Guida all'installazione di Flex 7500 Wireless Branch Controller

Sommario

Introduzione

In questo documento viene descritto come distribuire un controller di filiale wireless Cisco Flex 7500. Il presente documento ha lo scopo di:

- Illustrare i vari elementi di rete della soluzione Cisco FlexConnect e il relativo flusso di comunicazione.
- Fornire linee guida generali per l'installazione della soluzione di filiali wireless Cisco FlexConnect.
- Illustrare le funzionalità software della versione 7.2.103.0 che rafforzano la base di informazioni sul prodotto.

Nota: prima della versione 7.2, FlexConnect era denominato Hybrid REAP (HREAP). Ora si chiama FlexConnect.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Panoramica del prodotto

Figura 1: Cisco Flex 7500

Cisco Flex serie 7500 Cloud Controller è un controller per filiali altamente scalabile per installazioni wireless multisito. Installato nel cloud privato, il controller Cisco Flex serie 7500

estende i servizi wireless alle filiali distribuite con controllo centralizzato che riduce il costo totale delle operazioni.

Cisco Flex serie 7500 (Figura 1) è in grado di gestire punti di accesso wireless in un massimo di 500 sedi distaccate e consente ai responsabili IT di configurare, gestire e risolvere problemi relativi a un massimo di 3000 punti di accesso (AP) e 30.000 client dal centro dati. Il controller Cisco Flex serie 7500 supporta l'accesso guest sicuro, il rilevamento rogue per la conformità PCI (Payment Card Industry) e la funzionalità voce e video Wi-Fi in-branch (commutazione locale).

Questa tabella evidenzia le differenze di scalabilità tra i controller Flex 7500, WiSM2 e WLC 5500:

Scalabilità	Flex 7500	WiSM2	WLC 5500
Totale Access Point	6,000	1000	500
Totale client	64,000	15,000	7,000
Numero massimo gruppi FlexConnect	2000	100	100
Numero massimo di access point per gruppo FlexConnect	100	25	25
Numero massimo gruppi di punti di accesso	6000	1000	500

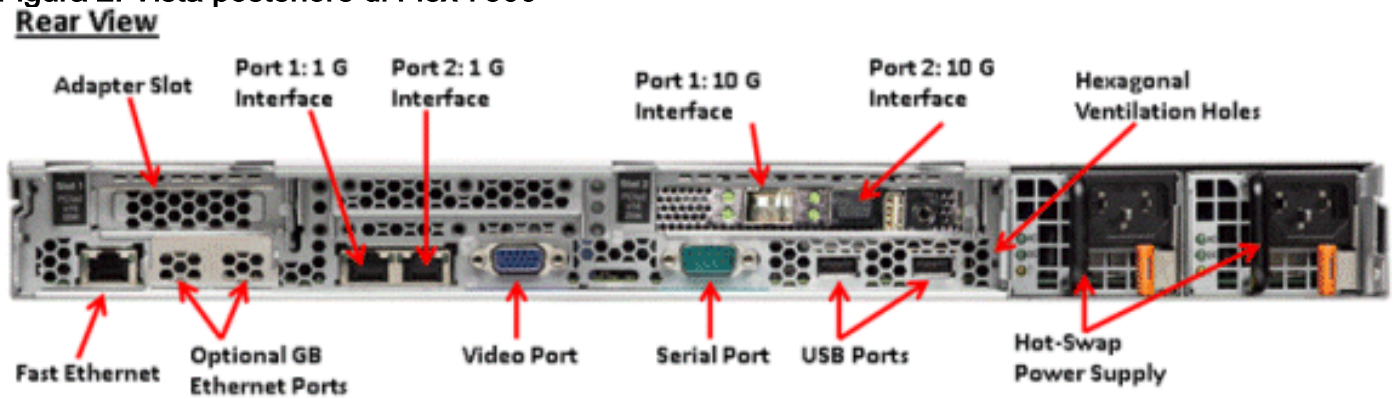
Specifiche del prodotto

Scheda tecnica

Fare riferimento a http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps11635/data_sheet_c78-650053.html.

Funzione piattaforma

Figura 2: Vista posteriore di Flex 7500



Porte di interfaccia di rete

Porte di interfaccia	Utilizzo
Fast Ethernet	Modulo di gestione integrato (IMM)

Porta 1: 1G	Porta servizio WLC
Porta 2: 1G	Porta ridondante WLC (RP)
Porta 1: 10 G	Interfaccia di gestione WLC
Porta 2: 10 G	Porta interfaccia di gestione backup WLC (errore porta)
Porte Gb Ethernet opzionali	N/D

Nota:

- Il supporto LAG per interfacce 2x10G consente il funzionamento del collegamento attivo-attivo con ridondanza del collegamento di failover rapido. Un collegamento 10G aggiuntivo attivo con LAG non modifica il throughput wireless del controller.
- Interfacce 2x10G
- Le interfacce 2x10G supportano solo cavi in fibra ottica con il numero di prodotto SFP-10G-SR.
- Switch side SFP n. 2-10GB-SR

Indirizzi MAC di sistema

Porta 1: 10G (interfaccia di gestione)	Indirizzo MAC di sistema/base
Porta 2: 10G(Interfaccia Di Gestione Dei Backup)	Indirizzo MAC di base + 5
Porta 1: 1G (porta servizio)	Indirizzo MAC di base + 1
Porta 2: 1G (porta ridondante)	Indirizzo MAC di base + 3

Reindirizzamento console seriale

Per impostazione predefinita, il WLC 7500 consente il reindirizzamento della console alla velocità in baud di 9600, simulando il terminale Vt100 senza controllo del flusso.

Informazioni sull'inventario

Figura 3: Console WLC 7500

```
(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
```

La tabella DMI (Desktop Management Interface) contiene informazioni sull'hardware del server e sul BIOS.

Il WLC 7500 visualizza la versione del BIOS, il PID/VID e il numero di serie come parte

dell'inventario.

Avvio di Flex 7500

Le opzioni del bootloader Cisco per la manutenzione del software sono identiche a quelle dei controller Cisco esistenti.

Figura 4: Ordine di avvio

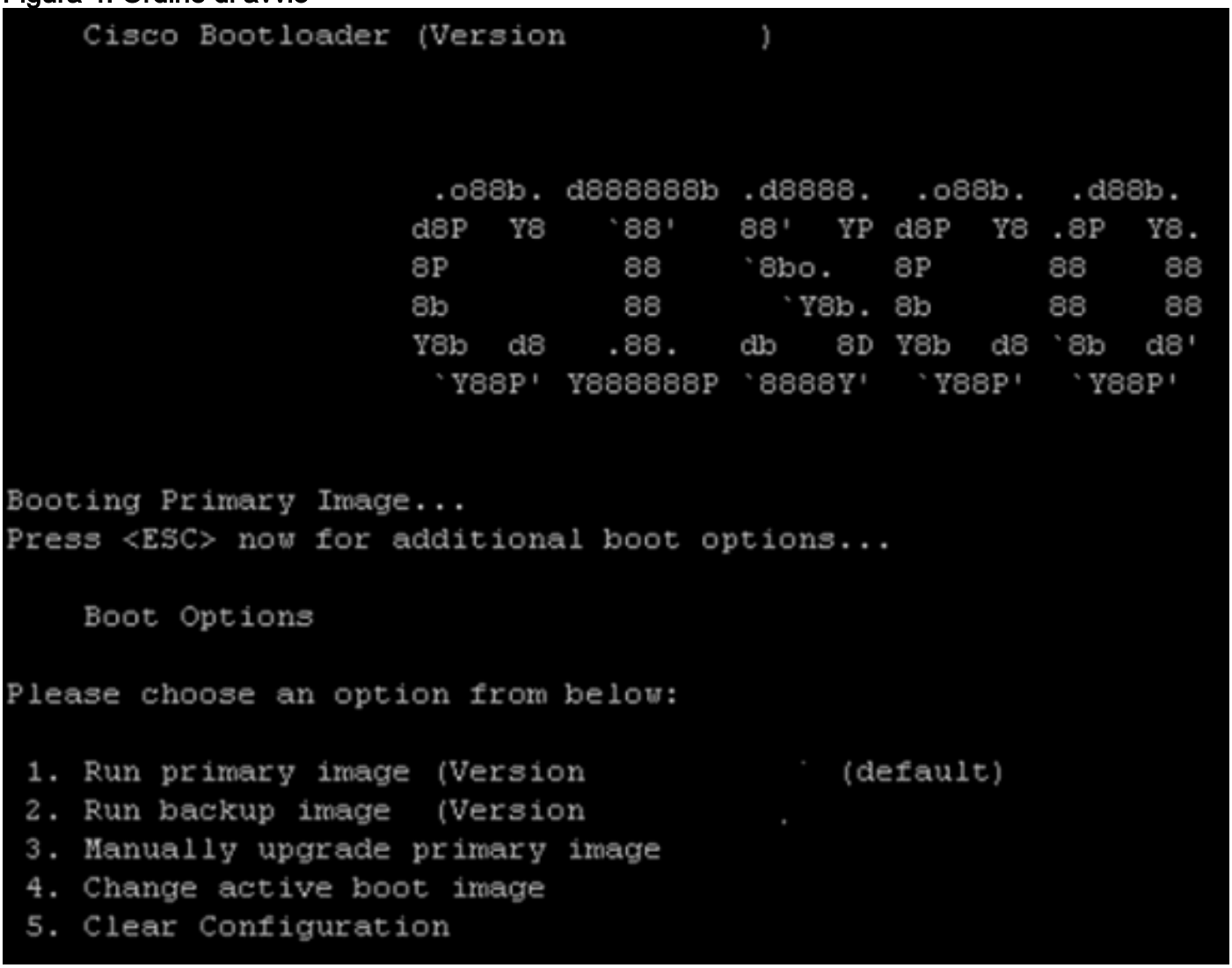


Figura 5: Configurazione guidata WLC

```
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
```


Nota: la sequenza di avvio di Flex 7500 è equivalente e coerente con le piattaforme controller esistenti. L'avvio iniziale richiede la configurazione WLC mediante la procedura guidata.

Licenze Flex 7500

Conteggio base licenze AP

SKU conteggio base AP
300

500
1000
2000
3000
6000

Licenze di aggiornamento AP

SKU di aggiornamento AP
100
250
500
1000

Ad eccezione del numero di base e degli aggiornamenti, l'intera procedura di licenza che copre l'ordine, l'installazione e la visualizzazione è simile alla licenza Cisco WLC 5508 esistente.

Fare riferimento alla guida alla configurazione del WLC 7.3, che descrive l'intera procedura di licenza.

Supporto per le versioni software

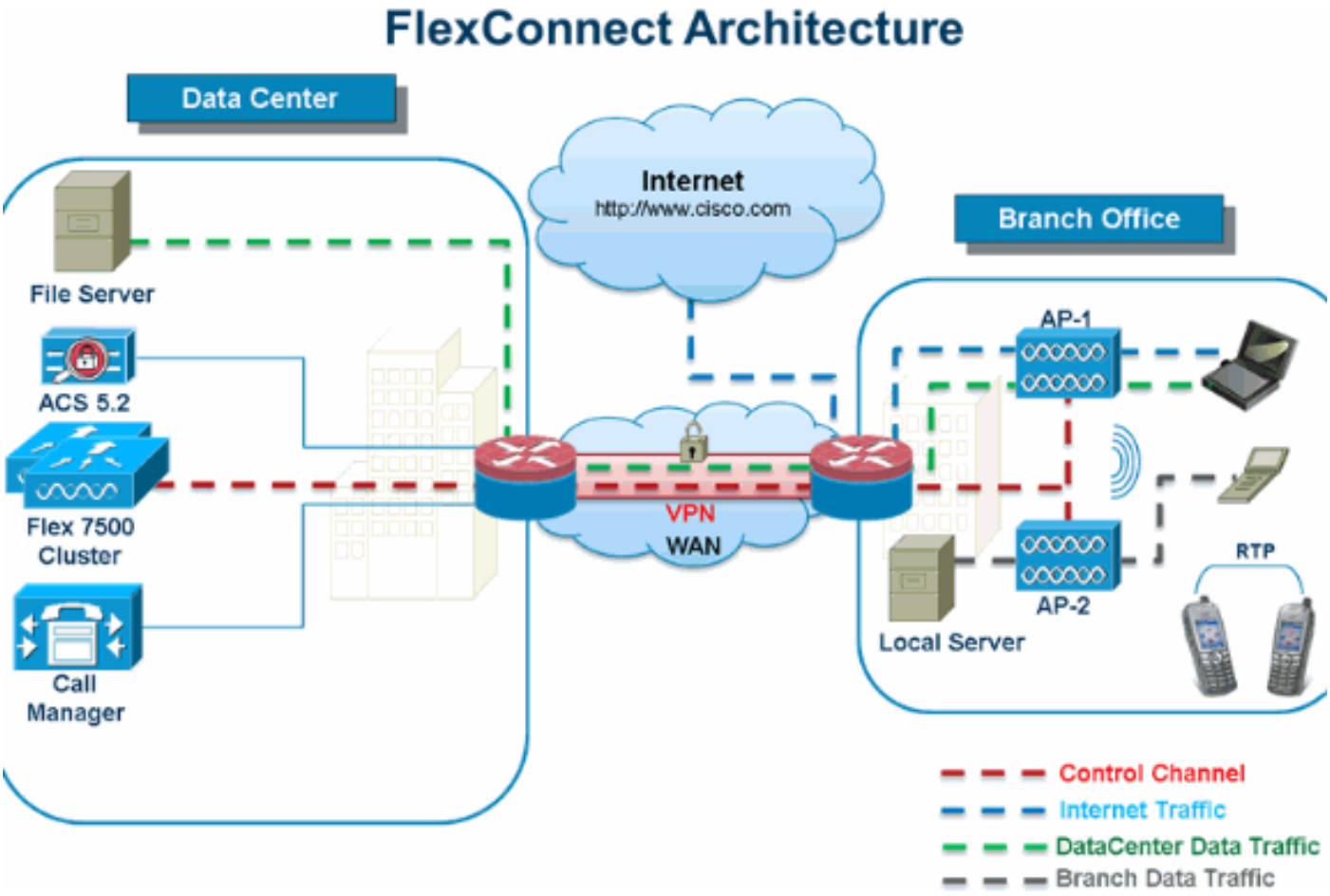
Flex 7500 supporta solo il codice WLC versione 7.0.116.x e successive.

Access point supportati

Flex 7500 supporta i punti di accesso 1040, 1130, 1140, 1550, 3500, 3600, 2600, 1250, 1260, 1240, OEAP 600, ISR 891 e ISR 881.

Architettura FlexConnect

Figura 6: Topologia tipica delle filiali wireless



FlexConnect è una soluzione wireless per le installazioni di filiali e uffici remoti. Viene anche definita una soluzione Hybrid REAP, ma nel presente documento verrà indicata come FlexConnect.

La soluzione FlexConnect consente al cliente di:

- Centralizzare il traffico di controllo e gestione dei punti di accesso dal centro dati.Il traffico di controllo è contrassegnato da trattini rossi nella Figura 6.
- Distribuire il traffico di dati client in ogni succursale.Il traffico di dati è contrassegnato da trattini blu, verdi e viola nella Figura 6.Ogni flusso di traffico raggiunge la destinazione finale nel modo più efficiente.

Vantaggi della centralizzazione del traffico di controllo dei punti di accesso

- Singolo riquadro di monitoraggio e risoluzione dei problemi
- Facilità di gestione
- Accesso sicuro e senza problemi alle risorse del centro dati
- Riduzione dell'ingombro delle filiali
- Aumento del risparmio operativo

Vantaggi della distribuzione del traffico di dati dei client

- Nessun tempo di inattività operativo (possibilità di sopravvivenza) a causa di guasti completi del collegamento WAN o indisponibilità del controller
- Resilienza della mobilità all'interno della filiale in caso di guasto del collegamento WAN

- Aumento della scalabilità delle filiali. Supporta diramazioni con scalabilità fino a 100 punti di accesso e 250.000 piedi quadrati (5.000 mq) per punto di accesso).

La soluzione Cisco FlexConnect supporta anche il traffico dati del client centrale, ma deve essere limitata solo al traffico dati del guest. Nella tabella seguente vengono descritte le restrizioni relative ai tipi di sicurezza L2 della WLAN solo per i client non guest il cui traffico di dati viene commutato centralmente nel data center.

Supporto della sicurezza L2 per utenti non guest con commutazione centrale

Sicurezza WLAN L2	Tipo	Risultato
Nessuna	N/D	Consentito
WPA + WPA2	802.1x	Consentito
	CCKM	Consentito
	802.1x + CCKM	Consentito
	PSK	Consentito
802.1x	WEP	Consentito
WEP statico	WEP	Consentito
WEP + 802.1x	WEP	Consentito
CKIP		Consentito

Nota: queste restrizioni di autenticazione non si applicano ai client il cui traffico di dati viene distribuito nella filiale.

Supporto della sicurezza L3 per utenti con switching centrale e locale

Sicurezza WLAN L3	Tipo	Risultato
Autenticazione Web	Interno	Consentito
	Esterna	Consentito
	Personalizzato	Consentito
Pass-through Web	Interno	Consentito
	Esterna	Consentito
	Personalizzato	Consentito
Reindirizzamento Web condizionale	Esterna	Consentito
Reindirizzamento Web pagina iniziale	Esterna	Consentito

Per ulteriori informazioni sulla distribuzione di Flexconnect WebAuth esterna, consultare la guida alla distribuzione di Flexconnect WebAuth esterna

Per ulteriori informazioni sugli stati dei punti di accesso HREAP/FlexConnect e sulle opzioni di commutazione del traffico dati, consultare il documento sulla configurazione di FlexConnect.

Modalità operative di FlexConnect

Modalità	Descrizione

FlexConnect	
Connesso	Un FlexConnect è impostato in modalità connessa quando il control plane CAPWAP che riporta al controller è attivo e operativo, ovvero il collegamento WAN non è inattivo.
Indipendente	La modalità standalone è specificata come stato operativo in cui FlexConnect entra quando non ha più la connettività con il controller. I punti di accesso FlexConnect in modalità standalone continueranno a funzionare con l'ultima configurazione nota, anche in caso di interruzione dell'alimentazione e guasto del WLC o della WAN.

Per ulteriori informazioni sulla teoria delle operazioni di FlexConnect, consultare la guida alla progettazione e all'installazione di H-Reap / FlexConnect.

Requisiti WAN

Gli access point FlexConnect vengono implementati sul sito della filiale e gestiti dal centro dati su un collegamento WAN. Si consiglia di mantenere la limitazione della larghezza di banda minima a 12,8 kbps per access point con una latenza di andata e ritorno non superiore a 300 ms per le distribuzioni di dati e a 100 ms per le distribuzioni di dati e voce. L'MTU (Maximum Transmission Unit) deve essere almeno di 500 byte.

Tipo di distribuzione	Larghezza di banda WAN (min)	Latenza WAN RTT (max)	Numero massimo di punti di accesso per filiale	Numero massimo client per filiale
Dati	64 kbps	300 ms	5	25
Dati + voce	128 kbps	100 ms	5	25
Monitor (Monitora)	64 kbps	2 sec.	5	N/D
Dati	640 kbps	300 ms	50	1000
Dati + voce	1.44 Mbps	100 ms	50	1000
Monitor (Monitora)	640 kbps	2 sec.	50	N/D

Progettazione della rete di filiali wireless

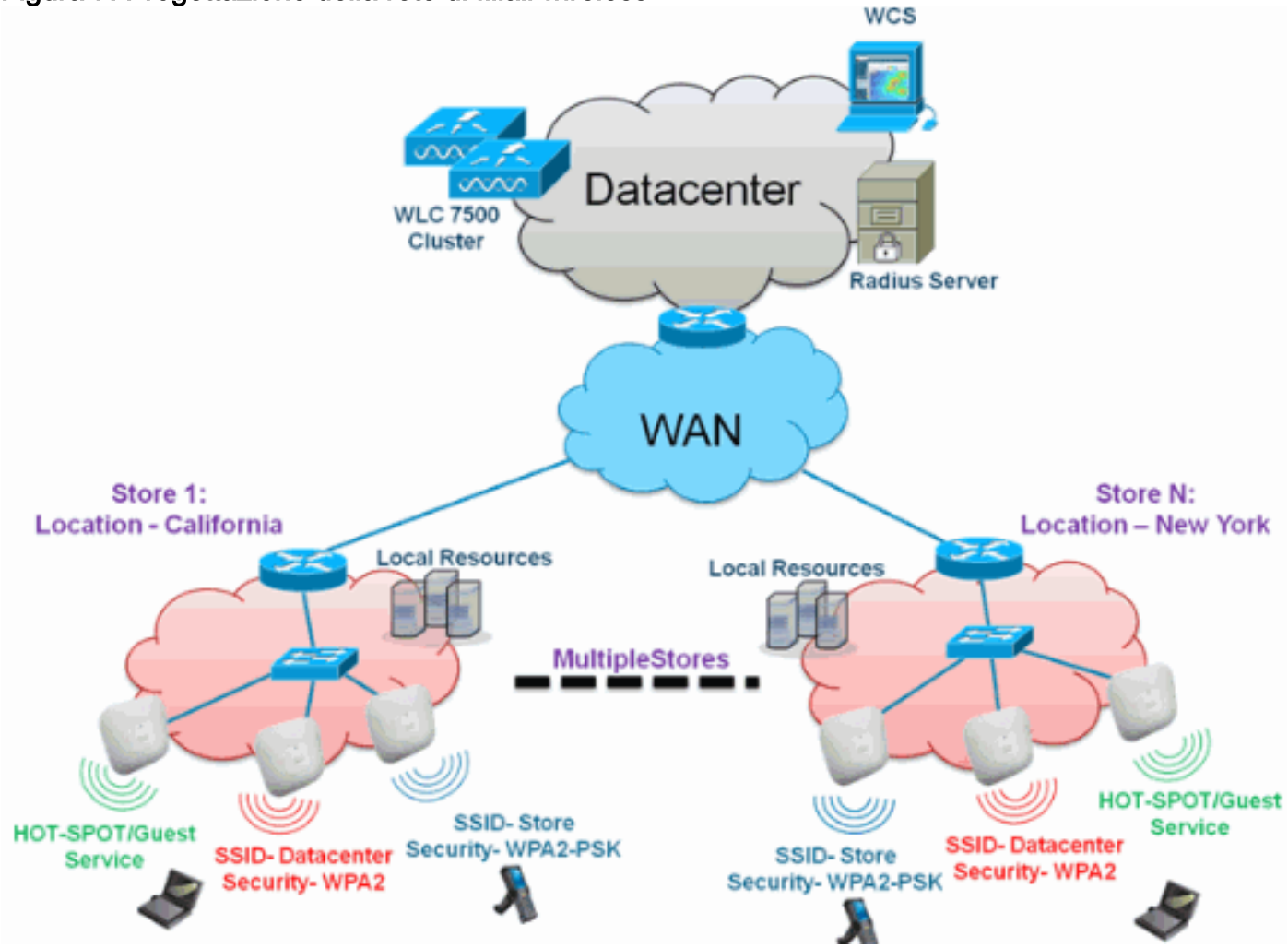
Nel prosieguo del documento vengono evidenziate le linee guida e descritte le best practice per l'implementazione di reti di filiali distribuite protette. L'architettura FlexConnect è consigliata per

reti di filiali wireless che soddisfano questi requisiti di progettazione.

Requisiti principali di progettazione

- Dimensioni della diramazione scalabili fino a 100 punti di accesso e 250.000 piedi quadrati (5.000 mq) piedi per access point)
- Gestione centralizzata e risoluzione dei problemi
- Nessun tempo di inattività operativo
- Segmentazione del traffico basata su client
- Connettività wireless perfetta e sicura per le risorse aziendali
- Compatibile con PCI
- Supporto per gli ospiti

Figura 7: Progettazione della rete di filiali wireless



Panoramica

Per i clienti delle filiali è sempre più difficile e costoso offrire servizi di rete scalabili e sicuri completi di ogni funzione in più aree geografiche. Per supportare i clienti, Cisco sta affrontando queste sfide introducendo Flex 7500.

La soluzione Flex 7500 virtualizza le complesse operazioni di sicurezza, gestione, configurazione e risoluzione dei problemi all'interno del centro dati e quindi estende in modo trasparente tali servizi a ciascuna filiale. Le installazioni con Flex 7500 sono più facili da configurare, gestire e, soprattutto, scalare per l'IT.

Vantaggi

- Maggiore scalabilità con il supporto di 6000 AP
- Maggiore resilienza con FlexConnect Fault Tolerance
- Aumento della segmentazione del traffico con FlexConnect (switching centrale e locale)
- Facilità di gestione grazie alla replica dei progetti di archivio tramite i gruppi AP e i gruppi FlexConnect.

Caratteristiche per la progettazione di reti di filiali

Le altre sezioni della guida illustrano l'utilizzo delle funzionalità e i consigli per realizzare il progetto di rete mostrato nella Figura 7.

Caratteristiche:

Caratteristiche principali	Caratteristiche
Gruppi di AP	Semplifica le operazioni e la gestione durante la gestione di più sedi distaccate. Offre inoltre la flessibilità di replicare le configurazioni per siti di succursale simili.
Gruppi FlexConnect	I gruppi FlexConnect offrono le funzionalità di backup locale Radius, roaming veloce CCKM/OKC e autenticazione locale.
Fault Tolerance	Migliora la resilienza delle filiali wireless e non fornisce downtime operativi.
ELM (Enhanced Local Mode for Adaptive wIPS)	Funzionalità wIPS adattiva per servire i client senza alcun impatto sulle prestazioni.
Limite client per WLAN	Limitazione del totale di client guest nella rete di succursale.
Download pre-immagine AP	Riduce i tempi di inattività durante l'aggiornamento della filiale.
Conversione automatica punti di accesso in FlexConnect	Funzionalità per la conversione automatica degli access point in FlexConnect per la filiale.
Accesso guest	Continuare l'architettura Cisco Guest Access con FlexConnect.

Matrice di supporto IPv6

Caratteristic	Commutazione	Commutazione

he	centrale		locale	
	5500 / WiSM-2	Flex 7500	5500 / WiSM-2	Flex 7500
IPv6 (mobilità client)	Supportato	Non supportato	Non supportato	Non supportato
Protezione RA IPv6	Supportato	Supportato	Supportato	Supportato
Protezione DHCP IPv6	Supportato	Non supportato	Non supportato	Non supportato
Protezione origine IPv6	Supportato	Non supportato	Non supportato	Non supportato
Limitazione RA / Limite di velocità	Supportato	Non supportato	Non supportato	Non supportato
ACL IPv6	Supportato	Non supportato	Non supportato	Non supportato
Visibilità client IPv6	Supportato	Non supportato	Non supportato	Non supportato
Cache di individuazione router adiacenti IPv6	Supportato	Non supportato	Non supportato	Non supportato
Bridging IPv6	Supportato	Non supportato	Supportato	Supportato

Matrice

Per una matrice delle caratteristiche della funzione FlexConnect, consultare il documento sulla matrice delle caratteristiche di FlexConnect.

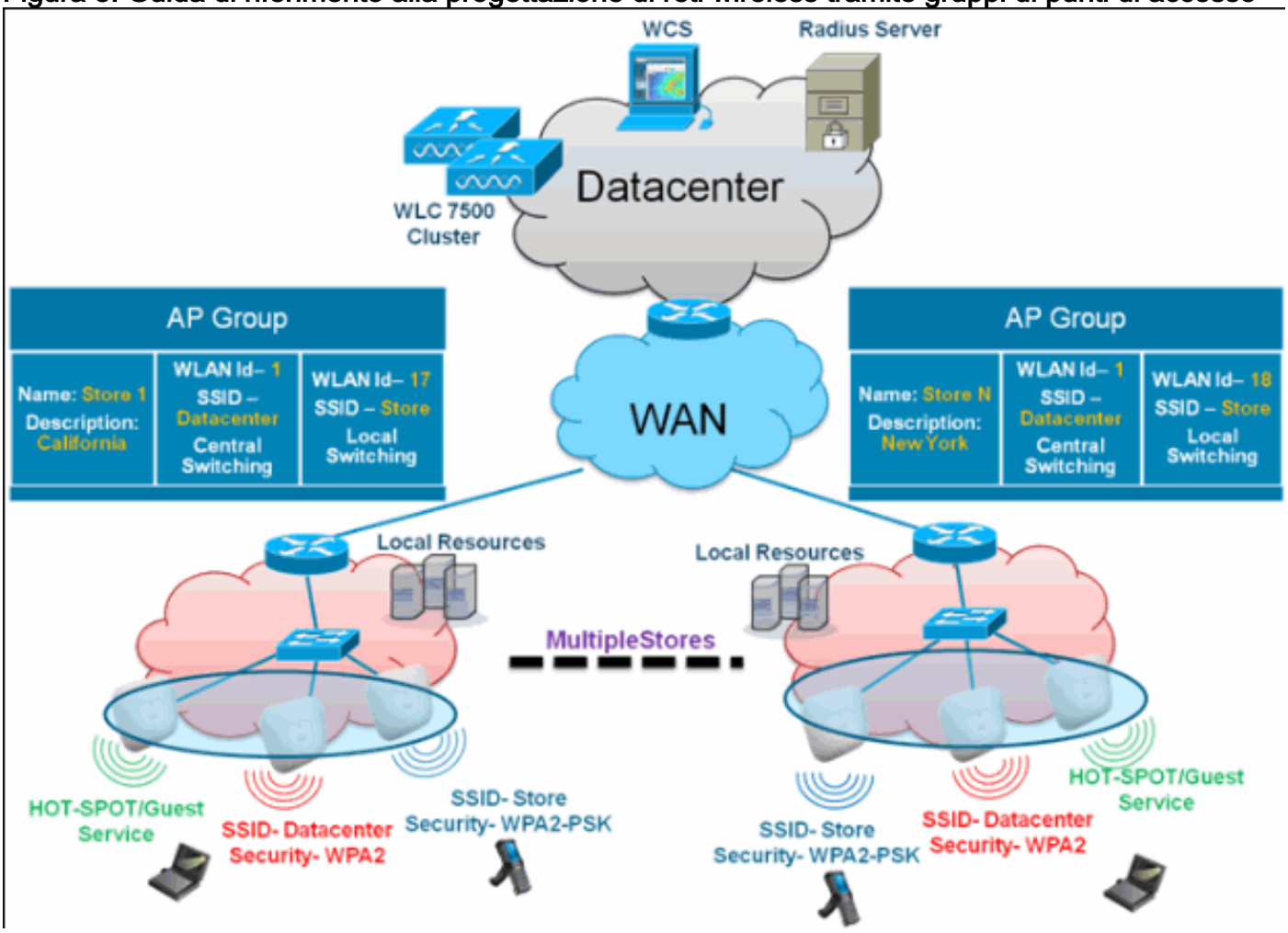
Gruppi di AP

Dopo aver creato le WLAN sul controller, è possibile pubblicarle in modo selettivo (utilizzando i gruppi di punti di accesso) su punti di accesso diversi per gestire meglio la rete wireless. In un'implementazione tipica, tutti gli utenti di una WLAN sono mappati su un'unica interfaccia sul controller. Pertanto, tutti gli utenti associati alla WLAN si trovano sulla stessa subnet o VLAN. È tuttavia possibile scegliere di distribuire il carico tra più interfacce o a un gruppo di utenti in base a criteri specifici, ad esempio singoli reparti (marketing, progettazione o operazioni), creando gruppi di punti di accesso. Inoltre, questi gruppi di punti di accesso possono essere configurati in VLAN separate per semplificare l'amministrazione della rete.

In questo documento vengono usati i gruppi di punti di accesso per semplificare l'amministrazione della rete quando si gestiscono più archivi in diverse aree geografiche. Per facilitare le operazioni, il documento crea un gruppo di punti di accesso per punto vendita per soddisfare i seguenti requisiti:

- Switched centralizzato SSID **Datacenter** in tutti gli archivi per l'accesso amministrativo di Local Store Manager.
- **Archivio** SSID commutato localmente con chiavi WPA2-PSK diverse in tutti gli archivi per gli scanner palmari.

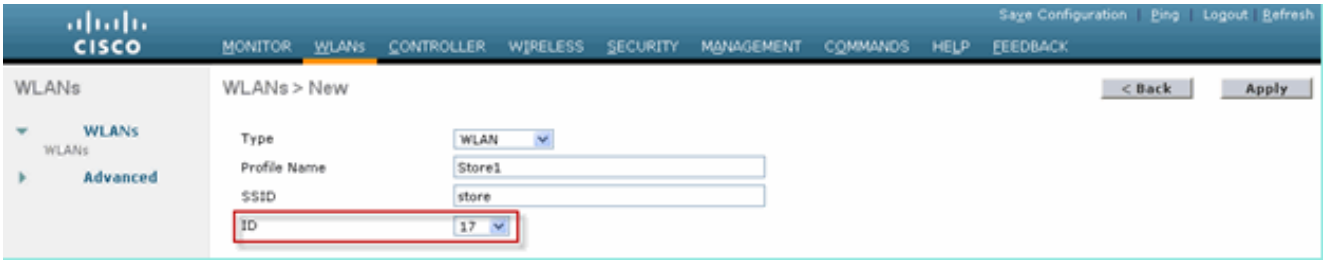
Figura 8: Guida di riferimento alla progettazione di reti wireless tramite gruppi di punti di accesso



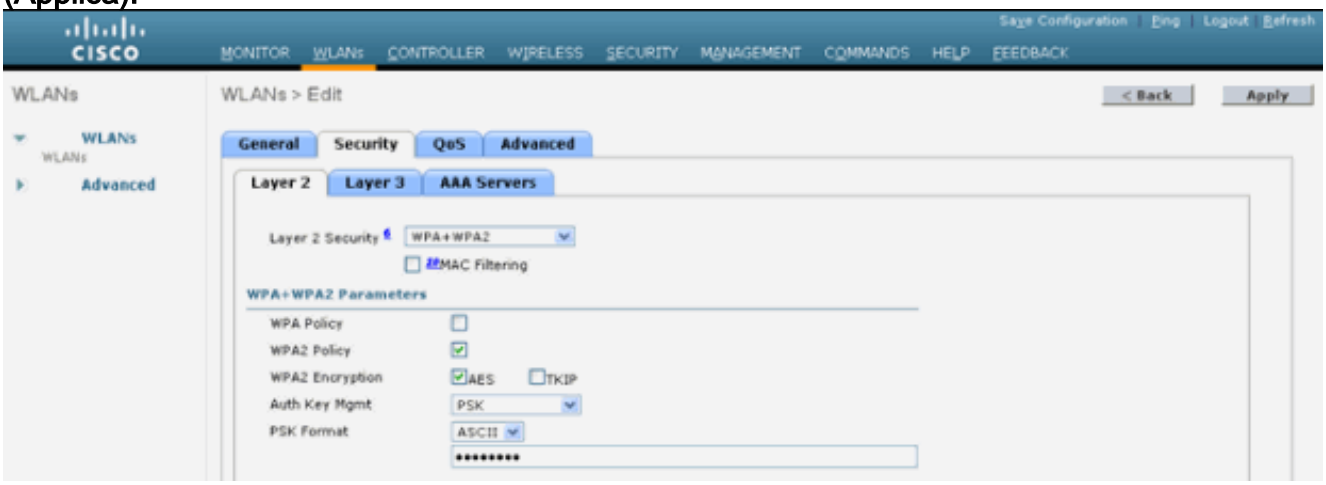
Configurazioni da WLC

Attenersi alla seguente procedura:

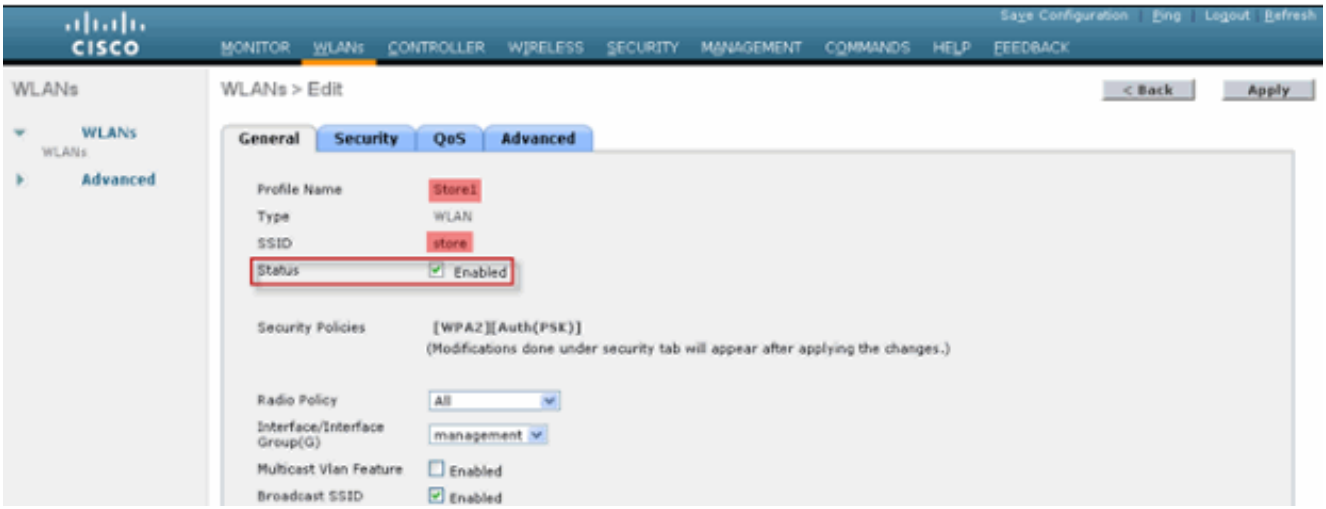
1. Nella pagina WLAN > Nuovo, immettere **Store1** nel campo Nome profilo, immettere **store** nel campo SSID e scegliere **17** dall'elenco a discesa ID.**Nota:** gli ID WLAN da 1 a 16 fanno parte del gruppo predefinito e non possono essere eliminati. Per soddisfare il requisito di utilizzare lo stesso punto vendita SSID per negozio con una diversa chiave WPA2-PSK, è necessario utilizzare l'ID WLAN 17 e versioni successive perché non fanno parte del gruppo predefinito e possono essere limitati a ciascun punto
vendita.



