

Flex 7500 controllerkaart voor draadloze tak

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Productoverzicht](#)

[Productspecificaties](#)

[Gegevensblad](#)

[Platform-functies](#)

[Flex 7500 Opstarten](#)

[Flex 7500 licenties](#)

[Licentie voor AP-basis](#)

[AP-upgrade-licentiëring](#)

[Ondersteuning van softwarerelease](#)

[Ondersteunde access points](#)

[FlexConnect-architectuur](#)

[Voordelen van centraliserend access point Control verkeer](#)

[Voordelen van het distribueren van clientgegevensverkeer](#)

[FlexConnect-manieren van werking](#)

[WAN-vereisten](#)

[Ontwerpen van draadloze branche](#)

[Primaire ontwerpvereisten](#)

[Overzicht](#)

[Voordelen](#)

[Functies voor adressering van vestigingsnetwerkontwerp](#)

[IPv6-ondersteuningsmatrix](#)

[Functiematrix](#)

[AP-groepen](#)

[Configuraties van WLC](#)

[Samenvatting](#)

[FlexConnect-groepen](#)

[Primaire doelstellingen van FlexConnect-groepen](#)

[FlexConnect Group Configuration via WLC](#)

[Verificatie met CLI](#)

[FlexConnect VLAN-override](#)

[Samenvatting](#)

[Procedure](#)

[Beperkingen](#)

[FlexConnect VLAN-gebaseerde Central-switching](#)

[Samenvatting](#)

[Procedure](#)

[Beperkingen](#)

[FlexConnect ACL](#)

[Samenvatting](#)

[Procedure](#)

[Beperkingen](#)

[FlexConnect Split-tunneling](#)

[Samenvatting](#)

[Procedure](#)

[Beperkingen](#)

[Tolerantie fout](#)

[Samenvatting](#)

[Beperkingen](#)

[Clientlimiet per WLAN](#)

[Primaire doelstelling](#)

[Beperkingen](#)

[WLC-configuratie](#)

[NCS configuratie](#)

[Peer-to-peer blokkering](#)

[Samenvatting](#)

[Procedure](#)

[Beperkingen](#)

[AP pre-image downloaden](#)

[Samenvatting](#)

[Procedure](#)

[Beperkingen](#)

[FlexConnect slimme AP-upgrade](#)

[Samenvatting](#)

[Procedure](#)

[Beperkingen](#)

[Auto-converteren APs in FlexConnect-modus](#)

[Handmatige modus](#)

[Auto-conversiemodus](#)

[Ondersteuning van FlexConnect WGB/WGB voor lokale switching WLAN's](#)

[Samenvatting](#)

[Procedure](#)

[Beperkingen](#)

[Ondersteuning voor een groter aantal radiogasers](#)

[Samenvatting](#)

[Procedure](#)

[Beperkingen](#)

[Uitgebreide lokale modus \(ELM\)](#)

[Gast access ondersteuning in Flex 7500](#)

[WLC 7500 beheren vanuit NCS](#)

[FAQ](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een Cisco Flex 7500 draadloze controller kunt implementeren. Dit document heeft tot doel:

- Leg verschillende netwerkelementen van de Cisco FlexConnect-oplossing, samen met hun communicatiestroom, uit.
- Geef algemene implementatierichtlijnen op voor het ontwerpen van de Cisco FlexConnect draadloze brandeoplossing.
- Leg de softwarefuncties uit in de 7.2.103.0-coderelease die de informatiebasis over het product ondersteunt.

Opmerking: Voor 7.2 heet FlexConnect Hybrid REAP (HREAP). Nu heet het FlexConnect.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\)](#) voor meer informatie over documentconventies.

Productoverzicht

Afbeelding 1: Cisco Flex 7500



De Cisco Flex 7500 Series Cloud Controller is een zeer schaalbare bijcontroller voor multisite [draadloze](#) implementaties. Geïmplementeerd in de particuliere cloud, breidt de Cisco Flex 7500 Series controller draadloze services uit naar gedistribueerde filialen met gecentraliseerde controle die de totale kosten van bewerkingen verlaagt.

De Cisco Flex 7500 Series ([afbeelding 1](#)) kunnen draadloze [access points](#) op maximaal 500 locaties beheren en IT-managers in staat stellen om tot 3000 access points (AP's) en 30.000 klanten uit het datacenter te configureren, beheren en probleemoplossing. De Cisco Flex 7500 Series controller ondersteunt beveiligde gasttoegang, robuuste detectie voor PCI-naleving (Payment Card Industry) en in-Branch (lokaal geschakeld) Wi-Fi spraak en video.

Deze tabel toont de schaalbaarheidsverschillen tussen de Flex 7500, WiSM2 en WLC 5500-controller:

schaalbaarheid	Flex 7500	WiSM2	WLC 5500
Totaal access points	6,000	1000	500
Totale clients	64,000	15,000	7,000
Max FlexConnect-groepen	2000	100	100
Max. AP's per FlexConnect-groep	100	25	25
Max. AP-groepen	6000	1000	500

[Productspecificaties](#)

[Gegevensblad](#)

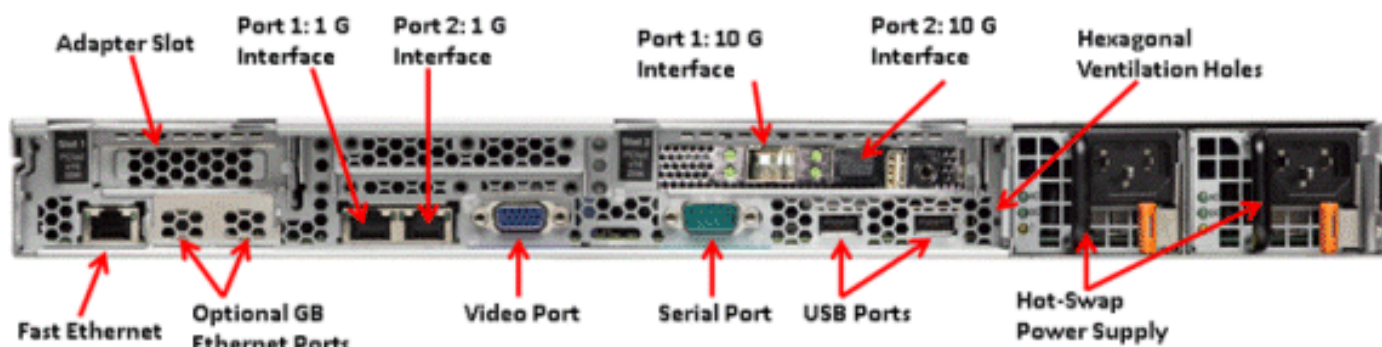
Raadpleeg

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

[Platform-functies](#)

Afbeelding 2: Flex 7500 achteraanzicht

Rear View



[Netwerkitterfacepoorten](#)

Interfacepoorten	Gebruik
Fast Ethernet	Geïntegreerde beheermodule (IMM)
Poorten 1: 1G	WLC-servicepoort
Port 2: 1G	WLC redundante poort (RP)
Poorten 1: 10G	WLC-beheerinterface

Port 2: 10G	WLC-interfacepoort voor back-upbeheer (poortfalen)
Optionele Gb Ethernet-poorten	N.v.t.

Opmerking:

- LAG-ondersteuning voor 2x10G-interfaces maakt actief-actieve link mogelijk met snelle failover-linkredundantie. Een extra actieve 10G-link met LAG verandert de draadloze doorvoersnelheid van de controller niet.
- 2x10G-interfaces
- 2x10G interfaces ondersteunen alleen optische kabels met SFP-product # SFP-10G-SR.
- Switch-zijde SFP-product # X2-10GB-SR

System MAC-adressen

Poorten 1: 10G (beheerinterface)	System/Base MAC-adres
Port 2: 10G(Reserve Management-interface)	Base MAC-adres + 5
Poorten 1: 1G (servicepoort)	Base MAC-adres + 1
Port 2: 1G (redundante poort)	Base MAC-adres + 3

Seriële console opnieuw direct

Met de WLC 7500 kan console standaard 9600 omleiden met een basissnelheid, waarbij Vt100-terminal zonder stroomcontrole wordt gesimuleerd.

Informatie over inventaris

Afbeelding 3: WLC 7500-console

```
(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
```

De DMI-tabel (Desktopbeheer Interface) bevat serverhardware en geprogrammeerde informatie.

De WLC 7500 wordt als onderdeel van de inventaris weergegeven in de volgende versies: PID/VID en Serienummer.

Flex 7500 Opstarten

Cisco-oplader-opties voor softwareonderhoud zijn identiek aan de huidige Cisco-controllers.

Afbeelding 4: Opstarten in volgorde

```
Cisco Bootloader (Version      )

      .o88b. d8888888b .d8888. .o88b. .d88b.
d8P  Y8  `88'  88'  YP d8P  Y8  .8P  Y8.
8P      88   `8bo.  8P      88   88
8b      88      `Y8b. 8b      88   88
Y8b  d8   .88.   db   8D Y8b  d8  `8b  d8'
`Y88P' Y8888888P `8888Y' `Y88P' `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
```

Afbeelding 5: Wizard WLC-configuratie

```
Would you like to terminate autoinstall? [yes]:
System Name [Cisco_65:db:6c] (31 characters max):
AUTO-INSTALL: process terminated -- no configuration loaded

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

Management Interface IP Address: 172.20.227.174
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 172.20.227.161
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 2]: 1 ← Management Port 1: 10G
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
```

Opmerking: De Flex 7500 opstart-reeks is gelijkwaardig en consistent met bestaande controllerplatforms. Voor het opstarten dient de WLC-configuratie te worden gebruikt met de Wizard.

[Flex 7500 licenties](#)

[Licentie voor AP-basis](#)

AP Base Count SKUs

300
500
1000
2000
3000
6000

[AP-upgrade-licentiëring](#)

AP-upgrade SKU's
100
250
500
1000

Behalve voor de basis- en upgrade-tellingen is de gehele licentieprocedure die het bestellen, de installatie en het weergeven betreft vergelijkbaar met de bestaande WLC 5508 van Cisco.

Raadpleeg de [configuratiehandleiding voor WLC 7.3](#), die de gehele licentieprocedure bestrijkt.

[Ondersteuning van softwarerelease](#)

Flex 7500 ondersteunt WLC codeversie 7.0.16.x en alleen later.

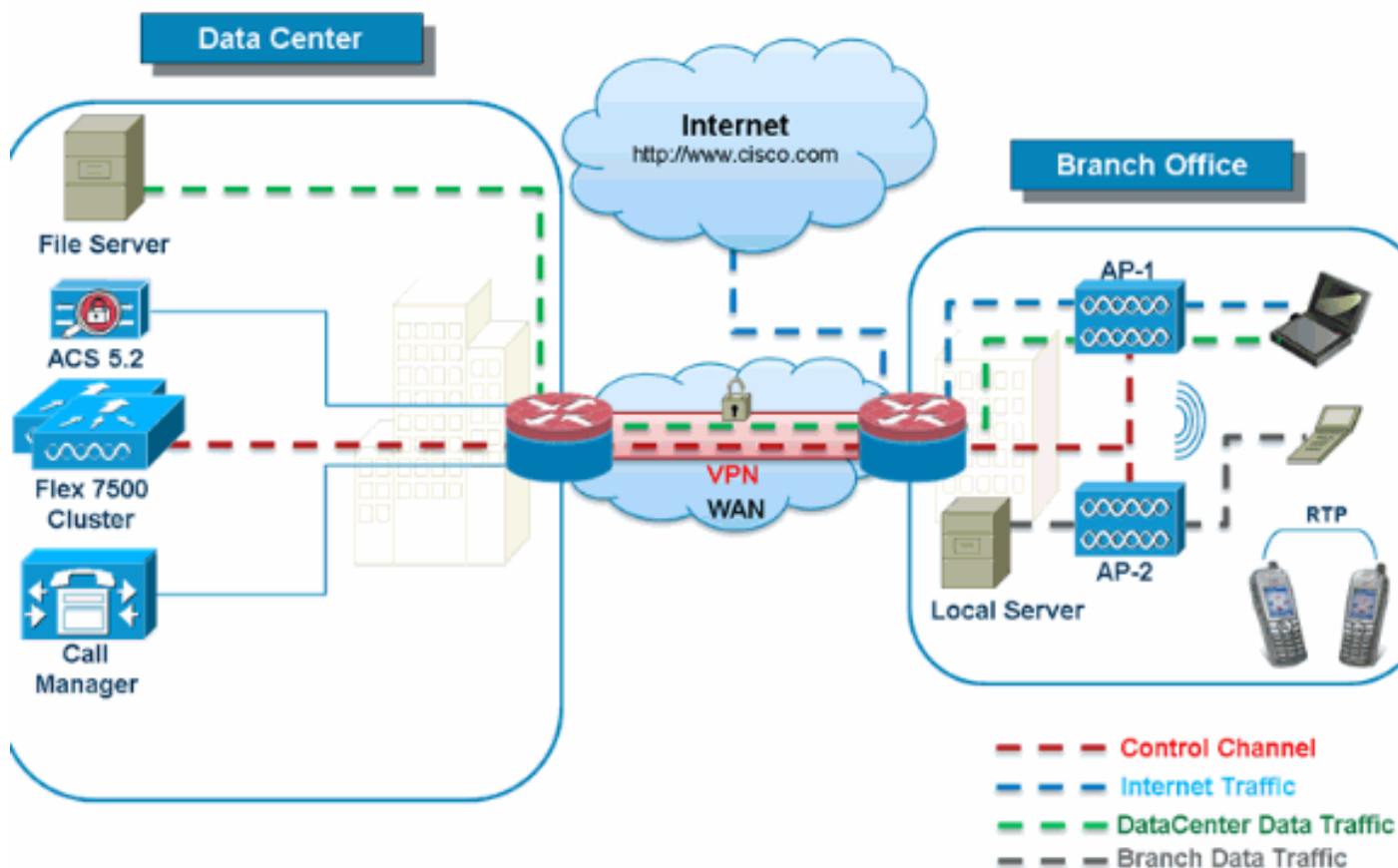
[Ondersteunde access points](#)

Access points 1040, 1130, 1140, 1550, 3500, 3600, 2600, 1250, 1260, 1240, OEAP 600, ISR 891 en ISR 881 wordt ondersteund met Flex 7500.

[FlexConnect-architectuur](#)

Afbeelding 6: Typische draadloze tak-topologie

FlexConnect Architecture



FlexConnect is een draadloze oplossing voor implementaties in vestigingen en kantoren op afstand. Het wordt ook wel een Hybrid REAP-oplossing genoemd, maar dit document zal het FlexConnect noemen.

De FlexConnect-oplossing stelt de klant in staat:

- Beheer en controle van AP's vanaf het datacenter centreren. Het controleverkeer wordt in [afbeelding 6](#) gemarkeerd met rode streepjes.
- Verdeel het clientgegevensverkeer in elk Vestigingskantoor. Het gegevensverkeer wordt in [afbeelding 6](#) gemarkeerd met de blauwe, groene en paarse streepjes. Elke verkeersstroom gaat op de meest efficiënte manier naar zijn eindbestemming.

Voordelen van centraliserend access point Control verkeer

- Enkelvoudig deelvenster met bewaking en probleemoplossing
- Eenvoudig beheer
- Beveiligde en naadloze mobiele toegang tot de middelen van datacenters
- Vermindering van de voetafdruk van de branche
- Verhoging van operationele besparingen

Voordelen van het distribueren van clientgegevensverkeer

- Geen operationele downtime (overlevingsmogelijkheid) tegen volledige WAN-link-mislukkingen of onbeschikbaarheid van de controller
- Mobiliteitsveerkracht binnen de aftakking tijdens WAN-link

- Toename in de schaalbaarheid. Ondersteunt de grootte van de tak die tot 100 APs en 250.000 vierkante voet (5000 vierkante voet) kan kunnen opschalen. voetjes per AP).

De Cisco FlexConnect-oplossing ondersteunt ook Central Client Data Traffic, maar deze mag alleen worden beperkt tot Guest-gegevensverkeer. In deze volgende tabel worden de beperkingen op WLAN L2-beveiligingstypen alleen beschreven voor niet-gastklanten wier gegevensverkeer ook centraal in het datacenter is geschakeld.

L2 beveiligingsondersteuning voor centraal switched niet-Guest-gebruikers

WLAN L2-beveiliging	Type	Resultaat
None	N.v.t.	toegestaan
WAP + WAP2	802,1x	toegestaan
	CCKM	toegestaan
	802.1x + CCKM	toegestaan
	PSK	toegestaan
802,1x	medegebruik	toegestaan
Statische Wi	medegebruik	toegestaan
EFN + 802.1x	medegebruik	toegestaan
CKIP		toegestaan

Toelichting: Deze beperkingen op de echtheidscontrole zijn niet van toepassing op cliënten wier gegevensverkeer in het bijkantoor wordt verspreid.

L3 Security ondersteuning voor Centraal- en Lokaal switched gebruikers

WLAN L3-beveiliging	Type	Resultaat
Web verificatie	Intern	toegestaan
	Extern	toegestaan
	Aangepast	toegestaan
Web Pass-Through	Intern	toegestaan
	Extern	toegestaan
	Aangepast	toegestaan
Voorwaardelijk web redirect	Extern	toegestaan
spaander pagina Web redirect	Extern	toegestaan

Raadpleeg de [Flexconnect-gids voor externe webauth](#) voor meer informatie over de [implementatie van Flexconnect](#)

Zie [FlexConnect](#) configureren voor meer informatie over de HREAP/FlexConnect AP-status en de opties voor het overschakelen van gegevens.

[FlexConnect-manieren van werking](#)

FlexConnect-modus	Beschrijving

Verbonden	Een FlexConnect wordt geacht in Connected Mode te zijn wanneer zijn CAPWAP-besturingsplane terug naar de controller is geïnstalleerd en gebruiksklaar is, wat betekent dat de WAN-link niet naar beneden is.
Standalone	Standalone modus wordt gespecificeerd aangezien de operationele status van FlexConnect wordt ingevoerd wanneer deze niet langer de connectiviteit weer naar de controller heeft. FlexConnect APs in de Standalone modus zullen blijven functioneren met laatste bekende configuratie, zelfs in het geval van stroomuitval en WLC of WAN-falen.

Raadpleeg de [H-Reap / FlexConnect Design and Deployment Guide](#) voor meer informatie over FlexConnect Operations.

WAN-vereisten

FlexConnect APs worden uitgevoerd op de Vestigingsplaats en beheerd van het datacenter via een WAN-link. Het is sterk aanbevolen dat de minimale bandbreedte-beperving 12,8 kbps per AP blijft met een retoursnelheid van niet meer dan 300 ms voor gegevensimplementaties en 100 ms voor data- + spraakimplementaties. De maximale transmissieeenheid (MTU) moet ten minste 500 bytes zijn.

Type implementatie	WAN-bandbreedte (min.)	WAN RTT-client (max.)	Max. AP's per bedrijfsterminal	Max. clients per bedrijfsterminal
Gegevens	64 kbps	300 ms	5	25
Data + spraak	128 kbps	100 ms	5	25
monitor	64 kbps	2 seconde	5	N.v.t.
Gegevens	640 kbps	300 ms	50	1000
Data + spraak	1,44 Mbps	100 ms	50	1000
monitor	640 kbps	2 seconde	50	N.v.t.

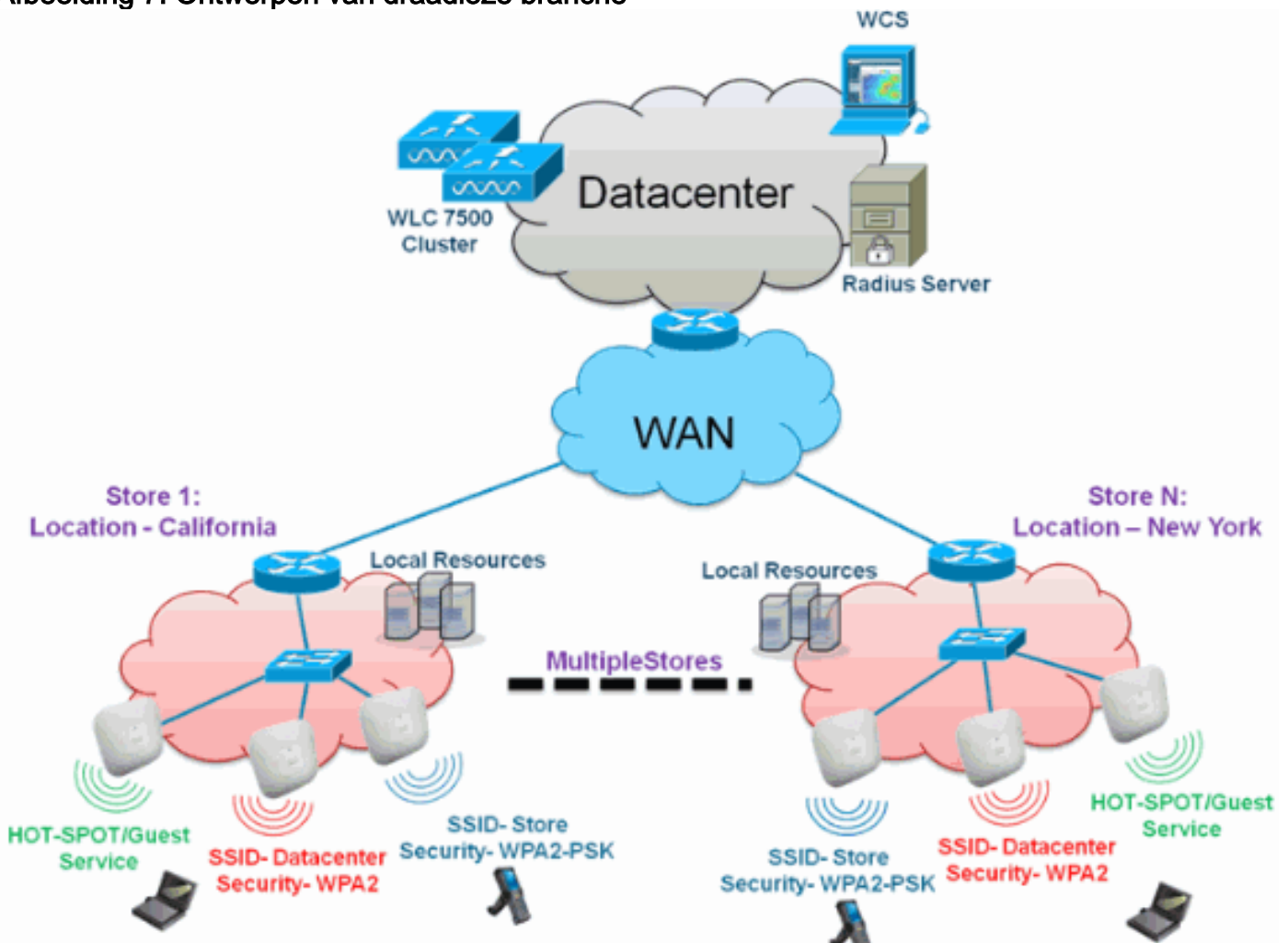
Ontwerpen van draadloze branche

De rest van dit document belicht de richtsnoeren en beschrijft de beste praktijken voor het implementeren van beveiligde gedistribueerde kantorenetten. FlexConnect Architecture wordt aanbevolen voor draadloze kanaalnetwerken die aan deze ontwerpvereisten voldoen.

Primaire ontwerpvereisten

- Vestigingsgrootte die kan worden uitgebreid tot 100 AP's en 250.000 vierkante voet (5.000 vierkante voet). voetjes per AP)
- Centraal beheer en probleemoplossing
- Geen operationele downtime
- Op client gebaseerde verkeerssegmentatie
- Draadloze mobiele verbindingen zonder afstanden en zonder beveiliging tegen bedrijfsmiddelen
- PCI-compatibel
- Steun voor gasten

Afbeelding 7: Ontwerpen van draadloze branche



Overzicht

Vestigingsklanten vinden het steeds moeilijker en duurder om volledig opgetuigde schaalbare en beveiligde netwerkdiensten op geografische locaties aan te bieden. Om klanten te ondersteunen, pakt Cisco deze uitdagingen aan door de Flex 7500 te introduceren.

De Flex 7500-oplossing virtualiseert de complexe security, beheer, configuraties en probleemoplossing binnen het datacenter en breidt deze services vervolgens op transparante wijze uit naar elke tak. Dankzij Flex 7500-implementaties kan de IT gemakkelijker worden opgezet, beheerd en, nog belangrijker, geschaald.

Voordelen

- Verhoogde schaalbaarheid met ondersteuning van 6000 AP
- Verhoogde veerkracht met FlexConnect fouttolerantie
- Verhoogde segmentatie van verkeer met FlexConnect (Central en Local Switching)
- Kunt u beheer vereenvoudigen door opslagontwerpen te kopiëren met AP-groepen en FlexConnect-groepen.

