

&Configuratie van de 9800 WLC-integratie met Aruba ClearPass - Dot1x FlexConnect voor implementatie van vestigingen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Traffic Flow](#)

[Netwerkdigram](#)

[De Catalyst 9800 draadloze controller configureren](#)

[C9800 - AAA-parameters configureren voor dot1x](#)

[C9800 - Het 'Corp' WLAN-profiel configureren](#)

[C9800 - Beleidsprofiel configureren](#)

[C9800 - Beleidsmarkering configureren](#)

[C9800 - Profiel voor AP Join](#)

[C9800 - Flex profiel](#)

[C9800 - Sitetag](#)

[C9800 - RF-tag](#)

[C9800 - Tags toewijzen aan AP](#)

[Aruba CPPM configureren](#)

[Eerste configuratie van Aruba ClearPass Policy Manager-server](#)

[Licenties toepassen](#)

[De C9800 draadloze controller toevoegen als netwerkapparaat](#)

[CPPM configureren om Windows AD als verificatiebron te gebruiken](#)

[CPPM Dot1X-verificatieservice configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de integratie van de Catalyst 9800 draadloze controller met Aruba ClearPass Policy Manager (CPPM) en Microsoft Active Directory (AD) om dot1x-verificatie te leveren aan draadloze clients in een Flexconnect-implementatie.

Voorwaarden

Vereisten

Cisco raadt aan dat u kennis hebt van deze onderwerpen en dat deze zijn geconfigureerd en geverifieerd:

- Catalyst 9800 draadloze controller
- Aruba ClearPass Server (vereist platformlicentie, toegangslicentie, on-board licentie)
- Operationele Windows AD
- Optionele certificeringsinstantie (CA)
- Operationele DHCP-server
- Operationele DNS-server (vereist voor certificaat-CRL-validatie)
- ESX.i
- Alle relevante componenten worden gesynchroniseerd met NTP en geverifieerd om de juiste tijd te hebben (vereist voor certificaatvalidatie)
- Kennis van onderwerpen: C9800 implementatie- en nieuwe Config-modelFlexConnect-handeling op C980 Dot1x-verificatie

