# Guida all'installazione di Flex 7500 Wireless Branch Controller

## Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Panoramica del prodotto Specifiche del prodotto Scheda tecnica Funzione piattaforma Avvio di Flex 7500 Licenze Flex 7500 Conteggio base licenze AP Licenze di aggiornamento AP Supporto per le versioni software Access point supportati Architettura FlexConnect Vantaggi della centralizzazione del traffico di controllo dei punti di accesso Vantaggi della distribuzione del traffico di dati dei client Modalità operative di FlexConnect **Requisiti WAN** Progettazione della rete di filiali wireless Requisiti principali di progettazione Panoramica Vantaggi Caratteristiche per la progettazione di reti di filiali Matrice di supporto IPv6 Matrice Gruppi di AP Configurazioni da WLC Riepilogo **Gruppi FlexConnect** Obiettivi principali dei gruppi FlexConnect Configurazione gruppo FlexConnect da WLC Verifica tramite CLI Override della VLAN FlexConnect Riepilogo

Procedura Limitazioni Switching centrale basato su VLAN FlexConnect Riepilogo Procedura Limitazioni ACL FlexConnect **Riepilogo** Procedura Limitazioni FlexConnect Split Tunneling Riepilogo Procedura Limitazioni **Fault Tolerance Riepilogo** Limitazioni Limite client per WLAN **Obiettivo principale** Limitazioni **Configurazione WLC Configurazione NCS** Blocco peer-to-peer Riepilogo **Procedura** Limitazioni Download pre-immagine AP Riepilogo Procedura Limitazioni Aggiornamento immagine FlexConnect Smart AP **Riepilogo** Procedura Limitazioni Conversione automatica dei punti di accesso in modalità FlexConnect Modalità manuale Modalità conversione automatica Supporto FlexConnect WGB/WGB per WLAN di switching locale Riepilogo Procedura Limitazioni Supporto per un maggior numero di server Radius Riepilogo Procedura Limitazioni

Modalità Enhanced Local (ELM) Supporto per l'accesso guest in Flex 7500 Gestione di WLC 7500 da NCS Domande frequenti Informazioni correlate

### **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 <u>Cisco sulle convenzioni</u> 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 <u>wireless</u> 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 (<u>Figura 1</u>) è in grado di gestire <u>punti di accesso</u> 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 Rear View



### 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	Indirizzo MAC di	
gestione)	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.

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

## 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
```

```
Cisco Bootloader (Version
                       .d88b. d88888b. d8888b. d8888b. d8888b.
                                       88' YP d8P
                                                    Y8 .8P
                     d8P
                          ¥8
                                `88'
                                                             Y8.
                     8P
                                 88
                                       `8bo.
                                               8P
                                                       88
                                                              88
                     8b
                                 88
                                         `Y8b. 8b
                                                       88
                                                              88
                     Y8b
                          d8
                                .88.
                                       db
                                            8D Y8b
                                                    d8 `8b
                                                             d8'
                      ,A88b, A88888b, S888b, A88b,
                                                         `Y88P'
Booting Primary Image ...
Press <ESC> now for additional boot options...
    Boot Options
Please choose an option from below:
 1. Run primary image (Version
                                            (default)
2. Run backup image
                      (Version
3. Manually upgrade primary image
4. Change active boot image
 5. Clear Configuration
```

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 (O = 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 <u>guida alla configurazione del WLC 7.3</u>, 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 Architecture



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 <u>Figura 6</u>. 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.

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

#### Supporto della sicurezza L2 per utenti non guest con commutazione centrale

**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	Тіро	Risultato
	Interno	Consentito
Autenticazione Web	Esterna	Consentito
	Personalizzato	Consentito
	Interno	Consentito
Pass-through Web	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 <u>guida</u> <u>alla distribuzione di Flexconnect WebAuth esterna</u>

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

### Modalità operative di FlexConnect

Modal	Descrizione	
ità		

FlexC	
onnec	
t	
	Un FlexConnect è impostato in modalità
Conn	connessa quando il control plane CAPWAP che
esso	riporta al controller è attivo e operativo, ovvero il
	collegamento WAN non è inattivo.
	La modalità standalone è specificata come stato
	operativo in cui FlexConnect entra quando non
Indina	ha più la connettività con il controller. I punti di
ndent	accesso FlexConnect in modalità standalone
	continueranno a funzionare con l'ultima
0	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 <u>guida alla</u> <u>progettazione e all'installazione di H-Reap / FlexConnect</u>.

### 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 distribu zione	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 (Monito ra)	64 kbps	2 sec.	5	N/D
Dati	640 kbps	300 ms	50	1000
Dati + voce	1.44 Mbps	100 ms	50	1000
Monitor (Monito ra)	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:

Caratteristich e 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

	centrale		locale	
he	5500 / WiSM 2	/ - Flex 7500	5500 / WiSM-2	Flex 7500
IPv6 (mobilità client)	Support to	a Non supportat o	Non supportat o	Non supportat o
Protezione RA IPv6	Support to	a Supportat o	Supportat o	Supportat o
Protezione DHCP IPv6	Support to	a Non supportat o	Non supportat o	Non supportat o
Protezione origine IPv6	Support to	a Non supportat o	Non supportat o	Non supportat o
Limitazione RA / Limite di velocità	Support to	a Non supportat o	Non supportat o	Non supportat o
ACL IPv6	Support to	a Non supportat o	Non supportat o	Non supportat o
Visibilità client IPv6	Support to	a Non supportat o	Non supportat o	Non supportat o
Cache di individuazion e router adiacenti IPv6	Support to	a Non supportat o	Non supportat o	Non supportat o
Bridging IPv6	Support to	a Non supportat o	Supportat o	Supportat o

# **Matrice**

Per una matrice delle caratteristiche della funzione FlexConnect, consultare il documento <u>sulla</u> <u>matrice delle caratteristiche di FlexConnect</u>.

## 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:

 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.

ahaha				Sage Configuration   Ping   Logout   Befresh
cisco	MONITOR WLANS CONTRO	OLLER WIRELESS SECURITY	MANAGEMENT COMMANDS HELP	EEEDBACK
WLANs	WLANs > New			< Back Apply
WLANS	Туре	WLAN M		
Advanced	Profile Name	Storel		
	SSID	store		
	ID	17 💌		

 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).						
cisco	MONITOR WLANS CONTR	OLLER WIRELESS SE	ECURITY MANAGEMENT	COMMANDS HELP	Sage Configuration Eing L	logout   <u>R</u> efresh
WLANs	WLANs > Edit				< Back	Apply
WLANS	General Security C	oS Advanced				
Advanced	Layer 2 Layer 3	AAA Servers				_
	Layer 2 Security 4 WPA	+WPA2 MAC Filtering				
	WPA+WPA2 Parameters					
	WPA Policy					
	WPA2 Policy	<b>•</b>				
	WPA2 Encryption	RAES TKIP				
	Auth Key Mgmt	PSK 💌				
	PSK Format	ASCII 💌				
		•••••				

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

VVLAN.						
cisco	MONITOR WLANS CON	TROLLER WIRELESS SECU	IRITY MANAGEMENT	COMMANDS HELP	Saye Configuration   Eing EEEDBACK	Logout Befresh
WLANs	WLANs > Edit				< Back	Apply
WLANS WLANS	General Security	QoS Advanced				
E Advanced	Profile Name	Store1				
	Type	WLAN				
	SSID	store				
	Status	Enabled				
	Security Policies	[WPA2][Auth(PSK)] (Modifications done under securi	ty tab will appear after a	applying the changes.)		
