

Konfigurieren der 9800 WLC-Integration mit Aruba ClearPass - Dot1x & Bereitstellung von FlexConnect für Zweigstellen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Datenverkehrsfluss](#)

[Netzwerkdiagramm](#)

[Konfigurieren des Catalyst 9800 Wireless Controllers](#)

[C9800 - Konfigurieren der AAA-Parameter für dot1x](#)

[C9800 - Konfigurieren des WLAN-Profiles der Firma](#)

[C9800 - Konfigurieren des Richtlinienprofils](#)

[C9800 - Konfigurieren des Richtlinien-Tags](#)

[C9800 - AP-Beitrittsprofil](#)

[C9800 - Flex Profile](#)

[C9800 - Site-Tag](#)

[C9800 - RF-Tag](#)

[C9800 - Zuweisen von Tags zu AP](#)

[Aruba CPPM konfigurieren](#)

[Aruba ClearPass Policy Manager Server - Erstkonfiguration](#)

[Lizenzen anwenden](#)

[Hinzufügen des C9800 Wireless Controllers als Netzwerkgerät](#)

[Konfigurieren von CPPM zur Verwendung von Windows AD als Authentifizierungsquelle](#)

[CPPM Dot1X-Authentifizierungsdienst konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Integration des Catalyst 9800 Wireless Controllers mit Aruba ClearPass Policy Manager (CPPM) und Microsoft Active Directory (AD) beschrieben, um Wireless-Clients in einer Flexconnect-Bereitstellung eine 802.1x-Authentifizierung bereitzustellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie diese Themen kennen und dass sie konfiguriert und verifiziert wurden:

- Catalyst Wireless Controller 9800
- Aruba ClearPass Server (erfordert Plattformlizenz, Zugriffslizenz, Onboard-Lizenz)
- Betriebliches Windows AD
- Optionale Zertifizierungsstelle (Certificate Authority, CA)
- Betriebs-DHCP-Server
- Operativer DNS-Server (für die Zertifikatsperrlisten-Validierung erforderlich)
- ESXi
- Alle relevanten Komponenten werden mit NTP synchronisiert und auf korrekte Zeit überprüft (für die Zertifikatsvalidierung erforderlich).
- Kenntnisse der Themen: C9800-Bereitstellung und neues Konfigurationsmodell FlexConnect-Betrieb auf C9800 802.1x-Authentifizierung

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Hardware- und Software-Versionen:

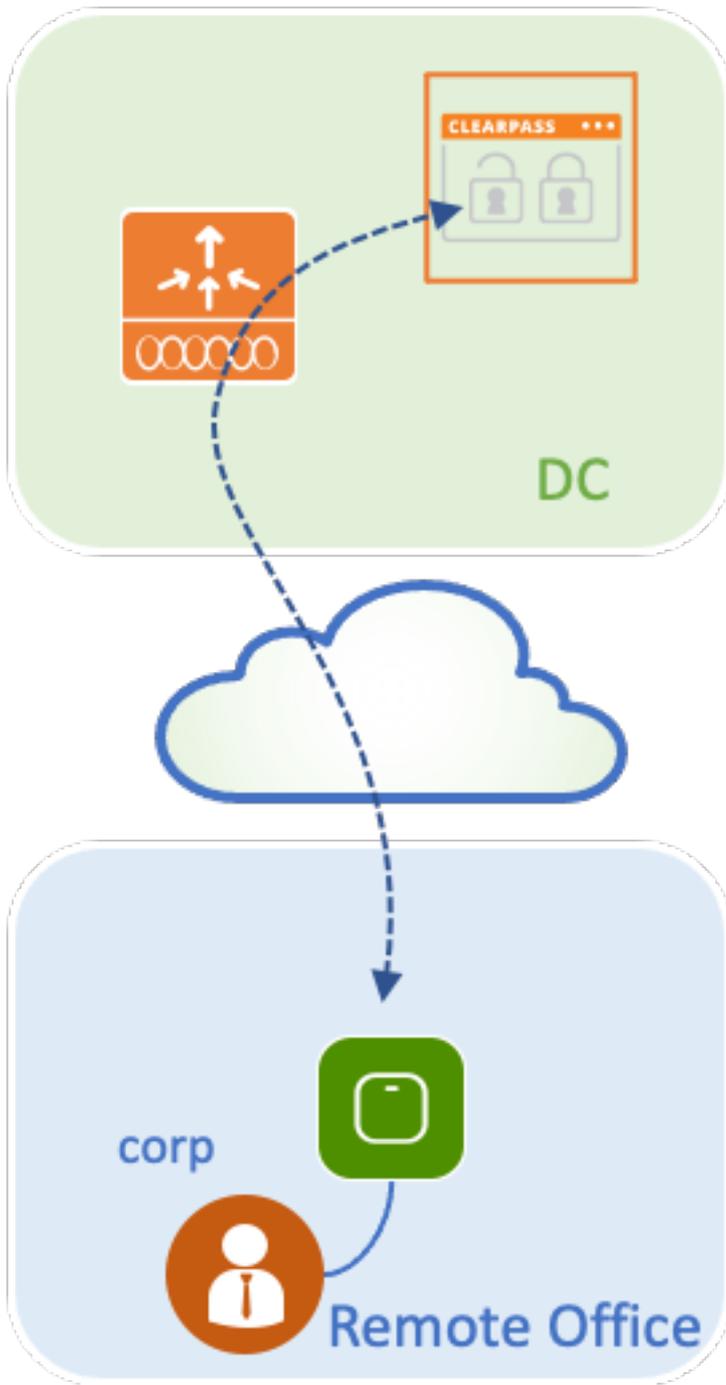
- C9800-L-C Cisco IOS-XE 17.3.3
- C9130AX, 4800 APs
- Aruba ClearPass, Patch 6-8-0-109592 und 6.8-3
- MS Windows-Server Active Directory (GP konfiguriert für die automatisierte, computerbasierte Zertifikatsausstellung an verwaltete Endpunkte) DHCP-Server mit Option 43 und Option 60 DNS-Server NTP-Server zur Zeitsynchronisierung aller Komponenten CA

