

Catalyst 9800 WLCでの認証を使用したFlexConnectの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

はじめに

このドキュメントでは、Catalyst 9800ワイヤレスLANコントローラで中央認証またはローカル認証を使用してFlexConnectを設定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ることが推奨されます。

- Catalyst Wireless 9800設定モデル
- FlexConnect
- 802.1X

使用するコンポーネント

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

- C9800-CL、Cisco IOS-XE® 17.3.4

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、クリアな(デフォルト)設定で作業を開始しています。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。

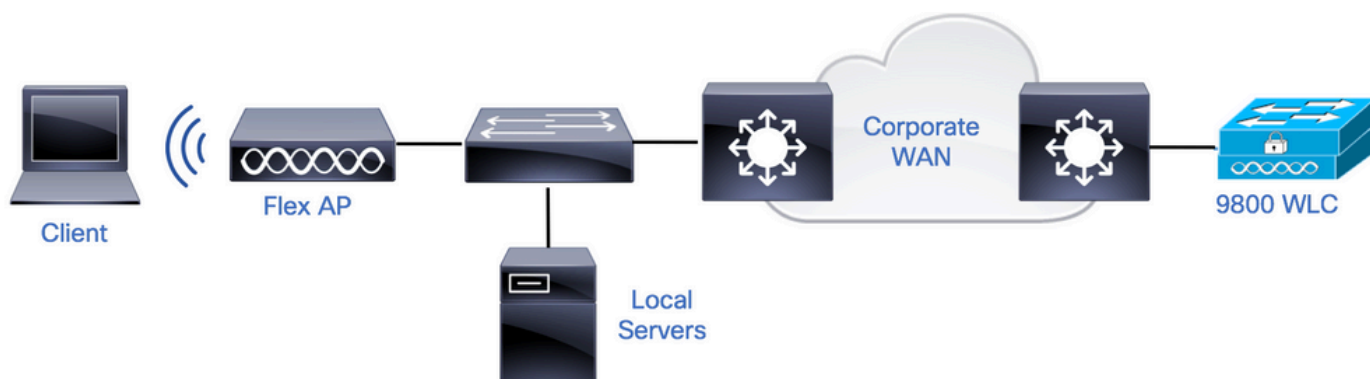
背景説明

FlexConnectは、リモートオフィスに導入するためのワイヤレスソリューションです。これにより、各ロケーションにコントローラを導入することなく、ワイドエリアネットワーク(WAN)リンクを介して企業オフィスから離れた場所にあるアクセスポイント(AP)を設定できます。FlexConnect APは、コントローラへの接続が失われたときに、クライアントデータトラフィックをローカルでスイッチングし、クライアント認証をローカルで実行できます。接続モード

では、FlexConnect APはローカル認証も実行できます。

設定

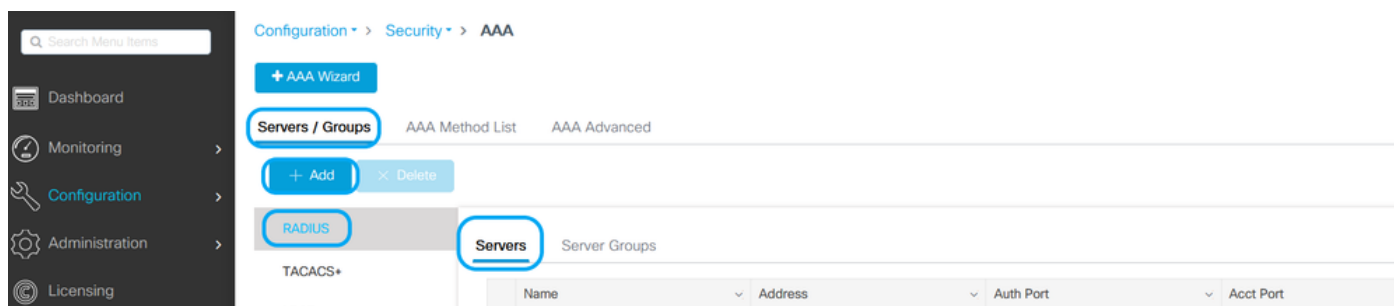
ネットワーク図



コンフィギュレーション

9800 WLCでのAAAの設定

ステップ 1 : RADIUSサーバを宣言します。**GUIから** : Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Addの順に移動し、RADIUSサーバの情報を入力します。



