAN für Central Switching (d. h. **Flex Local Switching** sollte nicht aktiviert
   werden)



2. Legen Sie die DHCP-Adressenzuweisung auf **Erforderlich fest**.



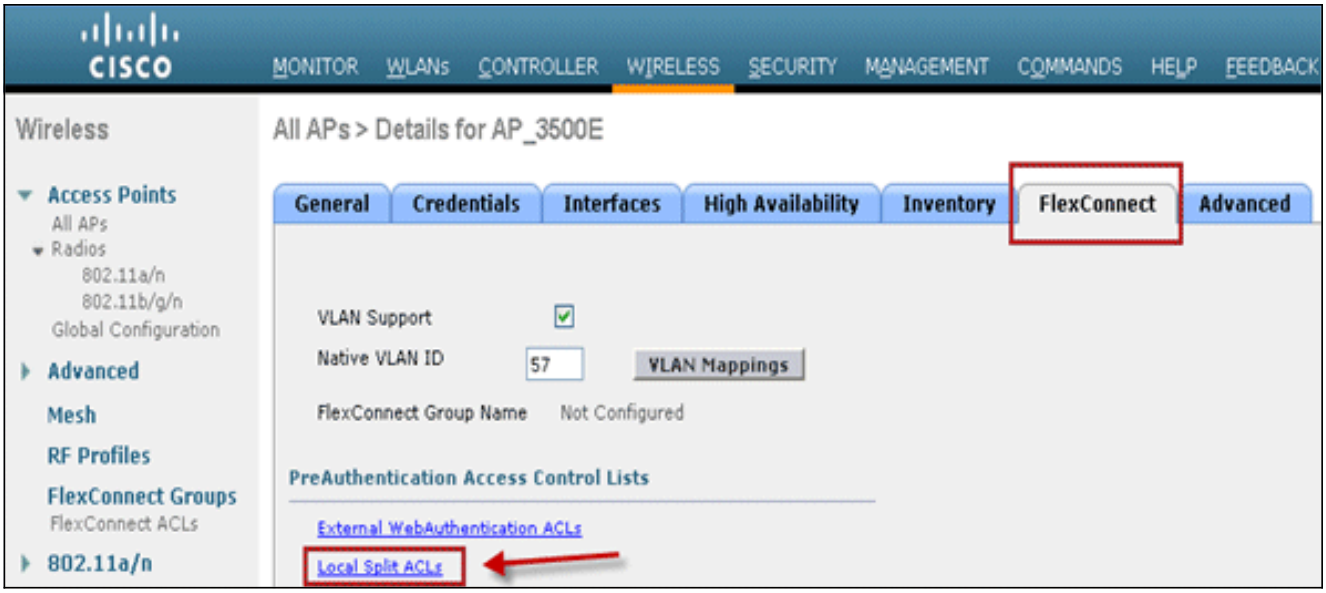
3. Legen Sie den AP-Modus auf **FlexConnect**



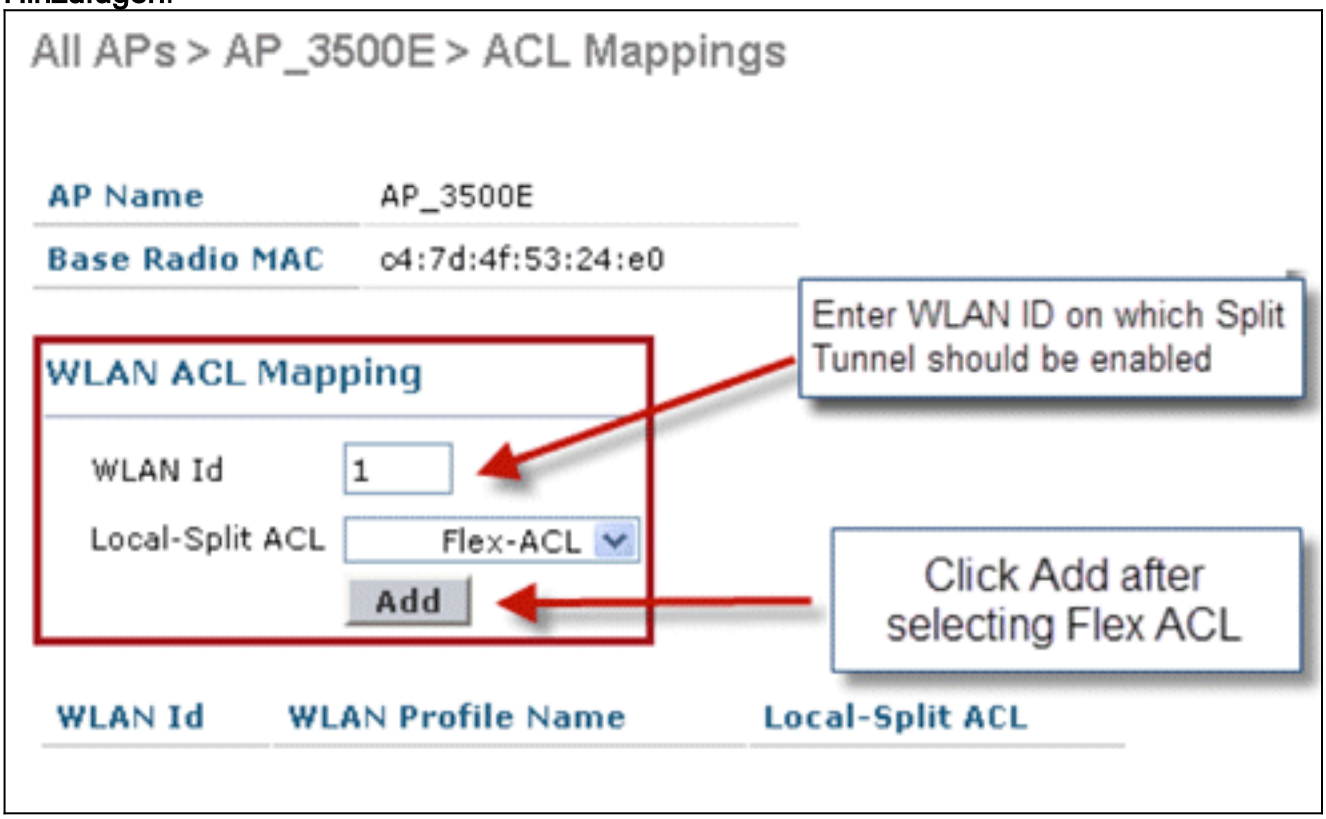
fest.

4. Konfigurieren Sie die FlexConnect-ACL mit einer Genehmigungsregel für Datenverkehr, der lokal auf dem zentralen Switch-WLAN geschaltet werden soll. In diesem Beispiel wird die FlexConnect ACL-Regel konfiguriert, sodass sie den ICMP-Datenverkehr von allen Clients im 9.6.61.0-Subnetz (d. h. auf der Zentrale vorhanden) auf 9.1.0.150 warnt, die lokal geschaltet werden, nachdem der NAT-Vorgang auf Flex AP angewendet wurde. Der restliche Datenverkehr wird durch eine implizite Deny-Regel blockiert und zentral über CAPWAP umgeleitet.

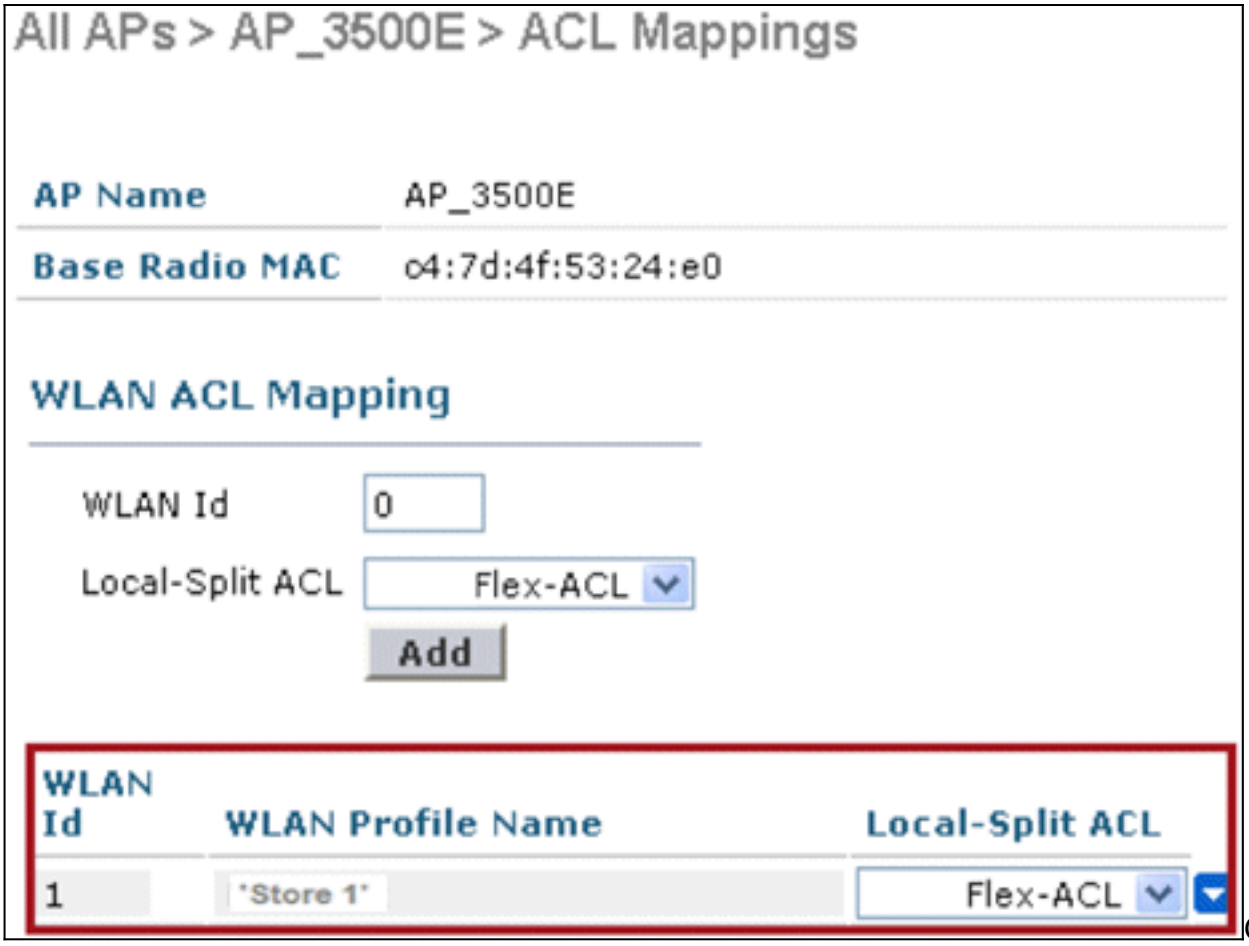
5. Diese erstellte FlexConnect-ACL kann als Split-Tunnel-ACL an einen einzelnen Flex-AP weitergeleitet oder an alle Flex-APs in einer Flex Connect-Gruppe weitergeleitet werden.Gehen Sie wie folgt vor, um Flex ACL als lokale Split-ACL an einen einzelnen Flex AP zu übertragen:Klicken Sie auf **ACLs mit lokaler Aufteilung**.



Wählen Sie die **WLAN-ID** aus, für die die Split Tunnel-Funktion aktiviert werden soll, wählen Sie **Flex-ACL aus**, und klicken Sie auf **Hinzufügen**.

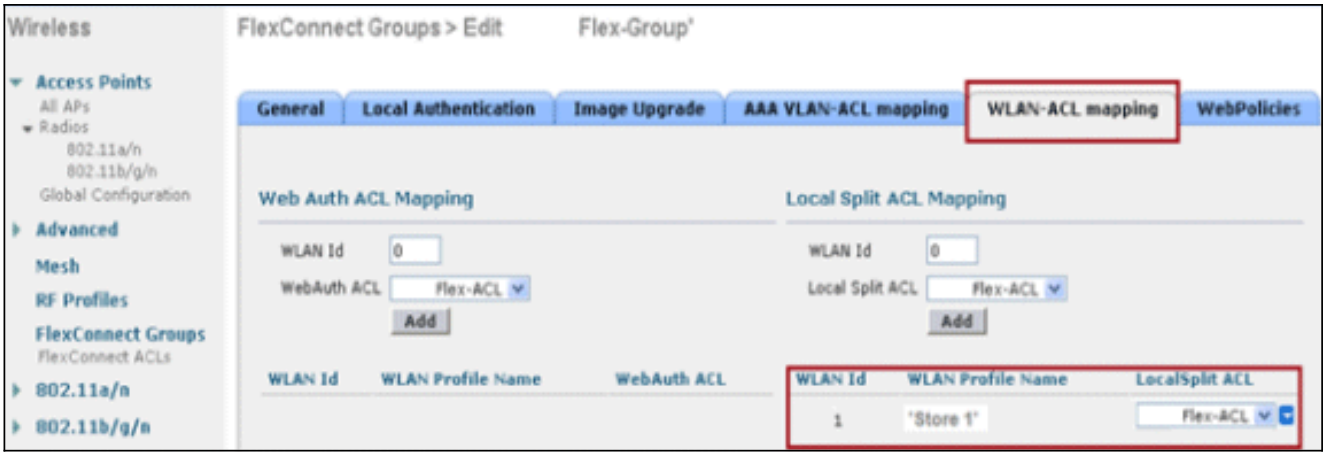


Flex-ACL wird als Local-Split ACL an den Flex AP übertragen.



Gehen Sie wie folgt vor, um Flex ACL als Local Split ACL an eine FlexConnect-Gruppe zu übertragen:Wählen Sie die WLAN-ID aus, für die die Split Tunneling-Funktion aktiviert werden soll. Wählen Sie auf der Registerkarte **WLAN-ACL-Zuordnung** FlexConnect ACL aus der FlexConnect-Gruppe aus, in der bestimmte Flex APs hinzugefügt werden, und klicken Sie auf **Hinzufügen**.