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

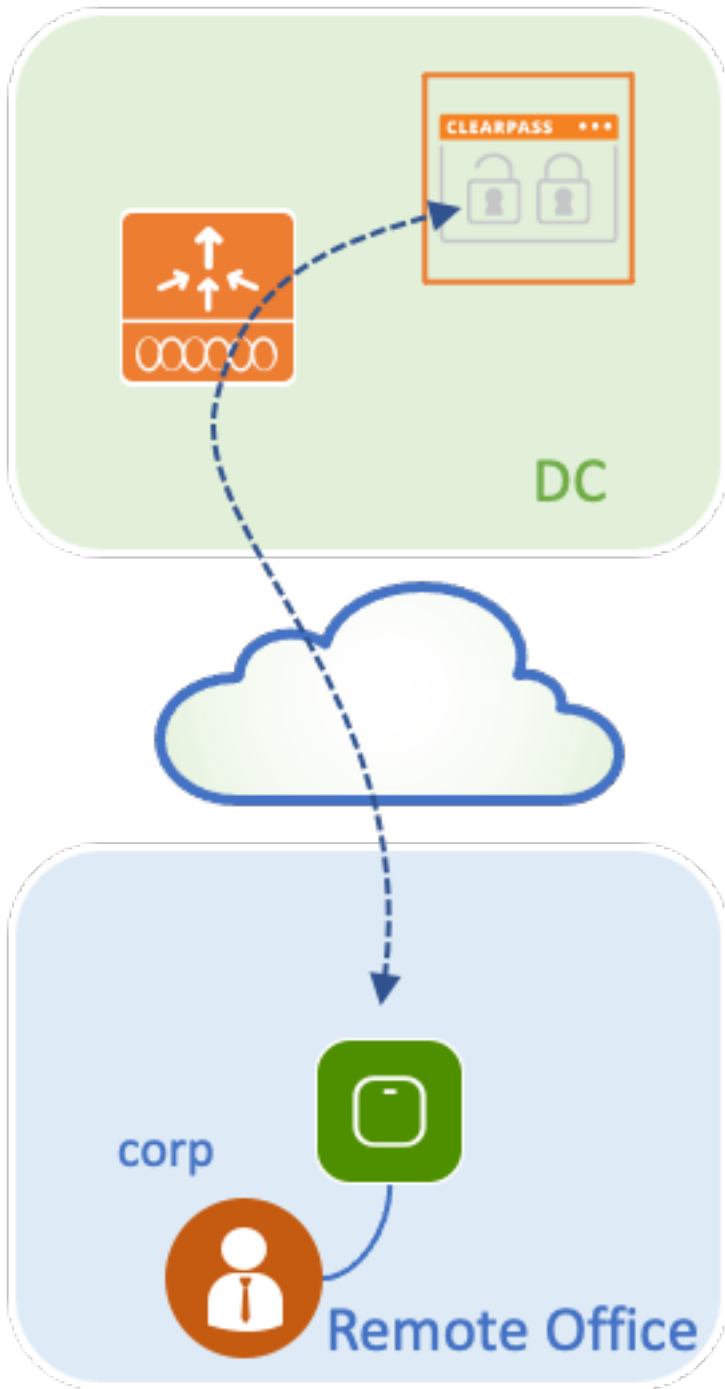
- C980-L-C Cisco IOS-XE 17.3.3
- C9130AXE, 4800 access points
- Aruba ClearPass, 6-8-0-109592 en 6.8-3 patch
- MS Windows-server Active Directory (GP geconfigureerd voor geautomatiseerde op machine gebaseerde afgifte van cert naar beheerde endpoints)DHCP-server met optie 43 en optie 60DNS-serverNTP-server om alle componenten te synchroniserenCA