Functies voor adressering van vestigingsnetwerkontwerp

De rest van de secties in het gebruik van de geleidingsopnamefunctie en aanbevelingen om het netwerkontwerp te realiseren dat in [afbeelding 7](#) wordt getoond.

Functies:

Primaire functies	markeren
AP-groepen	Verstrekt operationeel/beheer gemak bij de behandeling van meerdere filiaalplaatsen. Geeft ook de flexibiliteit van het repliceren van configuraties voor gelijksoortige filialen.
FlexConnect-groepen	FlexConnect-groepen bieden de functionaliteit van lokale back-upstraat, CCKM/OKC snelle roaming en lokale verificatie.
Tolerantie fout	Verbeterd de draadloze veerkracht van de tak en verstrekt geen operationele downtime.
ELM (uitgebreide lokale modus voor adaptieve WIPS)	Geef adaptieve WIPS-functionaliteit wanneer u klanten bedient zonder enig effect op clientprestaties.
Clientlimiet per WLAN	Beperking van het totaal aantal gastklanten op branchenetwerk.
AP pre-image downloaden	Vermindert downtime bij het verbeteren van uw tak.
Automatische conversie van AP's in FlexConnect	Functionaliteit om AP's automatisch te converteren in FlexConnect voor uw tak.
Gast Access	Ga door naar bestaande Cisco's Gast Access Architecture met FlexConnect.

IPv6-ondersteuningsmatrix

Functies	Centraal switched		Plaatselijk switched	
	5500 / WIS M-2	Flex 7500	5500 / WiSM-2	Flex 7500
IPv6 (clientmobiliteit)	Ondersteund	Niet ondersteund	Niet ondersteund	Niet ondersteund
IPv6-RA	Ondersteund	Ondersteund	Ondersteund	Ondersteund
IPv6 DHCP-bewaking	Ondersteund	Niet ondersteund	Niet ondersteund	Niet ondersteund
IPv6-bronbewaking	Ondersteund	Niet ondersteund	Niet ondersteund	Niet ondersteund
RA trotting / snelheidsbeperking	Ondersteund	Niet ondersteund	Niet ondersteund	Niet ondersteund
IPv6 ACL	Ondersteund	Niet ondersteund	Niet ondersteund	Niet ondersteund
IPv6-clientzichtbaarheid	Ondersteund	Niet ondersteund	Niet ondersteund	Niet ondersteund
IPv6-buurtontdekking	Ondersteund	Niet ondersteund	Niet ondersteund	Niet ondersteund
IPv6-overbrugging	Ondersteund	Niet ondersteund	Ondersteund	Ondersteund

Funciematrix

Raadpleeg [FlexConnect-functiekaart](#) voor een functiekaart voor de FlexConnect-functie.

AP-groepen

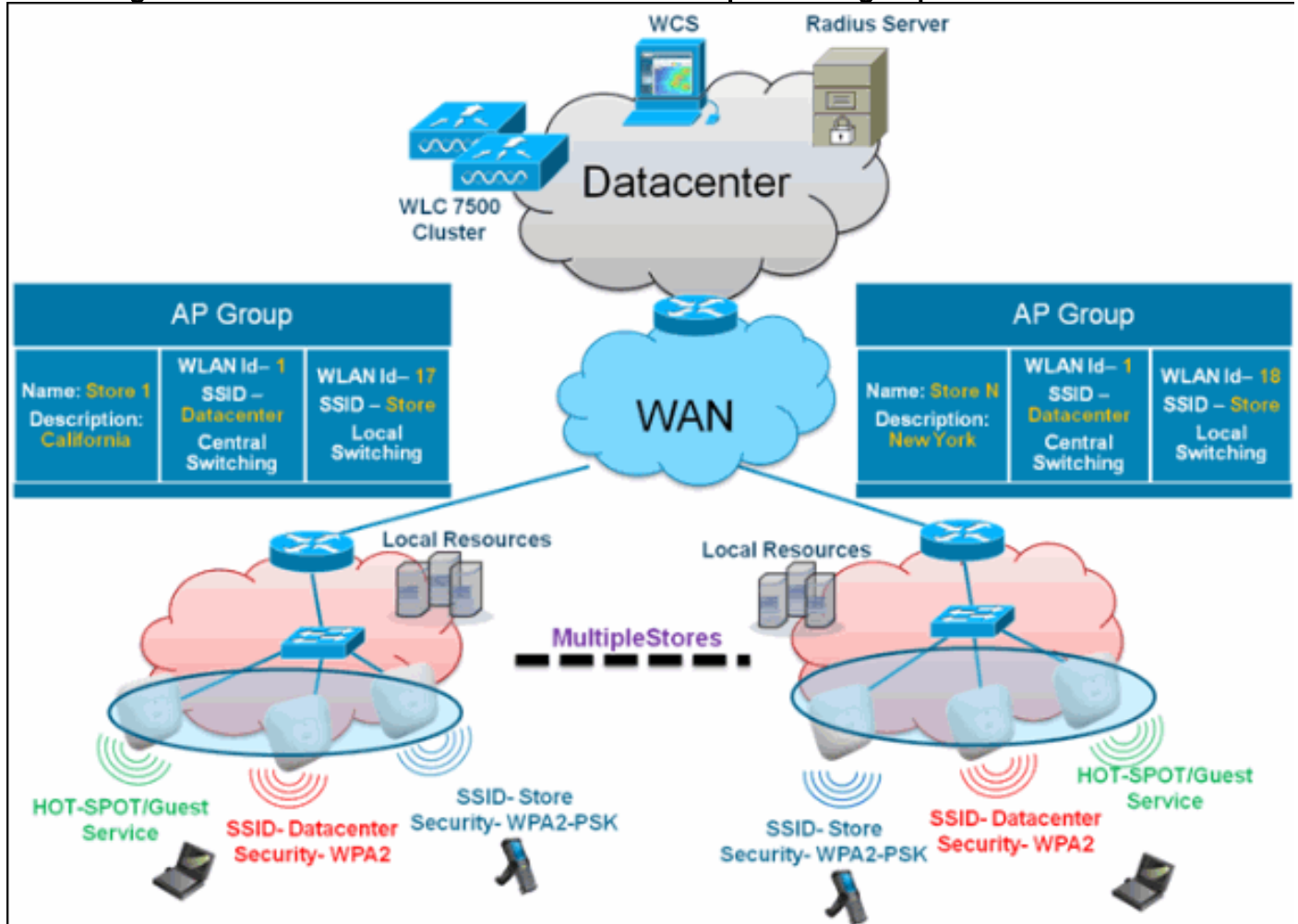
Nadat u WLAN's op de controller hebt gemaakt, kunt u deze selectief publiceren (met behulp van access point groepen) naar verschillende access points om uw draadloos netwerk beter te beheren. Bij een standaardimplementatie worden alle gebruikers op een WLAN-kaart in kaart gebracht aan één interface op de controller. Daarom zijn alle gebruikers die bij dat WLAN zijn aangesloten op dezelfde subnetwork of VLAN. U kunt er echter voor kiezen om de lading op verschillende interfaces of op een groep gebruikers te verdelen op basis van specifieke criteria zoals individuele afdelingen (zoals marketing, engineering of bewerkingen) door groepen access points te creëren. Daarnaast kunnen deze groepen access points in afzonderlijke VLAN's worden

geconfigureerd om netwerkbeheer te vereenvoudigen.

Dit document gebruikt AP groepen om netwerkbeheer te vereenvoudigen wanneer het beheer van meerdere winkels over geografische locaties plaatsvindt. Voor operationeel gemak maakt het document één AP-groep per winkel om aan deze vereisten te voldoen:

- Centraal Switched SSID **Datacenter** over alle winkels voor administratieve toegang tot Local Store Manager.
- Plaatselijk switched SSID **Store** met verschillende WAP2-PSK-toetsen in alle winkels voor Handheld-scanners.

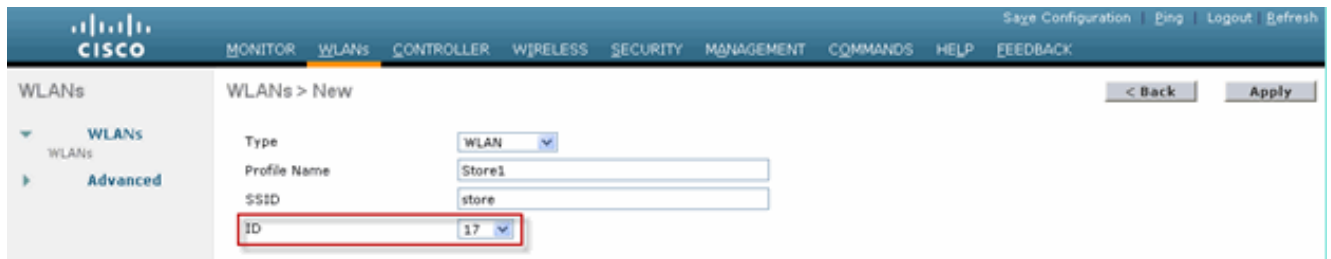
Afbeelding 8: Referentie voor draadloos netwerk ontwerp met AP-groepen



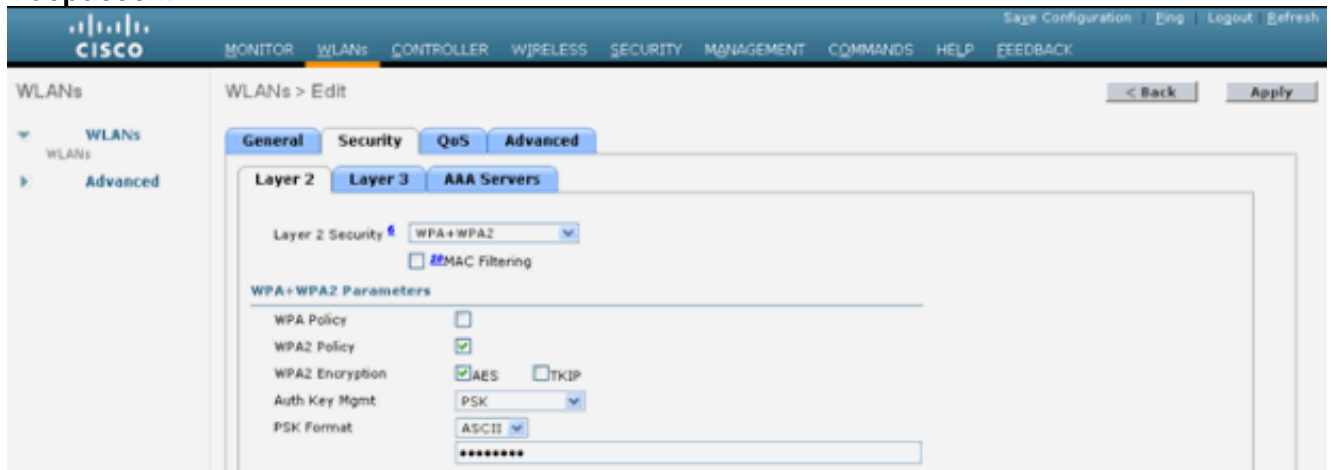
Configuraties van WLC

Voer de volgende stappen uit:

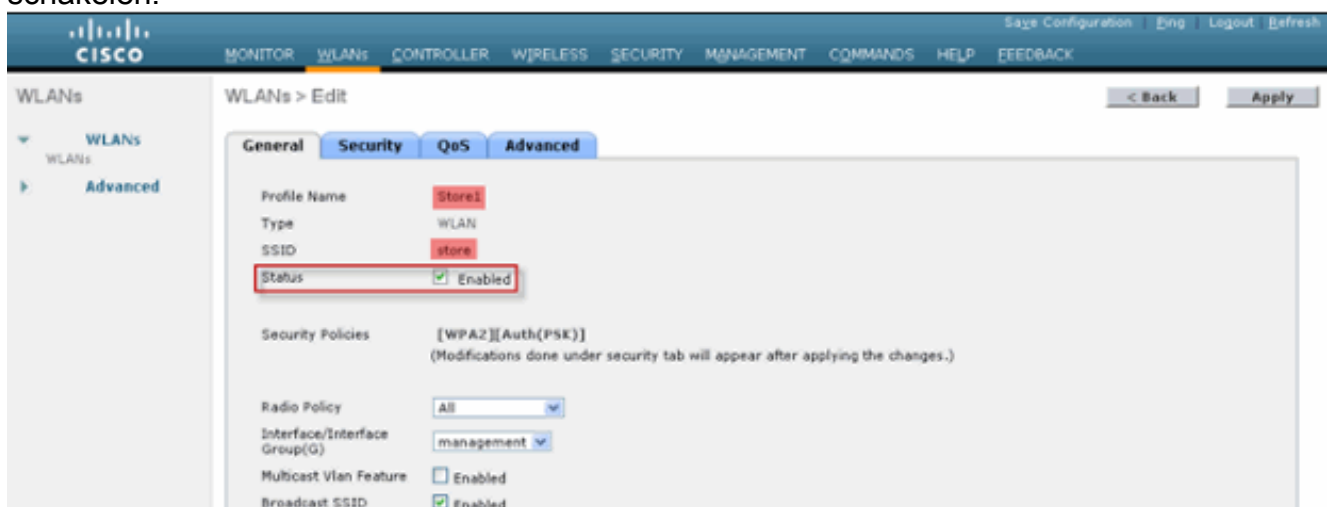
1. Op de WLAN's > Nieuwe pagina voert u **Store1** in het veld Profile Name in, voert u **winkel** in het SSID-veld in en kiest u **17** uit de vervolgkeuzelijst ID. **Opmerking:** WLAN-id's 1-16 maken deel uit van de standaardgroep en kunnen niet worden verwijderd. Om aan onze eis te voldoen om dezelfde SSID-winkel per winkel met een ander WAP2-PSK te gebruiken, moet u WLAN-id 17 en daarna gebruiken omdat deze geen deel uitmaken van de standaardgroep en tot elke winkel kunnen worden beperkt.



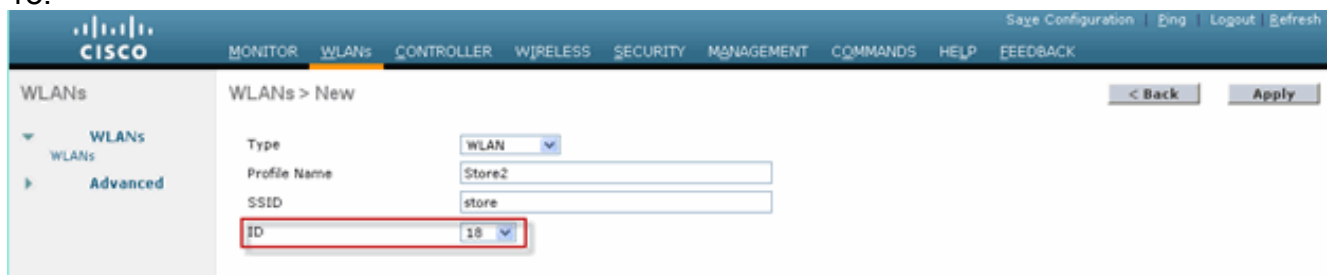
2. Kies onder WLAN > Security PSK uit de vervolgkeuzelijst Auth Key Mgmt, kies ASCII van de vervolgkeuzelijst PSK Format en klik op **Toepassen**.

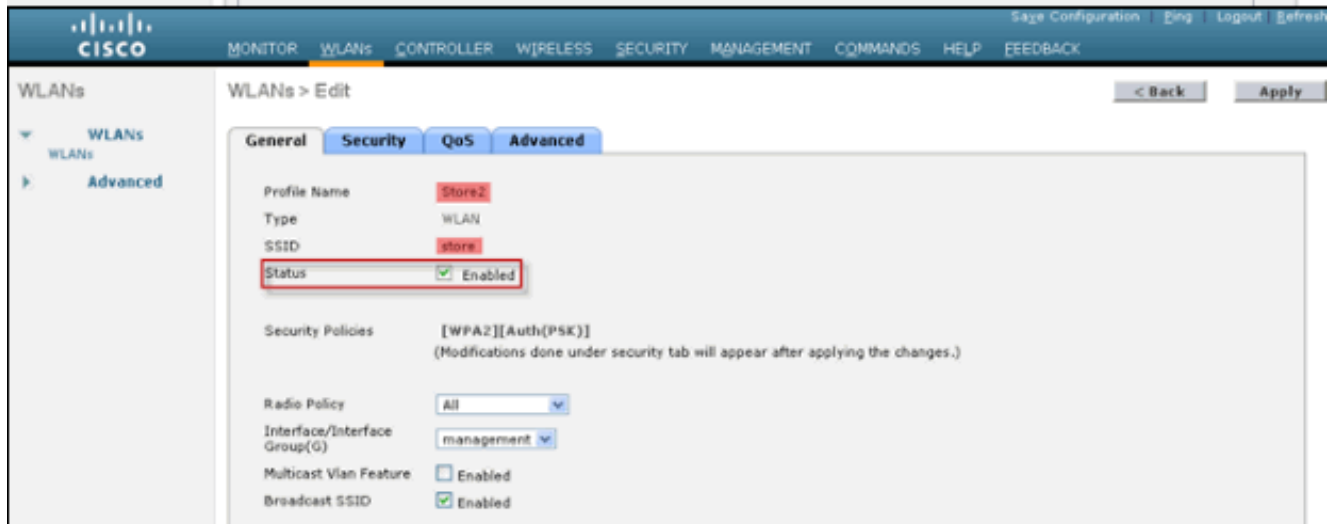
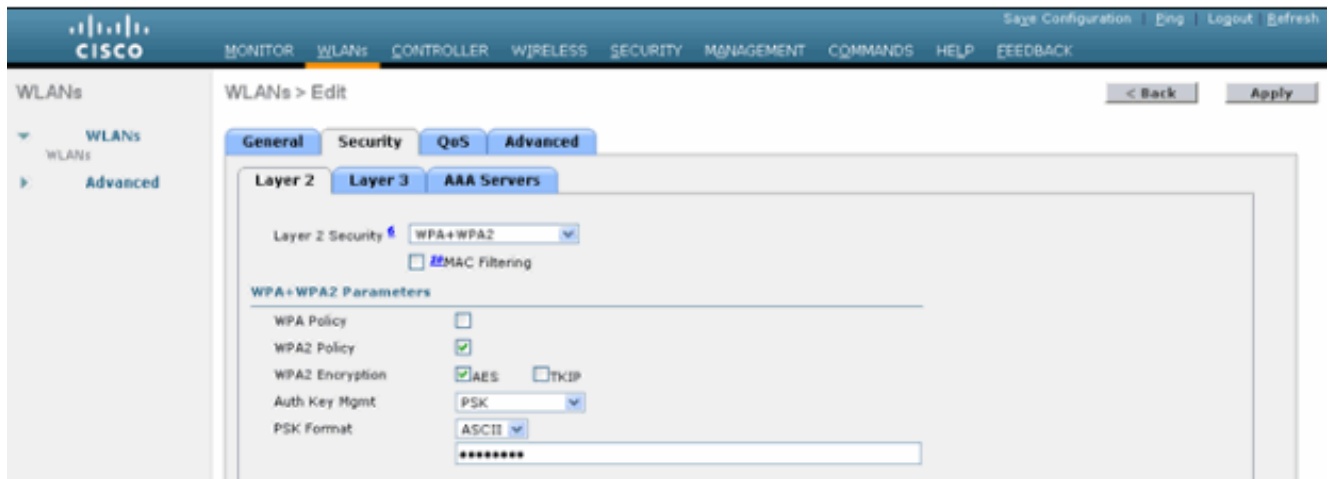


3. Klik op **WLAN > Algemeen**, controleer het beveiligingsbeleid en controleer het **statusvenster** om de WLAN in te schakelen.



4. Herhaal stappen 1, 2 en 3 voor het nieuwe WLAN-profiel **Store2**, met SSID **Store** en ID 18.

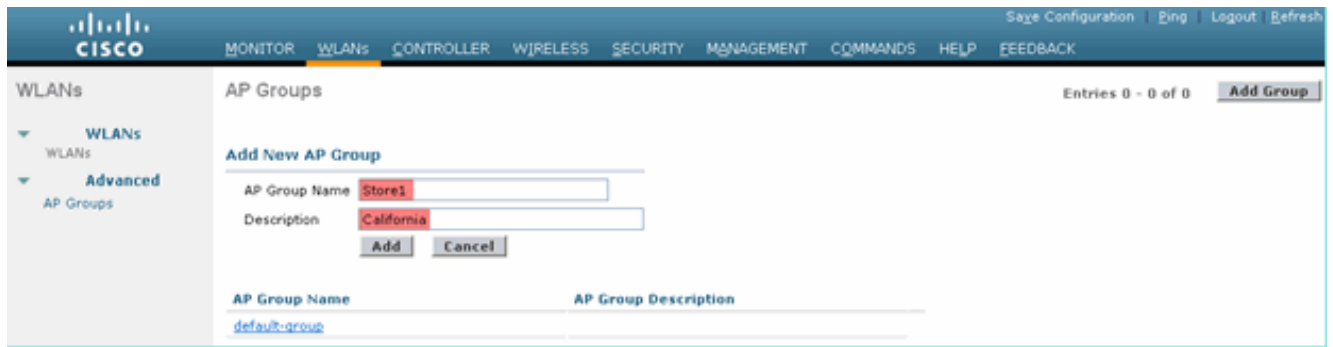




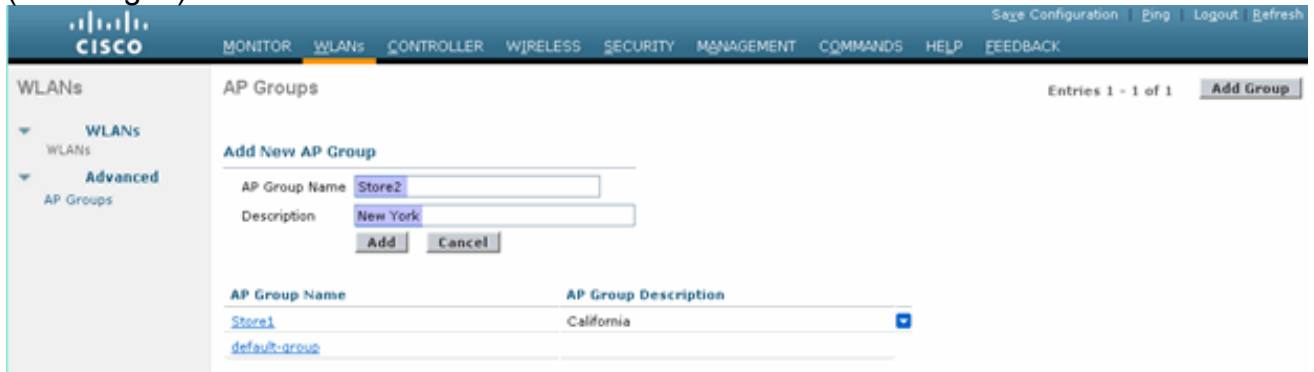
5. Maak en schakel het WLAN-profiel met **DataCenter** van de profiel, SSID **DataCenter** en ID 1 in. **Opmerking:** Bij het maken van deze programma's worden WLAN-id's van 1-16 automatisch onderdeel van de standaard-ap-groep.
6. Controleer onder WLAN de status van WLAN-id's 1, 17 en 18.



7. Klik op **WLAN > Geavanceerd > AP-groep > Add Group**.
8. Voeg AP Group Name **Store1** toe, zoals WLAN-profiel **Store1** en Description toe als locatie van de Store. In dit voorbeeld wordt Californië gebruikt als de locatie van de winkel.
9. Klik op **Toevoegen** als u klaar bent.



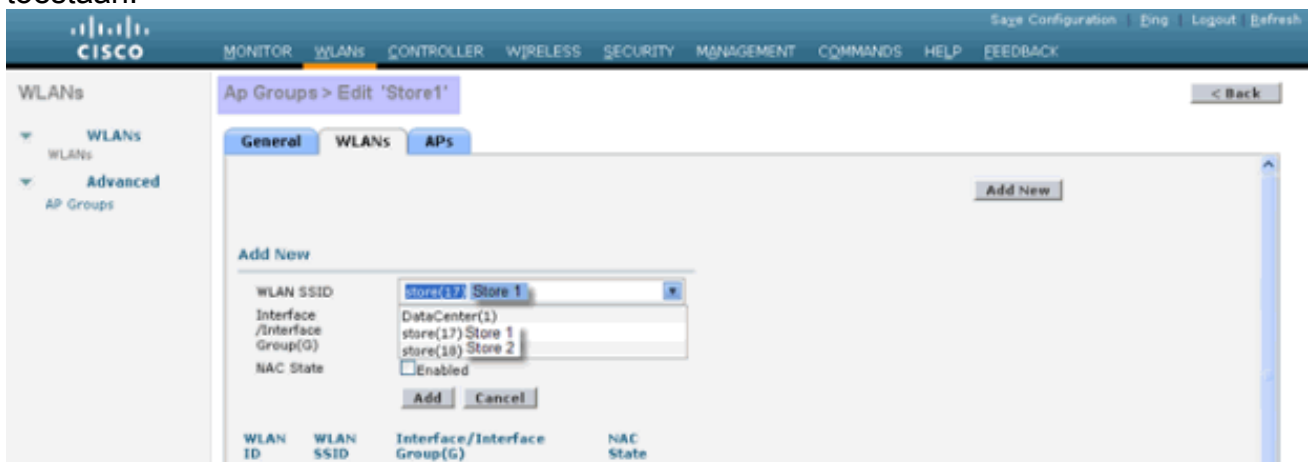
10. Klik op **Add Group** en selecteer AP Group Name **Store2** en Description New York.
11. Klik op **Add** (Toevoegen).