Die Flex-ACL wird als LocalSplit ACL an Flex APs in dieser Flex-Gruppe übertragen.



Einschränkungen

- Flex ACL-Regeln sollten nicht mit einer permit/deny-Anweisung mit demselben Subnetz wie Quelle und Ziel konfiguriert werden.
- Der Datenverkehr in einem zentralen Switching-WLAN, das für Split Tunneling konfiguriert ist, kann nur lokal geschaltet werden, wenn ein Wireless-Client den Datenverkehr für einen Host initiiert, der am lokalen Standort vorhanden ist. Wenn der Datenverkehr von Clients/Hosts an einem lokalen Standort für Wireless-Clients in diesen konfigurierten WLANs initiiert wird, kann er das Ziel nicht erreichen.
- Split Tunneling wird für Multicast-/Broadcast-Datenverkehr nicht unterstützt. Multicast-/Broadcast-Datenverkehr wird zentral umgeschaltet, selbst wenn er mit der Flex ACL übereinstimmt.

Fehlertoleranz

FlexConnect Fault Tolerance ermöglicht den Wireless-Zugriff und die Bereitstellung von Services für Zweigstellen-Clients in folgenden Fällen:

- FlexConnect Branch APs verlieren die Verbindung mit dem primären Flex 7500-Controller.
- FlexConnect Branch APs wechseln zum sekundären Flex 7500-Controller.
- FlexConnect Branch APs stellen die Verbindung zum primären Flex 7500-Controller wieder her.

FlexConnect Fault Tolerance bietet zusammen mit dem oben beschriebenen lokalen EAP während eines Netzwerkausfalls keine Ausfallzeiten in der Zweigstelle. Diese Funktion ist standardmäßig aktiviert und kann nicht deaktiviert werden. Sie erfordert keine Konfiguration auf dem Controller oder dem Access Point. Um jedoch sicherzustellen, dass Fehlertoleranz reibungslos funktioniert und anwendbar ist, sollten diese Kriterien beibehalten werden:

- Bestellung und Konfigurationen von WLANs müssen für die primären und Backup-Flex7500-Controller identisch sein.
- Die VLAN-Zuordnung muss für die primären und Backup-Flex7500-Controller identisch sein.
- Der Name der Mobility-Domäne muss für die primären und Backup-Flex7500-Controller identisch sein.
- Es wird empfohlen, Flex 7500 als primäre und Backup-Controller zu verwenden.

Zusammenfassung

- FlexConnect trennt Clients nicht, wenn der Access Point wieder eine Verbindung zum gleichen Controller herstellt, sofern die Konfiguration des Controllers unverändert bleibt.
- FlexConnect trennt die Clients bei der Verbindung mit dem Backup-Controller nicht, sofern die Konfiguration unverändert bleibt und der Backup-Controller mit dem primären Controller identisch ist.
- FlexConnect setzt seine Funkmodule beim Herstellen einer Verbindung zum primären Controller nicht zurück, sofern die Konfiguration des Controllers unverändert bleibt.

Einschränkungen

- Wird nur für FlexConnect mit Central/Local Authentication mit Local Switching unterstützt.
- Zentral authentifizierte Clients erfordern eine vollständige erneute Authentifizierung, wenn der Client-Sitzungs-Timer abläuft, bevor die FlexConnect AP-Switches vom Standalone- zum Connected-Modus wechseln.
- Die primären und Backup-Controller der Flex 7500-Serie müssen sich in derselben Mobilitätsdomäne befinden.

Client-Limit pro WLAN

Neben der Segmentierung des Datenverkehrs muss auch der gesamte Client, der auf die Wireless-Services zugreift, eingeschränkt werden.

Beispiel: Beschränkung der Gesamtzahl der Gastclients vom Tunneling der Zweigstelle zurück zum Rechenzentrum.

Um dieser Herausforderung zu begegnen, führt Cisco die Funktion "Client Limit per WLAN" ein, mit der die Gesamtzahl der pro WLAN zulässigen Clients eingeschränkt werden kann.

Hauptziel

- Legen Sie Höchstgrenzen für Clients fest.
- Einfacher Betrieb

Hinweis: Dies ist keine Form von QoS.

Standardmäßig ist das Feature deaktiviert und erzwingt keinen Grenzwert.

Einschränkungen

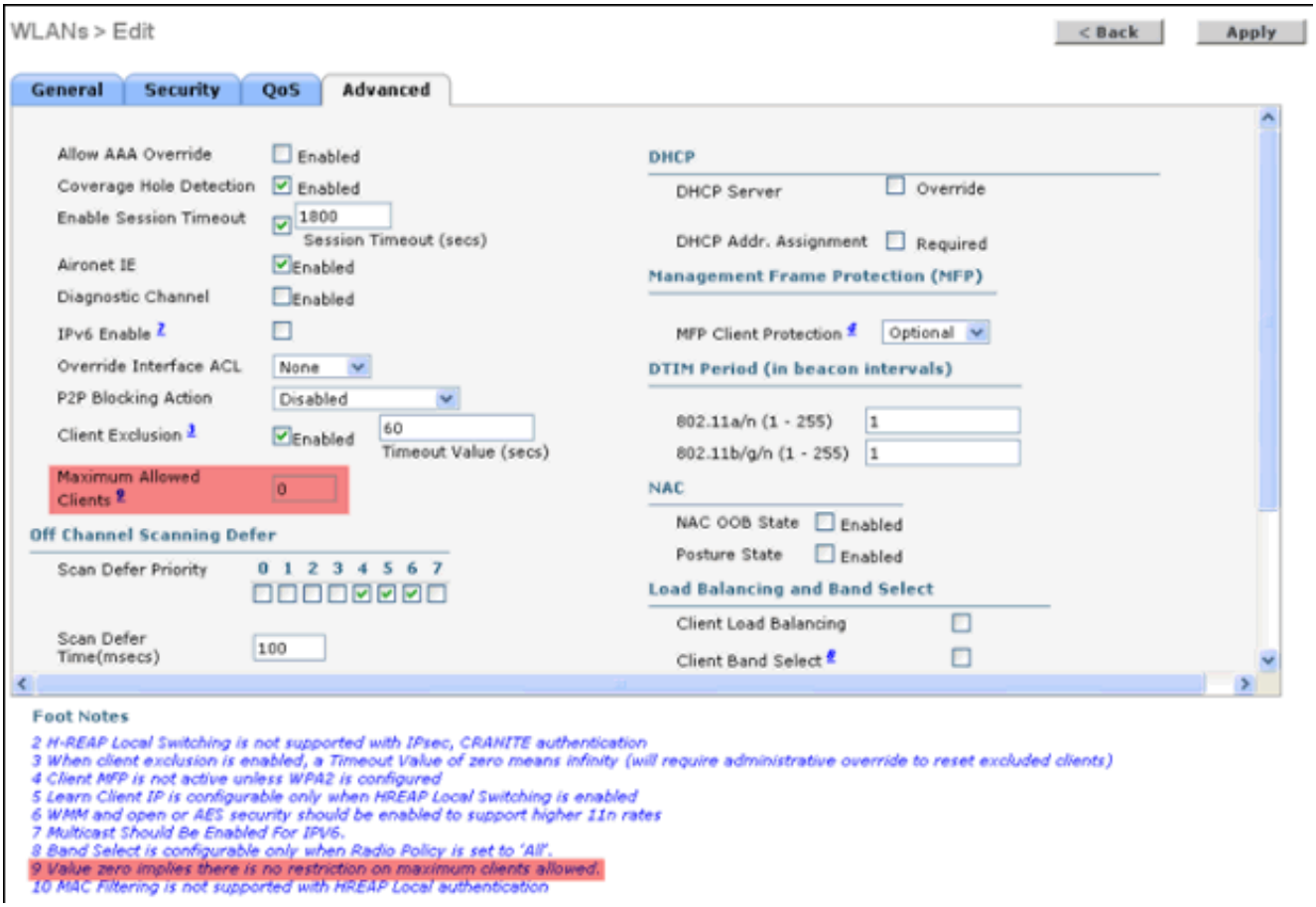
Diese Funktion setzt keine Client-Beschränkung durch, wenn sich FlexConnect im Standalone-Betriebszustand befindet.

WLC-Konfiguration

Führen Sie diese Schritte aus:

1. Wählen Sie die zentrale Switched WLAN ID 1 mit SSID **DataCenter aus**. Dieses WLAN wurde während der Erstellung der AP-Gruppe erstellt. Siehe Abbildung 8.
2. Klicken Sie auf die Registerkarte **Erweitert** für WLAN-ID 1.

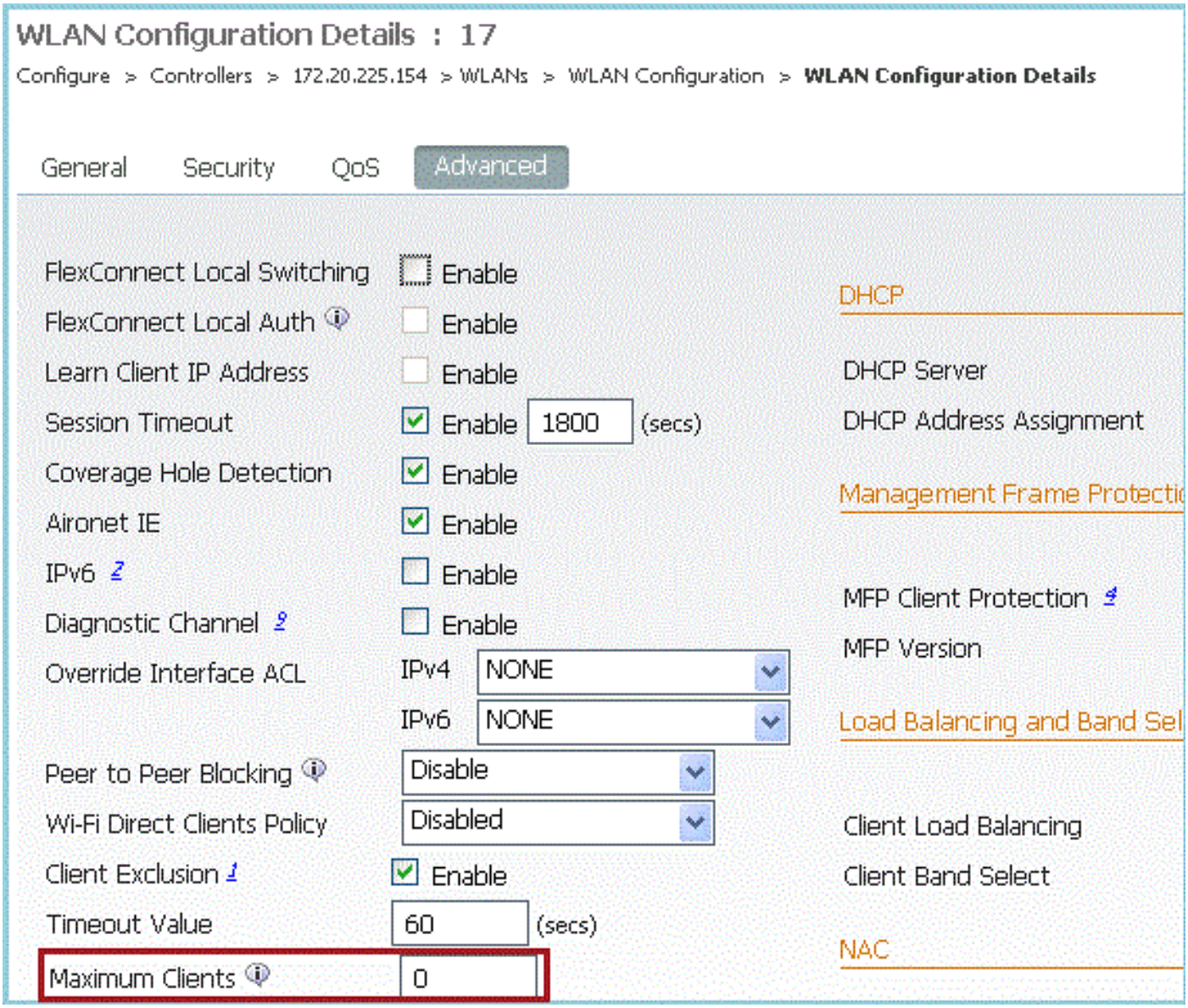
3. Legen Sie den Client-Grenzwert für das Textfeld Maximal zulässige Clients fest.
4. Klicken Sie auf **Übernehmen**, nachdem das Textfeld Maximal zulässige Clients eingestellt wurde.



Die Standardeinstellung für "Maximum Allowed Clients" (Maximal zulässige Clients) ist auf "0" (0) festgelegt. Dies bedeutet, dass keine Einschränkung besteht und die Funktion deaktiviert ist.