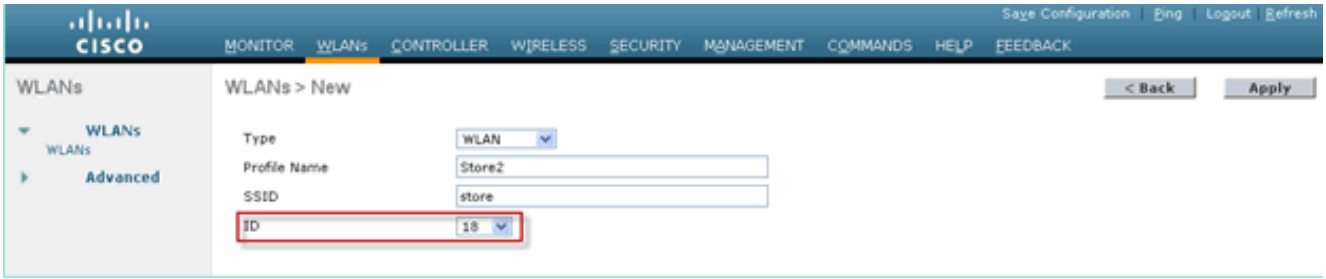
2. In WLAN > Security (WLAN > Sicurezza), selezionare **PSK** dall'elenco a discesa Auth Key Mgmt (Gestione tasti autenticazione), selezionare **ASCII** dall'elenco a discesa PSK Format (Formato PSK) e fare clic su **Apply (Applica).**

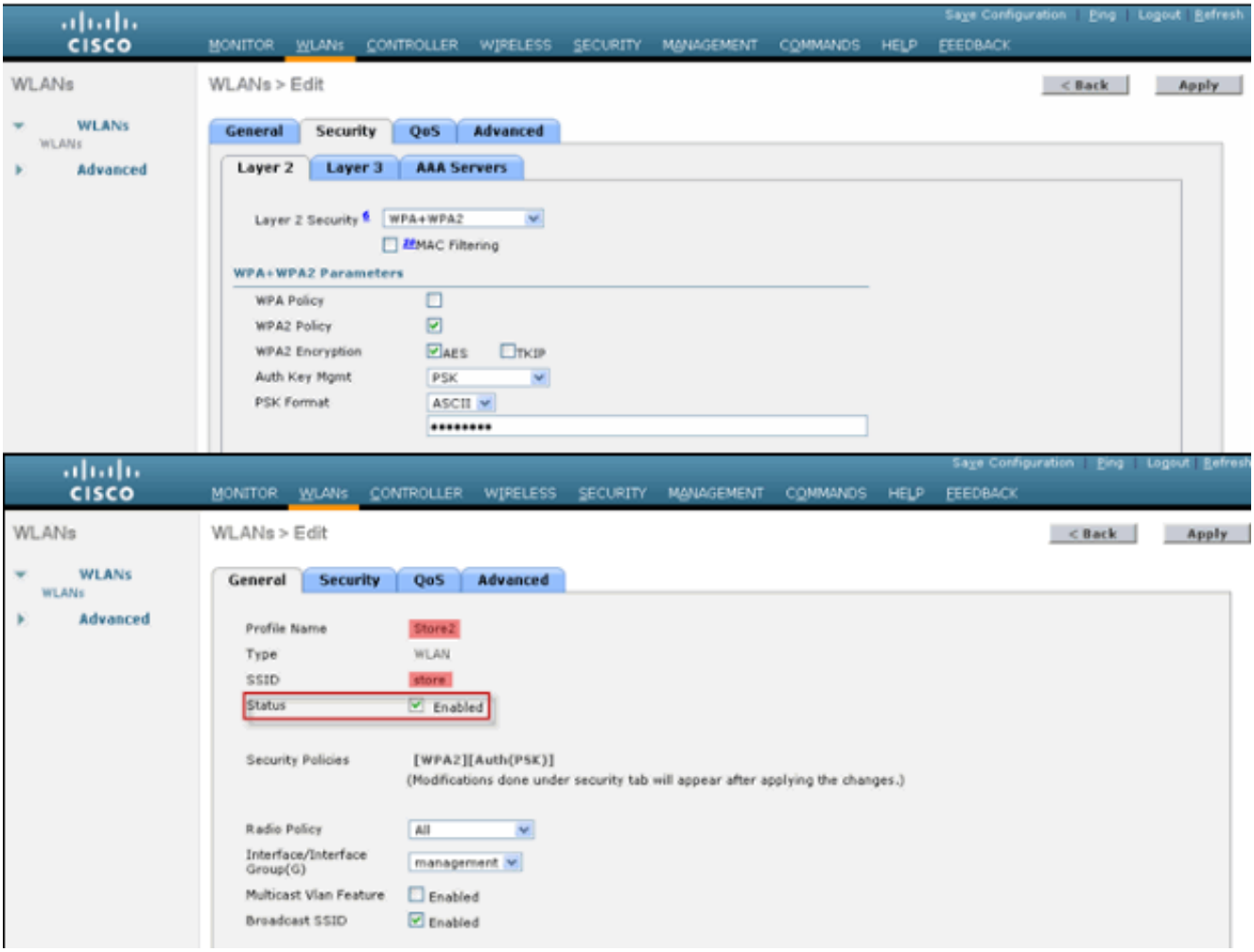


3. Fare clic su **WLAN > Generale**, verificare la modifica dei criteri di sicurezza e selezionare la casella **Stato** per abilitare la WLAN.



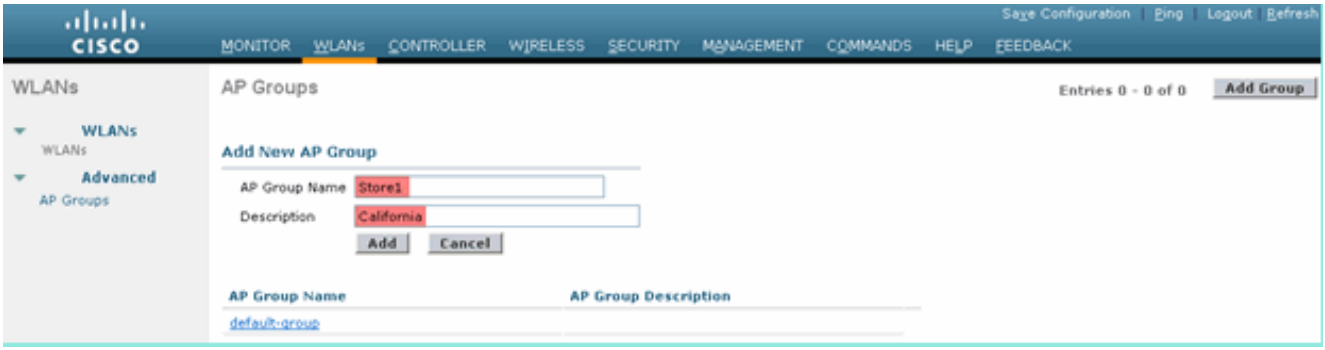
4. Ripetere i passaggi 1, 2 e 3 per il nuovo profilo WLAN **Store2**, con SSID **store** e ID 18.



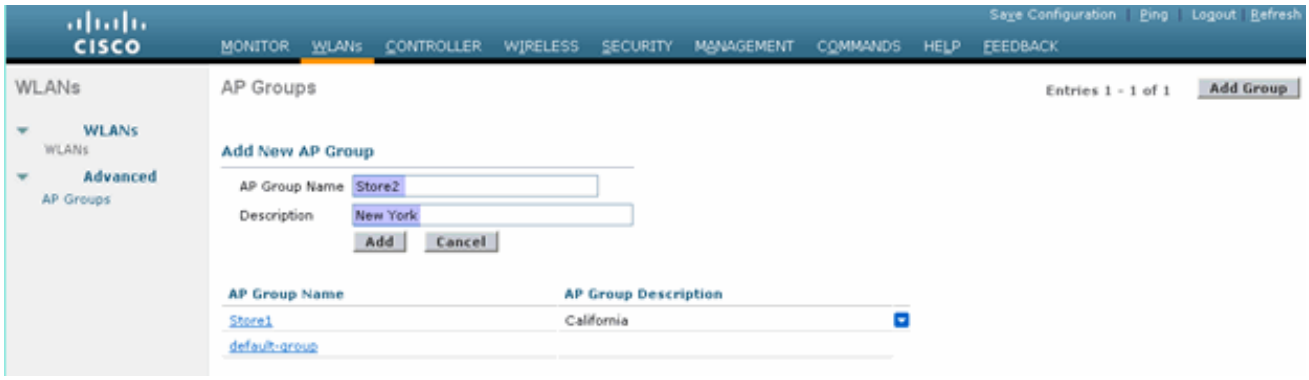


5. Creare e abilitare il profilo WLAN con nome profilo **DataCenter**, SSID **DataCenter** e ID 1.**Nota:** al momento della creazione, gli ID WLAN da 1 a 16 fanno automaticamente parte del gruppo di mappe predefinito.
6. In WLAN, verificare lo stato degli ID WLAN 1, 17 e 18.

7. Fare clic su **WLAN > Avanzate > Gruppo PA > Aggiungi gruppo**.
8. Aggiungere Nome gruppo AP **Store1**, lo stesso del profilo WLAN **Store1**, e Descrizione come Percorso dello Store. Nell'esempio, il percorso del punto vendita è California.
9. Al termine, fare clic su **Add** (Aggiungi).



10. Fare clic su **Add Group** (Aggiungi gruppo) e creare il nome del gruppo AP **Store2** e la descrizione New York.
11. Fare clic su **Add**.

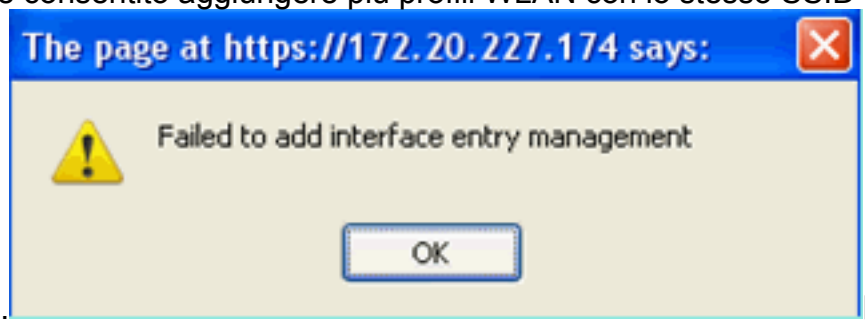


12. Verificare la creazione del gruppo facendo clic su **WLAN > Avanzate > Gruppi PA**.

13. Fare clic su AP Group Name **Store1** per aggiungere o modificare la WLAN.
14. Fare clic su **Add New** (Aggiungi nuovo) per selezionare la WLAN.
15. In WLAN, dall'elenco a discesa WLAN SSID, selezionare **WLAN ID 17 store(17)**.
16. Dopo aver selezionato l'ID WLAN 17, fare clic su **Add** (Aggiungi).
17. Ripetere i passaggi da 14 a 16 per il data center con ID WLAN 1(1). Questo passaggio è facoltativo e necessario solo se si desidera consentire l'accesso alle risorse remote.

18. Tornare alla schermata **WLAN > Avanzate >** Gruppi **PA**.

19. Fare clic su AP Group Name **Store2** per aggiungere o modificare una WLAN.
20. Fare clic su **Add New** (Aggiungi nuovo) per selezionare la WLAN.
21. In WLAN, dall'elenco a discesa WLAN SSID, selezionare **WLAN ID 18 store(18)**.
22. Dopo aver selezionato l'ID WLAN 18, fare clic su **Add** (Aggiungi).
23. Ripetere i passaggi da 14 a 16 per il data center con ID WLAN 1(1).

Nota: non è consentito aggiungere più profili WLAN con lo stesso SSID in un singolo gruppo AP. 

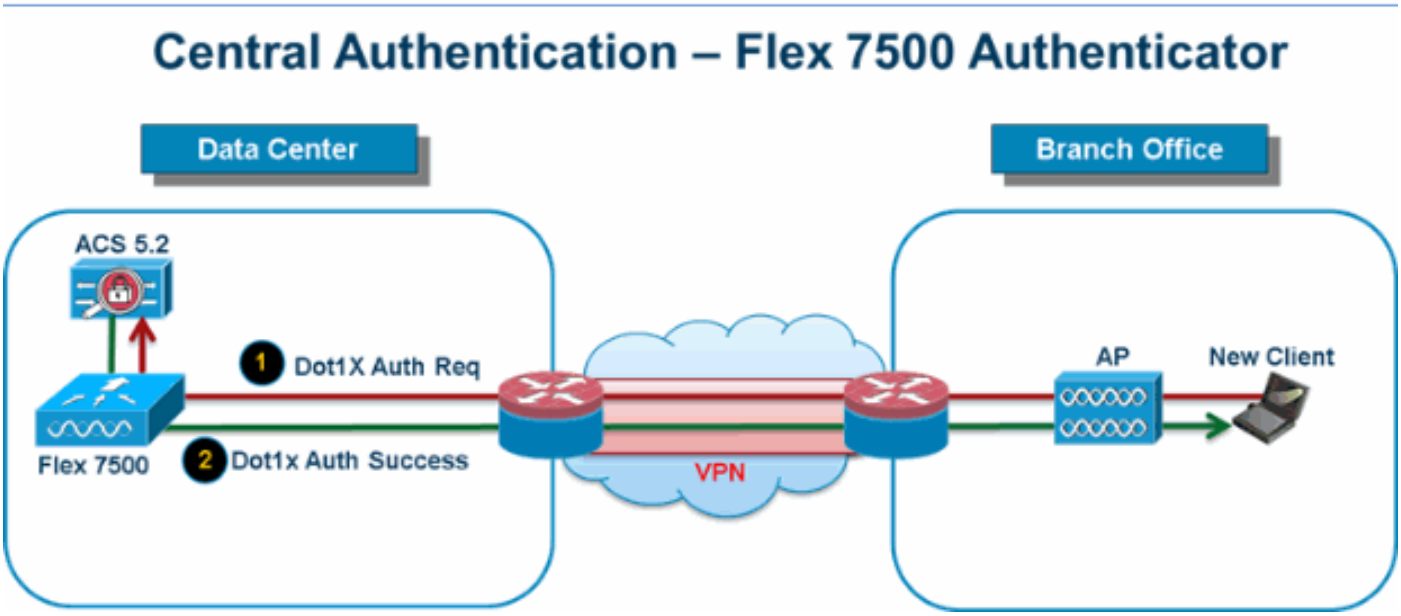
Nota: l'aggiunta di access point al gruppo di access point non viene illustrata in questo documento, ma è necessaria per consentire ai client di accedere ai servizi di rete.

Riepilogo

- I gruppi AP semplificano l'amministrazione della rete.
- Semplicità di risoluzione dei problemi con la granularità per filiale
- Maggiore flessibilità

Gruppi FlexConnect

Figura 9: Autenticazione Central Dot1X (Flex 7500 con funzione di autenticatore)



Nella maggior parte delle installazioni tradizionali di filiali, è facile prevedere che l'autenticazione client 802.1X venga eseguita a livello centrale nel centro dati, come illustrato nella Figura 9. Poiché lo scenario precedente è perfettamente valido, solleva i seguenti problemi:

- In che modo i client wireless possono eseguire l'autenticazione 802.1X e accedere ai servizi del centro dati in caso di guasto di Flex 7500?
- Come possono i client wireless eseguire l'autenticazione 802.1X se il collegamento WAN tra la filiale e il centro dati non riesce?
- Vi è un impatto sulla mobilità delle filiali durante i guasti della WAN?
- La soluzione FlexConnect non prevede tempi di inattività delle filiali?

FlexConnect Group è stato progettato principalmente per risolvere queste problematiche. Inoltre, facilita l'organizzazione di ciascun sito di succursale, in quanto tutti i punti di accesso FlexConnect di ciascun sito di succursale fanno parte di un unico gruppo FlexConnect.

Nota: i gruppi FlexConnect non sono analoghi ai gruppi AP.

Obiettivi principali dei gruppi FlexConnect

Backup failover server RADIUS

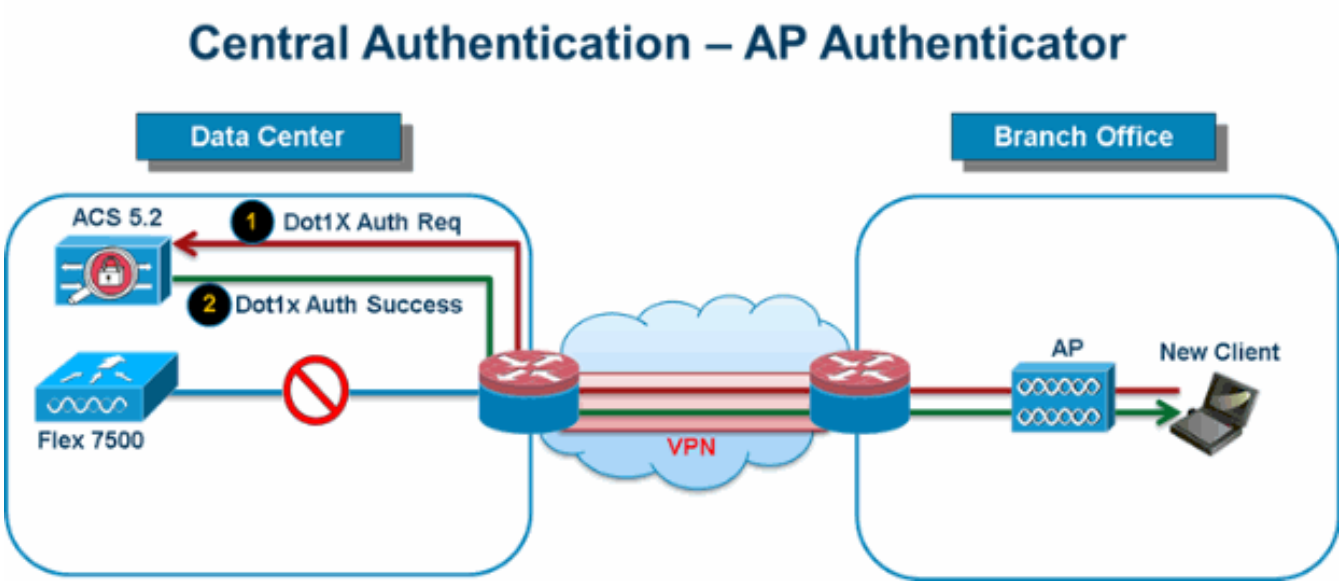
- Èpossibile configurare il controller in modo che un punto di accesso FlexConnect in modalità standalone esegua l'autenticazione 802.1X completa su un server RADIUS di backup. Per aumentare la resilienza della filiale, gli amministratori possono configurare un server RADIUS di backup primario o un server RADIUS di backup primario e secondario. Questi server vengono utilizzati solo quando il punto di accesso FlexConnect non è connesso al controller.

Nota: l'accounting RADIUS di backup non è supportato.

Autenticazione locale

- Prima della versione 7.0.98.0, l'autenticazione locale era supportata solo quando FlexConnect era in modalità standalone per garantire che la connettività dei client non venisse compromessa in caso di errore del collegamento WAN. Con la versione 7.0.116.0, questa funzione è ora supportata anche quando i punti di accesso FlexConnect sono in modalità connessa.**Figura 10: Autenticazione Central Dot1X (punti di accesso FlexConnect che**

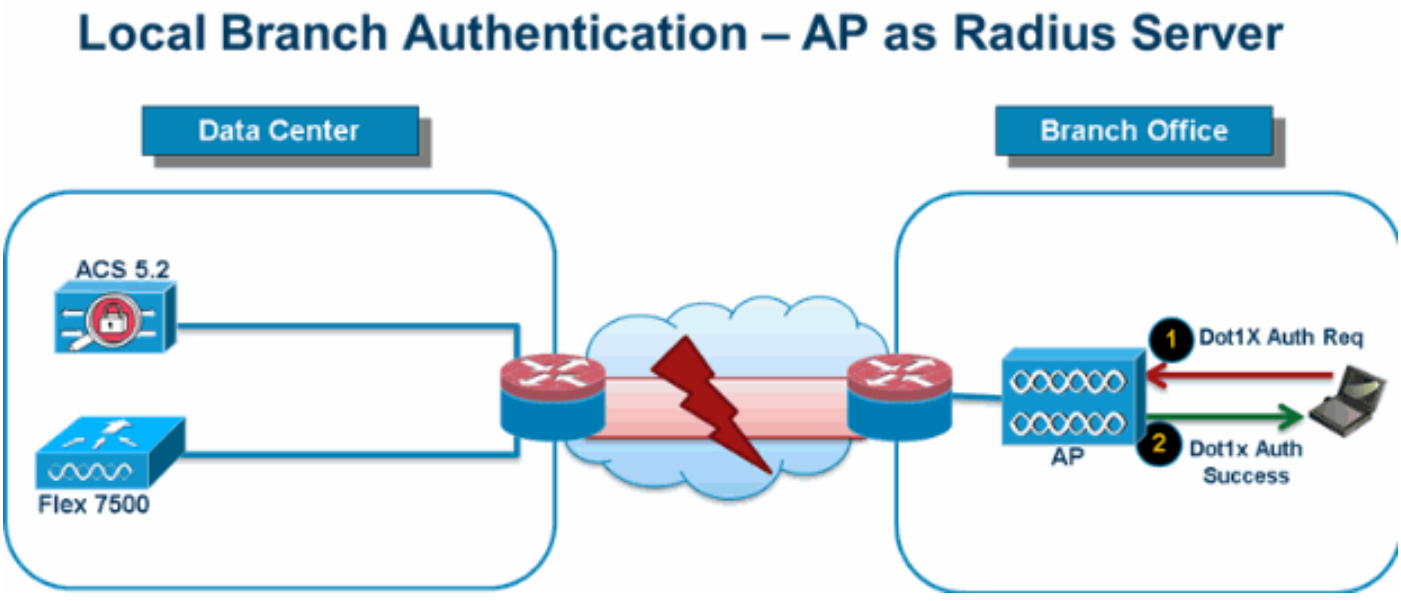
fungono da autenticatore)



Come mostrato nella Figura 10, i client delle filiali possono continuare a eseguire l'autenticazione 802.1X quando i FlexConnect Branch AP perdono la connettività con Flex 7500. Finché il server RADIUS/ACS è raggiungibile dal sito di succursale, i client wireless continueranno ad autenticarsi e ad accedere ai servizi wireless. In altre parole, se il RADIUS/ACS si trova all'interno della filiale, i client eseguiranno l'autenticazione e accederanno ai servizi wireless anche durante un'interruzione della rete WAN.**Nota:** questa funzione può essere utilizzata insieme alla funzione server RADIUS di backup di FlexConnect. Se un gruppo FlexConnect è configurato sia con il server RADIUS di backup che con l'autenticazione locale, il punto di accesso FlexConnect tenta sempre di autenticare i client utilizzando prima il server RADIUS di backup primario, quindi il server RADIUS di backup secondario (se il server primario non è raggiungibile) e infine il server EAP locale sul punto di accesso FlexConnect stesso (se il server primario e quello secondario non sono raggiungibili).

EAP locale (continuazione autenticazione locale)

Figura 11: Autenticazione Dot1X (punti di accesso FlexConnect che agiscono come server EAP locale)



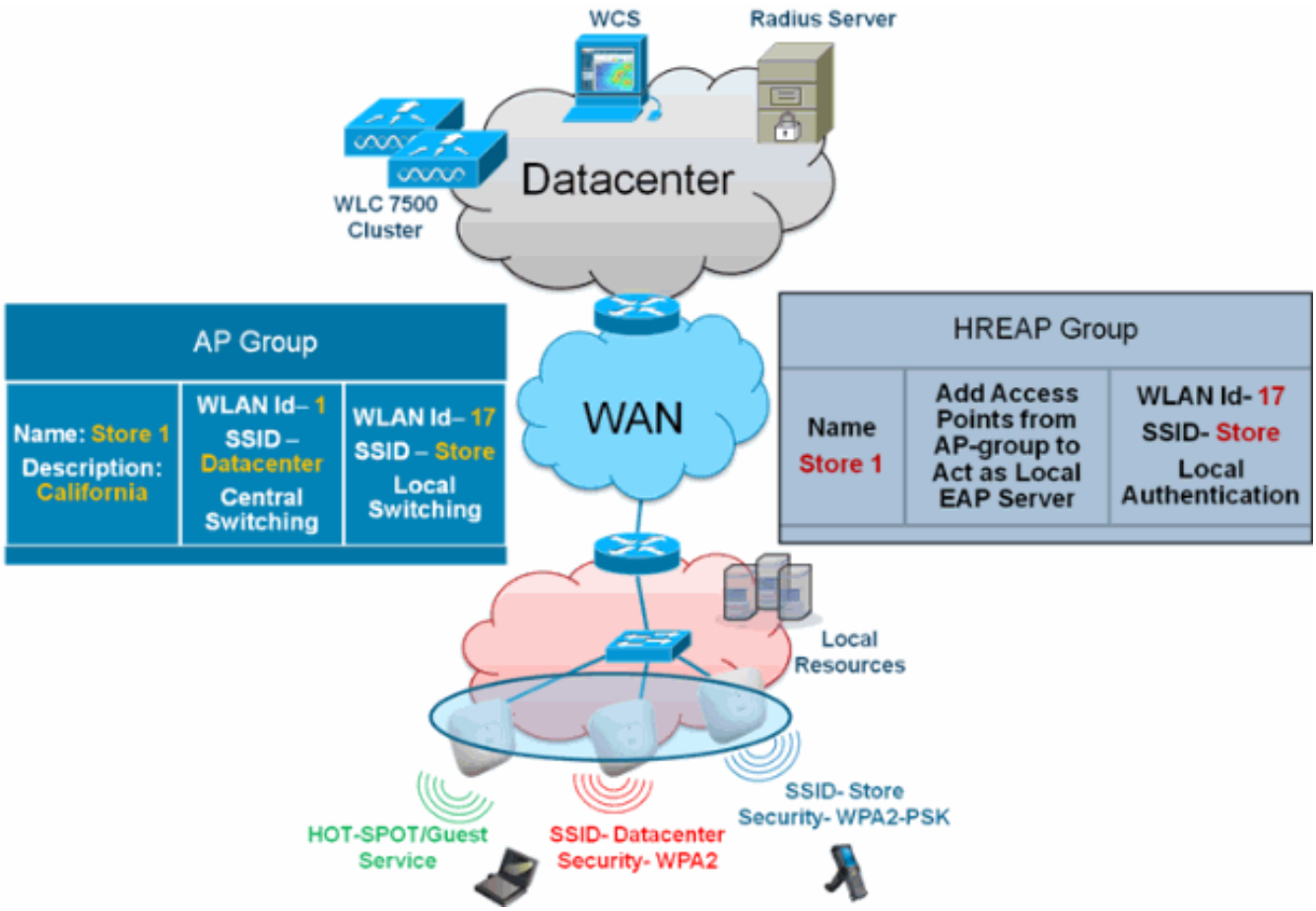
- Èpossibile configurare il controller in modo che un punto di accesso FlexConnect in modalità standalone o connessa esegua l'autenticazione LEAP o EAP-FAST per un massimo di 100

utenti configurati staticamente. Il controller invia l'elenco statico di nomi utente e password a ciascun punto di accesso FlexConnect di quel particolare gruppo FlexConnect quando si unisce al controller. Ogni punto di accesso del gruppo autentica solo i propri client associati.

- Questa funzione è ideale per i clienti che stanno eseguendo la migrazione da una rete con punto di accesso autonomo a una rete con punto di accesso FlexConnect leggero e non sono interessati a gestire un database di utenti di grandi dimensioni o ad aggiungere un altro dispositivo hardware per sostituire la funzionalità server RADIUS disponibile nel punto di accesso autonomo.
- Come mostrato nella Figura 11, se il server RADIUS/ACS all'interno del data center non è raggiungibile, i punti di accesso FlexConnect agiscono automaticamente come server Local-EAP per eseguire l'autenticazione Dot1X per i client delle filiali wireless.

CCKM/OKC Fast Roaming

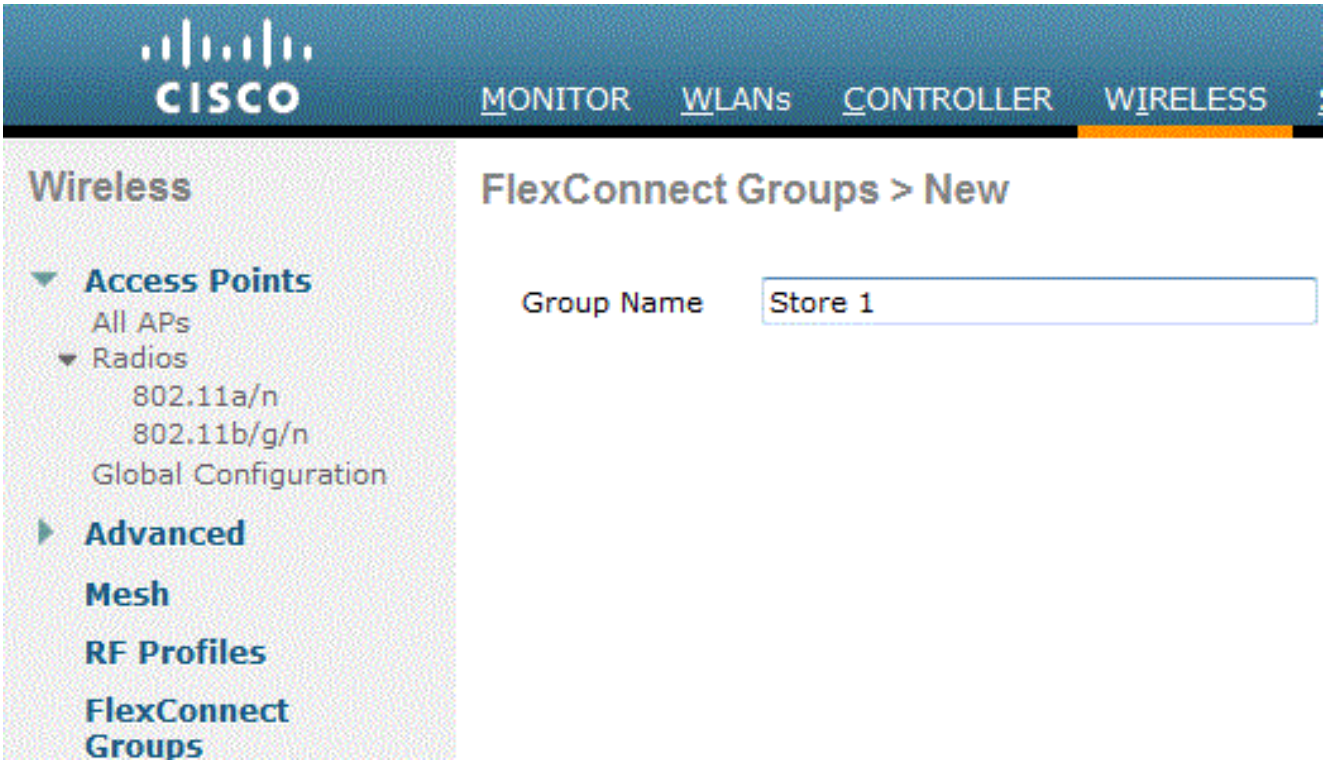
- I gruppi FlexConnect sono richiesti per il roaming veloce CCKM/OKC per funzionare con i punti di accesso FlexConnect. Il roaming veloce si ottiene memorizzando nella cache una derivata della chiave master da un'autenticazione EAP completa, in modo che lo scambio di chiave semplice e sicuro possa avvenire quando un client wireless esegue il roaming a un punto di accesso diverso. Questa funzionalità evita la necessità di eseguire un'autenticazione EAP RADIUS completa quando il client esegue il roaming da un punto di accesso a un altro. I punti di accesso FlexConnect devono ottenere le informazioni della cache CCKM/OKC per tutti i client che potrebbero associarsi, in modo da poterle elaborare rapidamente anziché restituirle al controller. Se, ad esempio, si dispone di un controller con 300 punti di accesso e 100 client che potrebbero essere associati, l'invio della cache CCKM/OKC per tutti i 100 client non è pratico. Se si crea un gruppo FlexConnect che comprende un numero limitato di punti di accesso (ad esempio, si crea un gruppo per quattro punti di accesso in una sede remota), i client eseguono il roaming solo tra questi quattro punti di accesso e la cache CCKM/OKC viene distribuita tra questi quattro punti di accesso solo quando i client si associano a uno di essi.
- Questa funzione, insieme al backup Radius e all'autenticazione locale (Local-EAP), garantisce **che non vi siano tempi di inattività operativi** per i siti di succursale.**Nota: il** roaming veloce CCKM/OKC tra i punti di accesso FlexConnect e non FlexConnect non è supportato.**Figura 12: Guida di riferimento alla progettazione di reti wireless con i gruppi FlexConnect**



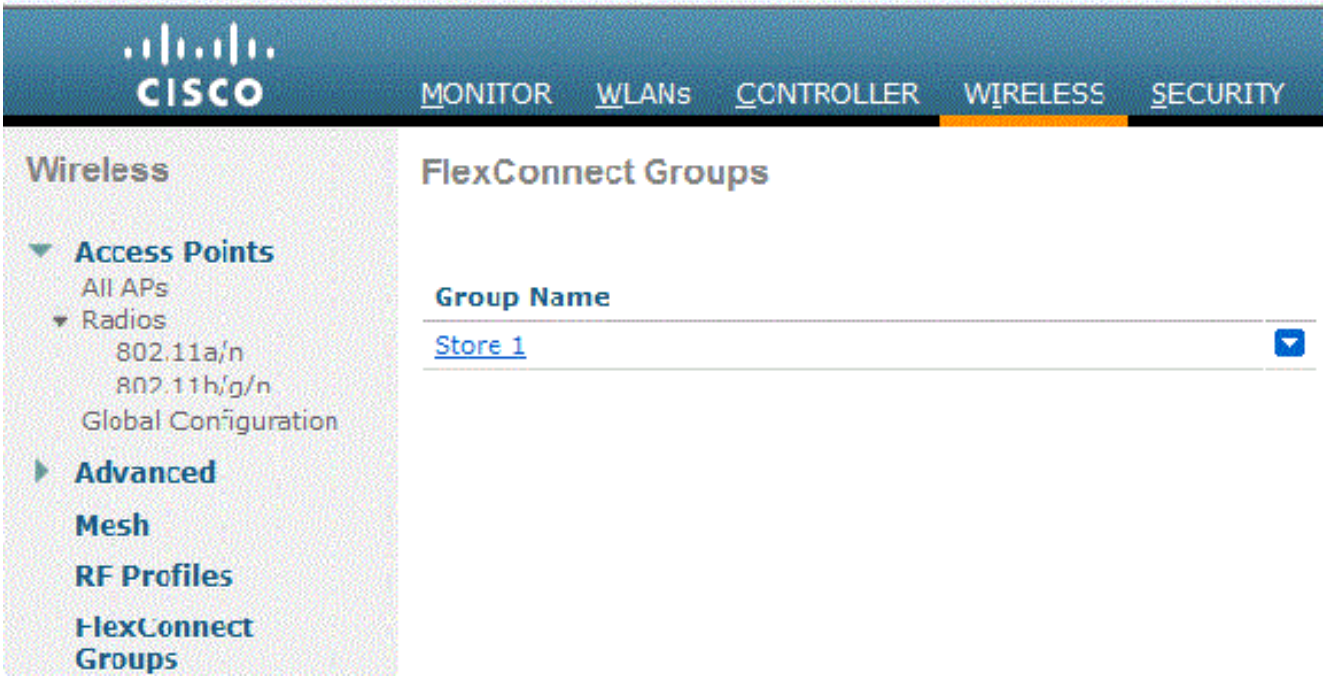
Configurazione gruppo FlexConnect da WLC

Completare la procedura descritta in questa sezione per configurare i gruppi FlexConnect in modo che supportino l'autenticazione locale con LEAP, quando FlexConnect è in modalità connessa o standalone. L'esempio di configurazione nella Figura 12 mostra le differenze tra gli obiettivi e il mapping 1:1 tra il gruppo AP e il gruppo FlexConnect.