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

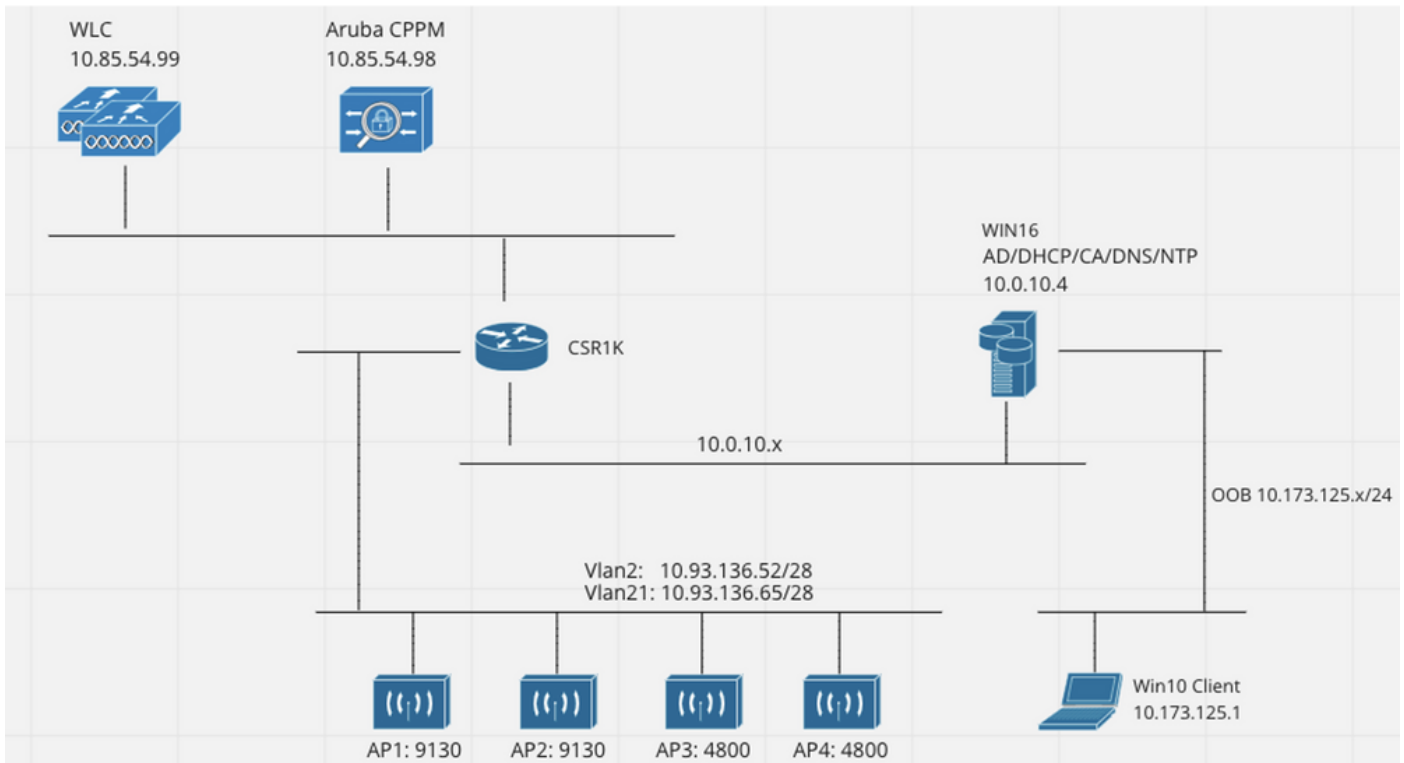
Achtergrondinformatie

Traffic Flow

In een typische bedrijfsplaatsing met meerdere bijkantoren, wordt elk bijkantoor opgericht om dot1x toegang tot de collectieve werknemers te verlenen. In dit configuratievoorbeeld wordt PEAP gebruikt om zakelijke gebruikers via een ClearPass-instantie in het centrale datacenter (DC) dot1x-toegang te bieden. Machinecertificaten worden gebruikt in combinatie met een onderzoek van de werknemersreferenties ten aanzien van een Microsoft AD server.