将来的にCoAを必要とするあらゆる種類のセキュリティを使用する予定の場合は、CoAのサポートが有効になっていることを確認します。

Name*

Server Address*

PAC Key

Key Type

Key* ⓘ

Confirm Key*

Auth Port

Acct Port

Server Timeout (seconds)

Retry Count

Support for CoA ENABLED

Cancel

Update & Apply to Device

注：注：Radius CoAは、Flex Connectのローカル認証導入ではサポートされません。を参照。

ステップ 2：RADIUSサーバをRADIUSグループに追加します。GUIから：Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Addの順に移動します。

The screenshot shows the configuration interface for AAA. The breadcrumb path is Configuration > Security > AAA. Under the AAA section, there are three tabs: Servers / Groups, AAA Method List, and AAA Advanced. The Servers / Groups tab is active. In this tab, there are buttons for '+ Add' and '× Delete'. Below these buttons, there are two main sections: RADIUS and TACACS+. The RADIUS section is expanded, showing a sub-tab for 'Server Groups' which is circled in red. Below the 'Server Groups' sub-tab, there is a table with columns for Name, Server 1, Server 2, and Server 3.

Edit AAA Radius Server Group



Name*	AmmlSE
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	2
Source Interface VLAN ID	76

Available Servers

^

v



Assigned Servers

AmmlSE

^

v



Cancel

Update & Apply to Device

ステップ 3 : 認証方式リストを作成します。**GUIから** : Configuration > Security > AAA > AAA Method List > Authentication > + Addの順に移動します。

Q Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication Authorization

+ Add × Delete

Name	Type
------	------

Quick Setup: AAA Authentication ×

Method List Name* AmmlSE

Type* dot1x ⓘ

Group Type group ⓘ

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- AmmlSE

Cancel Update & Apply to Device

CLI から :

```
# config t
# aaa new-model
```

```

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>

```

WLAN 設定

ステップ 1 : **GUIから** : Configuration > Wireless > WLANsの順に移動し、+Addをクリックして新しいWLANを作成し、WLAN情報を入力します。次に、Apply to Deviceをクリックします。

Configuration > Tags & Profiles > WLANs

+ Add × Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Status	Name	ID	SSID

Add WLAN

General Security Advanced

Profile Name* 802.1x-WLAN Radio Policy All

SSID* 802.1x Broadcast SSID **ENABLED**

WLAN ID* 1

Status **ENABLED**

Cancel Apply to Device

ステップ 2 : **GUIから** : Security タブに移動し、暗号化方式と、802.1xが使用されている場合の認証リストを使用する限り、レイヤ2/レイヤ3セキュリティモードを設定します。次に、Update & Apply to Deviceをクリックします。

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

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

FT + PSK + ...

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Cancel

Update & Apply to Device

ポリシープロファイルの設定

ステップ 1 : **GUIから** : Configuration > Tags & Profiles > Policyの順に移動し、+Addをクリックしてポリシープロファイルを作成します。



Search Menu Items



Dashboard

Configuration > Tags & Profiles > Policy

+ Add

× Delete

Status



Policy Profile Name

ステップ 2 : 名前を追加し、Central Switchingボックスのチェックマークを外します。この設定では、コントローラがクライアント認証を処理し、FlexConnectアクセスポイントがクライアントデータパケットをローカルでスイッチします。

⚠ 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*

Description

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching DISABLED

Central Authentication ENABLED


Central DHCP ENABLED

Central Association DISABLED

Flex NAT/PAT DISABLED

Cancel

Update & Apply to Device

 注：中央スイッチングが無効な場合、関連付けとスイッチングは常にペアになっている必要があります。中央スイッチングも、Flexconnect APの使用時にすべてのポリシープロファイルで無効にする必要があります。

ステップ 3 : **GUI**から：Access Policiesタブに移動し、ワイヤレスクライアントがデフォルトでこのWLANに接続するときに割り当てることができるVLANを割り当てます。

