

# 9800 WLCとAruba ClearPassの設定：ゲストアクセスとFlexConnect

## 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](#)

[CWAゲストエンタープライズ導入のトラフィックフローネットワーク図](#)

[設定](#)

[ゲストワイヤレスアクセスC9800パラメータの設定](#)

[C9800：ゲスト用AAA設定](#)

[C9800：リダイレクションACLの設定](#)

[C9800：ゲストWLANプロファイルの設定](#)

[C9800：ゲストポリシープロファイルの定義](#)

[C9800 – ポリシータグ](#)

[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プロファイル](#)

[C9800:APへのタグの割り当て](#)

[Aruba CPPMインスタンスの設定](#)

[Aruba ClearPassサーバの初期設定](#)

[ライセンスの申請](#)

[サーバホスト名](#)

[CPPM Webサーバ証明書\(HTTPS\)の生成](#)

[ネットワークデバイスとしてのC9800 WLCの定義](#)

[ゲストポータルページとCoAタイマー](#)

[ClearPass：ゲストCWAの設定](#)

[ClearPassエンドポイントメタデータ属性：Allow-Guest-Internet](#)

[ClearPass再認証適用ポリシー設定](#)

[ClearPassゲストポータルリダイレクト適用プロファイルの設定](#)

[ClearPassメタデータ強制プロファイルの設定](#)

[ClearPassゲストインターネットアクセス適用ポリシーの設定](#)

[ClearPassゲストのAUP後の適用ポリシーの設定](#)

[ClearPass MAB認証サービスの設定](#)

[ClearPass Webauthサービスの設定](#)

[ClearPass:Webログイン](#)

[検証：ゲストCWA認証](#)

[付録](#)

## 概要

このドキュメントでは、Catalyst 9800ワイヤレスLANコントローラ(WLC)をAruba ClearPassと統合して、アクセスポイント(AP)のFlexconnectモードでのワイヤレスクライアントへのセントラルWeb認証(CWA)を利用するゲストWireless Service Set Identifier(SSID)を提供する方法について説明します。

ゲストワイヤレス認証は、Anonymous acceptable user policy(AUP)ページを使用してゲストポータルでサポートされます。このページは、セキュアな非武装地帯(DMZ)セグメント内のAruba Clearpassでホストされます。

## 前提条件

このガイドでは、次のコンポーネントが設定および検証されていることを前提としています。

- 関連するすべてのコンポーネントがネットワークタイムプロトコル(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 )
- 動作可能なDNSサーバ(ゲストトラフィックフロー、証明書失効リスト(CRL)の検証に必要)
- DHCPサーバの動作
- オプションの認証局(CA) ( CPPMホスト型ゲストポータルへの署名に必要 )
- Catalyst 9800 WLC
- 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 )
- VMware ESXi

## 要件

次の項目に関する知識があることが推奨されます。

- C9800の導入と新しい設定モデル
- C9800でのFlexconnectスイッチング
- 9800 CWA認証(<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html>を参照)

## 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。

- 17.3.4cが稼働するCisco Catalyst C9800-L-C
- Cisco Catalyst C9130AX
- 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

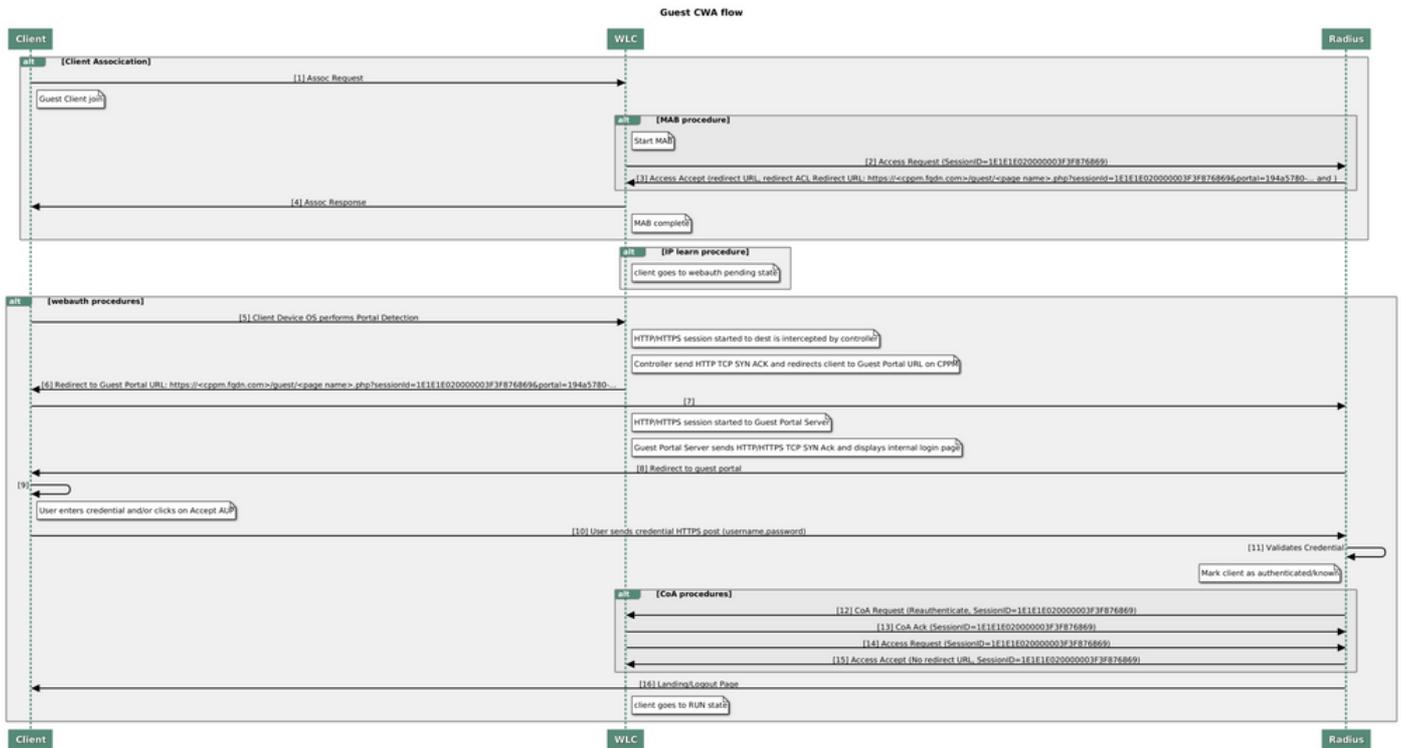
。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

次の図は、ゲストユーザがネットワークへの接続を許可される前に、ゲストWiFiアクセス交換の詳細を示しています。

- 1.ゲストユーザは、リモートオフィスのゲストWiFiに関連付けられます。
- 2.最初のRADIUSアクセス要求は、C9800によってRADIUSサーバにプロキシされます。
- 3.サーバは、ローカルMACエンドポイントデータベースで指定されたゲストMACアドレスを検索します。  
MACアドレスが見つからない場合、サーバはMAC認証バイパス(MAB)プロファイルで応答します。  
このRADIUS応答には次が含まれます。
  - URLリダイレクトアクセスコントロールリスト(ACL)
  - URL リダイレクト
- 4.クライアントは、IPアドレスが割り当てられたIP Learnプロセスを実行します。
5. C9800は、ゲストクライアント ( MACアドレスで識別される ) を「Web Auth Pending」状態に移行します。
- 6.ゲストWLANに関連する最新のデバイスOSのほとんどは、何らかのキャプティブポータル検出を実行します。  
正確な検出メカニズムは、特定のOSの実装によって異なります。クライアントOSは、RADIUS Access-Accept応答の一部として提供されるRADIUSサーバによってホストされるゲストポータルURLにC9800によってリダイレクトされたページを含むポップアップダイアログ ( 擬似ブラウザ ) を開きます。
- 7.ゲストユーザが表示されたポップアップで利用規約に同意するClearPassは、クライアントが認証を完了し、ルーティングテーブルに基づいてインターフェイスを選択することによって ( ClearPassに複数のインターフェイスがある場合 )、RADIUS認可変更(CoA)を開始したことを示すために、エンドポイントデータベース(DB)にクライアントMACアドレスのフラグを設定します。
8. WLCはゲストクライアントを「Run」状態に移行し、ユーザにはインターネットへのアクセス権が付与されますが、それ以上のリダイレクトは行われません。

注：Cisco 9800 Foreign、RADIUSを使用したアンカーワイヤレスコントローラの状態フロー図および外部でホストされるゲストポータルについては、この記事の「付録」セクションを参照してください。



