

Aruba ClearPassによる9800 WLC統合の設定 – Dot1x&FlexConnect for Branchesの導入

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[Traffic flow](#)

[ネットワーク図](#)

[Catalyst 9800ワイヤレスコントローラの設定](#)

[C9800:dot1xのAAAパラメータの設定](#)

[C9800:「Corp」WLANプロファイルの設定](#)

[C9800 : ポリシープロファイルの設定](#)

[C9800 : ポリシータグの設定](#)

[C9800:AP加入プロファイル](#)

[C9800:Flexプロファイル](#)

[C9800 – サイトタグ](#)

[C9800 - RFタグ](#)

[C9800:APへのタグの割り当て](#)

[Aruba CPPMの設定](#)

[Aruba ClearPass Policy Managerサーバの初期設定](#)

[ライセンスの適用](#)

[C9800ワイヤレスコントローラをネットワークデバイスとして追加する](#)

[Windows ADを認証ソースとして使用するためのCPPMの設定](#)

[CPPM Dot1X認証サービスの設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Catalyst 9800 Wireless Controller(WLC)をAruba ClearPass Policy Manager(CPPM)およびMicrosoft Active Directory(AD)と統合して、Flexconnectの展開でワイヤレスクライアントにdot1x認証を提供する方法について説明します。

前提条件

要件

次の項目に関する知識があり、設定および確認が完了していることを推奨します。

- Catalyst 9800ワイヤレスコントローラ
- Aruba ClearPass Server (プラットフォームライセンス、アクセスライセンス、オンボードライセンスが必要)
- 運用Windows AD
- オプションの認証局(CA)
- DHCPサーバの動作
- 動作可能なDNSサーバ (証明書CRL検証に必要)
- ESXi
- 関連するすべてのコンポーネントがNTPに同期され、正しい時刻であることが確認されます (証明書の検証に必要)
- トピックに関する知識: C9800の導入と新しい設定モデルC9800でのFlexConnectの動作Dot1x認証

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

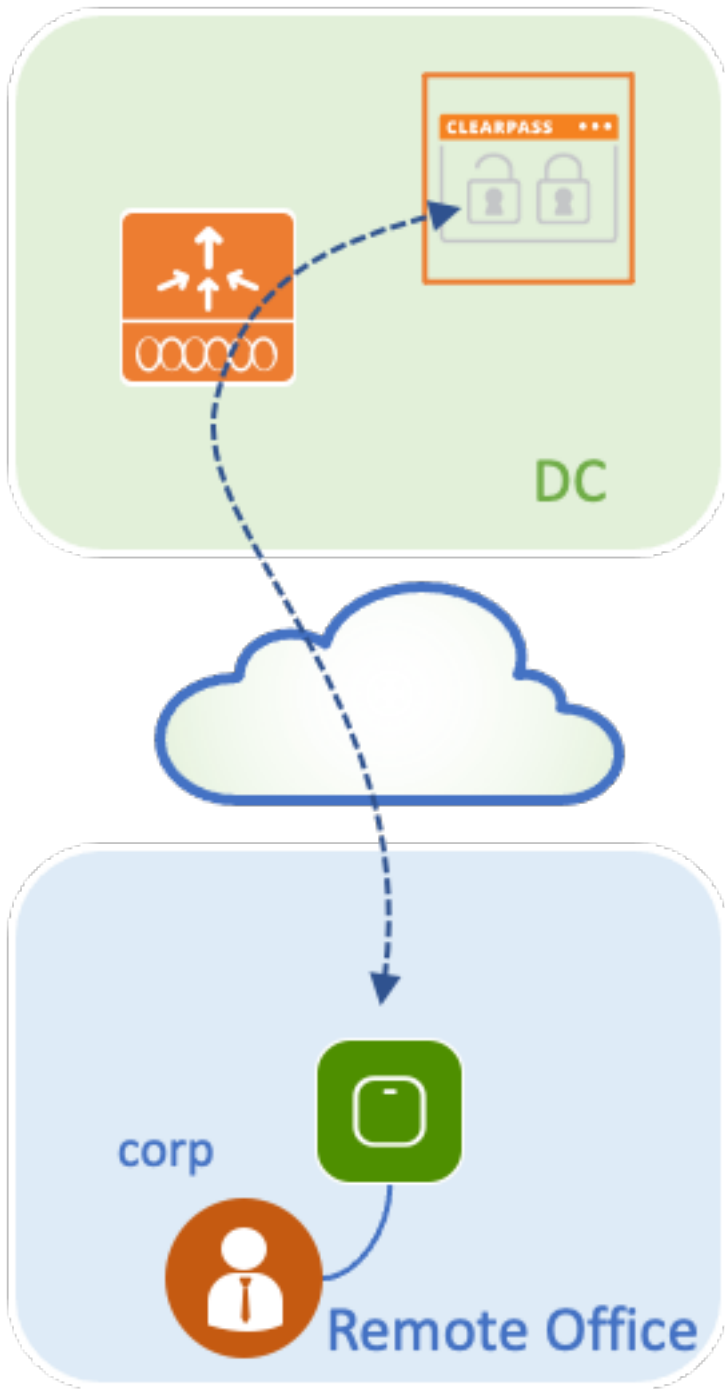
- C9800-L-C Cisco IOS-XE 17.3.3
- C9130AX、4800 AP
- Aruba ClearPass、6-8-0-109592および6.8-3パッチ
- MS Windowsサーバ Active Directory (管理対象エンドポイントへのマシンベースの証明書自動発行用に設定されたGP) オプション43およびオプション60のDHCPサーバDNSサーバすべてのコンポーネントを時刻同期するNTPサーバCA