ドロップダウンからVLAN名を1つ選択するか、ベストプラクティスとしてVLAN IDを手動で入力します。

Edit Policy Profile ✕

⚠ 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

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Disabled** ⓘ

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

ステップ 4 : **GUIから** : Advancedタブに移動し、WLANタイムアウト、DHCP、WLAN Flex Policy、およびAAAポリシーが使用されている場合にそれらを設定します。次に、Update & Apply to Deviceをクリックします。

✕
Edit Policy Profile

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

General
Access Policies
QOS and AVC
Mobility
Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

Policy Name ▾

Accounting List ▾ ⓘ

Fabric Profile ▾

mDNS Service Policy ▾ [Clear](#)

Hotspot Server ▾

User Defined (Private) Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map ▾ [Clear](#)

Flex DHCP Option for DNS ENABLED

DNS Traffic Redirect IGNORE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL ▾

Air Time Fairness Policies

2.4 GHz Policy ▾

5 GHz Policy ▾

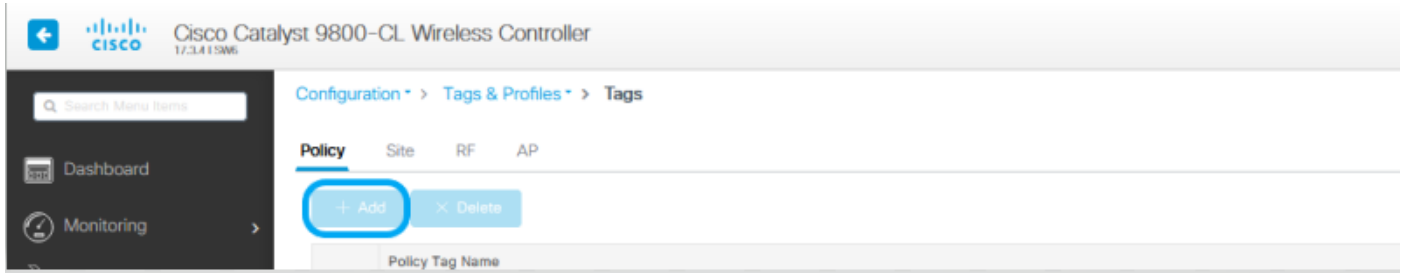
EoGRE Tunnel Profiles

↶ Cancel

↵
Update & Apply to Device

ポリシータグの設定

ステップ 1 : **GUIから** : Configuration > Tags & Profiles > Tags > Policy > +Addの順に移動します。