NCS-Konfiguration

Um diese Funktion vom NCS zu aktivieren, gehen Sie zu **Konfigurieren > Controller > Controller IP > WLANs > WLAN Configuration > WLAN Configuration Details (WLAN-Konfiguration > WLAN-Konfigurationsdetails).**

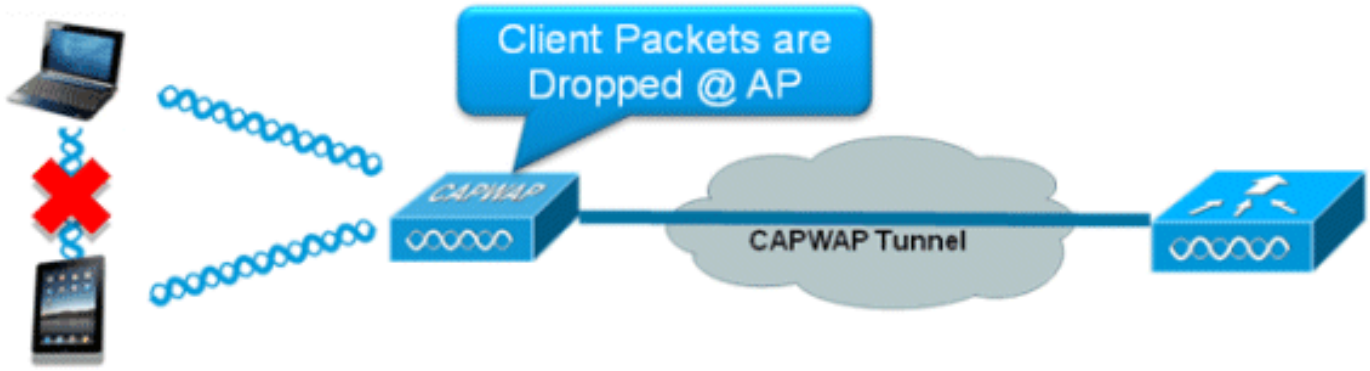


Peer-to-Peer-Blockierung

In Controller-Softwareversionen vor 7.2 wurde die Peer-to-Peer (P2P)-Blockierung nur für zentrale Switching-WLANs unterstützt. Peer-to-Peer-Blockierung kann im WLAN mit einer der folgenden drei Aktionen konfiguriert werden:

- **Deaktiviert** - Deaktiviert Peer-to-Peer-Blockierung und überbrückten Datenverkehr lokal im Controller für Clients im gleichen Subnetz. Dies ist der Standardwert.
- **Drop** - Der Controller verwirft Pakete für Clients im gleichen Subnetz.
- **Forward Up-Stream** (**Nach oben-Stream weiterleiten**): Bewirkt, dass das Paket im Upstream-VLAN weitergeleitet wird. Die Geräte oberhalb des Controllers entscheiden, welche Maßnahmen im Hinblick auf das Paket ergriffen werden sollen.

Ab Version 7.2 wird die Peer-to-Peer-Blockierung für Clients unterstützt, die in einem lokalen Switching-WLAN verbunden sind. Pro WLAN wird die Peer-to-Peer-Konfiguration vom Controller an den FlexConnect AP weitergeleitet.



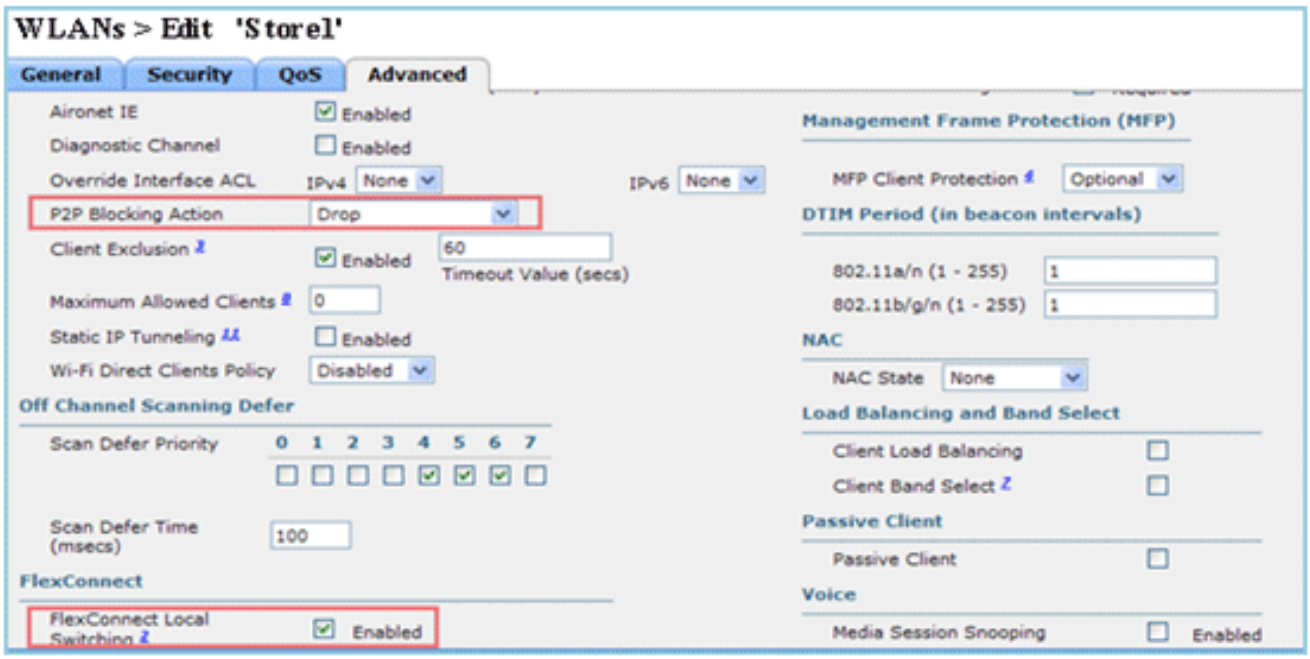
Zusammenfassung

- Peer-to-Peer-Blockierung wird pro WLAN konfiguriert.
- Pro WLAN wird die Peer-to-Peer-Blockierungskonfiguration von WLC an FlexConnect-APs übermittelt.
- Peer-to-Peer-Blockierungsaktion, die als Drop- oder Upstream-Forward im WLAN konfiguriert ist, wird als Peer-to-Peer-Blockierung behandelt, die auf dem FlexConnect AP aktiviert ist.

Vorgehensweise

Führen Sie diese Schritte aus:

1. Aktivieren Sie die Peer-to-Peer-Blockierungsaktion als **Drop** in WLAN, das für das lokale FlexConnect-Switching konfiguriert
   ist.



2. Sobald die P2P-Blockierungsaktion als **Drop** oder **Forward-Upstream** im WLAN konfiguriert ist, das für lokales Switching konfiguriert ist, wird sie vom WLC an den FlexConnect-AP weitergeleitet. Die FlexConnect-APs speichern diese Informationen im Flash-Speicher in der reap-Konfigurationsdatei. Selbst wenn sich der FlexConnect AP im Standalone-Modus befindet, kann er damit die P2P-Konfiguration auf die entsprechenden Subschnittstellen anwenden.

Einschränkungen

- In FlexConnect kann die Konfiguration der P2P-Blockierung der Lösung nicht nur auf einen bestimmten FlexConnect-AP oder einen Teilsatz von APs angewendet werden. Sie wird auf alle FlexConnect-APs angewendet, die die SSID übertragen.
- Die einheitliche Lösung für zentrale Switching-Clients unterstützt P2P Upstream-Forward. Dies wird jedoch in der FlexConnect-Lösung nicht unterstützt. Dies wird als P2P-Dropdown behandelt, und Client-Pakete werden verworfen, anstatt an den nächsten Netzwerkknoten weitergeleitet zu werden.
- Die einheitliche Lösung für zentrale Switching-Clients unterstützt die P2P-Blockierung für Clients, die unterschiedlichen APs zugeordnet sind. Diese Lösung ist jedoch nur auf Clients ausgerichtet, die mit demselben AP verbunden sind. FlexConnect-ACLs können als Problemumgehung für diese Einschränkung verwendet werden.

AP-Pre-Image-Download

Mit dieser Funktion kann der Access Point Code während des Betriebs herunterladen. Das AP-Pre-Image-Download ist äußerst hilfreich, um die Ausfallzeiten des Netzwerks während der Softwarewartung oder -aktualisierung zu reduzieren.

Zusammenfassung

- Einfache Softwareverwaltung
- Aktualisierung pro Geschäft ansetzen: hierfür ist das NCS erforderlich.
- Reduziert Ausfallzeiten

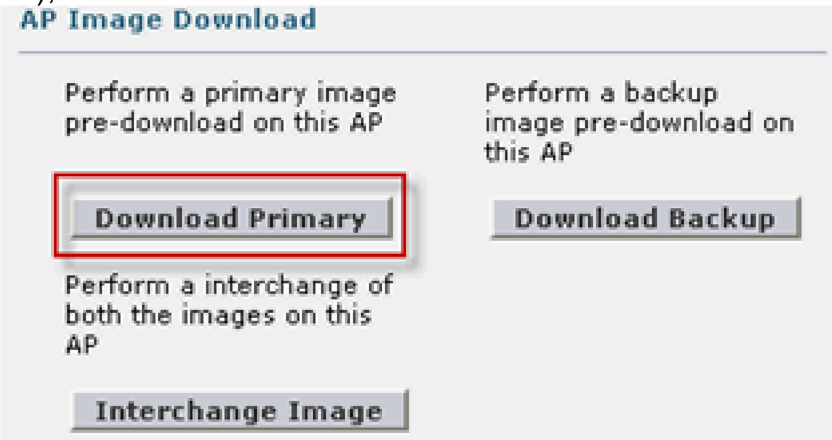
Vorgehensweise

Führen Sie diese Schritte aus:

1. Aktualisieren Sie das Image auf den primären und Backup-Controllern.Navigieren Sie unter **WLC GUI > Commands > Download File**, um den Download zu starten.


2. Speichern Sie die Konfigurationen auf den Controllern, starten Sie den Controller jedoch nicht neu.
3. Geben Sie den Befehl zum Herunterladen des AP-Pre-Image vom primären Controller aus.Navigieren Sie zu **WLC GUI > Wireless > Access Points > All APs** und wählen Sie den Access Point aus, um den Pre-Image-Download zu starten.Klicken Sie nach Auswahl des

Access Points auf die Registerkarte **Erweitert**.Klicken Sie auf **Download Primary (Primäres Download**), um den Vorab-Download zu



starten.

```
*Sep [redacted].903: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
Image [redacted] not found in flash, predownloading.
examining image...!
extracting info (326 bytes)
Image info:
    Version Suffix: k9w8-.wnbu_j_mr.201009101910
    Image Name: c1250-k9w8-mx.wnbu_j_mr.201009101910
    Version Directory: c1250-k9w8-mx.wnbu_j_mr.201009101910
    Ios Image Size: 5530112
    Total Image Size: 5550592
    Image Feature: WIRELESS LAN|LWAPP
    Image Family: C1250
    Wireless Switch Management Version: [redacted]
Extracting files...
c1250-k9w8-mx.wnbu_j_mr.201009101910/ (directory) 0 (bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_1.img (13696 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W5.bin (17372 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9w8-mx.wnbu_j_mr.20100910
1910 (5322509 bytes)!!!!!!
*Sep 13 21:25:43.747: Loading file /c1250-pre[redacted]..
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/8001.img (172792 bytes)!!!!!!!!
!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W2.bin (4848 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/info (326 bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_2.img (10880 bytes)!
extracting info.ver (326 bytes)
New software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910
archive download: takes 138 seconds

New backup software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.2010091019
10/c1250-k9w8-mx.wnbu_j_mr.201009101910
Reading backup version from flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9
w8-mx.wnbu_j_mr.201009101910done.
```

4. Starten Sie die Controller neu, nachdem alle AP-Images heruntergeladen wurden.Die APs kehren jetzt in den Standalone-Modus zurück, bis die Controller neu gestartet werden.**Hinweis:** Im Standalone-Modus behält die Fehlertoleranz die Zuordnung von Clients bei.Sobald der Controller wieder angeschlossen ist, werden die Access Points automatisch mit dem zuvor heruntergeladenen Image neu gestartet.Nach dem Neustart treten die APs dem primären Controller erneut bei und übernehmen die Fortsetzung der Client-Services.

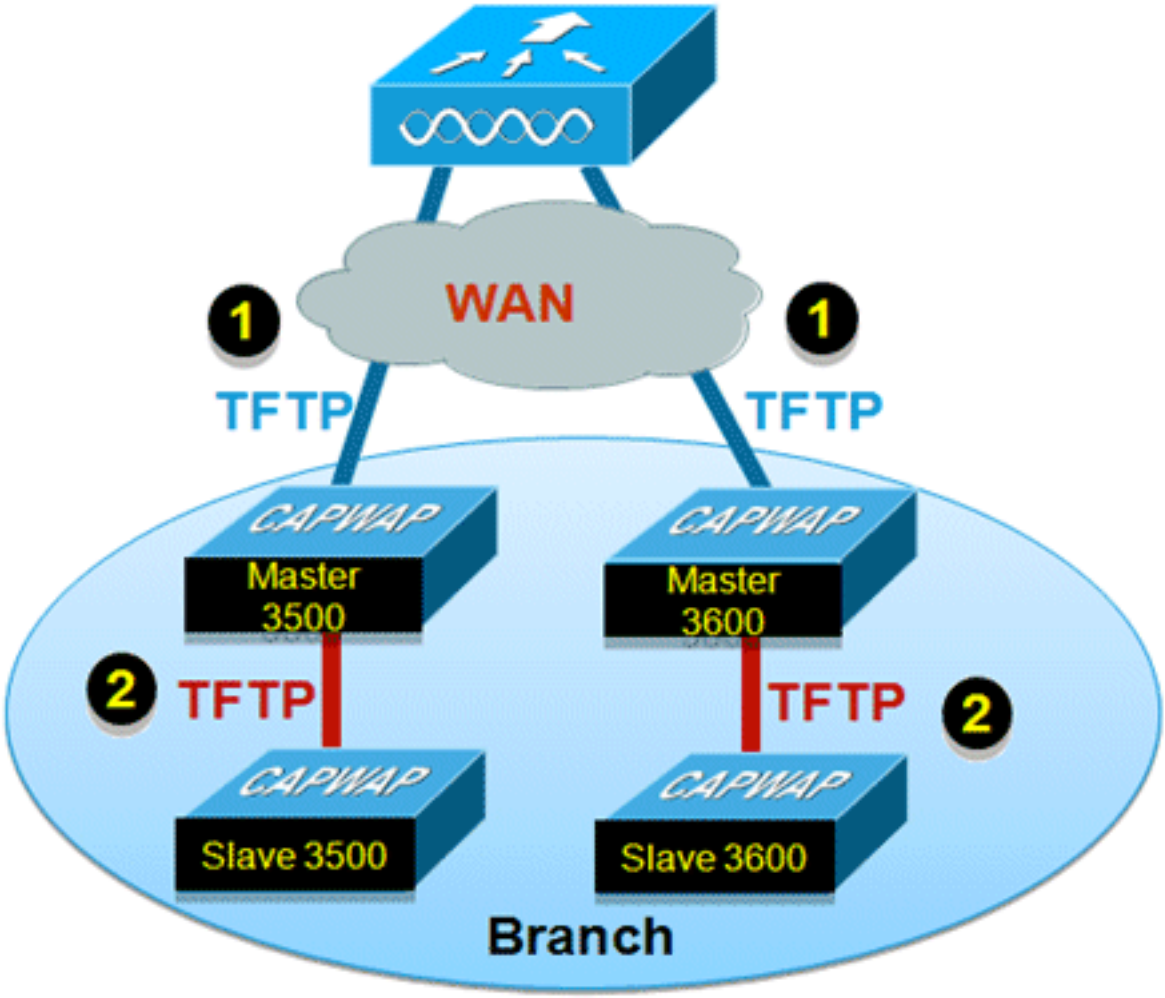
Einschränkungen

- Funktioniert nur mit CAPWAPs.