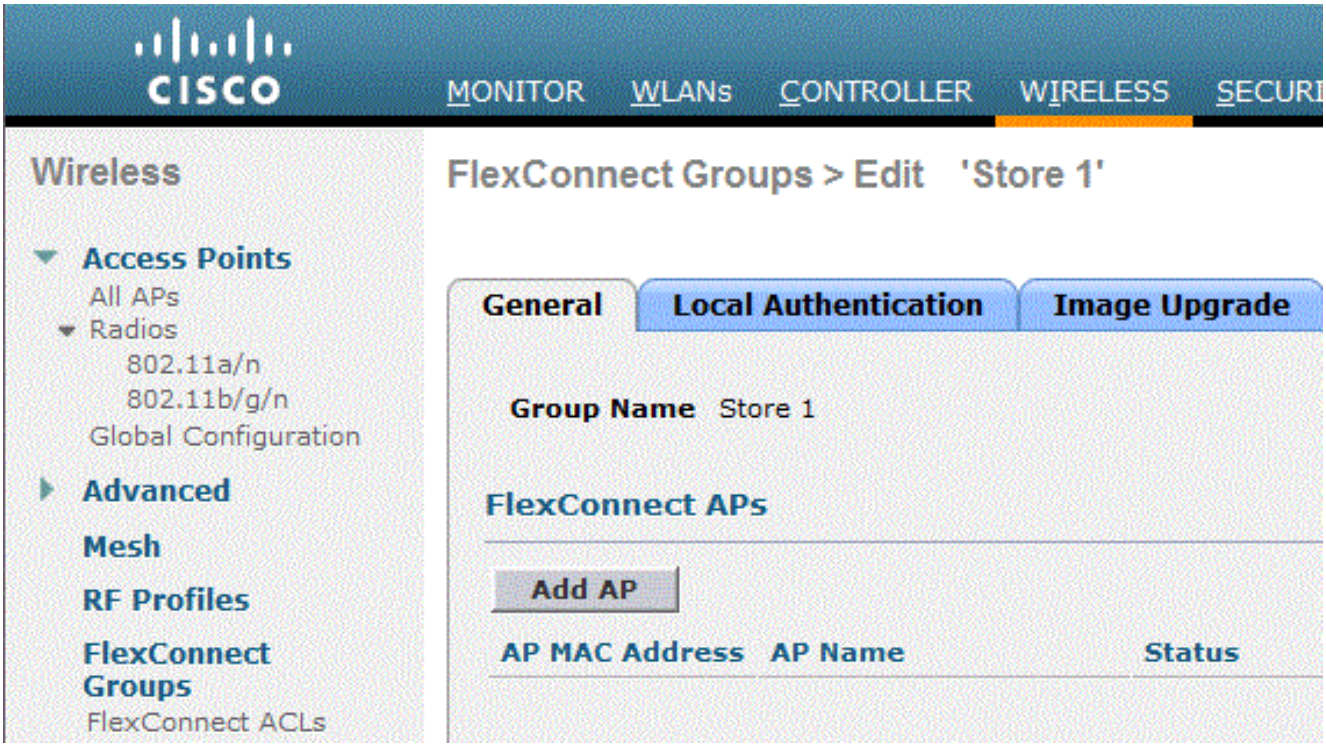
1. Fare clic su **Nuovo** in Wireless > FlexConnect Groups.
2. Assegnare il nome del gruppo Store 1, in modo simile alla configurazione di esempio, come mostrato nella Figura 12.
3. Fare clic su **Apply** (Applica) quando è impostato il nome del gruppo.



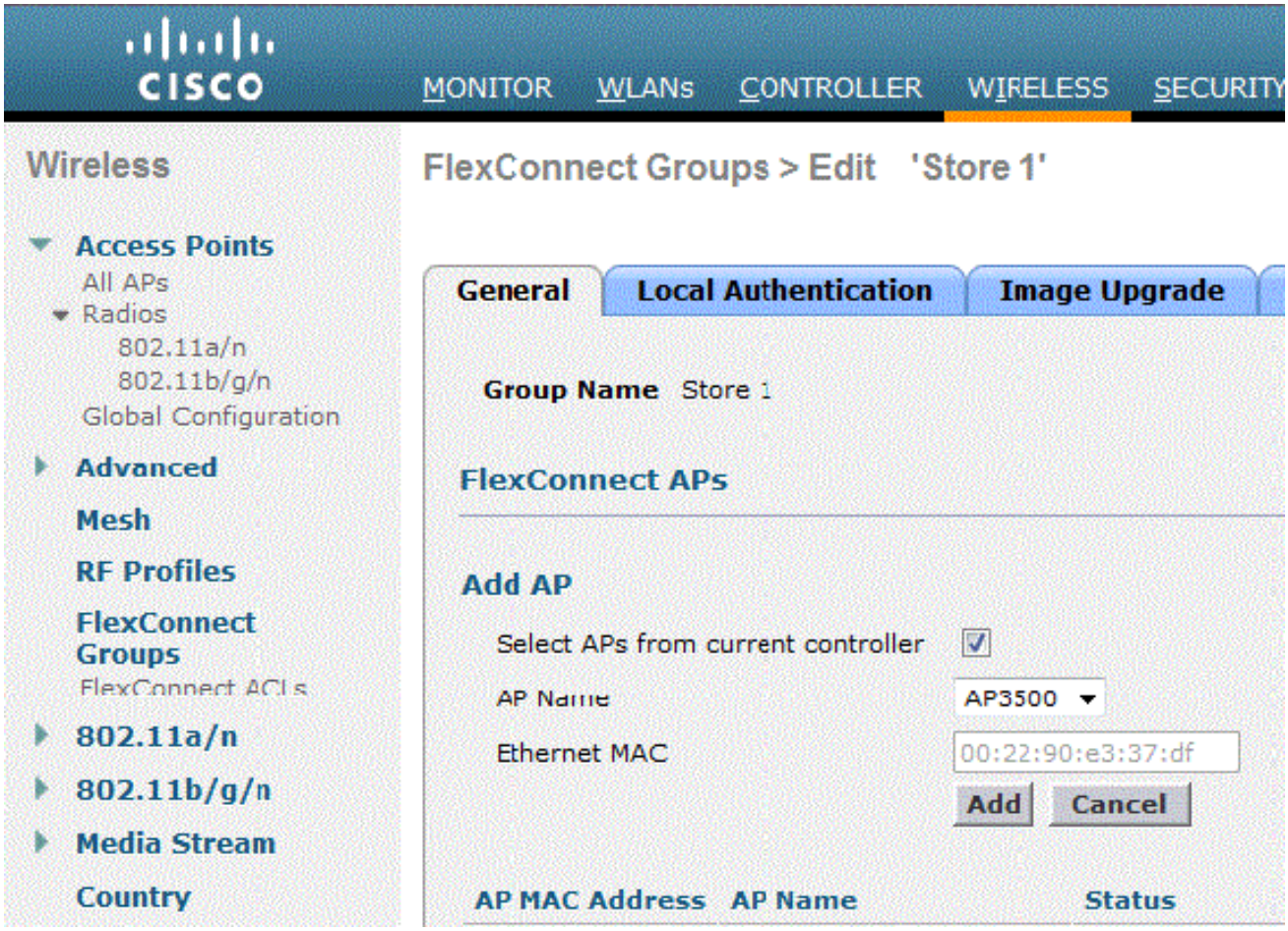
4. Fare clic sull'**Archivio** nomi gruppo **1** appena creato per un'ulteriore configurazione.



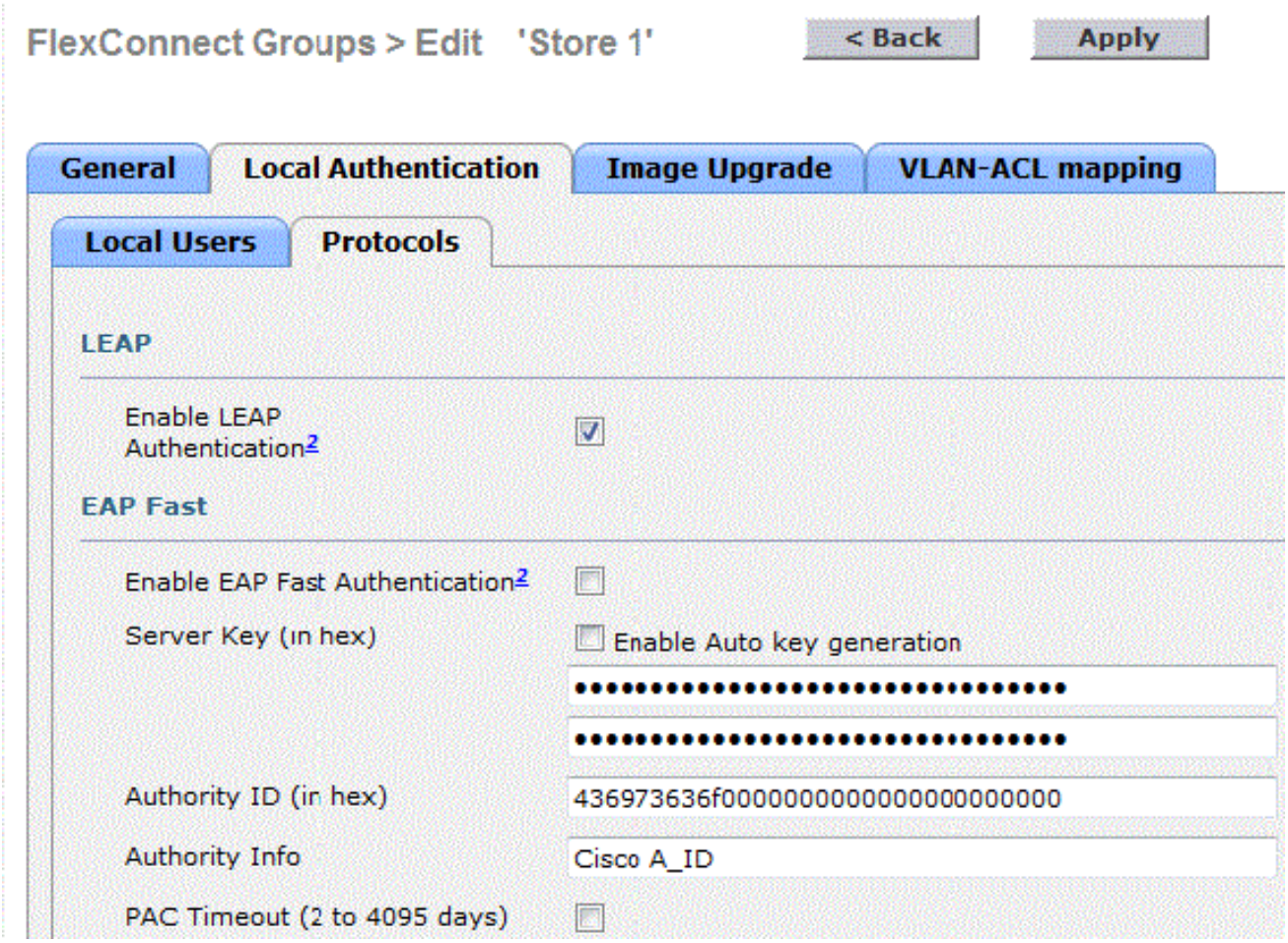
5. Fare clic su **Add AP**.



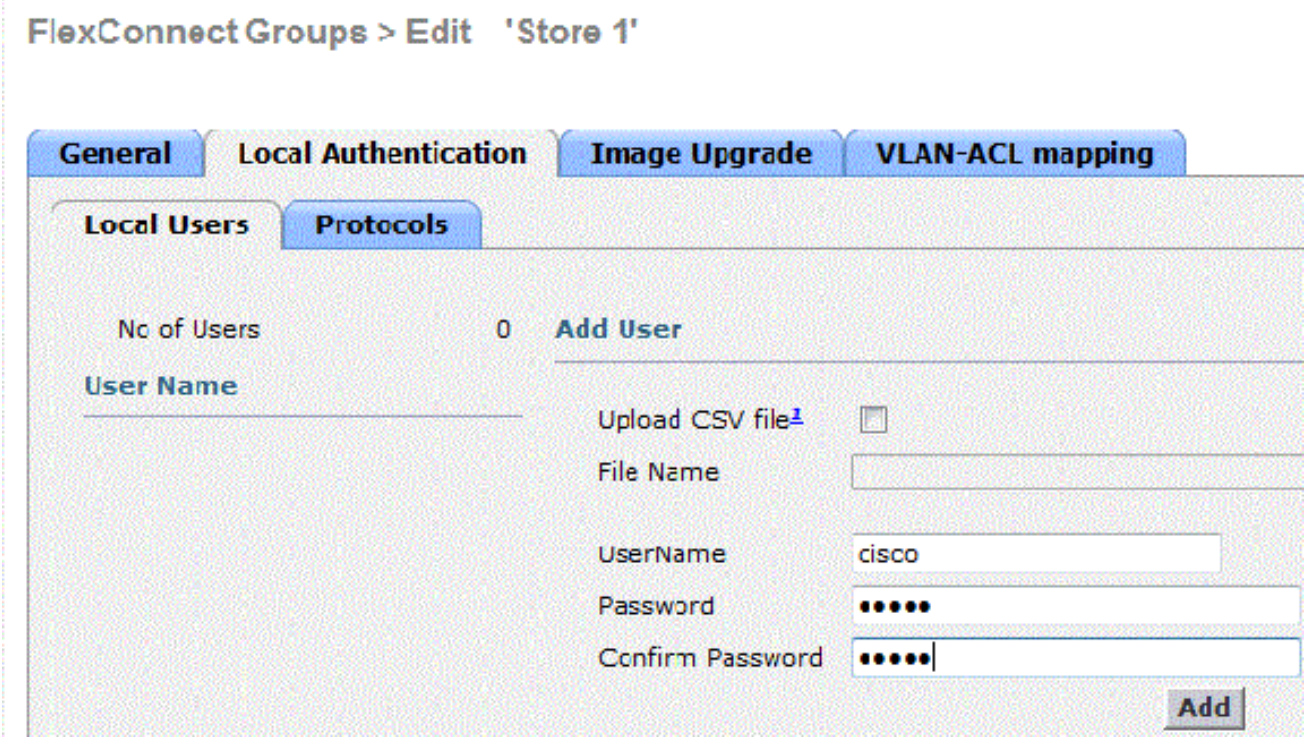
6. Selezionare la casella **Abilita autenticazione locale AP** per abilitare l'autenticazione locale quando l'access point è in modalità standalone.**Nota:** nel passaggio 20 viene mostrato come abilitare l'autenticazione locale per l'access point in modalità connessa.
7. Selezionare la casella **Select APs from current controller** per abilitare il menu a discesa AP Name (Nome access point).
8. Selezionare dall'elenco a discesa l'access point che deve far parte di questo gruppo FlexConnect.
9. Fare clic su **Add** (Aggiungi) dopo aver scelto l'access point dall'elenco a discesa.
10. Ripetere i passaggi 7 e 8 per aggiungere a questo gruppo FlexConnect tutti gli access point che fanno anche parte dell'archivio dei gruppi di access point 1. Vedere la Figura 12 per informazioni sul mapping 1:1 tra il gruppo di access point e il gruppo FlexConnect.Se è stato creato un gruppo di access point per Store (Figura 8), idealmente tutti gli access point di quel gruppo dovrebbero far parte di questo gruppo FlexConnect (Figura 12). Mantenere un rapporto 1:1 tra il gruppo AP e il gruppo FlexConnect semplifica la gestione della rete.



11. Fare clic su **Autenticazione locale > Protocolli** e selezionare la casella **Abilita autenticazione LEAP**.
12. Fare clic su **Apply** (Applica)dopo aver impostato la casella di controllo.**Nota:** se si dispone di un controller di backup, verificare che i gruppi FlexConnect siano identici e che le voci degli indirizzi MAC AP siano incluse per ciascun gruppo FlexConnect.



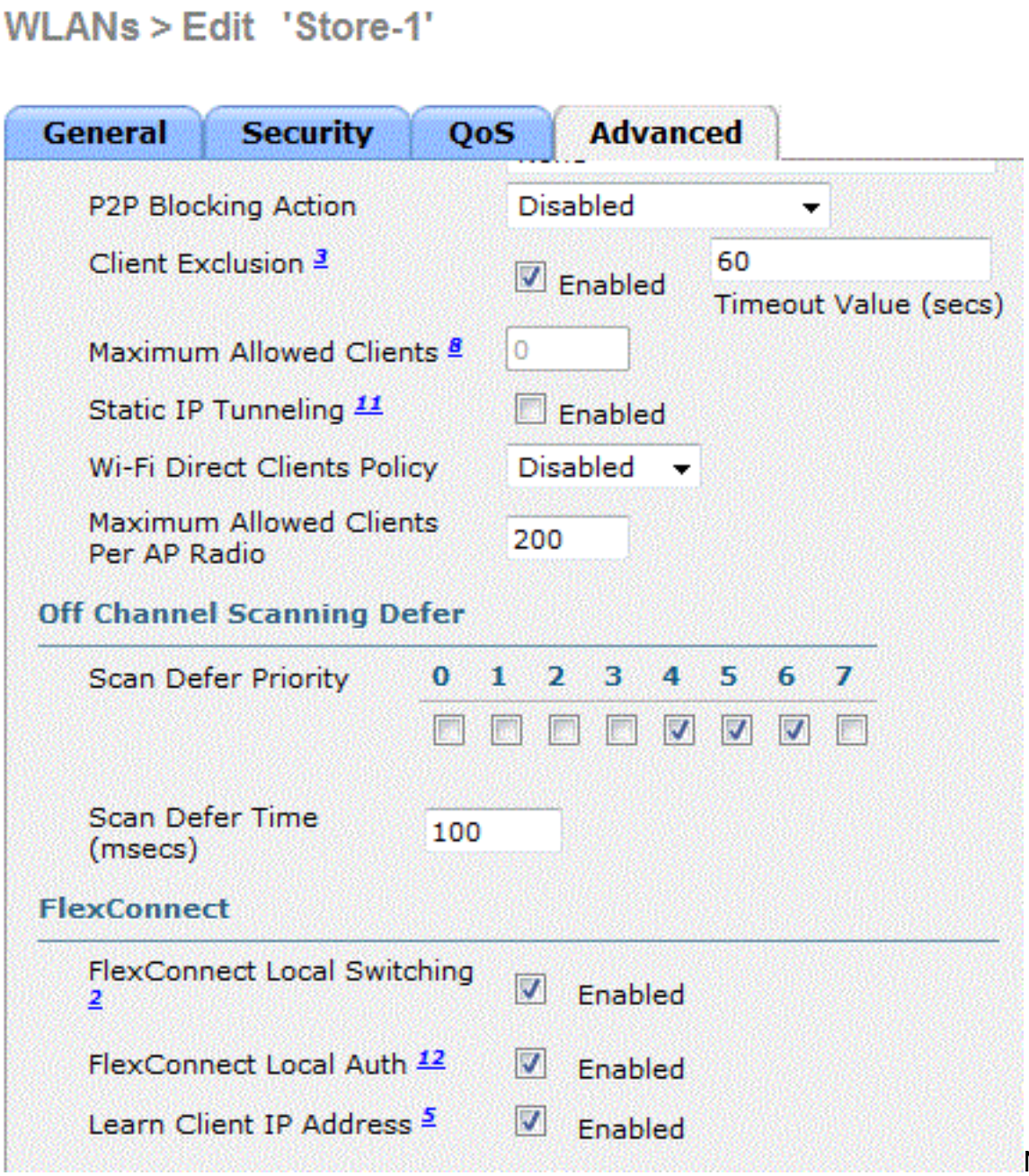
13. In Autenticazione locale fare clic su **Utenti locali**.
14. Impostare i campi Nome utente, Password e Conferma password, quindi fare clic su **Add** (Aggiungi) per creare una voce utente nel server EAP locale residente sull'access point.
15. Ripetere il passaggio 13 fino a esaurire l'elenco dei nomi utente locali. Impossibile configurare o aggiungere più di 100 utenti.
16. Fare clic su **Apply** (Applica) dopo aver completato il passo 14 e aver verificato il numero di utenti.



17. Nel riquadro superiore fare clic su **WLAN**.

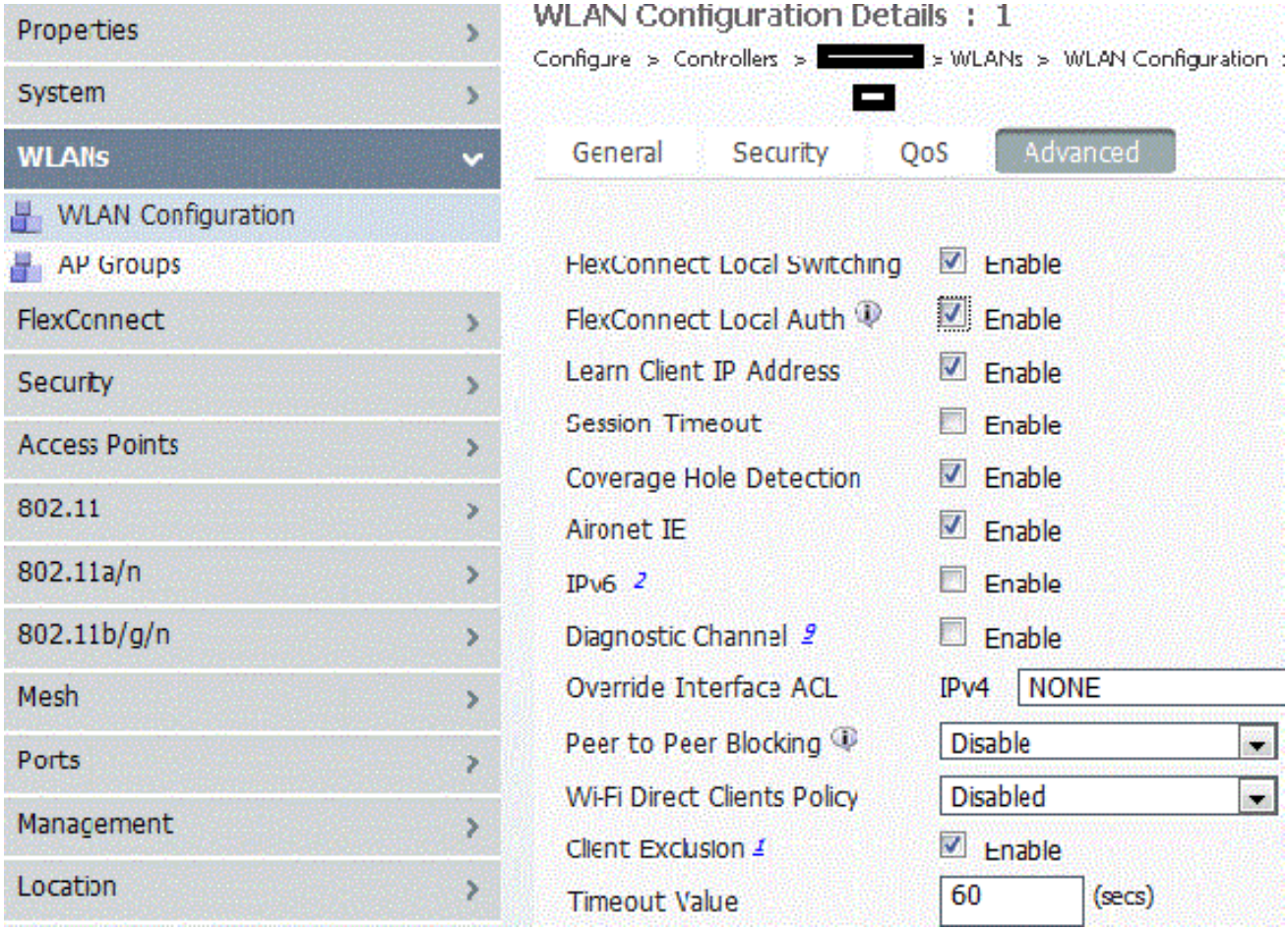
18. Fare clic su **ID WLAN 17**. Questa opzione è stata creata durante la creazione del gruppo AP. Vedere la Figura 8.

19. In WLAN > Modifica per ID WLAN 17, fare clic su **Avanzate**.
20. Per abilitare l'autenticazione locale in modalità connessa, selezionare la casella **FlexConnect Local Auth**.**Nota:** l'autenticazione locale è supportata solo per FlexConnect con switching locale.**Nota:** accertarsi sempre di creare il gruppo FlexConnect prima di abilitare l'autenticazione locale in

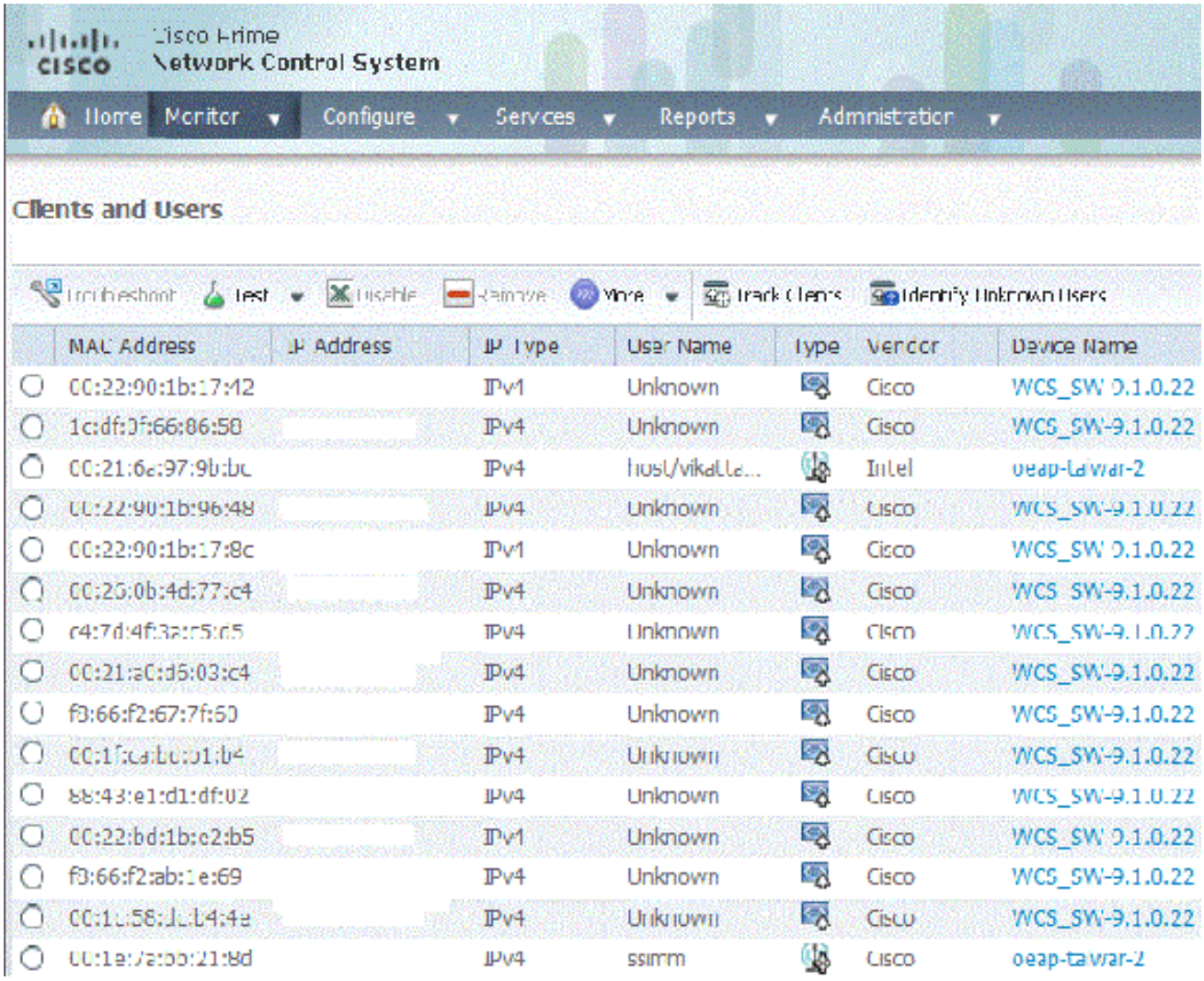


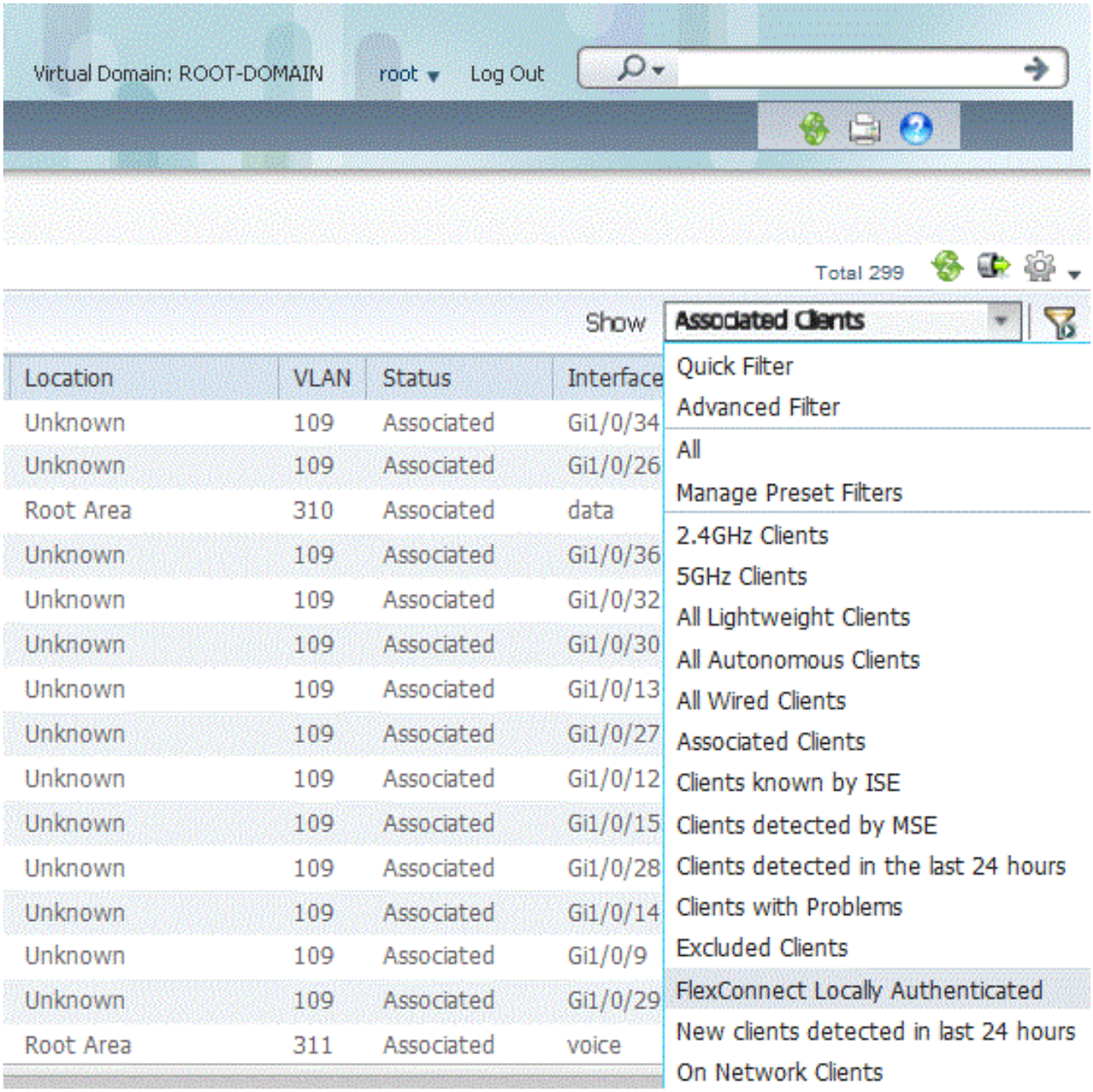
WLAN. N

CS fornisce inoltre la casella di controllo FlexConnect Local Auth per abilitare l'autenticazione locale in modalità connessa, come mostrato di seguito:



NCS fornisce inoltre la possibilità di filtrare e monitorare i client FlexConnect Locally Authenticated, come illustrato di
seguito:


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



Verifica tramite CLI

Lo stato di autenticazione del client e la modalità di commutazione possono essere verificati rapidamente utilizzando questa CLI sul WLC:

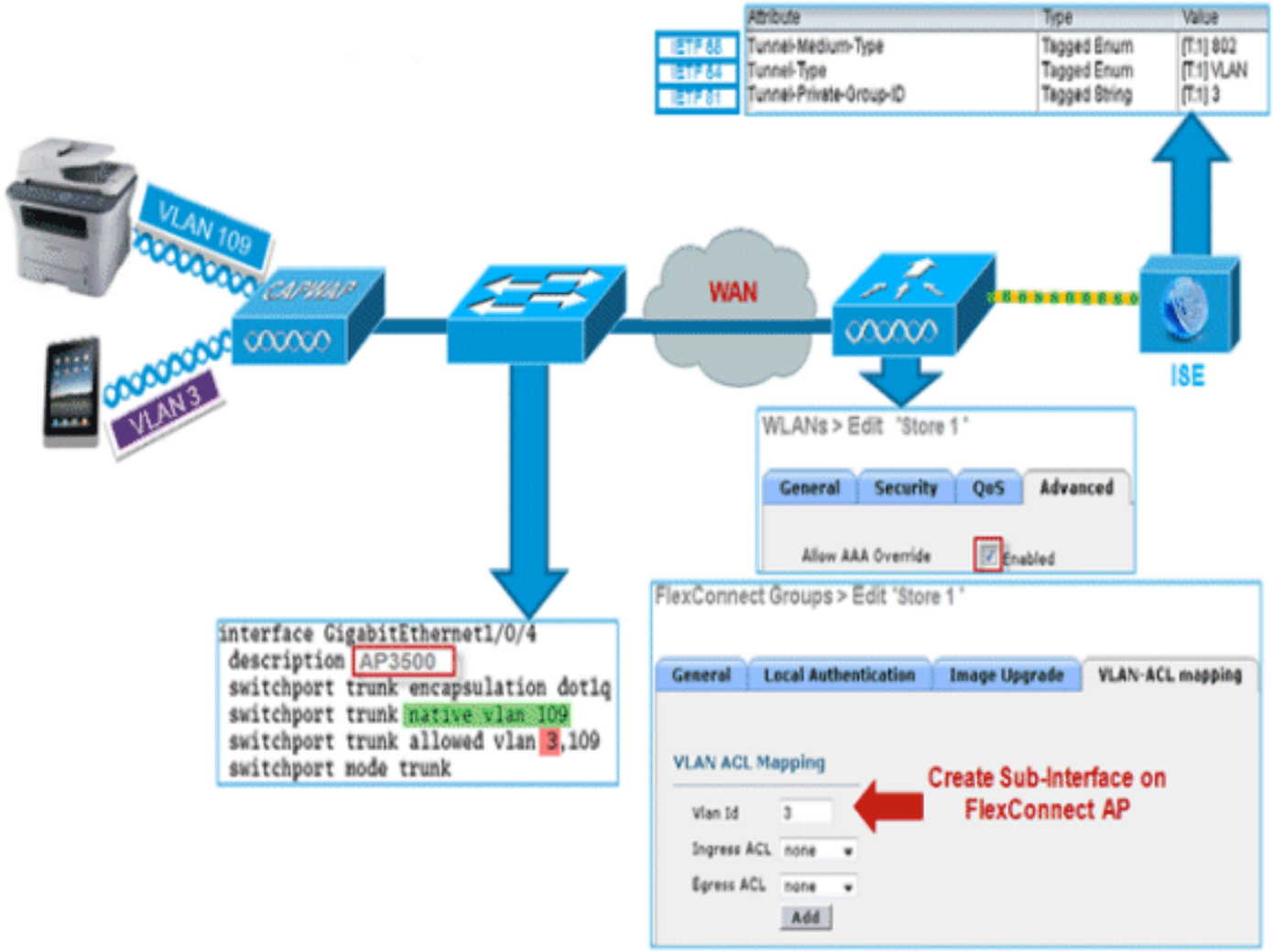
```
(Cisco Controller) >show client detail 00:24:d7:2b:7c:0c
Client MAC Address.............................. 00:24:d7:2b:7c:0c
Client Username ................................ N/A
AP MAC Address.................................. d0:57:4c:08:e6:70
Client State.................................... Associated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

Override della VLAN FlexConnect

Nell'architettura FlexConnect corrente, esiste una stretta mappatura tra la WLAN e la VLAN. Di conseguenza, il client che viene associato a una particolare WLAN su un access point

FlexConnect deve rispettare una VLAN mappata su di essa. Questo metodo presenta delle limitazioni, in quanto richiede che i client si associno a SSID diversi per ereditare policy basate su VLAN diverse.

Dalla versione 7.2 in poi, è supportata la sostituzione AAA della VLAN su una singola WLAN configurata per la commutazione locale. Per ottenere l'assegnazione dinamica della VLAN, l'access point deve avere le interfacce per la VLAN pre-create in base a una configurazione che utilizza il mapping WLAN-VLAN esistente per un singolo access point FlexConnect o utilizza il mapping ACL-VLAN su un gruppo FlexConnect. Il WLC viene utilizzato per creare preliminarmente le sottointerfacce nell'access point.



Riepilogo

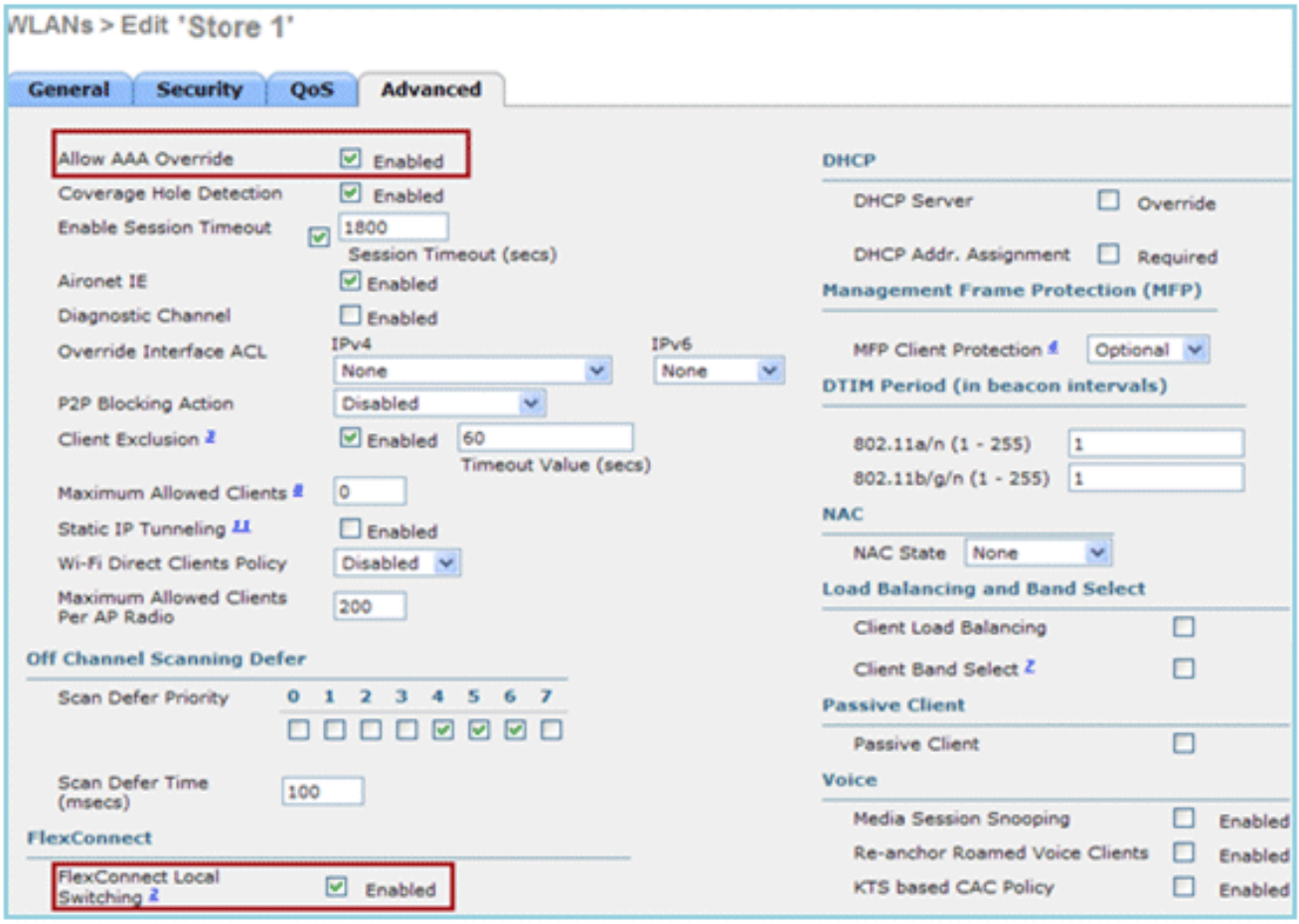
- L'override della VLAN AAA è supportato dalla versione 7.2 per le WLAN configurate per la commutazione locale in modalità di autenticazione centrale e locale.
- Ènecessario abilitare l'override AAA sulla WLAN configurata per la commutazione locale.
- Per l'assegnazione dinamica della VLAN, l'access point FlexConnect deve avere una VLAN precreata dal WLC.
- Se le VLAN restituite dall'override AAA non sono presenti sul client AP, riceveranno un IP dall'interfaccia VLAN predefinita dell'AP.

Procedura

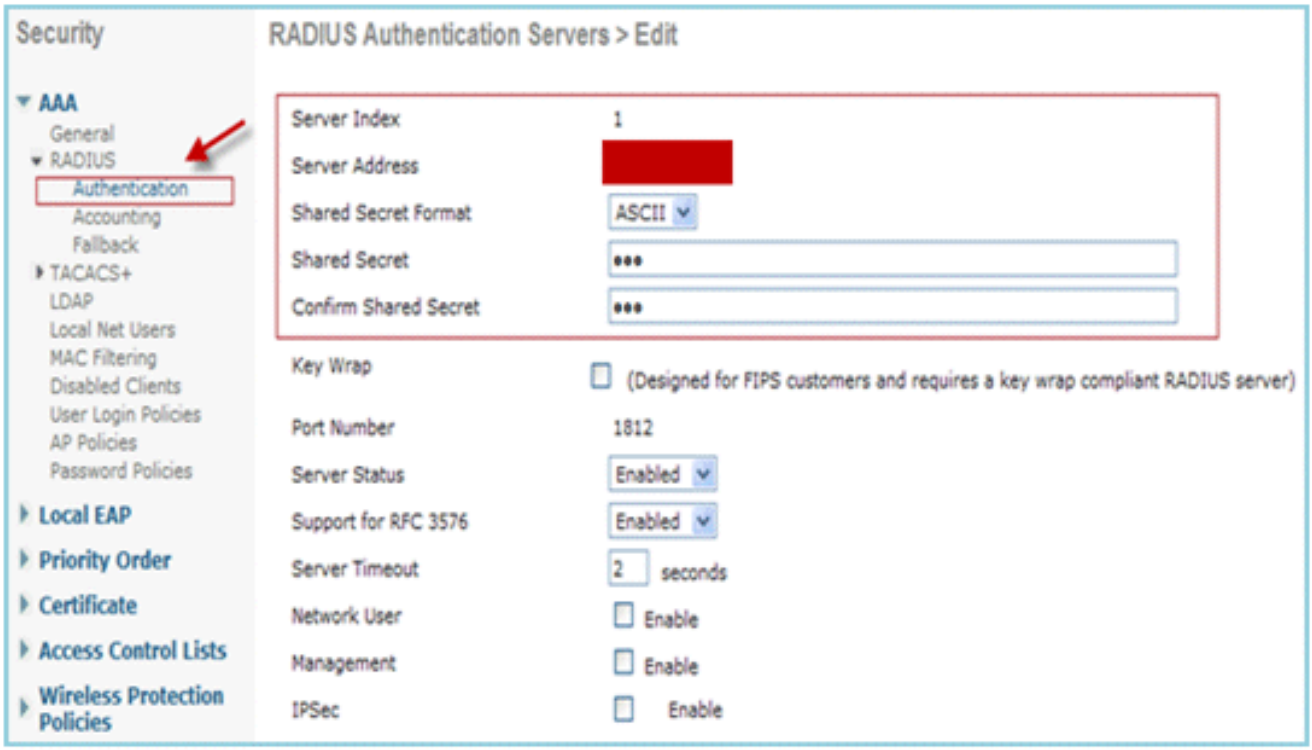
Attenersi alla seguente procedura:

1. Crea una WLAN per l'autenticazione 802.1x.

2. Abilitare il supporto dell'override AAA per la switching WLAN locale sul WLC. Selezionare **GUI WLAN > WLAN > ID WLAN >** scheda **Advance**.

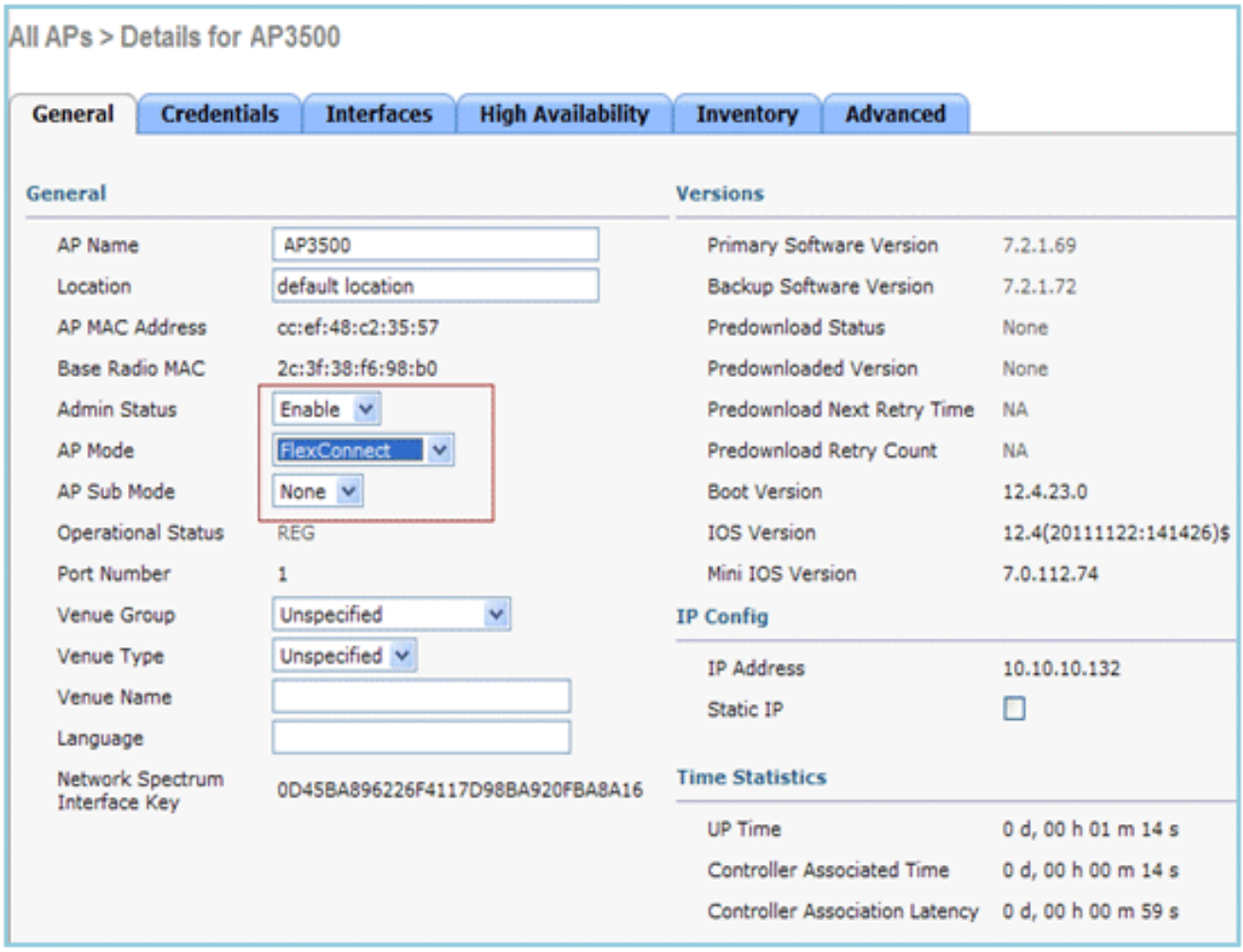


3. Aggiungere i dettagli del server AAA sul controller per l'autenticazione 802.1x. Per aggiungere il server AAA, selezionare WLC GUI > Security > AAA > **Radius > Authentication > New**.

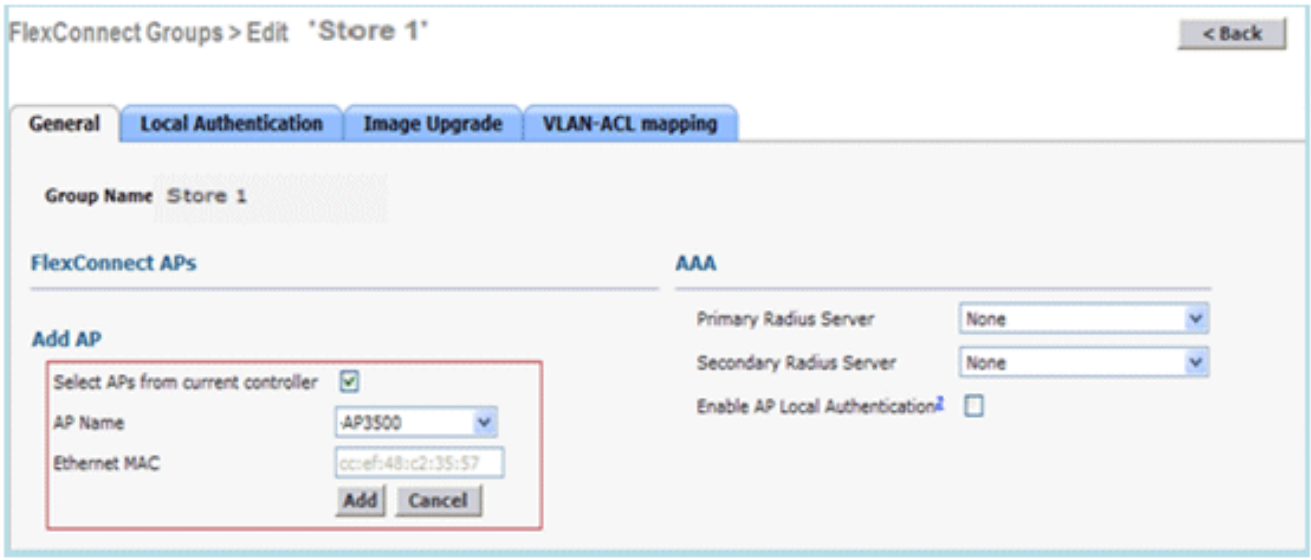


4. L'access point è in modalità locale per impostazione predefinita, quindi converti la modalità in modalità FlexConnect. I punti di accesso in modalità locale possono essere convertiti in modalità FlexConnect passando a **Wireless > Tutti i punti di accesso** e facendo clic sul punto di accesso

individuale.



5. Aggiungere i punti di accesso FlexConnect al gruppo FlexConnect.Selezionare WLC GUI > Wireless > FlexConnect Groups > **Select FlexConnect Group** > **General** tab >**Add AP**.

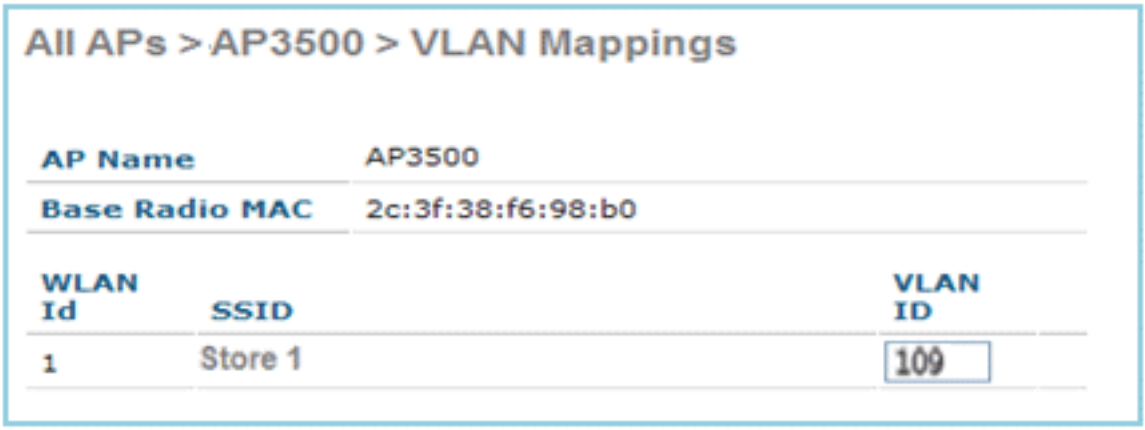


6. L'access point FlexConnect deve essere connesso a una porta trunk e la VLAN mappata alla WLAN e la VLAN sostituita dall'AAA devono essere consentite alla porta

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

trunk. **Nota:** in questa configurazione, la vlan 109 viene usata per il mapping della VLAN WLAN e la vlan 3 per l'override dell'AAA.

7. Configurare il mapping da WLAN a VLAN per l'access point FlexConnect. In base a questa configurazione, l'access point deve avere le interfacce per la VLAN. Quando l'access point riceve la configurazione VLAN, le sottointerfacce corrispondenti dot11 ed Ethernet vengono create e aggiunte a un bridge-group. Associare un client alla WLAN. Quando il client si associa, viene assegnata la VLAN (impostazione predefinita, basata sul mapping WLAN-VLAN).Selezionare GUI WLAN > **Wireless** > **Tutti gli AP** > fare clic sulla scheda AP > **FlexConnect** e fare clic su **Mapping**

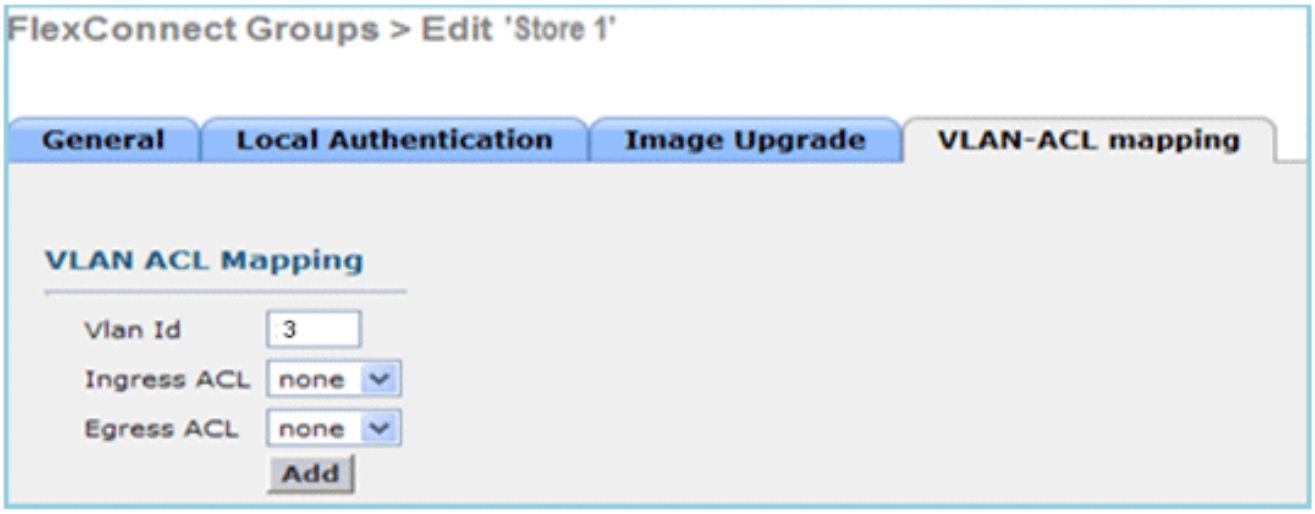


VLAN.

8. Creare un utente nel server AAA e configurare l'utente in modo che restituisca l'ID VLAN nell'attributo IETF
   Radius.

	Attribute	Type	Value
IETF 65	Tunnel-Medium-Type	Tagged Enum	[T:1] 802
IETF 64	Tunnel-Type	Tagged Enum	[T:1] VLAN
IETF 81	Tunnel-Private-Group-ID	Tagged String	[T:1] 3

9. Per ottenere l'assegnazione dinamica della VLAN, l'access point deve avere le interfacce per la VLAN dinamica pre-create in base alla configurazione usando il mapping WLAN-VLAN esistente per il singolo access point FlexConnect o usando il mapping ACL-VLAN sul gruppo FlexConnect.Per configurare la VLAN AAA sull'access point FlexConnect, selezionare WLC GUI > **Wireless** > **Gruppo FlexConnect** > fare clic sul gruppo FlexConnect specifico > **Mapping VLAN-ACL**, quindi immettere VLAN nel **campo Vlan ID**.



10. Associare un client alla WLAN e autenticarsi utilizzando il nome utente configurato nel server AAA per restituire la VLAN AAA.
11. Il client deve ricevere un indirizzo IP dalla VLAN dinamica restituita tramite il server AAA.
12. Per procedere alla verifica, fare clic su **WLC GUI > Monitor > Client >** fare clic sull'indirizzo MAC del client per controllare i dettagli del client.

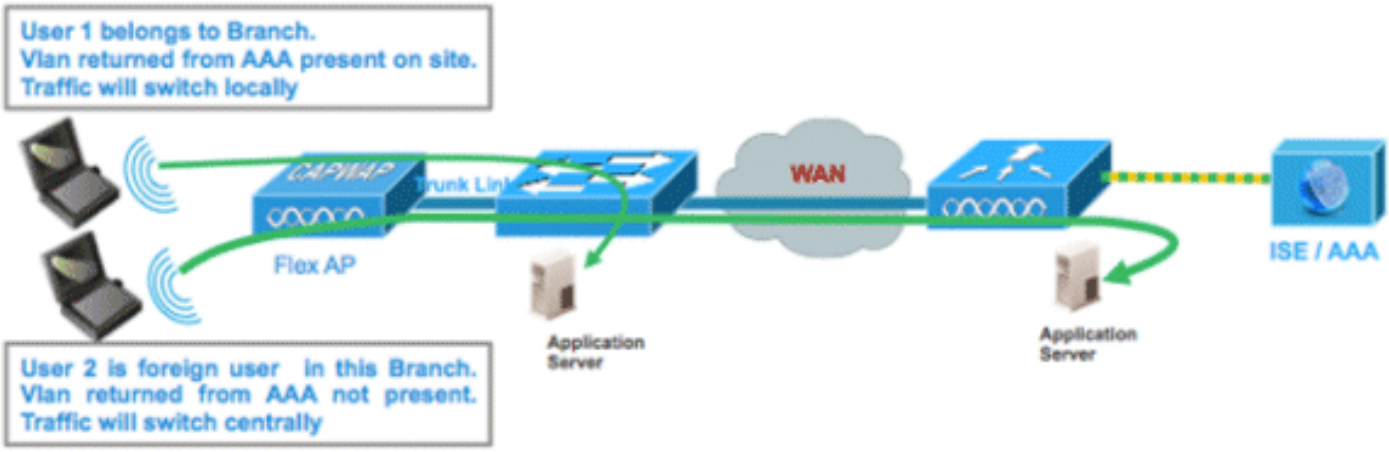
Limitazioni

- Gli attributi specifici di **Cisco Airespace** non saranno supportati e l'ID VLAN dell'attributo IETF sarà supportato solo.
- Èpossibile configurare un massimo di 16 VLAN in una configurazione per AP tramite il mapping WLAN-VLAN per un singolo access point FlexConnect o utilizzando il mapping ACL-VLAN sul gruppo FlexConnect.

Switching centrale basato su VLAN FlexConnect

Nel software dei controller versione 7.2, l'override AAA della VLAN (assegnazione VLAN dinamica) per le WLAN a commutazione locale inserirà i client wireless nella VLAN fornita dal server AAA. Se la VLAN fornita dal server AAA non è presente nel punto di accesso, il client viene indirizzato a una VLAN mappata WLAN su tale punto di accesso e il traffico verrà indirizzato localmente su tale VLAN. Inoltre, prima della versione 7.3, il traffico di una particolare WLAN proveniente dai punti di accesso FlexConnect può essere commutato a livello centrale o locale, a seconda della configurazione WLAN.

A partire dalla versione 7.3, il traffico proveniente dai punti di accesso FlexConnect può essere commutato a livello centrale o locale in base alla presenza di una VLAN su un punto di accesso FlexConnect.



Riepilogo

Flusso del traffico sulle WLAN configurate per lo switching locale quando i Flex AP sono in modalità connessa:

- Se la VLAN viene restituita come uno degli attributi AAA e la VLAN non è presente nel database Flex AP, il traffico verrà indirizzato centralmente e al client verrà assegnata questa VLAN/interfaccia restituita dal server AAA, a condizione che la VLAN sia presente sul WLC.
- Se la VLAN viene restituita come uno degli attributi AAA e la VLAN non è presente nel database Flex AP, il traffico verrà commutato centralmente. Se anche tale VLAN non è presente sul WLC, al client verrà assegnata una VLAN/interfaccia mappata su una WLAN sul WLC.
- Se la VLAN viene restituita come uno degli attributi AAA e la VLAN è presente nel database FlexConnect AP, il traffico verrà commutato localmente.
- Se la VLAN non viene restituita dal server AAA, al client verrà assegnata una VLAN mappata WLAN sull'access point FlexConnect e il traffico verrà commutato localmente.

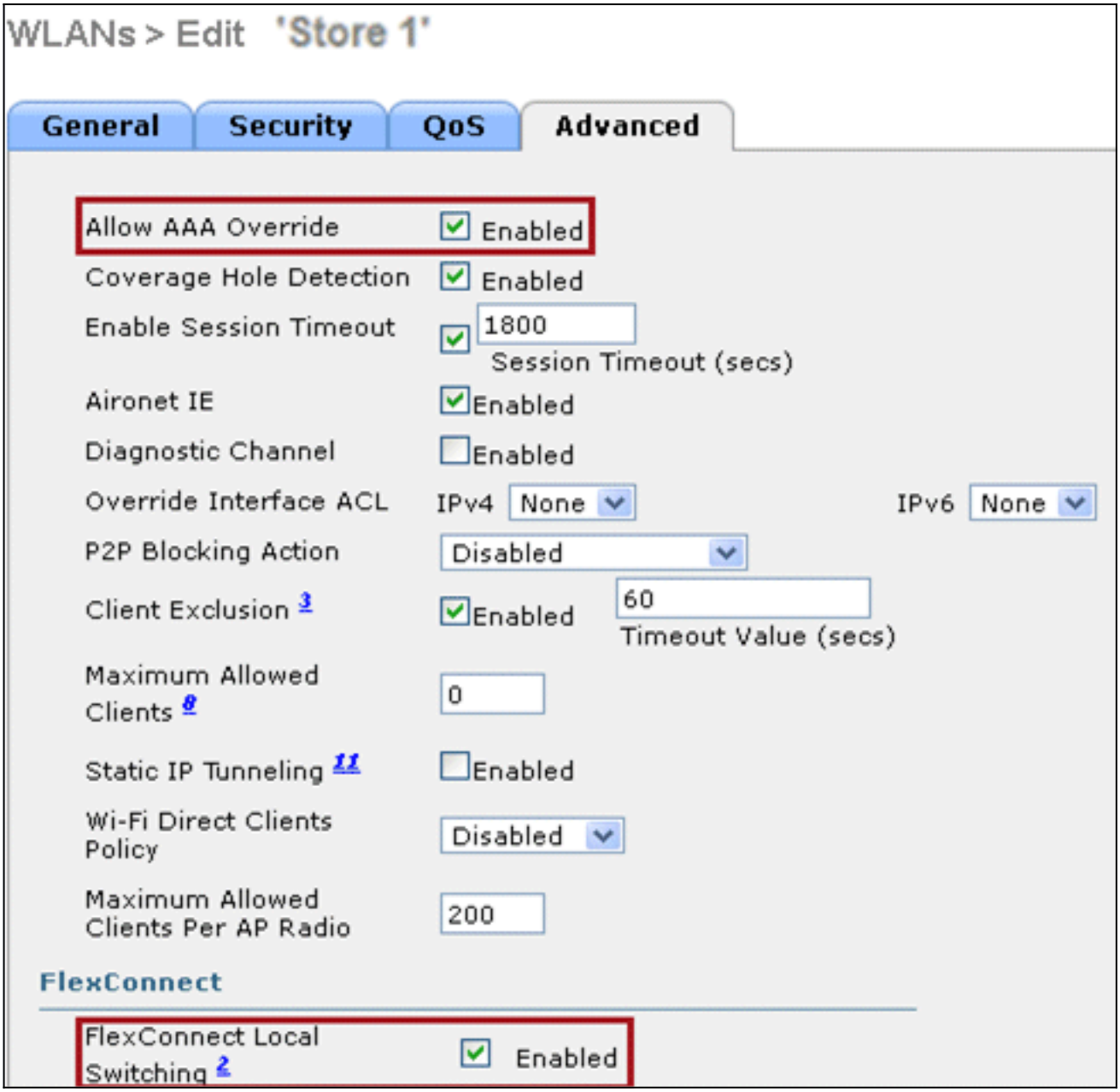
Flusso del traffico sulle WLAN configurate per lo switching locale quando i Flex AP sono in modalità standalone:

- Se la VLAN restituita da un server AAA non è presente nel database Flex AP, il client verrà impostato sulla VLAN predefinita (ossia, una VLAN mappata WLAN sull'access point Flex). Quando il punto di accesso si riconnette, il client viene deautenticato e il traffico viene commutato centralmente.
- Se la VLAN restituita da un server AAA è presente nel database Flex AP, il client verrà inserito in una VLAN restituita e il traffico verrà commutato localmente.
- Se la VLAN non viene restituita da un server AAA, al client verrà assegnata una VLAN mappata WLAN sull'access point FlexConnect e il traffico verrà commutato localmente.

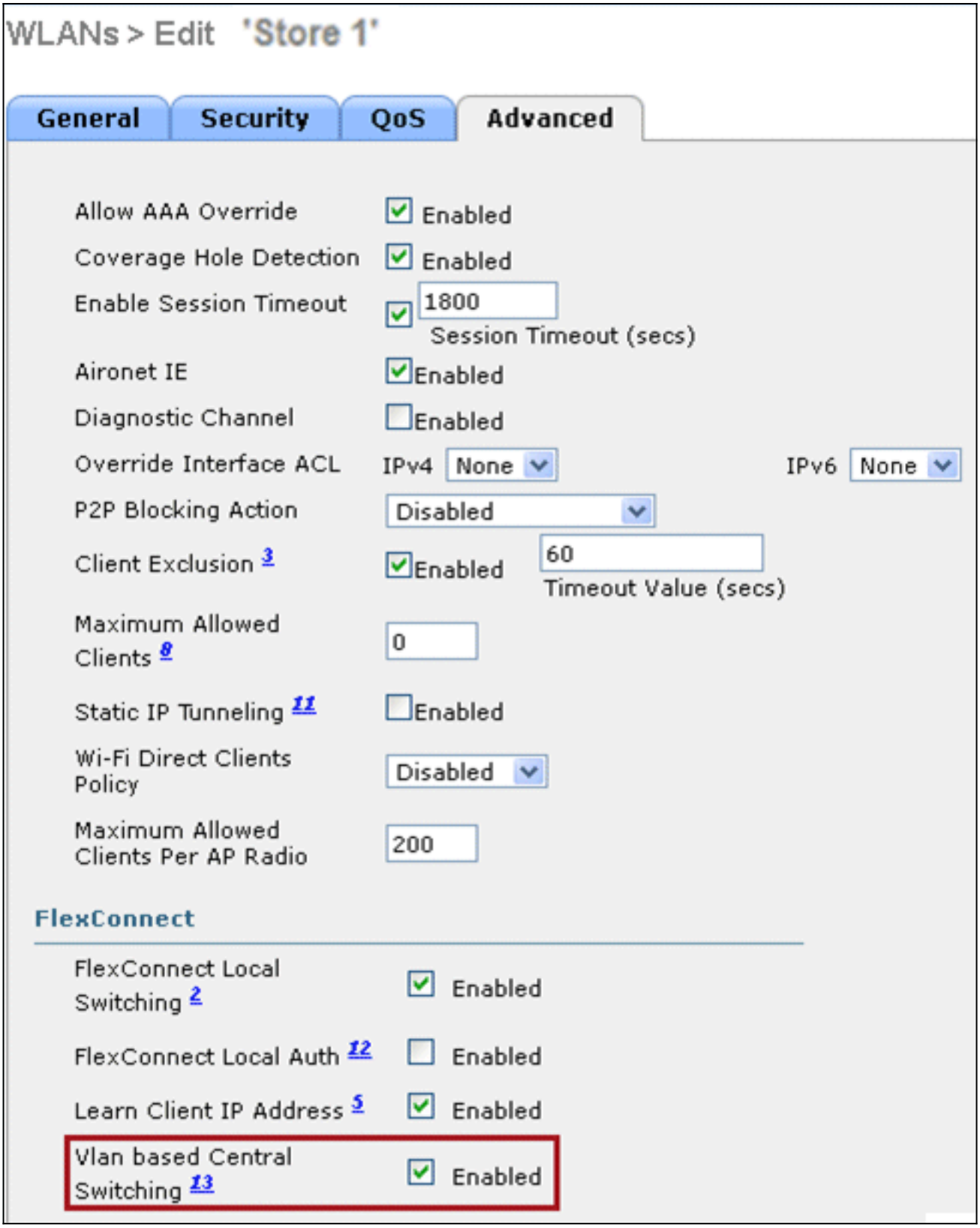
Procedura

Attenersi alla seguente procedura:

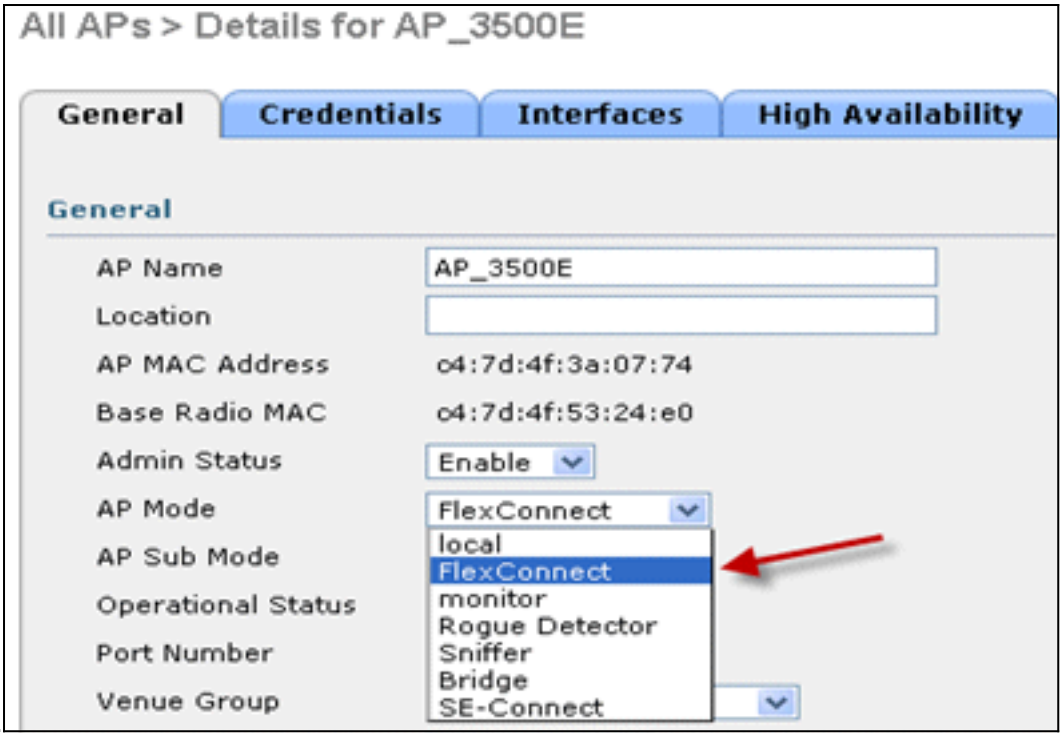
1. Configurare una WLAN per lo switching locale e abilitare l'override dell'AAA.



2. Abilitare la **commutazione centrale basata** sulla VLAN sulla WLAN appena creata.

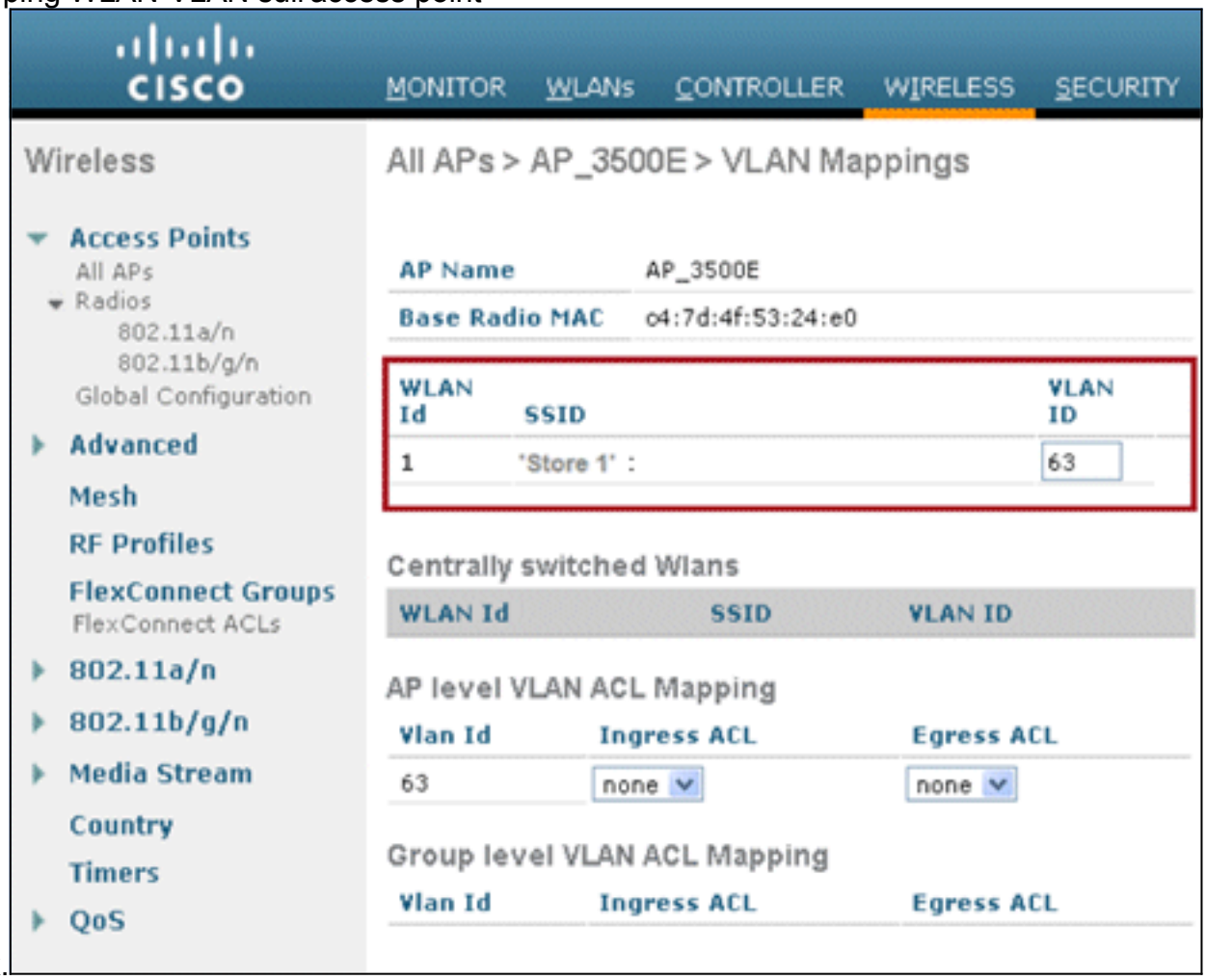


3. Impostare AP Mode (Modalità punto di accesso) su



FlexConnect.

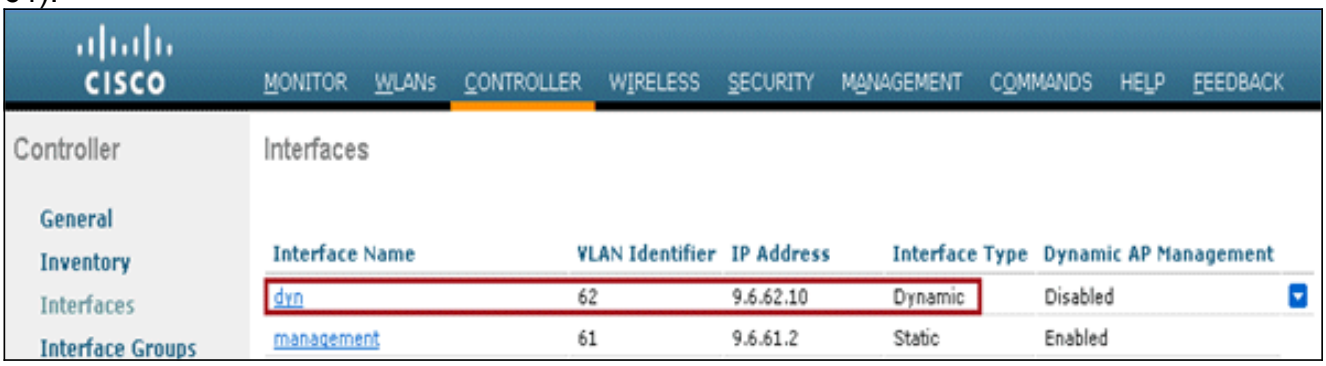
4. Verificare che il punto di accesso FlexConnect abbia una sottointerfaccia presente nel database, tramite il mapping WLAN-VLAN su un punto di accesso Flex specifico o configurando la VLAN da un gruppo Flex. Nell'esempio, la VLAN 63 è configurata nel mapping WLAN-VLAN sull'access point



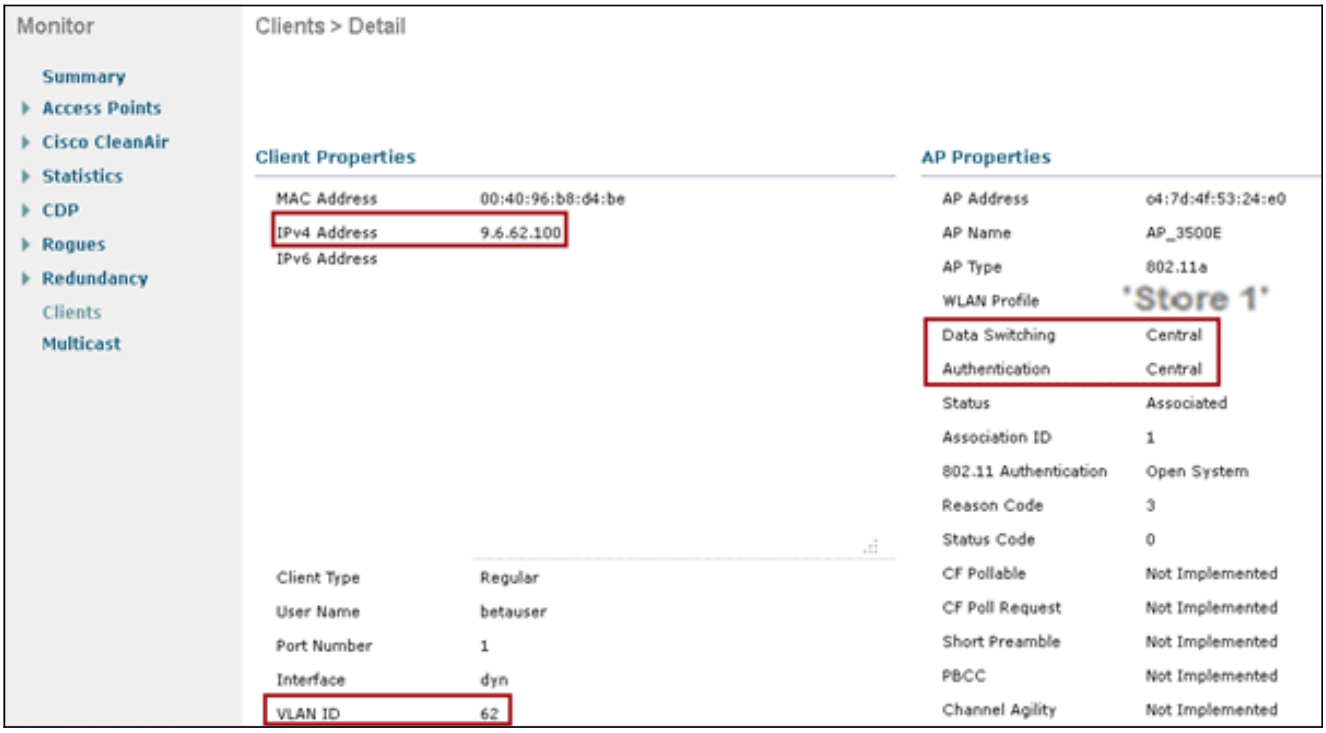
Flex.

5. Nell'esempio, la VLAN 62 è configurata sul WLC come una delle interfacce dinamiche e non è mappata alla WLAN sul WLC. La WLAN sul WLC è mappata alla VLAN di gestione (ossia, VLAN

61).

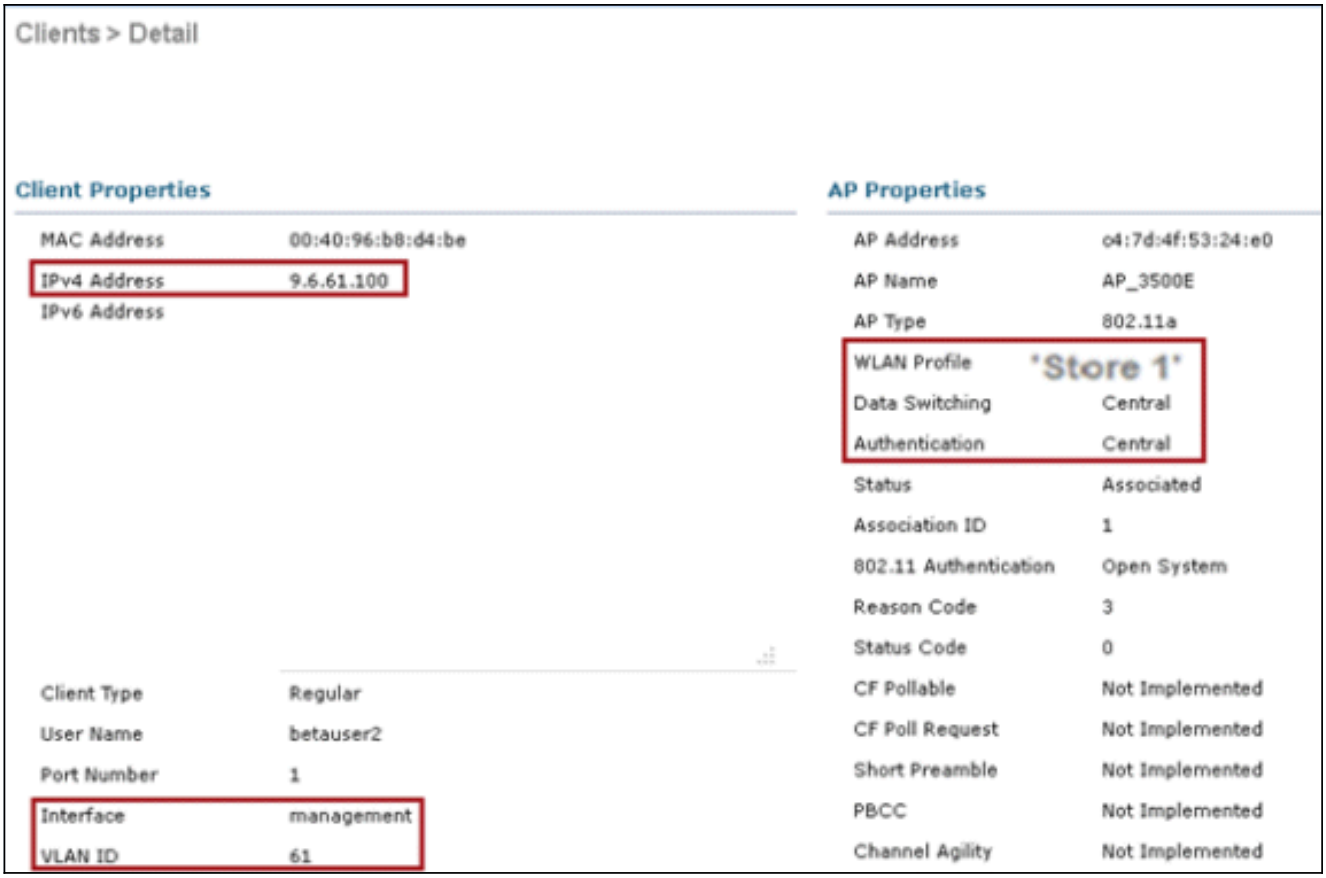