ステップ 2 : 名前を割り当て、事前に作成したポリシープロファイルとWLANプロファイルをマッピングします。

Edit Policy Tag



⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

Description

WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> 802.1x-WLAN	VLANX

10 items per page 1 - 1 of 1 items

Map WLAN and Policy

WLAN Profile*

Policy Profile*

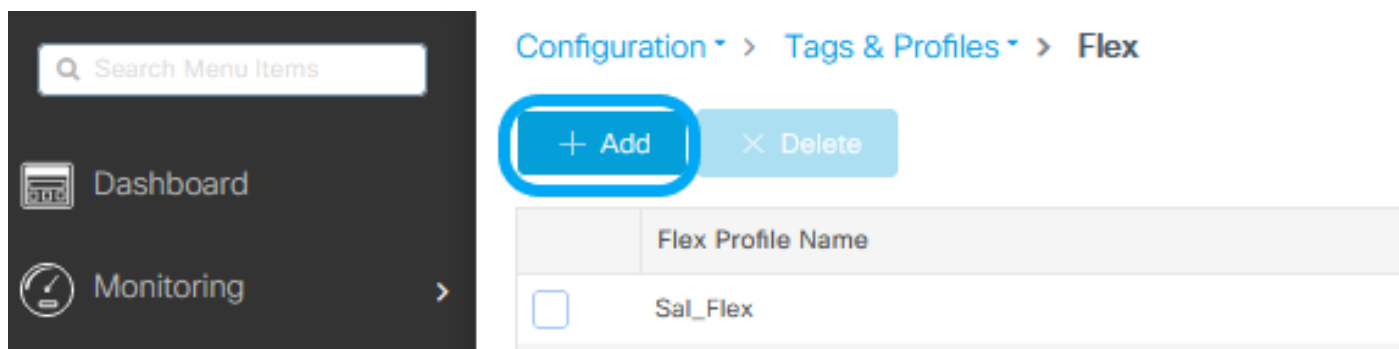


RLAN-POLICY Maps: 0

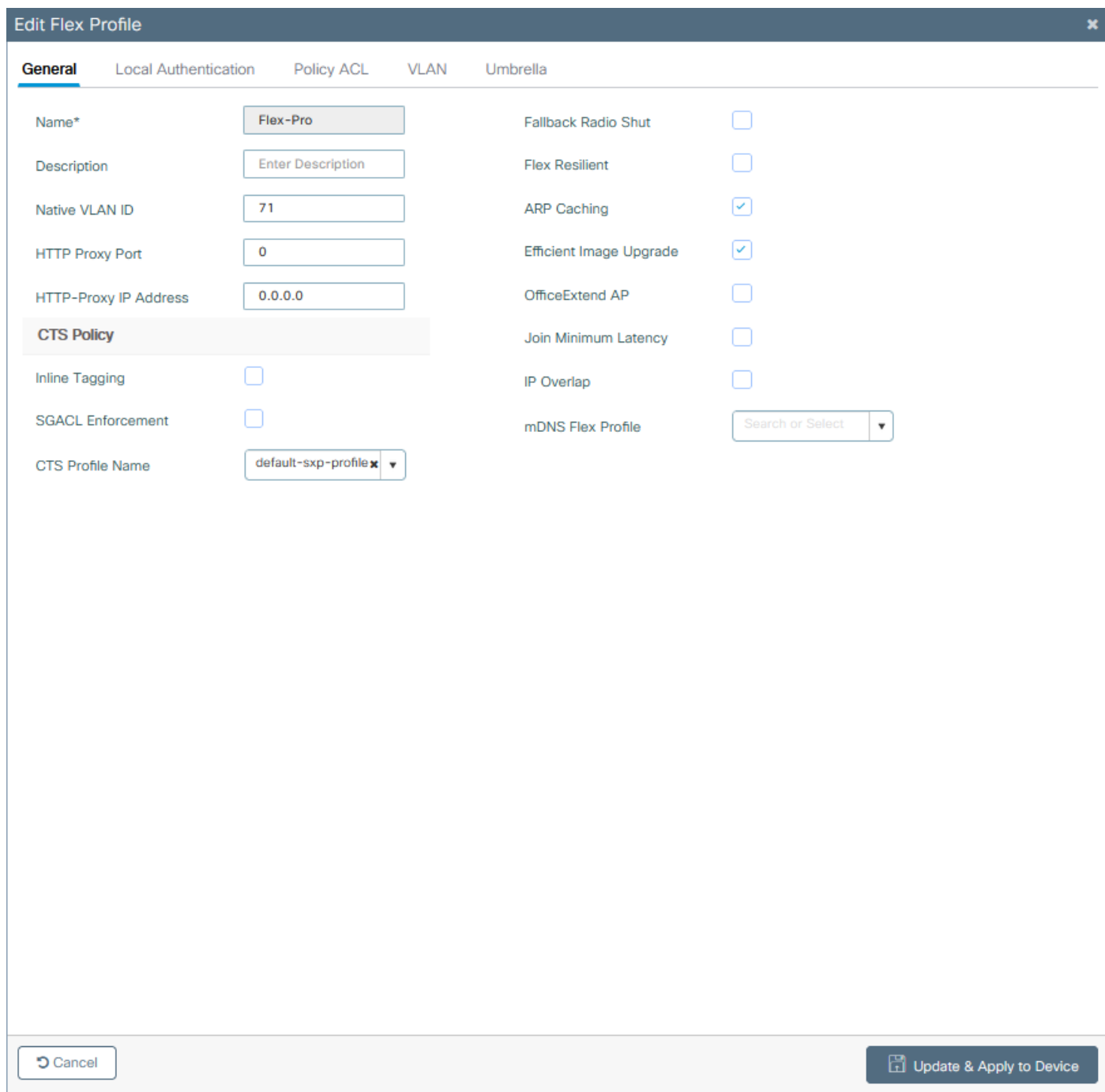
Cancel

Update & Apply to Device

ステップ1:**GUIから** : Configuration > Tags & Profiles > Flex に移動し、+Add をクリックして新しいプロファイルを作成します。