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

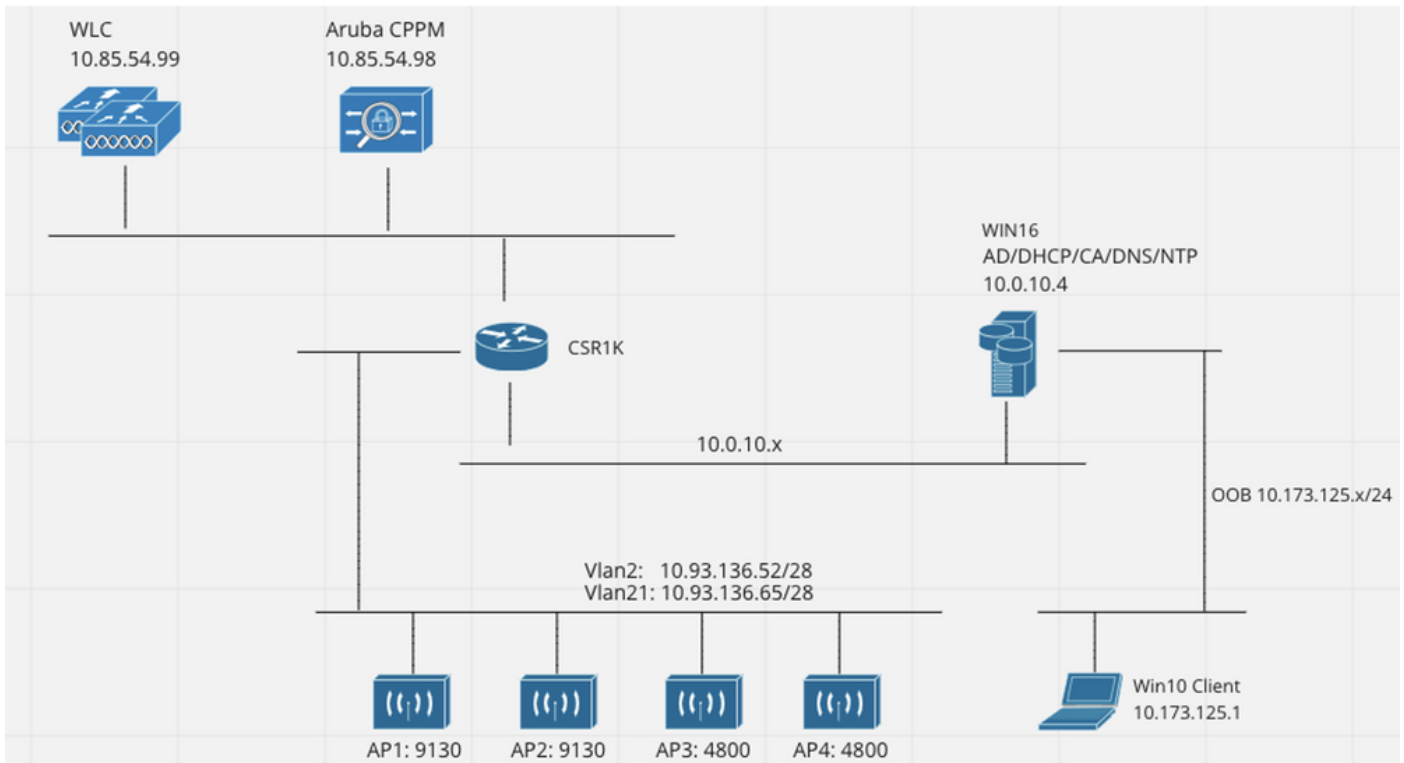
背景説明

Traffic flow

複数のブランチオフィスを持つ一般的な企業の導入では、各ブランチオフィスは企業の従業員にdot1xアクセスを提供するように設定されています。この設定例では、PEAPを使用して、中央データセンター(DC)に導入されたClearPassインスタンスを介して企業ユーザにdot1xアクセスを提供します。マシン証明書は、Microsoft ADサーバに対する従業員のクレデンシャルの検証とともに使用されます。