12. Controleer de groepscreatie door op **WLAN > Geavanceerd > AP-groepen** te klikken.



13. Klik op AP Group Name **Store1** om de WLAN toe te voegen of te bewerken.
14. Klik op **Add New** om de WLAN te selecteren.
15. Kies onder WLAN, vanuit de vervolgkeuzelijst WLAN SSID, **WLAN ID 17-winkel(17)**.
16. Klik op **Add** nadat WLAN-id 17 is geselecteerd.
17. Herhaal stappen 14-16 voor WLAN-id 1 DataCenter(1). Deze stap is alleen optioneel en alleen nodig als u toegang tot Remote Resource wilt toestaan.

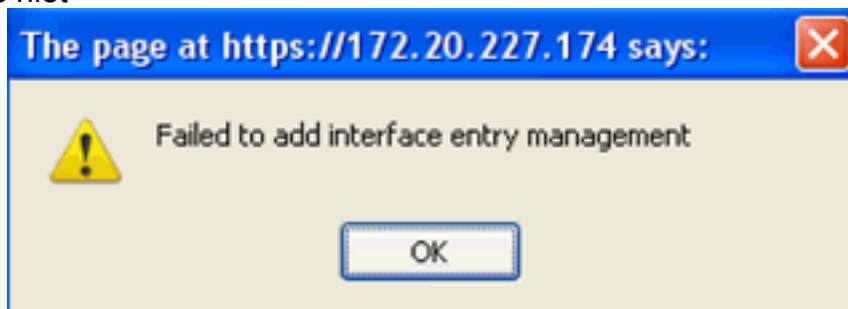


18. Ga terug naar het **WLAN > Geavanceerd > AP Groepen** scherm.
19. Klik op AP Group Name **Store2** om WLAN toe te voegen of te bewerken.

20. Klik op **Add New** om de WLAN te selecteren.
21. Kies onder WLAN, vanuit WLAN-vervolgkeuzelijst **WLAN ID 18-winkel (18)**.
22. Klik op **Add** nadat WLAN-id 18 is geselecteerd.
23. Herhaal stappen 14-16 voor WLAN-id 1
DataCenter(1).



Opmerking: Het toevoegen van meerdere WLAN-profielen met dezelfde SSID onder één AP-groep is niet



toegestaan.

Opmerking: het toevoegen van APs aan de APgroep wordt niet opgenomen in dit document, maar het is nodig voor klanten om tot netwerkdiensten toegang te hebben.

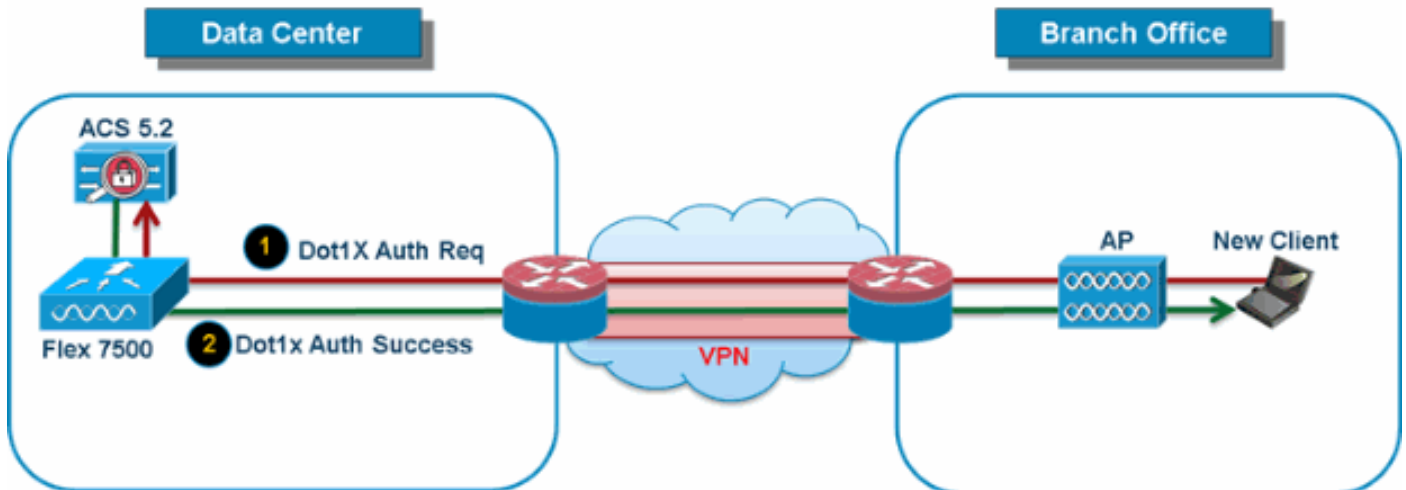
Samenvatting

- AP groepen vereenvoudigen netwerkbeheer.
- Problemen oplossen met granulariteit per bedrijfstak
- Verhoogde flexibiliteit

FlexConnect-groepen

Afbeelding 9: Central Dot1X-verificatie (Flex 7500 fungeren als verificator)

Central Authentication – Flex 7500 Authenticator



Bij de meeste typische implementaties in de branche is het gemakkelijk te voorspellen dat client 802.1X-verificatie centraal plaatsvindt in het datacenter zoals in [afbeelding 9](#) is aangetoond. Omdat het bovenstaande scenario volledig geldig is, roept het deze bezorgdheid op:

- Hoe kunnen draadloze klanten 802.1X authenticatie en toegang datacenter diensten uitvoeren als Flex 7500 mislukt?
- Hoe kunnen draadloze klanten 802.1X authenticatie uitvoeren als WAN-verbinding tussen Branch en Data Center mislukt?
- Is er enig effect op de mobiliteit van de kantoren tijdens de mislukkingen van WAN?
- Biedt de FlexConnect-oplossing geen operationele downtime aan?

FlexConnect Group is primair ontworpen en dient te worden opgericht om deze uitdagingen het hoofd te bieden. Daarnaast is het eenvoudiger om elke website van de tak te organiseren, omdat alle FlexConnect access points van elke website deel uitmaken van één FlexConnect Group.

Opmerking: FlexConnect-groepen zijn niet analoog aan AP-groepen.

Primaire doelstellingen van FlexConnect-groepen

Reserve RADIUS-serverfailover

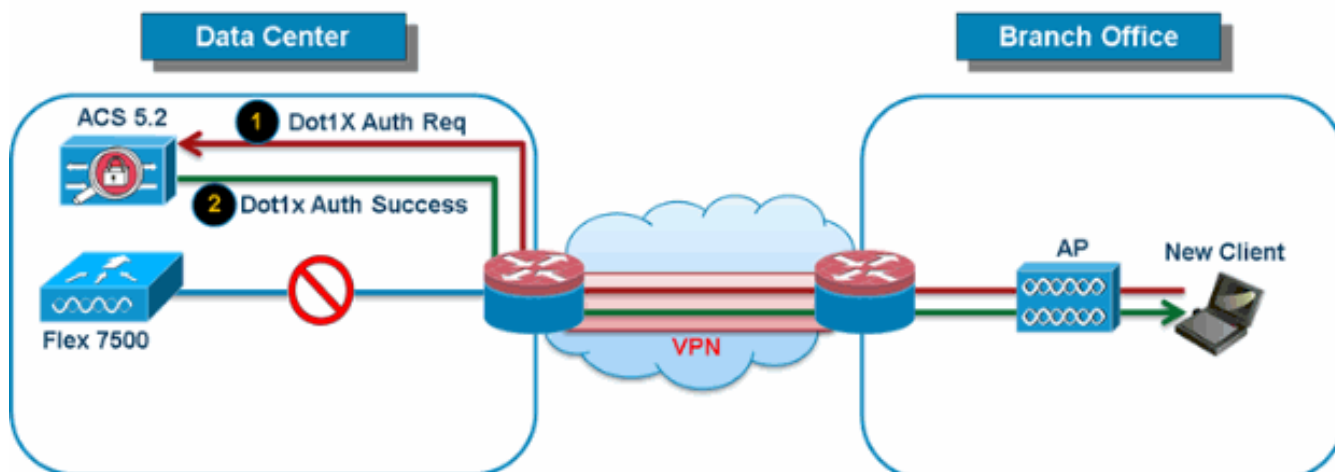
- U kunt de controller configureren zodat een FlexConnect-access point in de standalone modus volledig 802.1X-verificatie kan uitvoeren op een RADIUS-server met back-up. Om de veerkracht van de tak te vergroten, kunnen de beheerders een primaire RADIUS-server of zowel een primaire als secundaire RADIUS-server configureren. Deze servers worden alleen gebruikt wanneer het FlexConnect-access point niet is aangesloten op de controller.

Opmerking: Accounting van back-up RADIUS wordt niet ondersteund.

Lokale verificatie

- Voordat de 7.0.98.0-coderelease werd uitgevoerd, werd lokale verificatie alleen ondersteund wanneer FlexConnect in standalone modus is zodat client-connectiviteit niet wordt beïnvloed tijdens WAN-link. Deze functie wordt nu ondersteund met de release 7.0.16.0, ook wanneer FlexConnect-access points in Connected Mode zijn. **Afbeelding 10: Central Dot1X-verificatie (FlexConnect APs Acting as Authenticator)**

Central Authentication – AP Authenticator

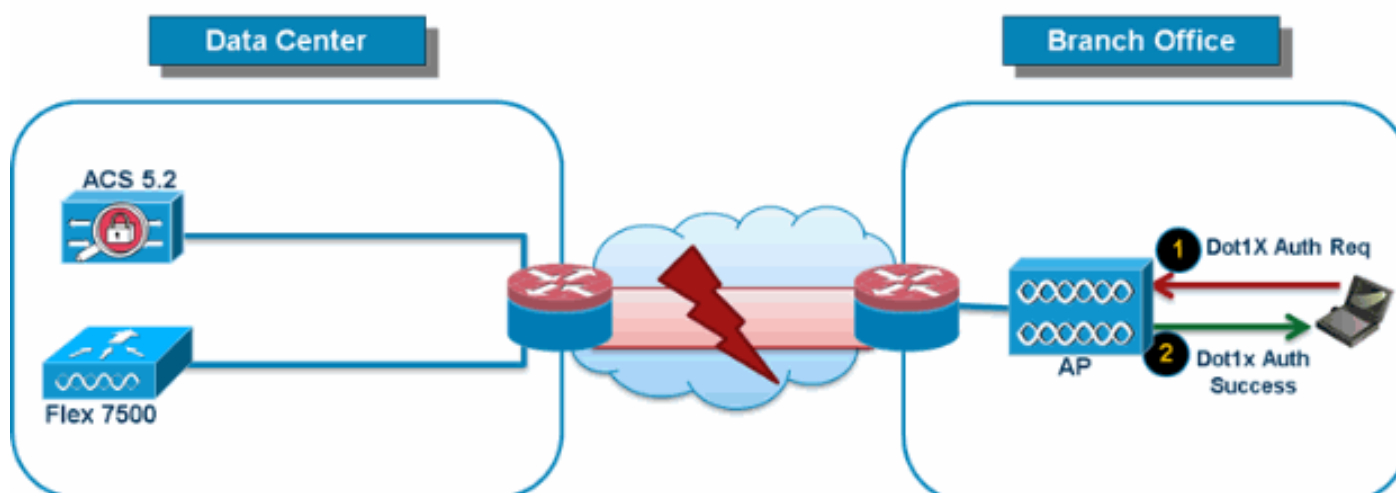


Zoals in [afbeelding 10](#) wordt getoond, kunnen filiaalklanten 802.1X verificatie blijven uitvoeren wanneer FlexConnect Branch APs connectiviteit met Flex 7500 verliezen. Zolang de RADIUS/ACS server bereikbaar is vanaf de Vestigingsite, zullen draadloze klanten draadloze services blijven authenticeren en benaderen. Met andere woorden, als RADIUS/ACS binnen de Vestiging gevestigd is, zullen de cliënten draadloze services zelfs tijdens een WAN-uitgang authenticeren en benaderen. **Opmerking:** Deze optie kan worden gebruikt in combinatie met de FlexConnect RADIUS-serverfunctie. Als een FlexConnect Group is geconfigureerd met zowel een RADIUS-server als een lokale verificatie, probeert het FlexConnect-access point altijd cliënten te authenticeren met eerst de primaire RADIUS-server, gevolgd door de secundaire RADIUS-server (indien de primaire RADIUS-server niet bereikbaar is) en uiteindelijk de lokale EAP-server op FlexConnect-toegangspunt zelf (indien de primaire en secundaire RADIUS niet bereikbaar zijn).

Plaatselijke MAP (lokale verificatievoortzetting)

Afbeelding 11: Dot1X-verificatie (FlexConnect APs Acting as Local-EAP Server)

Local Branch Authentication – AP as Radius Server



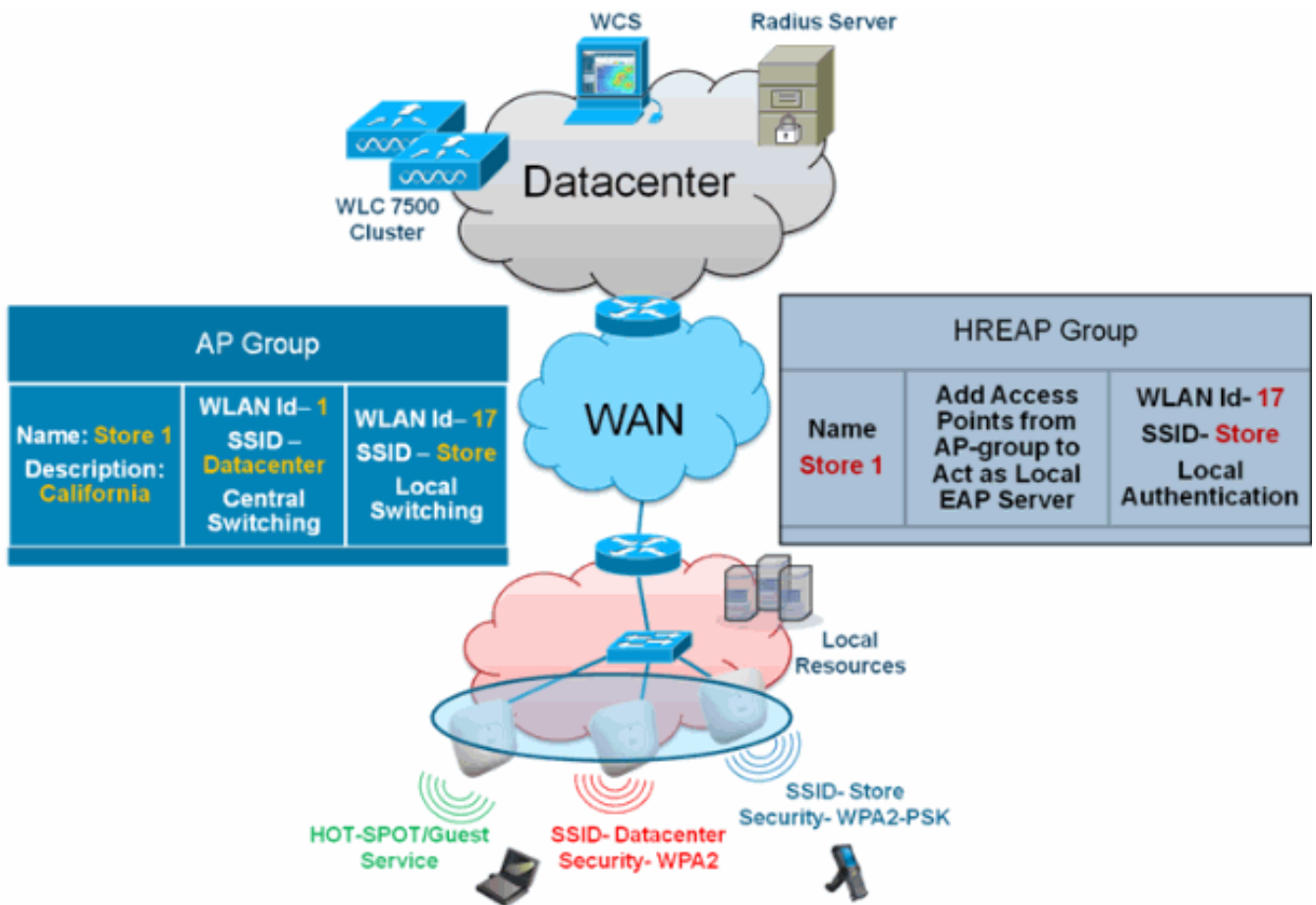
- U kunt de controller configureren zodat een FlexConnect-AP in een standalone of verbonden modus kan worden uitgevoerd voor LEAP of EAP-FAST-verificatie voor maximaal 100 statistisch gedefinieerde gebruikers. De controller stuurt de statische lijst met gebruikersnamen en wachtwoorden naar elk FlexConnect-access point van die specifieke

FlexConnect-groep wanneer deze zich bij de controller voegt. Elk toegangspunt in de groep authenticereert alleen de eigen verbonden klanten.

- Deze optie is ideaal voor klanten die van een autonoom netwerk van toegangspunten naar een lichtgewicht FlexConnect-toegangsnetwerk migreren en niet geïnteresseerd zijn in het onderhouden van een grote gebruikersdatabase of het toevoegen van een ander hardwareapparaat om de RADIUS-serverfunctionaliteit te vervangen die beschikbaar is in het autonome access point.
- Zoals in [afbeelding 11](#) wordt getoond, als de RADIUS/ACS-server binnen het datacenter niet bereikbaar is, dan fungeert FlexConnect APs automatisch als een Local-EAP Server om Dot1X-verificatie uit te voeren voor draadloze filiaalklanten.

CCKM/OKC snelle roaming

- FlexConnect-groepen zijn vereist voor CCKM/OKC snelle roaming om te kunnen werken met FlexConnect-access points. Snel roaming wordt bereikt door een derivaat van de hoofdtoets te casten van een volledige MAP-verificatie, zodat een eenvoudige en veilige belangrijke uitwisseling kan plaatsvinden wanneer een draadloze klant naar een ander toegangspunt beweegt. Deze optie voorkomt de noodzaak om een volledige MAP-verificatie van RADIUS uit te voeren omdat de client van het ene toegangspunt naar het andere stroomt. De FlexConnect-access points moeten de CCKM/OKC cache-informatie verkrijgen voor alle klanten die er mogelijk bij betrokken zijn, zodat zij deze snel kunnen verwerken in plaats van het terug te sturen naar de controller. Als je bijvoorbeeld een controller hebt met 300 access points en 100 klanten die zouden kunnen associëren, is het versturen van de CCKM/OKC cache voor alle 100 klanten niet praktisch. Als u een FlexConnect Group creëert die een beperkt aantal access points omvat (bijvoorbeeld, u creëert een groep voor vier access points in een extern kantoor), roemen de clients alleen tussen die vier access points en wordt het CCKM/OKC cache alleen verdeeld onder die vier access points wanneer de klanten met een van hen geassocieerd worden.
- Deze optie zorgt samen met Backup Radius en Local Authentication (Local-EAP) voor **geen operationele downtime** voor uw filiaalsites. **Opmerking:** CCKM/OKC fast roaming tussen FlexConnect en non-FlexConnect access points wordt niet ondersteund. **Afbeelding 12: Referentie voor draadloos netwerk ontwerp met FlexConnect-groepen**



[FlexConnect Group Configuration via WLC](#)

Voltooi de stappen in dit gedeelte om FlexConnect-groepen te configureren ter ondersteuning van lokale verificatie met LEAP, wanneer FlexConnect wordt aangesloten of in standalone modus. De configuratiesteekproef in [afbeelding 12](#) illustreert de objectieve verschillen en 1:1-omzetting tussen de AP Group en FlexConnect groep.

1. Klik op **New** onder Wireless > FlexConnect-groepen.
2. Toewijzen Group Name Store 1, vergelijkbaar met de voorbeeldconfiguratie zoals in [afbeelding 12](#).
3. Klik op **Toepassen** wanneer de groepsnaam is ingesteld.

The screenshot shows the Cisco Wireless configuration interface. At the top, there is a navigation bar with the Cisco logo and tabs for MONITOR, WLANs, CONTROLLER, and WIRELESS. The WIRELESS tab is selected. On the left, a sidebar menu is visible under the heading 'Wireless', with options for Access Points, Radios, Advanced, Mesh, RF Profiles, and FlexConnect Groups. The main content area is titled 'FlexConnect Groups > New'. It features a 'Group Name' label followed by a text input field containing the text 'Store 1'.

4. Klik op Group Name **Store 1** dat u voor de volgende configuratie hebt gemaakt.

The screenshot shows the Cisco Wireless configuration interface. At the top, there is a navigation bar with the Cisco logo and tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, and SECURITY. The WIRELESS tab is selected. On the left, a sidebar menu is visible under the heading 'Wireless', with options for Access Points, Radios, Advanced, Mesh, RF Profiles, and FlexConnect Groups. The main content area is titled 'FlexConnect Groups'. It features a 'Group Name' label followed by a dropdown menu with 'Store 1' selected, indicated by a blue downward arrow icon.

5. Klik op **AP toevoegen**.

The screenshot shows the Cisco Wireless configuration page for 'FlexConnect Groups > Edit 'Store 1''. The left sidebar contains a 'Wireless' menu with options like 'Access Points', 'Radios', 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups', and 'FlexConnect ACLs'. The main content area has three tabs: 'General', 'Local Authentication' (which is selected), and 'Image Upgrade'. Under the 'Local Authentication' tab, the 'Group Name' is 'Store 1'. Below this is a section titled 'FlexConnect APs' with an 'Add AP' button. At the bottom, there is a table header with columns for 'AP MAC Address', 'AP Name', and 'Status'.

6. Controleer het vakje **Local Authentication Enable AP** om lokale verificatie in te schakelen wanneer de AP in standalone modus staat. **Opmerking:** Stap 20 toont hoe u Lokale verificatie voor Connected Mode AP kunt inschakelen.
7. Controleer de **Select APs uit het huidige** vakje voor controller om het vervolgkeuzemenu AP Name in te schakelen.
8. Kies AP uit de vervolgkeuzelijst die deel van deze FlexConnect Groep moet uitmaken.
9. Klik op **Toevoegen** nadat de AP uit de vervolgkeuzelijst is geselecteerd.
10. Herhaal stap 7 en 8 om alle APs aan deze FlexConnect groep toe te voegen die ook deel uitmaken van AP-Group Store 1. Zie [afbeelding 12](#) om de 1:1 mapping tussen de AP-Group en FlexConnect groep te begrijpen. Als u een AP-Group per Store hebt gemaakt ([afbeelding 8](#)), dan zouden idealiter alle APs van die AP-Group deel moeten uitmaken van deze FlexConnect Group ([afbeelding 12](#)). Het handhaven van 1:1 verhouding tussen de AP-Group en FlexConnect groep vereenvoudigt netwerkbeheer.

The screenshot displays the Cisco FlexConnect Groups configuration interface. The left sidebar shows the navigation menu with 'FlexConnect Groups' selected. The main content area is titled 'FlexConnect Groups > Edit 'Store 1''. The 'Local Authentication' tab is active. Under the 'FlexConnect APs' section, the 'Add AP' form is visible. It includes a checked checkbox for 'Select APs from current controller', a dropdown menu for 'AP Name' with 'AP3500' selected, and a text input for 'Ethernet MAC' containing '00:22:90:e3:37:df'. There are 'Add' and 'Cancel' buttons below the form. At the bottom, a table header is partially visible with columns for 'AP MAC Address', 'AP Name', and 'Status'.

11. Klik op **Lokale verificatie > Protocollen** en controleer het vakje **LEAP-verificatie** inschakelen.
12. Klik op **Toepassen** nadat het aankruisvakje is ingesteld. **Opmerking:** Als u een reservekopie hebt, zorg er dan voor dat de FlexConnect-groepen identiek zijn en dat de AP MAC-adressen per FlexConnect-groep worden opgenomen.