The screenshot shows the left-hand navigation menu with 'Dashboard' and 'Monitoring' options. The main content area displays the breadcrumb path 'Configuration > Tags & Profiles > Flex'. Below the path are two buttons: '+ Add' (highlighted with a red circle) and '× Delete'. A table below shows a single entry with a checkbox and the name 'Sal_Flex' under the header 'Flex Profile Name'.




The 'Edit Flex Profile' window is shown with the 'General' tab selected. The configuration fields are as follows:

Field	Value	Field	Value
Name*	Flex-Pro	Fallback Radio Shut	<input type="checkbox"/>
Description	Enter Description	Flex Resilient	<input type="checkbox"/>
Native VLAN ID	71	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 ▼		

At the bottom of the window, there are two buttons: 'Cancel' and 'Update & Apply to Device'.

 注 : ネイティブVLAN IDは、このFlex Profileを割り当てることのできるAPによって使用さ

 れるVLANを指し、APが接続されているスイッチポートでネイティブとして設定されているVLAN IDと同じである必要があります。

ステップ 2 : VLANタブで、必要なVLAN、ポリシープロファイルを介してWLANにデフォルトで割り当てられているVLAN、またはRADIUSサーバによってプッシュされたVLANを追加します。次に、Update & Apply to Deviceをクリックします。

Edit 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 📄 Update & Apply to Device

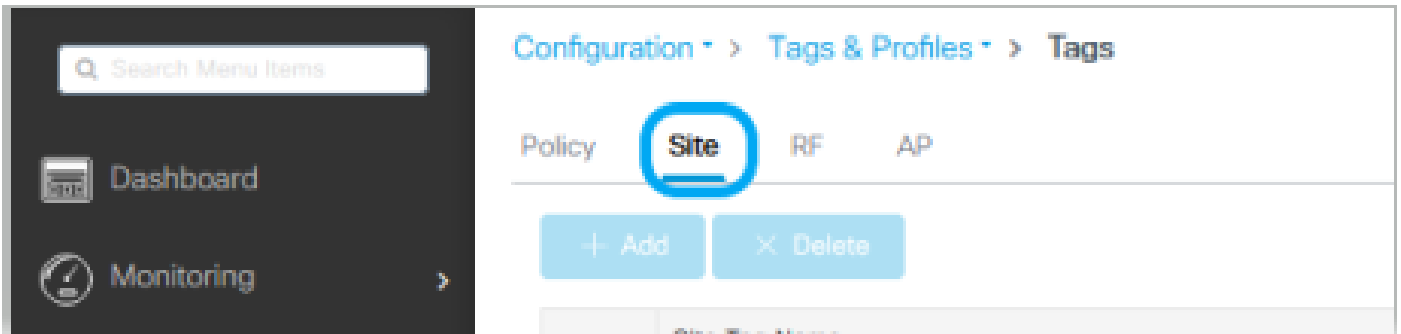
 注:Policy Profileでは、SSIDに割り当てられたデフォルトのVLANを選択します。この手順でVLAN名を使用する場合は、Flex Profile設定で同じVLAN名を使用していることを確認してください。そうしないと、クライアントはWLANに接続できません。

 注:AAAオーバーライドを使用してflexConnectのACLを設定するには、「ポリシーACL」で

 のみACLを設定します。ACLが特定のVLANに割り当てられている場合は、VLANを追加するときにACLを追加し、次に「ポリシーACL」でACLを追加します。

サイトタグの設定

ステップ 1 : **GUIから** : Configuration > Tags & Profiles > Tags > Siteの順に移動し、+Addをクリックして新しいサイトタグを作成します。Enable Local Siteボックスのチェックマークを外して、APがクライアントデータトラフィックをローカルにスイッチできるようにし、前に作成したFlex Profileを追加します。