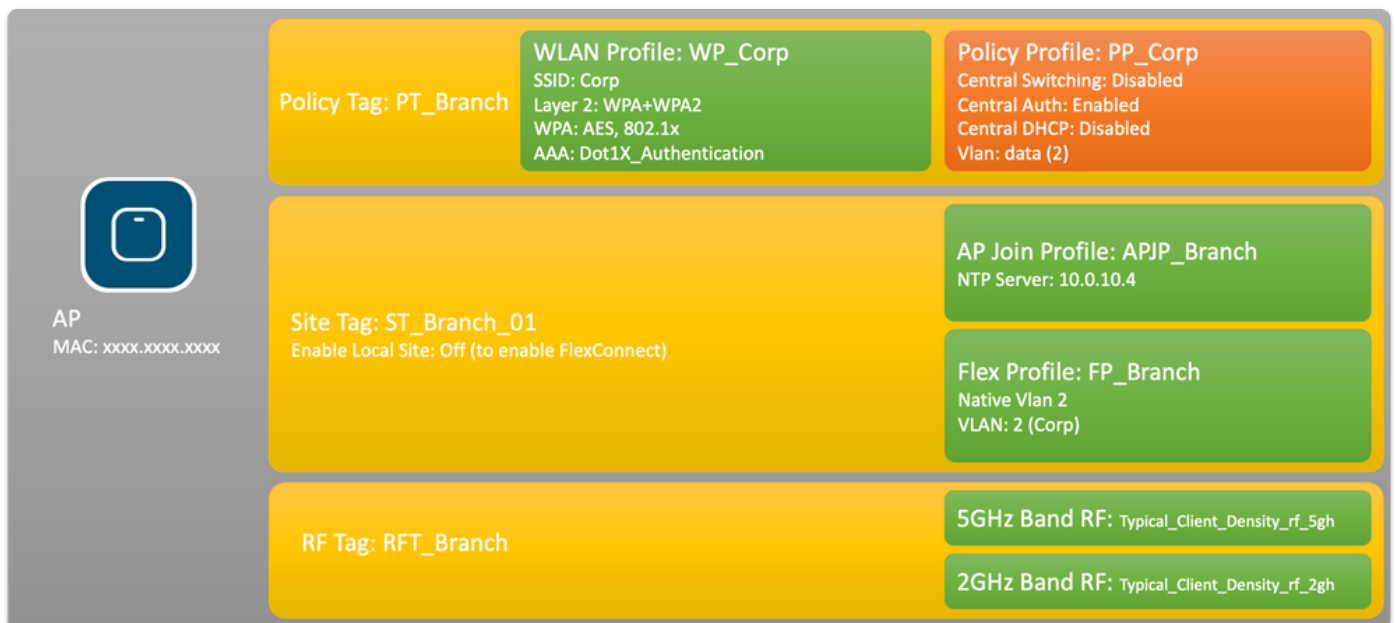


ネットワーク図



Catalyst 9800ワイヤレスコントローラの設定

この設定例では、C9800の新しい設定モデルを利用して、企業のブランチにdot1x企業アクセスを提供するために必要なプロファイルとタグを作成します。結果の設定を図にまとめます。



C9800:dot1xのAAAパラメータの設定

ステップ1: Aruba ClearPass Policy Manager 「Corp」 サーバを9800 WLC設定に追加します。
[Configuration] > [Security] > [AAA] > [Servers/Groups] > [RADIUS] > [Servers] に移動します。
[+Add]をクリックし、RADIUSサーバ情報を入力します。次の図に示すように、[Apply to Device]
ボタンをクリックします。

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

ステップ2：企業ユーザ用のAAAサーバグループを定義します。[Configuration] > [Security] > [AAA] > [Servers/Groups] > [RADIUS] > [Groups] に移動し、[+Add] をクリックして、RADIUSサーバグループ名を入力し、RADIUSサーバ情報を割り当てます。次の図に示すように、[Apply to Device] ボタンをクリックします。

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

ステップ3 : 企業ユーザのdot1x認証方式リストを定義します。[Configuration] > [Security] > [AAA] > [AAA Method List] > [Authentication] に移動し、[+Add] をクリックします。ドロップダウンメニューから[Type dot1x] を選択し、次の図に示すように[Apply to Device] ボタンをクリックします。

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: 「Corp」 WLANプロファイルの設定

ステップ1:[Configuration] > [Tags & Profiles] > [Wireless] に移動し、[+Add] をクリックします。プロファイル名、SSID「Corp」、および未使用のWLAN IDを入力します。