ゲストセントラルWeb認証(CWA)の状態図

## CWAゲストエンタープライズ導入のトラフィックフロー

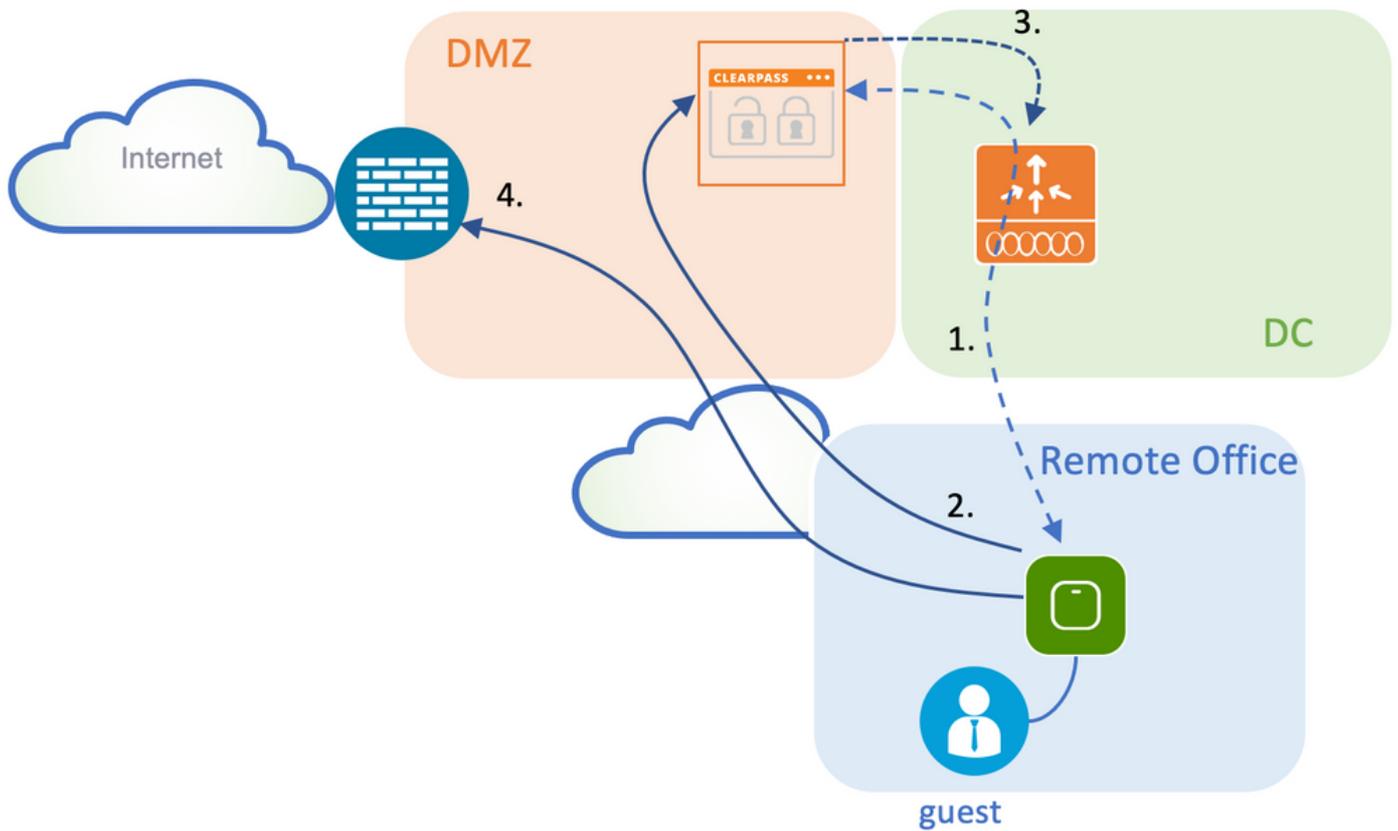
複数のブランチオフィスを持つ一般的なエンタープライズ展開では、各ブランチオフィスは、ゲストがEULAを受け入れると、ゲストポータルを介してゲストに安全なセグメント化されたアクセスを提供するように設定されます。

この設定例では、9800 CWAは、ネットワークのセキュアDMZ内のゲストユーザ用に排他的に導入される個別のClearPassインスタンスへの統合を介したゲストアクセスに使用されます。

ゲストは、DMZ ClearPassサーバが提供するWeb同意ポップアップポータルに記載された利用規約に同意する必要があります。この設定例では、匿名ゲストアクセス方式（つまり、ゲストポータルへの認証にゲストのユーザ名とパスワードは不要）に焦点を当てています。

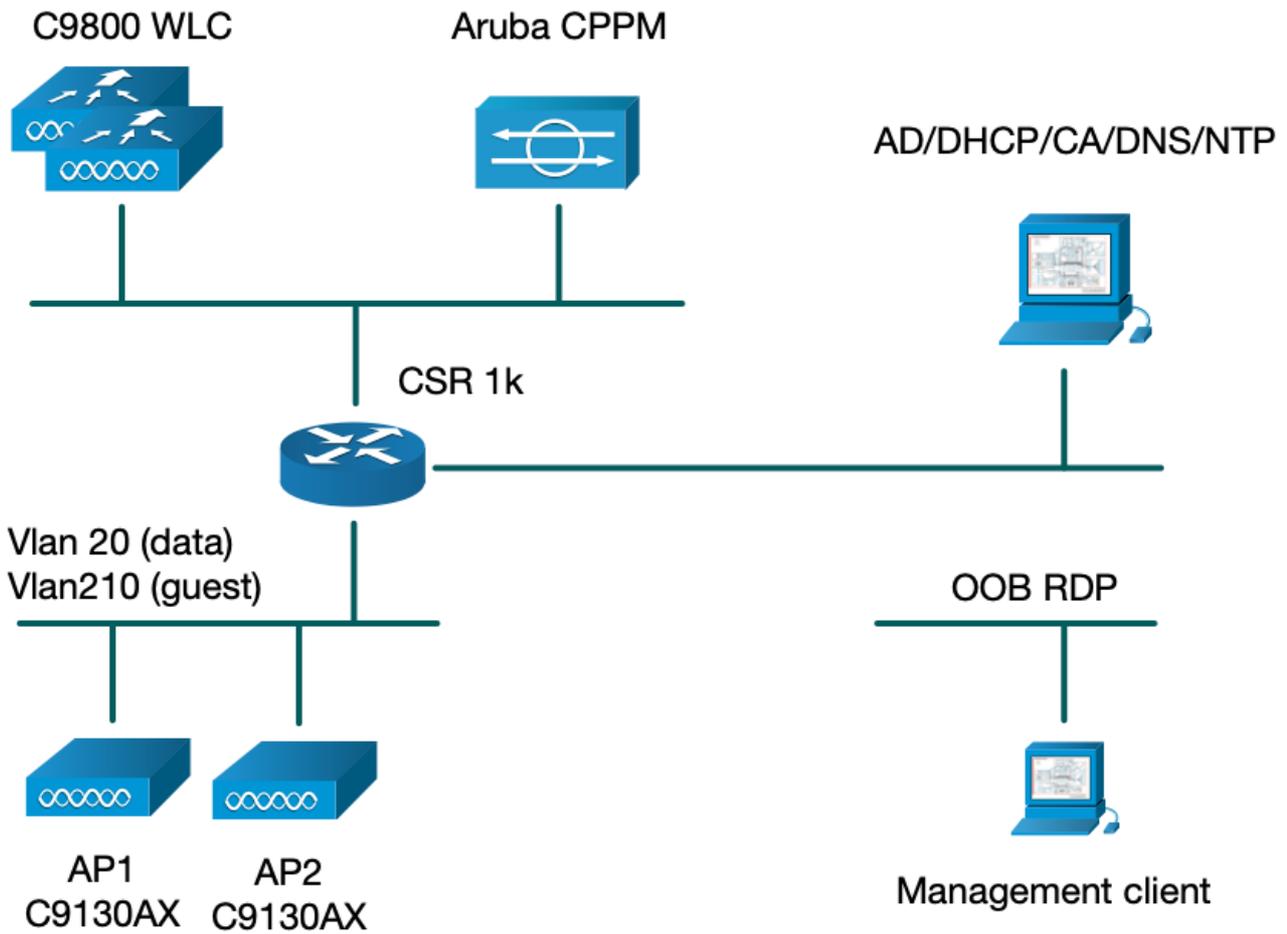
この導入に対応するトラフィックフローを図に示します。

1. RADIUS - MABフェーズ
2. ゲストポータルへのゲストクライアントURLリダイレクト
3. ゲストポータルでゲストがEULAを受け入れると、RADIUS CoA再認証がCPPMから9800 WLCに発行されます
4. ゲストはインターネットへのアクセスを許可される



## ネットワーク図

注：ラボのデモ目的では、単一または組み合わせられたAruba CPPMサーバインスタンスを使用して、ゲストと企業の両方のSSIDネットワークアクセスサーバ(NAS)機能を提供します。ベストプラクティスの実装では、独立したNASインスタンスを推奨します。



## 設定

この設定例では、C9800の新しい設定モデルを利用して、必要なプロファイルとタグを作成し、企業ブランチにdot1x企業アクセスとCWAゲストアクセスを提供します。結果の設定を次の図に示します。

AP  
MAC: xxxxx.xxxxx.xxxx

Policy Tag: PT\_CAN01

WLAN Profile: WP\_Guest  
SSID: Guest  
Layer 2: Security None  
Layer 2: MAC Filtering Enabled  
Authz List: AAA\_Authz-CPPM

Policy Profile: PP\_Guest  
Central Switching: Disabled  
Central Auth: Enabled  
Central DHCP: Disabled  
Vlan: guest (21)  
AAA Policy: Allow AAA Override Enabled  
AAA Policy: NAC State Enabled  
AAA Policy: NAC Type RADIUS  
AAA Policy Accounting List: Guest\_Accounting

Site Tag: ST\_CAN01  
Enable Local Site: Off

AP Join Profile: MyApProfile  
NTP Server: 10.0.10.4

Flex Profile: FP\_CAN01  
Native Vlan 2  
Policy ACL: CAPTIVE\_PORTAL\_REDIRECT,  
ACL CWA: Enabled  
VLAN: 21 (Guest)

RF Tag: Branch\_RF

5GHz Band RF: Typical\_Client\_Density\_rf\_5gh

2GHz Band RF: Typical\_Client\_Density\_rf\_2gh

## ゲストワイヤレスアクセスC9800パラメータの設定

### C9800 : ゲスト用AAA設定

注 : Cisco Bug ID [CSCvh03827](#)について、定義された認証、許可、アカウントिंग (AAA)サーバがロードバランスされていないことを確認します。このメカニズムは、ClearPass RADIUS交換に対してWLCのセッションIDの持続性に依存しているためです。