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

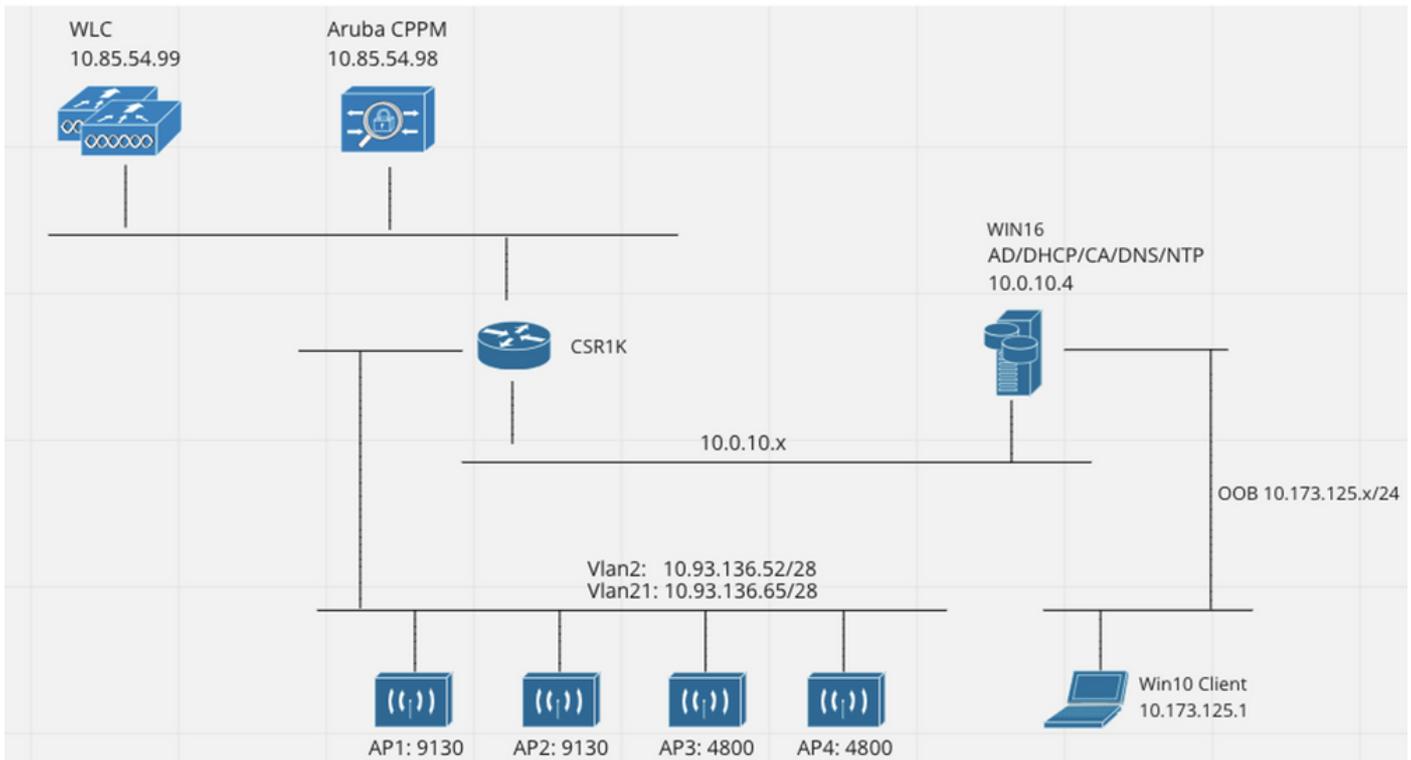
Hintergrundinformationen

Datenverkehrsfluss

In einer typischen Unternehmensbereitstellung mit mehreren Zweigstellen ist jede Zweigstelle so eingerichtet, dass sie den Mitarbeitern des Unternehmens einen 1-fach-Zugriff ermöglicht. In diesem Konfigurationsbeispiel wird PEAP verwendet, um Unternehmensbenutzern über eine im zentralen Rechenzentrum (DC) bereitgestellte ClearPass-Instanz einen 802.1x-Zugriff bereitzustellen. Systemzertifikate werden zusammen mit der Überprüfung der Anmeldeinformationen von Mitarbeitern auf einem Microsoft AD-Server verwendet.