General **Local Authentication** **Image Upgrade** **VLAN-ACL mapping**

Local Users **Protocols**

LEAP

Enable LEAP Authentication

EAP Fast

Enable EAP Fast Authentication

Server Key (in hex) Enable Auto key generation

.....

.....

Authority ID (in hex) 436973636f00000000000000000000000000000000

Authority Info Cisco_A_ID

PAC Timeout (2 to 4095 days)

13. Klik onder Lokale verificatie op **Lokale gebruikers**.
14. Stel de velden Gebruikersnaam, Wachtwoord en Wachtwoord bevestigen in en klik vervolgens op **Toevoegen** om gebruikersingang te maken in de lokale MAP-server die op de AP gevestigd is.
15. Herhaal stap 13 totdat de lokale gebruikersnaam is uitgeput. U kunt niet meer dan 100 gebruikers configureren of toevoegen.
16. Klik op **Toepassen** nadat stap 14 is voltooid en het aantal gebruikers is geverifieerd.

General **Local Authentication** **Image Upgrade** **VLAN-ACL mapping**

Local Users **Protocols**

Nc of Users 0 **Add User**

User Name

Upload CSV file

File Name

UserName cisco

Password

Confirm Password

Add

17. Klik vanuit het bovenste venster op **WLAN's**.

18. Klik op **WLAN-id 17**. Dit is gemaakt tijdens de creatie van de AP-groep. Zie [afbeelding 8](#).



19. Klik onder WLAN > Bewerken voor WLAN-id 17 op **Advanced**.

20. Controleer het dialoogvenster **FlexConnect Local Audio** om lokale verificatie in Connected Mode in te schakelen. **Opmerking:** Lokale verificatie wordt alleen ondersteund voor FlexConnect met Local Switching. **N.B.:** Zorg er altijd voor dat u de FlexConnect Group maakt voordat u Lokale verificatie onder WLAN

WLANs > Edit 'Store-1'

General	Security	QoS	Advanced
P2P Blocking Action			Disabled
Client Exclusion 3	<input checked="" type="checkbox"/> Enabled		60 Timeout Value (secs)
Maximum Allowed Clients 8			0
Static IP Tunneling 11	<input type="checkbox"/> Enabled		
Wi-Fi Direct Clients Policy			Disabled
Maximum Allowed Clients Per AP Radio			200
Off Channel Scanning Defer			
Scan Defer Priority			0 1 2 3 4 5 6 7
			<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Scan Defer Time (msecs)			100
FlexConnect			
FlexConnect Local Switching 2	<input checked="" type="checkbox"/> Enabled		
FlexConnect Local Auth 12	<input checked="" type="checkbox"/> Enabled		
Learn Client IP Address 5	<input checked="" type="checkbox"/> Enabled		

toestaat.

NCS biedt ook het selectieteken FlexConnect Local Auth aan om lokale verificatie in Connected Mode zoals hieronder wordt getoond, mogelijk te maken:

Properties > System > **WLANs** > WLAN Configuration > AP Groups > FlexConnect > Security > Access Points > 802.11 > 802.11a/n > 802.11b/g/n > Mesh > Ports > Management > Location

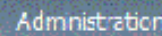
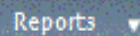
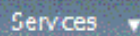
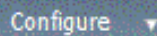
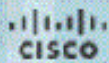
WLAN Configuration Details : 1

Configure > Controllers > [redacted] > WLANs > WLAN Configuration :

General Security QoS **Advanced**

HexConnect Local Switching	<input checked="" type="checkbox"/>	Enable
FlexConnect Local Auth ⓘ	<input checked="" type="checkbox"/>	Enable
Learn Client IP Address	<input checked="" type="checkbox"/>	Enable
Session Timeout	<input type="checkbox"/>	Enable
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enable
Aironet IE	<input checked="" type="checkbox"/>	Enable
IPv6 ⓘ	<input type="checkbox"/>	Enable
Diagnostic Channel ⓘ	<input type="checkbox"/>	Enable
Override Interface ACL	IPv4	NONE
Peer to Peer Blocking ⓘ		Disable
Wi-Fi Direct Clients Policy		Disabled
Client Exclusion ⓘ	<input checked="" type="checkbox"/>	Enable
Timeout Value		60 (secs)

NCS biedt ook een voorziening om FlexConnect lokaal geauthenticeerde klanten te filteren en te controleren zoals hier wordt getoond:



Clients and Users



Refresh



Test



Useful



Remove



More



Track Clients



Identify Unknown Users

	MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name
<input type="radio"/>	00:22:90:1b:17:42		IPv4	Unknown		Cisco	WCS_SW-0.1.0.22
<input type="radio"/>	1c:df:0f:66:86:50		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:21:6e:97:9b:bc		IPv4	husl/vikal...		Intel	oeap-ta-war-2
<input type="radio"/>	00:22:90:1b:96:48		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:22:90:1b:17:8c		IPv4	Unknown		Cisco	WCS_SW-0.1.0.22
<input type="radio"/>	00:25:0b:4d:77:c4		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	c4:7d:4f:3a:c5:d5		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:21:a0:d5:03:c4		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	f3:66:f2:67:7f:50		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:17:ca:bc:d1:b4		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	88:43:e1:d1:df:02		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:22:bd:1b:e2:b5		IPv4	Unknown		Cisco	WCS_SW-0.1.0.22
<input type="radio"/>	f3:66:f2:ab:1e:69		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:1c:58:d1:b4:4e		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:1e:7a:0b:21:8d		IPv4	ssimm		Cisco	oeap-ta-war-2

Virtual Domain: ROOT-DOMAIN root ▼ Log Out 🔍

Total 299

Location	VLAN	Status	Interface
Unknown	109	Associated	Gi1/0/34
Unknown	109	Associated	Gi1/0/26
Root Area	310	Associated	data
Unknown	109	Associated	Gi1/0/36
Unknown	109	Associated	Gi1/0/32
Unknown	109	Associated	Gi1/0/30
Unknown	109	Associated	Gi1/0/13
Unknown	109	Associated	Gi1/0/27
Unknown	109	Associated	Gi1/0/12
Unknown	109	Associated	Gi1/0/15
Unknown	109	Associated	Gi1/0/28
Unknown	109	Associated	Gi1/0/14
Unknown	109	Associated	Gi1/0/9
Unknown	109	Associated	Gi1/0/29
Root Area	311	Associated	voice

Associated Clients

- Quick Filter
- Advanced Filter
- All
- Manage Preset Filters
- 2.4GHz Clients
- 5GHz Clients
- All Lightweight Clients
- All Autonomous Clients
- All Wired Clients
- Associated Clients
- Clients known by ISE
- Clients detected by MSE
- Clients detected in the last 24 hours
- Clients with Problems
- Excluded Clients
- FlexConnect Locally Authenticated
- New clients detected in last 24 hours
- On Network Clients

Verificatie met CLI

Clientverificatiestatus en -switchmodus kunnen snel worden geverifieerd met behulp van deze CLI op de WLC:

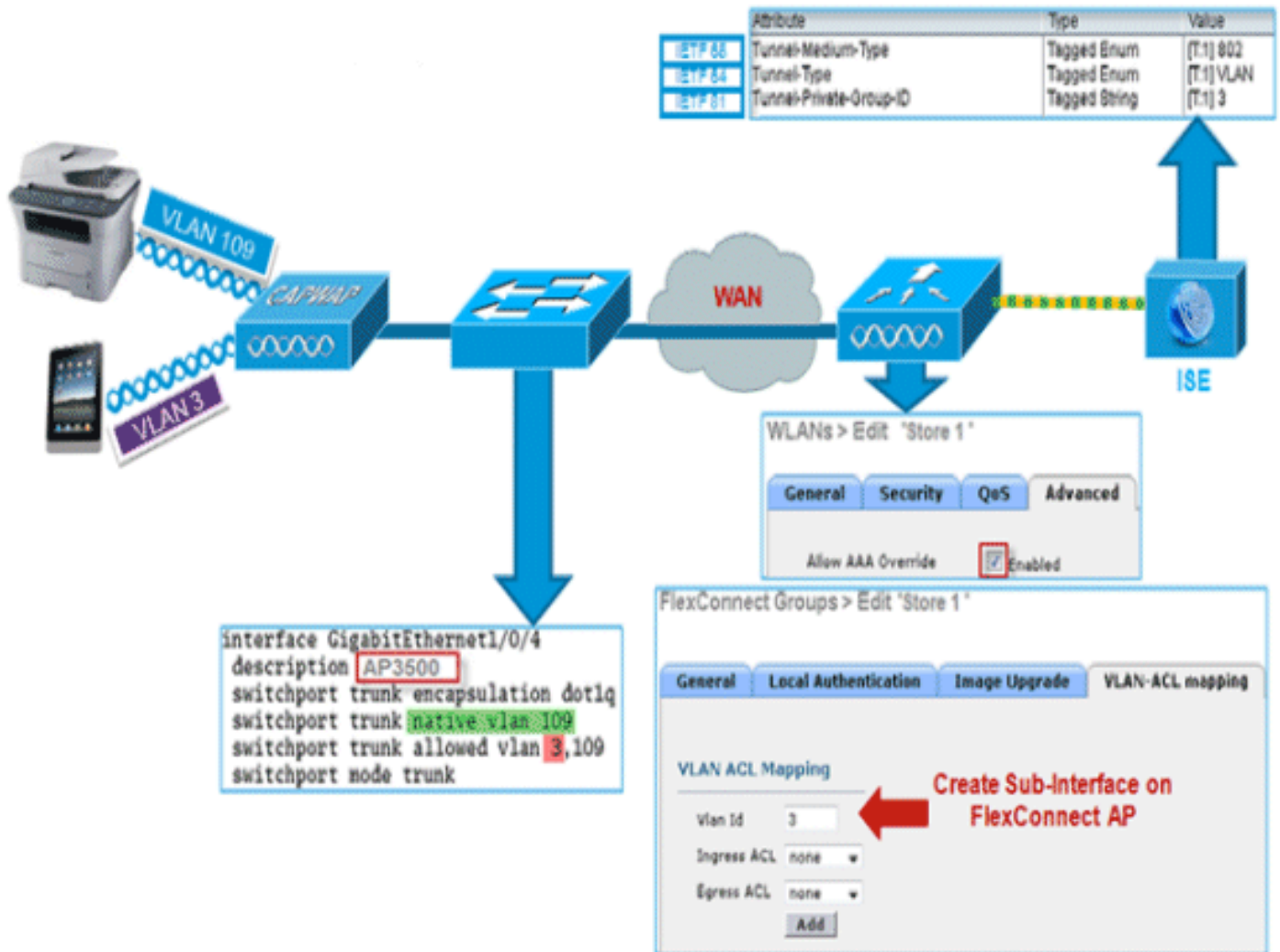
```
(Cisco Controller) >show client detail 00:24:d7:2b:7c:0c
Client MAC Address..... 00:24:d7:2b:7c:0c
Client Username ..... N/A
AP MAC Address..... d0:57:4c:08:e6:70
Client State..... Associated
H-REAP Data Switching..... Local
H-REAP Authentication..... Local
```

FlexConnect VLAN-override

In de huidige FlexConnect-architectuur is er een strikte mapping van WLAN naar VLAN's, en dus moet de client die wordt gekoppeld aan een bepaalde WLAN op FlexConnect AP zich houden aan

een VLAN dat er aan wordt gekoppeld. Deze methode heeft beperkingen, omdat het van cliënten vereist om met verschillende SSIDs te associëren om verschillend VLAN-gebaseerd beleid te erven.

Vanaf release 7.2 wordt AAA-opheffing van VLAN op individueel WLAN geconfigureerd voor lokale switching ondersteund. Om dynamische VLAN-toewijzing te hebben, zou AP de interfaces voor het VLAN vooraf gemaakt hebben op basis van een configuratie met bestaande WLAN-VLAN Toewijzing voor individuele FlexConnect AP of het gebruik van ACL-VLAN-mapping op een FlexConnect groep. De WLC wordt gebruikt om de subinterfaces aan te maken op de AP.



Samenvatting

- AAA VLAN-Override wordt ondersteund door release 7.2 voor WLAN's die zijn geconfigureerd voor lokale switching in centrale en lokale verificatiemodus.
- AAA-voorrang dient te worden ingeschakeld op WLAN dat voor lokale switching is geconfigureerd.
- FlexConnect AP moet VLAN hebben dat van WLC voor dynamische VLAN-toewijzing is gemaakt.
- Als VLAN's die door AAA zijn geretourneerd niet aanwezig zijn op een AP-client, krijgt u een IP vanuit de standaard VLAN-interface van AP.

Procedure

Voer de volgende stappen uit:

1. Maak een WLAN voor 802.1x-
verificatie.

The screenshot shows the 'WLANs > Edit 'Store 1'' configuration page. The 'Security' tab is selected, and the 'Layer 3' sub-tab is active. Under 'Layer 2 Security', 'WPA+WPA2' is selected in the dropdown menu, and 'MAC Filtering' is unchecked. The 'WPA+WPA2 Parameters' section is expanded, and a red box highlights the following settings: 'WPA Policy' is unchecked; 'WPA2 Policy' is checked; 'WPA2 Encryption' has 'AES' checked and 'TKIP' unchecked; 'Auth Key Mgmt' is set to '802.1X' in the dropdown; and 'WPA gtk-randomize State' is set to 'Disable' in the dropdown.

2. Ondersteuning van AAA inschakelen voor lokale WLAN-switching op de WLC Navigeer naar **WLAN GUI > WLAN > WLAN-id > Advance** tab.

WLANs > Edit 'Store 1'

General **Security** **QoS** **Advanced**

Allow AAA Override Enabled

Coverage Hole Detection Enabled

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 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

Off Channel Scanning Defer

Scan Defer Priority	0	1	2	3	4	5	6	7
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Scan Defer Time (msecs): 100

FlexConnect

FlexConnect Local Switching Enabled

DHCP

DHCP Server Override

DHCP Addr. Assignment Required

Management Frame Protection (MFP)

MFP Client Protection: Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255): 1

802.11b/g/n (1 - 255): 1

NAC

NAC State: None

Load Balancing and Band Select

Client Load Balancing

Client Band Select

Passive Client

Passive Client

Voice

Media Session Snooping Enabled

Re-anchor Roamed Voice Clients Enabled

KTS based CAC Policy Enabled

3. Voeg de AAA server details toe op de controller voor 802.1x verificatie. Als u de AAA-server wilt toevoegen, navigeer dan naar **WLC GUI > Security > AAA > RADIUS > Verificatie > New**.

Security **RADIUS Authentication Servers > Edit**

AAA

- General
- RADIUS**
 - Authentication
 - Accounting
 - Fallback
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies

Local EAP

Priority Order

Certificate

Access Control Lists

Wireless Protection Policies

Server Index: 1

Server Address: [REDACTED]

Shared Secret Format: ASCII

Shared Secret: ***

Confirm Shared Secret: ***

Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number: 1812

Server Status: Enabled

Support for RFC 3576: Enabled

Server Timeout: 2 seconds

Network User Enable

Management Enable

IPSec Enable

4. AP is standaard in lokale modus, dus zet u de modus naar FlexConnect om. Lokale mode APs kunnen in FlexConnect modus worden geconverteerd door naar **Draadloos > Alle APs** te gaan, en op Individuele AP te klikken.

All APs > Details for AP3500

General Credentials Interfaces High Availability Inventory Advanced

General

AP Name	AP3500	Primary Software Version	7.2.1.69
Location	default location	Backup Software Version	7.2.1.72
AP MAC Address	cc:ef:48:c2:35:57	Predownload Status	None
Base Radio MAC	2c:3f:38:f6:98:b0	Predownloaded Version	None
Admin Status	Enable	Predownload Next Retry Time	NA
AP Mode	FlexConnect	Predownload Retry Count	NA
AP Sub Mode	None	Boot Version	12.4.23.0
Operational Status	REG	IOS Version	12.4(20111122:141426)\$
Port Number	1	Mini IOS Version	7.0.112.74
Venue Group	Unspecified	IP Config	
Venue Type	Unspecified	IP Address	10.10.10.132
Venue Name		Static IP	<input type="checkbox"/>
Language		Time Statistics	
Network Spectrum Interface Key	0D45BA896226F4117D98BA920FBA8A16	UP Time	0 d, 00 h 01 m 14 s
		Controller Associated Time	0 d, 00 h 00 m 14 s
		Controller Association Latency	0 d, 00 h 00 m 59 s

5. Voeg de FlexConnect APs aan de FlexConnect groep toe.navigeren onder **WLC GUI > Draadloos > FlexConnect groepen > Selecteer FlexConnect Group > tabblad General > Add AP.**

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

Group Name Store 1

FlexConnect APs

Add AP

Select APs from current controller

AP Name AP3500

Ethernet MAC cc:ef:48:c2:35:57

Add Cancel

AAA

Primary Radius Server None

Secondary Radius Server None

Enable AP Local Authentication

6. FlexConnect AP zou op een boomstamport moeten worden aangesloten en WLAN in kaart gebrachte VLAN en AAA verbonden VLAN zou op de boompoort moeten worden

```

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

```

toegestaan.

Opmerking: In deze configuratie wordt VLAN 109 gebruikt voor WLAN VLAN-mapping en VLAN 3 wordt gebruikt voor AAA-Override.

7. Configuratie WLAN aan VLAN in kaart brengen voor FlexConnect AP. Gebaseerd op deze configuratie, zou AP de interfaces voor het VLAN hebben. Wanneer AP de configuratie van VLAN ontvangt, worden de overeenkomstige punt11 en Ethernet subinterfaces gecreëerd en aan een bridge-groep toegevoegd. Associeer een client op deze WLAN en wanneer de client associeert, wordt zijn VLAN (standaard, gebaseerd op de WLAN-VLAN-mapping) toegewezen. Navigeer naar **WLAN GUI > Draadloos > Alle APs > klik op het specifieke tabblad AP > FlexConnect** en klik op **VLAN-**

All APs > AP3500 > VLAN Mappings

AP Name		AP3500
Base Radio MAC		2c:3f:38:f6:98:b0
WLAN Id	SSID	VLAN ID
1	Store 1	109

toewijzing.

8. Maak een gebruiker in de AAA server en stel de gebruiker in om VLAN-id in de eigenschap IETF Radius terug te

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

geven.

9. Om dynamische VLAN-toewijzing te hebben, zou AP de interfaces voor het dynamische VLAN hebben vooraf gemaakt op basis van de configuratie met bestaande WLAN-VLAN Toewijzing voor de individuele FlexConnect AP of het gebruik van ACL-VLAN-mapping op FlexConnect groep. Om AAA VLAN op de FlexConnect AP te configureren kunt u **door naar WLC GUI > Wireless > FlexConnect Group > klikken op de specifieke FlexConnect groep > VLAN-ACL-afbeelding** en VLAN in het **VLAN ID-veld** invoeren.

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade **VLAN-ACL mapping**

VLAN ACL Mapping

Vlan Id

Ingress ACL

Egress ACL

10. Associeer een client op dit WLAN en bevestig het gebruik van de gebruikersnaam die in de AAA-server is ingesteld om het AAA VLAN terug te sturen.
11. De client moet een IP-adres ontvangen van het dynamische VLAN dat via de AAA-server wordt geretourneerd.
12. Klik om te controleren op **WLC GUI > Monitor > client** > op het specifieke client-MAC-adres om de clientgegevens te controleren.

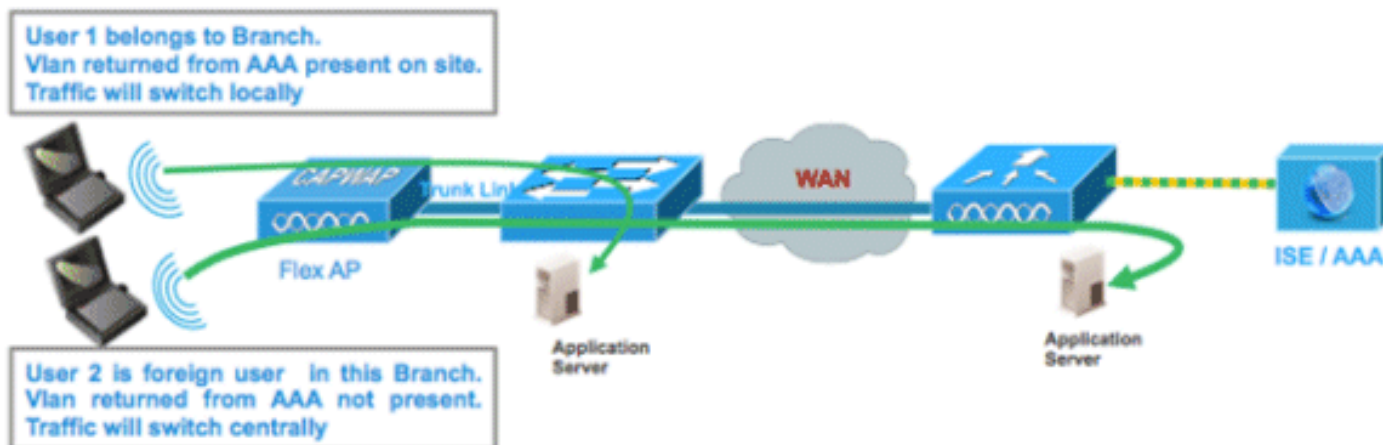
Beperkingen

- Eigenschappen die specifiek zijn voor Cisco Aironet worden niet ondersteund en id-id voor eigenschap IETF wordt alleen ondersteund.
- Een maximum van 16 VLAN's kan in elke-AP-configuratie worden geconfigureerd, via WLAN-VLAN in kaart brengen voor individuele FlexConnect AP of door ACL-VLAN-mapping te gebruiken in de FlexConnect-groep.

[FlexConnect VLAN-gebaseerde Central-switching](#)

In controller-software-releases 7.2, AAA Override of VLAN (Dynamische VLAN-toewijzing) voor lokaal geschakelde WLAN's zal draadloze clients plaatsen naar het VLAN dat door de AAA-server wordt geleverd. Als het VLAN dat door de AAA-server wordt geleverd niet aanwezig is bij AP, wordt de client geplaatst naar een WLAN-in kaart gebracht VLAN op die AP en zal het verkeer lokaal op dat VLAN switches. Bovendien kan, voorafgaand aan release 7.3, verkeer voor een bepaalde WLAN-functie van FlexConnect APs, afhankelijk van de WLAN-configuratie, centraal of lokaal worden geschakeld.

Vanaf release 7.3 kan verkeer van FlexConnect APs centraal of lokaal worden geschakeld, afhankelijk van de aanwezigheid van een VLAN op een FlexConnect AP.



Samenvatting

Traffic Flow op WLAN's ingesteld voor Local Switching wanneer Flex AP's in Connected Mode zijn:

- Als het VLAN wordt teruggegeven als één van de AAA eigenschappen en dat VLAN niet aanwezig is in de Flex AP database zal het verkeer centraal switches en de client zal dit VLAN/Interface die van de AAA server is teruggekeerd toegewezen op voorwaarde dat het VLAN op WLC bestaat.
- Als het VLAN wordt teruggegeven als één van de AAA eigenschappen en dat VLAN niet aanwezig is in de Flex AP gegevensbestand, zal het verkeer centraal switches. Als dat VLAN ook niet op de WLC aanwezig is, zal de client een VLAN/interface toegewezen krijgen die in kaart is gebracht in een WLAN op de WLC.
- Als het VLAN wordt teruggegeven als één van de AAA eigenschappen en dat VLAN in de FlexConnect AP database aanwezig is, zal het verkeer lokaal switches.
- Als het VLAN niet van de AAA-server wordt teruggegeven, wordt de client een WLAN-in kaart gebracht VLAN aan die FlexConnect AP toegewezen en zal het verkeer lokaal switches.

Traffic Flow op WLAN's ingesteld voor Local Switching wanneer Flex AP's in standalone modus zijn:

- Als het VLAN dat door een AAA-server is geretourneerd niet in de Flex AP-database aanwezig is, wordt de client in standaard VLAN gezet (dat wil zeggen, een WLAN in kaart gebracht VLAN op Flex AP). Wanneer AP terug verbindt, zal deze client worden gedesauthentiseerd en zal centraal verkeer switches.
- Als het VLAN dat door een AAA server is teruggegeven in de Flex AP database aanwezig is zal de client in een teruggestuurd VLAN worden gezet en zal het verkeer lokaal switches.
- Als het VLAN niet van een AAA-server wordt teruggegeven, wordt de client een WLAN-in kaart gebracht VLAN aan die FlexConnect AP toegewezen en zal het verkeer lokaal switches.