Edit Site Tag

Name*	<input type="text" value="Flex_Site"/>
Description	<input type="text" value="Flex_Site"/>
AP Join Profile	<input type="text" value="default-ap-profile"/>
Flex Profile	<input type="text" value="Flex-Pro"/>
Fabric Control Plane Name	<input type="text"/>
Enable Local Site	<input type="checkbox"/>

Cancel

Update & Apply to Device

 注:Enable Local Siteがディセーブルになっているため、このサイトタグを割り当てられた APをFlexConnectモードに設定できます。

ステップ 2 : **GUIから** : Configuration > Wireless > Access Points > AP nameの順に移動し、Site Tag とPolicy Tag を関連付けられたAPIに追加します。これにより、APがCAPWAPトンネルを再起動し、9800 WLCに戻る可能性があります。

Search Menu Items




Dashboard



Monitoring



[Configuration](#) > [Wireless](#) > **Access Points**

 **All Access Points**

Number of AP(s): 1

General

AP Name*	<input type="text" value="talomari1"/>
Location*	<input type="text" value="default location"/>
Base Radio MAC	b4de.31d7.b920
Ethernet MAC	005d.7319.bb2a
Admin Status	<input checked="" type="checkbox"/> ENABLED
AP Mode	<input style="border: 2px solid blue; border-radius: 10px;" type="text" value="Local"/>
Operation Status	Registered
Fabric Status	Disabled
LED State	<input checked="" type="checkbox"/> ENABLED
LED Brightness Level	<input type="text" value="8"/>

Version

Primary Software Version	17.3.4.154
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	17.3.4.154
Mini IOS Version	0.0.0.0

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

Policy	<input type="text" value="Policy"/>
Site	<input style="border: 2px solid blue; border-radius: 10px;" type="text" value="Flex_Site"/>
RF	<input type="text" value="default-rf-tag"/>
Write Tag Config to AP	<input type="checkbox"/>

IP Config

CAPWAP Preferred Mode	IPv4
DHCP IPv4 Address	10.48.70.77
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Time Statistics

Up Time	0 days 0 hrs 3 mins 28 secs
Controller Association Latency	2 mins 40 secs

APが再度加入すると、APがFlexConnectモードになっていることに注意してください。

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Configuration Status	Policy Tag	Site Tag	RF Tag	Tag Source	Location	Country
talaman1	AR-AP2802I-E-K9	2		10.48.70.77	b4de.31d7.8920	Flex	Registered	Healthy	Policy	Flex_Site	default-rf-tag	Static	default location	BE

外部RADIUSサーバを使用したローカル認証

ステップ 1 : APをネットワークデバイスとしてRADIUSサーバに追加します。例については、『[RADIUSサーバとしてのIdentity Service Engine\(ISE\)の使用法](#)』を参照してください。

ステップ 2 : WLANを作成します。

設定は、以前に設定した設定と同じにすることができます。

Add WLAN

- General
- Security
- Advanced

Profile Name*	<input type="text" value="Local auth"/>	Radio Policy	<input type="text" value="All"/>
SSID*	<input type="text" value="Local auth"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="9"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

ステップ 3 : ポリシープロファイルの設定。

新しいプロファイルを作成するか、以前に設定したプロファイルを使用できます。今回は、Central Switching、Central Authentication、Central DHCP、およびCentral Association Enableの各ボックスのチェックマークを外します。

。

⚠ 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*

Local

Description

Enter Description

Status

ENABLED



Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging



SGACL Enforcement



Default SGT

2-65519

WLAN Switching Policy

Central Switching

DISABLED

Central Authentication

DISABLED

Central DHCP

DISABLED

Central Association

DISABLED

Flex NAT/PAT

DISABLED

Cancel

Apply to Device

ステップ 4 : ポリシータグの設定。

設定したWLANと作成したポリシープロファイルを関連付けます。

ステップ 5 : Flex プロファイルの設定。

Flexプロファイルを作成し、Local Authenticationタブに移動して、RADIUSサーバグループを設定し、RADIUSボックスにチェックマークを付けます。