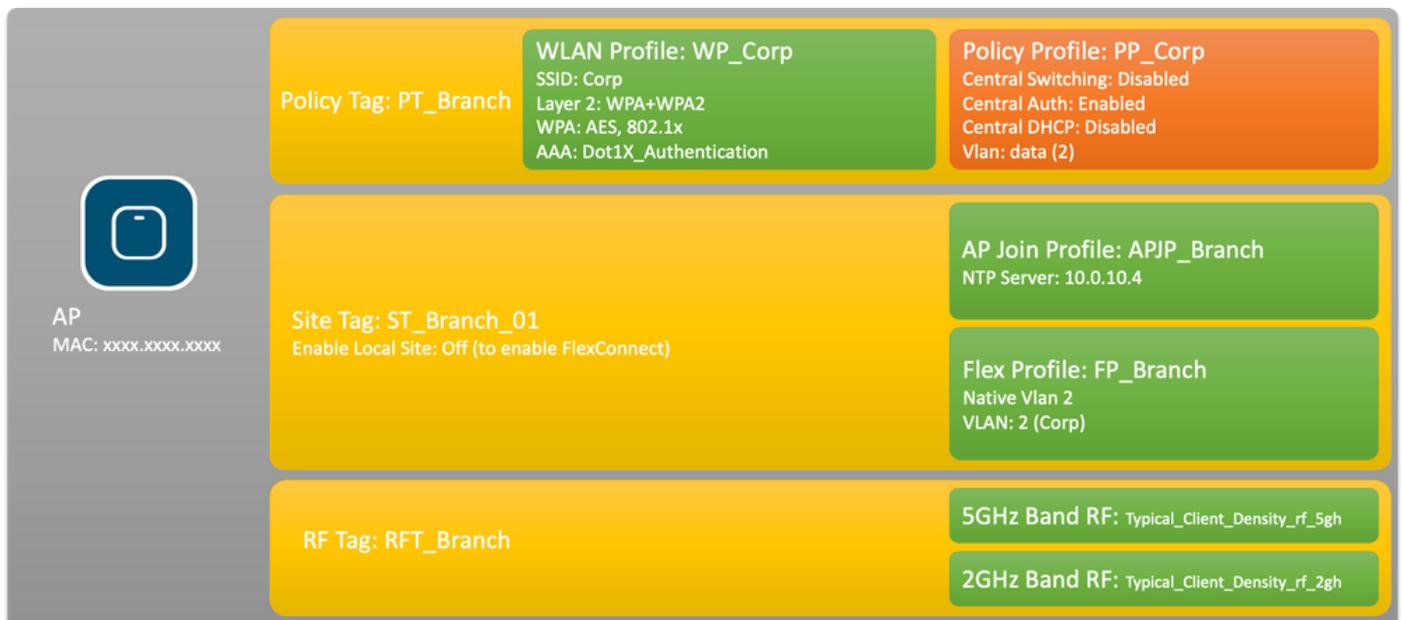


Netzwerkdiagramm



Konfigurieren des Catalyst 9800 Wireless Controllers

In diesem Konfigurationsbeispiel wird das neue Konfigurationsmodell auf dem C9800 verwendet, um die erforderlichen Profile und Tags zu erstellen, um dot1x Corporate Access für Zweigstellen bereitzustellen. Die resultierende Konfiguration ist im Diagramm zusammengefasst.



C9800 - Konfigurieren der AAA-Parameter für dot1x

Schritt 1: Fügen Sie den Corp-Server des Aruba ClearPass Policy Manager zur 9800 WLC-Konfiguration hinzu. Navigieren Sie zu **Konfiguration > Sicherheit > AAA > Server/Gruppen > RADIUS > Server**. Klicken Sie auf **+Hinzufügen**, und geben Sie die RADIUS-Serverinformationen ein. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.

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

Schritt 2: Definieren Sie eine AAA-Servergruppe für Unternehmensbenutzer. Navigieren Sie zu **Konfiguration > Sicherheit > AAA > Server/Gruppen > RADIUS > Gruppen**, und klicken Sie auf **+Hinzufügen**, geben Sie den Namen der RADIUS-Servergruppe ein, und weisen Sie die RADIUS-Serverinformationen zu. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.

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

Schritt 3: Definieren Sie die dot1x-Authentifizierungsmethodenliste für Unternehmensbenutzer. Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authentication**, und klicken Sie auf **+Add**. Wählen Sie **Type dot1x** aus dem Dropdown-Menü aus. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.

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 - Konfigurieren des WLAN-Profiles der Firma

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Wireless**, und klicken Sie auf **+Hinzufügen**. Geben Sie einen Profilnamen, die SSID "Corp" und eine WLAN-ID ein, die noch nicht verwendet wird.

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