FlexConnect Smart AP-Image-Upgrade

Die Funktion zum Herunterladen von Pre-Images reduziert die Ausfallzeiten bis zu einem gewissen Grad, aber dennoch müssen alle FlexConnect APs die entsprechenden AP-Images über den WAN-Link mit höherer Latenz vorab herunterladen.

Ein effizientes AP-Image-Upgrade reduziert die Ausfallzeiten für jeden FlexConnect AP. Die Grundidee ist, dass nur ein Access Point eines AP-Modells das Image vom Controller herunterlädt und als Master/Server fungiert, und die übrigen Access Points desselben Modells funktionieren wie Slave/Client und laden das AP-Image vorab vom Master herunter. Die Verteilung des AP-Images vom Server auf den Client erfolgt in einem lokalen Netzwerk, ohne dass die Latenz der WAN-Verbindung auftritt. Dadurch wird der Prozess schneller.



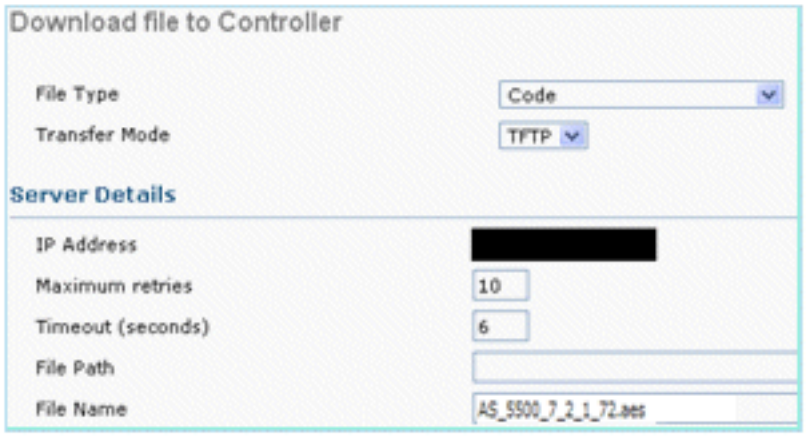
Zusammenfassung

- Master- und Slave-APs werden für jedes AP-Modell pro FlexConnect-Gruppe ausgewählt.
- Master lädt Image von WLC herunter
- Laden Sie Image von Master AP herunter.
- Reduziert Ausfallzeiten und spart WAN-Bandbreite

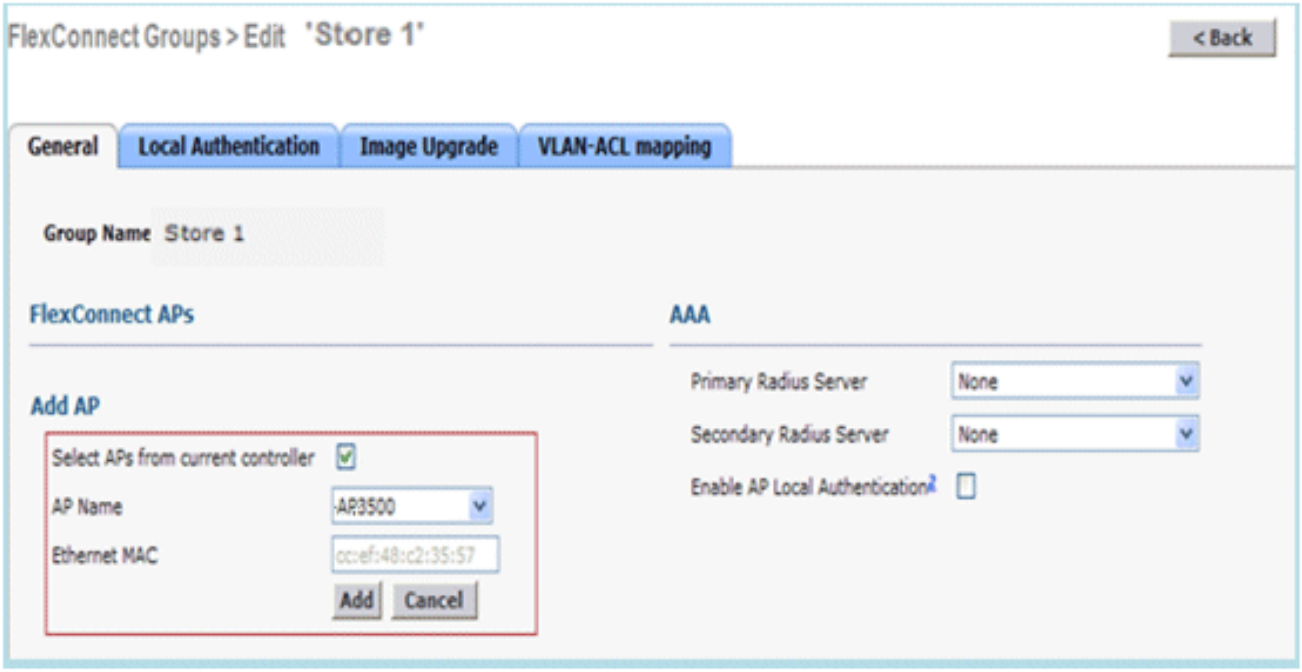
Vorgehensweise

Führen Sie diese Schritte aus:

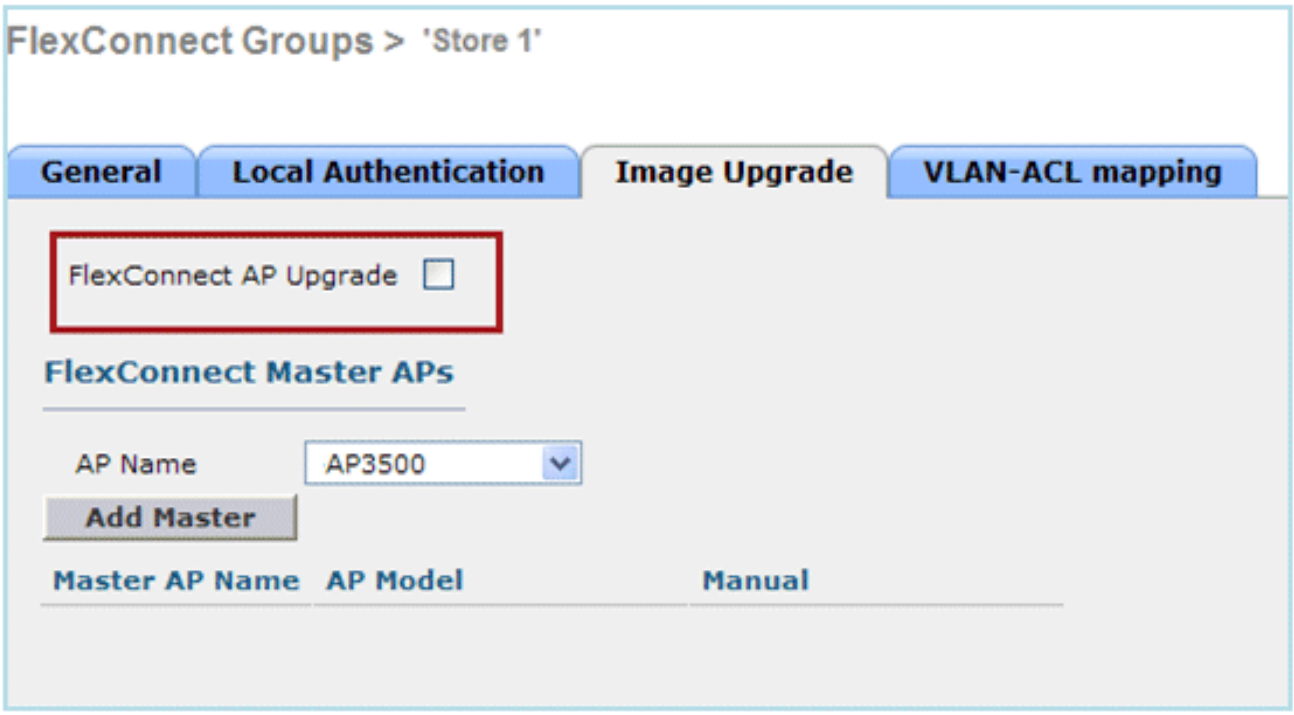
1. Aktualisieren Sie das Image auf dem Controller.Navigieren Sie zu **WLC GUI > Commands > Download File**, um mit dem Herunterladen zu beginnen.



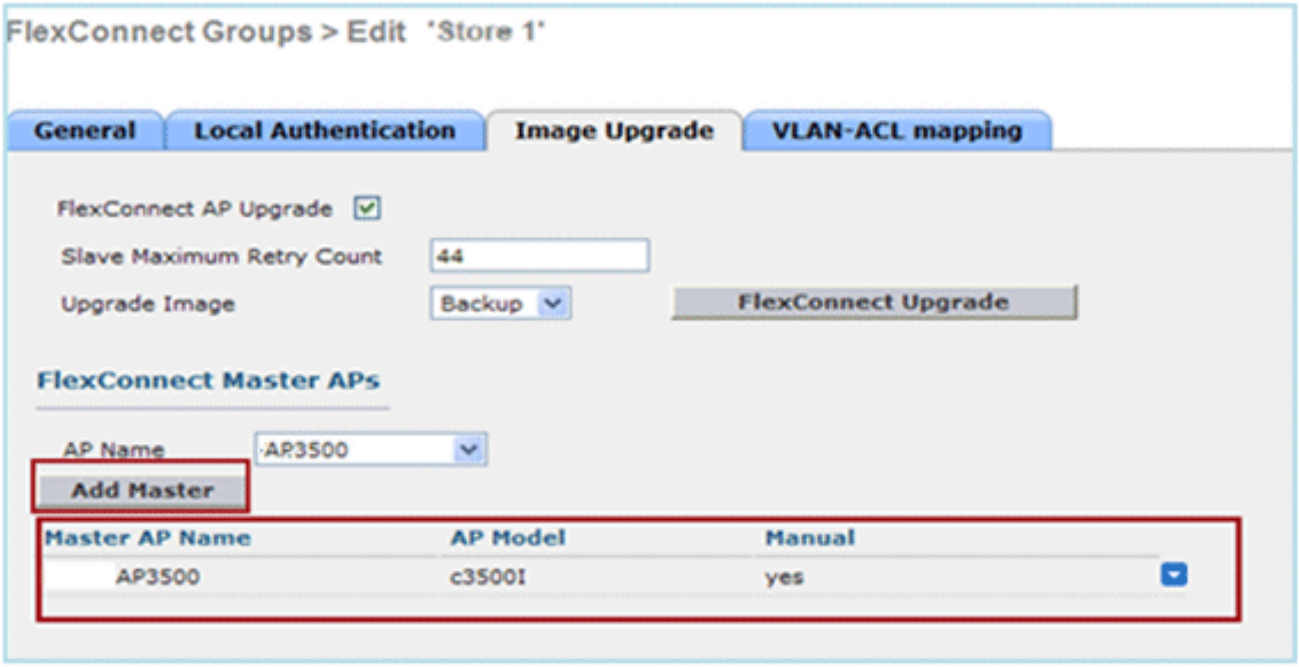
2. Speichern Sie die Konfigurationen auf den Controllern, starten Sie den Controller jedoch nicht neu.
3. Fügen Sie die FlexConnect-APs der FlexConnect-Gruppe hinzu.Navigieren Sie zu **WLC GUI > Wireless > FlexConnect Groups >** wählen Sie **FlexConnect Group > Registerkarte General (Allgemein) > Add AP.**