ステップ1:Aruba ClearPass DMZサーバを9800 WLC設定に追加し、認証方式リストを作成します。  
。 [Configuration] > [Security] > [AAA] > [Servers/Groups] > [RADIUS] > [Servers] > [+Add] に移動し、RADIUSサーバ情報を入力します。

## Create AAA Radius Server ✕

Name*	<input type="text" value="CPPM"/>
Server Address*	<input type="text" value="10.85.54.98"/>
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

Cancel

Apply to Device

ステップ2 : ゲスト用のAAAサーバグループを定義し、ステップ1.で設定したサーバをこのサーバグループに割り当てます。[Configuration] > [Security] > [AAA] > [Servers/Groups] > [RADIUS] > [Groups] > [+Add] に移動します。

## Create AAA Radius Server Group ✕

Name*	<input type="text" value="AAA_Radius_CPPM"/>
Group Type	<input type="text" value="RADIUS"/>
MAC-Delimiter	<input type="text" value="none"/>
MAC-Filtering	<input type="text" value="none"/>
Dead-Time (mins)	<input type="text" value="5"/>
Source Interface VLAN ID	<input type="text" value="1"/>

Available Servers

Assigned Servers



CPPM



Cancel

Apply to Device

ステップ3 : ゲストアクセスの認可方式リストを定義し、ステップ2で作成したサーバグループをマッピングします。[Configuration] > [Security] > [AAA] > [AAA Method List] > [Authorization] > [+Add] に移動します。Type Networkを選択し、次にステップ2で設定したAAA Server Groupを選択します。

### Quick Setup: AAA Authorization

Method List Name\*

Type\*  ⓘ

Group Type  ⓘ

Fallback to local

Authenticated

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- AAA\_Radius\_CPPM

ステップ4 : ゲストアクセス用のアカウント方式リストを作成し、ステップ2で作成したサーバグループをマッピングします。[Configuration] > [Security] > [AAA] > [AAA Method List] > [Accounting] > [+Add] に移動します。ドロップダウンメニューから[Type Identity] を選択し、次にステップ2で設定した[AAA Server Group] を選択します。

### Quick Setup: AAA Accounting

Method List Name\*

Type\*  ⓘ

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- AAA\_Radius\_CPPM

リダイレクトACLは、どのトラフィックをゲストポータルにリダイレクトする必要があるかを定義し、リダイレクトなしで通過できるようにします。この場合、ACL denyはリダイレクトまたはパススルーのバイパスを意味し、permitはポータルへのリダイレクトを意味します。トラフィッククラスごとに、アクセスコントロールエントリ(ACE)を作成し、入力トラフィックと出力トラフィックの両方に一致するACEを作成する際に、トラフィックの方向を考慮する必要があります。

[Configuration] > [Security] > [ACL] に移動し、CAPTIVE\_PORTAL\_REDIRECTという名前の新しいACLを定義します。次のACEでACLを設定します。

- ACE1:双方向のInternet Control Message Protocol(ICMP)トラフィックがリダイレクトをバイパスできるようにします。主に到達可能性を確認するために使用されます。
- ACE10、ACE30:DNSサーバ10.0.10.4への双方向DNSトラフィックフローを許可し、ポータルにリダイレクトされないようにします。ゲストフローをトリガーするには、応答のためのDNSルックアップと代行受信が必要です。
- ACE70、ACE80、ACE110、ACE120:ユーザにポータルを提示するために、ゲストキャプティブポータルへのHTTPおよびHTTPSアクセスを許可します。
- ACE150:すべてのHTTPトラフィック ( UDPポート80 ) がリダイレクトされます。

Sequence ▲	Action ▼	Source IP ▼	Source Wildcard ▼	Destination IP ▼	Destination Wildcard ▼	Protocol ▼	Source Port ▼	Destination Port ▼
1	deny	any		any		icmp		
10	deny	any		10.0.10.4		udp		eq domain
30	deny	10.0.10.4		any		udp	eq domain	
70	deny	any		10.85.54.98		tcp		eq 443
80	deny	10.85.54.98		any		tcp	eq 443	
110	deny	any		10.85.54.98		tcp		eq www
120	deny	10.85.54.98		any		tcp	eq www	
150	permit	any		any		tcp		eq www

## C9800 : ゲストWLANプロファイルの設定

ステップ1:[Configuration] > [Tags & Profiles] > [Wireless] > [+Add] に移動します。ゲストクライアントが関連付けるSSID「Guest」のプロードキャストを使用して、新しいSSIDプロファイルWP\_Guestを作成します。

## Add WLAN ✕

General Security Advanced

Profile Name*	<input type="text" value="WP_Guest"/>	Radio Policy	<input type="text" value="All"/>
SSID*	<input type="text" value="Guest"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="3"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

Cancel

Apply to Device

同じ[Add WLAN] ダイアログで、[Security] > [Layer 2] タブに移動します。

-レイヤ2セキュリティモード：なし

-MAC フィルタリング:有効

-許可リスト：ドロップダウンメニューからAAA\_Authz\_CPPM (AAA設定の一部としてステップ3で設定)

## Add WLAN ✕

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode	<input type="text" value="None"/>	Lobby Admin Access	<input type="checkbox"/>
MAC Filtering	<input checked="" type="checkbox"/>	Fast Transition	<input type="text" value="Adaptive Enab..."/>
OWE Transition Mode	<input checked="" type="checkbox"/>	Over the DS	<input type="checkbox"/>
Transition Mode WLAN ID*	<input type="text" value="1-4096"/>	Reassociation Timeout	<input type="text" value="20"/>
Authorization List*	<input type="text" value="AAA_Authz_C"/>		

Cancel

Apply to Device

C9800 : ゲストポリシープロファイルの定義

C9800 WLC GUIで、[Configuration] > [Tags & Profiles] > [Policy] > [+Add] に移動します。

[Name] : PP\_Guest

ステータス : 有効

中央スイッチング : Disabled

中央認証 : 有効

中央DHCP:Disabled

中央関連付け : Disabled

## Add Policy Profile



General

Access Policies

QOS and AVC

Mobility

Advanced

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

Name\*

PP\_Guest

Description

Policy Profile for Guest

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

ENABLED

Central DHCP

DISABLED

Central Association

DISABLED

Flex NAT/PAT

DISABLED

Cancel

Apply to Device

Add 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

---

Name*	PP_Guest	<b>WLAN Switching Policy</b>
Description	Profile for Branch Guest	Central Switching <input type="checkbox"/> DISABLED
Status	<input type="checkbox"/> DISABLED	Central Authentication <input checked="" type="checkbox"/> <b>ENABLED</b>
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
<b>CTS Policy</b>		Flex NAT/PAT <input type="checkbox"/> DISABLED
Inline Tagging	<input type="checkbox"/>	
SGACL Enforcement	<input type="checkbox"/>	
Default SGT	2-65519	

同じ[Add Policy Profile] ダイアログの[Access Policies] タブに移動します。

- RADIUSプロファイリング : 有効

- VLAN/VLANグループ : 210 (つまり、VLAN 210は各ブランチロケーションのゲストローカル VLANです)

注 : Flex用のゲストVLANは、VLANの下の9800 WLCでVLAN/VLANグループタイプVLAN番号で定義する必要はありません。

既知の不具合: Cisco Bug ID [CSCvn48234](#)では、同じFlexゲストVLANがWLCの下およびFlexプロファイルで定義されている場合、SSIDがブロードキャストされません。

⚠ 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 ⓘ

Local Subscriber Policy Name

Search or Select ▼

#### VLAN

VLAN/VLAN Group

210 ▼

Multicast VLAN

Enter Multicast VLAN

#### WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

#### URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

↶ Cancel

📄 Apply to Device

同じ[Add Policy Profile] ダイアログで、[Advanced] タブに移動します。

-Allow AAA Override : 有効

-NAC State : 有効

- NACタイプ : RADIUS

- アカウンティング一覧 : AAA\_Accounting\_CPPM ( AAA設定の一部としてステップ4で定義 )

⚠ 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)	<input type="text" value="1800"/>
Idle Timeout (sec)	<input type="text" value="300"/>
Idle Threshold (bytes)	<input type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input type="text" value="60"/>
Guest LAN Session Timeout	<input type="checkbox"/>

### DHCP

IPv4 DHCP Required	<input type="checkbox"/>
DHCP Server IP Address	<input type="text"/>

Show more >>>

### AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input checked="" type="checkbox"/>
NAC Type	<input type="text" value="RADIUS"/>
Policy Name	<input type="text" value="default-aaa-policy"/>
Accounting List	<input type="text" value="AAA_Accounting_"/>

Fabric Profile

mDNS Service Policy

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

注：C9800 WLCがRADIUS CoAメッセージを受け入れることができるようにするには、[Network Admission Control (NAC) State - Enable]が必要です。

## C9800 – ポリシータグ

C9800 GUIで、[Configuration] > [Tags & Profiles] > [Tags] > [Policy] > [+Add] に移動します。

-Name : PT\_CAN01

-説明:CAN01ブランチサイトのポリシータグ

同じダイアログボックスの[Add Policy Tag]で、[WLAN-POLICY MAPS]の下に[Add]をクリックし、以前に作成したWLANプロファイルポリシープロファイルにマッピングします。

- WLANプロフィール : WP\_Guest

- ポリシープロフィール : PP\_Guest

### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
◀ 0 ▶ 10 items per page <span>No items to display</span>	