Schritt 2: Navigieren Sie zur Registerkarte **Security (Sicherheit)** und zur Unterregisterkarte **Layer 2**. Die Standardparameter für dieses Konfigurationsbeispiel müssen nicht geändert werden.

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

Schritt 3: Navigieren Sie zur Unterregisterkarte **AAA**, und wählen Sie die zuvor konfigurierte Liste der Authentifizierungsmethoden aus. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List Dot1X_Authenticatio ⓘ

Local EAP Authentication

↶ Cancel 📄 Apply to Device

C9800 - Konfigurieren des Richtlinienprofils

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Richtlinie**, und klicken Sie auf **+Hinzufügen**, und geben Sie einen Namen und eine Beschreibung für das Richtlinienprofil ein. Aktivieren Sie die Richtlinie, und deaktivieren Sie das zentrale Switching, DHCP und die Verknüpfung, da der Datenverkehr der Unternehmensbenutzer lokal am Access Point geschwitcht wird, wie im Bild gezeigt.

⚠ 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	

Schritt 2: Navigieren Sie zur Registerkarte **Zugriffsrichtlinien**, und geben Sie die ID des VLANs, das in der Außenstelle für den Datenverkehr der Benutzer des Unternehmens verwendet werden soll, manuell ein. Dieses VLAN muss nicht auf dem C9800 selbst konfiguriert werden. Sie muss im Flex Profile-Tool konfiguriert werden (siehe Details weiter unten). Wählen Sie keinen VLAN-Namen aus der Dropdown-Liste aus (siehe Cisco Bug-ID [CSCvn48234](#) für weitere Informationen). Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.

⚠ 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 - Konfigurieren des Richtlinien-Tags

Nachdem das WLAN-Profil (WP_Corp) und das Richtlinienprofil (PP_Corp) erstellt wurden, muss wiederum ein Richtlinien-Tag erstellt werden, um diese WLAN- und Richtlinienprofile miteinander zu verbinden. Dieses Richtlinien-Tag wird auf Access Points angewendet. Weisen Sie diesen Policy Tag Access Points zu, um diese zu konfigurieren und die ausgewählten SSIDs zu aktivieren.