	Radio Policy	All				
	Interface/Interface Group(G)	management 💌				
	Multicest Vian Feature	Enabled				
	Broadcast SSID	Enabled				

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

10.								
սիսիս							Sage Configuration Ping	Logout   Befresh
cisco	MONITOR WLANS	CONTROLLER WI	IRELESS SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	
WLANs	WLANs > New						< Back	Apply
<ul> <li>WLANS WLANS</li> <li>Movanced</li> </ul>	Type Profile Name SSID ID	WLAN Store2 store 18	×					

ababa	Sa <u>v</u> e Configuration _ <u>Ping</u> Logout <u>B</u> e	fresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	
WLANs	WLANs > Edit < Back Appl	y
WLANS	General Security QoS Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Layer Z Security WPA+WPA2	
	Itemac Filtering	
	WPA+WPA2 Parameters	
	WPA Policy	
	WPA2 Policy	
	WPA2 Encryption VIAES LITKIP	
	PSK Format ASCIL	
	Save Configuration   Ping   Longuit	efrec
	MONITOR WEAK CONTROLLER WITELESS SECURITY MANAGEMENT COMMANDS WERE ESCREDUCY	
CISCO	Rousson Wass Zounorren alteress Scouth Sharesetti Shaanes urb. Pression	_
WLANs	WLANs > Edit < Beck App	ły
WLANS WLANS	General Security QoS Advanced	
Advanced	Profile Name Dore2	
	Type WLAN	
	SSID etore	
	Status 🕑 Enabled	
	Security Policies [WPA2][Auth(PSK)]	
	(modifications done under security tab will appear after applying the changes.)	
	Radio Policy All	
	Interface/Interface	
	Group(G)	
	Purpudeast SSTD Provided	
	Custom Custo	

- 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

ာျားပျား cisco	MONITOR	WLANS C	ONTROLLER WIREL	ESS SECURITY MANA	SEMENT COMMANDS HELP	Saye Configuration   Ping   Log EEEDBACK	out   <u>B</u> efree
WLANs	WLANs					Entries	1 - 3 of 3
WLANS WLANS	Current Filte	n: None	[Change Filter]	Clear Filter]	Create New S	Go	
	- INV AN 10	Twos	Deafile Name				
AP Groups	C WLAN ID	type	Promie Name	WLAN SSIE	Admin Stat	tus Security Policies	
AP Groups		WLAN	DataCenter	DataCenter	Enabled	[WPA + WPA2][Auth(802.1X)]	
AP Groups		WLAN	DataCenter Store1	DataCenter store	Enabled Enabled	[WPA + WPA2][Auth(802.1X)] [WPA2][Auth(PSK)]	0

- 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

A .I .I

Add.										
ahaha								Sage Configuration	Ping	Logout <u>R</u> efresh
cisco	MONITOR WLANS	CONTROLLER	WIRELESS ;	SECORITY MA	NAGEMENT	COMMANDS	HELP	EEEDBACK		
WLANs	AP Groups							Entries 1 - 1	l of 1	Add Group
<ul> <li>WLANS WLANS</li> <li>Advanced AP Groups</li> </ul>	Add New AP Group AP Group Name Description AP Group Name Store1 default-group	ID Store2 New York Add Cancel	AP Gr Califor	oup Description	n		Ĩ			

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

FA.									
ahaha								Save Configuration   Ping	Logout <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	
WLANs	AP Groups							Entries 1 - 2 of 2	Add Group
* WLANS									
WLANs	AP Group Name		APO	Group Descr	iption				
<ul> <li>Advanced</li> </ul>	Store1		Calif	fornia					
AP Groups	Store2		New	York					
	default-group								

- 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

ululu cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MAN	AGEMENT COMMANDS	HELP	Sage Configuration   Eine EEEDBACK	g   Logout   <u>B</u> efresh
WLANs	Ap Groups > Edit	'Store1'					< Back
WLANS	General WLA	APs					^
<ul> <li>Advanced AP Groups</li> </ul>					1	Add New	
	Add New						
	WLAN SSID Interface	DataCenter(1)					
	/Interface Group(G) NAC State	store(17) Store 1 store(18) Store 2 Enabled	_				
		Add Cancel					
	WLAN WLAN ID SSID	Interface/Interface Group(G)	NAC State				

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). uluulu cisco Eing Logout Bef WLANs Ap Groups > Edit 'Store2' < Back WLANS General WLANS APs WLANs Advanced Add New AP Groups Add New WLAN SSID store(16) Store 2 Interface /Interface Group(G) DataCenter(1) store(17) Store 1 tore(18) Store 2 NAC State Enabled Add Cancel Interface/Interface Group(G) WLAN WLAN ID SSID NAC

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)

## **Central Authentication – Flex 7500 Authenticator**



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

### **Central Authentication – AP Authenticator**



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)



## Local Branch Authentication – AP as Radius Server

• 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.

cisco	MONITOR	WLAN	ls	CONTROLLER	WIRELESS
Wireless	FlexConr	nect G	rou	ıps > New	
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>802.11a/n</li> <li>802.11b/g/n</li> <li>Global Configuration</li> </ul> </li> </ul>	Group Na	me	Stor	re 1	
Advanced					
Mesh					
RF Profiles					
FlexConnect Groups					

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

	MONITOR <u>W</u> LANS <u>C</u> CNTROLLER WIRELESS <u>S</u> ECURITY
Wireless	FlexConnect Groups
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>802.11a/n</li> <li>802.11b/g/n</li> <li>Global Configuration</li> </ul> </li> </ul>	Group Name Store 1
<ul> <li>Advanced</li> <li>Mesh</li> <li>RF Profiles</li> <li>HexConnect Groups</li> </ul>	
<sup>-</sup> are clic su <b>Add</b>	

AP.

cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>s</u> ecuri
Wireless	FlexConn	nect Gro	ups > Edit 'S	tore 1'	
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>802.11a/n</li> <li>802.11b/g/n</li> <li>Global Configuration</li> </ul> </li> </ul>	General Group	Local	Authentication	Image U	pgrade
<ul> <li>Advanced</li> <li>Mesh</li> <li>RF Profiles</li> <li>FlexConnect Groups</li> <li>FlexConnect ACLs</li> </ul>	FlexCor Add A AP MAC	Address	s AP Name	Sta	itus

- 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.