Map WLAN and Policy

WLAN Profile\*  Policy Profile\*

---

➤ RLAN-POLICY Maps: 0

## C9800:AP加入プロフィール

C9800 WLC GUIで、[Configuration] > [Tags & Profiles] > [AP Join] > [+Add] に移動します。

-Name : Branch\_AP\_Profile

-NTP サーバ:10.0.10.4 ( ラボトポロジ図を参照 )。これは、ブランチのAPが同期に使用するNTPサーバです。

## General

Client

CAPWAP

AP

Management

Security

ICap

QoS

Name\* Description LED State LAG Mode NTP Server GAS AP Rate Limit Apphost 

## OfficeExtend AP Configuration

Local Access Link Encryption Rogue Detection  Cancel Apply to Device

## C9800:Flexプロフィール

プロフィールとタグはモジュール化されており、複数のサイトで再利用できます。

FlexConnect導入の場合、すべてのブランチサイトで同じVLAN IDを使用すると、同じFlexプロフィールを再利用できます。

ステップ1:C9800 WLCのGUIで、[Configuration] > [Tags & Profiles] > [Flex] > [+Add] に移動します。

-Name : FP\_Branch

-ネイティブVLAN ID:10 ( デフォルト以外のネイティブVLANがあり、AP管理インターフェイスが必要な場合のみ必要 )

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

Name\*  Fallback Radio Shut

Description  Flex Resilient

Native VLAN ID  ARP Caching

HTTP Proxy Port  Efficient Image Upgrade

HTTP-Proxy IP Address  OfficeExtend AP

CTS Policy Join Minimum Latency

Inline Tagging  IP Overlap

SGACL Enforcement  mDNS Flex Profile

CTS Profile Name

同じ[Add Flex Profile] ダイアログで、[Policy ACL] タブに移動し、[Add] をクリックします。

-ACL 名:CAPTIVE\_PORTAL\_REDIRECT

- 中央Web認証：有効

Flexconnect導入では、C9800ではなくAPでリダイレクションが発生するため、管理対象の各APはローカルにリダイレクトACLをダウンロードすることが想定されます。

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

ACL Name	Central Web Auth	Pre Auth URL Filter
0	10	No items to display

10 items per page

ACL Name\*

Central Web Auth

Pre Auth URL Filter

同じ[Add Flex Profile] ダイアログで、[VLAN] タブに移動し、[Add] をクリックします ( ラボトポロジ図を参照 )。

- VLAN名：ゲスト

-VLAN ID:210

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add ✕ Delete

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

◀

VLAN Name\*

VLAN Id\*

ACL Name

✓ Save ↶ Cancel

↶ Cancel Apply to Device

## C9800 – サイトタグ

9800 WLC GUIで、[Configuration] > [Tags & Profiles] > [Tags] > [Site] > [Add] に移動します。

注：説明に従って、2つのワイヤレスSSIDをサポートする必要がある各リモートサイトに一意のサイトタグを作成します。

地理的な場所、サイトタグ、およびFlex Profile設定の間には1 ~ 1のマッピングがあります。

Flex Connectサイトには、Flex Connectプロファイルが関連付けられている必要があります。Flex Connectサイトごとに最大100のアクセスポイントを設定できます。

-Name : ST\_CAN01

- AP加入プロファイル : Branch\_AP\_Profile

- フレックスプロファイル : FP\_Branch

- ローカルサイトの有効化 : Disabled

Add Site Tag ✕

Name\*

Description

AP Join Profile

Flex Profile

Fabric Control Plane Name

Enable Local Site

↶ Cancel Apply to Device

## C9800:RFプロファイル

9800 WLC GUIで、[Configuration] > [Tags & Profiles] > [Tags] > [RF] > [Add] に移動します。

-Name : Branch\_RF

- 5 GHz帯域無線周波数(RF)プロファイル : Typical\_Client\_Density\_5gh ( システム定義オプション )

- 2.4 GHz帯域RFプロファイル : Typical\_Client\_Density\_2gh ( システム定義オプション )

Add RF Tag

Name\* Branch\_RF

Description Typical Branch RF

5 GHz Band RF Profile Client\_Density\_rf\_5gh

2.4 GHz Band RF Profile Typical\_Client\_Densi

Cancel Apply to Device

## C9800:APへのタグの割り当て

展開内の個々のAPに定義済みタグを割り当てるには、次の2つのオプションがあります。

- AP名ベースの割り当て。これは、[AP Name]フィールド([Configure] > [Tags & Profiles] > [Tags] > [AP] > [Filter])のパターンに一致する正規表現ルールを利用します。

- APイーサネットMACアドレスベースの割り当て([Configure] > [Tags & Profiles] > [Tags] > [AP] > [Static] )

DNA Centerを使用した実稼働環境への導入では、手動によるAP単位の割り当てを避けるために、DNACとAPのPNPワークフローを使用するか、9800で使用可能な静的な一括のカンマ区切り値(CSV)アップロード方式を使用することを強く推奨します。[Configure] > [Tags & Profiles] > [Tags] > [AP] > [Static] > [Add] に移動します([Upload File] オプションに注意してください)。

-AP MACアドレス:<AP\_ETHERNET\_MAC>

- ポリシータグ名 : PT\_CAN01

- サイトタグ名 : ST\_CAN01

- RFタグ名 : Branch\_RF

注 : Cisco IOS®-XE 17.3.4cの時点では、コントローラの制限ごとに最大1,000個の正規表現規則があります。導入環境のサイト数がこの数を超える場合は、MAC単位の静的な割り当てを利用する必要があります。

## Associate Tags to AP



AP MAC Address*	aaaa.bbbb.cccc
Policy Tag Name	PT_CAN01
Site Tag Name	ST_CAN01
RF Tag Name	Branch_RF

Cancel

Apply to Device

注：または、AP名の正規表現ベースのタグ割り当て方法を利用するには、[Configure] > [Tags & Profiles] > [Tags] > [AP] > [Filter] > [Add] に移動します。

-Name : BR\_CAN01

- AP名regex:BR-CAN01-.(7)(このルールは、組織内で採用されているAP名の表記法に一致します。この例では、タグは、「BR\_CAN01-」の後に7文字が続くAP名フィールドを持つAPに割り当てられます)。

-Priority:1

-ポリシータグ名 : PT\_CAN01 (定義どおり)

-サイトタグ名 : ST\_CAN01

-RFタグ名 : Branch\_RF

## Associate Tags to AP



⚠ Rule "BR-CAN01" has this priority. Assigning it to the current rule will swap the priorities.

Rule Name*	BR_CAN01	Policy Tag Name	PT_CAN01
AP name regex*	BR-CAN01-.{7}	Site Tag Name	ST_CAN01
Active	YES <input checked="" type="checkbox"/>	RF Tag Name	Branch_RF
Priority*	1		

Cancel

Apply to Device

## Aruba CPPMインスタンスの設定

Aruba CPPM構成に基づく実稼働/ベストプラクティスについては、最寄りのHPE Aruba SEリソ

ースにお問い合わせください。

## Aruba ClearPassサーバの初期設定

Aruba ClearPassは、次のリソースを割り当てるESXi <>サーバ上でOpen Virtualization Format(OVF)テンプレートを使用して導入されます。

- 2つの予約済み仮想CPU
- 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 )

## ライセンスの申請

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。Platform、Access、およびOnboardライセンスを追加します。

## サーバホスト名

[Administration] > [Server Manager] > [Server Configuration] に移動し、新しくプロビジョニングされたCPPMサーバを選択します。

-Hostname : cppm

- FQDN:cppm.example.com

- 管理ポートのIPアドレスとDNSの確認

Administration » Server Manager » Server Configuration - cppm

Server Configuration - cppm (10.85.54.98)

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Hostname:	cppm				
FQDN:	cppm.example.com				
Policy Manager Zone:	default				Manage F
Enable Performance Monitoring Display:	<input checked="" type="checkbox"/> Enable this server for performance monitoring display				
Insight Setting:	<input checked="" type="checkbox"/> Enable Insight <input checked="" type="checkbox"/> Enable as Insight Master Current Master:cppm(10.85.54.98)				
Enable Ingress Events Processing:	<input type="checkbox"/> Enable Ingress Events processing on this server				
Master Server in Zone:	Primary master				
Span Port:	-- None --				
		IPv4	IPv6	Action	
Management Port	IP Address	10.85.54.98		Configure	
	Subnet Mask	255.255.255.224			
	Default Gateway	10.85.54.97			
Data/External Port	IP Address			Configure	
	Subnet Mask				
	Default Gateway				
DNS Settings	Primary	10.85.54.122		Configure	
	Secondary				
	Tertiary				
	DNS Caching	Disabled			

## CPPM Webサーバ証明書(HTTPS)の生成

この証明書は、ClearPassゲストポータルページがHTTPS経由でブランチのゲストWiFiに接続するゲストクライアントに提示されるときに使用されます。

ステップ1:CAパブリッシャチェーン証明書をアップロードします。

[Administration] > [Certificates] > [Trust List] > [Add] に移動します。

-使用方法：他を有効にする

### View Certificate Details

Subject DN:	
Issuer DN:	
Issue Date/Time:	Dec 23, 2020 16:55:10 EST
Expiry Date/Time:	Dec 24, 2025 17:05:10 EST
Validity Status:	Valid
Signature Algorithm:	SHA256WithRSAEncryption
Public Key Format:	X.509
Serial Number:	86452691282006080280068723651711271611
Enabled:	true
Usage:	<input checked="" type="checkbox"/> EAP <input checked="" type="checkbox"/> RadSec <input checked="" type="checkbox"/> Database <input checked="" type="checkbox"/> Others

ステップ2：証明書署名要求を作成します。

[Administration] > [Certificates] > [Certificate Store] > [Server Certificates] > [Usage:HTTPSサーバ証明書]。

- [Create] [Certificate Signing Request]をクリックします

- 共通名：CPPM

-組織:cppm.example.com

SANフィールドに入力してください（必要に応じて、IPおよびその他のFQDNと同様に、SANに

も共通名が存在する必要があります)。形式はDNSです。<fqdn1>,DNS:<fqdn2>,IP<ip1>。

Common Name (CN):	cppm
Organization (O):	Cisco
Organizational Unit (OU):	Engineering
Location (L):	Toronto
State (ST):	ON
Country (C):	CA
Subject Alternate Name (SAN):	DNS:cppm.example.com
Private Key Password:	.....
Verify Private Key Password:	.....
Private Key Type:	2048-bit RSA
Digest Algorithm:	SHA-512

Submit Cancel

ステップ3：選択したCAで、新しく生成されたCPPM HTTPSサービスCSRに署名します。

ステップ4:[Certificate Template] > [Web Server] > [Import Certificate] に移動します。

- 証明書タイプ：サーバ証明書

-使用方法：HTTPサーバ証明書

- 証明書ファイル：CA署名付きCPPM HTTPSサービス証明書を参照して選択します

Certificate Type:	Server Certificate
Server:	cppm
Usage:	HTTPS Server Certificate
Upload Method:	Upload Certificate and Use Saved Private Key
Certificate File:	Browse... No file selected.