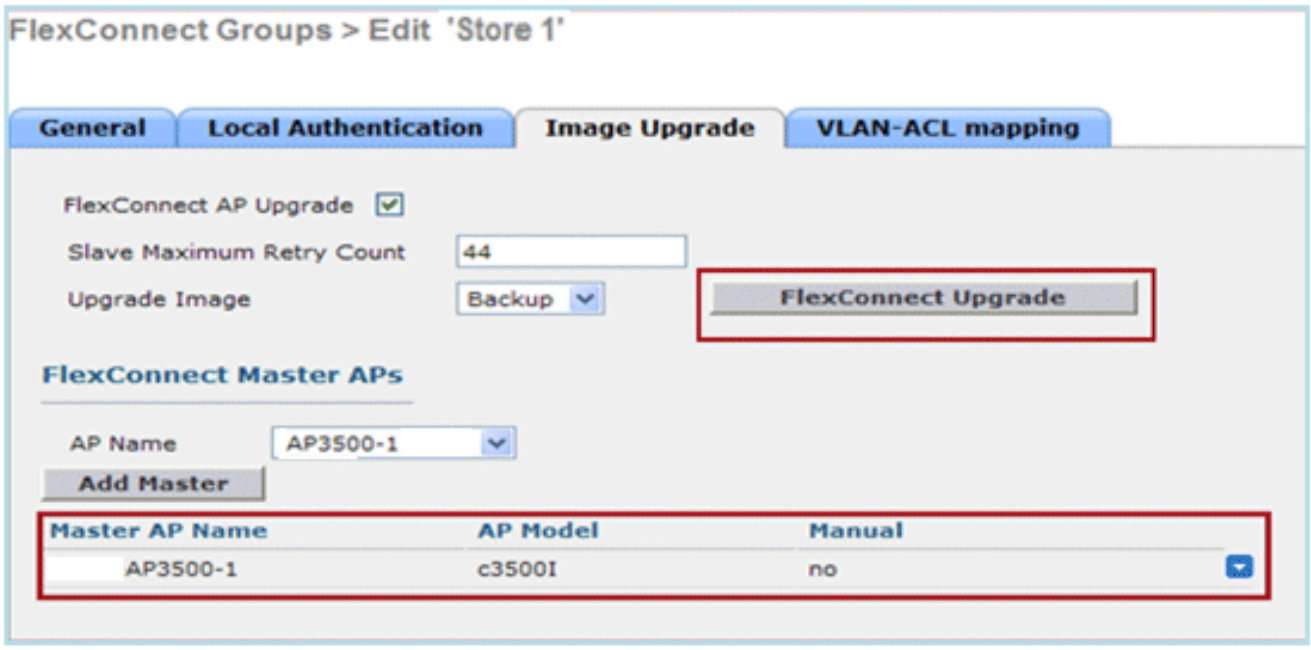
4. Aktivieren Sie das Kontrollkästchen **FlexConnect AP Upgrade**, um ein effizientes AP-Image-Upgrade zu erzielen.Navigieren Sie zu **WLC-GUI > Wireless > FlexConnect Groups >** wählen Sie **FlexConnect Group > Registerkarte Image Upgrade** (FlexConnect-**Gruppe > FlexConnect-Gruppen).**



5. Der Master-Zugangspunkt kann manuell oder automatisch ausgewählt werden:Um den Master-Access manuell auszuwählen, navigieren Sie zu WLC GUI > Wireless > FlexConnect Groups > wählen Sie FlexConnect Group > Image Upgrade tab > FlexConnect Master APs, wählen Sie **AP** aus der Dropdown-Liste aus, und klicken Sie auf **Master hinzufügen.**

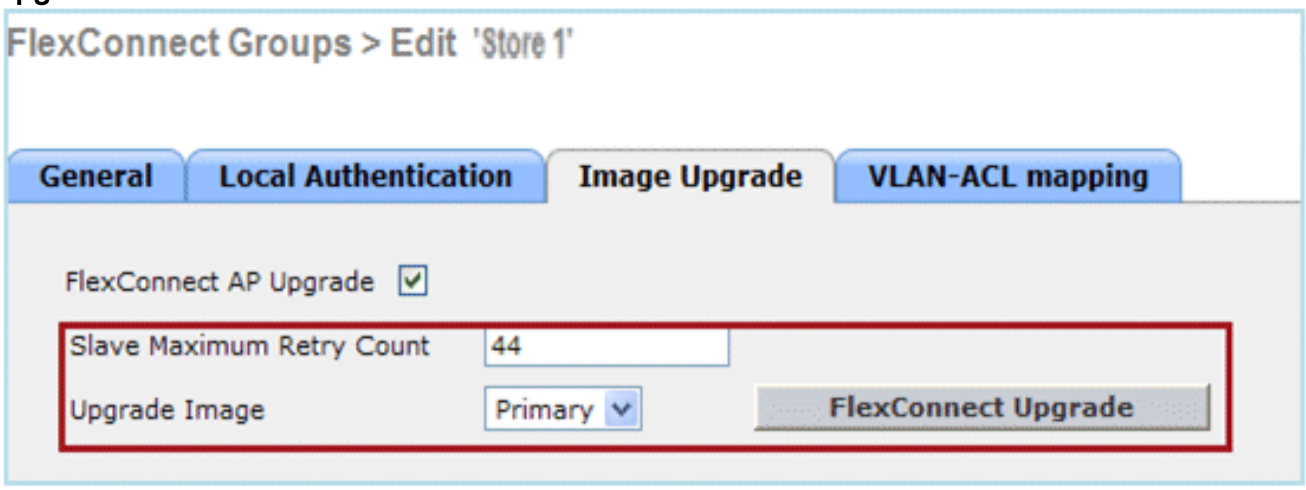


Hinweis: Pro Modell kann nur ein Access Point als Master Access Point konfiguriert werden. Wenn Master AP manuell konfiguriert wird, wird das Feld Manuell mit **Ja** aktualisiert.Um automatisch Master AP auszuwählen, navigieren Sie zu **WLC GUI > Wireless > FlexConnect Groups** > wählen Sie **FlexConnect Group > Image Upgrade Registerkarte, und klicken Sie auf FlexConnect Upgrade.**



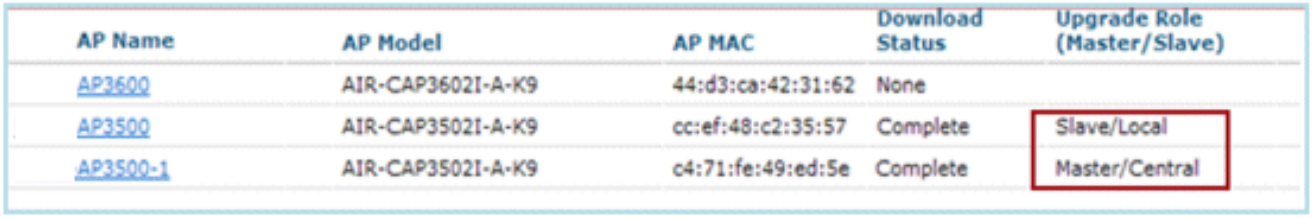
Hinweis: Wenn Master AP automatisch ausgewählt wird, wird das Feld Manual (Manuell) mit **no** aktualisiert.

6. Um ein effizientes AP-Image-Upgrade für alle APs unter einer bestimmten FlexConnect-Gruppe zu starten, klicken Sie auf **FlexConnect Upgrade**.Navigieren Sie zu **WLC-GUI > Wireless > FlexConnect Groups >** wählen Sie **FlexConnect**-Gruppe **> Registerkarte Image Upgrade (FlexConnect-Gruppen), und klicken Sie auf FlexConnect Upgrade.**



Hinweis: Slave Maximum Retry Count ist die Anzahl der Versuche (standardmäßig 44), in denen der Slave Access Point ein Bild vom Master Access Point herunterladen wird, nach dem es zurückfällt, um das Bild vom WLC herunterzuladen. Es wird 20 Versuche gegen WLC unternehmen, um ein neues Image herunterzuladen, nach dem der Administrator den Download-Prozess neu starten muss.

7. Nach der Initiierung der FlexConnect-Aktualisierung wird das Image nur vom Master-Access Point vom WLC heruntergeladen. Auf der Seite All AP (Alle AP) wird **"Upgrade Role"** (**Upgrade-Rolle**) als **Master/Central** aktualisiert, was bedeutet, dass Master AP das Image vom WLC heruntergeladen hat, der sich an der zentralen Stelle befindet. Der Slave-AP lädt das Bild vom Master Access Point, der sich am lokalen Standort befindet und der Grund ist unter All AP-Seite **"Upgrade Role"** wird aktualisiert als **Slave/Local**.Um dies zu überprüfen, navigieren Sie zu **WLC GUI > Wireless**.



AP Name	AP Model	AP MAC	Download Status	Upgrade Role (Master/Slave)
AP3600	AIR-CAP3602I-A-K9	44:d3:ca:42:31:62	None	
AP3500	AIR-CAP3502I-A-K9	cc:ef:48:c2:35:57	Complete	Slave/Local
AP3500-1	AIR-CAP3502I-A-K9	c4:71:fe:49:ed:5e	Complete	Master/Central

8. Starten Sie die Controller neu, nachdem alle AP-Images heruntergeladen wurden. Die APs kehren jetzt in den Standalone-Modus zurück, bis die Controller neu gestartet werden.**Hinweis:** Im Standalone-Modus behält die Fehlertoleranz die Zuordnung von Clients bei.Sobald der Controller wieder angeschlossen ist, werden die Access Points automatisch mit dem zuvor heruntergeladenen Image neu gestartet.Nach dem Neustart treten die APs dem primären Controller erneut bei und übernehmen die Dienste des Clients wieder.

Einschränkungen

- Die Master-AP-Auswahl erfolgt pro FlexConnect-Gruppe und pro AP-Modell in jeder Gruppe.
- Nur drei Slave-APs desselben Modells können gleichzeitig von ihrem Master-AP aufgerüstet werden, und die übrigen Slave-APs verwenden den zufälligen Back-Off-Timer, um erneut für den Master-AP zu versuchen, um das AP-Image herunterzuladen.
- Wenn der Slave AP aus irgendeinem Grund das Image nicht vom Master Access Point herunterladen kann, wird er zum WLC gehen, um das neue Image abzurufen.
- Dies funktioniert nur mit CAPWAPs.

Automatische Umwandlung von APs im FlexConnect-Modus

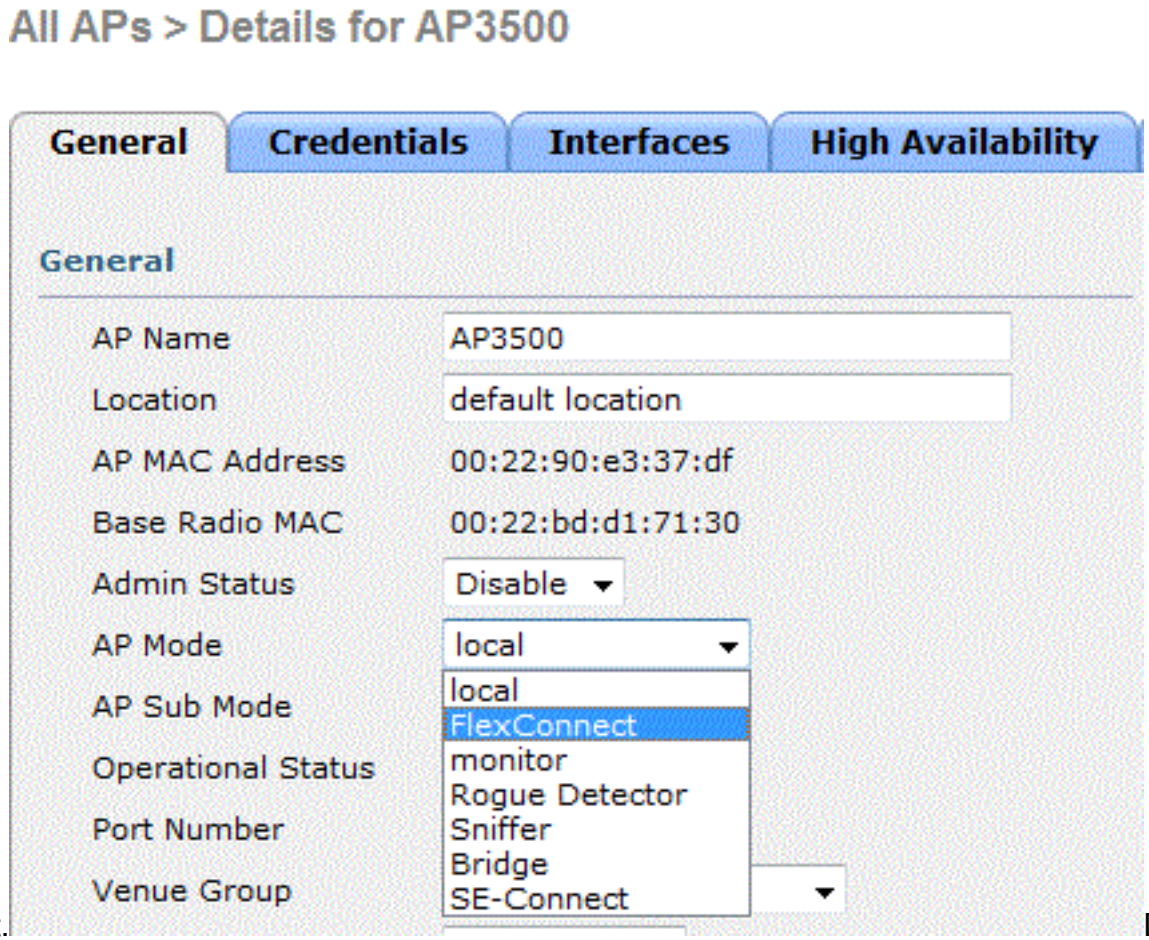
Der Flex 7500 bietet die folgenden beiden Optionen für die Umwandlung des AP-Modus in FlexConnect:

- Manueller Modus
- Auto-Converter-Modus

Manueller Modus

Dieser Modus ist auf allen Plattformen verfügbar und ermöglicht die Änderung nur auf AP-Basis.

1. Navigieren Sie zu **WLC GUI > Wireless > All APs** und wählen Sie den Access Point aus.
2. Wählen Sie **FlexConnect** als AP-Modus aus, und klicken Sie dann auf **Übernehmen**.
3. Wenn Sie den AP-Modus ändern, wird der Access Point neu



gestartet. Die se Option ist auch auf allen aktuellen WLC-Plattformen verfügbar.