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

ステップ2:[Security] タブと[Layer2] サブタブに移動します。この設定例のデフォルトパラメータを変更する必要はありません。

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

ステップ3:[AAA] サブタブに移動し、以前に設定した認証方式リストを選択します。次の図に示すように、[Apply to Device] ボタンをクリックします。

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List Dot1X_Authenticatio ▼ i

Local EAP Authentication

↶ Cancel Apply to Device

C9800 : ポリシープロファイルの設定

ステップ1:[Configuration] > [Tags & Profiles] > [Policy] に移動し、[Add] をクリックして、ポリシープロファイルの名前と説明を入力します。図に示すように、企業ユーザトラフィックがAPでローカルにスイッチングされるため、ポリシーを有効にし、中央スイッチング、DHCP、およびアソシエーションを無効にします。

⚠ 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*	<input type="text" value="PP_Corp"/>			WLAN Switching Policy
Description	<input type="text" value="Policy Profile for Corp"/>			Central Switching <input type="checkbox"/> DISABLED
Status	<input type="checkbox"/> ENABLED <input checked="" type="checkbox"/>			Central Authentication <input type="checkbox"/> 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 <input type="checkbox"/> DISABLED
Inline Tagging	<input type="checkbox"/>			
SGACL Enforcement	<input type="checkbox"/>			
Default SGT	<input type="text" value="2-65519"/>			