6. Associare un client alla WLAN configurata nel passaggio 1 su questo Flex AP e restituire la VLAN 62 dal server AAA. La VLAN 62 non è presente sul Flex AP, ma è presente sul WLC come interfaccia dinamica, quindi il traffico verrà commutato centralmente e al client verrà assegnata la VLAN 62 sul WLC. Nell'output mostrato di seguito, al client è stata assegnata la VLAN 62 e lo switching e l'autenticazione dei dati sono impostati su **Central**.



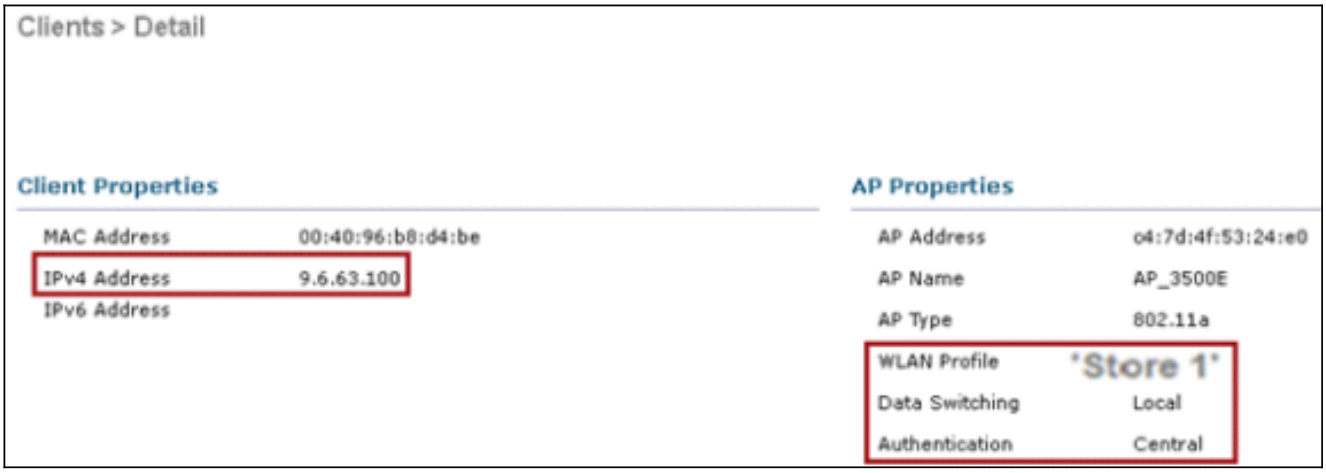
Nota: sebbene la WLAN sia configurata per lo switching locale, il campo Switching dei dati per questo client ha valore centrale in base alla presenza di una VLAN (ossia, la VLAN 62, restituita dal server AAA, non è presente nel database AP).

7. Se un altro utente si associa allo stesso access point su una WLAN creata e una VLAN viene restituita dal server AAA che non è presente sull'access point e sul WLC, il traffico verrà commutato centralmente e al client verrà assegnata l'interfaccia mappata sulla WLC (ossia, la VLAN 61 in questa configurazione di esempio), in quanto la WLAN è mappata sull'interfaccia di gestione configurata per la VLAN 61



Nota: sebbene la WLAN sia configurata per lo switching locale, il campo Switching dei dati per questo client è centrale in base alla presenza di una VLAN. Vale a dire che la VLAN 61, restituita dal server AAA, non è presente nel database AP ma neanche nel database WLC. Di conseguenza, al client viene assegnata un'interfaccia VLAN/interfaccia predefinita mappata alla WLAN. Nell'esempio, la WLAN è mappata a un'interfaccia di gestione (ossia, VLAN 61), quindi il client ha ricevuto un indirizzo IP dalla VLAN 61.

8. Se un altro utente lo associa alla WLAN creata e la VLAN 63 viene restituita dal server AAA (presente sul Flex AP), al client verrà assegnata la VLAN 63 e il traffico verrà commutato localmente.

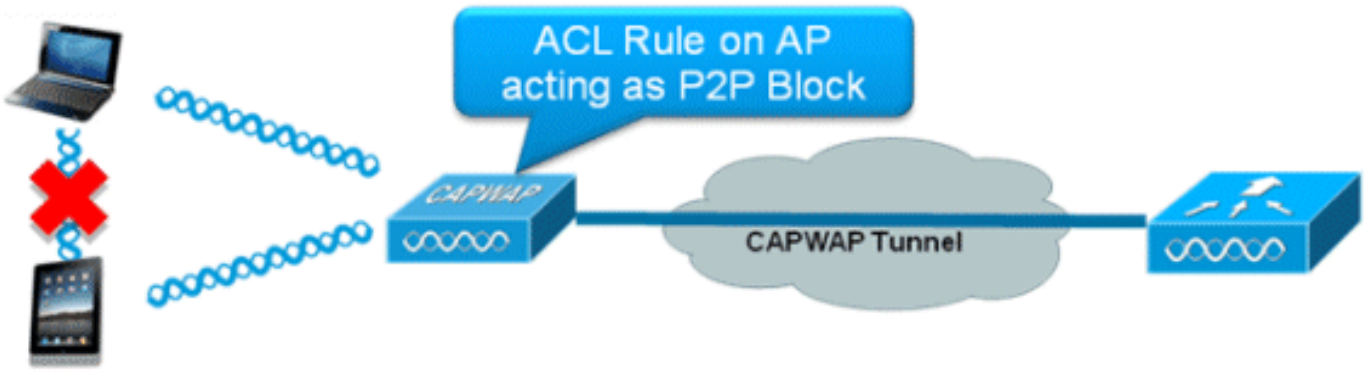


Limitazioni

- Lo switching centrale basato su VLAN è supportato solo sulle WLAN configurate per l'autenticazione centrale e lo switching locale.
- La sottointerfaccia AP (ossia, il mapping VLAN) deve essere configurata sull'access point FlexConnect.

ACL FlexConnect

Con l'introduzione degli ACL su FlexConnect, è disponibile un meccanismo che soddisfa la necessità di controllare l'accesso all'access point FlexConnect per la protezione e l'integrità del traffico di dati commutato localmente dall'access point. Gli ACL FlexConnect vengono creati sul WLC e devono essere configurati con la VLAN presente sull'access point FlexConnect o sul gruppo FlexConnect utilizzando il mapping VLAN-ACL che sarà per le VLAN di override AAA. che vengono quindi trasferiti all'AP.



Riepilogo

- Creare un ACL FlexConnect sul controller.
- Applicare la stessa procedura su una VLAN presente sull'access point FlexConnect in un mapping ACL VLAN a livello di access point.
- Può essere applicato su una VLAN presente nel gruppo FlexConnect con mapping VLAN-ACL (in genere eseguito per le VLAN con override AAA).
- Quando si applica l'ACL sulla VLAN, selezionare la direzione da applicare: "in entrata", "in uscita" o "in entrata e in uscita".

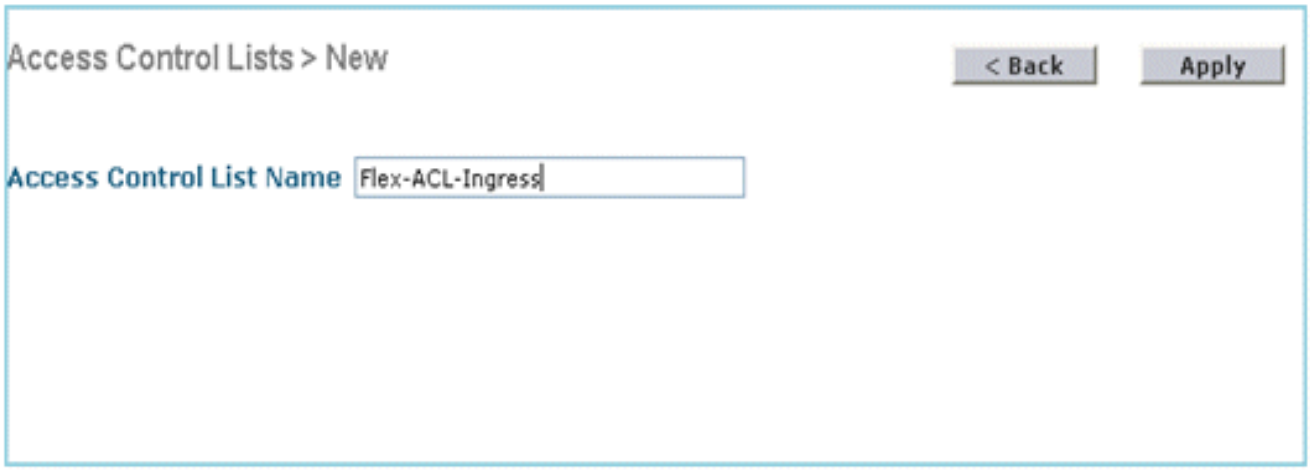
Procedura

Attenersi alla seguente procedura:

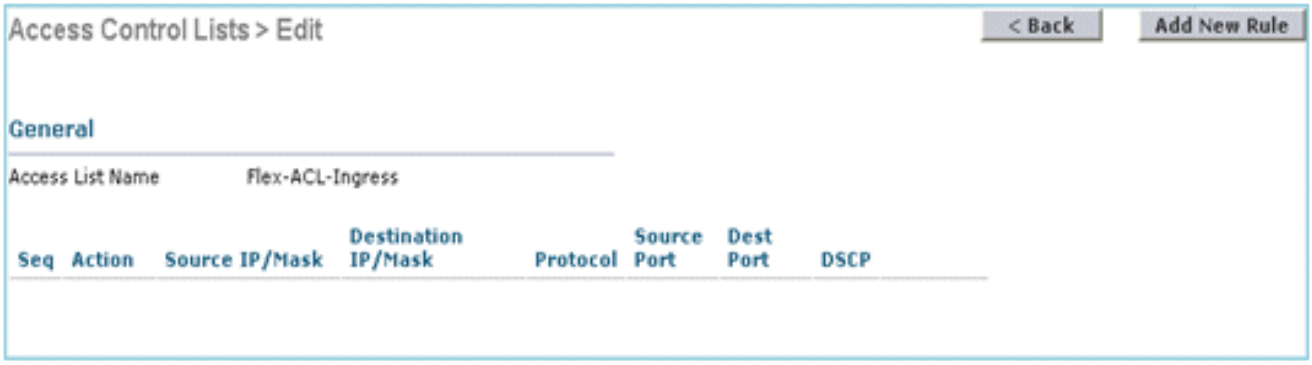
1. Creare un ACL FlexConnect sul WLC. Selezionare **WLC GUI > Security > Access Control List > ACL di FlexConnect**.

2. Fare clic su **New**.
3. Configurare il nome

ACL.



4. Fare clic su **Apply** (Applica).
5. Creare regole per ciascun ACL. Per creare le regole, selezionare **WLC GUI > Security > Access Control List > FlexConnect ACL**, quindi fare clic sull'ACL precedentemente creato.

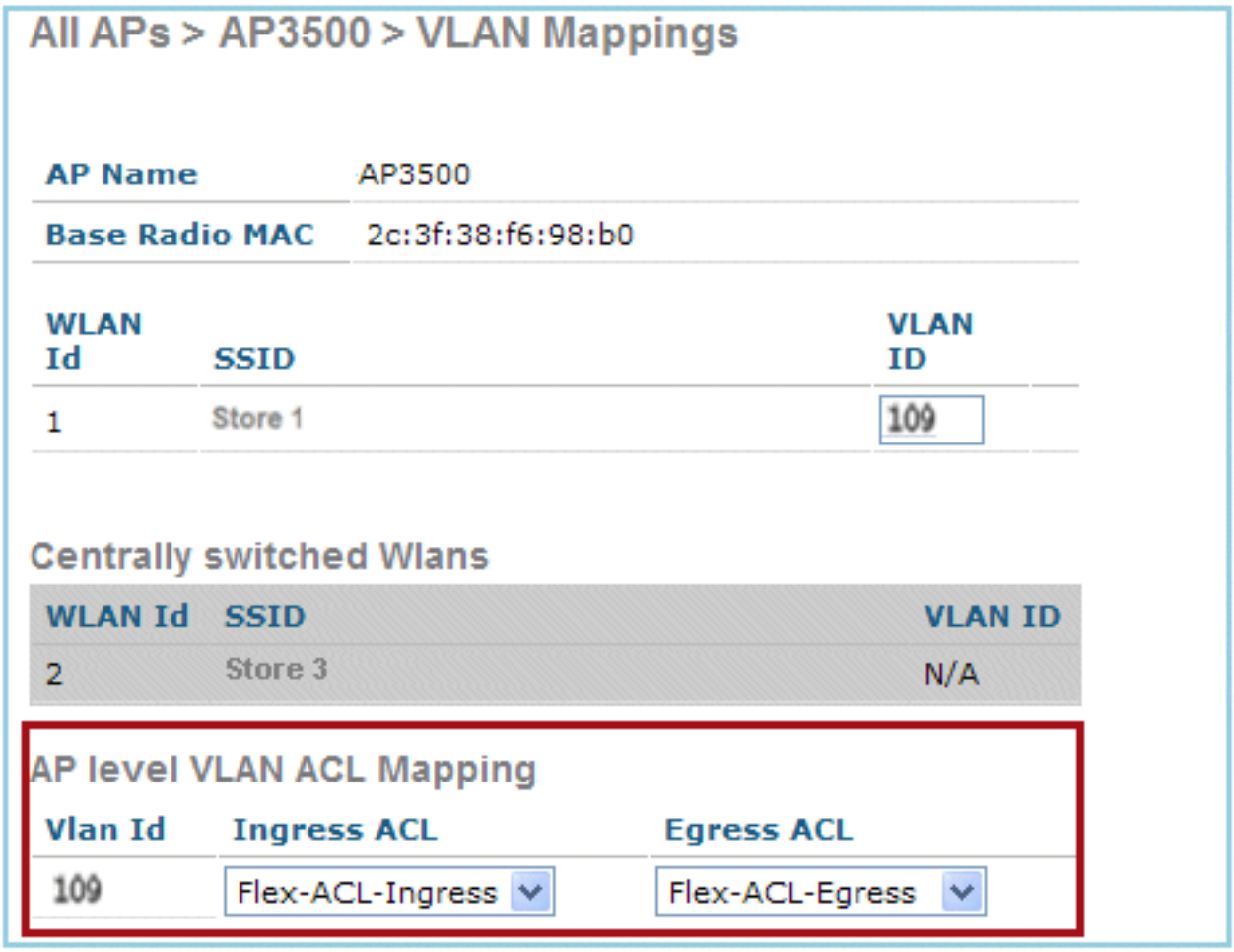


6. Fare clic su **Aggiungi nuova regola**.

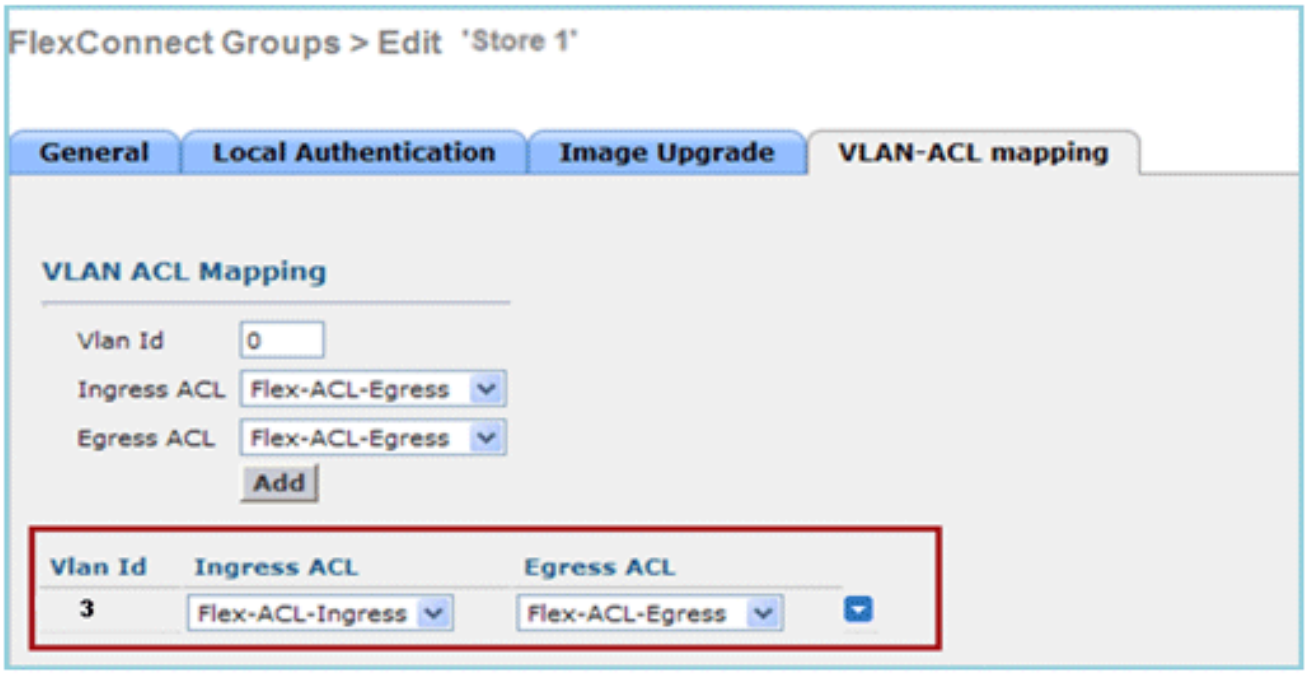
Nota: configurare le regole in base al requisito. Se alla fine non è configurata alcuna regola, viene generato un rifiuto implicito che bloccherà tutto il traffico.

7. Una volta creati gli ACL FlexConnect, è possibile mapparli per il mapping WLAN-VLAN in un singolo access point FlexConnect o applicarli sul mapping VLAN-ACL nel gruppo FlexConnect.
8. Mappare l'ACL FlexConnect configurato in precedenza a livello di access point per le singole VLAN nelle mappature VLAN per i singoli access point FlexConnect. Selezionare WLC GUI

> **Wireless** > **All AP** > fare clic sull'access point specifico > **scheda FlexConnect** > **Mapping VLAN**.



9. FlexConnect ACL può essere applicato anche al mapping VLAN-ACL nel gruppo FlexConnect. Le VLAN create con il mapping VLAN-ACL nel gruppo FlexConnect vengono usate principalmente per l'override della VLAN dinamica.



Limitazioni

- Èpossibile configurare un massimo di 512 ACL FlexConnect sul WLC.
- Ogni singolo ACL può essere configurato con 64 regole.
- Èpossibile mappare un massimo di 32 ACL per gruppo FlexConnect o per punto di accesso FlexConnect.
- In un determinato momento, il limite massimo è di 16 VLAN e 32 ACL sull'access point FlexConnect.

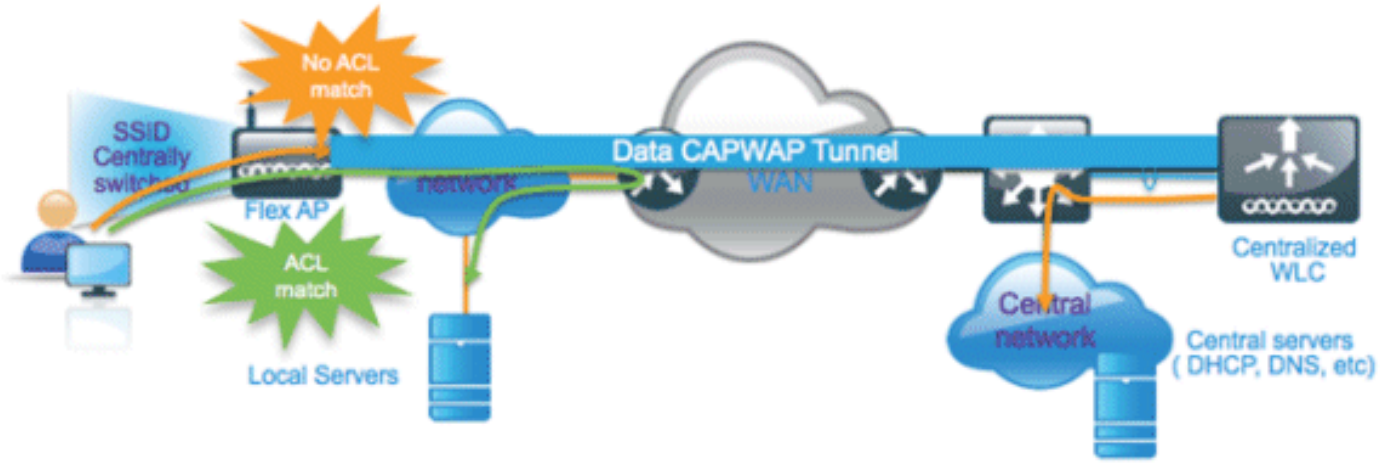
FlexConnect Split Tunneling

Nelle versioni WLC precedenti alla 7.3, se un client che si connette a un access point FlexConnect associato a una WLAN a commutazione centrale deve inviare del traffico a un dispositivo presente sul sito/rete locale, deve inviare il traffico su CAPWAP al WLC e quindi restituire lo stesso traffico al sito locale tramite CAPWAP o utilizzando una connettività off-band.

A partire dalla release 7.3, il **tunneling** in **split** introduce un meccanismo con cui il traffico inviato dal client viene classificato in base al contenuto del pacchetto **usando l'ACL Flex**. I pacchetti corrispondenti vengono scambiati localmente da Flex AP e gli altri pacchetti vengono scambiati centralmente su CAPWAP.

La funzionalità di tunneling ripartito è un ulteriore vantaggio dell'installazione di OEAP AP, in cui i client di un SSID aziendale possono comunicare direttamente con i dispositivi di una rete locale (stampanti, computer cablato su una porta LAN remota o dispositivi wireless su un SSID personale) senza utilizzare la larghezza di banda della WAN inviando pacchetti su CAPWAP. Il tunneling ripartito non è supportato sui punti di accesso OEAP 600. È possibile creare ACL Flex con regole per autorizzare tutti i dispositivi presenti sulla rete o sul sito locale. Quando i pacchetti provenienti da un client wireless sull'SSID aziendale soddisfano le regole nell'ACL Flex configurato sull'access point OEAP, il traffico viene commutato localmente e il resto del traffico (ossia, il traffico di negazione implicita) viene commutato centralmente su CAPWAP.

La soluzione di tunneling ripartito presume che la subnet/VLAN associata a un client nel sito centrale non sia presente nel sito locale (ossia, il traffico per i client che ricevono un indirizzo IP dalla subnet presente nel sito centrale non saranno in grado di passare localmente). La funzionalità di tunneling ripartito è progettata per commutare il traffico localmente per le subnet che appartengono al sito locale al fine di evitare il consumo della larghezza di banda della WAN. Il traffico che soddisfa le regole dell'ACL Flex viene commutato localmente e il funzionamento NAT viene eseguito modificando l'indirizzo IP di origine del client nell'indirizzo IP dell'interfaccia BVI del Flex AP che può essere instradato sulla rete o sul sito locale.



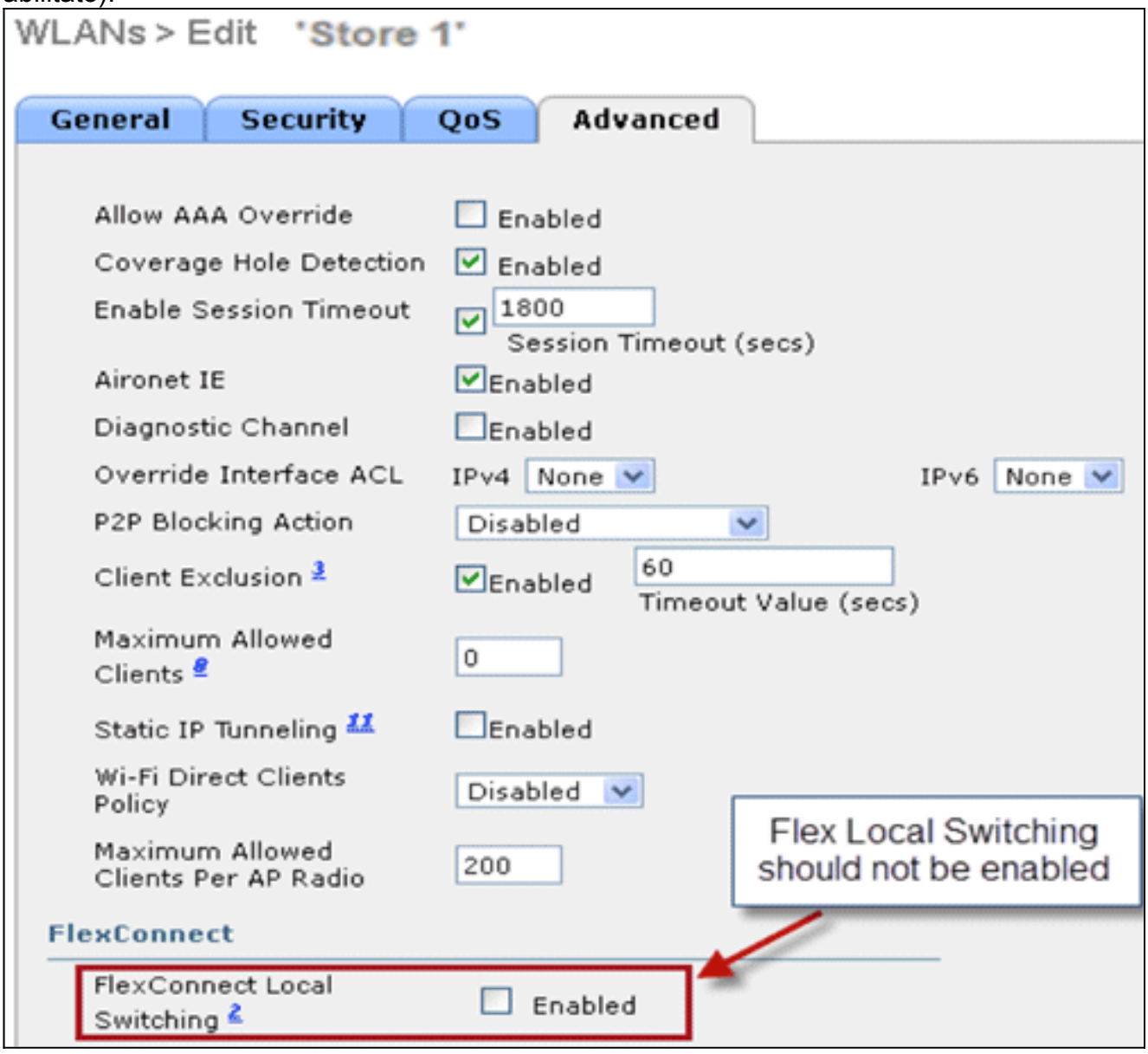
Riepilogo

- La funzionalità di tunneling ripartito è supportata sulle WLAN configurate per la commutazione centrale annunciate solo dai Flex AP.
- Il DHCP richiesto deve essere abilitato sulle WLAN configurate per il tunneling ripartito.
- La configurazione del tunneling ripartito viene applicata per ciascuna WLAN configurata per la commutazione centrale su ciascun Flex AP o su tutti i Flex AP di un gruppo FlexConnect.

Procedura

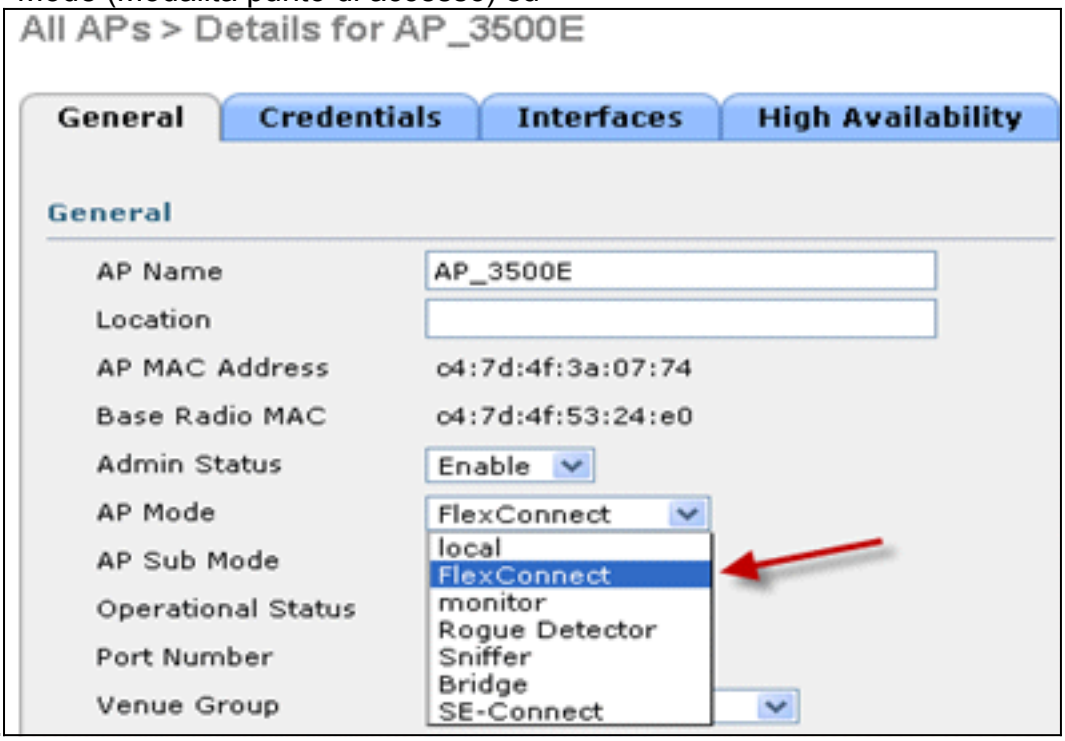
Attenersi alla seguente procedura:

1. Configurare una WLAN per lo switching centrale (ossia, lo **switching locale Flex** non deve essere
abilitato).



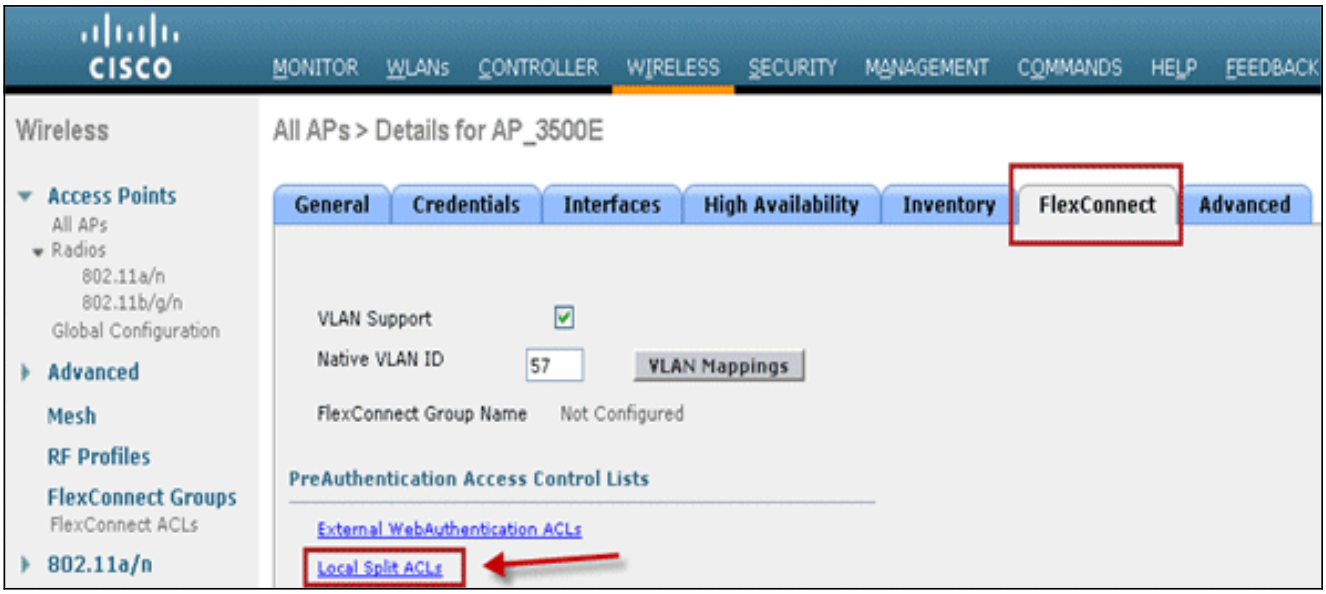
2. Impostare Assegnazione indirizzo DHCP su **Obbligatorio**.

3. Impostare AP Mode (Modalità punto di accesso) su FlexConnect.

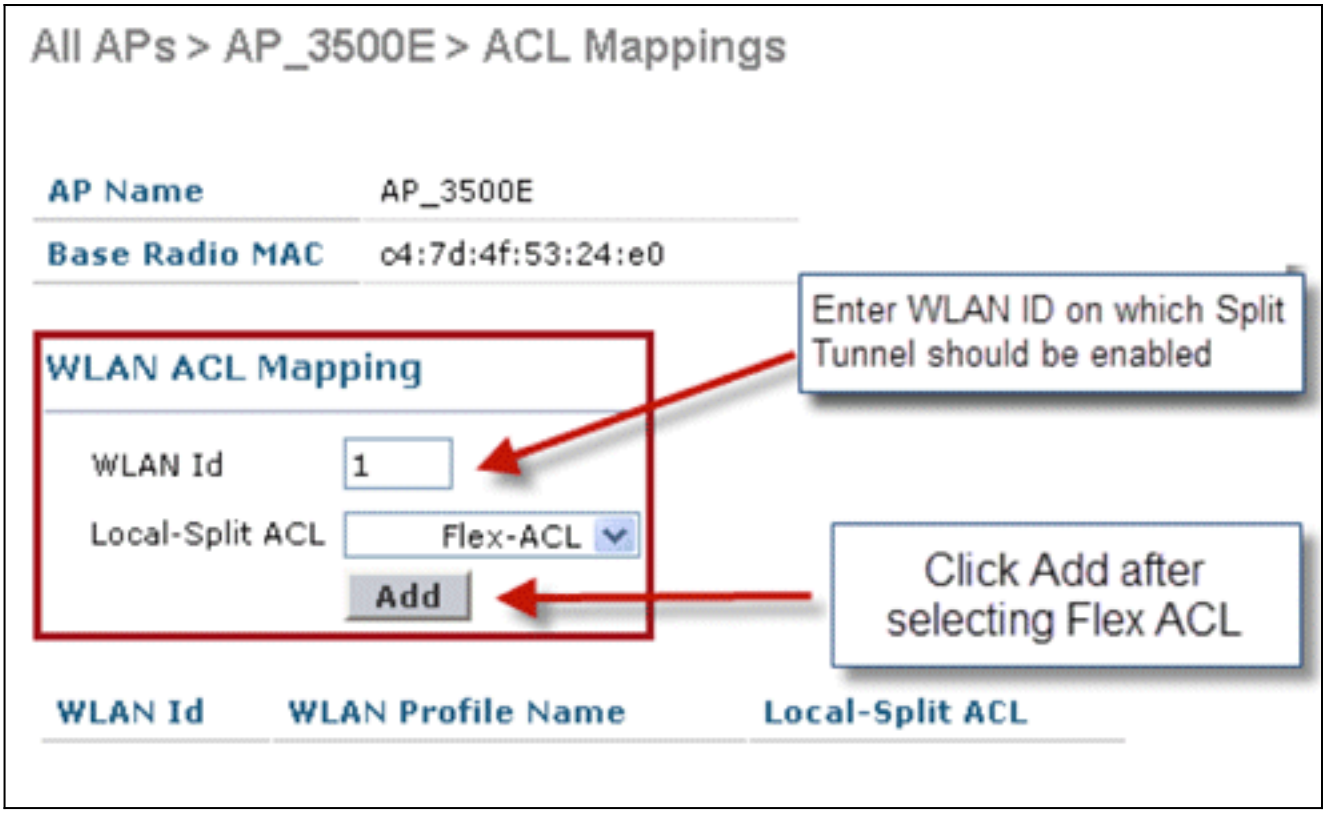


4. Configurare l'ACL di FlexConnect con una regola di autorizzazione per il traffico che deve essere commutato localmente sulla WLAN dello switch centrale. Nell'esempio, la regola ACL di FlexConnect è configurata in modo da avvisare il traffico ICMP da tutti i client che si trovano nella subnet 9.6.61.0 (ossia, che si trovano nel sito centrale) alla subnet 9.1.0.150 in modo che vengano commutati localmente dopo l'applicazione dell'operazione NAT sull'access point Flex. Il resto del traffico verrà bloccato da una regola di negazione implicita e verrà scambiato centralmente su CAPWAP.

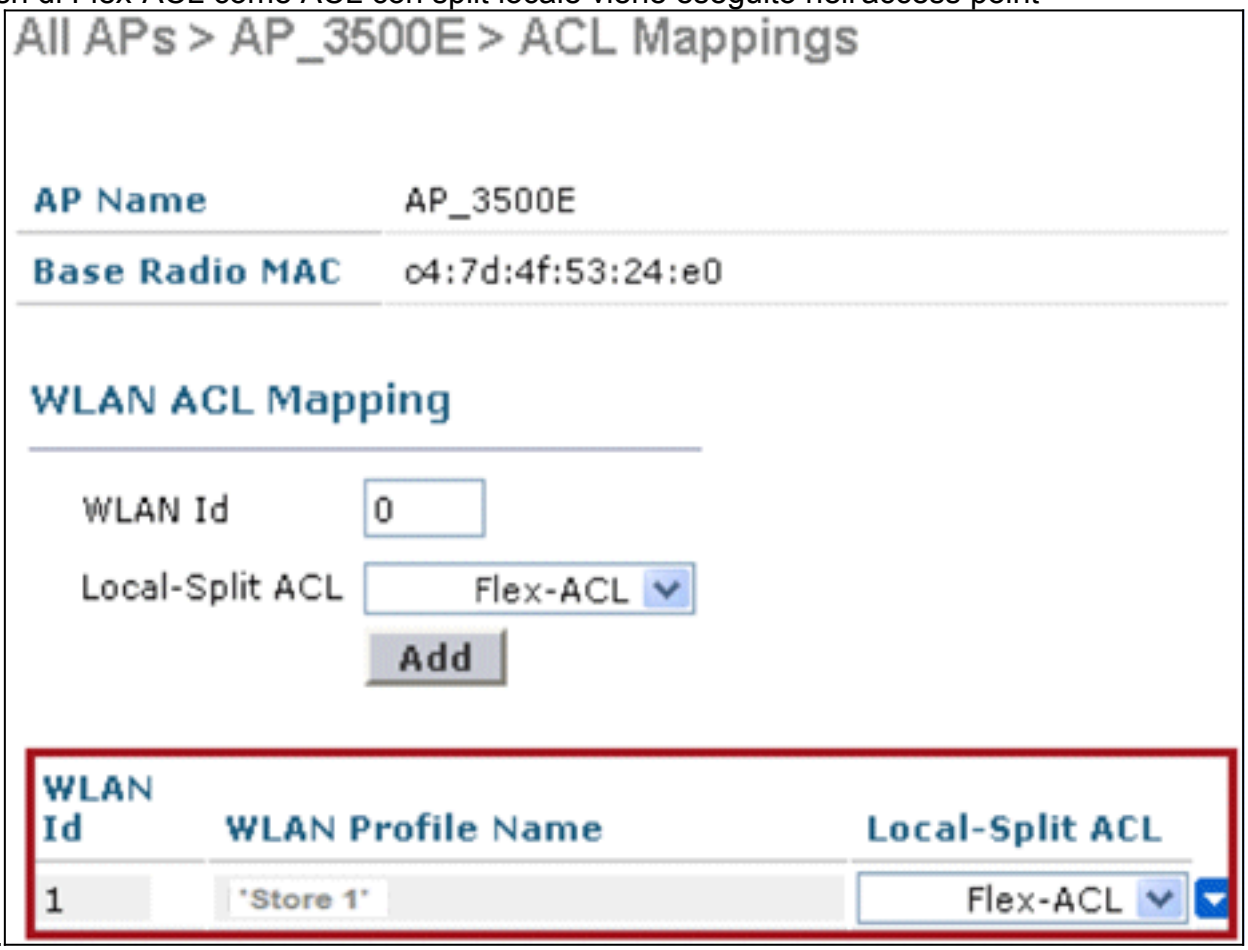
5. Èpossibile eseguire il push di questo ACL FlexConnect creato come ACL con tunnel suddiviso in un singolo Flex AP o in tutti gli Flex AP di un gruppo Flex Connect.Completare questa procedura per eseguire il push di un ACL Flex come ACL con split locale su un singolo Flex AP:Fare clic su **ACL suddivisi locali**.



Selezionare l'**ID WLAN** su cui abilitare la funzione Split Tunnel, scegliere **Flex-ACL** e fare clic su **Add**.