Procedure

Voer de volgende stappen uit:

1. Configureer een WLAN voor lokale switching en stel AAA-voorrang in.

WLANs > Edit 'Store 1'

General	Security	QoS	Advanced
Allow AAA Override	<input checked="" type="checkbox"/>	Enabled	
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enabled	
Enable Session Timeout	<input checked="" type="checkbox"/>	<input type="text" value="1800"/>	Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/>	Enabled	
Diagnostic Channel	<input type="checkbox"/>	Enabled	
Override Interface ACL		IPv4 <input type="text" value="None"/>	IPv6 <input type="text" value="None"/>
P2P Blocking Action		<input type="text" value="Disabled"/>	
Client Exclusion ³	<input checked="" type="checkbox"/>	Enabled	<input type="text" value="60"/> Timeout Value (secs)
Maximum Allowed Clients ⁶		<input type="text" value="0"/>	
Static IP Tunneling ¹¹	<input type="checkbox"/>	Enabled	
Wi-Fi Direct Clients Policy		<input type="text" value="Disabled"/>	
Maximum Allowed Clients Per AP Radio		<input type="text" value="200"/>	
FlexConnect			
FlexConnect Local Switching ²	<input checked="" type="checkbox"/>	Enabled	

2. Schakel VLAN-gebaseerde Central Switching in op het nieuw gemaakte WLAN.

WLANs > Edit 'Store 1'

General

Security

QoS

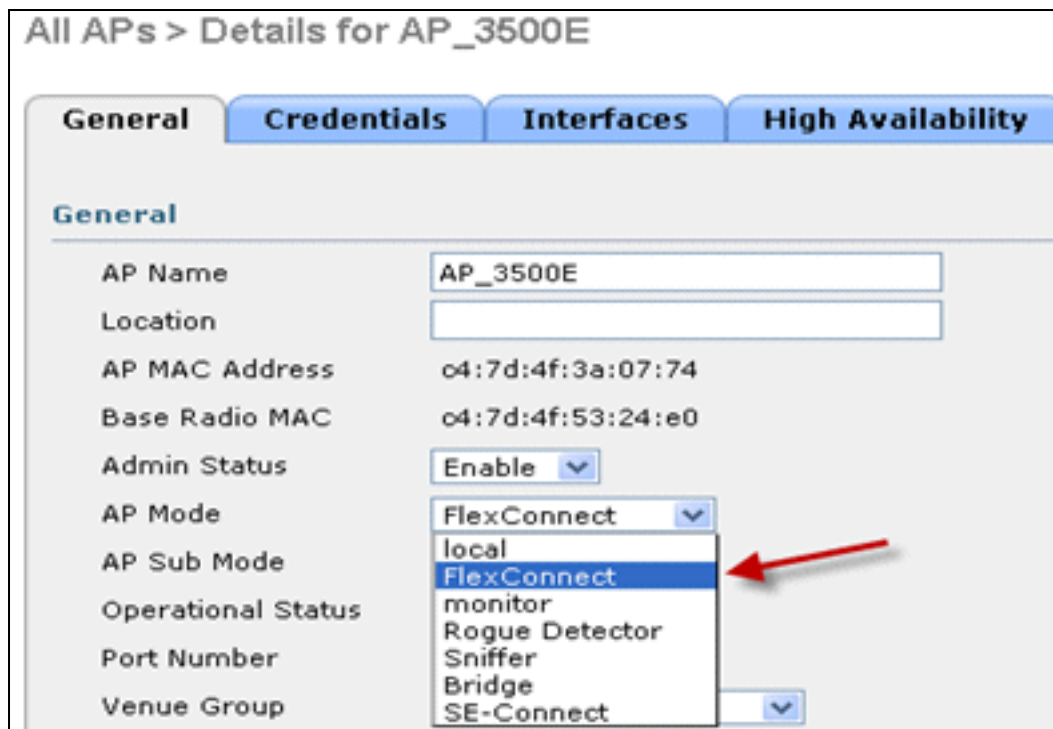
Advanced

- Allow AAA Override Enabled
- Coverage Hole Detection Enabled
- Enable Session Timeout
Session Timeout (secs)
- Aironet IE Enabled
- Diagnostic Channel Enabled
- Override Interface ACL IPv4 IPv6
- P2P Blocking Action
- Client Exclusion [3](#) Enabled
Timeout Value (secs)
- Maximum Allowed Clients [8](#)
- Static IP Tunneling [11](#) Enabled
- Wi-Fi Direct Clients Policy
- Maximum Allowed Clients Per AP Radio

FlexConnect

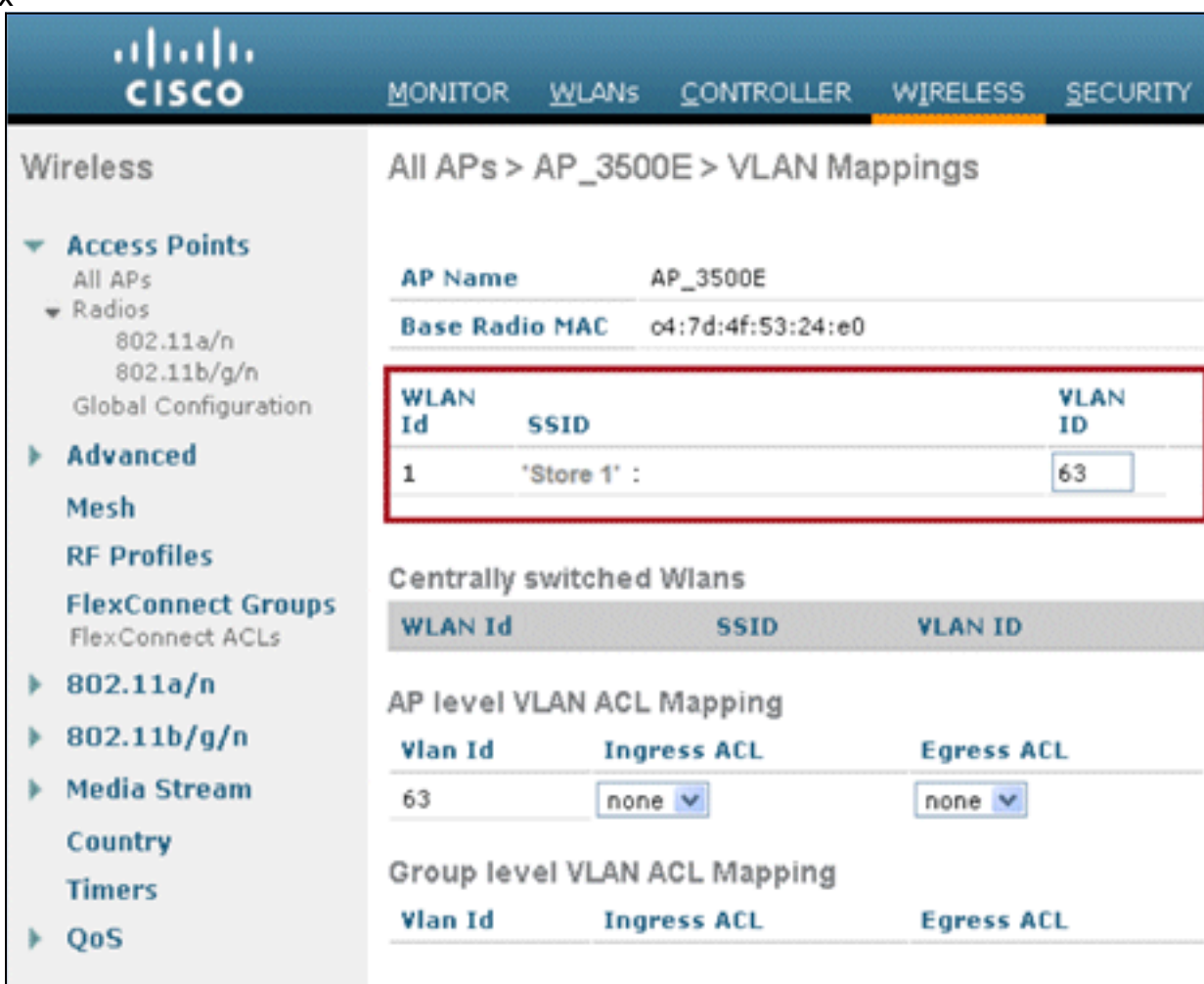
- FlexConnect Local Switching [2](#) Enabled
- FlexConnect Local Auth [12](#) Enabled
- Learn Client IP Address [5](#) Enabled
- Vlan based Central Switching [13](#) Enabled

3. Stel AP Mode in op



FlexConnect.

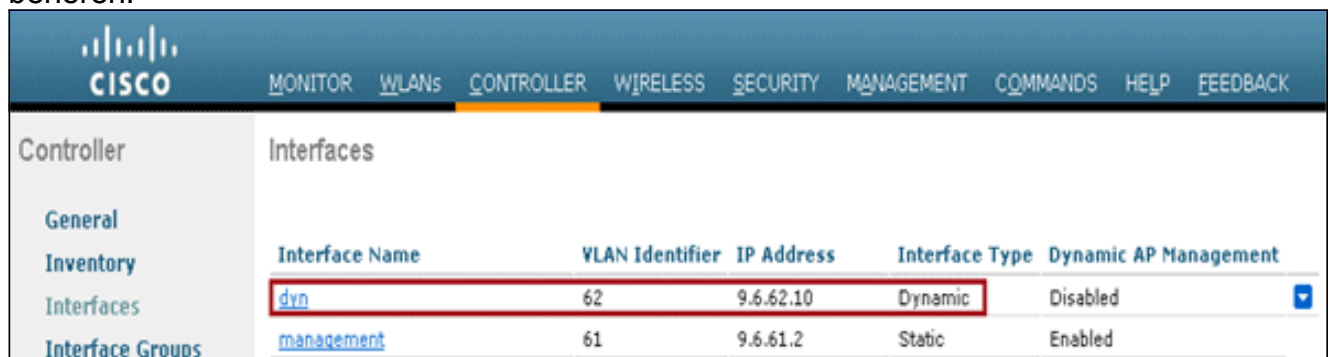
- Zorg ervoor dat FlexConnect AP een of ander subinterface aanwezig in zijn database heeft, of via WLAN-VLAN Mapping op een bepaalde Flex AP of via het configureren van VLAN van een Flex groep. In dit voorbeeld wordt VLAN 63 geconfigureerd in WLAN-VLAN-mapping op Flex



AP.

- In dit voorbeeld wordt VLAN 62 op WLC geconfigureerd als een van de dynamische interfaces en wordt niet in kaart gebracht in het WLAN op de WLC. WLAN op de WLC wordt in kaart gebracht om VLAN (dwz. VLAN 61) te

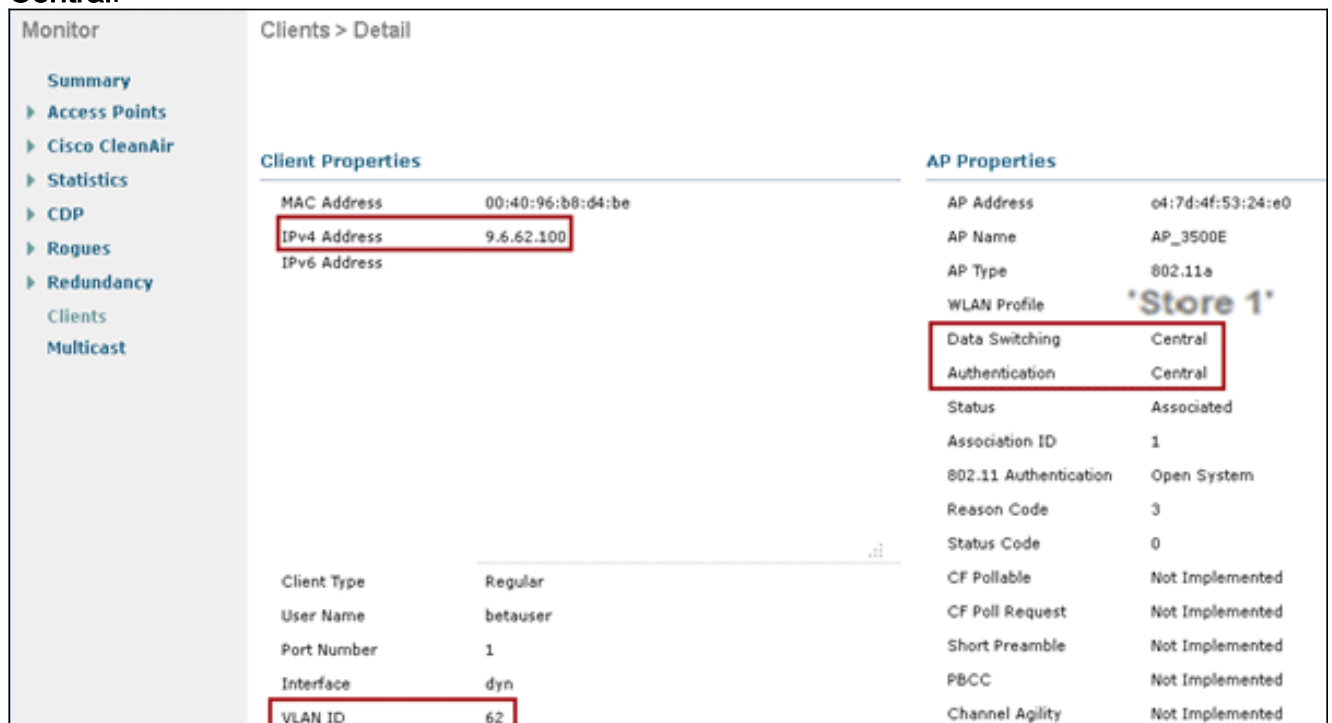
beheren.



The screenshot shows the Cisco Controller's 'Interfaces' page. A table lists two interfaces: 'dyn' and 'management'. The 'dyn' interface is highlighted with a red box. The table has columns for Interface Name, VLAN Identifier, IP Address, Interface Type, and Dynamic AP Management.

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
dyn	62	9.6.62.10	Dynamic	Disabled
management	61	9.6.61.2	Static	Enabled

6. Associeer een client aan WLAN die in Stap 1 is geconfigureerd op deze Flex AP en breng VLAN 62 vanuit de AAA-server terug. VLAN 62 is niet aanwezig op deze Flex AP, maar het is aanwezig op WLC als dynamische interface zodat het verkeer centraal zal switches en de client VLAN 62 op WLC zal worden toegewezen. In de hier opgenomen uitvoer is de client VLAN 62 toegewezen en Data Switching en Verificatie worden ingesteld op **Central**.



The screenshot shows the 'Clients > Detail' page in the Cisco Controller. It displays client and AP properties. The 'Client Properties' section shows the IPv4 Address as 9.6.62.100. The 'AP Properties' section shows the WLAN Profile as 'Store 1' and the Data Switching and Authentication settings as 'Central'. The 'VLAN ID' is also shown as 62.

Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d:4f:53:24:e0
IPv4 Address	9.6.62.100	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	Open System
		Reason Code	3
		Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
		Short Preamble	Not Implemented
		PBCC	Not Implemented
		Channel Agility	Not Implemented

Client Type	Regular
User Name	betauser
Port Number	1
Interface	dyn
VLAN ID	62

Opmerking: Merk op dat, alhoewel WLAN is geconfigureerd voor Local Switching, het veld Data Switching voor deze client centraal is gebaseerd op de aanwezigheid van een VLAN (dwz: VLAN 62, dat van de AAA-server wordt teruggestuurd, niet aanwezig is in de AP-database).

7. Als een andere gebruiker zich op dezelfde AP op deze gemaakte WLAN associeert en een deel VLAN van de AAA-server die niet aanwezig is op zowel het AP als de WLC wordt, zal het verkeer centraal switches en de client de WLAN-in kaart gebrachte interface op de WLC (dat wil zeggen VLAN 61 in deze voorbeeldinstelling) ontvangen, omdat het WLAN in kaart wordt gebracht aan de beheerinterface die voor VLAN 61 is geconfigureerd

Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d: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
Client Type	Regular	Status	Associated
User Name	betauser2	Association ID	1
Port Number	1	802.11 Authentication	Open System
Interface	management	Reason Code	3
VLAN ID	61	Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
		Short Preamble	Not Implemented
		PBCC	Not Implemented
		Channel Agility	Not Implemented

Opmerking: Let op dat, hoewel WLAN is geconfigureerd voor Local Switching, het veld Data Switching voor deze client is Central gebaseerd op de aanwezigheid van een VLAN. Dat wil zeggen, VLAN 61, dat van de AAA server wordt teruggegeven, is niet aanwezig in de AP Database maar is ook niet aanwezig in de WLC database. Als resultaat hiervan wordt de client een standaard interface VLAN/interface toegewezen die in kaart wordt gebracht in het WLAN. In dit voorbeeld, wordt WLAN in kaart gebracht aan een beheerinterface (dwz, VLAN 61) en heeft de client een IP-adres van VLAN 61 ontvangen.

8. Als een andere gebruiker zich op dit gemaakte WLAN en VLAN 63 van de AAA-server (die op deze Flex AP aanwezig is) aan deze client wordt toegewezen VLAN 63 en zal het verkeer lokaal switches.

Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d: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

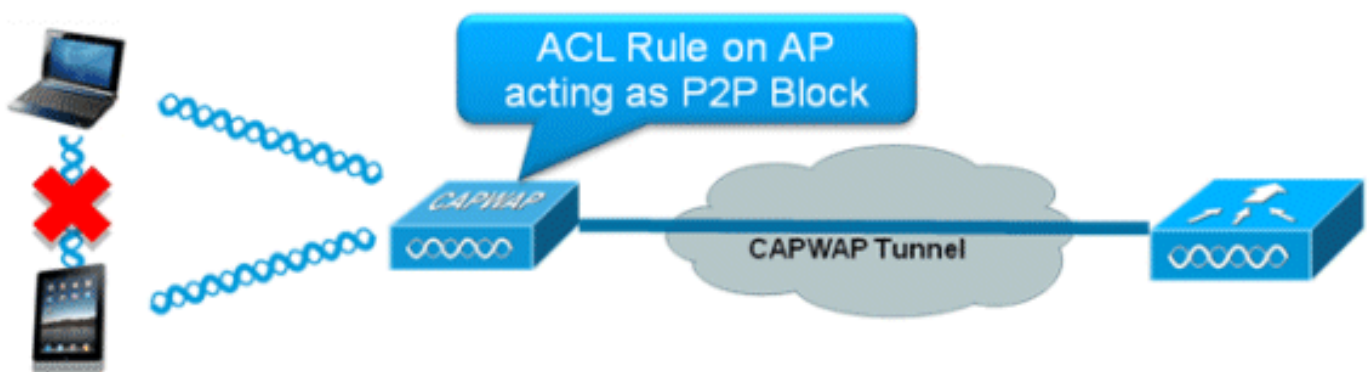
Beperkingen

- VLAN-gebaseerde Central Switching wordt alleen ondersteund op WLAN's die zijn geconfigureerd voor Centrale verificatie en lokale switching.

- De AP sub-interface (d.w.z. VLAN in kaart brengen) moet op de FlexConnect AP worden geconfigureerd.

FlexConnect ACL

Door de introductie van ACL's op FlexConnect wordt voorzien in een mechanisme om rekening te houden met de behoefte aan toegangscontrole op de FlexConnect AP voor bescherming en integriteit van lokaal geschakeld gegevensverkeer van de AP. FlexConnect ACL's worden gemaakt op de WLC en moeten dan worden geconfigureerd met het VLAN dat aanwezig is op de FlexConnect AP of FlexConnect groep met VLAN-ACL-mapping, die bedoeld is voor AAA-Override VLAN's. Deze worden dan naar de AP gedrukt.



Samenvatting

- Maak FlexConnect ACL op de controller.
- Pas hetzelfde op een VLAN toe dat aanwezig is op FlexConnect AP onder AP Level VLAN-mapping.
- Kan worden toegepast op een VLAN dat aanwezig is in FlexConnect Group onder VLAN-ACL-mapping (over het algemeen gemaakt voor AAA-overschreven VLAN's).
- Tijdens het toepassen van ACL op VLAN, selecteer de toe te passen richting die "binnendringing", "stress" of "ingang en uitgang" zal zijn.

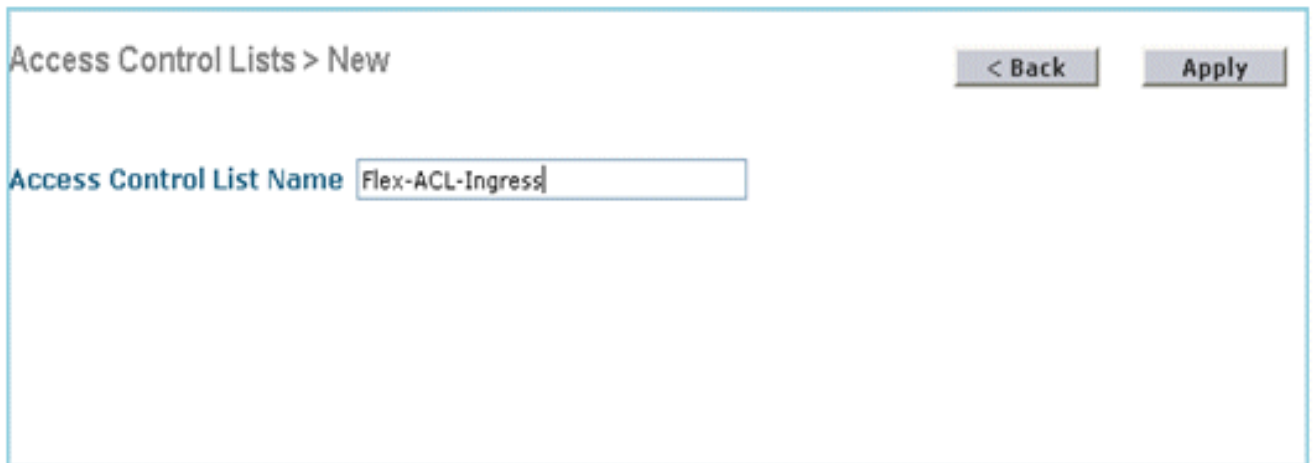
Procedure

Voer de volgende stappen uit:

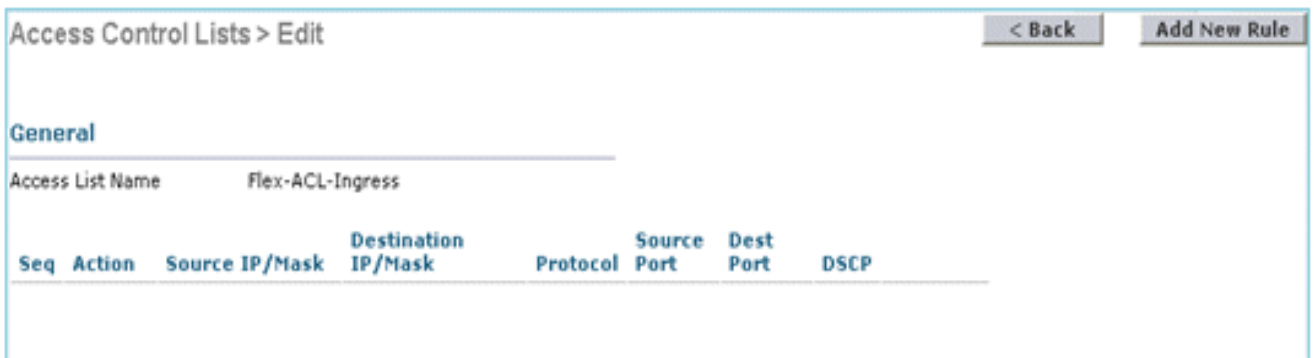
1. Maak een FlexConnect ACL op de WLC. Navigeer naar **WLC GUI > Security > Access Control List > FlexConnect ACL's**.



2. Klik op **New** (Nieuw).
3. Configureer de ACL-naam.



4. Klik op **Apply** (Toepassen).
5. Maak regels voor elke ACL. Om regels te maken, navigeer naar **WLC GUI > Security > Access Control List > FlexConnect ACL's** en klik op de bovenstaande gemaakte ACL's.



6. Klik op **Nieuwe regel toevoegen**.

Access Control Lists > Rules > New < Back Apply

Sequence:

Source: IP Address: Netmask:

Destination: IP Address: Netmask:

Protocol:

DSCP:

Action:

Opmerking: Configureer de regels overeenkomstig de eis. Als de vergunning om het even welke regel niet wordt gevormd aan het eind, is er een impliciete ontkenning die al verkeer zal blokkeren.

7. Nadat de FlexConnect ACL's zijn gemaakt, kan deze voor WLAN-VLAN-mapping worden uitgevoerd onder individuele FlexConnect AP of worden toegepast op VLAN-ACL-mapping op de FlexConnect groep.
8. Kaart FlexConnect ACL hierboven ingesteld op AP-niveau voor afzonderlijke VLAN's onder VLAN-mappings voor individuele FlexConnect AP. Navigeer naar **WLC GUI > Draadloos > Alle AP >** klik op het specifieke AP > **FlexConnect** tabblad > **VLAN-mapping**.