FlexConnect G	Sroups >	Edit	'Store 1	•
---------------	----------	------	----------	---

|--|

Apply

General Lo	cal Authentication	Image Upgrade	VLAN-ACL mapping
Local Users	Protocols		
LEAP			
Enable LEAF Authenticati	on <sup>2</sup>		
EAP Fast			
Enable EAP	Fast Authentication <sup>2</sup>		
Server Key	(in hex)	🔲 Enable Auto key ge	neration
		•••••	
		••••••	•••••
Authority ID	(in hex)	436973636f00000000	000000000000
Authority In	fo	Cisco A_ID	
PAC Timeou	it (2 to 4095 days)		

13. In Autenticazione locale fare clic su Utenti locali.

FlexConnect Groups > Edit 'Store 1'

- 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.

eneral Loc	al Authentica	tion	Image Upgrade	VLAN-ACL mapping
Local Users	Protocols			
No of Users		0	Add User	
User Name				
			Upload CSV file <sup>1</sup>	
			File Name	
			UserName	cisco
			Password	
			Confirm Password	

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 <u>Figura</u>

8.    cisco	MONITOR	WLANS		WIRELESS	<u>s</u> ecurity m <u>a</u> nagei
WLANs	WLANs				
WIANS	Current Fi	lter: No	ine [ <u>Cha</u>	nge Eilter] [Cle	<u>ar Filter]</u>
Advanced		ID Type	Profile N	lame	WLAN SSID
	□ 2	WLAN	Guest		Guest
	□ <u>17</u>	WLAN	Store-1		Store

- 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

```
WLANs > Edit 'Store-1'
```

General	Security	Qos	S	Adva	nced			
P2P Block	ing Action		Disab	oled		•	-	
Client Exc		🔽 Er	abled	60 Tir	60 Timeout Value (secs			
Maximum	Allowed Clie	nts 🚨	0					
Static IP 1	Funneling 11		🔳 En	abled				
Wi-Fi Dire	ct Clients Pol	icy	Disat	oled	-			
Maximum Per AP Ra	Allowed Clien idio	nts	200					
Off Channel	Scanning D	efer						
Scan Defe	er Priority	0 1	2	з (	4 5	6	7	
					<b>V V</b>	]		
Scan Defe (msecs)	er Time	100						
FlexConnec	t							
FlexConne 2	ect Local Swit	ching	<b></b> ₹	Enable	d			
FlexConne	ect Local Auth	1 <u>12</u>	🔽 e	Enable	d			
Learn Clie	ent IP Addres	s <mark>5</mark>	E E	Enable	d			

#### WLAN.

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

Properties	>	WLAN Configuration De	tails : 1	
System	>			が説
WLANs	~	General Security	QoS Advanced	
H WLAN Configuration				
AP Groups		HexConnect Local Switching	) 🗹 Enable	
FlexConnect	>	FlexConnect Local Auth 🔍	🗹 Enable	
Security	>	Learn Client IP Address	🗹 Enable	
Access Points	,	Session Timeout	Enable	
802.11	,	Coverage Hole Detection	Enable	
000 44-4-		Aironet IE	Enable	
802.11a/n	,	IPv6 <sup>2</sup>	Enable	
802.11b/g/n	>	Diagnostic Channel 🙎	Enable	
Mesh	>	Override Interface ACL	IPv4 NONE	etter
Ports		Peer to Peer Blocking 🔍	Disable	-
Manacement	>	Wi-Fi Direct Clients Policy	Disabled	
Location	>	Client Exclusion 4	Enable	
		Timeouc value		

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

•1  C	cisco Network Control System								
6	Ilome Monitor	Configure	▼ Services	<ul> <li>Reports</li> </ul>	▼ Adı	nnistration			
<b>cil</b> e	nts and Users								
R	urcubeshoot 🍐 lest	• 🗶 usable	- Kamave 🧕	More 💌 🚟 Irai	rk Clents	Soldenniy	Hoknown Hisers		
	MAC Address	IP Address	IP iype	User Name	lype	Vendor	Device Name		
0	00:22:90:1b:17:42		₽v1	Unknown		Cisco	WCS_SW 0.1.0.2		
0	1c:df:0f:66:86:58		₽v4	Unknown	5	Cisco	WC5_SW-9.1.0.2		
0	00:21:6a:97:9b:bc		₽v4	host/vikatta		Intel	oeap-laiwar-2		
0	00:22:90:15:96:48		IPv4	Unknown	-	LISCO	WCS_SW-9.1.0.2		
0	00:22:90:1b:17:8c		₽v1	Unknown	<b></b>	Cisco	WCS_SW 0.1.0.2		
Q	00:25:0b:4d:77:c4		₽v4	Unknown	5	Cisco	WCS_SW-9.1.0.2		
0	c4:7d:4f:3a:c5:d5		IPv4	Unknown		CISCO	WCS_SW-9.1.0.2		
0	00:21:a0:d5:03:c4		IPv4	Unknown	<b></b>	Cisco	WCS_SW-9.1.0.2		
Û	f3:66:f2:67:7f:60		₽v4	Unknown	5	Cisco	WC5_SW-9.1.0.2		
0	00:15ca:b0:01:b4		₽v4	Unknown	2	Cisco	WCS_SW-9.1.0.2		
0	88:43:e1:d1:df:02		IPv4	Unknown	<b></b>	LISCO	WCS_SW-9.1.0.2		
0	00:22:bd:1b:e2:b5		₽v1	Unknown	<b></b>	Cisco	WCS_SW 0.1.0.2		
0	f3:66:f2:ab:1e:69		₽v4	Unknown	5	Cisco	WC5_SW-9.1.0.2		
Ō.	00:10:58:dc:b4:4e		₽v4	Unknown	8	Ciscu	WCS_SW-9.1.0.2		
$\cap$	00:1e:/a:bb:21:8d		IPv4	ssimm	618	CISCO	oean-ta viar-7		

Virtual Domain: ROOT-DOMAIN

root 🗸 Log Out

2+

E (2)

			Show	Associated Clients 🔹 🍸
Location	VLAN	Status	Interface	Quick Filter
Unknown	109	Associated	Gi1/0/34	Advanced Filter
Unknown	109	Associated	Gi1/0/26	All
Root Area	310	Associated	data	Manage Preset Filters
Unknown	109	Associated	Gi1/0/36	2.4GHz Clients
Unknown	109	Associated	Gi1/0/32	5GHz Clients
Unknown	109	Associated	Gi1/0/30	All Lightweight Clients
Unknown	109	Associated	Gi1/0/13	All Wired Clients
Unknown	109	Associated	Gi1/0/27	Associated Clients
Unknown	109	Associated	Gi1/0/12	Clients known by ISE
Unknown	109	Associated	Gi1/0/15	Clients detected by MSE
Unknown	109	Associated	Gi1/0/28	Clients detected in the last 24 hours
Unknown	109	Associated	Gi1/0/14	Clients with Problems
Unknown	109	Associated	Gi1/0/9	Excluded Clients
Unknown	109	Associated	Gi1/0/29	FlexConnect Locally Authenticated
Root Area	311	Associated	voice	New clients detected in last 24 hours