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Tags**, wählen Sie die Registerkarte **Policy** aus, und klicken Sie auf **+Hinzufügen**. Geben Sie den Namen und die Beschreibung der Policy Tag-Nummer ein. Klicken Sie auf **+Hinzufügen** unter **WLAN-POLICY Maps**. Wählen Sie das WLAN-Profil und das Richtlinienprofil aus, die Sie zuvor erstellt haben, und klicken Sie dann auf das Kontrollkästchen, wie in diesem Bild gezeigt.

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

Schritt 2: Überprüfen Sie, und klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in dieser Abbildung dargestellt.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 1

+ Add ✕ Delete

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**

↶ Cancel

📄 Apply to Device

C9800 - AP-Beitrittsprofil

AP-Join-Profile und Flex-Profile müssen konfiguriert und Access Points mit Site-Tags zugewiesen werden. Für jede Außenstelle muss eine andere Site-Tag-Nummer verwendet werden, um den schnellen Übergang (802.11r Fast Transition, FT) innerhalb einer Außenstelle zu unterstützen. Die Verteilung der Client-PMK auf die Access Points dieser Außenstelle ist jedoch zu begrenzen. Es ist wichtig, dieselbe Site-Tag nicht für mehrere Außenstelle zu verwenden. Konfigurieren eines Zugangsprofils für den Access Point Sie können ein einzelnes Zugangsprofil verwenden, wenn alle Zweige ähnlich sind, oder mehrere Profile erstellen, wenn einige der konfigurierten Parameter unterschiedlich sein müssen.

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > AP Join**, und klicken Sie auf **+Add**. Geben Sie den Namen und die Beschreibung des AP Join-Profiles ein. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.

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 Profile

Konfigurieren Sie jetzt ein Flex Profile. Auch hier können Sie ein einziges Profil für alle Zweigstellen verwenden, wenn diese ähnlich sind, und die gleiche VLAN/SSID-Zuordnung haben. Sie können auch mehrere Profile erstellen, wenn einige der konfigurierten Parameter, z. B. die VLAN-Zuweisungen, unterschiedlich sind.

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Flex**, und klicken Sie auf **+Hinzufügen**. Geben Sie den Flex Profile-Namen und die entsprechende Beschreibung ein.

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

Schritt 2. Navigieren Sie zur Registerkarte **VLAN**, und klicken Sie auf **+Hinzufügen**. Geben Sie den VLAN-Namen und die ID des lokalen VLANs in der Außenstelle ein, die der Access Point zum lokalen Umschalten des Datenverkehrs des Unternehmens verwenden muss. Klicken Sie auf die

Schaltfläche **Speichern**, wie in diesem Bild dargestellt.

The screenshot shows the 'Add Flex Profile' dialog box with the 'VLAN' tab selected. The 'Add' button is highlighted. The form fields are: VLAN Name* (CorpData), VLAN Id* (2), and ACL Name (Select ACL). The 'Save' button is highlighted.

Schritt 3: Überprüfen Sie, und klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in dieser Abbildung dargestellt.

The screenshot shows the 'Add Flex Profile' dialog box with the 'VLAN' tab selected. The 'Apply to Device' button is highlighted.

C9800 - Site-Tag

Site-Tags werden verwendet, um Join-Profile und Flex-Profile Access Points zuzuweisen. Wie bereits erwähnt, muss für jede Verzweigung ein anderes Site-Tag verwendet werden, um 802.11r Fast Transition (FT) innerhalb einer Verzweigung zu unterstützen. Die Verteilung der Client-PMK auf die Access Points dieser Verzweigung ist jedoch auf diese beschränkt. Es ist wichtig, denselben Site-Tag nicht über mehrere Verzweigungen hinweg zu verwenden.

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Tags**, wählen Sie die Registerkarte **Site aus**, und klicken Sie auf **+Hinzufügen**. Geben Sie einen Site-Tag-Namen und eine Beschreibung ein, wählen Sie das erstellte AP-Join-Profil aus, deaktivieren Sie das Kontrollkästchen **Lokalen Standort aktivieren**, und wählen Sie schließlich das zuvor erstellte Flex-Profil aus. Deaktivieren Sie das Kontrollkästchen **Lokalen Standort aktivieren**, um den Access Point von **Lokaler Modus** in **FlexConnect** zu ändern. Klicken Sie abschließend auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.