All APs > AP3500 > VLAN Mappings

AP Name AP3500

Base Radio MAC 2c:3f:38:f6:98:b0

WLAN Id	SSID	VLAN ID
1	Store 1	<input type="text" value="109"/>

Centrally switched Wlans

WLAN Id	SSID	VLAN ID
2	Store 3	N/A

AP level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL
109	<input type="text" value="Flex-ACL-Ingress"/>	<input type="text" value="Flex-ACL-Egress"/>

9. FlexConnect ACL kan ook worden toegepast op VLAN-ACL-omzetting in de FlexConnect-groep. VLAN's die onder VLAN-ACL-omzetting in FlexConnect-groep zijn gemaakt, worden

voornamelijk gebruikt voor dynamische VLAN-excuus.

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade **VLAN-ACL mapping**

VLAN ACL Mapping

Vlan Id

Ingress ACL Flex-ACL-Egress ▼

Egress ACL Flex-ACL-Egress ▼

Add

Vlan Id	Ingress ACL	Egress ACL
3	Flex-ACL-Ingress ▼	Flex-ACL-Egress ▼

Beperkingen

- Een maximum van 512 FlexConnect ACL's kan op WLC worden geconfigureerd.
- Elke ACL kan met 64 regels worden ingesteld.
- U kunt maximaal 32 ACL's per FlexConnect-groep of per FlexConnect-AP in kaart brengen.
- Op een bepaald moment in de tijd, is er een maximum van 16 VLAN's en 32 ACL's op FlexConnect AP.

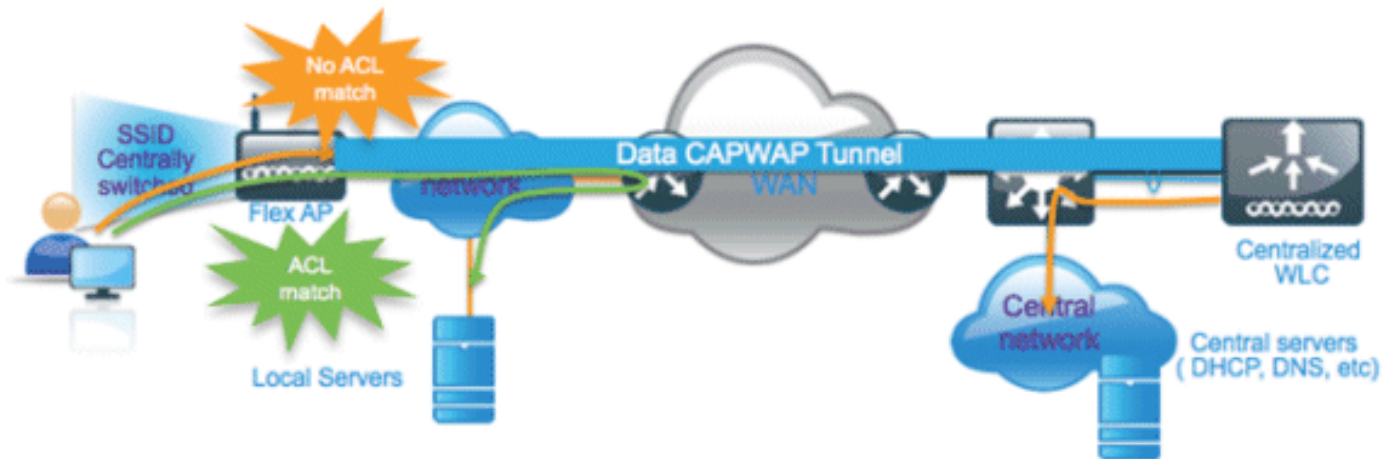
FlexConnect Split-tunneling

In WLC-releases voorafgaand aan 7.3, als een client die verbinding maakt met een FlexConnect AP gekoppeld aan een centraal geschakeld WLAN wat verkeer naar een apparaat dat aanwezig is in de lokale site/het netwerk moet sturen, moet hij verkeer via CAPWAP naar de WLC verzenden en dan hetzelfde verkeer terugbrengen naar de lokale site via CAPWAP of gebruik maken van een of andere off-band connectiviteit.

Vanaf release 7.3 introduceert **Split Tunneling** een mechanisme waarmee het verkeer dat door de client wordt verstuurd geclassificeerd wordt op basis van pakketinhoud **met Flex ACL**. Overeenkomende pakketten worden lokaal van Flex AP geschakeld en de rest van de pakketten worden centraal over CAPWAP geschakeld.

De functie Split Tunneling is een extra voordeel voor OEAP AP-instellingen waar klanten op een Corporate SSID met apparaten op een lokaal netwerk kunnen praten (printers, bekabelde machine op een Remote LAN-poort of draadloze apparaten op een Mobile SSID) zonder WAN-bandbreedte te gebruiken door pakketten via CAPWAP te verzenden. Split-tunneling wordt niet ondersteund op OEAP 600 AP's. Flex ACL kan met regels worden gecreëerd om alle apparaten toe te staan die op de lokale plaats/het netwerk aanwezig zijn. Wanneer pakketten van een draadloze client op de Corporate SSID overeenkomen met de regels in Flex ACL die op OEAP zijn ingesteld, wordt dat verkeer lokaal geschakeld en de rest van het verkeer (dat betekent impliciet ontkennen van verkeer) centraal over CAPWAP switch.

De oplossing van het Split Tunneling veronderstelt dat Subnet/VLAN verbonden met een client in de centrale plaats niet aanwezig is in de lokale plaats (dat is verkeer voor klanten die een IP adres van het netwerk ontvangen dat op de centrale plaats aanwezig is zal niet lokaal kunnen switches). De functie Split Tunneling is ontworpen om lokaal verkeer te switches voor subnetten die tot de lokale plaats behoren om WAN-bandbreedteverbruik te voorkomen. Het verkeer dat met de Flex ACL-regels overeenkomt wordt lokaal geschakeld en NAT-handeling wordt uitgevoerd om het IP-adres van de bron van de client te wijzigen naar het BVI-adres van de Flex AP dat op de lokale site/het netwerk routeerbaar is.



Samenvatting

- De Split Tunneling-functionaliteit wordt ondersteund op WLAN's die zijn geconfigureerd voor Central Switching die alleen door Flex AP's worden geadverteerd.
- DHCP vereist moet worden ingeschakeld op WLAN's die zijn geconfigureerd voor Split-tunneling.
- De configuratie van Split Tunneling wordt toegepast per WLAN-instelling, geconfigureerd voor centrale switching op Flex AP of voor alle Flex APs in een FlexConnect-groep.

Procedure

Voer de volgende stappen uit:

1. Het configureren van een WLAN voor Central-switching (dat wil zeggen, **Flex Local Switching** dient niet ingeschakeld te zijn).

WLANs > Edit 'Store 1'

General **Security** **QoS** **Advanced**

Allow AAA Override Enabled

Coverage Hole Detection Enabled

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 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 Enabled

Flex Local Switching should not be enabled

2. Stel DHCP-adrestoewijzing in op vereist.

WLANs > Edit 'Store 1'

General **Security** **QoS** **Advanced**

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout 1800
Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 None IPv6 None

DHCP

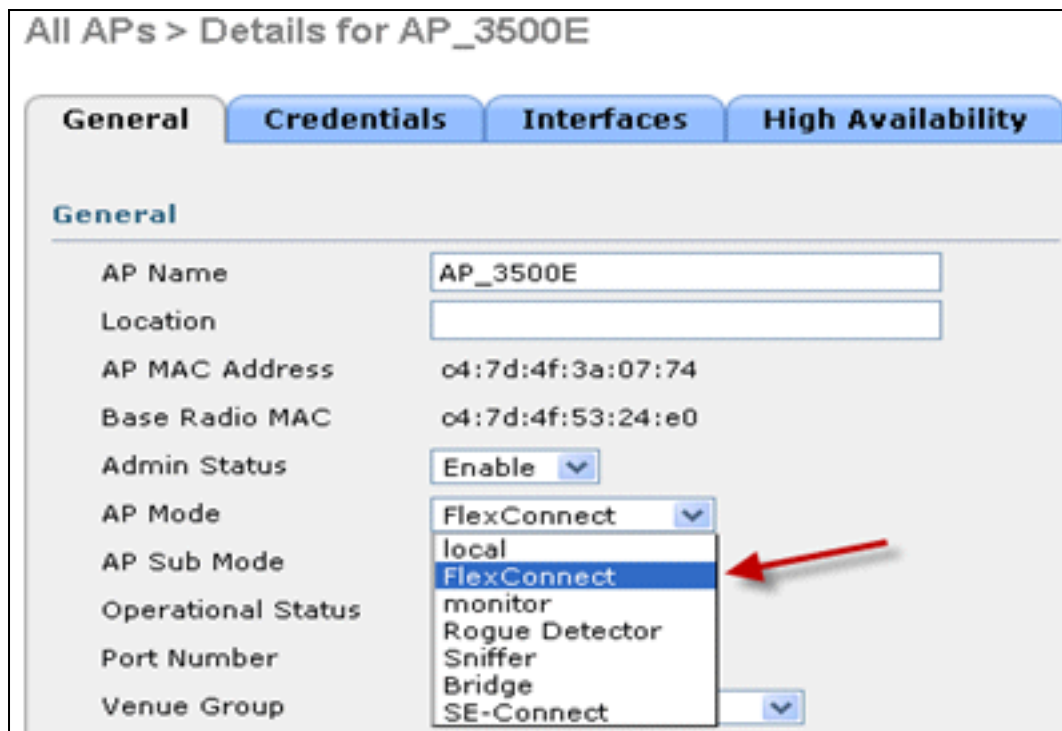
DHCP Server Override

DHCP Addr. Assignment Required

Management Frame Protection (MFP)

MFP Client Protection Optional

3. Stel AP Mode in op



FlexConnect.

4. Configureer FlexConnect ACL met een vergunningsregel voor verkeer die lokaal op de Central Switch WLAN moet worden ingeschakeld. In dit voorbeeld wordt de FlexConnect ACL-regel zo geconfigureerd dat het ICMP-verkeer waarschuwt van alle klanten die op 9.6.61.0-net (dwz, bestaan op de centrale site) tot 9.1.0.150 zijn ingeschakeld nadat de NAT-handeling op Flex AP is toegepast. De rest van het verkeer zal een impliciete ontkenningsregel raken en centraal over CAPWAP worden geschakeld.



5. Deze gemaakte FlexConnect ACL kan als Split Tunnel ACL naar individuele Flex AP worden geduwd of kan ook naar alle Flex APs in een Flex Connect groep worden geduwd. Voltooi deze stappen om Flex ACL als lokale Split naar individuele Flex AP te duwen: Klik op **Local Split ACL's**.

The screenshot shows the Cisco Wireless Controller interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK. The main content area is titled "All APs > Details for AP_3500E". The "FlexConnect" tab is selected and highlighted with a red box. Below the tabs, the "VLAN Support" checkbox is checked. The "Native VLAN ID" is set to 57. The "FlexConnect Group Name" is "Not Configured". Under "PreAuthentication Access Control Lists", there are two links: "External WebAuthentication ACLs" and "Local Split ACLs". The "Local Split ACLs" link is highlighted with a red box and has a red arrow pointing to it.

Selecteer WLAN-id op welke splitter-tunnelfunctie ingeschakeld moet worden, kies Flex-ACL en klik op Add.

The screenshot shows the "All APs > AP_3500E > ACL Mappings" page. The "AP Name" is AP_3500E and the "Base Radio MAC" is c4:7d:4f:53:24:e0. The "WLAN ACL Mapping" form is highlighted with a red box. It contains the following fields: "WLAN Id" with the value 1, "Local-Split ACL" with a dropdown menu set to "Flex-ACL", and an "Add" button. Two callout boxes with red arrows provide instructions: "Enter WLAN ID on which Split Tunnel should be enabled" points to the "WLAN Id" field, and "Click Add after selecting Flex ACL" points to the "Add" button. Below the form is a table with the following headers: "WLAN Id", "WLAN Profile Name", and "Local-Split ACL".

Flex-ACL wordt geduwd als lokaal-gesplitste ACL naar Flex

All APs > AP_3500E > ACL Mappings

AP Name AP_3500E

Base Radio MAC 04:7d:4f:53:24:e0

WLAN ACL Mapping

WLAN Id

Local-Split ACL

WLAN Id	WLAN Profile Name	Local-Split ACL
1	'Store 1'	Flex-ACL <input type="button" value="Add"/>

AP. V
 oltooi deze stappen om Flex ACL als lokale Split naar een FlexConnect-groep te duwen: Selecteer de WLAN-id waarop de functie Split-tunneling moet worden ingeschakeld. Selecteer FlexConnect ACL's op het tabblad **WLAN-ACL** en klik op **Add** van de FlexConnect-groep waar bepaalde Flex AP's worden toegevoegd.

Wireless FlexConnect Groups > Edit Flex-Group'

General Local Authentication Image Upgrade AAA VLAN-ACL mapping **WLAN-ACL mapping** WebPolicies

Web Auth ACL Mapping

WLAN Id WebAuth ACL

Local Split ACL Mapping

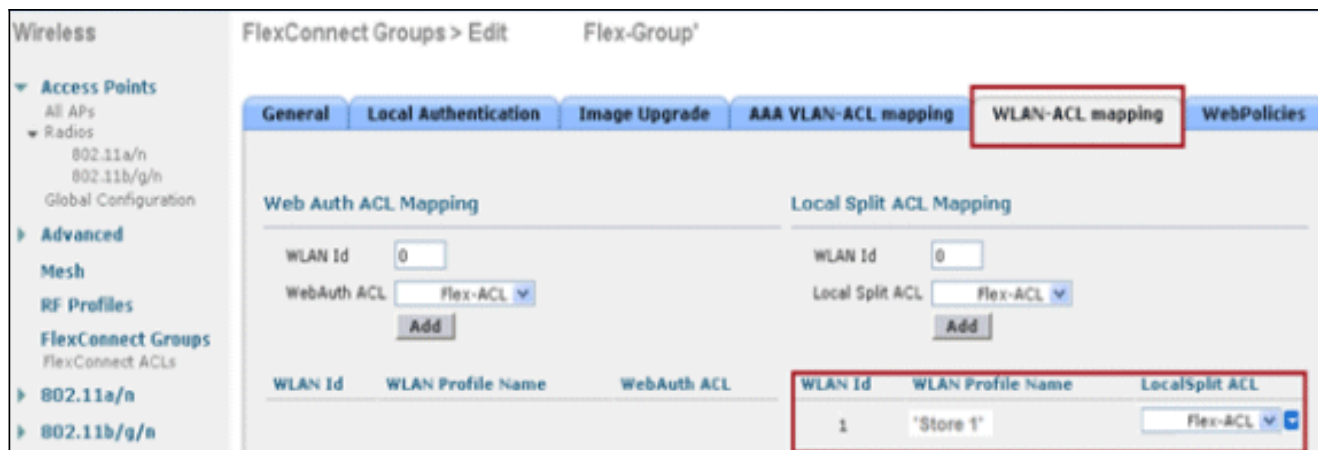
WLAN Id Local Split ACL

Enter WLAN ID on which Split Tunnel should be enabled

Click ADD after selecting Flex ACL

WLAN Id	WLAN Profile Name	WebAuth ACL	WLAN Id	WLAN Profile Name	LocalSplit ACL

Flex-ACL wordt geduwd als Local Split ACL naar Flex AP's in die Flex groep.



Beperkingen

- Flex ACL-regels dienen niet te worden ingesteld met licentie/ontkenningsverklaring met hetzelfde subnet als bron en bestemming.
- Verkeer op een Centraal Switched WLAN dat is geconfigureerd voor Split Tunneling kan alleen lokaal worden geschakeld wanneer een draadloze client verkeer initieert voor een host die zich op de lokale site bevindt. Als het verkeer wordt geïnitieerd door klanten/host op een lokale website voor draadloze klanten op deze geconfigureerde WLAN's, kan het de bestemming niet bereiken.
- Split-tunneling wordt niet ondersteund voor multicast/broadcast-verkeer. Multicast/broadcast-verkeer switches centraal, zelfs als dit overeenkomt met Flex ACL.

Tolerantie fout

FlexConnect-fouttolerantie maakt draadloze toegang en services mogelijk voor filiaalklanten wanneer:

- FlexConnect Vestiging APs verliezen connectiviteit met de primaire Flex 7500 controller.
- FlexConnect Branch APs worden overgeschakeld naar de secundaire Flex 7500 controller.
- FlexConnect Branch APs herstellen de verbinding met de primaire Flex 7500 controller.

FlexConnect-fout tolerantie, samen met het hierboven beschreven lokale MAP, bieden samen nul filiaaldowntime tijdens een netwerkstoring. Deze optie is standaard ingeschakeld en kan niet worden uitgeschakeld. Er is geen configuratie voor nodig van de controller of het AP. Om ervoor te zorgen dat de Faulttolerantie goed werkt en van toepassing is, moeten deze criteria echter worden gehandhaafd:

- WLAN-bestellen en -configuraties moeten identiek zijn voor de primaire en reservekopie Flex 7500-controllers.
- VLAN-mapping moet identiek zijn voor de primaire en reservekopie Flex 7500-controllers.
- Mobility domeinnaam moet identiek zijn voor de primaire en reservekopie Flex 7500 controllers.
- Het wordt aanbevolen Flex 7500 te gebruiken als zowel de primaire als de back-upcontrollers.

Samenvatting

- FlexConnect zal geen klanten loskoppelen wanneer de AP weer op dezelfde controller

aangesloten is op voorwaarde dat er geen verandering in configuratie op de controller optreedt.

- FlexConnect zal geen klanten loskoppelen bij de aansluiting op de back-upcontroller op voorwaarde dat de configuratie niet verandert en de back-upcontroller identiek is aan de primaire controller.
- FlexConnect stelt zijn radio's niet opnieuw in bij het aansluiten op de primaire controller, mits de configuratie van de controller niet verandert.

Beperkingen

- Alleen ondersteund voor FlexConnect met Central/Local Configuration met Local Switching.
- Voor Centraal geauthentiseerde klanten moet volledige herauthenticatie zijn als de timer voor de clientsessie vervalft voordat de FlexConnect AP switches van Standalone naar Connected Mode zijn.
- Flex 7500 primaire en back-up controllers moeten in hetzelfde mobiliteitsdomein zijn.

Clientlimiet per WLAN

Samen met verkeerssegmentering is het noodzakelijk de totale klant die toegang tot de draadloze diensten heeft, te beperken.

Voorbeeld: Beperking van het totaal aantal clients van filialen die terugkeren naar het datacenter.

Om deze uitdaging aan te pakken, introduceert Cisco Clientlimiet per WLAN-functie die de totale client kan beperken die op een WLAN-basis is toegestaan.

Primaire doelstelling

- Maximale limieten voor maximale klanten vaststellen
- Operationeel gemak

Opmerking: dit is geen vorm van QoS.

Standaard wordt de optie uitgeschakeld en wordt de limiet niet verplicht.

Beperkingen

Deze optie dwingt clientlimiet niet af wanneer FlexConnect in standalone toestand verkeert.

WLC-configuratie

Voer de volgende stappen uit:

1. Selecteer de Centraal Switched WLAN ID 1 met SSID **DataCenter**. Dit WLAN is gecreëerd tijdens het maken van de AP Group. Zie [afbeelding 8](#).
2. Klik op het **tabblad Geavanceerd** voor WLAN-id 1.
3. Stel de clientgrenswaarde in voor het tekstveld Maximum aantal toegestane clients.
4. Klik op **Toepassen** nadat het tekstveld voor maximaal toegestane clients is ingesteld.

WLANs > Edit < Back Apply

General **Security** **QoS** **Advanced**

Allow AAA Override Enabled
 Coverage Hole Detection Enabled
 Enable Session Timeout 1800
 Session Timeout (secs)
 Aironet IE Enabled
 Diagnostic Channel Enabled
 IPv6 Enable [?](#)
 Override Interface ACL
 P2P Blocking Action
 Client Exclusion Enabled 60
 Timeout Value (secs)
Maximum Allowed Clients

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7
 Scan Defer Time(msecs)

DHCP

DHCP Server Override

DHCP Addr. Assignment Required

Management Frame Protection (MFP)

MFP Client Protection

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)
 802.11b/g/n (1 - 255)

NAC

NAC OOB State Enabled
 Posture State Enabled

Load Balancing and Band Select

Client Load Balancing
 Client Band Select

Foot Notes

2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
 4 Client MFP is not active unless WPA2 is configured
 5 Learn Client IP is configurable only when HREAP Local Switching is enabled
 6 WMM and open or AES security should be enabled to support higher 11n rates
 7 Multicast Should Be Enabled For IPV6.
 8 Band Select is configurable only when Radio Policy is set to 'All'.
 9 Value zero implies there is no restriction on maximum clients allowed.
 10 MAC Filtering is not supported with HREAP Local authentication

Standaard voor maximaal toegestane clients is ingesteld op 0, wat impliceert dat er geen beperking is en dat de optie is uitgeschakeld.

NCS configuratie

Ga om deze functie vanuit het NCS in te schakelen naar **Configureren > controllers > IP-controller > WLANs > WLAN-configuratie > WLAN-details.**

WLAN Configuration Details : 17

Configure > Controllers > 172.20.225.154 > WLANs > WLAN Configuration > **WLAN Configuration Details**

General Security QoS **Advanced**

FlexConnect Local Switching	<input checked="" type="checkbox"/> Enable	
FlexConnect Local Auth ⁱ	<input type="checkbox"/> Enable	
Learn Client IP Address	<input type="checkbox"/> Enable	
Session Timeout	<input checked="" type="checkbox"/> Enable	1800 (secs)
Coverage Hole Detection	<input checked="" type="checkbox"/> Enable	
Aironet IE	<input checked="" type="checkbox"/> Enable	
IPv6 [?]	<input type="checkbox"/> Enable	
Diagnostic Channel [?]	<input type="checkbox"/> Enable	
Override Interface ACL	IPv4	NONE <input type="button" value="v"/>
	IPv6	NONE <input type="button" value="v"/>
Peer to Peer Blocking ⁱ		Disable <input type="button" value="v"/>
Wi-Fi Direct Clients Policy		Disabled <input type="button" value="v"/>
Client Exclusion [!]	<input checked="" type="checkbox"/> Enable	
Timeout Value		60 (secs)
Maximum Clients ⁱ		0

DHCP

DHCP Server
DHCP Address Assignment

Management Frame Protection

MFP Client Protection [!]
MFP Version

Load Balancing and Band Sel

Client Load Balancing
Client Band Select

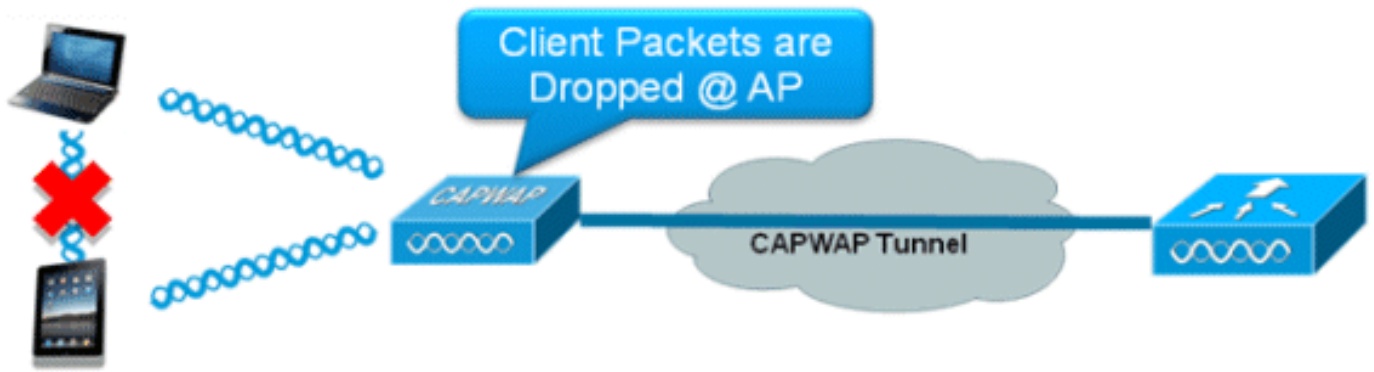
NAC

Peer-to-peer blokkering

In controller-software releases vóór 7.2 werd peer-to-peer (P2P) blokkering alleen ondersteund voor centrale switching WLAN's. Peer-to-peer blokkering kan op WLAN worden geconfigureerd met een of meer van deze drie acties:

- **Uitgeschakeld** - schakelt peer-to-peer blokkering en overbrugging lokaal binnen de controller uit voor klanten in hetzelfde net. Dit is de standaardwaarde.
- **Drop** - veroorzaakt dat de controller pakketten voor klanten in hetzelfde net weggooit.
- **Forward-Stream** - veroorzaakt dat het pakket op het upstream VLAN wordt doorgestuurd. De apparaten boven de controller beslissen welke actie u moet ondernemen met betrekking tot het pakket.