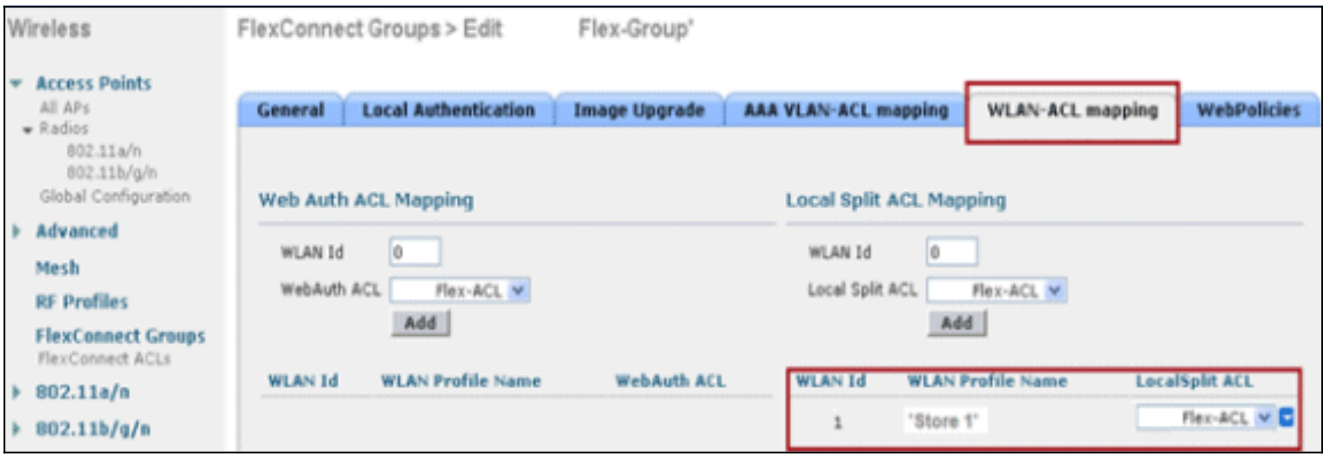
Il push di Flex-ACL come ACL con split locale viene eseguito nell'access point



Flex.

Completare questa procedura per eseguire il push di un ACL Flex come ACL con split locale in un gruppo FlexConnect:Selezionare l'ID WLAN su cui abilitare la funzione di tunneling ripartito. Nella scheda **Mappatura WLAN-ACL**, selezionare FlexConnect ACL dal gruppo FlexConnect a cui sono stati aggiunti determinati Flex AP, quindi fare clic su **Aggiungi**.

Il push dell'ACL Flex-Express come ACL LocalSplit viene eseguito sugli AP Flex del gruppo Flex.



Limitazioni

- Le regole ACL Flex non devono essere configurate con l'istruzione allow/deny con la stessa subnet dell'origine e della destinazione.
- Il traffico su una WLAN con switching centrale configurata per il tunneling ripartito può essere commutato localmente solo quando un client wireless avvia il traffico per un host presente sul sito locale. Se il traffico viene avviato dai client/host su un sito locale per i client wireless su queste WLAN configurate, non sarà possibile raggiungere la destinazione.
- Tunneling ripartito non supportato per il traffico multicast/broadcast. Il traffico multicast/broadcast si commuta centralmente anche se corrisponde all'ACL Flex.

Fault Tolerance

FlexConnect Fault Tolerance consente l'accesso wireless e i servizi ai client delle filiali quando:

- I FlexConnect Branch AP perdono la connettività con il controller Flex 7500 principale.
- Èin corso il passaggio dei FlexConnect Branch AP al controller Flex 7500 secondario.
- Gli access point FlexConnect Branch stanno ristabilendo la connessione al controller Flex 7500 primario.

FlexConnect Fault Tolerance, insieme all'EAP locale come descritto in precedenza, forniscono tempi di inattività zero per le filiali durante un'interruzione della rete. Questa funzionalità è abilitata per impostazione predefinita e non può essere disabilitata. Non richiede alcuna configurazione sul controller o sull'access point. Tuttavia, per garantire che la tolleranza di errore funzioni correttamente e sia applicabile, è opportuno mantenere questo criterio:

- Le configurazioni e gli ordini delle WLAN devono essere identici sui controller primario e di backup Flex 7500.
- La mappatura della VLAN deve essere identica sui controller primario e di backup Flex 7500.
- Il nome del dominio di mobilità deve essere identico nei controller primario e di backup Flex 7500.
- Si consiglia di utilizzare Flex 7500 sia come controller principale che come controller di backup.

Riepilogo

- FlexConnect non disconnetterà i client quando l'access point si riconnette allo stesso controller, a condizione che non vi siano modifiche nella configurazione del controller.
- FlexConnect non disconnette i client durante la connessione al controller di backup, a condizione che non vi siano modifiche nella configurazione e che il controller di backup sia identico al controller primario.
- FlexConnect non reimposta le proprie radio al momento della connessione al controller primario, a condizione che non vi siano modifiche nella configurazione del controller.

Limitazioni

- Supportato solo per FlexConnect con autenticazione centrale/locale con switching locale.
- I client autenticati centralmente richiedono una riautenticazione completa se il timer della sessione client scade prima che il punto di accesso FlexConnect passi dalla modalità standalone alla modalità connessa.
- I controller primario e di backup Flex 7500 devono trovarsi nello stesso dominio di mobilità.

Limite client per WLAN

Oltre alla segmentazione del traffico, è necessario limitare il totale dei client che accedono ai servizi wireless.

Esempio: Limitazione del totale dei client guest dal tunneling delle filiali al data center.

Per risolvere questo problema, Cisco sta introducendo la funzione Client Limit per WLAN, che può limitare il totale di client autorizzati per singola WLAN.

Obiettivo principale

- Imposta limiti per il numero massimo di client
- Semplicità operativa

Nota: questa non è una forma di QoS.

Per impostazione predefinita, la funzione è disattivata e non impone il limite.

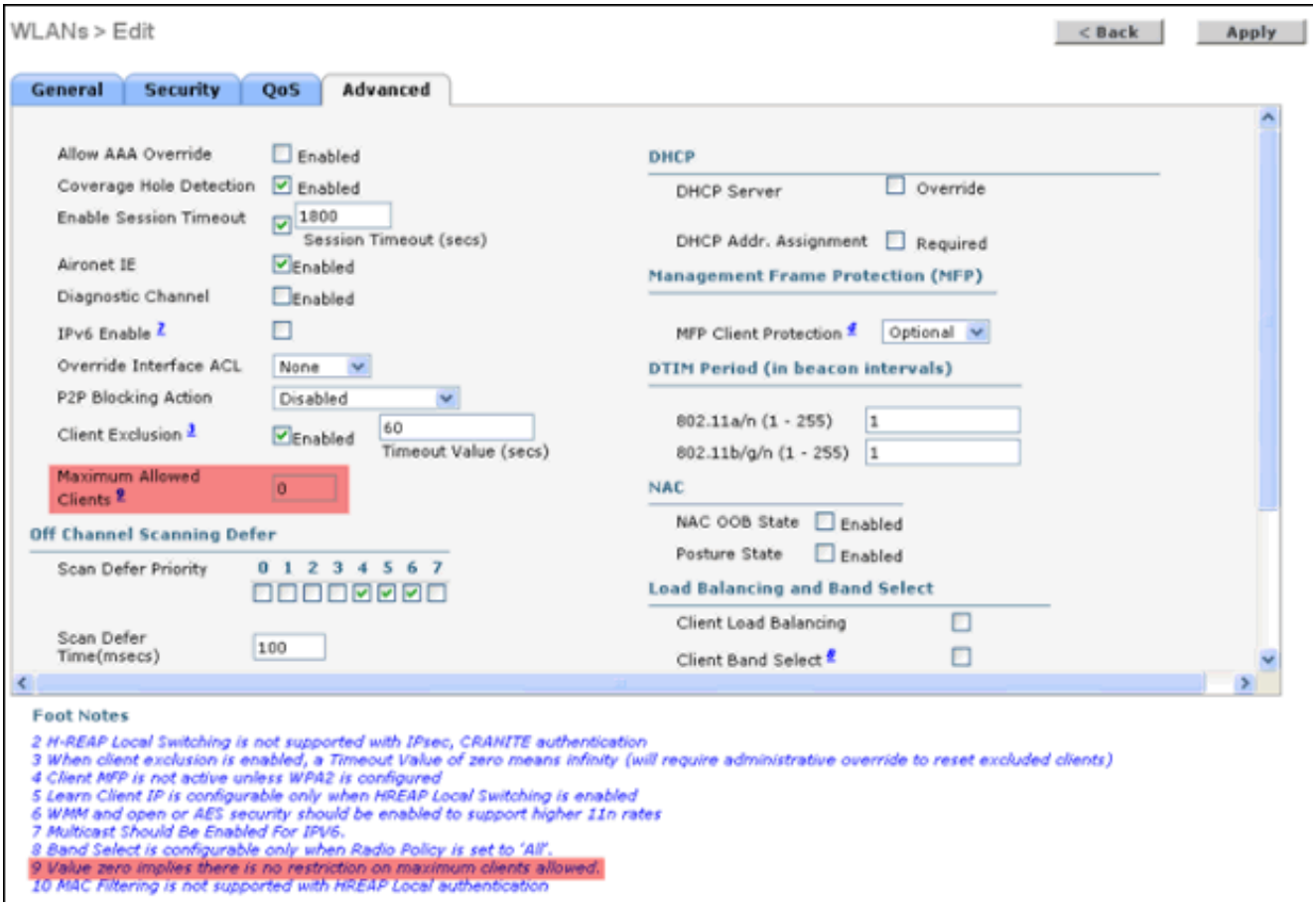
Limitazioni

Questa funzione non applica il limite client quando FlexConnect è in stato Standalone.

Configurazione WLC

Attenersi alla seguente procedura:

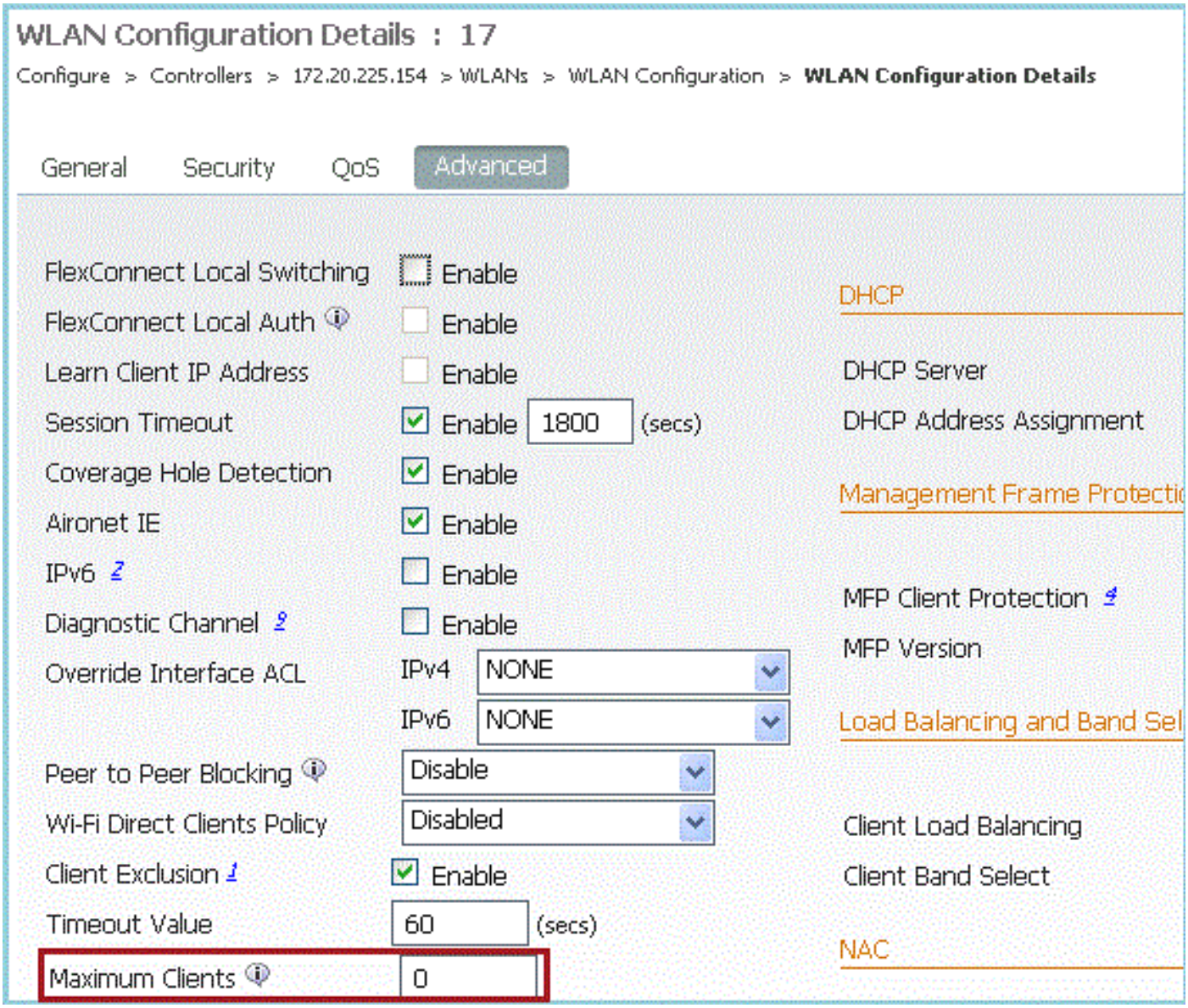
1. Selezionare l'ID WLAN 1 con commutazione centrale con SSID **DataCenter**. Questa WLAN è stata creata durante LA creazione del gruppo AP. Vedere la Figura 8.
2. Fare clic sulla scheda **Advanced** (Avanzate) per l'ID WLAN 1.
3. Impostare il valore del limite client per il campo di testo Numero massimo client consentiti.
4. Fare clic su **Applica** dopo aver impostato il campo di testo per Numero massimo client autorizzati.



L'impostazione predefinita per Numero massimo client consentiti è 0, il che implica che non esistono restrizioni e che la funzione è disabilitata.

Configurazione NCS

Per abilitare questa funzione dall'NCS, selezionare Configurazione > Controller > IP controller > **WLAN > Configurazione WLAN > Dettagli configurazione WLAN**.

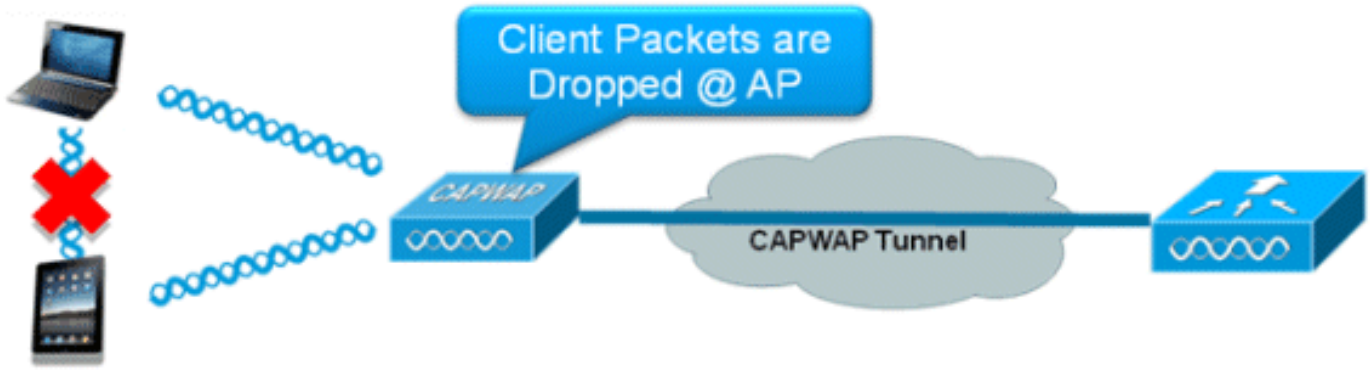


Blocco peer-to-peer

Nelle versioni software dei controller precedenti alla 7.2, il blocco P2P (peer-to-peer) era supportato solo per le WLAN di switching centrale. Il blocco peer-to-peer può essere configurato sulla WLAN in uno dei tre modi seguenti:

- **Disabilitato**: disabilita il blocco peer-to-peer e il traffico con bridging locale nel controller per i client nella stessa subnet. Questo è il valore predefinito.
- **Drop**: causa l'eliminazione dei pacchetti dei client nella stessa subnet.
- **Forward Up-Stream**: determina l'inoltro del pacchetto sulla VLAN upstream. Le periferiche sopra il controller decidono quale azione intraprendere riguardo al pacchetto.

A partire dalla versione 7.2, il blocco peer-to-peer è supportato per i client associati alla WLAN di switching locale. In base alla WLAN, la configurazione peer-to-peer viene trasferita dal controller all'access point FlexConnect.



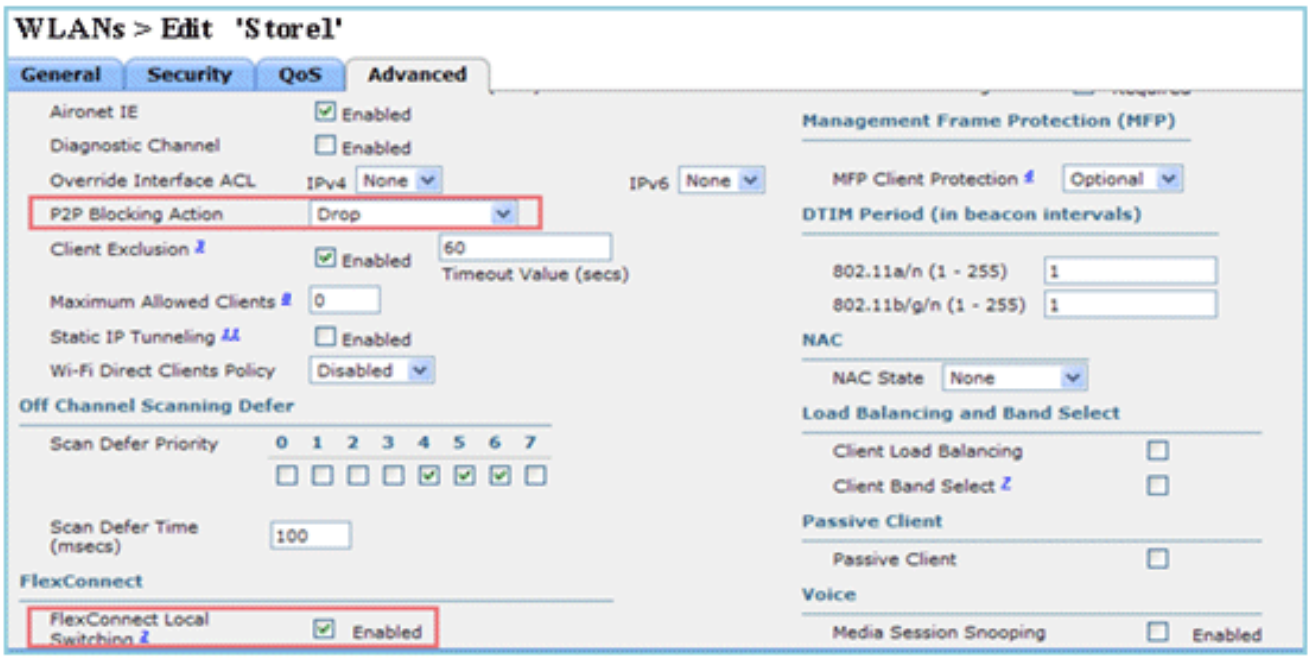
Riepilogo

- Il blocco peer-to-peer è configurato per WLAN
- In base alla WLAN, la configurazione del blocco peer-to-peer viene trasferita dal WLC ai FlexConnect AP.
- L'azione di blocco peer-to-peer configurata come drop o upstream-forward sulla WLAN viene considerata come blocco peer-to-peer abilitato sull'access point FlexConnect.

Procedura

Attenersi alla seguente procedura:

1. Abilita l'azione di blocco peer-to-peer come **drop** sulla WLAN configurata per lo switching locale
   FlexConnect.



2. Una volta configurata l'azione di blocco P2P come **Drop** o **Forward-Upstream** sulla WLAN configurata per la commutazione locale, l'azione viene trasferita dal WLC all'access point FlexConnect. I punti di accesso FlexConnect memorizzeranno queste informazioni nel file di configurazione del mapping nella memoria flash. Con questo, anche quando FlexConnect AP è in modalità standalone, può applicare la configurazione P2P sulle sottointerfacce corrispondenti.

Limitazioni

- In FlexConnect, la configurazione del blocco P2P della soluzione non può essere applicata solo a un determinato punto di accesso FlexConnect o a un sottoinsieme di punti di accesso. Viene applicata a tutti gli access point FlexConnect che trasmettono l'SSID.
- La soluzione unificata per client di switching centrale supporta il upstream-forward P2P. Tuttavia, questa funzionalità non è supportata nella soluzione FlexConnect. Questa operazione viene considerata come rilascio P2P e i pacchetti client vengono scartati anziché inoltrati al nodo di rete successivo.
- La soluzione unificata per i client di switching centrale supporta il blocco P2P per i client associati a diversi punti di accesso. Tuttavia, questa soluzione è destinata solo ai client connessi allo stesso access point. Per risolvere questo problema, è possibile usare gli ACL FlexConnect.

Download pre-immagine AP

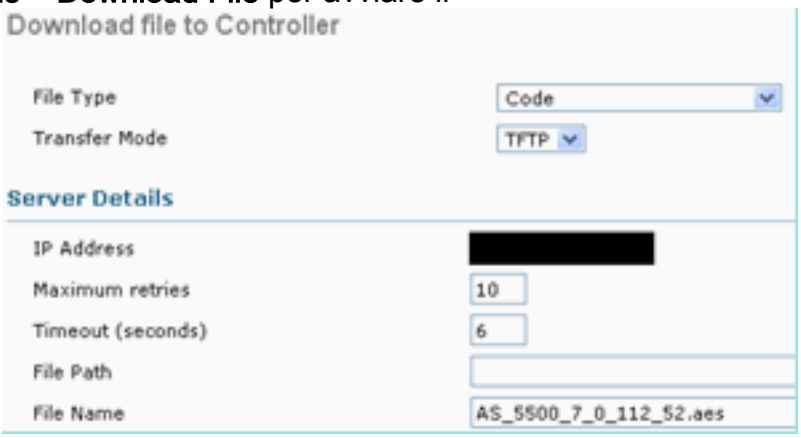
Questa funzione consente all'access point di scaricare il codice mentre è operativo. Il download pre-immagine dell'access point è estremamente utile per ridurre il downtime della rete durante la manutenzione o gli aggiornamenti del software.

Riepilogo

- Facilità di gestione del software
- Pianificazione aggiornamenti per punto vendita: l'NCS è necessaria per raggiungere questo obiettivo
- Riduzione dei tempi di inattività

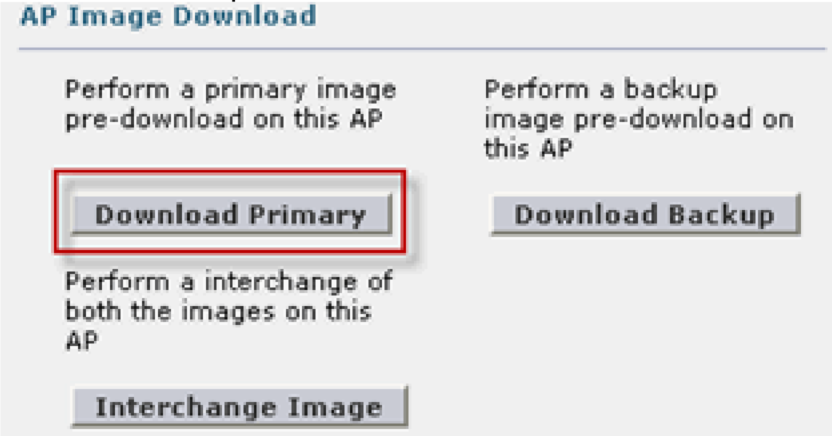
Procedura

Attenersi alla seguente procedura:

1. Aggiornare l'immagine nei controller primario e di backup.Selezionare **WLC GUI > Commands > Download File** per avviare il download.


2. Salvare le configurazioni sui controller, ma non riavviare il controller.
3. Eseguire il comando AP pre-image download dal controller primario.Selezionare **WLC GUI > Wireless > Access Point > All AP** (Interfaccia utente WLC > Wireless > Access Point > Tutti gli AP) e scegliere il punto di accesso per avviare il download pre-immagine.Una volta scelto

il punto di accesso, fare clic sulla scheda **Avanzate**.Fare clic su **Scarica principale** per avviare il download di una pre-immagine.