Import Cancel

ネットワークデバイスとしてのC9800 WLCの定義

[Configuration] > [Network] > [Devices] > [Add] に移動します。

-Name : WLC\_9800\_Branch

- IPアドレスまたはサブネットアドレス : 10.85.54.99 ( ラボトポロジ図を参照 )

- RADIUS Shared Cisco:<WLC RADIUSパスワード>

-ベンダー名 : 『シスコ』

- [Enable RADIUS Dynamic Authorization]:1700

Device	SNMP Read Settings	SNMP Write Settings	CLI Settings	OnConnect Enforcement	Attributes
Name:	WLC_9800_Branch				
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:	Cisco 9800 WLC for Branch Guest Wifi				
RADIUS Shared Secret:	.....		Verify:	.....	
TACACS+ Shared Secret:	[redacted]		Verify:	[redacted]	
Vendor Name:	Cisco				
Enable RADIUS Dynamic Authorization:	<input checked="" type="checkbox"/> Port: 1700				
Enable RadSec:	<input type="checkbox"/>				

**Add** **Cancel**

## ゲストポータルページとCoAタイマー

設定全体を通して正しいタイマー値を設定することが非常に重要です。タイマーが調整されていない場合は、クライアントが「実行状態」でない状態で、循環するWebポータルリダイレクトが発生する可能性があります。

注意すべきタイマー：

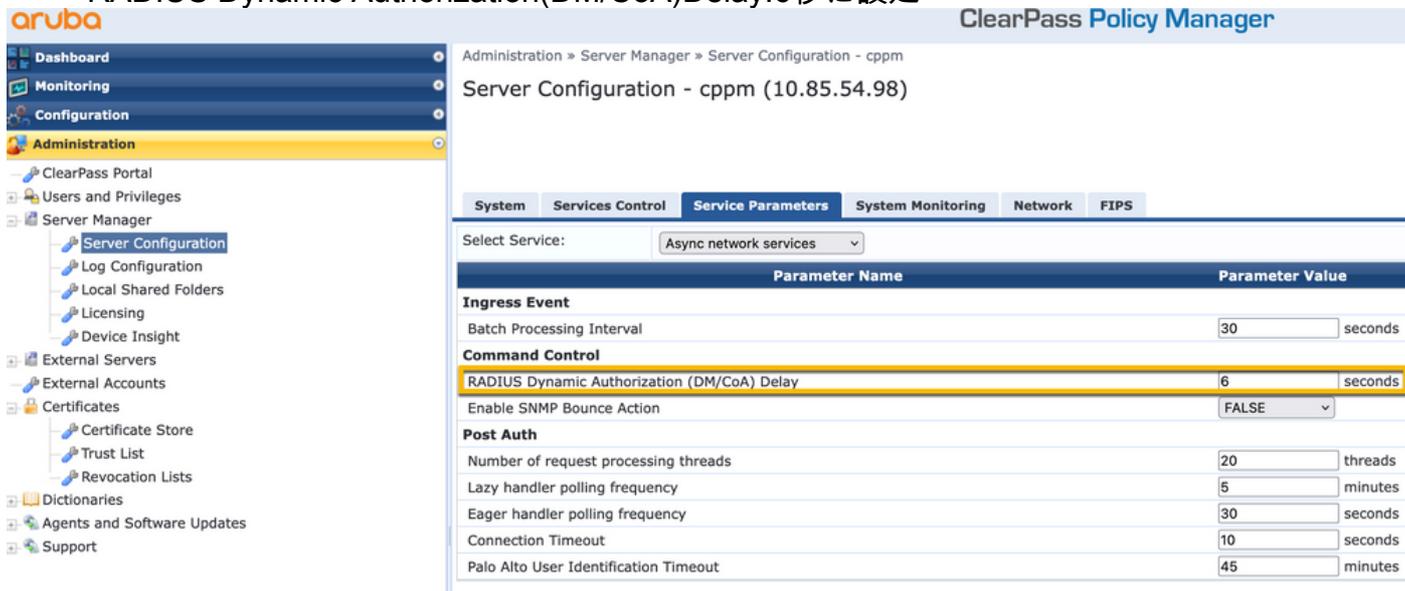
- ポータルWebログインタイマー：このタイマーは、リダイレクトページがゲストポータルページへのアクセスを許可する前にリダイレクトページを遅延させ、CPPMサービスに状態遷移を通知し、エンドポイントカスタム属性の「Allow-Guest-Internet」値を登録し、CPPMからWLCへのCoAプロセスをトリガーします。[Guest] > [Configuration] > [Pages] > [Web Logins] に移動します。
  - ゲストポータル名を選択します。ラボ匿名ゲスト登録 ( このゲストポータルページの設定は次のように詳細に説明されています )
  - [Edit] をクリックします。
  - ログイン遅延 : 6 seconds

\* Login Delay: 6 The time in seconds to delay while displaying the login message.

- ClearPass CoA遅延タイマー：これにより、ClearPassからWLCへのCoAメッセージの発信が遅延します。これは、CoA確認応答(ACK)がWLCから戻る前に、CPPMがクライアントエン

ドポイントの状態を内部で正常に移行するために必要です。ラボテストでは、WLCからの1ミリ秒未満の応答時間が示されます。また、CPPMがエンドポイント属性の更新を完了していない場合、WLCからの新しいRADIUSセッションは非認証MABサービス適用ポリシーに一致し、クライアントには再びリダイレクトページが与えられます。[CPPM] > [Administration] > [Server Manager] > [Server Configuration] に移動し、[CPPM Server] > [Service Parameters] を選択します。

- RADIUS Dynamic Authorization(DM/CoA)Delay:6秒に設定



## ClearPass : ゲストCWAの設定

ClearPass側のCWA設定は、(3)サービスポイント/ステージで構成されます。

ClearPassコンポーネント	サービスタイプ	目的
1.ポリシーマネージャ	Service ( サービス ) : MAC 認証	カスタム属性Allow-Guest-InternetがTRUEの場合は、ネットワーク接続を許可します。それ以外の場合は、Redirectをトリガーし、CWAを再認証。
2.ゲスト	Webログイン	匿名ログインAUPページを表示します。
3.ポリシーマネージャ	Service ( サービス ) : Web ベースの認証	Post-auth set custom attribute Allow-Guest-Internet = TRUE。エンドポイントを既知に更新。カスタム属性Allow-Guest-InternetがTRUEに設定します。COA:再認証

## ClearPassエンドポイントメタデータ属性 : Allow-Guest-Internet

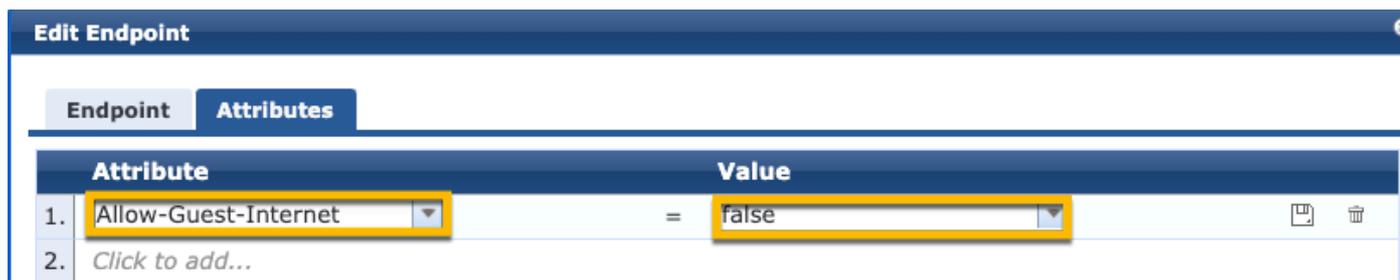
タイプがブールのメタデータ属性を作成して、クライアントが「Webauth Pending」と「Run」状態の間を遷移するときにゲストエンドポイントの状態を追跡します。

- wifiに接続する新しいゲストには、デフォルトのメタデータ属性がAllow-Guest-Internet=falseに設定されています。この属性に基づいて、クライアント認証はMABサービスを通過します

- [AUP Accept]ボタンをクリックすると、ゲストクライアントのメタデータ属性がAllow-Guest-Internet=trueに更新されます。この属性をTrueに設定した後続のMABは、インターネットへのリダイレクトされないアクセスを許可します

[ClearPass] > [Configuration] > [Endpoints]に移動し、リストから任意のエンドポイントを選択して、[Attributes] タブをクリックし、値をfalseにしてAllow-Guest-Internetを追加し、さらに値をSaveにします。

注：同じエンドポイントを編集し、この属性を後で削除することもできます。この手順では、ポリシーで使用できるエンドポイントメタデータDBにフィールドを作成するだけです。



The screenshot shows the 'Edit Endpoint' window with the 'Attributes' tab selected. It contains a table with two columns: 'Attribute' and 'Value'. The first row shows 'Allow-Guest-Internet' as the attribute and 'false' as the value. The second row is a placeholder 'Click to add...'. There are also icons for adding and deleting attributes.