Automatischer Konvertierungsmodus

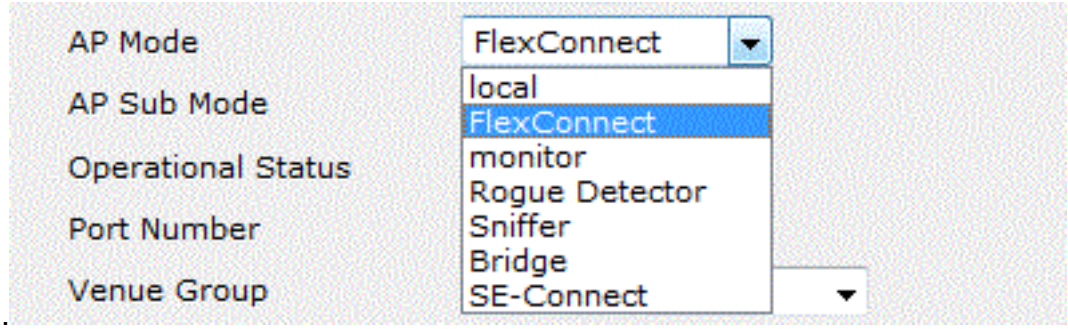
Dieser Modus ist nur für den Flex 7500-Controller verfügbar und wird nur über die CLI unterstützt. Dieser Modus löst Änderungen an allen angeschlossenen APs aus. Es wird empfohlen, Flex 7500 in einer anderen Mobilitätsdomäne als die vorhandenen WLC-Campus-Controller bereitzustellen, bevor Sie diese CLI aktivieren:

```
(Cisco Controller) >config ap autoconvert ?

disable         Disables auto conversion of unsupported mode APs to supported
                  modes when AP joins
flexconnect     Converts unsupported mode APs to flexconnect mode when AP joins
monitor         Converts unsupported mode APs to monitor mode when AP joins

(Cisco Controller) >
```

1. Die Funktion für die automatische Konvertierung ist standardmäßig deaktiviert. Sie kann mithilfe des folgenden Befehls **show** überprüft werden:

   ```
   (Cisco Controller) >show ap autoconvert

   AP Autoconvert ..................................... Disabled
   ```

   Nicht unterstützte AP-Modi = Lokaler Modus, Sniffer, Rogue Detector und



Bridge. Diese Option ist derzeit nur über CLIs verfügbar.Diese CLIs sind nur auf dem WLC 7500 verfügbar.

2. Die **Flexconnect** CLI-CLI **mit** automatischer **Konfigurationskonvertierung** konvertiert alle APs im Netzwerk mit nicht unterstütztem AP-Modus in den FlexConnect-Modus. APs, die sich bereits in FlexConnect oder im Überwachungsmodus befinden, sind nicht betroffen.

```
(Cisco Controller) >config ap autoconvert flexconnect


(Cisco Controller) >show ap autoconvert

AP Autoconvert ................................ FlexConnect

(Cisco Controller) >
```

3. Die CLI des **Monitor** für die automatische **Konfigurationskonvertierung** konvertiert alle APs im Netzwerk mit nicht unterstütztem AP-Modus in Überwachungsmodus. APs, die sich bereits in FlexConnect oder im Überwachungsmodus befinden, sind nicht betroffen.

```
(Cisco Controller >config ap autoconvert monitor


(Cisco Controller) >show ap autoconvert

AP Autoconvert ................................ Monitor
```

Es gibt keine Option, sowohl **config ap autokonvertflexconnect** als auch **config ap autoConverter Monitor** gleichzeitig auszuführen.

FlexConnect WGB/uWGB-Unterstützung für lokale Switching-WLANs

Ab Version 7.3 werden WGB/uWGB- und kabelgebundene/Wireless-Clients hinter WGBs unterstützt und funktionieren als normale Clients auf WLANs, die für lokales Switching konfiguriert sind.

Nach der Zuordnung sendet die WGB die IAPP-Nachrichten für die einzelnen kabelgebundenen/Wireless-Clients, und der Flex AP verhält sich wie folgt:

- Wenn sich der Flex AP im Modus "Connected" (Verbindung) befindet, werden alle IAPP-Nachrichten an den Controller weitergeleitet, und der Controller verarbeitet die IAPP-Nachrichten wie AP im lokalen Modus. Der Datenverkehr für kabelgebundene/Wireless-Clients wird lokal von Flex APs umgeleitet.
- Wenn sich der Access Point im Standalone-Modus befindet, verarbeitet er die IAPP-Nachrichten, müssen kabelgebundene/Wireless-Clients im WGB registriert und die Registrierung aufheben können. Beim Wechsel in den Modus "Connected" sendet Flex AP die Informationen von kabelgebundenen Clients zurück an den Controller. WGB sendet dreimal Registrierungsnachrichten, wenn Flex AP vom Standalone- in den Connected-Modus

wechselt.

Kabelgebundene/Wireless-Clients erben die WGB-Konfiguration. Für Clients hinter dem WGB sind daher keine separaten Konfigurationen wie AAA-Authentifizierung, AAA-Override und FlexConnect-ACL erforderlich.

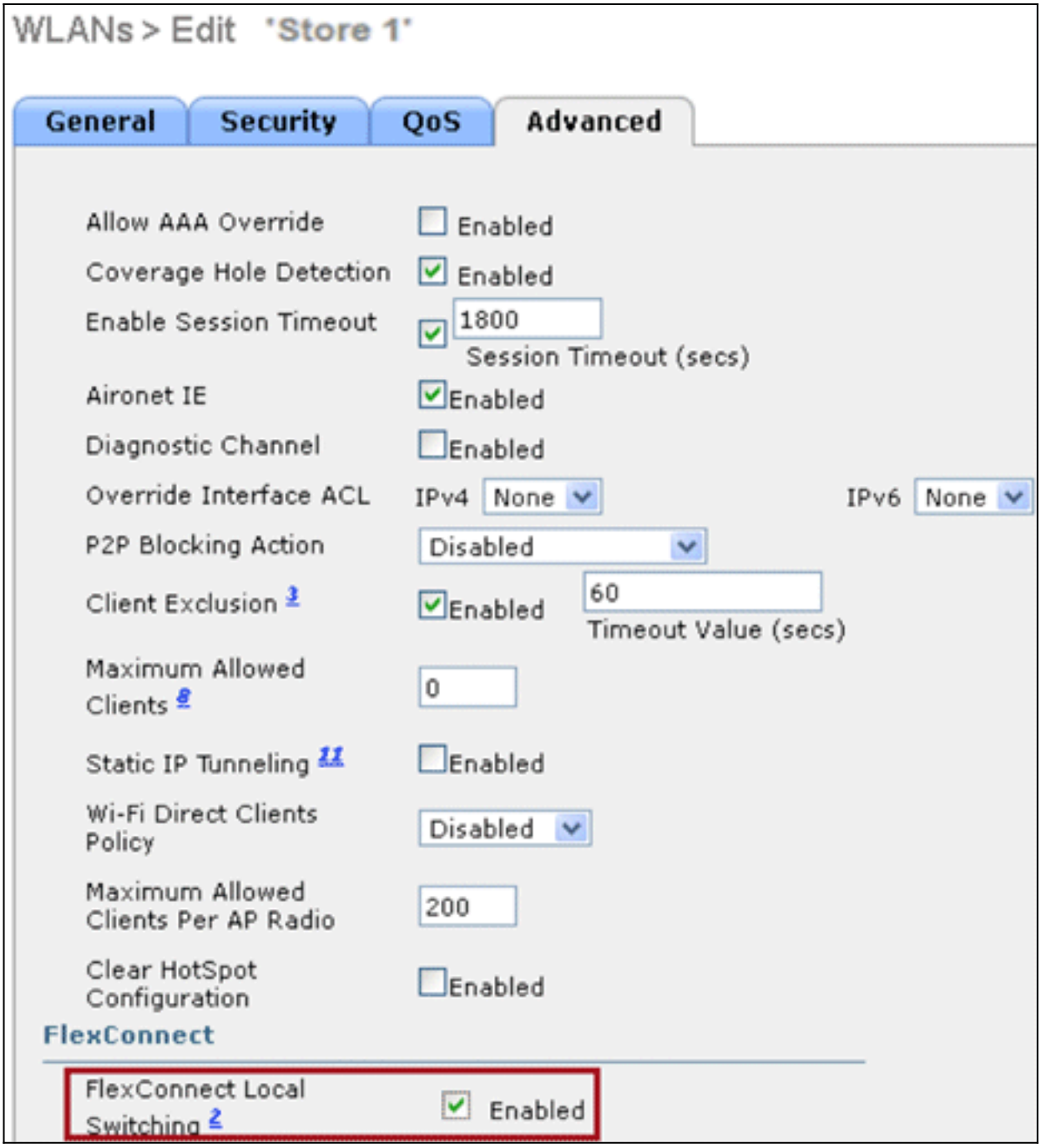
Zusammenfassung

- Für WLC ist keine spezielle Konfiguration erforderlich, um WGB auf Flex AP zu unterstützen.
- Fault Tolerance wird für WGB und Clients hinter WGB unterstützt.
- WGB wird von einem IOS AP unterstützt: 1240, 1130, 1140, 1260 und 1250.

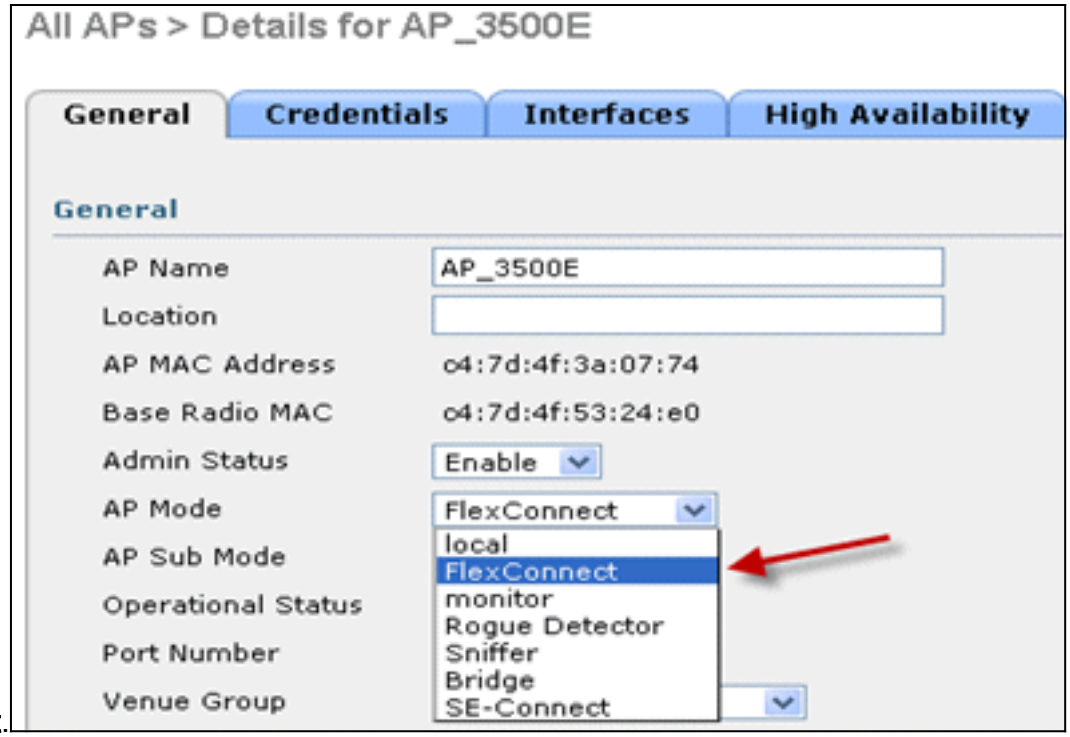
Vorgehensweise

Führen Sie diese Schritte aus:

1. Es ist keine spezielle Konfiguration erforderlich, um die WGB/uWGB-Unterstützung auf FlexConnect-APs für WLANs zu aktivieren, die für lokales Switching als WGB konfiguriert sind. Darüber hinaus werden Clients hinter dem WGB auf lokalen Switching-konfigurierten WLANs von Flex APs als normale Clients behandelt. Aktivieren Sie **FlexConnect Local Switching** in einem
   WLAN.