Radius Server Group	<input type="text" value="AmmlSE"/>	LEAP	<input type="checkbox"/>
Local Accounting Radius Server Group	<input type="text" value="Select Accounting S"/>	PEAP	<input type="checkbox"/>
Local Client Roaming	<input type="checkbox"/>	TLS	<input type="checkbox"/>
EAP Fast Profile	<input type="text" value="Select Profile"/>	RADIUS	<input checked="" type="checkbox"/>

Users

Select CSV File

Username	
No items to display	

手順 6 : サイトタグの設定。
ステップ5で設定したFlex Profileを設定し、Enable Local Siteボックスのチェックマークを外します。

Add Site Tag ✕

Name*	<input type="text" value="Local Auth"/>
Description	<input type="text" value="Enter Description"/>
AP Join Profile	<input type="text" value="default-ap-profile"/> ▼
Flex Profile	<input type="text" value="Local"/> ▼
Fabric Control Plane Name	<input type="text"/> ▼
Enable Local Site	<input type="checkbox"/>

確認

GUIから：Monitoring > Wireless > Clients に移動し、Policy Manager StateとFlexConnectパラメータを確認します。

中央認証：

[General](#)[QoS Statistics](#)[ATF Statistics](#)[Mobility History](#)[Call Statistics](#)[Client Properties](#)[AP Properties](#)[Security Information](#)[Client Statistics](#)[QoS Properties](#)

MAC Address	484b.aa52.5937
IPv4 Address	172.16.76.41
User Name	address1
Policy Profile	VLAN2669
Flex Profile	RemoteSite1
Wireless LAN Id	1
Wireless LAN Name	eWLC_do1x
BSSID	38ed.18c6.902f
Uptime(sec)	9 seconds
CCX version	No CCX support
Power Save mode	OFF
Supported Rates	9.0,18.0,36.0,48.0,54.0
Policy Manager State	Run
Last Policy Manager State	IP Learn Complete
Encrypted Traffic Analytics	No
Multicast VLAN	0
Access VLAN	2669
Anchor VLAN	0
Server IP	10.88.173.94
DNS Snooped IPv4 Addresses	None
DNS Snooped IPv6 Addresses	None
IPv6 DNS Capable	No
FlexConnect Data Switching	Local
FlexConnect DHCP Status	Local
FlexConnect Authentication	Central
FlexConnect Central Association	Yes

ローカル認証:

General	QoS Statistics	ATF Statistics	Mobility History	Call Statistics
Client Properties	AP Properties	Security Information	Client Statistics	QoS Properties
MAC Address		484b.aa52.5937		
IPv4 Address		172.16.76.41		
IPv6 Address		fe80::80c6e782:7c78:68f9		
User Name		address1		
Policy Profile		VLAN2669		
Flex Profile		RemoteSite1		
Wireless LAN Id		1		
Wireless LAN Name		eWLC_do1x		
BSSID		38ed.18c6.932f		
Uptime(sec)		11 seconds		
CCX version		No CCX support		
Power Save mode		OFF		
Policy Manager State		Run		
Last Policy Manager State		IP Learn Complete		
Encrypted Traffic Analytics		No		
Multicast VLAN		0		
Access VLAN		2669		
Anchor VLAN		0		
DNS Snooped IPv4 Addresses		None		
DNS Snooped IPv6 Addresses		None		
11v DMS Capable		No		
FlexConnect Data Switching		Local		
FlexConnect DHCP Status		Local		
FlexConnect Authentication		Local		
FlexConnect Central Association		No		


次のコマンドを使用して、現在の設定を確認できます。

CLI から :

```
# show wlan { summary | id | name | all }
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

トラブルシュート

WLC 9800には、常時接続のトレース機能があります。これにより、クライアント接続に関連するすべてのエラー、警告、および通知レベルのメッセージが常にログに記録され、インシデントまたは障害状態が発生した後にログを表示できます。

 注：生成されるログの量に基づいて、数時間から数日に戻ることができます。

9800 WLCがデフォルトで収集したトレースを表示するには、SSH/Telnet経由で9800 WLCに接続し、次の手順を実行します（セッションをテキストファイルに記録していることを確認します）。

ステップ 1：問題が発生した時点までのログを追跡できるように、コントローラの現在時刻を確認します。

CLI から：