```
*Sep 13 21:21:14.903: %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. Riavviare i controller dopo aver scaricato tutte le immagini AP.Ora gli access point tornano in modalità standalone finché i controller non vengono riavviati.**Nota:** in modalità standalone, Fault Tolerance mantiene i client associati.Una volta ripristinato il controller, gli access point si riavviano automaticamente con l'immagine scaricata in precedenza.Dopo il riavvio, gli access point si uniscono nuovamente al controller primario e riprendono i servizi del client.

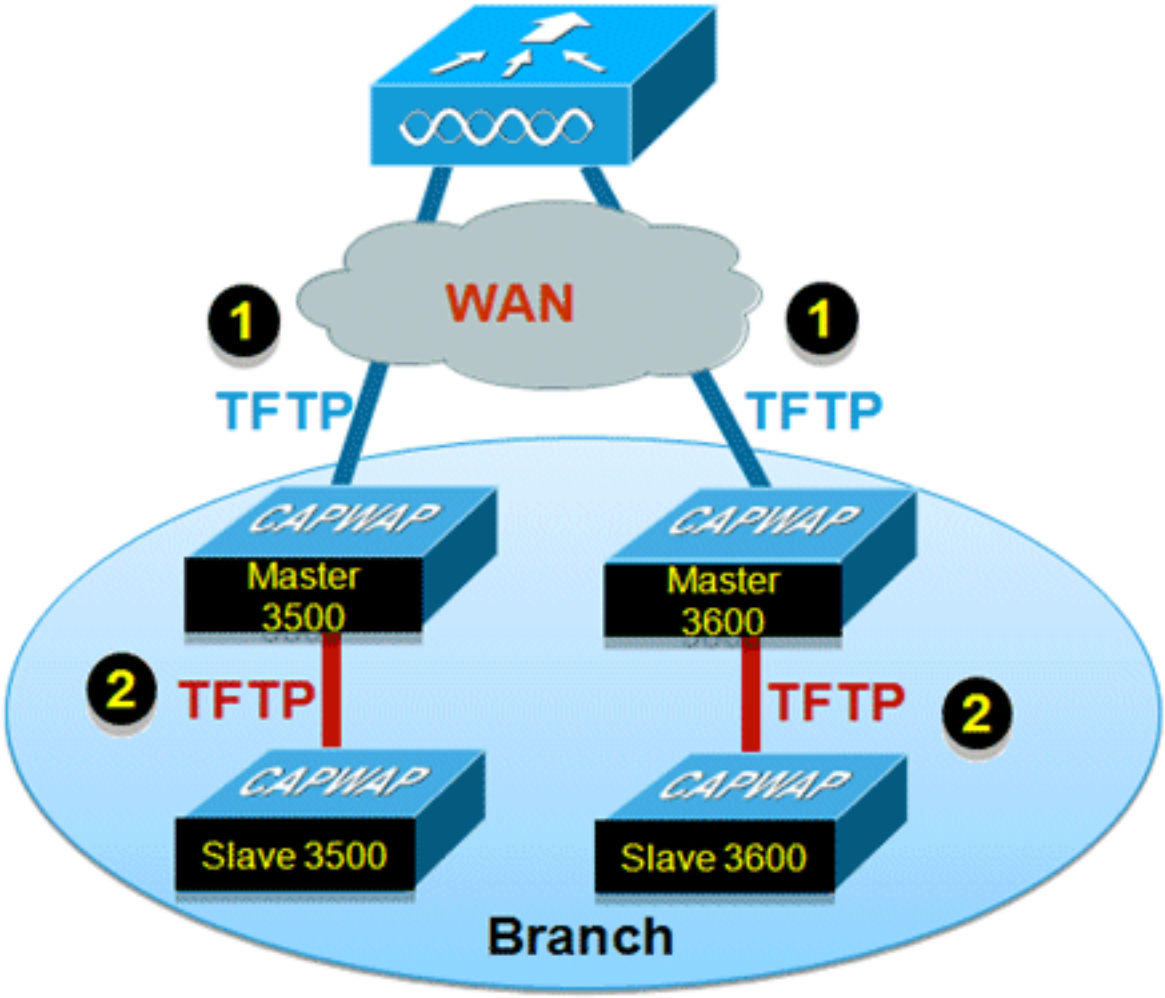
Limitazioni

- Funziona solo con i CAPWAP AP.

Aggiornamento immagine FlexConnect Smart AP

La funzione di download pre-immagine riduce in una certa misura la durata del downtime, ma tutti i punti di accesso FlexConnect devono comunque pre-scaricare le rispettive immagini dei punti di accesso sul collegamento WAN con una latenza maggiore.

L'aggiornamento efficiente dell'immagine AP ridurrà i tempi di inattività di ciascun punto di accesso FlexConnect. L'idea di base è che solo un punto di accesso per ogni modello di punto di accesso scaricherà l'immagine dal controller e agirà come Master/Server, mentre gli altri punti di accesso dello stesso modello funzioneranno come Slave/Client e pre-scaricheranno l'immagine dal master. La distribuzione dell'immagine AP dal server al client avverrà su una rete locale e non avrà la latenza del collegamento WAN. Di conseguenza, il processo sarà più rapido.



Riepilogo

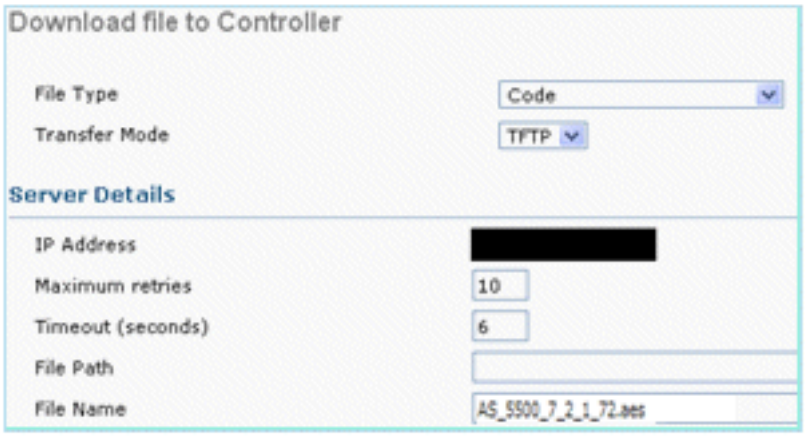
- Gli AP master e slave vengono selezionati per ciascun modello AP per ciascun gruppo FlexConnect
- Master scarica l'immagine dal WLC
- Slave scarica l'immagine dal punto di accesso master

- Riduzione dei tempi di inattività e risparmio della larghezza di banda della WAN

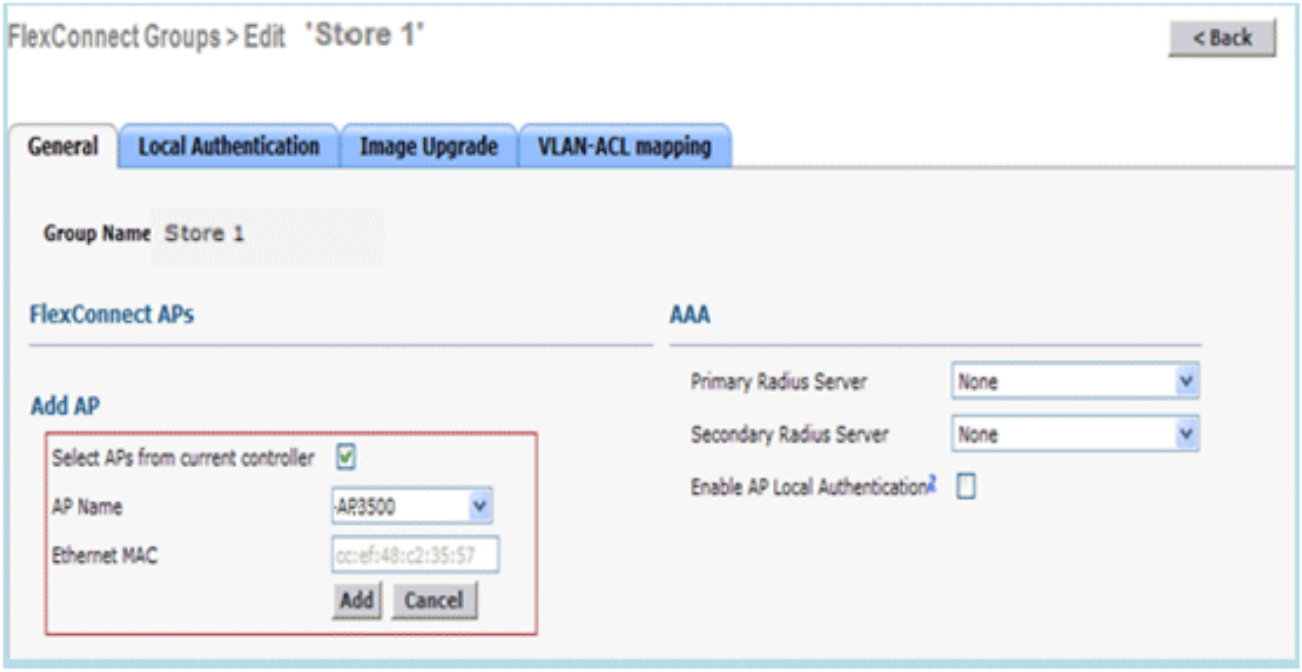
Procedura

Attenersi alla seguente procedura:

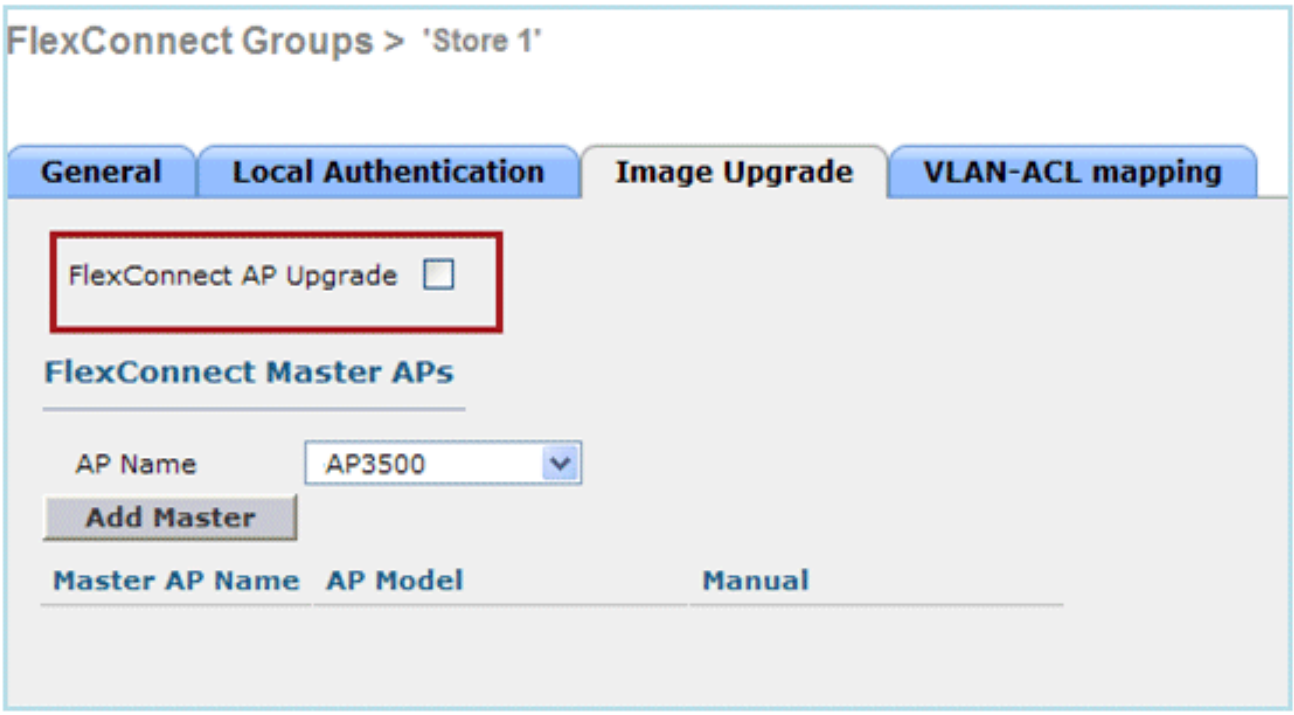
1. Aggiornare l'immagine sul controller.Per avviare il download, selezionare **WLC GUI > Commands > Download File** (Interfaccia utente WLC **> Comandi >** Scarica file).



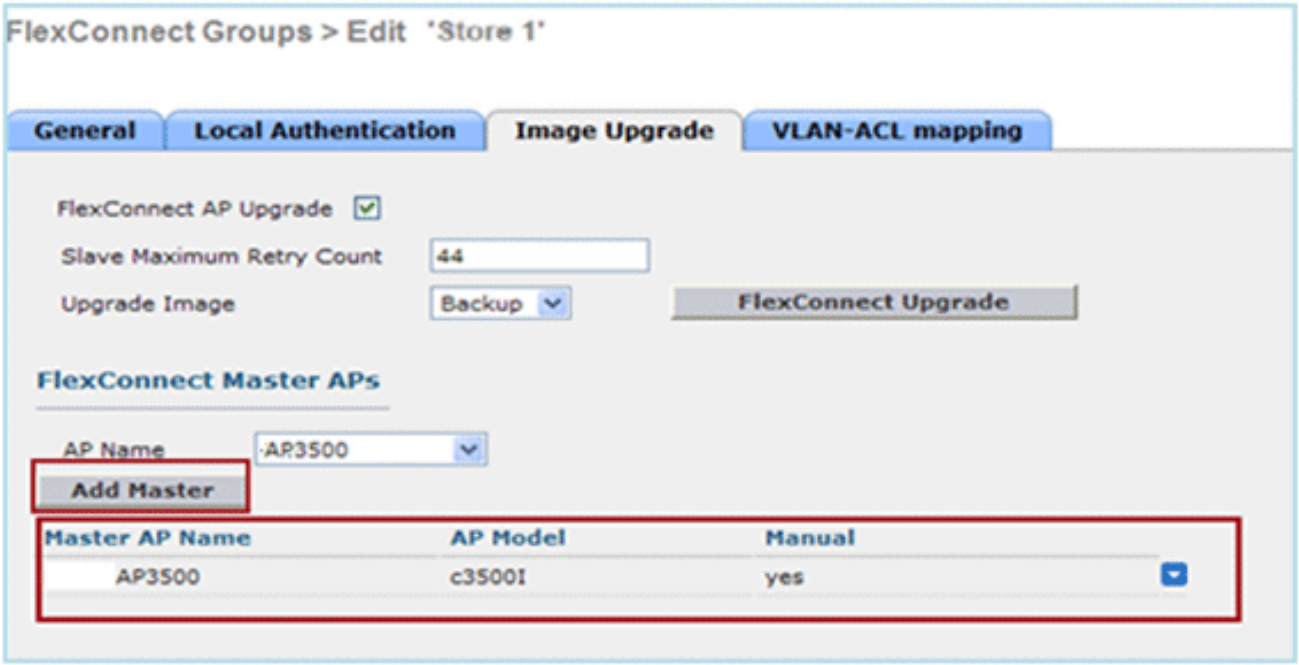
2. Salvare le configurazioni sui controller, ma non riavviare il controller.
3. Aggiungere i punti di accesso FlexConnect al gruppo FlexConnect.Selezionare WLC GUI > Wireless > FlexConnect Groups > select **FlexConnect Group > General** tab > **Add AP**.



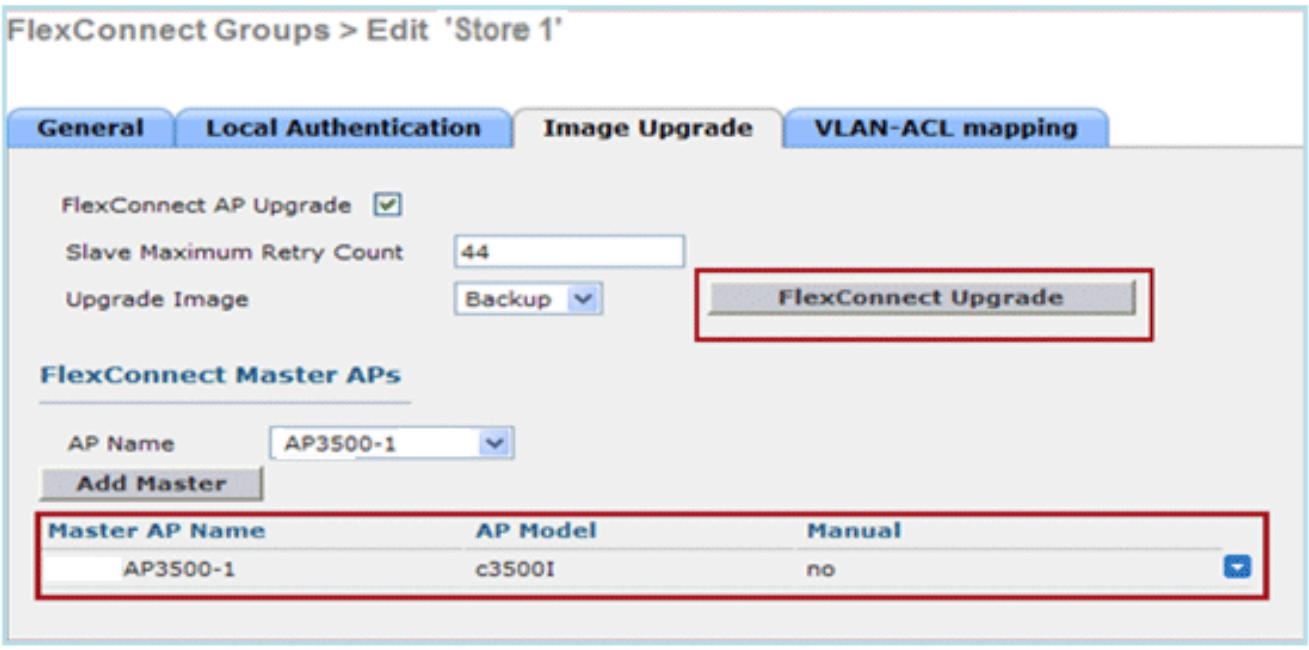
4. Per aggiornare l'immagine AP in modo efficiente, selezionare la casella di controllo **FlexConnect AP Upgrade**.Selezionare GUI WLC **> Wireless > Gruppi FlexConnect >** selezionare **Gruppo FlexConnect > Scheda Aggiornamento immagine**.



5. L'access point master può essere selezionato manualmente o automaticamente:Per selezionare manualmente l'access point master, selezionare GUI WLC > Wireless > FlexConnect Groups > select FlexConnect Group > Image Upgrade tab > FlexConnect Master AP, selezionare l'access point dall'elenco a discesa e fare clic su **Add Master**.

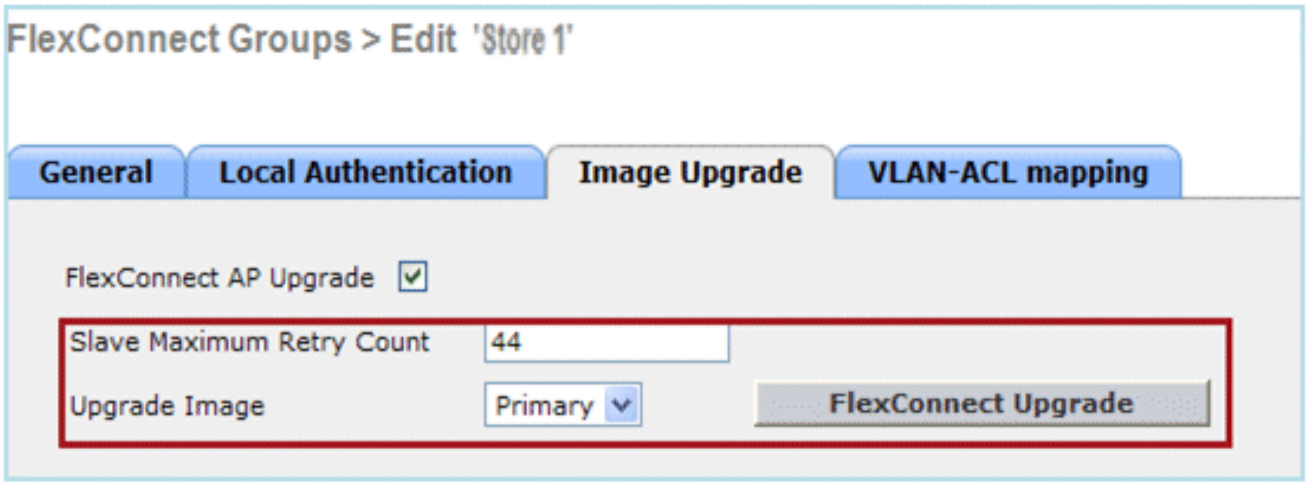


Nota: è possibile configurare come punto di accesso principale un solo punto di accesso per modello. Se l'access point master è configurato manualmente, il campo Manual (Manuale) verrà aggiornato in **modo affermativo**.Per selezionare automaticamente il punto di accesso principale, selezionare GUI WLC > Wireless > FlexConnect Groups > select **FlexConnect Group** > **Image Upgrade** tab, quindi fare clic su **FlexConnect Upgrade**.



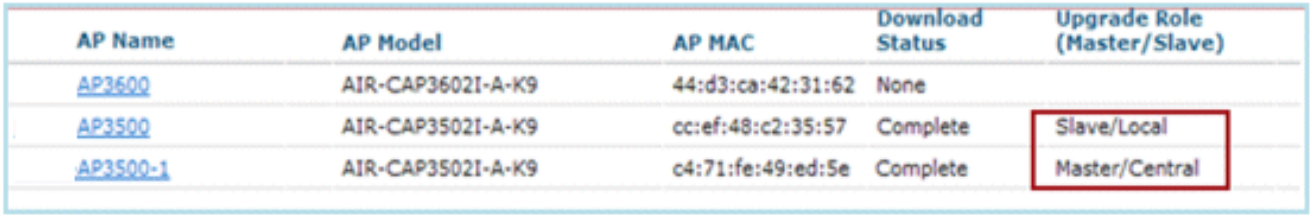
Nota: se il punto di accesso principale viene selezionato automaticamente, il campo Manuale verrà aggiornato in **modo** da visualizzare **no**.

6. Per avviare un aggiornamento efficiente dell'immagine AP per tutti gli access point di uno specifico gruppo FlexConnect, fare clic su **Aggiornamento FlexConnect**.Selezionare GUI WLC > Wireless > Gruppi FlexConnect > selezionare il gruppo **FlexConnect** > scheda **Aggiornamento immagine**, quindi fare clic su **Aggiornamento FlexConnect**.



Nota: numero massimo di tentativi slave indica il numero di tentativi (44 per impostazione predefinita) che l'access point slave compie per scaricare un'immagine dall'access point master, dopo di che tornerà a scaricare l'immagine dal WLC. Eseguirà 20 tentativi contro il WLC per scaricare una nuova immagine, dopo di che l'amministratore deve riavviare il processo di download.

7. Una volta avviato l'aggiornamento FlexConnect, solo l'access point master scaricherà l'immagine dal WLC. Nella pagina All AP (Tutti i punti di accesso), "**Upgrade Role**" (Ruolo di aggiornamento) verrà aggiornato come **Master/Central**, il che significa che il punto di accesso principale ha scaricato l'immagine dal WLC che si trova nella posizione centrale. Il punto di accesso slave scaricherà l'immagine dal punto di accesso master che si trova sul sito locale ed è il motivo in All AP page "**Upgrade Role**" (Ruolo di **aggiornamento)** verrà aggiornato come **Slave/Locale**.Per verificare questa condizione, selezionare **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. Riavviare i controller dopo aver scaricato tutte le immagini AP. Ora gli access point tornano in modalità standalone finché i controller non vengono riavviati.**Nota:** in modalità standalone, Fault Tolerance mantiene i client associati.Una volta ripristinato il controller, gli access point si riavviano automaticamente con l'immagine scaricata in precedenza.Dopo il riavvio, gli access point si uniscono nuovamente al controller primario e riprendono i servizi del client.

Limitazioni

- La selezione dell'access point master è per gruppo FlexConnect e per modello di access point in ogni gruppo.
- Solo 3 access point slave dello stesso modello possono essere aggiornati contemporaneamente dal loro access point master e il resto degli access point slave useranno il timer di back-off casuale per riprovare a scaricare l'immagine dell'access point master.
- Nel caso in cui l'access point slave non riesca a scaricare l'immagine dall'access point master per qualche motivo, passerà al WLC per recuperare la nuova immagine.
- Questa procedura funziona solo con i CAPWAP AP.

Conversione automatica dei punti di accesso in modalità FlexConnect

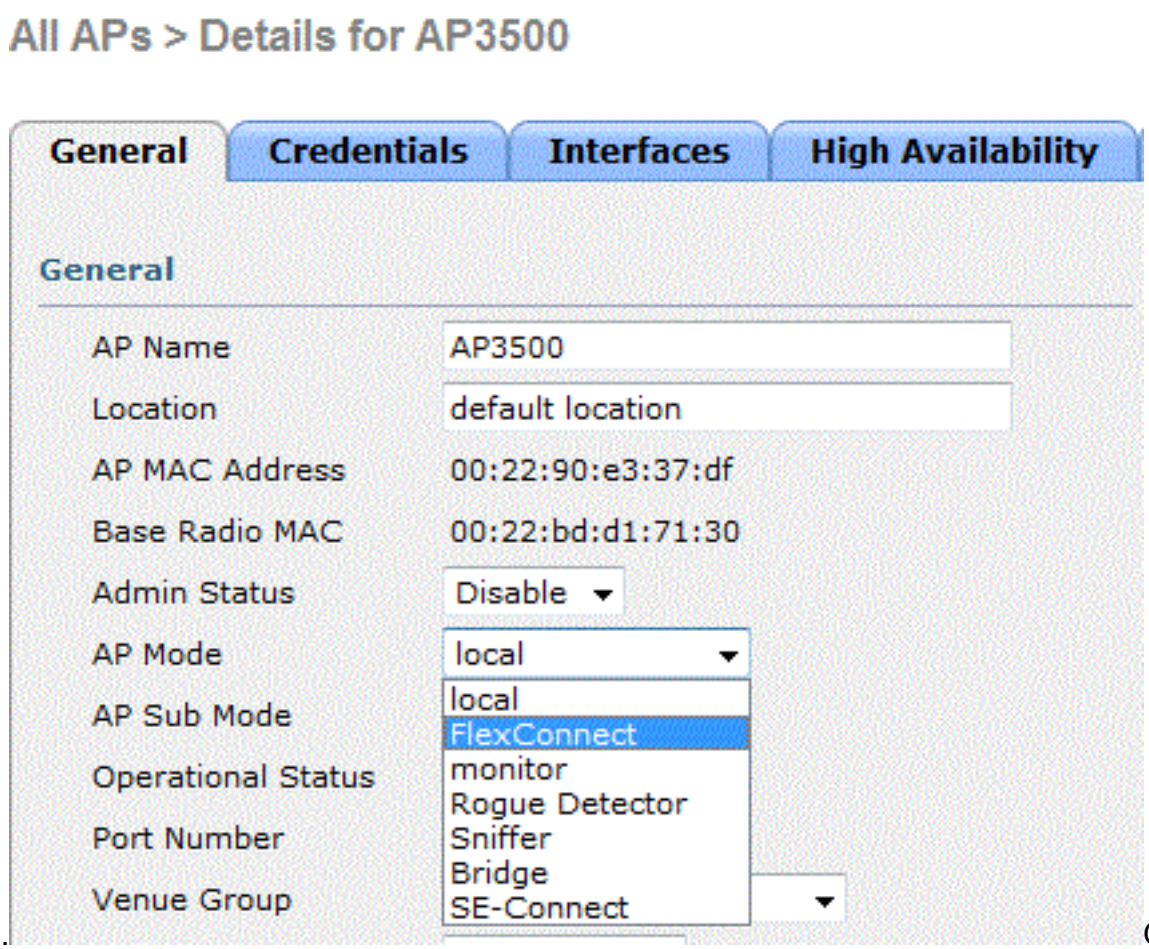
Flex 7500 fornisce le due opzioni seguenti per convertire la modalità AP in FlexConnect:

- Modalità manuale
- Modalità di conversione automatica

Modalità manuale

Questa modalità è disponibile su tutte le piattaforme e consente la modifica solo per punto di accesso.

1. Selezionare **WLC GUI > Wireless > All AP** (Tutti gli access point) e scegliere l'access point.
2. Selezionare **FlexConnect** come modalità AP, quindi fare clic su **Applica**.
3. Se si modifica la modalità, l'access point viene



riavviato. Questa opzione è disponibile anche su tutte le piattaforme WLC correnti.

Modalità conversione automatica

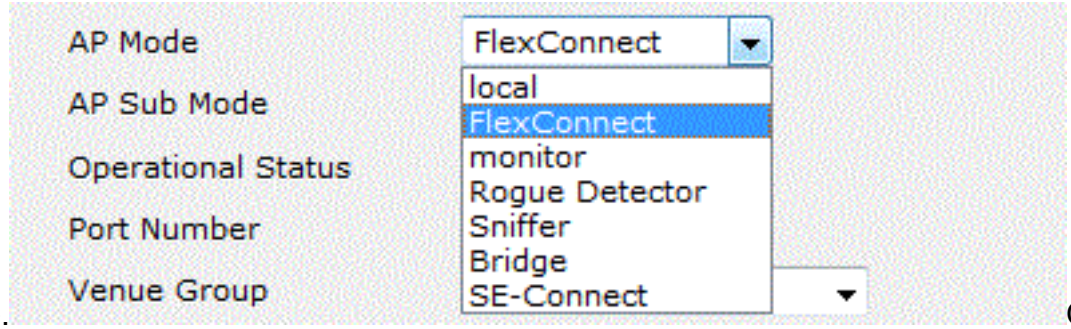
Questa modalità è disponibile solo per il controller Flex 7500 ed è supportata solo dalla CLI. Questa modalità attiva la modifica su tutti gli access point collegati. Prima di abilitare questa CLI, si consiglia di installare Flex 7500 in un dominio di mobilità diverso dai controller WLC campus esistenti:

```
(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. La funzione di conversione automatica è disabilitata per impostazione predefinita e può essere verificata utilizzando questo comando **show**:

   ```
   (Cisco Controller) >show ap autoconvert

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

   Modalità AP non supportate = Modalità locale, Sniffer, Rogue Detector e



Bridge. Questa opzione è attualmente disponibile solo tramite CLI.queste CLI sono disponibili solo sul WLC 7500.