### 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:d7:28	o: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.

neral	Security	QoS A	dvanced		
ayer 2	Layer 3	AAA Serv	ers		
Layer 2	Security 🧧	WPA+WPA2	1	*	
		_			
		2MAC Filteri	ng		
PA+WPA	2 Paramete	2MAC Filteri	ng		
WPA Po	2 Paramete	ers	ng		
WPA Po WPA Po	2 Paramete	ers	ng		
WPA Po WPA2 P WPA2 E	2 Paramete licy olicy ncryption	I gMAC Filteri		-	
WPA Po WPA2 P WPA2 E Auth Ke	2 Paramete licy olicy ncryption by Mgmt	In PMAC Filteri			

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

Allow AAA Override	Enabled	DHCP	
Coverage Hole Detection	Enabled	DHCP Server	verride
Enable Session Timeout	Session Timeout (secs)	DHCP Addr. Assignment 🔲 Re	quired
Aironet IE	Enabled	Management Frame Protection ()	HFP)
Diagnostic Channel	Enabled		
Override Interface ACL	IPv4 IPv6 None V None V	MFP Client Protection d Optiona	el 🗸
P2P Blocking Action	Disabled	DTIM Period (in beacon intervals	)
Client Exclusion 2	Enabled 60	802.11a/n (1 - 255) 1	
Maximum Allowed Clients	Timeout Value (secs)	802.11b/g/n (1 - 255) 1	
Static IP Tunneling 👭	Enabled	NAC	
Wi-Fi Direct Clients Policy	Disabled V	NAC State None 💌	
Maximum Allowed Clients	200	Load Balancing and Band Select	
Per AP Radio		Client Load Balancing	
ff Channel Scanning Defer		Client Band Select Z	
Scan Defer Priority 0	1 2 3 4 5 6 7	Passive Client	
		Passive Client	
Scan Defer Time		Voice	
(msecs)		Media Session Snooping	Enable
lexconnect		Re-anchor Roamed Voice Clients	Enable
FlexConnect Local	Enabled	KTS based CAC Policy	Enable

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.

Security	RADIUS Authentication S	Servers > Edit
T AAA General	Server Index	1
• RADIUS	Server Address	
Accounting	Shared Secret Format	ASCII V
Fallback TACACS+	Shared Secret	•••
LDAP Local Net Users	Confirm Shared Secret	•••
MAC Filtering Disabled Clients	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
User Login Policies AP Policies	Port Number	1812
Password Policies	Server Status	Enabled 💌
Local EAP	Support for RFC 3576	Enabled 🛩
Priority Order	Server Timeout	2 seconds
Certificate	Network User	Enable
Access Control Lists	Management	Enable
Wireless Protection     Policies	IPSec	Enable

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.

ll APs > De	tails for AP3	3500					
General	Credentials	Interfaces	High Availa	bility	Inventory	Advanced	
General				,	Versions		
AP Name	4	P3500			Primary Soft	ware Version	7.2.1.69
Location	d	efault location			Backup Softw	vare Version	7.2.1.72
AP MAC A	ddress co	::ef:48:c2:35:57			Predownload	Status	None
Base Radio	MAC 2	c:3f:38:f6:98:b0			Predownload	ed Version	None
Admin Stat	tus E	nable 💌			Predownload	Next Retry Time	NA
AP Mode	E	lexConnect 🗸 🗸			Predownload	Retry Count	NA
AP Sub Mo	de N	one 🗸			Boot Version		12.4.23.0
Operationa	al Status R	EG			IOS Version		12.4(20111122:141426)\$
Port Numb	er 1				Mini IOS Vers	sion	7.0.112.74
Venue Gro	up U	nspecified	¥	1	IP Config		
Venue Typ	e U	nspecified 🔽			IP Address		10.10.10.132
Venue Nan	ne				Static IP		
Language							
Network S Interface K	pectrum 0 Key	D45BA896226F4117	D98BA920FBA	8A16	Time Statistics		
					UP Time		0 d, 00 h 01 m 14 s
					Controller As	sociated Time	0 d, 00 h 00 m 14 s
					Controller As	sociation Latency	0 d, 00 h 00 m 59 s

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

Local Authentication	Image Upgrade VLAN	I-ACL mapping		
Group Name Store 1				
exConnect APs		Ала		
id AP		Primary Radius Server	None	*
Select APs from current controller	V	Secondary Radius Server	None	~
	AP3500 ¥	Enable AP Local Authentication		
AP Name				

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


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

AP Nam	e	AP3500	
Base Ra	adio MAC	2c:3f:38:f6:98:b0	
WLAN Id	SSID		VLAN ID
1	Store 1		109

VLAN.

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

Radius.

	Attribute	Туре	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.

General Loo	cal Authentication	Image Upgrade	VLAN-ACL mapping
VLAN ACL Map Vlan Id Ingress ACL Egress ACL	3 none V		

- 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.

WLANs > Edit 'Store 1	*
General Security	QoS Advanced
Allow AAA Override	
Coverage Hole Detection	
Enable Session Timeout	✓ 1800 Session Timeout (secs)
Aironet IE	✓Enabled
Diagnostic Channel	Enabled
Override Interface ACL	IPv4 None 💙 IPv6 None 💙
P2P Blocking Action	Disabled 💌
Client Exclusion <sup>3</sup>	Enabled 60 Timeout Value (secs)
Maximum Allowed Clients 🖉	0
Static IP Tunneling 👭	Enabled
Wi-Fi Direct Clients Policy	Disabled 💌
Maximum Allowed Clients Per AP Radio	200
FlexConnect	
FlexConnect Local Switching 省	Enabled

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

WLANs > Edit 'Store 1'	*
General Security	QoS Advanced
Allow AAA Override	✓ Enabled
Coverage Hole Detection	Enabled
Enable Session Timeout	Session Timeout (secs)
Aironet IE	Enabled
Diagnostic Channel	Enabled
Override Interface ACL	IPv4 None 💌 IPv6 None 💌
P2P Blocking Action	Disabled 💌
Client Exclusion <sup>3</sup>	Enabled 60 Timeout Value (secs)
Maximum Allowed Clients <sup>g</sup>	0
Static IP Tunneling 🎞	Enabled
Wi-Fi Direct Clients Policy	Disabled 💌
Maximum Allowed Clients Per AP Radio	200
FlexConnect	
FlexConnect Local Switching <sup>2</sup>	Enabled
FlexConnect Local Auth 💶	Enabled
Learn Client IP Address 5	Enabled
Vlan based Central Switching <sup><u>13</u></sup>	Enabled

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

All APs > De	tails for AP_3	3500E		
General	Credentials	Interfaces	High Availa	bility
General				
AP Name	AP.	_3500E		
Location				
AP MAC A	ddress o4:	7d:4f:3a:07:74		
Base Radio	o MAC o4:	7d:4f:53:24:e0		
Admin Sta	tus En	able 💌		
AP Mode	Fle	xConnect 🔽		
AP Sub Mo	de loc	al xConnect	and the second se	
Operationa	al Status mo	nitor		
Port Numb	er Sn	iffer		
Venue Gro	oup SE	dge -Connect	~	

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

ululu cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY
Wireless	All APs >	AP_3500	DE > VLAN Ma	ppings	
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>802.11a/n</li> <li>802.11b/a/n</li> </ul> </li> </ul>	AP Name Base Rad	io MAC o	AP_3500E x4:7d:4f:53:24:e0		
Global Configuration	WLAN	SSID			VLAN ID
Advanced	1	'Store 1' :			63
Mesh					
RF Profiles	Centrally	switched	Wlans		
FlexConnect Groups FlexConnect ACLs	WLAN Id		SSID	VLAN ID	
▶ 802.11a/n	AP level	VLAN ACL	Mapping		
▶ 802.11b/g/n	Vlan Id	Ingr	ess ACL	Egress A	CL
▶ Media Stream	63	none	• •	none 💌	
Country Timers	Group le	vel VLAN A	CL Mapping		
▶ QoS	Vlan Id	Ingr	ess ACL	Egress A	CL

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).