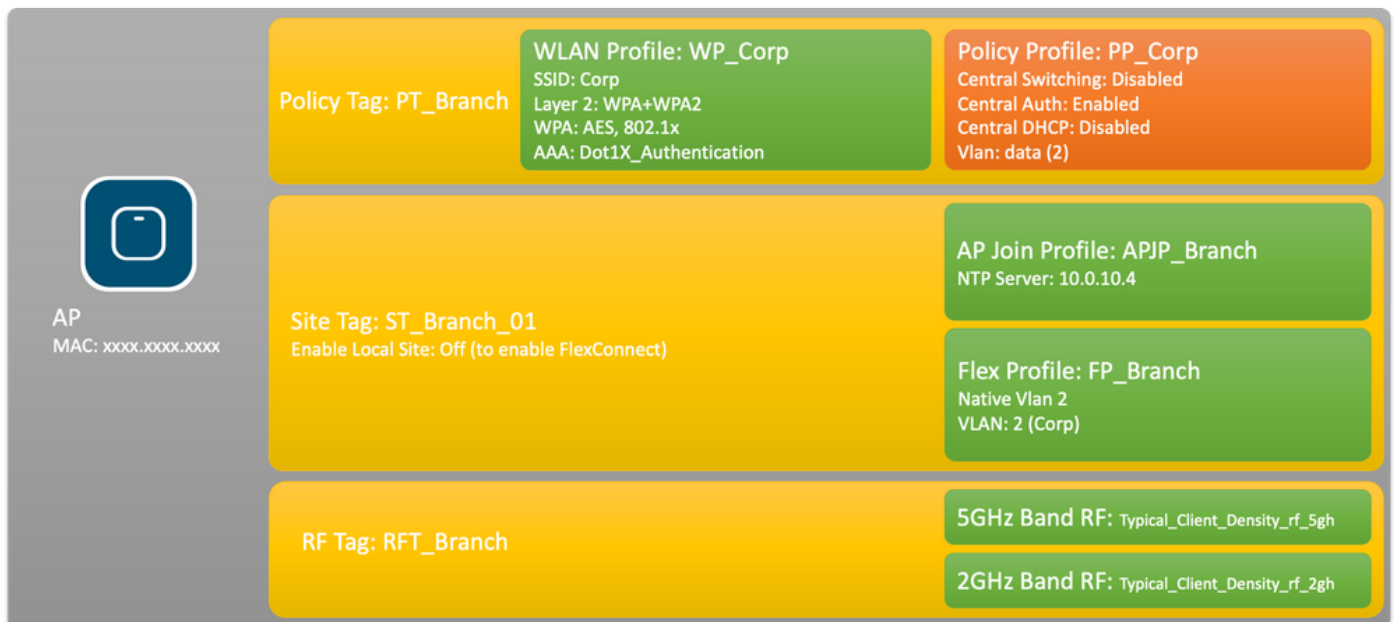


Netzwerkdiagramm



De Catalyst 9800 draadloze controller configureren

In dit configuratievoorbeeld wordt het nieuwe configuratiemodel op C9800 gebruikt om de benodigde profielen en tags te maken voor dot1x Corporate Access naar de bedrijfsonderdelen. De resulterende configuratie wordt in het diagram samengevat.



C9800 - AAA-parameters configureren voor dot1x

Stap 1. Voeg de Aruba ClearPass Policy Manager 'Corp'-server toe aan de 9800 WLC-configuratie. Navigeer naar **Configuratie > Beveiliging > AAA > servers/groepen > RADIUS > servers**. Klik op **+Add** en voer de RADIUS-serverinformatie in. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

Create AAA Radius Server ✕

Name*	<input type="text" value="CPPM_Corp"/>
Server Address*	<input type="text" value="10.85.54.97"/>
PAC Key	<input type="checkbox"/>
Key Type	<input type="text" value="Clear Text"/>
Key* ⓘ	<input type="text" value="....."/>
Confirm Key*	<input type="text" value="....."/>
Auth Port	<input type="text" value="1812"/>
Acct Port	<input type="text" value="1813"/>
Server Timeout (seconds)	<input type="text" value="5"/>
Retry Count	<input type="text" value="3"/>
Support for CoA	<input checked="" type="checkbox"/> ENABLED

Stap 2. Definieer AAA-servergroep voor zakelijke gebruikers. Navigeer naar **Configuratie > Beveiliging > AAA > Servers/groepen > RADIUS > Groepen** en klik op **+Add**, voer de naam van de RADIUS-servergroep in en wijs de RADIUS-serverinformatie toe. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

Create AAA Radius Server Group ✕

Name*	AAA_Group_Corp
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	5
Source Interface VLAN ID	none

Available Servers		Assigned Servers
CPPM_Guest	>	CPPM_Corp
	<	
	>>	
	<<	

↶ Cancel Apply to Device

Stap 3. Definieer de dot1x-verificatiemethode voor zakelijke gebruikers. Navigeer naar **Configuratie > Beveiliging > AAA > AAA-methodelijst > Verificatie** en klik op **+Add**. Selecteer **Type dot1x** in het vervolgkeuzemenu. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

Quick Setup: AAA Authentication



Method List Name*

Dot1X_Authentication

Type*

dot1x



Group Type

group



Fallback to local

Available Server Groups

radius
ldap
tacacs+
WLC_Tacacs_Servers
AAA_Group_Guest



Assigned Server Groups

AAA_Group_Corp



Cancel

Apply to Device

C9800 - Het 'Corp' WLAN-profiel configureren

Stap 1. Navigeer naar **Configuration > Tags en profielen > Draadloos** en klik op **+Add**. Voer een profielnaam, de SSID 'Corp' en een WLAN-id in die nog niet in gebruik is.