	Attribute	Value		
1.	Allow-Guest-Internet	= false		
2.	Click to add...			

### ClearPass再認証適用ポリシー設定

ゲストポータルページでクライアントがAUPを受け入れた直後にゲストクライアントに割り当てられる強制プロファイルを作成します。

[ClearPass] > [Configuration] > [Profiles] > [Add] に移動します。

- テンプレート : RADIUS動的認可

-Name : Cisco\_WLC\_Guest\_COA

## Enforcement Profiles

Profile	Attributes	Summary		
Template:	RADIUS Dynamic Authorization			
Name:	Cisco_WLC_Guest_COA			
Description:				
Type:	RADIUS_CoA			
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop			
Device Group List:	<div style="display: flex; align-items: center;"> <div style="flex-grow: 1;"> <table border="1" style="width: 100%; height: 50px;"> <tr> <td style="width: 50%;"></td> <td style="width: 50%;"></td> </tr> </table> </div> <div style="margin-left: 10px;"> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px; width: 60px; text-align: center;">Remove</div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px; width: 60px; text-align: center;">View Details</div> <div style="border: 1px solid #ccc; padding: 2px; width: 60px; text-align: center;">Modify</div> </div> </div> <div style="margin-top: 5px;"> <div style="border: 1px solid #ccc; padding: 2px; width: 100%;">--Select--</div> </div>			

半径 : IETF	Calling-Station-Id	%{Radius:IETF:Calling-Station
半径 : Cisco	Cisco-AVPair	subscriber:command=reauthen
半径 : Cisco	Cisco-AVPair	e
半径 : Cisco	Cisco-AVPair	%{Radius:Cisco:Cisco-
		AVPair:subscriber:audit-sessio
		subscriber:reauthenticate-type
		type=last

### ClearPassゲストポータルリダイレクト適用プロファイルの設定

「Allow-Guest-Internet」が「true」に設定されたCPPMエンドポイントデータベースでMACアドレスが見つからない場合、初期MABフェーズでゲストに適用される強制プロファイルを作成します。

これにより、9800 WLCは外部認証のためにゲストクライアントをCPPMゲストポータルにリダイレクトします。

[ClearPass] > [Enforcement] > [Profiles] > [Add] に移動します。

-Name : Cisco\_Portal\_Redirect

-タイプ:RADIUS

-Action:Accept

## Enforcement Profiles

Profile	Attributes	Summary
Template:	Aruba RADIUS Enforcement	
Name:	Cisco_Portal_Redirect	
Description:		
Type:	RADIUS	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:		<div style="text-align: right;"> <input type="button" value="Remove"/>   <input type="button" value="View Details"/>   <input type="button" value="Modify"/> </div>
	--Select--	

ClearPassリダイレクト強制プロファイル

同じダイアログの[Attributes] タブで、次のイメージに従って2つの属性を設定します。

Enforcement Profiles - Cisco\_Portal\_Redirect

Summary	Profile	Attributes
Type	Name	Value
1. Radius: Cisco	Cisco-AVPair	= url-redirect-acl=CAPTIVE_PORTAL_REDIRECT
2. Radius: Cisco	Cisco-AVPair	= url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=%{Connection:Client-Mac-Address-Hyphen}&switchip=%{Radius:IETF:NAS-IP-Address}

ClearPassリダイレクトプロファイル属性

url-redirect-acl属性は、C9800で作成されたACLの名前であるCAPTIVE-PORTAL-REDIRECTに設定されます。

注：RADIUSメッセージでは、ACLへの参照だけが渡され、ACLの内容は渡されません。9800 WLC上で作成されたACLの名前が、次に示すように、このRADIUS属性の値と正確に一致することが重要です。

url-redirect属性は、複数のパラメータで構成されます。

- ゲストポータルがホストされているターゲット URL (<https://cppm.example.com/guest/iaccept.php>)
- ゲストクライアントMAC、マクロ%{Connection:Client-Mac-Address-Hyphen}
- 認証者IP (9800 WLCがリダイレクトをトリガー)、マクロ%{Radius:IETF:NAS-IP-Address}
- cmd-login action

ClearPass Guest Web LoginページのURLは、[CPPM] > [Guest] > [Configuration] > [Pages] > [Web Logins] > [Edit] に移動すると表示されます。

この例では、CPPMのゲストポータルページ名はiacceptとして定義されています。

注：ゲストポータルページの設定手順は次のとおりです。

The screenshot shows the Aruba configuration interface. On the left is a navigation menu with categories: Guest, Devices, Onboard, Configuration (highlighted), Authentication, Content Manager, Guest Manager, Hotspot Manager, Pages (expanded to show Fields, Forms, List Views, Self-Registrations, Web Logins, and Web Pages), and Web Pages. The main content area shows the breadcrumb 'Home » Configuration » Pages » Web Logins' and the title 'Web Login (Lab Anonymous Guest Registration)'. Below the title is a form with the following fields:

- \* Name: Lab Anonymous Guest Registration (with a link: Enter a name for this web login page.)
- Page Name: iaccept (highlighted with a yellow box, with a link: Enter a page name for this web login. The web login will be accessible from "/guest/)
- Description: (with a link: Comments or descriptive text about the web login)
- \* Vendor Settings: Aruba Networks (with a link: Select a predefined group of settings suitable)

注：シスコデバイスの場合、通常はaudit\_session\_idが使用されますが、他のベンダーではサポートされていません。

### ClearPassメタデータ強制プロファイルの設定

CPPMによる状態遷移の追跡に使用されるEndpointメタデータ属性を更新するように、強制プロファイルを作成します。

このプロファイルは、エンドポイントデータベースのゲストクライアントMACアドレスエントリに適用され、「Allow-Guest-Internet」引数を「true」に設定します。

[ClearPass] > [Enforcement] > [Profiles] > [Add] に移動します。

- テンプレート：ClearPassエンティティ更新の強制

- タイプ: Post\_Authentication

## Enforcement Profiles

Profile	Attributes	Summary
Template:	ClearPass Entity Update Enforcement	
Name:	Make-Cisco-Guest-Valid	
Description:		
Type:	Post_Authentication	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="display: flex; justify-content: flex-end; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 5px;">Remove</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">View Details</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">Modify</div> </div>	

同じダイアログで、[Attributes] タブを選択します。

-タイプ:エンドポイント

-Name : Allow-Guest-Internet

注：この名前をドロップダウンメニューに表示するには、手順で説明されているように、少なくとも1つのエンドポイントに対してこのフィールドを手動で定義する必要があります。

-値:true

## Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Endpoint	Allow-Guest-Internet	= true
2. Click to add...		

## ClearPassゲストインターネットアクセス適用ポリシーの設定

[ClearPass] > [Enforcement] > [Policies] > [Add] に移動します。

-Name : WLCのCiscoゲスト許可

-適用タイプ : RADIUS

-デフォルトプロファイル : Cisco\_Portal\_Redirect

## Enforcement Policies

Enforcement	Rules	Summary
Name:	WLC Cisco Guest Allow	
Description:		
Enforcement Type:	<input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+ <input type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application <input type="radio"/> Event	
Default Profile:	Cisco_Portal_Redirect	<input type="button" value="View Details"/> <input type="button" value="Modify"/>

同じダイアログで、[Rules] タブに移動し、[Add Rule] をクリックします。

-タイプ:エンドポイント

-Name : Allow-Guest-Internet

-Operator : [Equals]

- 値True

- プロファイル名/追加する選択 : [RADIUS] [Allow Access Profile]

Conditions			
Match ALL of the following conditions:			
Type	Name	Operator	Value
1. Endpoint	Allow-Guest-Internet	EQUALS	true
2.	Click to add...		

Enforcement Profiles	
Profile Names:	[RADIUS] [Allow Access Profile] <input type="button" value="Move Up ↑"/> <input type="button" value="Move Down ↓"/> <input type="button" value="Remove"/> --Select to Add--

### ClearPassゲストのAUP後の適用ポリシーの設定

[ClearPass] > [Enforcement] > [Policies] > [Add] に移動します。

-Name : Cisco WLC Webauth適用ポリシー

- 適用タイプ : WEBAUTH ( SNMP/エージェント/CLI/CoA )

- デフォルトプロファイル : [RADIUS\_CoA] Cisco\_Reauthenticate\_Session

## Enforcement Policies

Enforcement	Rules	Summary
Name:	Cisco WLC Webauth Enforcement Policy	
Description:		
Enforcement Type:	<input type="radio"/> RADIUS <input type="radio"/> TACACS+ <input checked="" type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application <input type="radio"/> Event	
Default Profile:	[RADIUS_CoA] Cisco_Reauth	<input type="button" value="View Details"/> <input type="button" value="Modify"/>

同じダイアログで、[Rules] > [Add] に移動します。

-条件 : [Authentication]

-Name : ステータス

-Operator : [Equals]

-値:User

- プロファイル名 : <それぞれに追加>

- [Post Authentication] [Update Endpoint Known]

- [認証後] [Make-Cisco-Guest-Valid]

- [RADIUS\_CoA] [Cisco\_WLC\_Guest\_COA]

**Rules Editor**

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Authentication	Status	EQUALS	User
2.	Click to add...		