```
# show clock
```

ステップ 2：システム設定に従って、コントローラバッファまたは外部syslogからsyslogを収集します。これにより、システムの健全性とエラー（ある場合）をすばやく確認できます。

CLI から：

```
# show logging
```

ステップ 3：デバッグ条件が有効になっているかどうかを確認します。

CLI から：


```
# show debugging
IOSXE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

```
IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address _____|_____ Port
```

 注：リストされている条件は、有効な条件 (MACアドレス、IPアドレスなど) に遭遇するすべてのプロセスについて、トレースがデバッグレベルでログに記録されていることを意味します。これにより、ログの量が増加します。したがって、デバッグが必要ないときは、すべての条件をクリアすることをお勧めします。

ステップ 4：テスト対象のMACアドレスがステップ3の条件としてリストされなかったと仮定した場合、特定のMACアドレスのalways-on notice level(AIP)トレースを収集します。

CLI から：

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-
```

セッションで内容を表示するか、ファイルを外部 TFTP サーバーにコピーできます。

CLI から：

```
# more bootflash:always-on-<FILENAME.txt>  
or  
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

条件付きデバッグおよび無線アクティブトレース

常時接続トレースで、調査中の問題のトリガーを判別するのに十分な情報が得られない場合は、条件付きデバッグを有効にしてRadio Active(RA)トレースをキャプチャできます。これにより、指定された条件 (この場合はクライアントMACアドレス) と対話するすべてのプロセスにデバッグレベルのトレースを提供できます。条件付きデバッグを有効にするには、次の手順を実行します。

ステップ 5：デバッグ条件が有効になっていないことを確認します。

CLI から：


```
# clear platform condition all
```


手順 6：監視するワイヤレスクライアントのMACアドレスのデバッグ条件を有効にします。

このコマンドは、指定されたMACアドレスの監視を30分間 (1800秒) 開始します。必要に応じて、この時間を最大 2085978494 秒まで増やすことができます。

CLI から：

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

 注:複数のクライアントを同時にモニタするには、MACアドレスごとにdebug wireless mac <aaaa.bbbb.cccc>コマンドを実行します。

 注:すべての内容は後で表示できるように内部でバッファされるため、ターミナルセッションのクライアントアクティビティの出力は表示されません。

手順 7 : 監視する問題または動作を再現します。

ステップ 8 : デフォルトまたは設定されたモニタ時間がアップする前に問題が再現した場合は、デバッグを停止します。

CLI から :

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

モニター時間が経過するか、debug wireless が停止すると、9800 WLC では次の名前のローカルファイルが生成されます。

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

ステップ 9 : MAC アドレスアクティビティのファイルを収集します。 ra trace.log を外部サーバーにコピーするか、出力を画面に直接表示できます。

RAトレースファイルの名前を確認します

CLI から :

```
# dir bootflash: | inc ra_trace
```

ファイルを外部サーバーにコピーします。

CLI から :

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

内容を表示します。


CLI から :

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

ステップ 10 : 根本原因がまだ明らかでない場合は、デバッグレベルのログのより詳細なビューである内部ログを収集します。すでに収集されて内部的に保存されているデバッグログを詳細に調べたので、クライアントを再度デバッグする必要はありません。

CLI から :

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file r
```

 注 : このコマンド出力は、すべてのプロセスのすべてのログレベルのトレースを返し、非常に大量です。これらのトレースを解析する場合は、Cisco TAC にお問い合わせください。

ra-internal-FILENAME.txt を外部サーバーにコピーするか、出力を画面に直接表示できます。

ファイルを外部サーバーにコピーします。

CLI から :

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

内容を表示します。


CLI から :

```
# more bootflash:ra-internal-<FILENAME>.txt
```

ステップ 11 デバッグ条件を削除します。

CLI から :

```
# clear platform condition all
```

 注：トラブルシューティングセッションの後は、必ずデバッグ条件を削除してください。

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。