Vanaf release 7.2 wordt peer-to-peer blokkering ondersteund voor klanten die zijn gekoppeld aan lokale switching WLAN. Per WLAN wordt de peer-to-peer configuratie door de controller naar FlexConnect AP gestuurd.



Samenvatting

- Peer-to-peer blokkering wordt ingesteld per WLAN
- Per WLAN wordt de peer-to-peer blokkeringsconfiguratie gestuurd door WLC naar FlexConnect APs.
- Peer-to-peer blokkerende actie die als drop-of upstream-voorwaarts op WLAN is ingesteld wordt behandeld als peer-to-peer blokkering die FlexConnect AP mogelijk maakt.

Procedure

Voer de volgende stappen uit:

1. Schakel peer-to-peer blokkerende actie in als **Drop** op WLAN ingesteld voor FlexConnect Local Switching.

WLANs > Edit 'Store1'

Advanced

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 IPv6

P2P Blocking Action

Client Exclusion Enabled Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling Enabled

Wi-Fi Direct Clients Policy

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7

Scan Defer Time (msecs)

FlexConnect

FlexConnect Local Switching Enabled

Management Frame Protection (MFP)

MFP Client Protection

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

NAC State

Load Balancing and Band Select

Client Load Balancing

Client Band Select

Passive Client

Passive Client

Voice

Media Session Snooping Enabled

2. Wanneer de P2P-blokkerende actie eenmaal is geconfigureerd als **Drop** of **Forward-Upstream** op WLAN's die zijn geconfigureerd voor lokale switching, wordt deze gestuurd van de WLC naar de FlexConnect AP. FlexConnect APs zal deze informatie in het reep configuratiebestand in flitser opslaan. Hiervoor kan, zelfs wanneer FlexConnect AP in standalone modus is, de P2P configuratie op de corresponderende subinterfaces worden toegepast.

Beperkingen

- In FlexConnect kan de configuratie van oplossing P2P-blokkering niet alleen worden toegepast op een bepaalde FlexConnect AP of een subset van AP's. Het wordt toegepast op alle FlexConnect APs die de SSID uitzenden.
- Unified oplossing voor centrale switching klanten ondersteunt P2P upstream-forward. Dit wordt echter niet ondersteund in de FlexConnect-oplossing. Dit wordt behandeld als P2P-druppel en clientpakketten worden niet naar het volgende netwerkknooppunt verzonden, maar laten vallen.
- Unified oplossing voor centrale schakelingscliënten ondersteunt P2P blokkering voor klanten geassocieerd met verschillende APs. Deze oplossing is echter alleen gericht op klanten die verbonden zijn met dezelfde AP. FlexConnect ACL's kunnen als tijdelijke oplossing voor deze beperking worden gebruikt.

AP pre-image downloaden

Met deze functie kan AP code downloaden terwijl het operationeel is. Het downloaden van AP pre-image van AP is zeer nuttig in het verminderen van netwerkdown-time tijdens software onderhoud of upgrades.

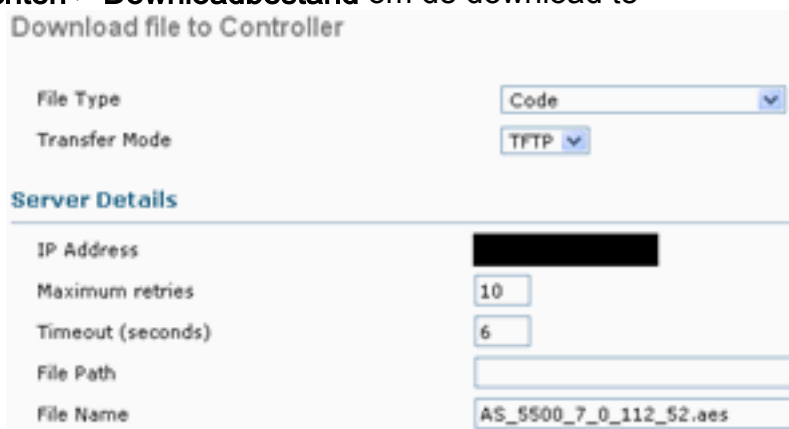
Samenvatting

- Eenvoudig softwarebeheer
- Rooster per winkel-upgrades: Het NCS is nodig om dit voor elkaar te krijgen
- Vermindert downtime

Procedure

Voer de volgende stappen uit:

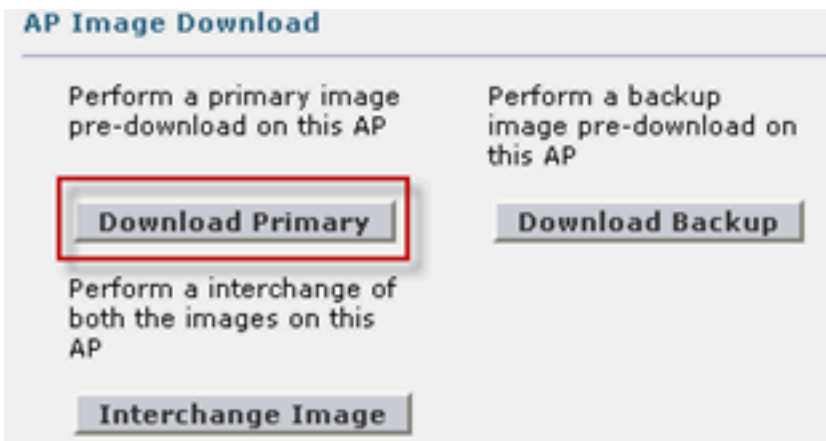
1. Upgradeer het beeld op de primaire en back-upcontrollers. Navigeer onder **WLC GUI > Opdrachten > Downloadbestand** om de download te



The screenshot shows a web form titled "Download file to Controller". It has two main sections: "File Type" and "Transfer Mode" at the top, and "Server Details" below. "File Type" is a dropdown menu set to "Code". "Transfer Mode" is a dropdown menu set to "TFTP". The "Server Details" section contains several fields: "IP Address" (redacted with a black box), "Maximum retries" (input field with "10"), "Timeout (seconds)" (input field with "6"), "File Path" (empty input field), and "File Name" (input field with "AS_5500_7_0_112_52.aes").

starten.

2. Bewaar de configuraties op de controllers, maar start de controller niet opnieuw op.
3. Geef de downloadopdracht AP van de primaire controller uit. Navigeer naar **WLC GUI > Draadloos > Access Point > Alle AP's** en kies het access point om preimage download te starten. Klik op het tabblad **Geavanceerd** als het toegangspunt is geselecteerd. Klik op **Primair downloaden** om preimage te



downloaden.

```
*Sep 13 21:21:14.903: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
Image [REDACTED] not found in flash, predownloading.
examining image...!
extracting info (326 bytes)
Image info:
  Version Suffix: k9w8-.wnbu_j_mr.201009101910
  Image Name: c1250-k9w8-mx.wnbu_j_mr.201009101910
  Version Directory: c1250-k9w8-mx.wnbu_j_mr.201009101910
  Ios Image Size: 5530112
  Total Image Size: 5550592
  Image Feature: WIRELESS LAN|LWAPP
  Image Family: C1250
  Wireless Switch Management Version: [REDACTED]
Extracting files...
c1250-k9w8-mx.wnbu_j_mr.201009101910/ (directory) 0 (bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_1.img (13696 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W5.bin (17372 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9w8-mx.wnbu_j_mr.20100910
1910 (5322509 bytes)!!!!!!
*Sep 13 21:25:43.747: Loading file /c1250-pre [REDACTED].
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/8001.img (172792 bytes)!!!!!!
!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W2.bin (4848 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/info (326 bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_2.img (10880 bytes)!
extracting info.ver (326 bytes)
New software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910
archive download: takes 138 seconds

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

- Herstart de controllers nadat alle AP-afbeeldingen zijn gedownload. AP's vallen nu terug naar Standalone modus tot de controllers herstart. **Opmerking:** In de standalone modus houdt fouttolerantie clients geassocieerd. Als de controller weer is, worden de AP's automatisch opnieuw opgestart met de vooraf gedownload afbeelding. Na het opnieuw opstarten voegen de AP's zich opnieuw bij de primaire controller aan en hervatten de diensten van de klant.

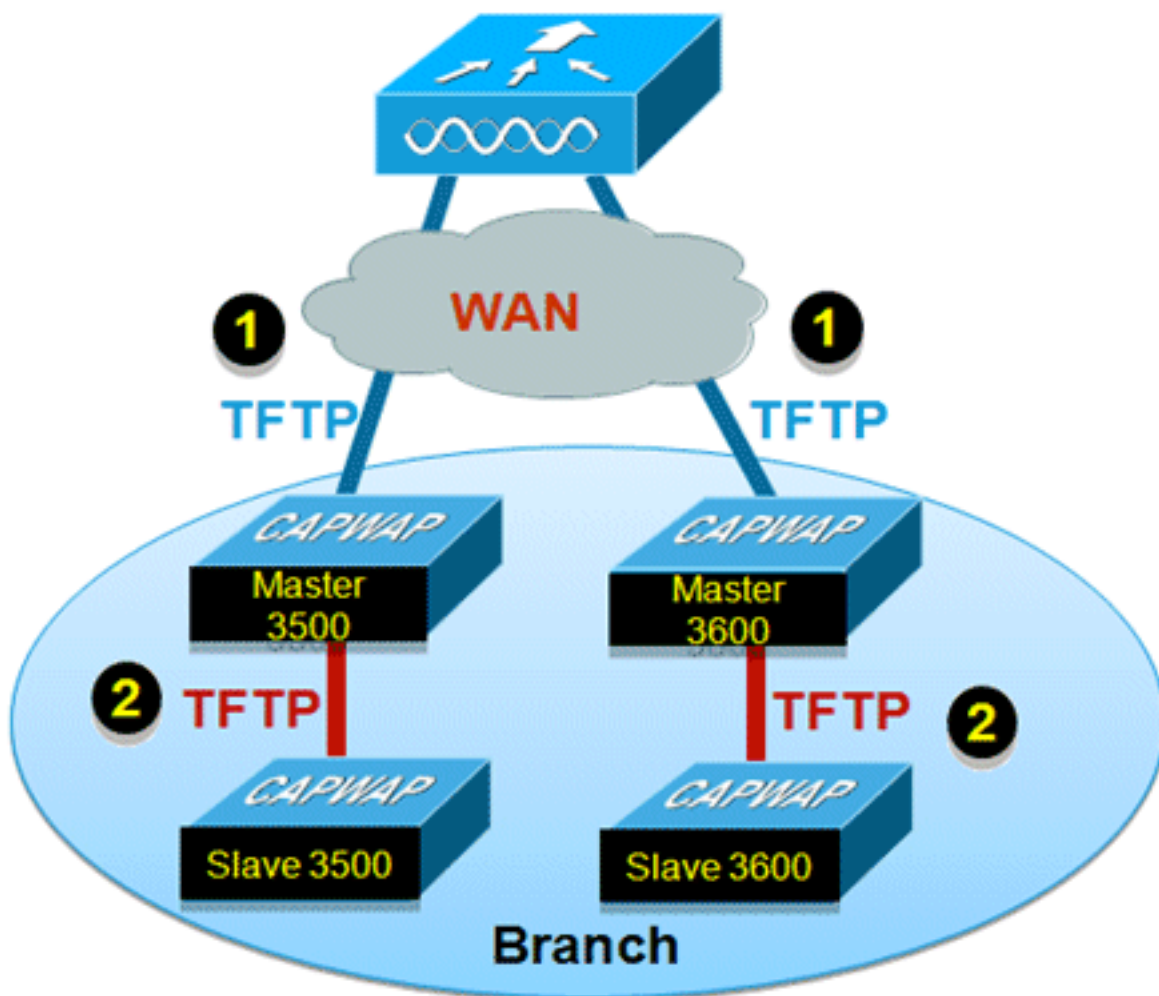
Beperkingen

- Werkt alleen met CAPWAP AP's.

FlexConnect slimme AP-upgrade

De downloadfunctie van pre-image beperkt de downtime-duur tot op zekere hoogte, maar alle FlexConnect APs moeten de respectieve AP-afbeeldingen vooraf downloaden via de WAN-link met een hogere vertraging.

Efficiënt AP beeld upgrade zal de downtime voor elk FlexConnect AP verminderen. Het basisidee is slechts één AP van elk AP-model zal de afbeelding van de controller downloaden en als Master/Server fungeren, en de rest van AP's van hetzelfde model zal als Slave/Client werken en het AP-beeld van de master downloaden. De distributie van AP beeld van de server aan de cliënt zal op een lokaal netwerk zijn en zal niet de latentie van de WAN verbinding ervaren. Als gevolg daarvan zal het proces sneller verlopen.



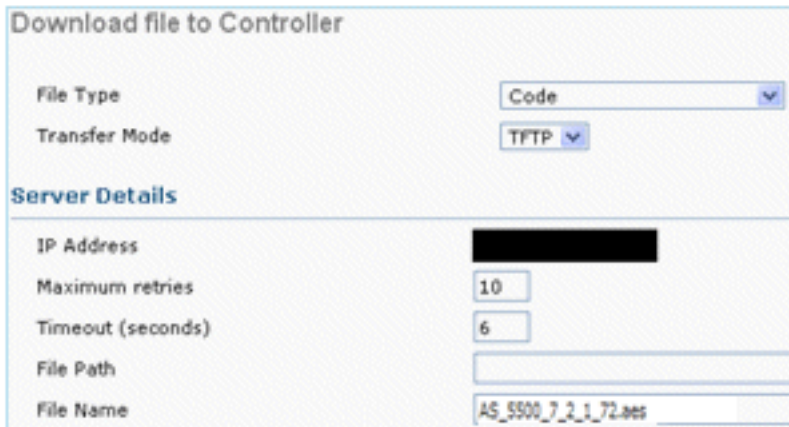
Samenvatting

- APs van het hoofd en van het Slaaf worden geselecteerd voor elk AP Model per FlexConnect Groep
- Afbeelding van hoofddownloads van WLC
- Afbeelding van Master AP downloaden
- Vermindert downtime en slaat WAN-bandbreedte op

Procedure

Voer de volgende stappen uit:

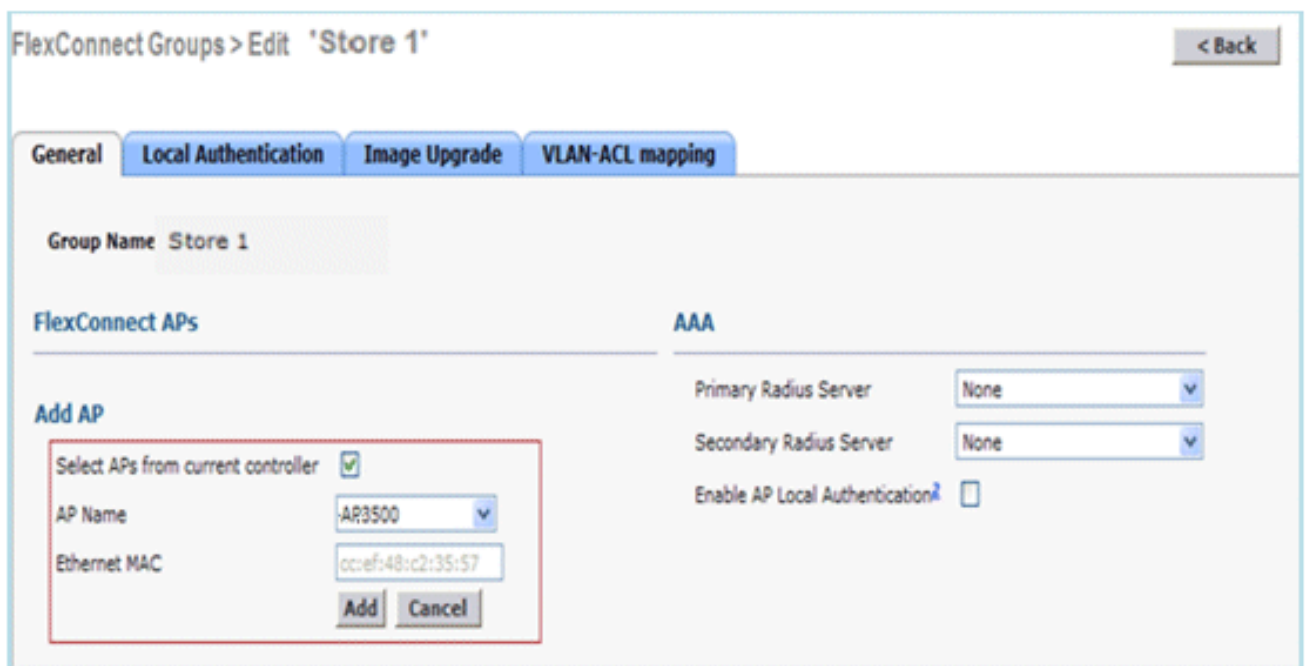
1. upgrade van de afbeelding op de controller. Navigeer naar **WLC GUI > Opdrachten > Downloadbestand** om de download te



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

starten.

2. Bewaar de configuraties op de controllers, maar start de controller niet opnieuw op.
3. Voeg de FlexConnect APs aan FlexConnect groep toe. Blader naar **WLC GUI > Draadloos > FlexConnect groepen > selecteer FlexConnect Group > tabblad General > Add AP**.



FlexConnect Groups > Edit 'Store 1'	
Group Name Store 1	
FlexConnect APs	
Add AP	
Select APs from current controller	<input checked="" type="checkbox"/>
AP Name	AR3500
Ethernet MAC	00ef:48:c2:35:57
Add Cancel	
AAA	
Primary Radius Server	None
Secondary Radius Server	None
Enable AP Local Authentication	<input type="checkbox"/>

4. Klik op het selectieteken **FlexConnect AP Upgrade** om een efficiënte AP-beeldupgrade te bereiken. Navigeer naar **WLC GUI > Draadloos > FlexConnect Groepen > selecteer FlexConnect Group > tabblad Afbeelding upgrade**.

FlexConnect Groups > 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

FlexConnect AP Upgrade

FlexConnect Master APs

AP Name AP3500

Add Master

Master AP Name	AP Model	Manual

5. U kunt het Master AP handmatig of automatisch selecteren: Als u de Master AP handmatig wilt selecteren, navigeer dan naar WLC GUI > Wireless > FlexConnect Groepen > selecteer FlexConnect Group > Image Upgrade tab > FlexConnect Master AP, selecteer AP van de vervolgkeuzelijst en klik op **Add Master**.

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

FlexConnect AP Upgrade

Slave Maximum Retry Count 44

Upgrade Image Backup FlexConnect Upgrade

FlexConnect Master APs

AP Name AR3500

Add Master

Master AP Name	AP Model	Manual
AP3500	c3500I	yes

Opmerking: slechts één AP per model kan als Master AP worden geconfigureerd. Als Master AP handmatig is ingesteld, wordt het veld Handmatig ja bijgewerkt. Als u automatisch Master AP wilt selecteren, navigeer dan naar WLC GUI > Draadloos > FlexConnect-groepen > FlexConnect-groep > tabblad Image Upgrade en klik op FlexConnect-upgrade.

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

FlexConnect AP Upgrade

Slave Maximum Retry Count

Upgrade Image

FlexConnect Master APs

AP Name

Master AP Name	AP Model	Manual
AP3500-1	c3500I	no

N.B.: Als Master AP automatisch is geselecteerd, wordt het veld Handmatig **zonder** wachtwoord bijgewerkt.

- Om een efficiënte AP-beeldupgrade te starten voor alle AP's onder een specifieke FlexConnect-groep, klikt u op **FlexConnect-upgrade**. Navigeer naar **WLC GUI > Draadloos > FlexConnect groepen > selecteer FlexConnect groep > tabblad Afbeelding upgrade** en klik op **FlexConnect upgrade**.

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

FlexConnect AP Upgrade

Slave Maximum Retry Count

Upgrade Image

Opmerking: Maximale aantal opnieuw proberen is het aantal pogingen (44 standaard) waarin slaaf AP zich ontwikkelt om een afbeelding te downloaden van de Master AP, waarna het neervalt om de afbeelding te downloaden van de WLC. Er worden 20 pogingen tegen WLC ondernomen om een nieuwe afbeelding te downloaden, waarna de beheerder het downloadproces opnieuw moet starten.

- Wanneer de upgrade van FlexConnect is gestart, kan alleen de Master AP de afbeelding van de WLC downloaden. Onder All AP pagina, zal "**Upgrade role**" worden bijgewerkt als **Master/Central** wat betekent dat Master AP het beeld van de WLC heeft gedownload die op de centrale plaats is. AP Slave zal het beeld van Master AP downloaden dat op de lokale site is en de reden onder Alle AP pagina "**Upgraderol**" is zal als **Slave/Local** worden bijgewerkt. Om dit te verifiëren, navigeer naar **WLC GUI > Draadloos**.

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. Herstart de controllers nadat alle AP-afbeeldingen zijn gedownload. APs vallen nu terug naar Standalone modus tot de controllers herstart. **Opmerking:** In de standalone modus houdt fouttolerantie clients geassocieerd. Als de controller weer is, worden de AP's automatisch opnieuw opgestart met de vooraf gedownload afbeelding. Na het opnieuw opstarten voegen de AP's zich opnieuw bij de primaire controller aan en hervatten de diensten van de klant.

Beperkingen

- De selectie van Master AP is per FlexConnect groep en per AP model in elke groep.
- Slechts 3 slave AP's van het zelfde model kunnen gelijktijdig van hun hoofdAP en de rest van de slaaf AP's gebruiken de willekeurige terug-off timer om voor de Master AP opnieuw te proberen om het AP beeld te downloaden.
- In het geval dat AP Slave het beeld om één of andere reden niet van de Masterplaats kan downloaden AP, zal het naar de WLC gaan om de nieuwe afbeelding te halen.
- Dit werkt alleen met CAPWAP AP's.

Auto-converteren APs in FlexConnect-modus

Flex 7500 biedt deze twee opties om de AP-modus te converteren naar FlexConnect:

- Handmatige modus
- Auto converteren

Handmatige modus

Deze modus is beschikbaar op alle platforms en maakt het mogelijk dat de wijziging alleen per AP-basis plaatsvindt.

1. Navigeer naar **WLC GUI > Draadloos > Alle AP** en kies AP.
2. Selecteer **FlexConnect** als de AP-modus en klik vervolgens op **Toepassen**.
3. Door het wijzigen van de AP-modus wordt de AP opnieuw

All APs > Details for AP3500

General	Credentials	Interfaces	High Availability
General			
AP Name	AP3500		
Location	default location		
AP MAC Address	00:22:90:e3:37:df		
Base Radio MAC	00:22:bd:d1:71:30		
Admin Status	Disable ▼		
AP Mode	local ▼		
AP Sub Mode	local FlexConnect monitor Rogue Detector Sniffer Bridge SE-Connect		
Operational Status			
Port Number			
Venue Group			

opgestart.

De

ze optie is ook beschikbaar op alle huidige WLC-platforms.

Auto-conversiemodus

Deze modus is alleen beschikbaar voor de Flex 7500 controller en wordt alleen ondersteund met CLI. Deze modus activeert de wijziging op alle aangesloten AP's. Het wordt aanbevolen Flex 7500 toe te passen op een ander mobiliteitsdomein dan de bestaande WLC campus controllers voordat u deze CLI instelt:

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

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

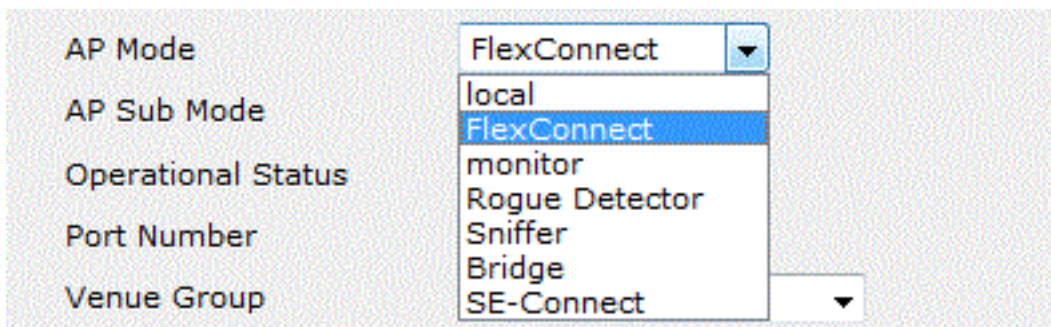
```
(Cisco Controller) >
```

1. De optie Auto-conversie is standaard uitgeschakeld. Dit kan worden geverifieerd door gebruik te maken van deze opdracht **show**:

```
(Cisco Controller) >show ap autoconvert
```

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

Niet-ondersteunde AP-modi = lokale modus, Snijkop, Ruggendetector en



Bridge. Deze optie is momenteel alleen beschikbaar via CLI's. Deze CLI's zijn alleen beschikbaar op de WLC 7500.

2. Het uitvoeren van een configuratiescherm om flexconnect CLI te converteren zet alle APs in het netwerk om met niet-ondersteunde AP-modus naar FlexConnect-modus. APs die reeds in FlexConnect of de Beeldmodus zijn beïnvloed niet.

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

```
(Cisco Controller) >show ap autoconvert
```

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

```
(Cisco Controller) >
```

3. Het uitvoeren van de configuratie optie autoconverteert monitor CLI alle APs in het netwerk met niet-ondersteunde AP modus om wijze te controleren. APs die reeds in FlexConnect of de monitor modus zijn niet beïnvloed.

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

```
(Cisco Controller) >show ap autoconvert
```

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

Er is geen optie om zowel configuratie ap autoconversie en configuratie ap tegelijkertijd monitor tegelijkertijd te uitvoeren.

Ondersteuning van FlexConnect WGB/WGB voor lokale switching WLAN's

Vanaf release 7.3 worden WGB/WGB en bekabelde/draadloze klanten achter WGB's ondersteund en zullen zij als normale klanten werken op WLAN's die zijn geconfigureerd voor lokale switching.

Na associatie stuurt WGB de IAPP-berichten voor elk van de bekabelde/draadloze clients en Flex AP zich als volgt te gedragen:

- Wanneer Flex AP in verbonden modus is, verstuurt het alle IAPP-berichten naar de controller en de controller verwerkt de IAPP-berichten op dezelfde manier als de lokale modus AP. Het verkeer voor bekabelde/draadloze klanten zal lokaal van Flex APs worden geschakeld.
- Wanneer AP in standalone modus is, verwerkt het de IAPP berichten, bedrade/draadloze cliënten op de WGB moeten kunnen registreren en deregistreren. Na de overgang naar de verbonden modus, stuurt Flex AP de informatie van de bekabelde klanten terug naar de controller. WGB stuurt drie keer registratieberichten wanneer Flex AP overschakelt van Standalone naar Connected Mode.

Draadloos/draadloos klanten zullen de configuratie van WGB erven, wat betekent dat geen

afzonderlijke configuratie zoals AAA-verificatie, AAA-opheffing en FlexConnect ACL vereist is voor klanten achter WGB.



Samenvatting

- Er is geen speciale configuratie vereist voor WLC om WGB op Flex AP te ondersteunen.
- Foutentolerantie wordt ondersteund voor WGB en klanten achter WGB.
- WGB wordt ondersteund op een IOS AP: 1240, 1130, 1140, 1260 en 1250.

Procedure

Voer de volgende stappen uit:

1. Er is geen speciale configuratie nodig om WGB/uWGB-ondersteuning op FlexConnect APs mogelijk te maken voor WLAN's die zijn geconfigureerd voor lokale switching als WGB. Ook worden klanten achter WGB behandeld als normale cliënten op lokale, switched WLAN's door Flex AP's. Schakel **FlexConnect Local Switching** in op een WLAN.

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 IPv6

P2P Blocking Action

Client Exclusion Enabled
Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

Clear HotSpot Configuration Enabled

FlexConnect

FlexConnect Local Switching Enabled

2. Stel AP Mode in op

All APs > Details for AP_3500E

General Credentials Interfaces High Availability

General

AP Name AP_3500E

Location

AP MAC Address 04:7d:4f:3a:07:74

Base Radio MAC 04:7d:4f:53:24:e0

Admin Status Enable

AP Mode FlexConnect

AP Sub Mode

Operational Status

Port Number

Venue Group

local
FlexConnect
monitor
Rogue Detector
Sniffer
Bridge
SE-Connect

FlexConnect.

3. Associeer WGB met bekabelde klanten achter deze geconfigureerde WLAN.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Clients

Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	Protocol	Status	Auth	Port	WGB
00:40:96:b8:d4:be	AP_3500E	*Store 1*	*Store 1*	N/A	Associated	Yes	1	No
00:50:b6:09:e5:3b	AP_3500E	*Store 1*	*Store 1*	N/A	Associated	Yes	1	No
04:7d:4f:3a:08:10	AP_3500E	*Store 1*	*Store 1*	802.11an	Associated	Yes	1	Yes

4. Ga om de gegevens voor WGB te controleren naar **monitor > Clients** en selecteer **WGB** in de lijst met klanten.

Clients > Detail

Client Properties		AP Properties	
MAC Address	04:7d:4f:3a:08:10	AP Address	04:7d: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 Authentication	Open System
		Reason Code	1
		Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
Client Type	WGB		
Number of Wired Client(s)	2		

5. Ga naar **monitor > Clients** en selecteer de client voor controle van de details van de bekabelde/draadloze clients achter WGB.

Clients > Detail

Client Properties		AP Properties	
MAC Address	00:50:b6:09:e5:3b	AP Address	04:7d:4f:53:24:e0
IPv4 Address	96.63.100	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
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
Client Type	WGB Client		
WGB MAC Address	04:7d:4f:3a:08:10		

Beperkingen

- Draadloze klanten achter WGB zullen altijd op hetzelfde VLAN zijn als WGN zelf. Ondersteuning van meerdere VLAN's voor klanten achter WGB wordt niet ondersteund op Flex AP voor WLAN's die zijn geconfigureerd voor lokale switching.
- Een maximum van 20 klanten (bekabeld/draadloos) wordt ondersteund achter WGB wanneer deze gekoppeld wordt aan Flex AP op WLAN ingesteld voor lokale switching. Dit getal is hetzelfde als wat we vandaag hebben voor WGB-ondersteuning in lokale modus AP.

- Web Auth wordt niet ondersteund voor klanten achter WGB dat is gekoppeld aan WLAN's die zijn geconfigureerd voor lokale switching.

Ondersteuning voor een groter aantal radiogasers

Voorafgaand aan release 7.4 werd de configuratie van RADIUS-servers in de FlexConnect-groep uitgevoerd vanaf een globale lijst met RADIUS-servers op de controller. Het maximale aantal RADIUS-servers dat in deze globale lijst kan worden ingesteld, is 17. Met een toenemend aantal bijkantoren is het een vereiste om een RADIUS-server per locatie te kunnen configureren. Vanaf release 7.4 kunnen primaire en back-up RADIUS-servers worden configureren per FlexConnect-groep die al dan niet deel kan uitmaken van de globale lijst van 17 RADIUS-verificatieservers die zijn ingesteld op de controller.

Ook een AP-specifieke configuratie voor de RADIUS-servers wordt ondersteund. De AP-specifieke configuratie zal een grotere prioriteit hebben dan de FlexConnect groepsconfiguratie.

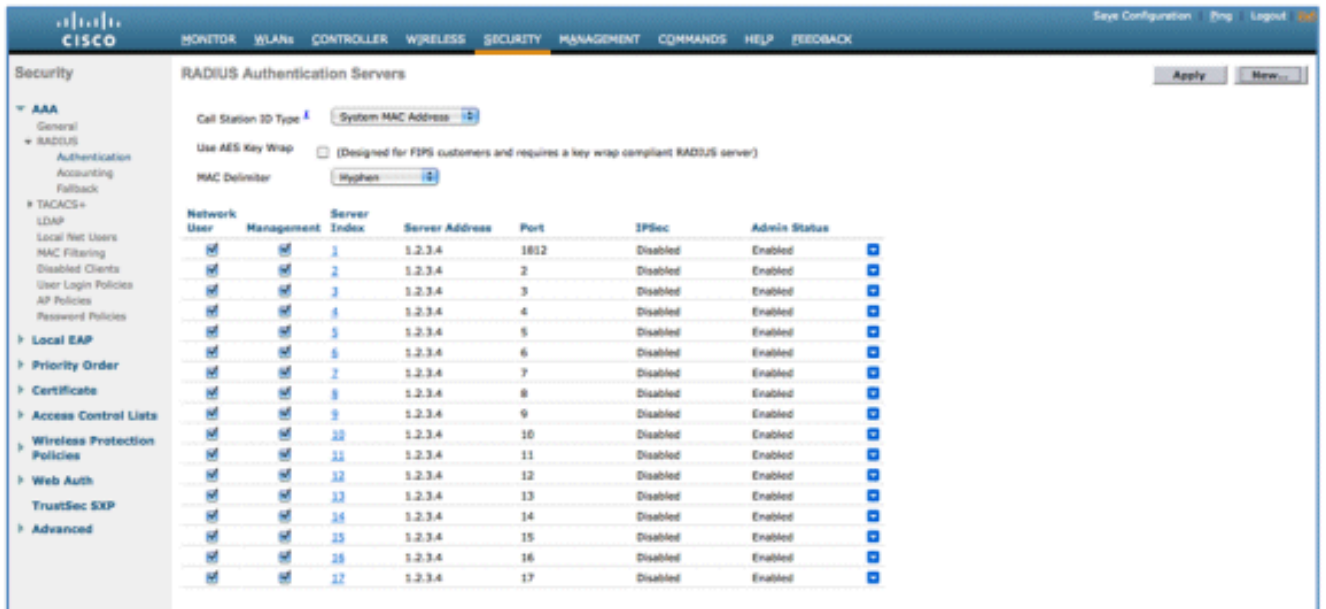
De bestaande configuratieopdracht in de FlexConnect Group, die de index van de RADIUS-server in de globale RADIUS-serverlijst van de controller nodig heeft, wordt afgekeurd en vervangen door een configuratieopdracht, die een RADIUS-server in de Flexconnect-groep vormt met behulp van het IP-adres van de server en gedeeld geheim.

Samenvatting

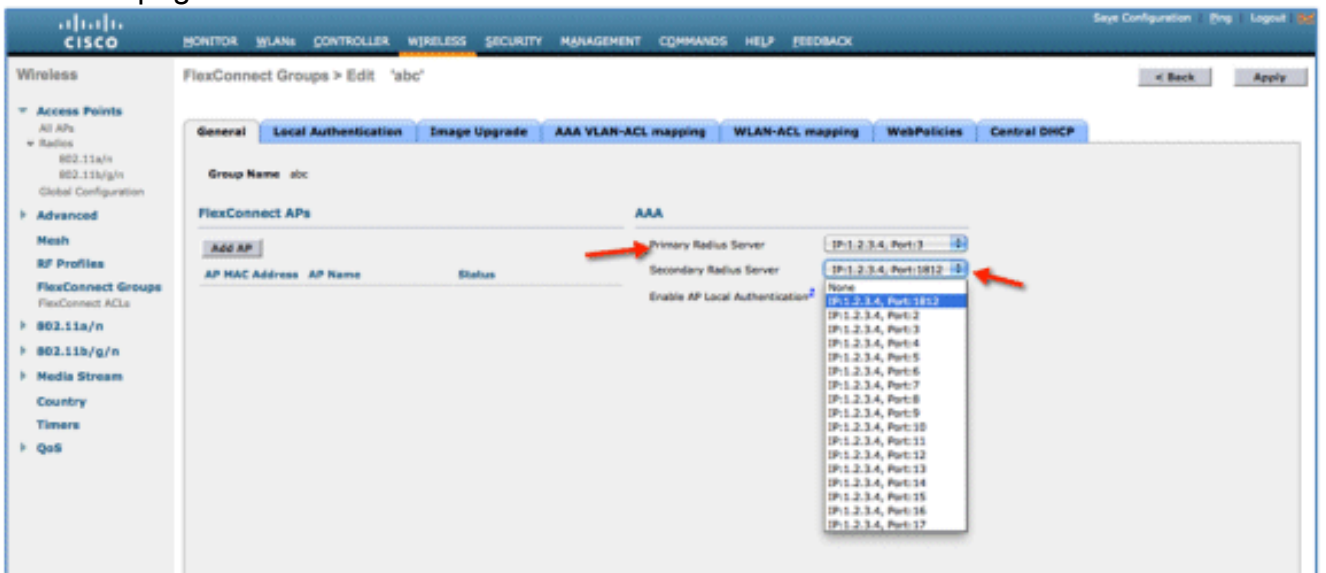
- Ondersteuning voor configuratie van primaire en back-up RADIUS-servers per FlexConnect-groep, die al dan niet aanwezig kan zijn in de globale lijst van RADIUS-verificatieservers.
- Het maximale aantal unieke RADIUS-servers dat op een WLC kan worden toegevoegd, is het aantal FlexConnect-groepen dat op een bepaald platform tweemaal kan worden ingesteld. Een voorbeeld is één primaire en één secundaire RADIUS-server per FlexConnect groep.
- De software upgrade van een vorige release naar release 7.4 veroorzaakt geen verlies van de RADIUS-configuratie.
- Het wissen van de primaire RADIUS-server is toegestaan zonder dat de secundaire RADIUS-server moet worden verwijderd. Dit is consistent met de huidige FlexConnect groepsconfiguratie voor de RADIUS-server.

Procedure

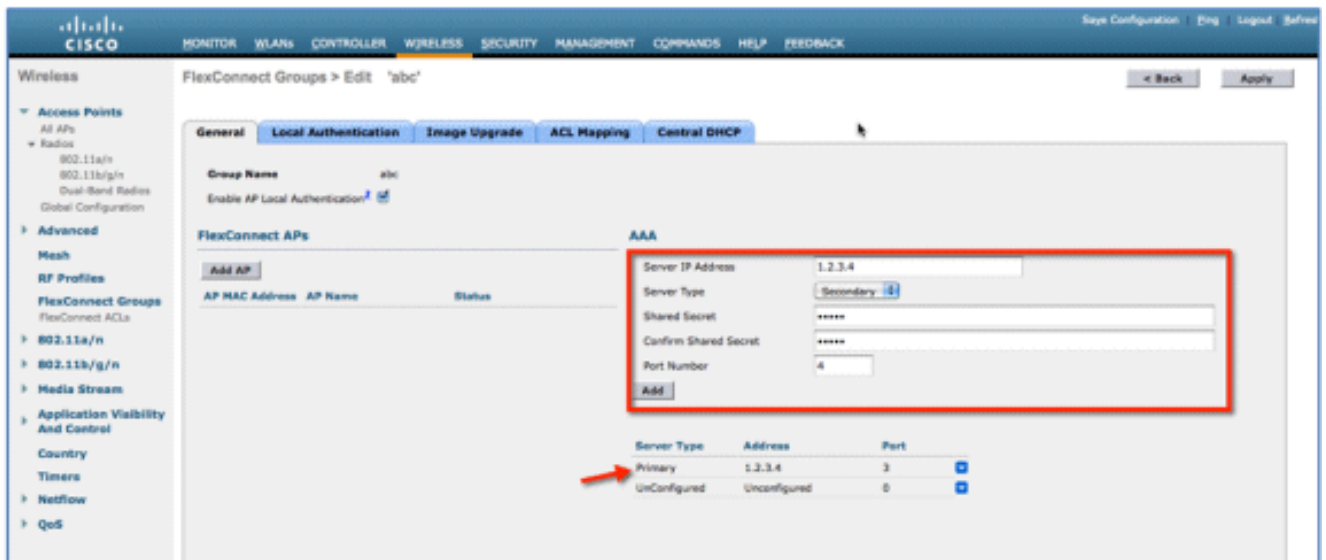
1. Configuratie voorafgaand aan release 7.4. U kunt maximaal 17 RADIUS-servers configureren onder de AAA-verificatieconfiguratie.



2. Primaire en secundaire RADIUS-servers kunnen worden gekoppeld aan een FlexConnect-groep met behulp van een vervolgkeuzelijst met RADIUS-servers die zijn geconfigureerd op de AAA-verificatiepagina.



3. Configuratie bij FlexConnect Group in release 7.4. Primaire en secundaire RADIUS-servers kunnen onder de FlexConnect-groep worden geconfigureerd met behulp van een IP-adres, poortnummer en gedeeld geheim.



Beperkingen

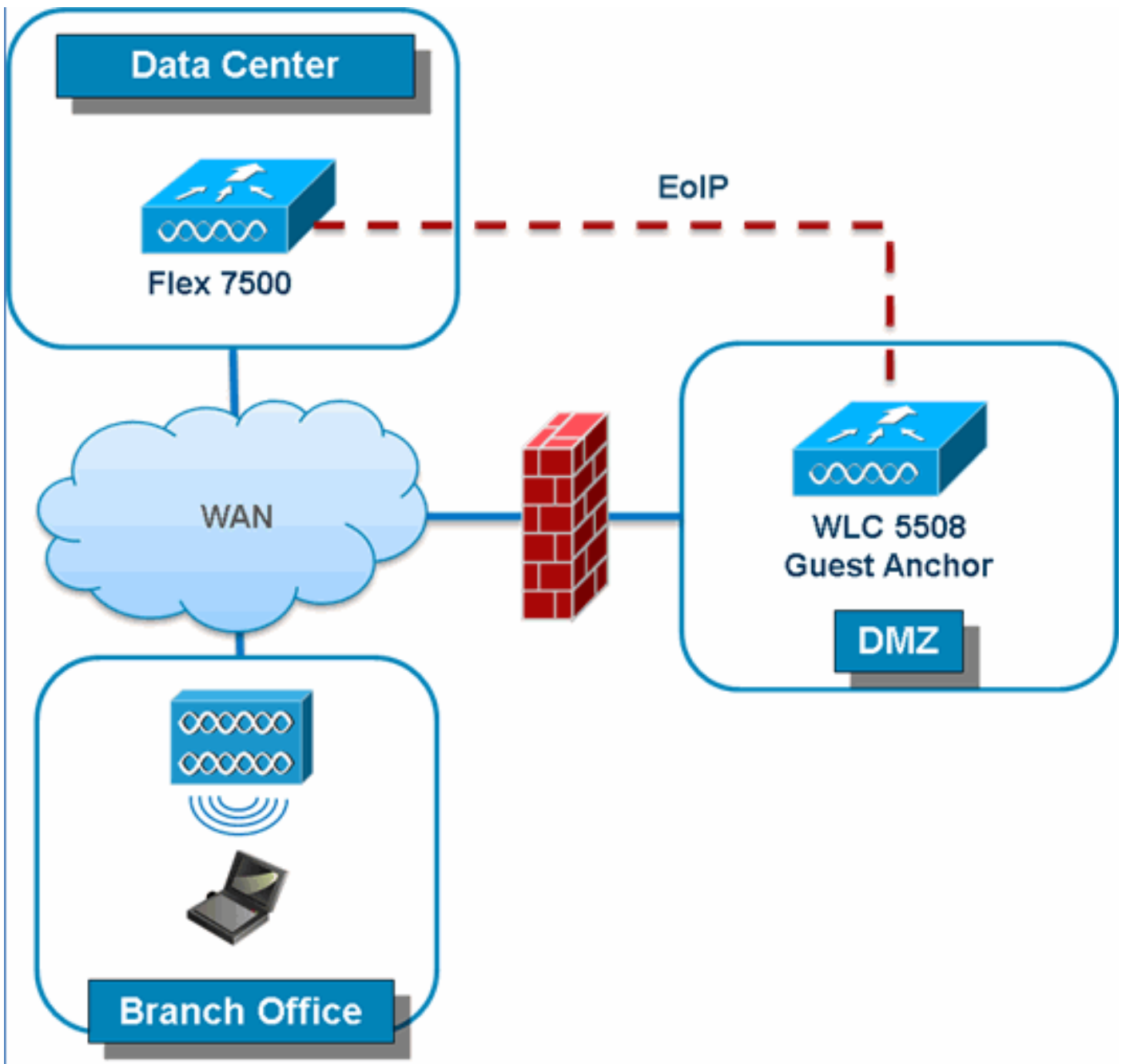
- Software-upgrade van release 7.4 naar een vorige release behoudt de configuratie maar met enkele beperkingen.
- Het configureren van een primaire/secundaire RADIUS-server wanneer een vorige wordt geconfigureerd zal ervoor zorgen dat de oudere ingang door de nieuwe wordt vervangen.

Uitgebreide lokale modus (ELM)

ELM wordt ondersteund op de FlexConnect-oplossing. Raadpleeg de handleiding voor beste praktijken bij ELM voor meer informatie.

Gast access ondersteuning in Flex 7500

Afbeelding 13: Gast access ondersteuning in Flex 7500



Flex 7500 biedt ondersteuning voor het maken van EoIP-tunnels voor uw gastpresentator in DMZ. Raadpleeg de Gastimplementatiegids voor beste praktijken voor de oplossing voor draadloze toegang.

[WLC 7500 beheren vanuit NCS](#)

Het beheer van de WLC 7500 van het NCS is identiek aan de bestaande WLCs van Cisco.

Monitor ▾ Reports ▾ Configure ▾ Services ▾

Add Controllers

Configure > Controllers > Add Controllers

General Parameters

Add Format Type: Device Info ▾

IP Addresses: **WLC 7500 IP Address**

Network Mask: 255.255.255.0

Verify Telnet/SSH Capabilities ⓘ

SNMP Parameters ⓘ

Version: v2c ▾

Retries: 2

Timeout: 10 (secs)

Community: private

Telnet/SSH Parameters ⓘ

User Name: admin

Password: ●●●●●●

Confirm Password: ●●●●●●

Retries: 3

Timeout: 60 (secs)

OK Cancel

Controllers -- Select a command --

Configure > Controllers

<input type="checkbox"/>	IP Address	Controller Name	Type	Location	Software Version	Mobility Group Name	Reachability Status	Audit Status
<input type="checkbox"/>	172.20.227.174 ⓘ	Ambassador	7500		7.0.112.62	mobility	Reachable	Identical
<input type="checkbox"/>	172.20.227.172 ⓘ	5508-Primary	5500		7.0.112.52	mobility	Reachable	Identical

Entries 1
1 2 3 4

Raadpleeg de [Cisco Configuration Guide](#) voor draadloos controlesysteem, [release 7.0.172.0](#) voor meer informatie over het beheer van [WLC en het ontdekken van sjablonen](#).

FAQ

Vraag Als ik LAP's op een afgelegen locatie configureren als FlexConnect, kan ik deze LAP's dan een primaire en secundaire controller geven?

Voorbeeld: Er is een primaire controller op site A en een secundaire controller op site B. Als de controller op site A faalt, overslaat de LAP op de controller op site B. Als beide controllers niet beschikbaar zijn, valt de LAP in de standalone FlexConnect-modus?

A. Ja. Ten eerste faalt de LAP bij de tweede. Alle WLAN's die lokaal worden geschakeld, hebben geen wijzigingen. Bij alle WLAN's die centraal worden geschakeld, wordt het verkeer alleen naar de nieuwe controller verplaatst. En als het secundaire FALSE mislukt, blijven alle WLAN's die

gemarkeerd zijn voor lokale switching (en open/vooraf gedeelde belangrijke authenticatie/u doet AP-authenticator) omhoog.

Vraag Hoe gaan toegangspunten die in lokale modus zijn ingesteld om met WLAN's die zijn geconfigureerd met FlexConnect Local Switching?

A. Local mode access points behandelen deze WLAN's als normale WLAN's. Verificatie en gegevensverkeer worden teruggezet naar de WLC. Tijdens een WAN-koppelingsfout is deze WLAN volledig uitgeschakeld en zijn geen klanten actief op deze WLAN totdat de verbinding met de WLC wordt hersteld.

Vraag Kan ik web authenticatie doen met lokale switching?

A. Ja, u kunt een SSID hebben met Web-Verificatie toegelaten en het verkeer plaatselijk na web-authenticatie laten vallen. Webverificatie met lokale switching werkt prima.

Vraag Kan ik mijn Guest-Portal op de controller voor een SSID gebruiken, dat lokaal wordt verwerkt door de H REAP? Zo ja, wat gebeurt er als ik de verbinding met de controller verlies? Dalen de huidige klanten onmiddellijk?

A. Ja. Aangezien deze WLAN lokaal is ingeschakeld, is de WLAN beschikbaar maar geen nieuwe klanten kunnen authenticeren omdat de webpagina niet beschikbaar is. Maar de bestaande klanten worden niet afgezet.

Vraag Kan FlexConnect PCI-conformiteit bevestigen?

A. Ja. FlexConnect-oplossing ondersteunt schurkendetectie om PCI-overeenstemming te bereiken.

Gerelateerde informatie

- [Ontwerpgids en implementatie van HREAP](#)
- [Cisco 4400 Series draadloze LAN-controllers](#)
- [Cisco 2000 Series draadloze LAN-controllers](#)
- [Cisco draadloos beheersysteem](#)
- [Cisco 3300 Series Mobility Services Engine](#)
- [Cisco Aironet 3500 Series](#)
- [Cisco Secure Access Control-systeem](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)