Enforcement Profiles

Profile Names:	[Post Authentication] [Update Endpoint Known] [Post Authentication] Make-Cisco-Guest-Valid [RADIUS_CoA] Cisco_WLC_Guest_COA	<input type="button" value="Move Up ↑"/> <input type="button" value="Move Down ↓"/> <input type="button" value="Remove"/>
	<input type="text" value="--Select to Add--"/>	

注：継続的なゲストポータルリダイレクト疑似ブラウザのポップアップが表示されるシナリオが発生した場合は、CPPMタイマーの調整が必要か、CPPMと9800 WLCの間でRADIUS CoAメッセージが正しく交換されていないことを示しています。これらのサイトを確認します。

- [CPPM] > [Monitoring] > [Live Monitoring] > [Access Tracker] に移動し、RADIUSログエントリにRADIUS CoAの詳細が含まれていることを確認します。

- 9800 WLCで、[Troubleshooting] > [Packet Capture] に移動し、RADIUS CoAパケットの到着が予想されるインターフェイスでpcapを有効にし、RADIUS CoAメッセージがCPPMから受信され

ることを確認します。

## ClearPass MAB認証サービスの設定

サービスは、属性値(AV)ペアのRADIUSで照合されます。『シスコ | CiscoAVPair | cisco-wlan-ssid

[ClearPass] > [Configuration] > [Services] > [Add] に移動します。

[Service]タブ :

-Name : ゲストポータル – Mac認証

-タイプ:MAC 認証

- その他のオプション : [Authorization]、[Profile Endpoints]の選択

- 一致ルールの追加 :

-タイプ:Radius: 『シスコ

-Name : Cisco-AVPair

-Operator : [Equals]

-値:cisco-wlan-ssid=Guest ( 設定したゲストSSID名と一致 )

注 : 「Guest」は、9800 WLCによってブロードキャストされるゲストSSIDの名前です。

Configuration » Services » Add

### Services

Service Authentication Authorization Roles Enforcement Profiler Summary

Type:

Name:

Description:

Monitor Mode:  Enable to monitor network access without enforcement

More Options:  Authorization  Audit End-hosts  Profile Endpoints  Accounting Proxy

Service Rule

Matches  ANY or  ALL of the following conditions:

Type	Name	Operator	Value	
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4.	Radius:Cisco	Cisco-AVPair	EQUALS	cisco-wlan-ssid=Guest

同じダイアログで、[Authentication] タブを選択します。

-認証方式:[MAC AUTH]を削除し、[Allow All MAC AUTH]を追加します。

- 認証元 : [エンドポイントリポジトリ][ローカルSQL DB]、[ゲストユーザリポジトリ][ローカルSQL DB]

aruba ClearPass Policy Manager

Configuration » Services » Edit - GuestPortal - Mac Auth

### Services - GuestPortal - Mac Auth

Summary Service **Authentication** Authorization Roles Enforcement Profiler

Authentication Methods: [Allow All MAC AUTH]

Authentication Sources: [Endpoints Repository] [Local SQL DB] [Guest User Repository] [Local SQL DB]

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

同じダイアログで、[Enforcement] タブを選択します。

– 適用ポリシー : WLCのCiscoゲスト許可

Configuration » Services » Add

## Services

Service Authentication Roles **Enforcement** Summary

Use Cached Results:  Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: WLC Cisco Guest Allow **Modify**

**Enforcement Policy Details**

Description:	MAB Enforcement Redirect
Default Profile:	Cisco_Portal_Redirect
Rules Evaluation Algorithm:	first-applicable

Conditions	Enforcement Profiles
1. (Endpoint:Allow-Guest-Internet EQUALS true)	[Allow Access Profile]

同じダイアログで、[Enforcement] タブを選択します。

Configuration » Services » Add

## Services

Service Authentication Authorization Roles Enforcement **Profiler** Summary

Endpoint Classification: Select the classification(s) after which an action must be triggered -

RADIUS CoA Action: Cisco\_Reauthenticate\_Session **View Details** **Modify**

## ClearPass Webauthサービスの設定

[ClearPass] > [Enforcement] > [Policies] > [Add] に移動します。

-Name : Guest\_Portal\_Webauth

-タイプ:Web ベースの認証

Configuration » Services » Add

### Services

Service	Authentication	Roles	Enforcement	Summary
Type:	Web-based Authentication			
Name:	Guest			
Description:				
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance			
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name			
1.	Host	CheckType		
2.	Click to add...			

同じダイアログの[Enforcement] タブで、[Enforcement Policy: Cisco WLC Webauth Enforcement Policy]。

Configuration » Services » Add

### Services

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	Cisco WLC Webauth Enforcement Policy <a href="#">Modify</a>			<a href="#">Add New Enforcement Poli</a>
Enforcement Policy Details				
Description:				
Default Profile:	Cisco_Reauthenticate_Session			
Rules Evaluation Algorithm:	first-applicable			
Conditions	Enforcement Profiles			
1. (Authentication:Status EQUALS User)	[Update Endpoint Known], Make-Cisco-Guest-Valid, Cisco_Reauthenticate_Session			

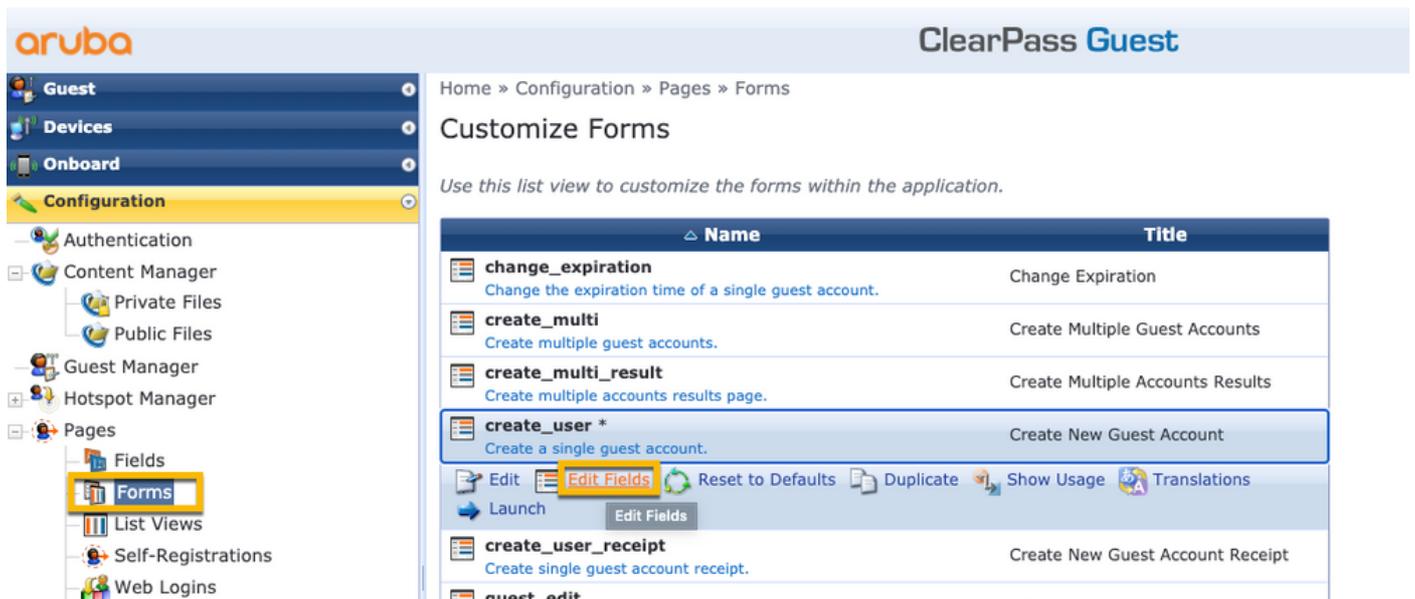
## ClearPass:Webログイン

Anonymous AUP Guest Portalページでは、パスワードフィールドのない単一のユーザ名を使用します。

使用するユーザ名には、次のフィールドが定義または設定されている必要があります。

username\_auth |ユーザ名認証 : | 1

ユーザの「username\_auth」フィールドを設定するには、そのフィールドを最初に「edit user」フォームで公開する必要があります。[ClearPass] > [Guest] > [Configuration] > [Pages] > [Forms] に移動し、[create\_user] フォームを選択します。



visitor\_name ( 行20 ) を選択し、[Insert After] をクリックします。

Home » Configuration » Pages » Forms

## Customize Form Fields (create\_user)

Use this list view to modify the fields of the form **create\_user**.

Rank	Field	Type	Label	Description
1	enabled	dropdown	Account Status:	Select an option for changing the status of this account.
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.
13	sponsor_profile_name	text	Sponsor's Profile:	Profile of the person sponsoring this account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.
20	<b>visitor_name</b>	text	Guest's Name:	Name of the guest.

[Edit](#)
[Edit Base Field](#)
[Remove](#)
[Insert Before](#)
[Insert After](#)
[Disable Field](#)

## Customize Form Field (new)

Use this form to add a new field to the form `create_user`.