Add WLAN



General

Security

Advanced

Profile Name*

WP_Corp

Radio Policy

All

SSID*

Corp

Broadcast SSID

ENABLED



WLAN ID*

3

Status

ENABLED



Cancel

Apply to Device

Stap 2. Navigeer naar het tabblad **Beveiliging** en het subtabblad **Layer 2**. U hoeft de standaardparameters voor dit configuratievoorbeeld niet te wijzigen.

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Auth Key Mgmt 802.1x
 PSK
 CCKM
 FT + 802.1x
 FT + PSK
 802.1x-SHA256
 PSK-SHA256

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Stap 3. Navigeer naar het subtabblad **AAA** en selecteer de Lijst met verificatiemethoden die eerder is geconfigureerd. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List Dot1X_Authenticatio ⓘ

Local EAP Authentication

↶ Cancel Apply to Device

C9800 - Beleidsprofiel configureren

Stap 1. Navigeer naar **Configuration > Tags & profielen > Beleid** en klik op **+Add** en voer een naam en beschrijving van het beleidsprofiel in. Schakel het beleid in en schakel de centrale switching, DHCP en associatie uit, aangezien het bedrijfsgebruikersverkeer lokaal is ingeschakeld op het toegangspunt zoals in het afbeelding wordt getoond.

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General	Access Policies	QOS and AVC	Mobility	Advanced
Name*	PP_Corp		WLAN Switching Policy	
Description	Policy Profile for Corp		Central Switching	<input type="checkbox"/> DISABLED
Status	ENABLED <input checked="" type="checkbox"/>		Central Authentication	ENABLED <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED		Central DHCP	<input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED		Central Association	<input type="checkbox"/> DISABLED
CTS Policy		Flex NAT/PAT		
Inline Tagging	<input type="checkbox"/>		<input type="checkbox"/> DISABLED	
SGACL Enforcement	<input type="checkbox"/>		<input type="checkbox"/> DISABLED	
Default SGT	2-65519		<input type="checkbox"/> DISABLED	

Stap 2. Navigeer naar het tabblad **Toegangsbeleid** en voer handmatig de ID van het VLAN in die moet worden gebruikt in de aftakking voor het bedrijfsgebruikersverkeer. Dit VLAN hoeft niet te worden geconfigureerd op de C9800 zelf. Het moet worden geconfigureerd in het Flex Profile, zoals verder uitgewerkt. Selecteer een VLAN-naam niet in de vervolgkeuzelijst (zie Cisco bug-id [CSCvn48234](#) voor meer informatie). Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General	Access Policies	QOS and AVC	Mobility	Advanced
RADIUS Profiling	<input type="checkbox"/>			
HTTP TLV Caching	<input type="checkbox"/>			
DHCP TLV Caching	<input type="checkbox"/>			
WLAN Local Profiling				
Global State of Device Classification	<input type="checkbox"/>			
Local Subscriber Policy Name	<input type="text" value="Search or Select"/>			
VLAN				
VLAN/VLAN Group	<input type="text" value="2"/>			
Multicast VLAN	<input type="text" value="Enter Multicast VLAN"/>			
				WLAN ACL
				IPv4 ACL <input type="text" value="Search or Select"/>
				IPv6 ACL <input type="text" value="Search or Select"/>
URL Filters				
				Pre Auth <input type="text" value="Search or Select"/>
				Post Auth <input type="text" value="Search or Select"/>
<input type="button" value="Cancel"/>				<input type="button" value="Apply to Device"/>

C9800 - Beleidsmarkering configureren

Zodra het WLAN-profiel (WP_Corp) en het beleidsprofiel (PP_Corp) zijn gemaakt, moet er een beleidstag worden gemaakt om deze WLAN- en beleidsprofielen samen te binden. Deze beleidsmarkering wordt toegepast op access points. Wijs deze beleidstag toe aan access points om de configuratie van deze toegangspunten te activeren om de geselecteerde SSID's op deze toegangspunten in te schakelen.