li.ili. cisco	MONITOR W	<u>v</u> lans (	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>a</u> nagement ci	<u>o</u> mmands	HELP FEEDBAC	ж
Controller	Interfaces								
General Inventory	Interface Na	ime	¥L.	AN Identifier	IP Address	Interface Ty	pe Dynamic	AP Management	t _
Interfaces	<u>dyn</u>		62		9.6.62.10	Dynamic	Disabled		
Interface Groups	management		61		9.6.61.2	Static	Enabled		

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.				
Monitor	Clients > Detail			
Summary				
Access Points				
Cisco CleanAir	Client Properties		AP Properties	
Statistics	HAC Address	00.40.05.50.44.5	AD Address	
▶ CDP	IDud Address	00:40:96:00:04:06	AP Notress	04:70:41:53:24:60
Rogues	IPv6 Address	9.6.62.100	AP Name	AP_3500E
Redundancy			WI AN Brofile	'Store 1'
Clients			Data Switching	Central
Multicast			Authentication	Central
			Status	Associated
			Association ID	1
			802.11 Authentication	Open System
			Reason Code	3
			 Status Code	0
	Client Type	Regular	CF Pollable	Not Implemented
	User Name	betauser	CF Poll Request	Not Implemented
	Port Number	1	Short Preamble	Not Implemented
	Interface	dyn	PBCC	Not Implemented
	VLAN ID	62	Channel Agility	Not Implemented

**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).

 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

Clients > Detail			
Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	o4:7d:4f:53:24:e0
IPv4 Address	9.6.61.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	Store 1'
		Data Switching	Central
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authentication	n Open System
		Reason Code	3
		: Status Code	0
Client Type	Regular	CF Pollable	Not Implemented
User Name	betauser2	CF Poll Request	Not Implemented
Port Number	1	Short Preamble	Not Implemented
Interface	management	PBCC	Not Implemented
VLAN ID	61	Channel Agility	Not Implemented

**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

Clients > Detail			
<b>Client Properties</b>		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	o4:7d:4f:53:24:e0
IPv4 Address	9.6.63.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central

### **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:

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

FlexConnect Access Control Lists	Entries 0 - 0 of 0	New
Acl Name		

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

ACL.

Access Control Lists > New	< Back Apply
Access Control List Name Flex-ACL-Ingress	

- 4. Fare clic su **Apply** (Applica).
- 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.

Acce	ss Con	trol Lists > Edit						< Back	Add New Rule
Gene	ral	e Elev-ACL	Incress						
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP		
Seq	Action	Source IP/Mask	IP/Mask	Protocol	Port	Port	DSCP		

6. Fare clic su Aggiungi nuova

regola.					
Access Control Lis	sts > Rules > New			< Back	Apply
Sequence	1				
Source	IP Address 💌	IP Address 0.0.0.0	0.0.0.0	]	
Destination	IP Address 💌	IP Address 0.0.0.0	Netmask 0.0.0.0	]	
Protocol	Any 💌				
DSCP	Any 💌				
Action	Deny 💌				
L					

**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.

Base Rad	lio MAC	2c:3f:38:f6:98:	:60	
WLAN Id	SSID			VLAN ID
1	Store 1			109
Centrally	switche	d Wlans		
WLAN Id	SSID			VLAN ID

 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.

ieneral	Lo	cal Authenticati	on	Image Upgrade	VLAN-ACL map	ping
LAN AC	L Maj	oping				
Vlan Id	6	0				
Ingress	ACL [	Flex-ACL-Earess	~			
Egress A	CL	Flex-ACL-Egress	~			
	L					

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.