ステップ2:[Access Policies] タブに移動し、ブランチで企業ユーザトラフィックに使用する VLAN の ID を手動で入力します。この VLAN は、C9800 自体で設定する必要はありません。詳細に従って、Flex Profile で設定する必要があります。ドロップダウンリストから VLAN 名を選択しないでください(Cisco Bug ID [CSCvn48234](#)を参照)。を参照してください。次の図に示すように、[Apply to Device] ボタンをクリックします。

⚠ 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"/>			

C9800 : ポリシータグの設定

WLANプロファイル(WP_Corp)とポリシープロファイル(PP_Corp)を作成したら、これらのWLANとポリシープロファイルをバインドするためにポリシータグを作成する必要があります。このポリシータグは、アクセスポイントに適用されます。このポリシータグをアクセスポイントに割り当て、アクセスポイント上で選択したSSIDを有効にするこれらの設定をトリガーします。

ステップ1:[Configuration] > [Tags & Profiles] > [Tags] に移動し、[Policy] タブを選択して、[Add] をクリックします。ポリシータグの名前と説明を入力します。[WLAN-POLICY Maps] の下の [Add] をクリックします。先ほど作成したWLANプロファイルとポリシープロファイルを選択し、次の図に示すようにチェックマークボタンをクリックします。

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

ステップ2：確認し、次の図に示すように[Apply to Device] ボタンをクリックします。

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:AP加入プロファイル

AP加入プロファイルとFlexプロファイルを設定し、サイトタグを使用してアクセスポイントに割り当てる必要があります。ブランチ内で802.11r Fast Transition(FT)をサポートし、そのブランチのAP間でのクライアントPMKの配布だけを制限するには、ブランチごとに異なるサイトタグを使用する必要があります。複数のブランチ間で同じサイトタグを再利用しないことが重要です。AP加入プロファイルを設定します。すべてのブランチが類似している場合は単一のAP加入プロファイルを使用でき、設定パラメータの一部が異なっている必要がある場合は複数のプロファイルを作成できます。

ステップ1:[Configuration] > [Tags & Profiles] > [AP Join] に移動し、[Add] をクリックします。AP加入プロファイルの名前と説明を入力します。次の図に示すように、[Apply to Device] ボタンをクリックします。

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"/>		

C9800:Flexプロファイル

次に、Flex Profileを設定します。ここでも、すべてのブランチが類似していて、同じVLAN/SSIDマッピングを持つ場合は、単一のプロファイルを使用できます。また、VLAN割り当てなどの設定パラメータが異なる場合は、複数のプロファイルを作成できます。

ステップ1:[Configuration] > [Tags & Profiles] > [Flex] に移動し、[+Add] をクリックします。Flexプロファイルの名前と説明を入力します。

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	<input type="text" value="Search or Select"/>
CTS Profile Name	default-sxp-profile ✕		

ステップ2:[VLAN] タブに移動し、[Add] をクリックします。APが企業ユーザトラフィックをローカルでスイッチするために使用する必要がある、ブランチのローカルVLANのVLAN名とIDを入力します。次の図に示すように、[Save] ボタンをクリックします。

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add ✕ Delete

VLAN Name	ID	ACL Name
0	10	items per page
No items to display		

VLAN Name*

VLAN Id*

ACL Name

✓ Save
↶ Cancel

↶ Cancel
📄 Apply to Device

ステップ3：確認し、次の図に示すように[Apply to Device] ボタンをクリックします。

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add ✕ Delete

VLAN Name	ID	ACL Name
CorpData	2	
1 - 1 of 1 items		

↶ Cancel
📄 Apply to Device

C9800 – サイトタグ

サイトタグは、接続プロファイルとFlexプロファイルをアクセスポイントに割り当てるために使用されます。前に説明したように、ブランチ内で802.11r Fast Transition(FT)をサポートし、そのブランチのAP間でのクライアントPMKの配布だけを制限するには、ブランチごとに異なるサイトタグを使用する必要があります。