Stap 1. Navigeer naar **Configuration > Tags & profielen > Tags**, selecteer het tabblad **Policy** en klik op **+Add**. Voer de naam en beschrijving van de beleidstag in. Klik op **+Add** onder **WLAN-POLICY Maps**. Selecteer het eerder gemaakte WLAN-profiel en -beleidsprofiel en klik vervolgens op de knop voor het selectieteken zoals in deze afbeelding.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
No items to display	

Map WLAN and Policy

WLAN Profile*

Policy Profile*

➤ RLAN-POLICY Maps: 0

Stap 2. Controleer en klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

Add Policy Tag ✕

Name*

Description

▼ **WLAN-POLICY Maps: 1**

WLAN Profile	Policy Profile
<input checked="" type="checkbox"/> WP_Corp	PP_Corp

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

➤ **RLAN-POLICY Maps: 0**

C9800 - Profiel voor AP Join

AP Join Profiles en Flex Profiles moeten worden geconfigureerd en toegewezen aan access points met Site Tags. Voor elke tak moet een andere Site Tag worden gebruikt om 802.11r Fast Transition (FT) binnen een tak te ondersteunen, maar de distributie van de client PMK alleen tussen de AP's van die tak te beperken. Het is belangrijk om niet dezelfde site tag over meerdere takken te gebruiken. Configureer een AP Join Profile. U kunt één enkel AP Join Profiel gebruiken als alle takken gelijkaardig zijn, of tot meerdere profielen leiden als sommige van de gevormde parameters verschillend moeten zijn.

Stap 1. Navigeer naar **Configuration > Tags en profielen > AP Join** en klik op **+Add**. Voer de naam en beschrijving van het AP Join Profile in. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

Add AP Join Profile ✕

General Client CAPWAP AP Management Security ICap QoS

Name*	APJP_Branch	OfficeExtend AP Configuration	
Description	Profiles for branches	Local Access	<input checked="" type="checkbox"/>
LED State	<input checked="" type="checkbox"/>	Link Encryption	<input checked="" type="checkbox"/>
LAG Mode	<input type="checkbox"/>	Rogue Detection	<input type="checkbox"/>
NTP Server	0.0.0.0		
GAS AP Rate Limit	<input type="checkbox"/>		
Apphost	<input type="checkbox"/>		

↶ Cancel Apply to Device

C9800 - Flex profiel

Configureer nu een Flex-profiel. Opnieuw kunt u één profiel gebruiken voor alle vertakkingen als deze gelijk zijn en dezelfde VLAN/SSID-toewijzing hebben. U kunt ook meerdere profielen maken als bepaalde ingestelde parameters, zoals de VLAN-toewijzingen, anders zijn.

Stap 1. Navigeer naar **Configuration > Tags en profielen > Flex** en klik op **+Add**. Voer de naam en beschrijving van Flex Profile in.

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

Name*	FP_Branch	Fallback Radio Shut	<input type="checkbox"/>
Description	Flex Profile for branches	Flex Resilient	<input type="checkbox"/>
Native VLAN ID	1	ARP Caching	<input checked="" type="checkbox"/>
HTTP Proxy Port	0	Efficient Image Upgrade	<input checked="" type="checkbox"/>
HTTP-Proxy IP Address	0.0.0.0	OfficeExtend AP	<input type="checkbox"/>
CTS Policy		Join Minimum Latency	<input type="checkbox"/>
Inline Tagging	<input type="checkbox"/>	IP Overlap	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>	mDNS Flex Profile	Search or Select ▼
CTS Profile Name	default-sxp-profile ✕ ▼		

↶ Cancel Apply to Device

Stap 2. Navigeer naar het tabblad **VLAN** en klik op **+Add**. Voer de VLAN-naam en -id in van het lokale VLAN bij de aftakking die het toegangspunt moet gebruiken om het bedrijfsgebruikersverkeer lokaal te switches. Klik op de knop **Opslaan** zoals in deze afbeelding.