Form Field Editor	
* Field Name:	<input type="text" value="username_auth"/> <small>Select the field definition to attach to the form.</small>
<b>Form Display Properties</b> <small>These properties control the user interface displayed for this field.</small>	
Field:	<input checked="" type="checkbox"/> Enable this field <small>When checked, the field will be included as part of the form.</small>
* Rank:	<input type="text" value="22"/> <small>Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.</small>
* User Interface:	<input type="text" value="No user interface"/> <input type="button" value="Revert"/> <small>The kind of user interface element to use when entering or editing this field.</small>
<b>Form Validation Properties</b> <small>These properties control how the value of this field is checked.</small>	
Field Required:	<input type="checkbox"/> Field value must be supplied <small>Select this option if the field cannot be omitted or left blank.</small>
Initial Value:	<input type="text" value="1"/> <input type="button" value="Revert"/> <small>Value to initialize this field with when the form is first displayed.</small>
* Validator:	<input type="text" value="IsValidBool"/> <small>The function used to validate the contents of a field.</small>
Validator Param:	<input type="text" value="(None)"/> <small>Optional name of field whose value will be supplied as the argument to a validator.</small>
Validator Argument:	<input type="text"/> <small>Optional value to supply as the argument to a validator.</small>
Validation Error:	<input type="text"/> <small>The error message to display if the field's value fails validation and the validator does not return an error message directly.</small>

ここで、AUPゲストポータルページの背後で使用するユーザ名を作成します。

[CPPM] > [Guest] > [Guest] > [Manage Accounts] > [Create] に移動します。

- ゲスト名 : GuestWiFi

- 会社名 : 『シスコ

- 電子メールアドレス : guest@example.com

- ユーザ名認証 : ユーザ名のみを使用してゲストアクセスを許可する : 有効

- アカウントの有効化 : 現在

- アカウントの有効期限 : アカウントは期限切れになりません

- 使用条件 : 私がスポンサーです。有効

## Create Guest Account

New guest account being created by **admin**.

Create New Guest Account	
* Guest's Name:	<input type="text" value="GuestWiFi"/> Name of the guest.
* Company Name:	<input type="text" value="Cisco"/> Company name of the guest.
* Email Address:	<input type="text" value="guest@example.com"/> The guest's email address. This will become their username to log into the network.
Username Authentication:	<input checked="" type="checkbox"/> Allow guest access using their username only Guests will require the login screen setup for username-based authentication as well.
Account Activation:	<input type="text" value="Now"/> Select an option for changing the activation time of this account.
Account Expiration:	<input type="text" value="Account will not expire"/> Select an option for changing the expiration time of this account.
* Account Role:	<input type="text" value="[Guest]"/> Role to assign to this account.
Password:	<b>281355</b>
Notes:	<input type="text"/>
* Terms of Use:	<input checked="" type="checkbox"/> I am the sponsor of this account and accept the <a href="#">terms of use</a>
<input type="button" value="Create"/>	

Webログインフォームを作成します。[CPPM] > [Guest] > [Configuration] > [Web Logins] に移動します。

事後認証セクションのエンドポイント属性：

username |ユーザー名  
visitor\_name |訪問者名  
cn |訪問者名  
visitor\_phone |ビジターの電話番号  
電子メール |電子メール  
メール |電子メール  
sponsor\_name |スポンサー名  
sponsor\_email |スポンサー電子メール  
**Allow-Guest-Internet | true**



CPPMで、[Live Monitoring] > [Access Tracker] に移動します。

MABサービスに接続してトリガーする新しいゲストユーザ。

[Summary]タブ :

Summary	Input	Output	RADIUS CoA
Login Status:		ACCEPT	
Session Identifier:		R0000471a-01-6282a110	
Date and Time:		May 16, 2022 15:08:00 EDT	
End-Host Identifier:		d4-3b-04-7a-64-7b (Computer / Windows / Windows)	
Username:		d43b047a647b	
Access Device IP/Port:		10.85.54.99:73120 (WLC_9800_Branch / Cisco)	
Access Device Name:		wlc01	
System Posture Status:		UNKNOWN (100)	

Policies Used -	
Service:	Guest SSID - GuestPortal - Mac Auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository]
Roles:	[Employee], [User Authenticated]
Enforcement Profiles:	Cisco_Portal_Redirect

◀ ◀ Showing 8 of 1-8 records ▶ ▶ [Change Status](#) [Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

同じダイアログで、[Input] タブに移動します。

**Request Details**

Summary Input Output **RADIUS CoA**

Username:	d43b047a647b
End-Host Identifier:	d4-3b-04-7a-64-7b (Computer / Windows / Windows)
Access Device IP/Port:	10.85.54.99:73120 (WLC_9800_Branch / Cisco)

**RADIUS Request**

Radius:Airespace:Airespace-Wlan-Id	4
Radius:Cisco:Cisco-AVPair	audit-session-id=6336550A00006227CE452457
Radius:Cisco:Cisco-AVPair	cisco-wlan-ssid=Guest
Radius:Cisco:Cisco-AVPair	client-iif-id=1728058392
Radius:Cisco:Cisco-AVPair	method=mab
Radius:Cisco:Cisco-AVPair	service-type=Call Check
Radius:Cisco:Cisco-AVPair	vlan-id=21
Radius:Cisco:Cisco-AVPair	wlan-profile-name=WP_Guest
Radius:IETF:Called-Station-Id	14-16-9d-df-16-20:Guest
Radius:IETF:Calling-Station-Id	d4-3b-04-7a-64-7b

◀ ◀ Showing 8 of 1-8 records ▶ ▶ **Change Status** **Show Configuration** **Export** **Show Logs** **Close**

同じダイアログで、[Output] タブに移動します。

**Request Details**

Summary Input **Output** RADIUS CoA

Enforcement Profiles:	Cisco_Portal_Redirect
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

**RADIUS Response**

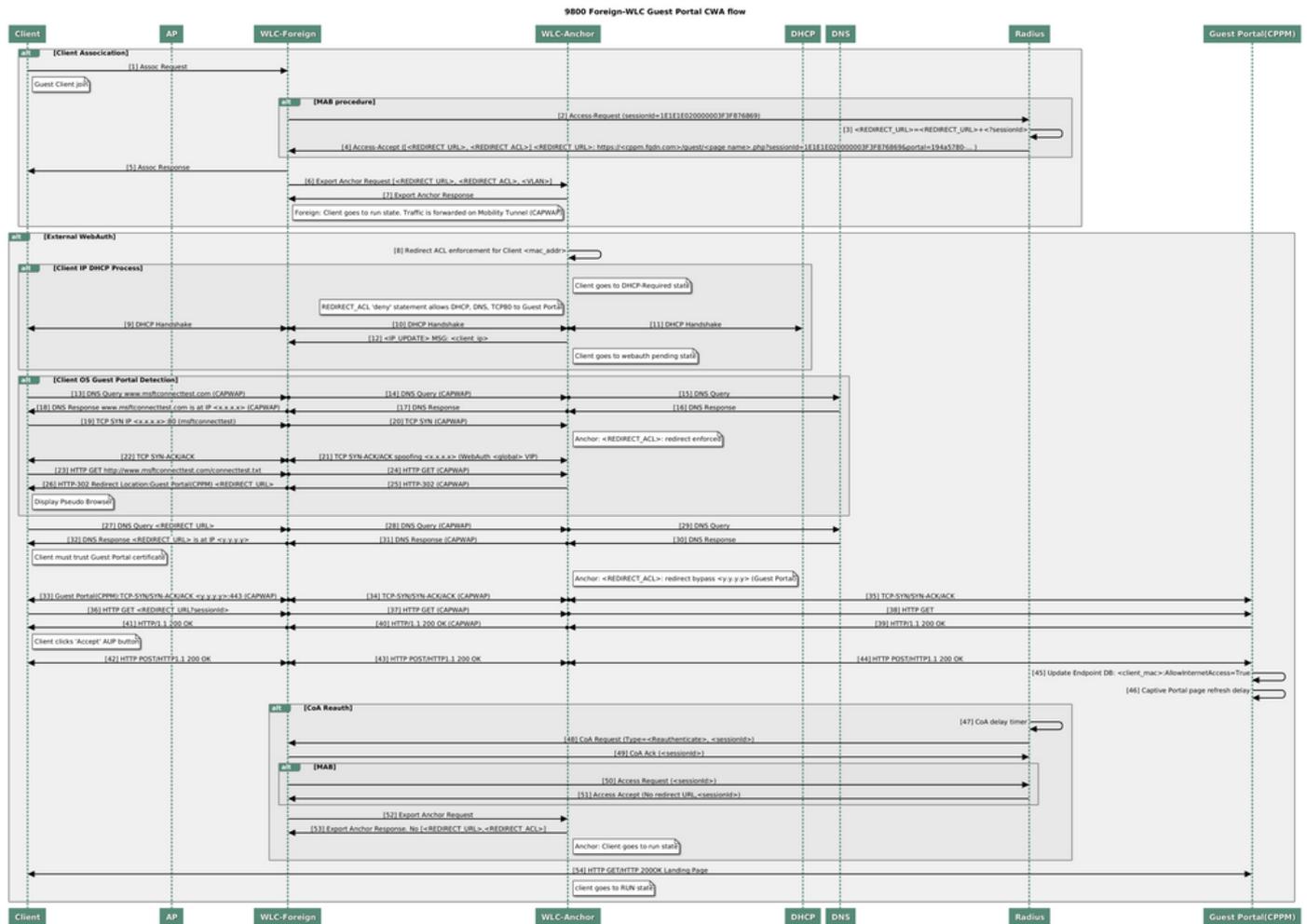
Radius:Cisco:Cisco-AVPair	url-redirect-acl=CAPTIVE_PORTAL_REDIRECT
Radius:Cisco:Cisco-AVPair	url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=d4-3b-04-7a-64-7b&switchip=10.85.54.99

◀ ◀ Showing 8 of 1-8 records ▶ ▶ **Change Status** **Show Configuration** **Export** **Show Logs** **Close**

## 付録

参考として、Cisco 9800外部、アンカーコントローラとRADIUSサーバおよび外部ホスト型ゲス

トポータルとのインタラクションの状態フロー図を示します。



アンカーWLCを使用したゲストセントラルWeb認証の状態図

## 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。