ステップ1:[Configuration] > [Tags & Profiles] > [Tags] に移動し、[Site] タブを選択して、[Add] をクリックします。サイトタグの名前と説明を入力し、作成したAP加入プロファイルを選択し、[Enable Local Site] ボックスのチェックマークを外して、最後に以前に作成したFlexプロファイルを選択します。[Enable Local Site] ボックスをオフにして、アクセスポイントを[Local Mode] から[FlexConnect] に変更します。最後に、次の図に示すように[Apply to Device] ボタンをクリックします。

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タグ

ステップ1:[Configuration] > [Tags & Profiles] > [Tags] に移動し、[RF] タブを選択して、[Add] をクリックします。RFタグの名前と説明を入力します。ドロップダウンメニューからシステム定義のRFプロファイルを選択します。次の図に示すように、[Apply to Device] ボタンをクリックします。

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:APへのタグの割り当て

これで、アクセスポイントの設定に必要なさまざまなポリシーとプロファイルを含むタグが作成されました。これらのタグをアクセスポイントに割り当てる必要があります。このセクションでは、アクセスポイントに割り当てられたスタティックタグを、そのイーサネットMACアドレスに基づいて手動で実行する方法を示します。製品の実稼働環境では、Cisco DNA Center AP PNP Workflowを使用するか、9800で使用可能な静的バルクCSVアップロード方式を使用することをお勧めします。

ステップ1:[Configure] > [Tags & Profiles] > [Tags] に移動し、[AP] タブ、[Static] タブの順に選択します。+Addをクリックし、APのMACアドレスを入力して、以前に定義したPolicy Tag、Site Tag、およびRF Tagを選択します。次の図に示すように、Apply to Deviceボタンをクリックします。

Associate Tags to AP ✕

AP MAC Address*	380e.4dbf.589a
Policy Tag Name	PT_Branch ▼
Site Tag Name	ST_Branch_01 ▼
RF Tag Name	RFT_Branch ▼

↶ Cancel 📄 Apply to Device

Aruba CPPMの設定

Aruba ClearPass Policy Managerサーバの初期設定

Aruba clearpassは、次のリソースを使用してESXiサーバ上のOVFテンプレート経由で導入されます。

- 予約済み仮想CPU X 2
- メモリ 6 GB
- 80 GBディスク (マシンの電源を入れる前に、最初のVM導入後に手動で追加する必要がある)

ライセンスの適用

プラットフォームライセンスを適用するには、[Administration] > [Server Manager] > [Licensing] を選択します。アクセスの追加とオンボード

C9800ワイヤレスコントローラをネットワークデバイスとして追加する

次の図に示すように、[Configuration] > [Network] > [Devices] > [Add] に移動します。

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

Windows ADを認証ソースとして使用するためのCPPMの設定

[Configuration] > [Authentication] > [Sources] > [Add] に移動します。タイプでActive Directoryを選択します。

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 Remove

CPPMの設定 Dot1X認証サービス

ステップ1：複数のRADIUS属性に一致する「サービス」を作成します。

- 半径：IETF | 名前：nas-ip-address | EQUALS | <IPアドレス>
- 半径：IETF | 名前：Service-Type | EQUALS | 1,2,8

ステップ2：実稼働環境では、「NAS-IP-Address」ではなくSSID名を照合して、1つの条件で十

分なマルチWLC環境を実現することをお勧めします。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	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--

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報ははありません。

関連情報

- 『Cisco 9800 Deployment Best Practices Guide』

- [Catalyst 9800ワイヤレスコントローラの設定モデルについて](#)
- [Catalyst 9800ワイヤレスコントローラでのFlexConnectについて](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。