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add ✕ Delete

VLAN Name	ID	ACL Name
No items to display		

10 items per page

VLAN Name*

VLAN Id*

ACL Name

✓ Save ↻ Cancel

↻ Cancel Apply to Device

Stap 3. Controleer en klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add ✕ Delete

VLAN Name	ID	ACL Name
<input checked="" type="checkbox"/> CorpData	2	

10 items per page

1 - 1 of 1 items

↻ Cancel **Apply to Device**

C9800 - Sitetag

Site-tags worden gebruikt om Join Profiles en Flex Profiles toe te wijzen aan access points. Zoals eerder vermeld, moet voor elke tak een andere Site-tag worden gebruikt om 802.11r Fast Transition (FT) binnen een tak te ondersteunen, maar de verdeling van de client-PMK over alleen de AP's van die tak te beperken. Het is belangrijk om dezelfde site-tag niet opnieuw te gebruiken over meerdere takken.

Stap 1. Navigeer naar **Configuration > Tags & profielen > Tags**, selecteer het tabblad **Site** en klik op **+Add**. Voer een naam en beschrijving van de sitetag in, selecteer het profiel samenvoegen met het toegangspunt, deselecteer het vakje **Lokale site inschakelen** en selecteer ten slotte het eerder gemaakte Flex-profiel. Schakel het vakje **Local Site inschakelen uit** om het toegangspunt van **Local Mode** in **FlexConnect** te wijzigen. Klik tot slot op de knop **Toepassen op apparaat** zoals in dit beeld.

Add Site Tag ✕

Name*	<input type="text" value="ST_Branch_01"/>
Description	<input type="text" value="Site Tag for Branch 01"/>
AP Join Profile	<input type="text" value="APJP_Branch"/> ▼
Flex Profile	<input type="text" value="FP_Branch"/> ▼
Fabric Control Plane Name	<input type="text" value=""/> ▼
Enable Local Site	<input checked="" type="checkbox"/>

↶ Cancel
📄 Apply to Device

C9800 - RF-tag

Stap 1. Navigeer naar **Configuration > Tags & profielen > tags**, selecteer het **tabblad RF** en klik op **+Add**. Voer een naam en beschrijving in voor de RF-tag. Selecteer de door het systeem gedefinieerde **RF-profielen in het vervolgkeuzemenu**. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

Add RF Tag ✕

Name*	<input type="text" value="RFT_Branch"/>
Description	<input type="text" value="RF in Typical Branch"/>
5 GHz Band RF Profile	<input type="text" value="Typical_Client_Densi"/> ▼
2.4 GHz Band RF Profile	<input type="text" value="Typical_Client_Densi"/> ▼

↶ Cancel
📄 Apply to Device

C9800 - Tags toewijzen aan AP

Nu de tags worden gecreëerd die de verschillende beleidslijnen en profielen bevatten die nodig zijn om de access points te configureren, moeten we ze toewijzen aan de access points. Deze paragraaf laat zien hoe u een statische tag kunt uitvoeren die handmatig aan een access point wordt toegewezen, op basis van het Ethernet MAC-adres. Voor productproductieomgevingen wordt aanbevolen de Cisco DNA Center AP PNP Workflow te gebruiken, of een statische, bulk-CSV-uploadmethode te gebruiken die beschikbaar is in 9800.