- II 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

WLANs > Ed	it 'Store	1'							
General	Security	QoS	Advan	ced					
Allow AAA	Override	🔲 Ena	abled						
Coverage	Hole Detection	n 🗹 Ena	🗹 Enabled						
Enable Ses	ssion Timeout	✓ 180 Se	00 ssion Tim	eout (:	secs)				
Aironet IE		Ena	bled						
Diagnostic	Channel	Ena	Enabled						
Override I	nterface ACL	IPv4	IPv4 None 💌 IPv6 None 💌						
P2P Blocki	ng Action	Disab	Disabled						
Client Excl	usion ²	☑Ena	Enabled Timeout Value (secs)						
Maximum Clients 🔮	Allowed	0	0						
Static IP To	unneling 👭	Ena	bled						
Wi-Fi Direc Policy	t Clients	Disab	led 💌	Г	Floy Los	al Curitabina			
Maximum Clients Per	Allowed • AP Radio	200			should no	ot be enabled			
FlexConnect				_	/				
FlexConne Switching	ct Local 2	<b></b>	Enabled	-					

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

WLANs > Edit 'St	lore 1"				
General Securi	ity QoS Advanced				
Allow AAA Overrid	e Enabled		DHCP		
Coverage Hole De	tection 🔽 Enabled		DHC	D Server	Override
Enable Session Tin	meout 🖂 1800		bho	- Server	
	Session Timeout (secs)		DHC	P Addr. Assignment	Required
Aironet IE	Enabled		Manage	ment Frame Prot	tection (MFP)
Diagnostic Channe	Enabled				
Override Interface	ACL IPv4 None ⊻	IPv6 None 🛩	MFP	Client Protection 🔮	Optional 💌
Impostare AP Ma	General Credent	AP_3500E	aces	High Ava	ailability
Impostare AP Ma	General Credent	AP_3500E	aces	High Ava	ailability
Impostare AP M	General AP Name	AP_3500E	aces	High Ava	ailability
Impostare AP M	General AP Name Location	AP_3500E	aces	High Ava	ailability
Impostare AP M	General AP Name Location AP MAC Address	AP_3500E	aces 07:74	High Ava	ailability
Impostare AP M	General AP Name Location AP MAC Address Base Radio MAC	AP_3500E AP_3500E AP_3500E 04:7d:4f:3a: 04:7d:4f:53:	aces 07:74 24:e0	High Ava	ailability
Impostare AP M	General Credent General Credent AP Name Location AP MAC Address Base Radio MAC Admin Status	AP_3500E AP_3500E AP_3500E 04:7d:4f:3a: 04:7d:4f:53: Enable	aces 07:74 24:e0	High Ava	ailability
Impostare AP M	General General AP Name Location AP MAC Address Base Radio MAC Admin Status AP Mode	AP_3500E AP_3500E AP_3500E 04:7d:4f:3a: 04:7d:4f:53: Enable V FlexConnect local	aces 07:74 24:e0	High Ava	ailability
Impostare AP Ma	General Credent General Credent AP Name Location AP MAC Address Base Radio MAC Admin Status AP Mode AP Sub Mode	AP_3500E AP_3500E AP_3500E 04:7d:4f:3a: 04:7d:4f:3a: 04:7d:4f:53: Enable V FlexConnect local FlexConnect monitor	aces 07:74 24:e0	High Ava	ailability
Impostare AP M	General Credent General Credent AP Name Location AP MAC Address Base Radio MAC Admin Status AP Mode AP Sub Mode Operational Status	AP_3500E AP_3500E AP_3500E AP_3500E 04:7d:4f:3a: 04:7d:4f:53: Enable V FlexConnect Iocal FlexConnect monitor Rogue Detector	aces 07:74 24:e0	High Ava	ailability
Impostare AP M	General Credent General Credent AP Name Location AP MAC Address Base Radio MAC Admin Status AP Mode AP Sub Mode Operational Status Port Number	AP_3500E AP_3500E AP_3500E AP_3500E 04:7d:4f:3a: 04:7d:4f:53: Enable FlexConnect Iocal FlexConnect monitor Rogue Detect Sniffer Bridge	aces 07:74 24:e0	High Ava	ailability

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.

cisco	MONI	tor y	<u>N</u> LANs	CONTRO	LLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Wireless	Acce	ess Co	ntrol Li	sts > Ed	it						
Access Points     All APs     Radios     802.11a/n     802.11b/n/n	Gene	eral s List Nar	me	F	lex-A0	u					
Global Configuration	Sea	Action	Sourc	e IP/Mar	ik I	estination P/Mask	Protoco	Source Port	Dest Port	DSCP	
Advanced Mesh	1	Permit	9.6.61	1.0	1 9	0.1.0.150	ICMP	Any	Any	Any	۰
RF Profiles FlexConnect Groups FlexConnect ACLs											

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.									
սիսիս cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	неџр	EEEDBACK
Wireless	All APs >	Details f	for AP_3500E						
Access Points     All APs	General	Cred	entials Inter	faces Hi	gh Availability	y Inventory	FlexConne	ect A	Advanced
✓ Radios 802.11a/n 802.11b/g/n Global Configuration	VLAN S	upport					L		
Advanced	Native	VLAN ID	57	VLAN Ma	ppings				
Mesh	FlexCo	nnect Grou	up Name Not C	onfigured					
RF Profiles	PreAuthe	ONITOR       WLANS       CONTROLLER       WIRELESS       SECURITY       MANAGEMENT       COMMANDS       HELP       EEEDBACK         II APs > Details for AP_3500E       General       Credentials       Interfaces       High Availability       Inventory       FlexConnect       Advanced         VLAN Support       Image: Connect Group Name       Not Configured       FlexConnect Group Name       Not Configured							
FlexConnect Groups FlexConnect ACLs	Externa	l WebAuth	entication ACLs						
▶ 802.11a/n	Local S	olit ACLs	-						

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

AP Name	AP_3500E	
Base Radio	MAC 04:7d:4f:53:24:e0	
WLAN Id	0	
Local-Split	ACL Flex-ACL V	
Local-Split WLAN Id WI	ACL Flex-ACL V Add	Local-Split ACL

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**.



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

Wireless	FlexConnect Groups > Edit	Flex-Group'		
Access Points     All APs     Radios	General Local Authentication	Image Upgrade A	AA VLAN-ACL mapping WLAN	ACL mapping WebPolicies
802.11a/n 802.11b/g/n Global Configuration	Web Auth ACL Mapping		Local Split ACL Mapping	
<ul> <li>Advanced</li> <li>Mesh</li> </ul>	WLAN Id 0		WLAN Id 0	
RF Profiles	Add		bba	
FlexConnect Groups FlexConnect ACLs			Landson and L	
▶ 802.11a/n	WLAN Id WLAN Profile Name	WebAuth ACL	WLAN Id WLAN Profile Na	me LocalSplit ACL
≱ 802.11b/g/n			1 'Store 1'	Flex-ACL 💌 🖬

# **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.

### <u>Riepilogo</u>

- 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

ANs > Edit			< Back	Appl
eneral Securi	ty Qo	S Advance	٦	
Allow AAA Overrid		Enabled	DHCP	
Coverage Hole De	tection 🗹	Enabled	DHCP Server 🔲 Override	
Enable Session Tir Aironet IE	neout 🗹	1800 Session Timeor Enabled	(secs) DHCP Addr. Assignment Required Nanagement Frame Protection (NFP)	
IPv6 Enable 2		]Enabled	MFP Client Protection 🐔 Optional 💌	
Override Interface	ACL N	ione 🔽	DTIM Period (in beacon intervals)	
P2P Blocking Actio		Enabled 60 Time	802.11a/n (1 - 255)         1           ut Value (secs)         802.11b/g/n (1 - 255)         1	
Clients 2	0		NAC	
f Channel Scanni	g Defer		NAC OOB State Enabled	
Scan Defer Priorit	0	1 2 3 4 5 6	7 Posture State Enabled	
			Load Balancing and Band Select	
Scan Defer	_		Client Load Balancing	
Time(msecs)	100		Client Band Select 🐔 📃	
				>
H-REAP Local Switci When client exclusis Client MPP is not ac Learn Client IP is co WMM and open or A Multicast Should Be Band Select is confi Value zero implies	ing is not : n is enable ive unless nfigurable ES security Enabled Fo purable on here is po	supported with IF ed, a Timeout Vai WPA2 is configur only when HREAI v should be enabl vr IPV6. ly when Radio Po restriction on ma	ec, CRANITE authentication e of zero means infinity (will require administrative override to reset excluded clients) d Local Switching is enabled d to support higher IIn rates cy is set to 'Ail'.	

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.