Add Site Tag ✕

Name*

Description

AP Join Profile

Flex Profile

Fabric Control Plane Name

Enable Local Site

↶ Cancel 📄 Apply to Device

C9800 - RF-Tag

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Tags**, wählen Sie die Registerkarte **RF**, und klicken Sie auf **+Hinzufügen**. Geben Sie einen Namen und eine Beschreibung für das RF-Tag ein. Wählen Sie die systemdefinierten **RF-Profilen aus dem Dropdown-Menü aus**. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.

Add RF Tag ✕

Name*

Description

5 GHz Band RF Profile

2.4 GHz Band RF Profile

↶ Cancel 📄 Apply to Device

C9800 - Zuweisen von Tags zu AP

Nachdem die Tags erstellt wurden, die die verschiedenen Richtlinien und Profile enthalten, die für die Konfiguration der Access Points erforderlich sind, müssen diese den Access Points zugewiesen werden. In diesem Abschnitt wird gezeigt, wie ein statisches Tag, das einem Access Point manuell zugewiesen wird, basierend auf seiner Ethernet-MAC-Adresse ausgeführt wird. Für Produktivumgebungen wird empfohlen, den Cisco DNA Center AP PNP Workflow oder eine statische CSV-Upload-Methode zum Hochladen großer Mengen aus dem 9800 zu verwenden.

Schritt 1: Navigieren Sie zu **Konfigurieren > Tags & Profile > Tags**, wählen Sie die Registerkarte **AP** und dann die **Registerkarte Statisch** aus. Klicken Sie auf **+Hinzufügen**, geben Sie die AP-MAC-Adresse ein, und wählen Sie die zuvor definierte Policy-Tag-, Site-Tag- und RF-Tag-Nummer aus. Klicken Sie auf die Schaltfläche **Auf Gerät anwenden**, wie in diesem Bild dargestellt.

Associate Tags to AP ✕

AP MAC Address*

Policy Tag Name

Site Tag Name

RF Tag Name

Aruba CPPM konfigurieren

Aruba ClearPass Policy Manager Server - Erstkonfiguration

Aruba ClearPass wird über die OVF-Vorlage auf dem ESXi-Server mit folgenden Ressourcen bereitgestellt:

- 2 reservierte virtuelle CPUs
- 6 GB RAM
- 80 GB Festplatte (muss manuell nach der anfänglichen VM-Bereitstellung hinzugefügt werden, bevor der Computer eingeschaltet wird)

Lizenzen anwenden

Wenden Sie die Plattformlizenz an über: **Administration > Server Manager > Licensing (Verwaltung > Server-Manager > Lizenzierung)**. Zugriff hinzufügen und integrieren

Hinzufügen des C9800 Wireless Controllers als Netzwerkgerät

Navigieren Sie zu **Konfiguration > Netzwerk > Geräte > Hinzufügen**, wie in dieser Abbildung dargestellt.

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

Konfigurieren von CPPM zur Verwendung von Windows AD als Authentifizierungsquelle

Navigieren Sie zu **Konfiguration > Authentifizierung > Quellen > Hinzufügen**. Typ auswählen: **Active Directory** aus dem Dropdown-Menü, wie in diesem Bild dargestellt.

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:

Add Backup Move Up ↑ Move Down ↓ Remove

Konfigurieren von CPPM Do1X-Authentifizierungsdienst

Schritt 1: Erstellen Sie einen 'Dienst', der mit mehreren RADIUS-Attributen übereinstimmt:

- Radius:IETF | Name: NAS-IP-Adresse | GLEICH | <IP-ADDR>
- Radius:IETF | Name: Servicetyp | GLEICH | 1,2,8

Schritt 2: Für die Produktion wird empfohlen, den SSID-Namen anstelle von "NAS-IP-Adresse" abzugleichen, sodass eine Bedingung für eine Multi-WLC-Bereitstellung ausreicht.
 Radius: Cisco: Cisco-AVPair | cisco-wlan-ssid | 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	NAS-IP-Address	EQUALS	10.85.54.99
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	<i>Click to add...</i>		

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--

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Cisco 9800 - Best Practices-Leitfaden zur Bereitstellung](#)
- [Catalyst Wireless Controller der Serie 9800 - Konfigurationsmodell](#)
- [FlexConnect auf Catalyst 9800 Wireless Controller verstehen](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.