Stap 1. Navigeer om te **configureren > Tags & profielen > tags**, selecteer het **AP-tabblad** en vervolgens het **tabblad Statisch**. Klik op **+Add** en voer het MAC-adres van het AP in en selecteer de eerder gedefinieerde Policy Tag, Site Tag en RF-tag. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

Associate Tags to AP ✕

AP MAC Address*	<input type="text" value="380e.4dbf.589a"/>
Policy Tag Name	<input type="text" value="PT_Branch"/> ▼
Site Tag Name	<input type="text" value="ST_Branch_01"/> ▼
RF Tag Name	<input type="text" value="RFT_Branch"/> ▼

Aruba CPPM configureren

Eerste configuratie van Aruba ClearPass Policy Manager-server

Aruba clearpass wordt via OVF-sjabloon op ESXi-server ingezet met deze bronnen:

- 2 gereserveerde virtuele CPU's
- 6 GB RAM
- 80 GB schijf (moet handmatig worden toegevoegd na eerste VM-implementatie voordat de machine wordt ingeschakeld)

Licenties toepassen

Platformlicentie toepassen via: **Beheer > Server Manager > Licentie**. Toegang en ingebouwd toevoegen

De C9800 draadloze controller toevoegen als netwerkapparaat

Ga naar **Configuratie > Netwerk > Apparaten > Toevoegen** zoals in deze afbeelding.

Edit Device Details

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes

Name: >WLC-10.85.54.99

IP or Subnet Address: 10.85.54.99 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)

Description: LAB WLC 9800

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name: Cisco

Enable RADIUS Dynamic Authorization: Port: 1700

Enable RadSec:

Copy Save Cancel

CPPM configureren om Windows AD als verificatiebron te gebruiken

Navigeer naar **Configuratie > Verificatie > Bronnen > Toevoegen**. Selecteer **Type: Active Directory** in het vervolgkeuzemenu zoals in deze afbeelding.

aruba ClearPass Policy Manager

Configuration » Authentication » Sources » Add

Authentication Sources

General | Primary | Attributes | Summary

Name: LAB_AD

Description:

Type: Active Directory

Use for Authorization: Enable to use this Authentication Source to also fetch role mapping attributes

Authorization Sources: -- Select --

Server Timeout: 10 seconds

Cache Timeout: 36000 seconds

Backup Servers Priority: Move Up ↑ Move Down ↓ Add Backup Remove

CPPM configureren Dot1X-verificatieservice

Stap 1. Maak een 'service' die overeenkomt met verschillende RADIUS-kenmerken:

- Straal:IETF | Naam: NAS-IP-adres | GELIJKHEID | <IP-ADRES>
- Straal:IETF | Naam: Service-type | GELIJKHEID | 1,2,8

Stap 2. Voor de productie wordt aanbevolen een SSID-naam te gebruiken in plaats van 'NAS-IP-

Adres', zodat één voorwaarde volstaat voor een multi-WLC-implementatie. | cisco-WLAN | Dot1XSSID

ClearPass Policy Manager

Configuration » Services » Edit - G _DOT1X

Services - DOT1X

Summary **Service** Authentication Roles Enforcement

Name: DOT1X
Description: 802.1X Wireless Access Service
Type: 802.1X Wireless
Status: Enabled
Monitor Mode: Enable to monitor network access without enforcement
More Options: Authorization Posture Compliance Audit End-hosts Profile Endpoints Accounting Proxy

Matches: ANY or ALL of the following conditions:

Type	Name	Operator	Value
1.	Radius:IETF	EQUALS	10.85.54.99
2.	Radius:IETF	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)

ClearPass Policy Manager

Configuration » Services » Edit - G _DOT1X

Services - DOT1X

Summary **Service** **Authentication** Roles Enforcement

Authentication Methods:
EAP PEAP]
EAP FAST]
EAP TLS]
EAP TTLS]
--Select to Add--

Authentication Sources:
LAB_AD [Active Directory]
--Select to Add--

Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefix

Service Certificate: --Select to Add--

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- [Handleiding voor best practices voor Cisco 9800 implementaties](#)

- [Inzicht in Catalyst 9800 configuratiemodel voor draadloze controllers](#)
- [Begrijp FlexConnect op Catalyst 9800 draadloze controller](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.