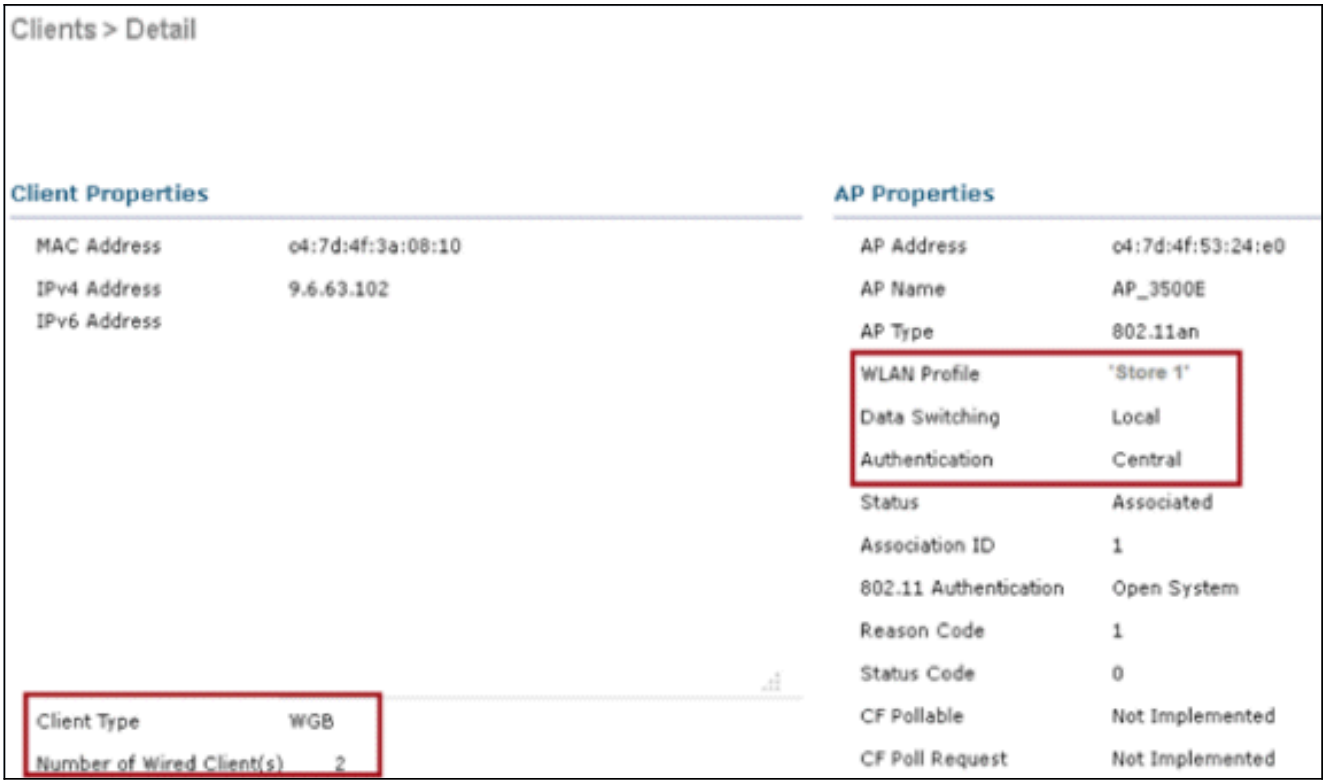
2. Legen Sie den AP-Modus auf **FlexConnect**



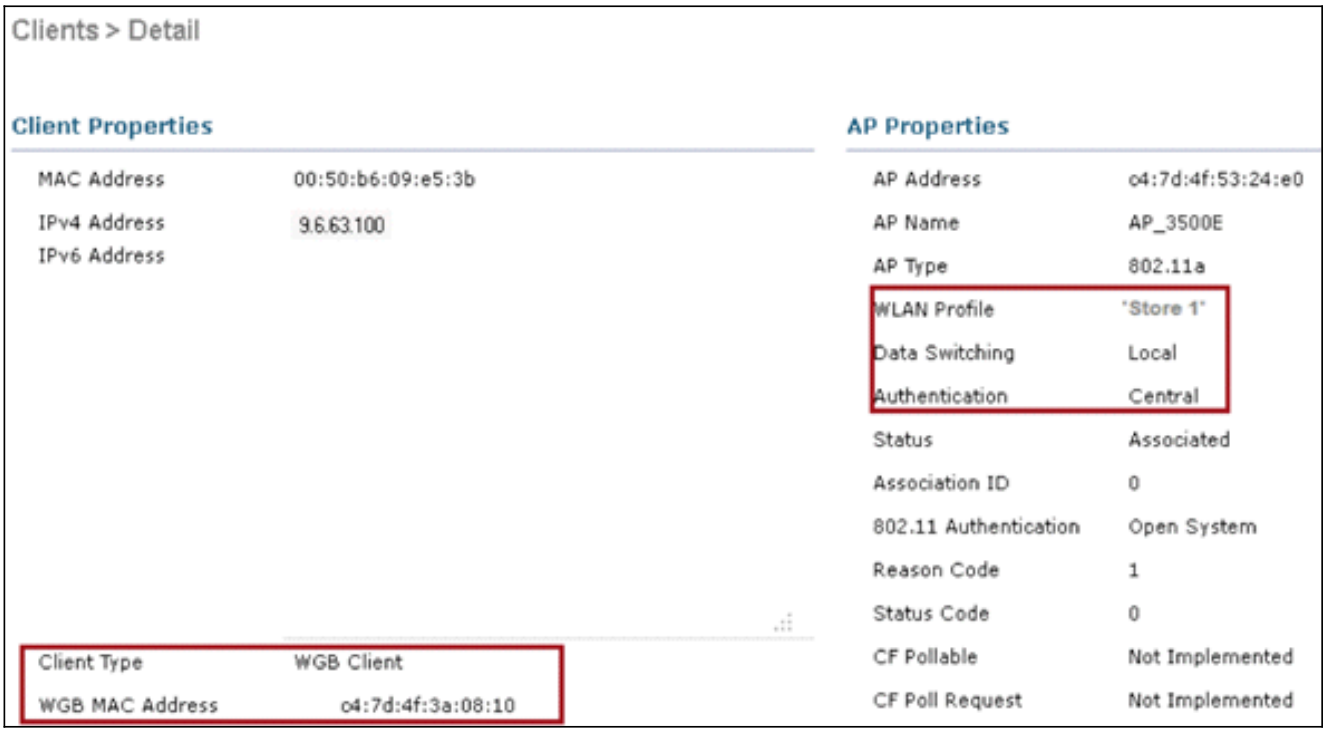
fest.

3. Verknüpfen Sie WGB mit kabelgebundenen Clients hinter diesem konfigurierten WLAN.

4. Um die Details für WGB zu überprüfen, gehen Sie zu **Monitor > Clients**, und wählen Sie **WGB** aus der Liste der Clients
aus.



5. Um die Details der kabelgebundenen/Wireless-Clients hinter dem WGB zu überprüfen, gehen Sie zu **Monitor > Clients**, und wählen Sie den Client aus.



Einschränkungen

- Kabelgebundene Clients hinter dem WGB befinden sich immer im selben VLAN wie das WGN selbst. Die Unterstützung mehrerer VLANs für Clients hinter WGB wird auf Flex AP für WLANs, die für lokales Switching konfiguriert sind, nicht unterstützt.
- Hinter dem WGB werden maximal 20 Clients (kabelgebunden/Wireless) unterstützt, wenn sie dem Flex AP im WLAN zugewiesen sind, das für lokales Switching konfiguriert wurde. Diese Nummer entspricht der aktuellen Anzahl für die WGB-Unterstützung auf dem AP im lokalen

Modus.
- Web-Auth wird nicht für Clients hinter WGB unterstützt, die in WLANs mit lokaler Switching-Konfiguration verknüpft sind.

Unterstützung einer höheren Anzahl von Radius-Servern

Vor Version 7.4 wurde die Konfiguration von RADIUS-Servern in der FlexConnect-Gruppe über eine globale Liste von RADIUS-Servern auf dem Controller vorgenommen. Die maximale Anzahl der RADIUS-Server, die in dieser globalen Liste konfiguriert werden können, beträgt 17. Angesichts der zunehmenden Anzahl von Zweigstellen muss pro Zweigstelle ein RADIUS-Server konfiguriert werden können. Ab Version 7.4 können Primär- und Backup-RADIUS-Server pro FlexConnect-Gruppe konfiguriert werden, die möglicherweise Teil der globalen Liste der 17 RADIUS-Authentifizierungsserver sind, die auf dem Controller konfiguriert sind.

Eine AP-spezifische Konfiguration für die RADIUS-Server wird ebenfalls unterstützt. Die AP-spezifische Konfiguration hat eine höhere Priorität als die FlexConnect-Gruppenkonfiguration.

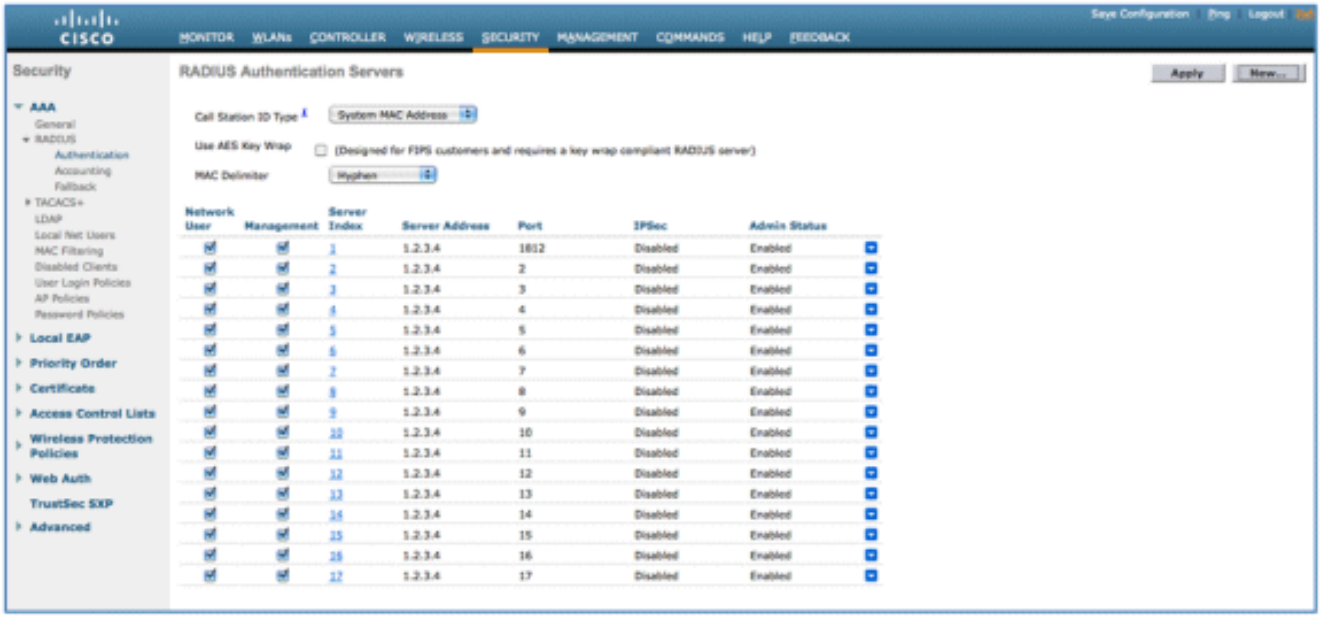
Der bestehende Konfigurationsbefehl in der FlexConnect-Gruppe, der den Index des RADIUS-Servers in der globalen RADIUS-Serverliste auf dem Controller benötigt, wird veraltet und durch einen Konfigurationsbefehl ersetzt, der einen RADIUS-Server in der Flexconnect-Gruppe mithilfe der IP-Adresse des Servers und des gemeinsam genutzten geheimen Codes konfiguriert.

Zusammenfassung

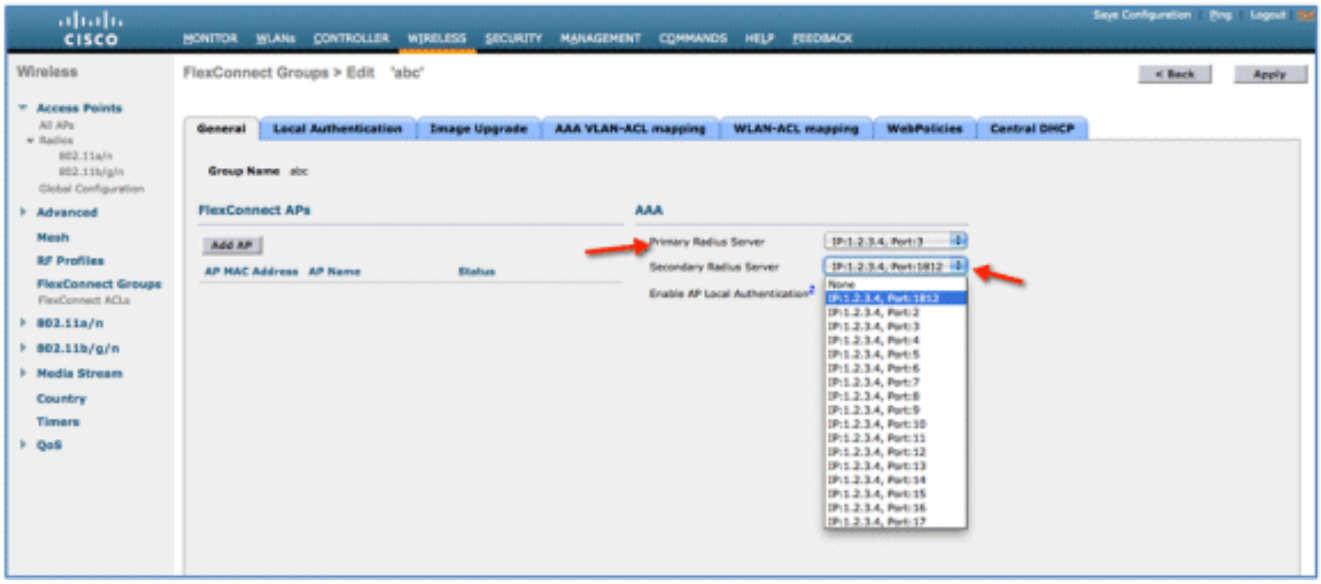
- Unterstützung für die Konfiguration von primären und Backup-RADIUS-Servern pro FlexConnect-Gruppe, die möglicherweise in der globalen Liste der RADIUS-Authentifizierungsserver vorhanden ist oder nicht.
- Die maximale Anzahl eindeutiger RADIUS-Server, die einem WLC hinzugefügt werden können, ist die Anzahl der FlexConnect-Gruppen, die auf einer bestimmten Plattform zweimal konfiguriert werden können. Ein Beispiel ist ein primärer und ein sekundärer RADIUS-Server pro FlexConnect-Gruppe.
- Ein Software-Upgrade von einer früheren Version auf Version 7.4 führt nicht zu einem Verlust der RADIUS-Konfiguration.
- Das Löschen des primären RADIUS-Servers ist zulässig, ohne dass der sekundäre RADIUS-Server gelöscht werden muss. Dies entspricht der aktuellen FlexConnect-Gruppenkonfiguration für den RADIUS-Server.