WLAN Configuration Deta	ils : 17	
Configure > Controllers > 172.20.229	.154 $>$ WLANs $>$ WLAN Configuration $>$ W	LAN Configuration Details
General Security QoS	Advanced	
FlexConnect Local Switching	Enable	DUCD
FlexConnect Local Auth 🔍	Enable	
Learn Client IP Address	Enable	DHCP Server
Session Timeout	Enable 1800 (secs)	DHCP Address Assignment
Coverage Hole Detection	🗹 Enable	Management Frame Protectio
Aironet IE	🗹 Enable	management rame rroteca
IPv6 Z	🛄 Enable	MED Client Distoction
Diagnostic Channel 2	🔲 Enable	MPP Client Protection 2
Override Interface ACL	IPv4 NONE	MFP Version
	IPv6 NONE	Load Balancing and Band Sel
Peer to Peer Blocking 🔍	Disable	
Wi-Fi Direct Clients Policy	Disabled 🗸	Client Load Balancing
Client Exclusion 🕹	🗹 Enable	Client Band Select
Timeout Value	60 (secs)	
Maximum Clients 🔍	0	NAC

# 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

lexconnect.				
WLANs > Edit 'S to	wel'			
General Security (	QoS Advanced			
Aironet IE	Enabled		Management Frame Protection	(MFP)
Override Interface ACL	IPv4 None V	IPv6 None 💌	MFP Client Protection # Opti	onal 💌
P2P Blocking Action	Drop 💌		DTIM Period (in beacon interva	als)
Client Exclusion 2	Enabled 60 Timeout Value (s	secs)	802.11a/n (1 - 255)	
Maximum Allowed Clients			802.11b/g/n (1 - 255) 1	
Static IP Tunneling 44	Enabled		NAC	
Wi-Fi Direct Clients Policy	Disabled 💌		NAC State None 💌	
Off Channel Scanning Defe	r		Load Balancing and Band Selec	t
Scan Defer Priority 0	1 2 3 4 5 6 7		Client Load Balancing	
C			Client Band Select Z	
Scan Defer Time	00		Passive Client	
(materia)			Passive Client	
FlexConnect			Voice	
FlexConnect Local Switching 2	Enabled		Media Session Snooping	Enabled

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 file to Controller	
	File Type	Code
	Transfer Mode	TFTP 💌
	Server Details	
	IP Address	
	Maximum retries	10
	Timeout (seconds)	6
	File Path	
download	File Name	AS_5500_7_0_112_52.aes

- 2. Salvare le configurazioni sui controller, ma non riavviare il controller.
- 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-



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:

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

Download file to Controller		
File Type	Code	~
Transfer Mode	TFTP 💌	
Server Details		
IP Address		
Maximum retries	10	
Timeout (seconds)	6	
File Path		
File Name	AS_5500_7_2_1_72.aes	

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

eneral	Local Authentication	Image Upgrade	VLAN-ACL mapping			
Group N	ame Store 1					
lexCon	nect APs		AAA			
dd AP			Prima	ary Radius Server	None	v
Calant A	Ps from current controller	<b>V</b>	Seco	ndary Radius Server	None	*
SCIECT N			Enab	le AP Local Authentication		
AP Nam	e	AR3500 ¥				

 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.

FlexConnec	t Groups > 'Store 1'		
General	Local Authentication	Image Upgrade	VLAN-ACL mapping
FlexConnec FlexConne	t AP Upgrade		
AP Name Add Mast	AP3500	~	
Master AP I	Name AP Model	Manual	

 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.

eneral Local Authentica	tion Image Upgra	de VLAN-ACL mapping	
FlexConnect AP Upgrade 🗹			
Slave Maximum Retry Count	44		
Upgrade Image	Backup 💌	FlexConnect Upgrade	
lexConnect Master APs			
lexConnect Master APs			
AP Name AP3500	~		
AP Name AR3500 Add Master	×		
AP Name Add Master Master AP Name	M AP Model	Manual	

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.

eneral Local Authentic	ation Image Upg	rade VLAN-ACL mapping	
FlexConnect AP Upgrade Slave Maximum Retry Count Upgrade Image IexConnect Master APs	44 Backup 💌	FlexConnect Upgrade	
AP Name AP3500-1 Add Master	~		
	AP Model	Manual	
Master AP Name	Pit House		

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

 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.

lexConne	ct Groups > Edit	'Store 1'			
General	Local Authenticat	tion Image Up	grade	VLAN-ACL mapping	
FlexConne	ect AP Upgrade 🔽				
Slave Max	kimum Retry Count	44			
Upgrade I	Image	Primary 💙		FlexConnect Upgrade	

**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.

# <u>Conversione automatica dei punti di accesso in modalità</u> <u>FlexConnect</u>

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

# All APs > Details for AP3500

General 🦲	Credentials	Interfaces	High Availability		
eneral					
AP Name	AP3	500			
Location	defa	ault location	1975		
AP MAC Add	lress 00:	00:22:90:e3:37:df			
Base Radio I	MAC 00:	00:22:bd:d1:71:30			
Admin Statu	s Dis	Disable 👻			
AP Mode	loca	al 🔻			
AP Sub Mod	e loca	Connect			
Operational	Status mor	monitor			
Port Number	r Rog Snif	ue Detector fer			
Venue Group	p Brid	lge Connect	-		

riavviato.

esta 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 Control)	ler) >config ap autoconvert ?
disable	Disables auto conversion of unsupported mode APs to supported modes when AP joins
flexconnect monitor	Converts unsupported mode APs to flexconnect mode when AP joins 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

AP Mode	FlexConnect 🔹	
AR Sub Mode	local	
AF 300 Mode	FlexConnect	
Operational Status	monitor	
	Rogue Detector	
Port Number	Sniffer	
	Bridge	
Venue Group	SE-Connect	-

Bridge.

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:

 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.

Concert Concerts	0.0			)		
General Security	QoS	Adv	anced	L		
Allow AAA Override Coverage Hole Detection	Ena	bled				
Enable Session Timeout	✓ 180 Se:	10 ssion T	imeout (	secs)		
Aironet IE	Enat	oled				
Diagnostic Channel	Enat	oled				
Override Interface ACL	IPv4	Vone 🖪	/		IPv6	None N
P2P Blocking Action	Disab	led	1	•		
Client Exclusion <sup>3</sup>	☑Enat	oled	60 Timeout	Value (sec	] :s)	
Maximum Allowed Clients <sup>g</sup>	0					
Static IP Tunneling 👭	Enat	oled				
Wi-Fi Direct Clients Policy	Disab	led 🔽				
Maximum Allowed Clients Per AP Radio	200					
Clear HotSpot Configuration FlexConnect	Enat	oled				
FlexConnect Local Switching <sup>2</sup>	<b>⊻</b> E	nabled				

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

All APs > De	etails for AP_	3500E		
General	Credentials	Interfaces	High Availa	bility
General				
AP Name	AP.	_3500E		
Location				
AP MAC A	ddress o4	7d:4f:3a:07:74		
Base Radi	o MAC o4	7d:4f:53:24:e0		
Admin Sta	atus En	able 💌		
AP Mode	Fle	xConnect 💌		
AP Sub M	ode loc	al	and the second se	
Operation	al Status mo	onitor		
Port Numi	ber Sn	iffer		
Venue Gr	oup SE	dge -Connect	~	

3. Associare WGB ai client cablati dietro la WLAN

configu	urata.											
MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK				
Clients												
Current Fil	iter	None	[Change Filte	r] [Clear Filter	1							
Client NA	C Addr	AP Name		WLA	N Profile	WLAN SSID		Protocol	Status	Auth	Port	WGB
00:40:96:8	8:d4:be	AP_3500E		*Stor	e 1'	'Store 1'		N/A	Associated	Yes	1	No
00:50:b6:0	19:e5:3b	AP_3500E		'Sto	re 1'	'Store 1'		N/A	Associated	Yes	1	No
o4:7d:4f:3	a:08:10	AP 3500E		*Stor	re 1'	'Store 1'		802.11an	Associated	Yes	1	Yes

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

Clients > Detail			
Client Properties		AP Properties	
MAC Address	o4:7d:4f:3a:08:10	AP Address	o4:7d:4f:53:24:e0
IPv4 Address	9.6.63.102	AP Name	AP_3500E
IPv6 Address		AP Type	802.11an
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authenticati	ion Open System
		Reason Code	1
		Status Code	0
Client Type	WGB	CF Pollable	Not Implemented
Number of Wired Cli	ient(s) 2	CF Poll Request	Not Implemented

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

client.			
Clients > Detail			
Client Properties		AP Properties	
MAC Address	00:50:b6:09:e5:3b	AP Address	o4:7d:4f:53:24:e0
IPv4 Address	9.6.63.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central
		Status	Associated
		Association ID	0
		802.11 Authentication	Open System
		Reason Code	1
		: Status Code	0
Client Type	WGB Client	CF Pollable	Not Implemented
WGB MAC Address	o4:7d:4f:3a:08:10	CF Poll Request	Not Implemented

## **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.

	MONETOR	WLANS O	ONTROLLER	WRELESS 2	ICURITY	MANAGEMENT	COMMANDS	нер	EEGBACK	Saya Configuration
lecurity	RADIUS	Authentical	tion Serve	irs						Appl
AAA	Call Stat	ion 30 Type 🖡	System N	AC Address						
+ RADIUS	Use AES	Key Wap	(Designed	for FIPS customers	and require	a key wrap comp	iant RADDUS se	rver)		
Accounting	MAC Del	miter	Hyphen							
Fallback # TACACS+ LDAP	Network	Management	Server Index	Server Address	Port	19	Sec	Admin	Status	
NAC Filtering	2		1	1.2.3.4	1012	Di	abled	Enables	đ	
Disabled Clients	<b>M</b>	8	2	1.2.3.4	2	Di	belded	Enables	đ	
User Login Policies	8		3	1.2.3.4	3	DA	belded	Enabler	6	
AP Poscies Password Policies	5	8	4	1.2.3.4	4	Di	sabled	Enables	6	
	8	5	5	1.2.3.4	5	Di	unbled	Enables	8	
Call LAP	8		6	1.2.3.4	6	Di	Labled	Enables	6	
riority Order	8		2	1.2.3.4	7	Di	abled	Enables	đ	
ertificate	1	<b>M</b>	8	1.2.3.4		Di	beldes	Enables	đ	
ccess Control Lists	2		2	1.2.3.4	9	Di	beldes	Enables	đ	
Vireless Protection	2	<b>M</b>	22	1.2.3.4	10	Di	abled	Enables	đ	
olicies	2		22	1.2.3.4	11	Di	beldes	Enables	đ	
Veb Auth	2	1	32	1.2.3.4	12	Di	bolded	Enables	đ	
and the first	1		33	1.2.3.4	13	Di	abled	Enables	đ	
rustaec axp	8	8	16	1.2.3.4	14	De	belded	Enabler	đ	
Idvanced	6	8	15	1.2.3.4	15	DA	beldes	Enables	6	
	1	6	15	1.2.3.4	16	Di	abled	Enables	6	
	5	5	12	1.2.3.4	17	Di	abled	Enables	4	

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



 Modalità di configurazione in FlexConnect Group nella release 7.4.1 server RADIUS primario e secondario possono essere configurati nel gruppo FlexConnect utilizzando un indirizzo IP, un numero di porta e un segreto condiviso.
 cisco	Says Carligueston Big Lagest But HONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wineless Al APs * Radio 802.11a/n 002.11b/g/n Dual Bend Relies Global Configuration	FlexConnect Groups > Edit 'abc'     < Back     Apply       General     Local Authentication     Image Upgrade     ACL Mapping     Central DHCP       Group Name     aix       Enable AP Local Authentication?     Image Upgrade     ACL Mapping
<ul> <li>Advanced Meah RF Profiles PlesConnect Groups InscConnect ACLs</li> <li>802.11a/n</li> <li>802.11b/g/n</li> <li>Hedia Stream</li> <li>Application Viaibility And Centrol Country Timers</li> </ul>	FlexConnect APs     AAA       AAI AP     Server Type     Server Type       AP NAC Address     AP Name     Blatus       Stared Secret        Carlier Shared Secret        Add        Server Type     Address       Part        Yonay     1.2.3.4
Netflow     QoS	Uncorrigunes Uncorriguied o M

### **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.

🚡 Monitor	r ▼ <u>R</u> eports		jure 🔻	<u>S</u> ervices	•
Add Contr	ollers				
Configure > Co	ntrollers > Add	Controller	8		
General Pa	rameters				
Add Forma	at Type	Device I	nfo	~	
IP Address	ses	WLC 7	'500 IP	Addres	S
Network M	lask	255.255.25	55.0		
Verify	Telnet/SSH (	Capabilities			
SNMP Para	meters 🕸				
Version		v2c		*	
Retries		2			
Timeout		10		(secs)	
Communit	tà.	private			
Telnet/SSH	Parameters	5 (Q)			
User Name	е	admin			
Password		•••••			
Confirm P	assword	•••••			
Retries		3			
Timeout		60		(secs)	
OK Cano	el				
Controllers Configure > Controllers					
P Address	Controller Name	Type	Locat	ion	Se

7500

5500

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.

7.0.112.62

7.0.112.52

-- Select a command --

mobility

mobility

Reachability St

Reachable

Reachable

Entries (

Identica

Identical

## Domande frequenti

172.20.227.174 d Ambassador

172.20.227.177 @ 5508-Primary

## 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
- <u>Cisco serie 4400 Wireless LAN Controller</u>
- <u>Cisco serie 2000 Wireless LAN Controller</u>
- <u>Cisco Wireless Control System</u>
- <u>Cisco serie 3300 Mobility Services Engine</u>
- <u>Cisco Aironet serie 3500</u>
- <u>Cisco Secure Access Control System</u>
- Documentazione e supporto tecnico Cisco Systems