2. L'esecuzione della **configurazione AP con la conversione automatica della** CLI **flexconnect** converte tutti gli access point nella rete con modalità AP non supportata in modalità FlexConnect. Ciò non influisce sugli access point già in modalità FlexConnect o Monitor.

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


(Cisco Controller) >show ap autoconvert

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

(Cisco Controller) >
```

3. L'esecuzione della **configurazione della** CLI di **monitoraggio della conversione automatica AP** converte tutti gli access point della rete con modalità AP non supportata in modalità Monitor. Ciò non influisce sugli access point già in modalità FlexConnect o Monitor.

```
(Cisco Controller >config ap autoconvert monitor


(Cisco Controller) >show ap autoconvert

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

   Non è possibile eseguire contemporaneamente sia la **configurazione ap autoconvertflexconnect** che la **configurazione ap autoconvert monitor**.

Supporto FlexConnect WGB/WGB per WLAN di switching locale

A partire dalla versione 7.3, i client WGB/uWGB e i client wired/wireless dietro i WGB sono supportati e funzioneranno come client normali sulle WLAN configurate per la commutazione locale.

Dopo l'associazione, WGB invia i messaggi IAPP per ciascuno dei propri client cablati/wireless e Flex AP si comporta come segue:

- Quando Flex AP è in modalità connessa, inoltra tutti i messaggi IAPP al controller che li elaborerà allo stesso modo dell'access point in modalità locale. Il traffico per i client cablati/wireless verrà commutato localmente dai Flex AP.
- Quando l'access point è in modalità standalone, elabora i messaggi IAPP, i client cablati/wireless sul WGB devono essere in grado di registrarsi e annullare la registrazione. Dopo il passaggio alla modalità connessa, Flex AP invia le informazioni dei client cablati al controller. WGB invierà messaggi di registrazione tre volte quando Flex AP passa dalla modalità standalone alla modalità connessa.

I client wireless/cablati erediteranno la configurazione WGB, il che significa che non è necessaria alcuna configurazione separata come l'autenticazione AAA, l'override AAA e l'ACL FlexConnect

per i client dietro WGB.

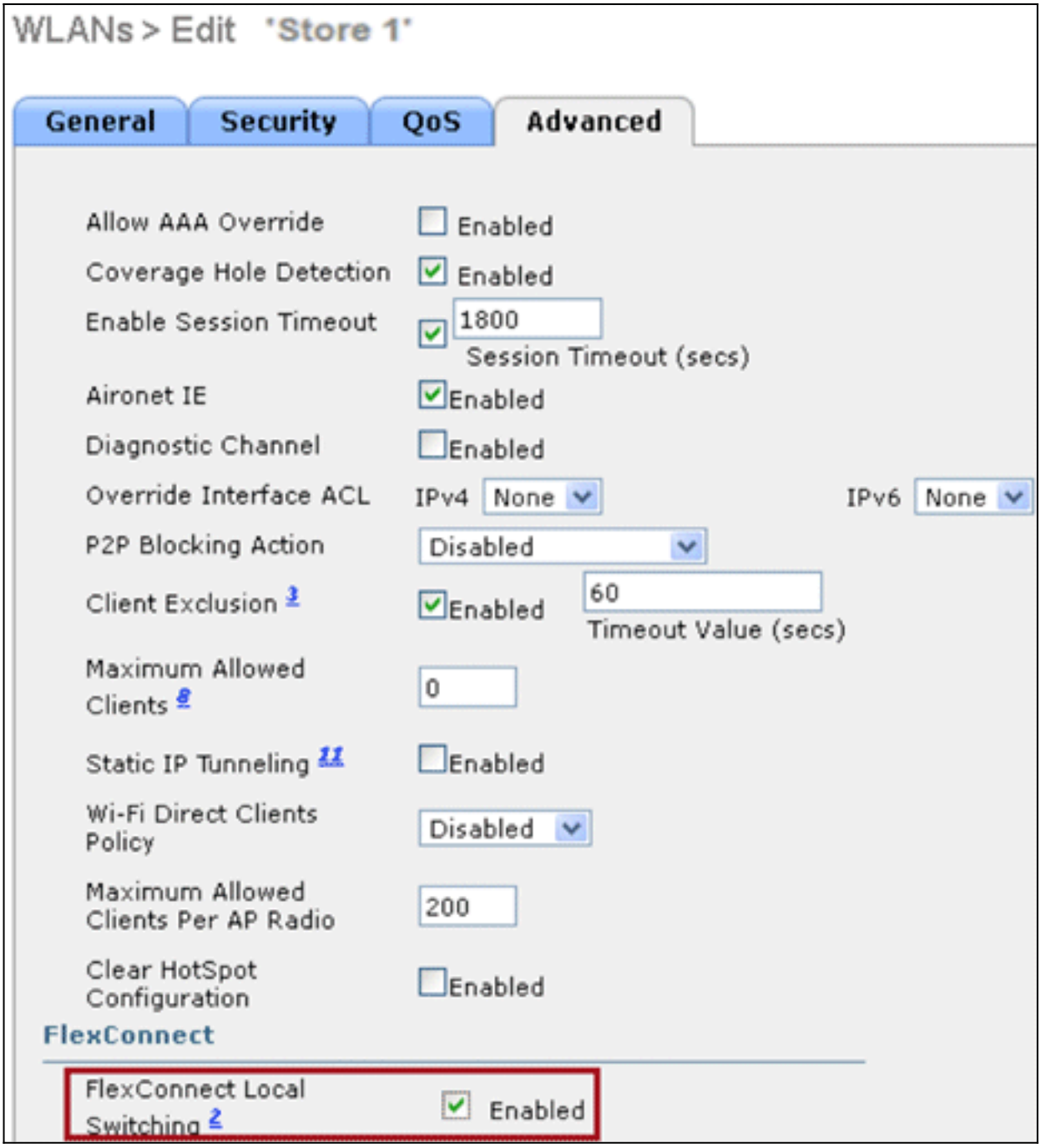
Riepilogo

- Per supportare WGB su Flex AP, non è necessaria alcuna configurazione speciale sul WLC.
- Fault Tolerance è supportato per WGB e i client dietro WGB.
- WGB è supportato su un access point IOS: 1240, 1130, 1140, 1260 e 1250.

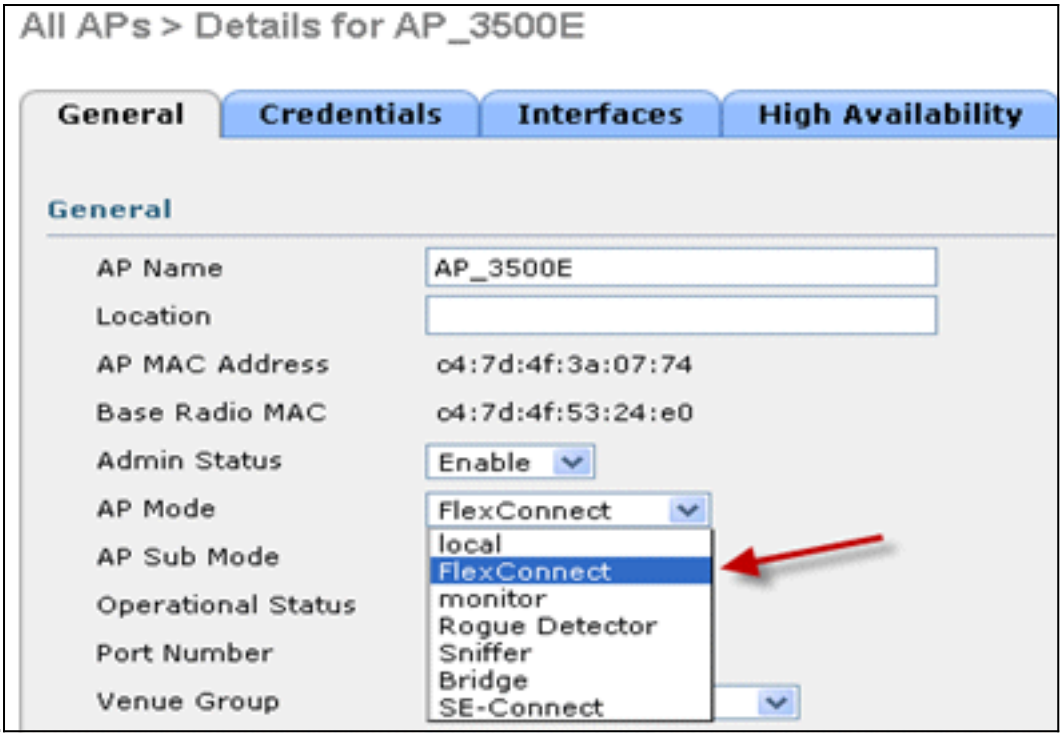
Procedura

Attenersi alla seguente procedura:

1. Non è necessaria alcuna configurazione speciale per abilitare il supporto di WGB/WGB sui punti di accesso FlexConnect per le WLAN configurate per lo switching locale come WGB. Inoltre, i client dietro WGB vengono trattati come client normali sulla commutazione locale configurata dalle WLAN dai Flex AP. Abilitare **FlexConnect Local Switching** su una WLAN.



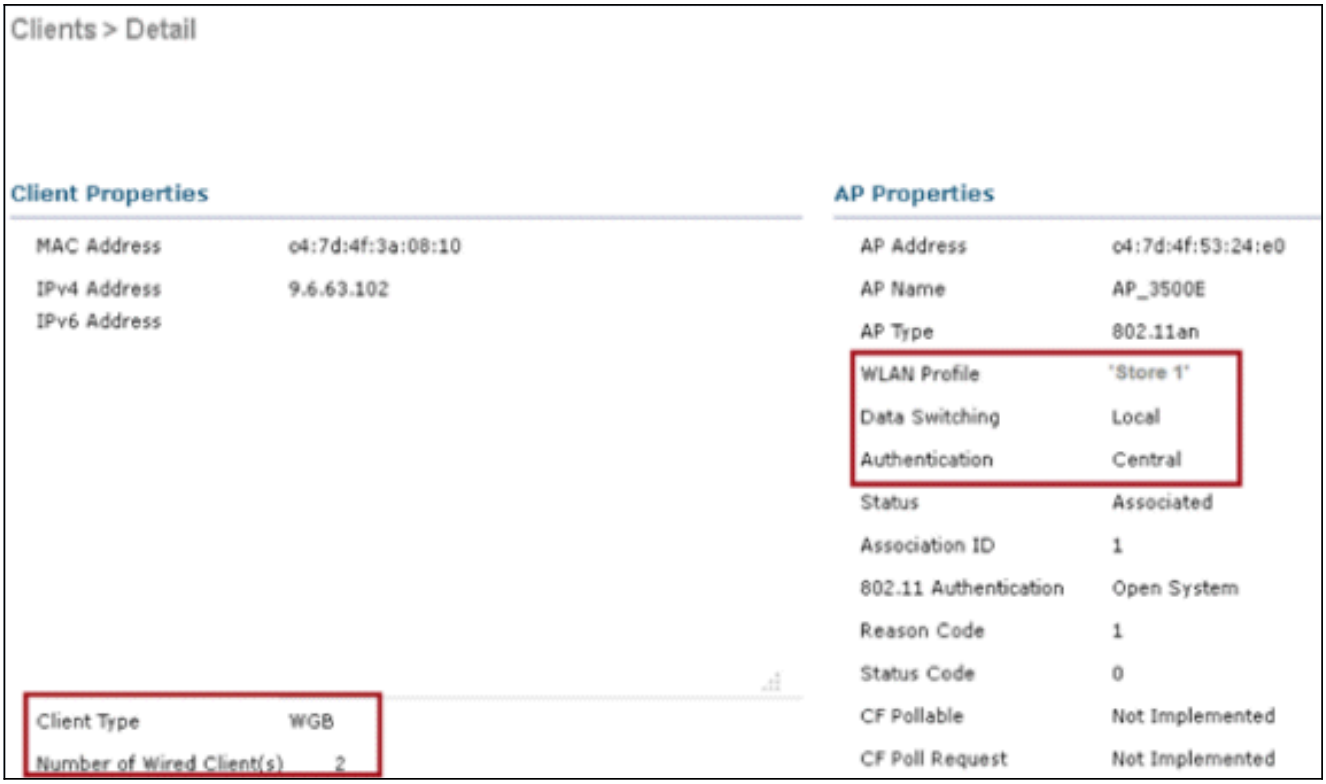
2. Impostare AP Mode (Modalità punto di accesso) su



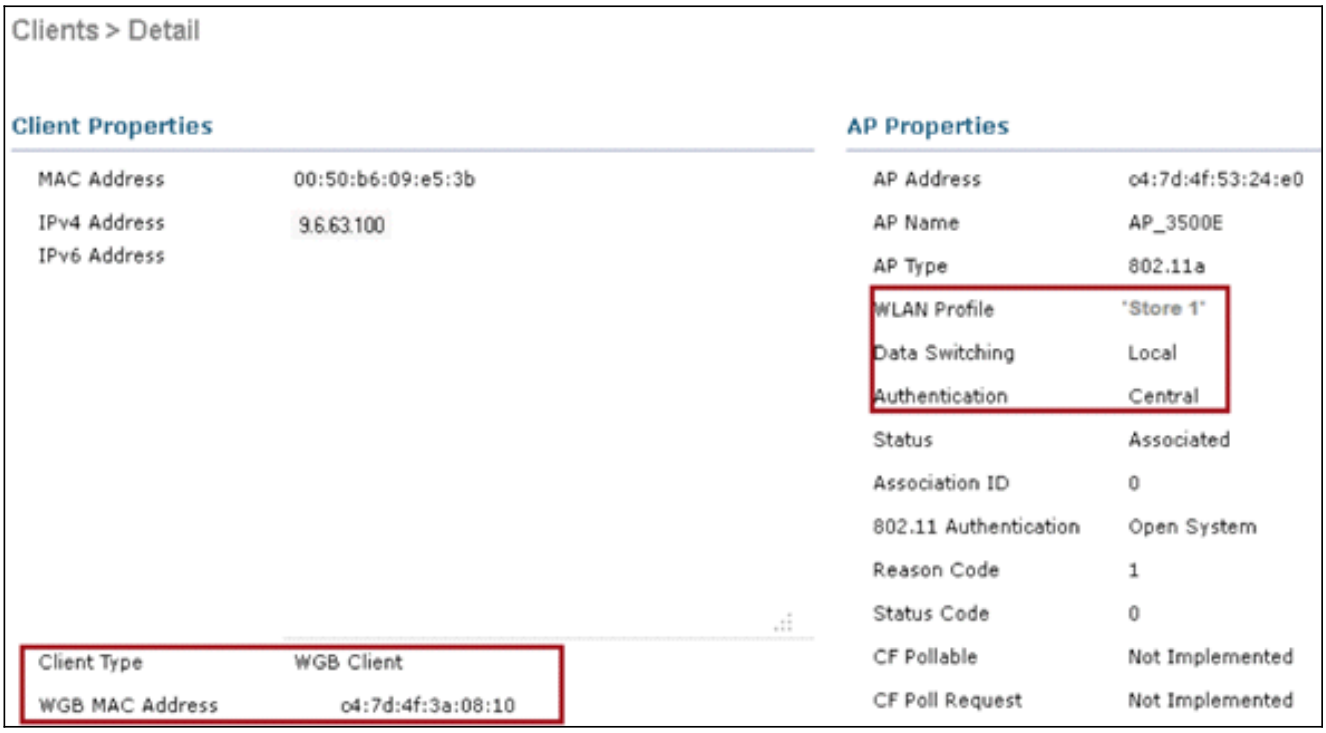
FlexConnect.

3. Associare WGB ai client cablati dietro la WLAN configurata.

4. Per controllare i dettagli relativi a WGB, selezionare **Monitor > Clients**, quindi selezionare **WGB** dall'elenco dei client.



5. Per controllare i dettagli dei client cablati/wireless dietro WGB, andare a **Monitor > Client** e selezionare il
client.



Limitazioni

- I client cablati dietro WGB saranno sempre sulla stessa VLAN di WGN. Il supporto di più VLAN per i client dietro WGB non è supportato in Flex AP per le WLAN configurate per lo switching locale.
- Un massimo di 20 client (cablati/wireless) sono supportati da WGB se associati a Flex AP su WLAN configurati per lo switching locale. Questo numero è lo stesso di quello attuale per il supporto WGB sull'access point in modalità locale.

- L'autenticazione Web non è supportata per i client dietro WGB associati alle WLAN configurate per la commutazione locale.

Supporto per un maggior numero di server Radius

Prima della versione 7.4, la configurazione dei server RADIUS nel gruppo FlexConnect veniva eseguita da un elenco globale di server RADIUS sul controller. Il numero massimo di server RADIUS che è possibile configurare in questo elenco globale è 17. Con un numero crescente di succursali, è necessario poter configurare un server RADIUS per ogni sito di succursale. A partire dalla versione 7.4, sarà possibile configurare i server RADIUS primari e di backup per ciascun gruppo FlexConnect che potrebbe far parte o meno dell'elenco globale di 17 server di autenticazione RADIUS configurati sul controller.

Sarà inoltre supportata una configurazione specifica del punto di accesso per i server RADIUS. La configurazione specifica dell'access point avrà priorità maggiore della configurazione del gruppo FlexConnect.

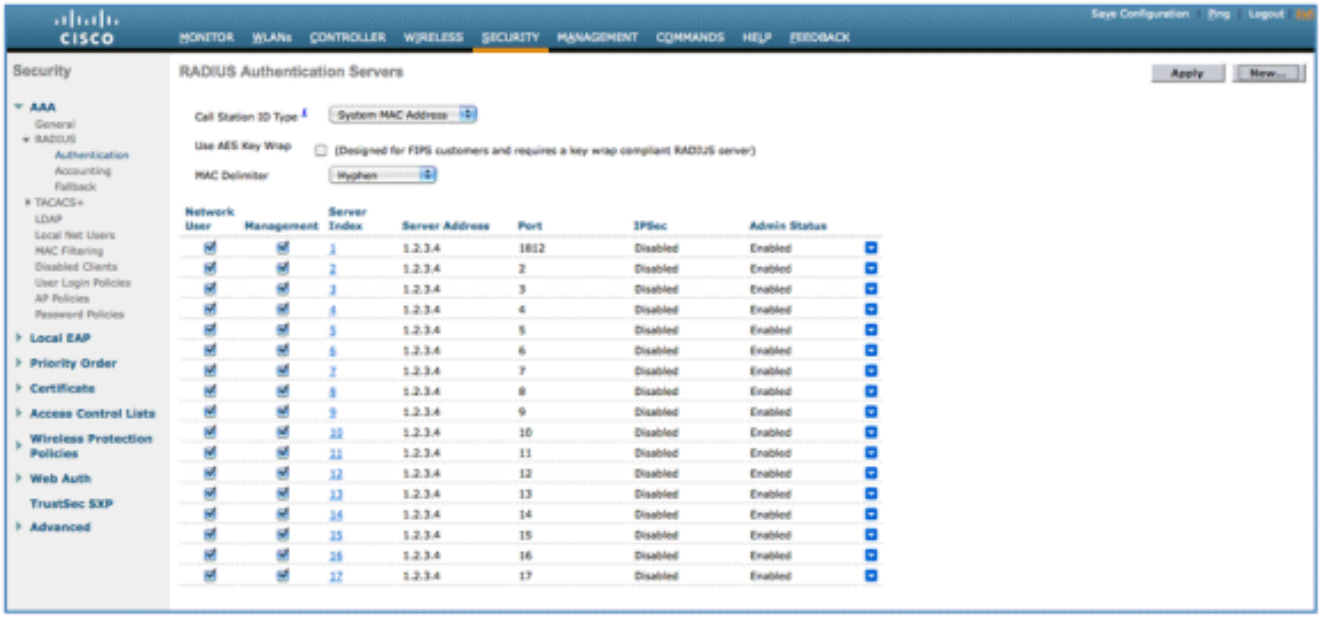
Il comando di configurazione esistente nel gruppo FlexConnect, che richiede l'indice del server RADIUS nell'elenco globale dei server RADIUS sul controller, verrà deprecato e sostituito con un comando di configurazione, che configura un server RADIUS nel gruppo Flexconnect utilizzando l'indirizzo IP del server e il segreto condiviso.

Riepilogo

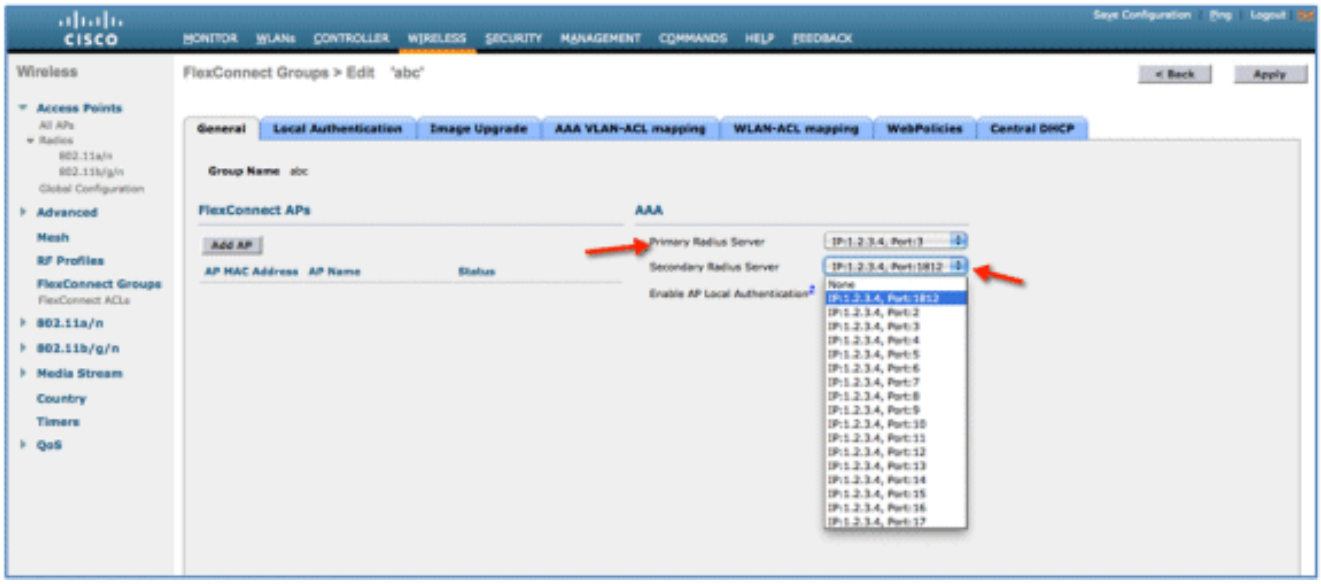
- Supporto per la configurazione dei server RADIUS primari e di backup per gruppo FlexConnect, che può essere presente o meno nell'elenco globale dei server di autenticazione RADIUS.
- Il numero massimo di server RADIUS univoci che possono essere aggiunti a un WLC è il numero di gruppi FlexConnect che possono essere configurati su una determinata piattaforma moltiplicato per due. Un esempio è costituito da un server RADIUS primario e uno secondario per ciascun gruppo FlexConnect.
- L'aggiornamento del software da una release precedente alla release 7.4 non causerà alcuna perdita di configurazione RADIUS.
- L'eliminazione del server RADIUS primario è consentita senza dover eliminare il server RADIUS secondario. Ciò è coerente con la configurazione corrente del gruppo FlexConnect per il server RADIUS.

Procedura

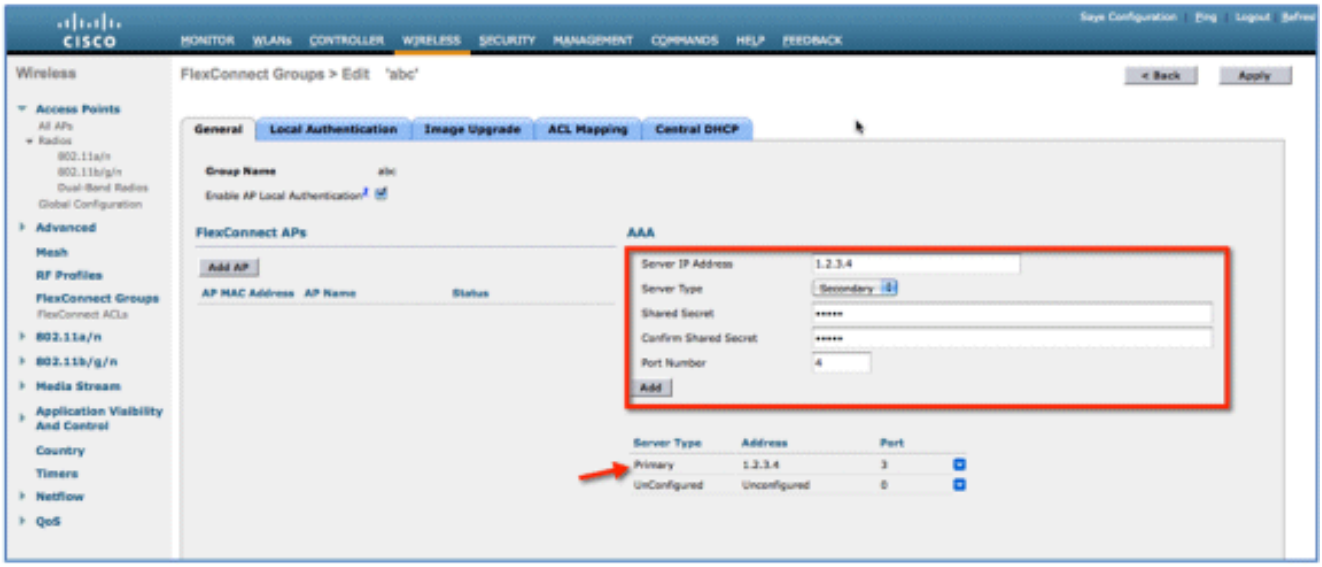
1. Modalità di configurazione precedente alla release 7.4.Nella configurazione dell'autenticazione AAA è possibile configurare un massimo di 17 server RADIUS.



2. I server RADIUS primario e secondario possono essere associati a un gruppo FlexConnect utilizzando un elenco a discesa che include i server RADIUS configurati nella pagina Autenticazione
AAA.



3. Modalità di configurazione in FlexConnect Group nella release 7.4.I server RADIUS primario e secondario possono essere configurati nel gruppo FlexConnect utilizzando un indirizzo IP, un numero di porta e un segreto
condiviso.



Limitazioni

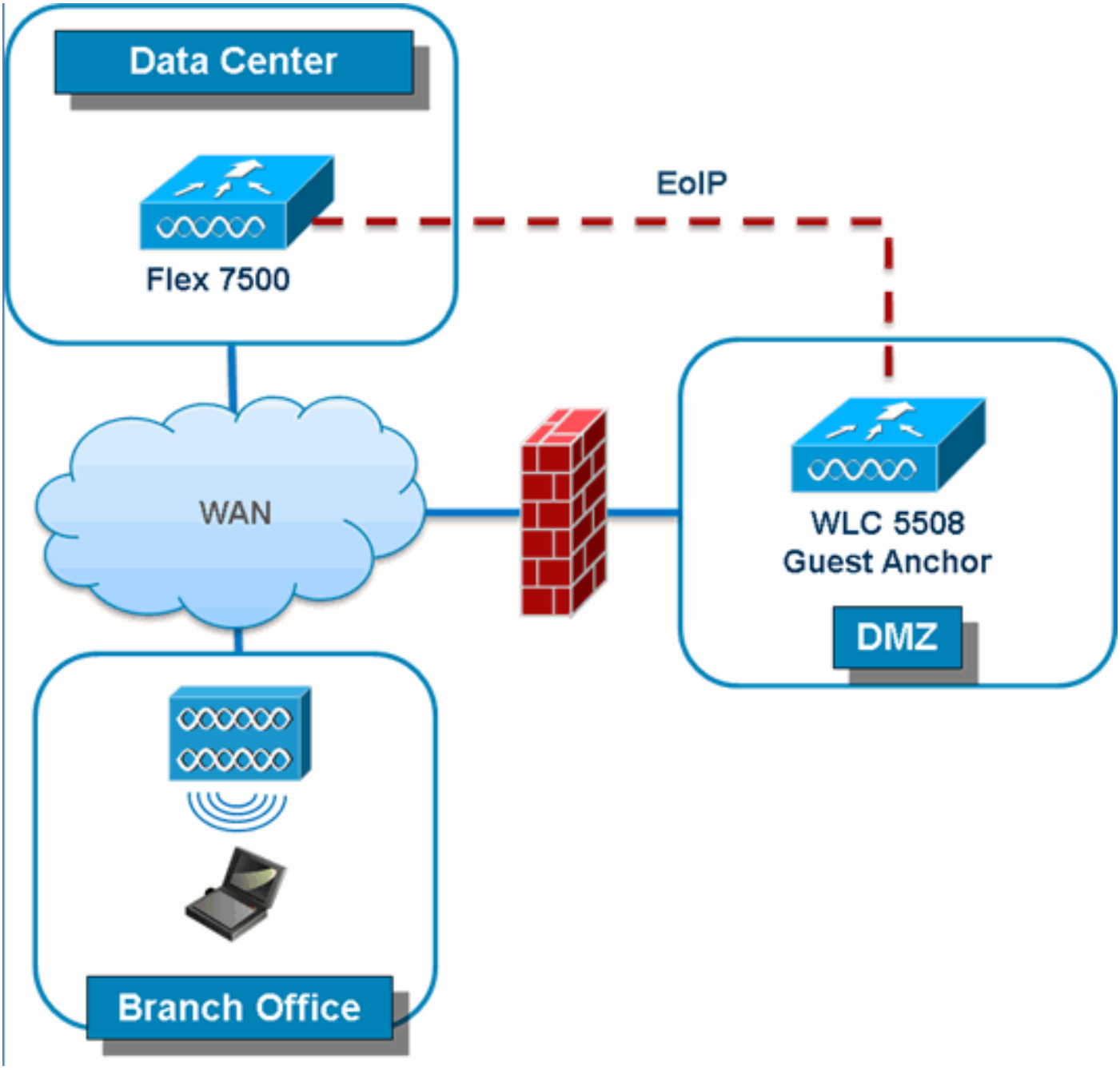
- Il downgrade del software dalla release 7.4 a una release precedente manterrà la configurazione, ma con alcune limitazioni.
- Configurando un server RADIUS primario/secondario quando ne è configurato uno precedente, la voce precedente verrà sostituita da quella nuova.

Modalità Enhanced Local (ELM)

ELM è supportato dalla soluzione FlexConnect. Per ulteriori informazioni, consultare la guida alle procedure ottimali su ELM.

Supporto per l'accesso guest in Flex 7500

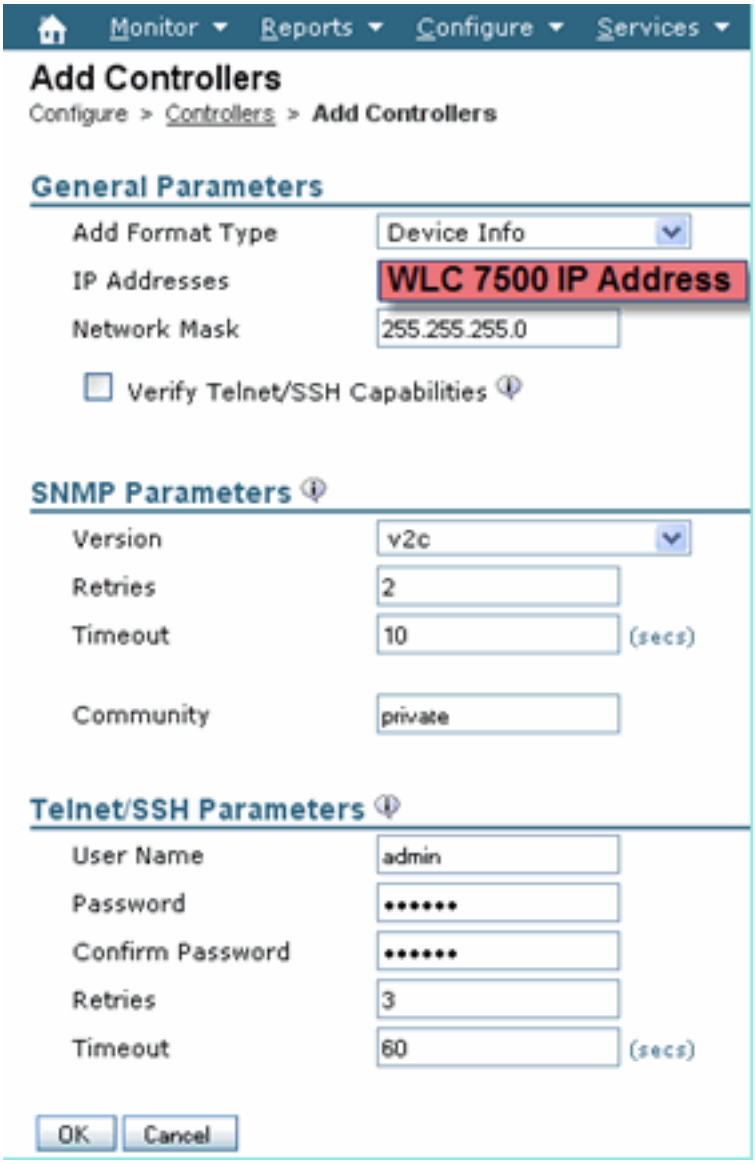
Figura 13: Supporto per l'accesso guest in Flex 7500



Flex 7500 consentirà e continuerà a supportare la creazione di tunnel EoIP per il controller di ancoraggio guest in DMZ. Per le procedure ottimali relative alla soluzione di accesso guest wireless, consultare la Guida alla distribuzione guest.

Gestione di WLC 7500 da NCS

La gestione del WLC 7500 dall'NCS è identica a quella dei WLC esistenti di Cisco.



Per ulteriori informazioni sulla gestione dei WLC e l'individuazione dei modelli, consultare la guida alla configurazione di Cisco Wireless Control System, versione 7.0.172.0.

Domande frequenti

D. Se i LAP vengono configurati in una postazione remota come FlexConnect, è possibile assegnargli un controller primario e secondario?

Esempio: Il sito A contiene un controller primario e il sito B un controller secondario. Se il controller del sito A ha esito negativo, il LAP esegue il failover sul controller del sito B. Se entrambi i controller non sono disponibili, il LAP entra in modalità standalone FlexConnect?

R. Sì. Prima il LAP passa alla versione secondaria. Tutte le WLAN commutate localmente non presentano modifiche e tutte le WLAN commutate centralmente devono trasmettere il traffico al nuovo controller. Inoltre, se il secondo si guasta, tutte le WLAN contrassegnate per la

commutazione locale (e autenticazione a chiave aperta/precondivisa/si sta eseguendo l'autenticatore AP) rimangono attive.

D. Come interagiscono i punti di accesso configurati in modalità locale con le WLAN configurate con FlexConnect Local Switching?

R. I punti di accesso in modalità locale considerano le WLAN come WLAN normali. L'autenticazione e il traffico di dati vengono rimandati al WLC. Durante un errore di collegamento WAN, la WLAN è completamente inattiva e nessun client è attivo su questa WLAN finché non viene ripristinata la connessione al WLC.

D. È possibile eseguire l'autenticazione Web con la commutazione locale?

R. Sì, è possibile avere un SSID con l'autenticazione Web abilitata e rilasciare il traffico localmente dopo l'autenticazione Web. L'autenticazione Web con la commutazione locale funziona correttamente.

D. È possibile utilizzare il portale guest sul controller per un SSID gestito localmente dal punto di accesso remoto? Se sì, cosa succede se si perde la connettività al controller? I clienti attuali vengono eliminati immediatamente?

R. Sì. Poiché la WLAN è commutata localmente, la WLAN è disponibile ma nessun nuovo client è in grado di eseguire l'autenticazione poiché la pagina Web non è disponibile. Ma i clienti esistenti non vengono abbandonati.

D. FlexConnect può certificare la conformità PCI?

R. Sì. La soluzione FlexConnect supporta il rilevamento rogue per soddisfare la conformità PCI.

Informazioni correlate

- Guida alla progettazione e alla distribuzione di HREAP
- Cisco serie 4400 Wireless LAN Controller
- Cisco serie 2000 Wireless LAN Controller
- Cisco Wireless Control System
- Cisco serie 3300 Mobility Services Engine
- Cisco Aironet serie 3500
- Cisco Secure Access Control System
- Documentazione e supporto tecnico – Cisco Systems