Vorgehensweise

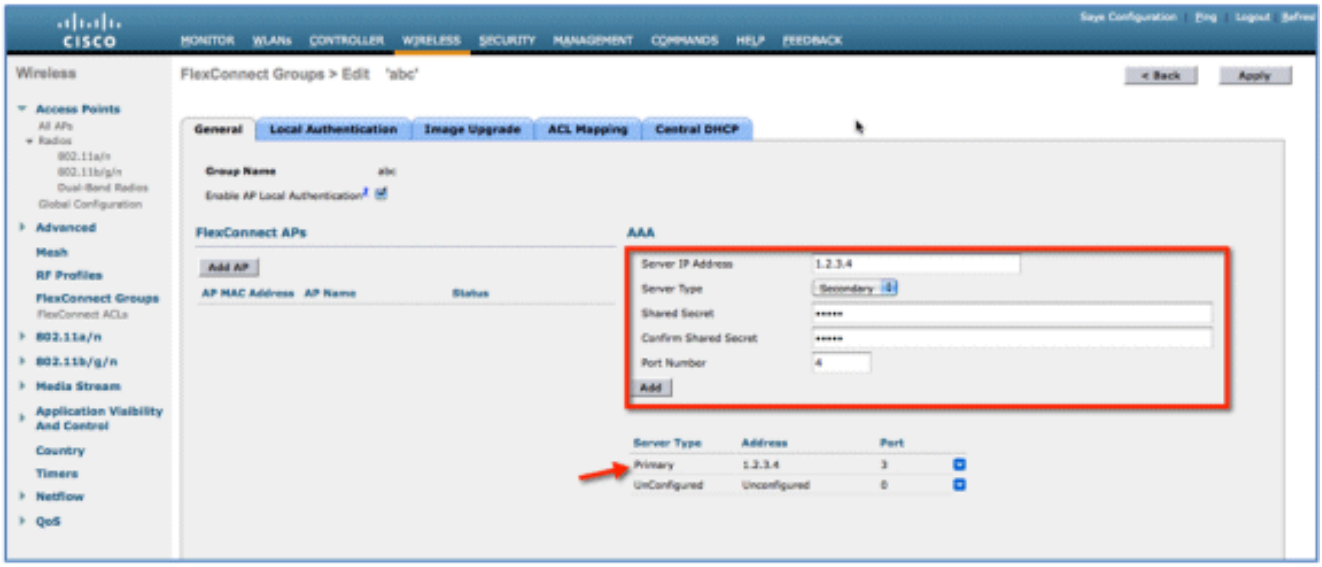
1. Konfigurationsmodus vor Version 7.4.In der AAA-Authentifizierungskonfiguration können maximal 17 RADIUS-Server konfiguriert
werden.



2. Primäre und sekundäre RADIUS-Server können einer FlexConnect-Gruppe mithilfe einer Dropdown-Liste zugeordnet werden, die aus RADIUS-Servern besteht, die auf der Seite "AAA Authentication" (AAA-Authentifizierung) konfiguriert sind.



3. Konfigurationsmodus bei der FlexConnect Group in Version 7.4.Primäre und sekundäre RADIUS-Server können unter der FlexConnect-Gruppe mithilfe einer IP-Adresse, Portnummer und eines Shared Secret konfiguriert werden.



Einschränkungen

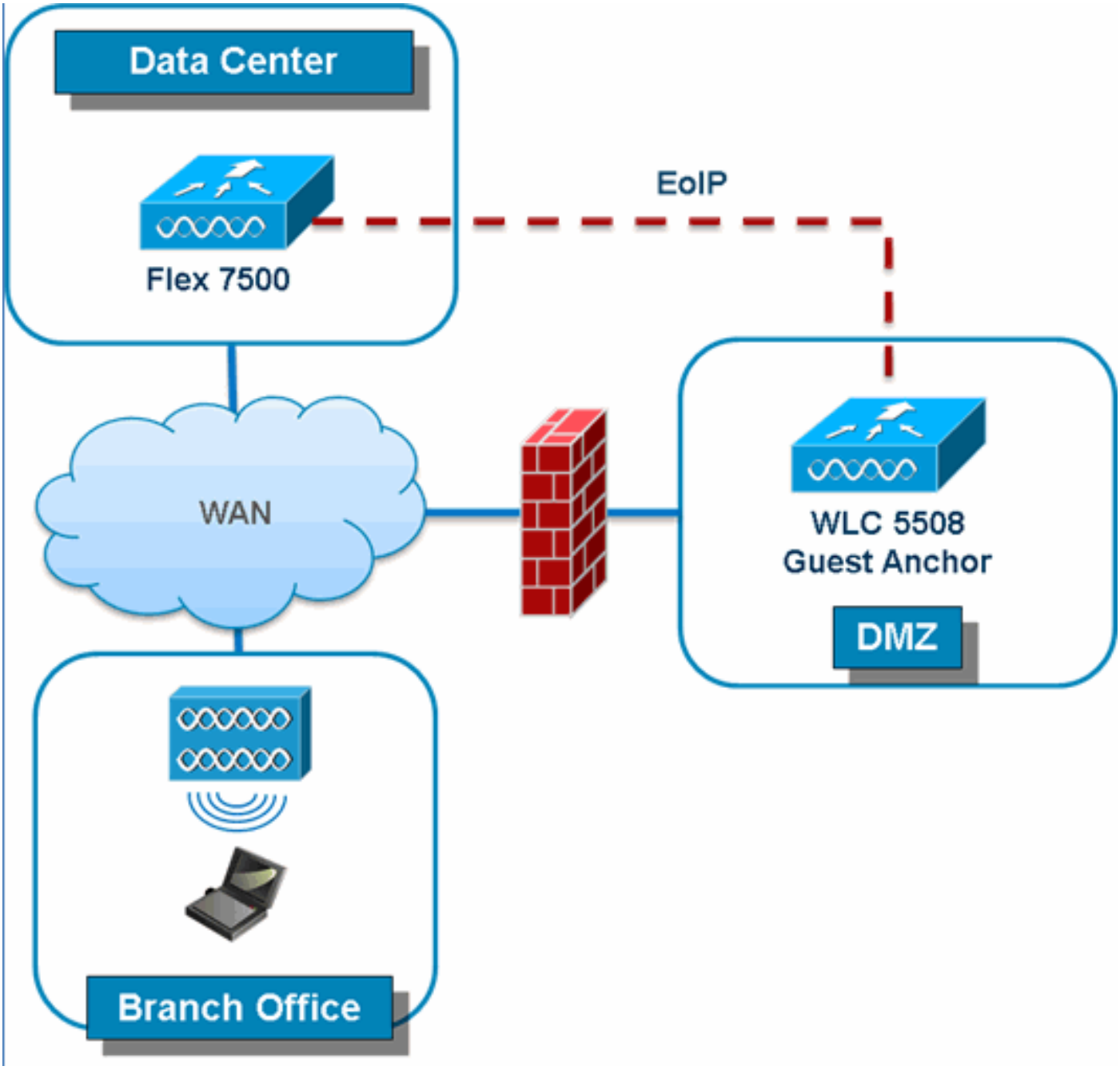
- Ein Software-Downgrade von Version 7.4 auf eine frühere Version behält die Konfiguration bei, jedoch mit einigen Einschränkungen.
- Wenn ein primärer/sekundärer RADIUS-Server konfiguriert wird, wird der ältere Eintrag durch den neuen ersetzt.

Enhanced Local Mode (ELM)

ELM wird von der FlexConnect-Lösung unterstützt. Weitere Informationen finden Sie im Leitfaden zu Best Practices für ELM.

Unterstützung für Gastzugriff in Flex 7500

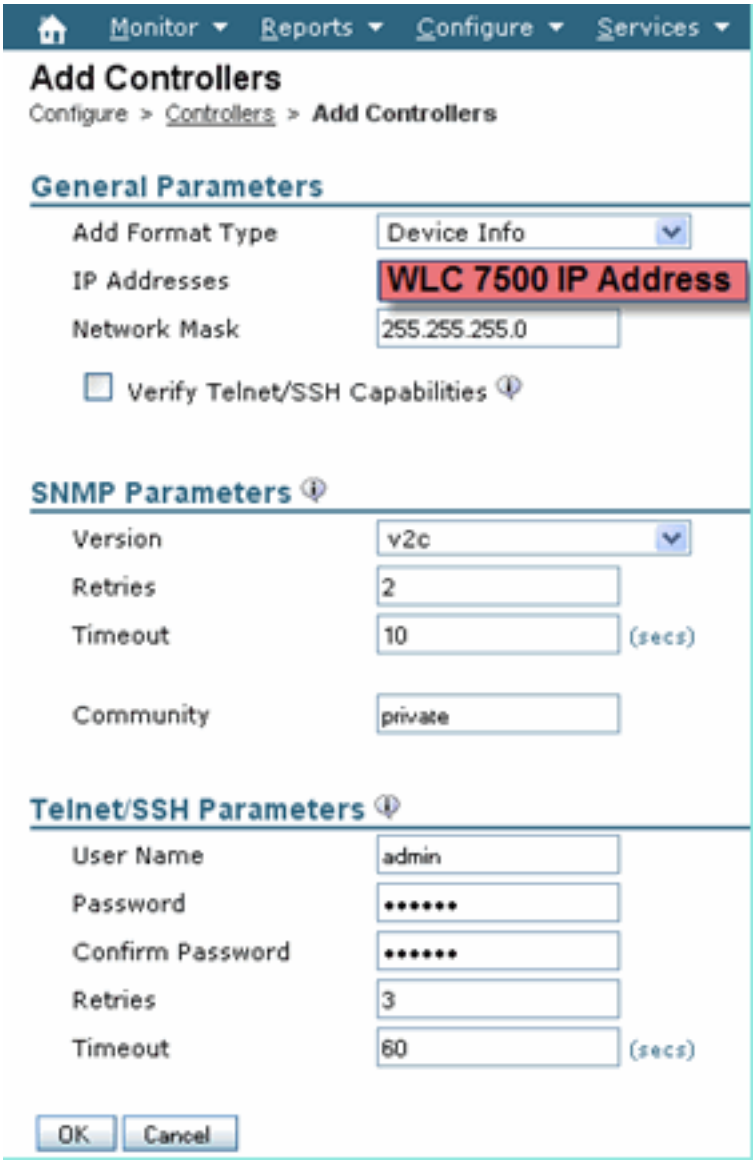
Abbildung 13: Unterstützung für Gastzugriff in Flex 7500



Flex 7500 ermöglicht und unterstützt weiterhin die Erstellung eines EoIP-Tunnels zu Ihrem Guest Anker Controller in der DMZ. Best Practices für die Wireless-Gastzugangslösung finden Sie im Bereitstellungsleitfaden für Gäste.

Verwalten des WLC 7500 vom NCS

Die Verwaltung des WLC7500 vom NCS ist identisch mit den vorhandenen WLCs von Cisco.



Weitere Informationen zum Verwalten von WLC und Ermitteln von Vorlagen finden Sie im Konfigurationshandbuch für Cisco Wireless Control System, Version 7.0.172.0.

Häufig gestellte Fragen

F. Wenn ich LAPs an einem Remote-Standort als FlexConnect konfiguriere, kann ich diesen LAPs dann einen primären und einen sekundären Controller zuweisen?

Beispiel: Ein primärer Controller ist an Standort A und ein sekundärer Controller an Standort B vorhanden. Wenn der Controller an Standort A ausfällt, führt die LAP ein Failover zum Controller an Standort B durch. Wenn beide Controller nicht verfügbar sind, fällt die LAP in den FlexConnect-Standalone-Modus?

Antwort: Ja. Zuerst fällt die LAP auf die Sekundäreinheit aus. Alle lokal geswitchten WLANs haben keine Änderungen, und bei allen zentral geswitchten WLANs wird nur der Datenverkehr an den

neuen Controller geleitet. Wenn das sekundäre Gerät ausfällt, bleiben alle WLANs, die für lokales Switching (und offene/Pre-Shared Key Authentication/Sie tun AP-Authentifizierer) markiert sind, aktiv.

F. Wie werden im lokalen Modus konfigurierte Access Points mit WLANs behandelt, die mit FlexConnect Local Switching konfiguriert wurden?

Antwort: Access Points im lokalen Modus behandeln diese WLANs als normale WLANs. Authentifizierung und Datenverkehr werden zurück zum WLC getunnelt. Bei einem Ausfall eines WAN-Links ist dieses WLAN vollständig ausgefallen, und in diesem WLAN sind keine Clients aktiv, bis die Verbindung zum WLC wiederhergestellt ist.

F. Kann ich Web-Authentifizierung mit lokalem Switching durchführen?

Antwort: Ja, Sie können eine SSID mit aktivierter Webauthentifizierung einrichten und den Datenverkehr nach der Webauthentifizierung lokal verwerfen. Die Webauthentifizierung mit lokalem Switching funktioniert einwandfrei.

F. Kann ich mein Gastportal auf dem Controller für eine SSID verwenden, die lokal vom H REAP verwaltet wird? Wenn ja, was geschieht, wenn die Verbindung zum Controller unterbrochen wird? Gehen aktuelle Clients sofort verloren?

Antwort: Ja. Da dieses WLAN lokal geswitcht ist, ist das WLAN verfügbar, aber keine neuen Clients können sich authentifizieren, da die Webseite nicht verfügbar ist. Die bestehenden Clients werden jedoch nicht verworfen.

F. Kann FlexConnect die PCI-Konformität zertifizieren?

Antwort: Ja. Die FlexConnect-Lösung unterstützt die Erkennung von unautorisierten Access Points, um die PCI-Konformität zu gewährleisten.

Zugehörige Informationen

- Designleitfaden für HREAP-Bereitstellung
- Cisco Wireless LAN Controller der Serie 4400
- Cisco Wireless LAN Controller der Serie 2000
- Cisco Wireless Control System
- Cisco Mobility Services Engine der Serie 3300
- Cisco Aironet Serie 3500
- Cisco Secure Access Control System
- Technischer Support und Dokumentation für Cisco Systeme