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

内容

関連情報

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。

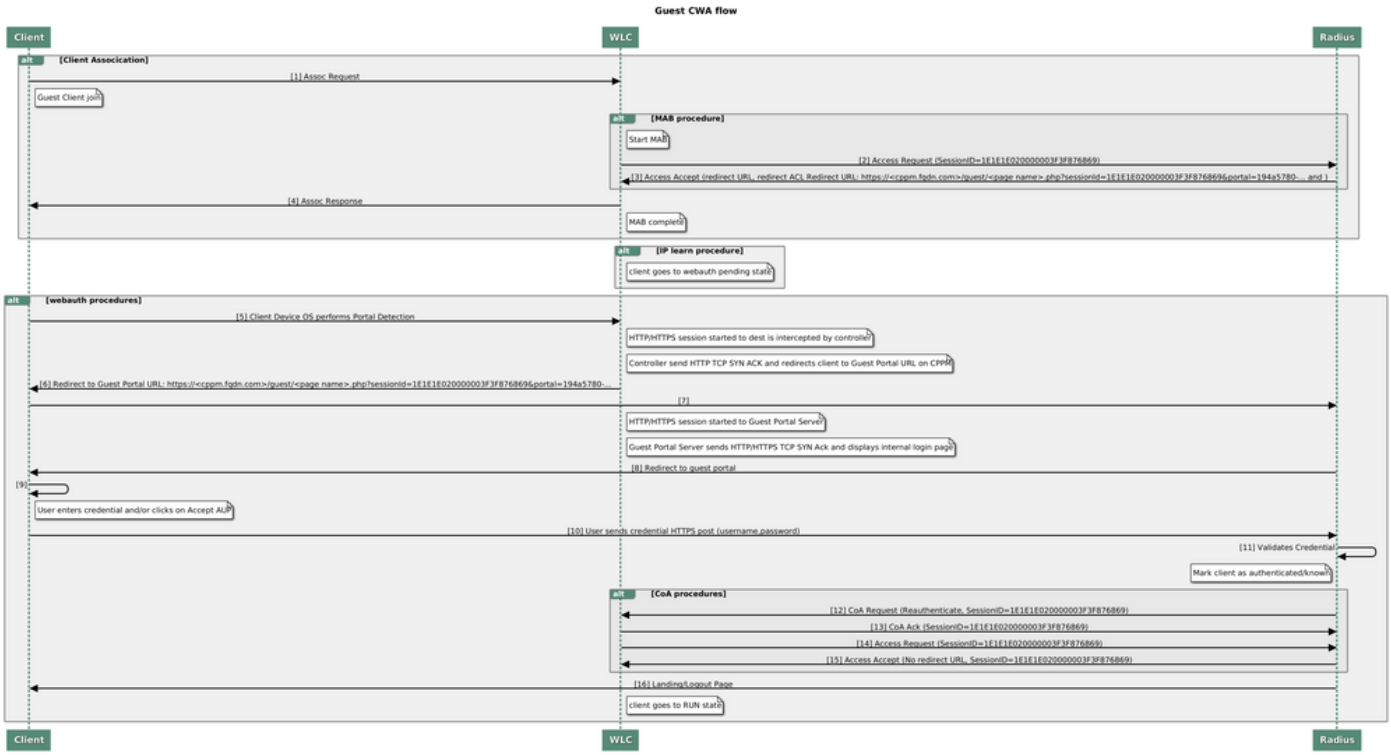
5. C9800は、ゲストクライアント（MACアドレスで識別される）を「Web Auth Pending」状態に移行します。

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。

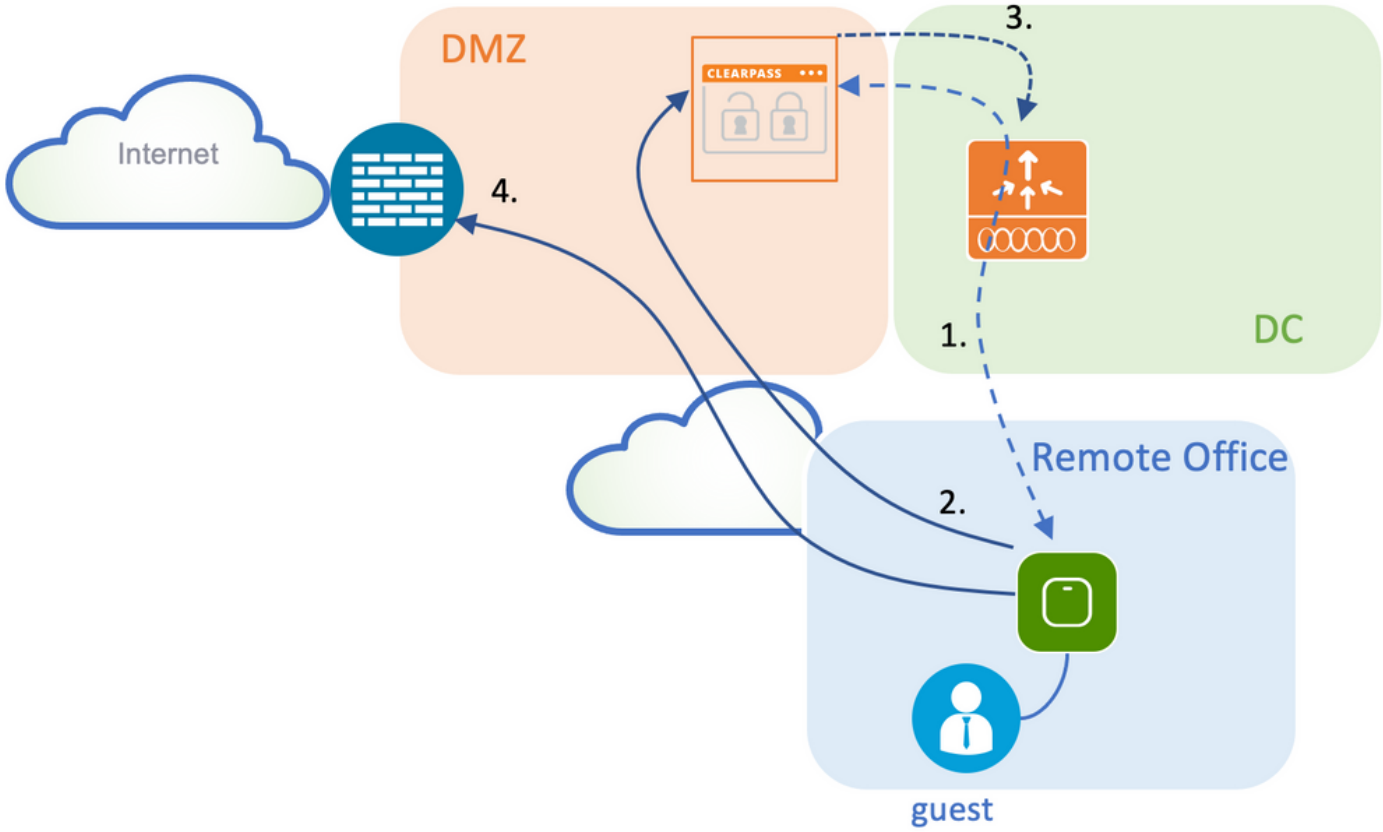
この導入に対応するトラフィックフローを図に示します。

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

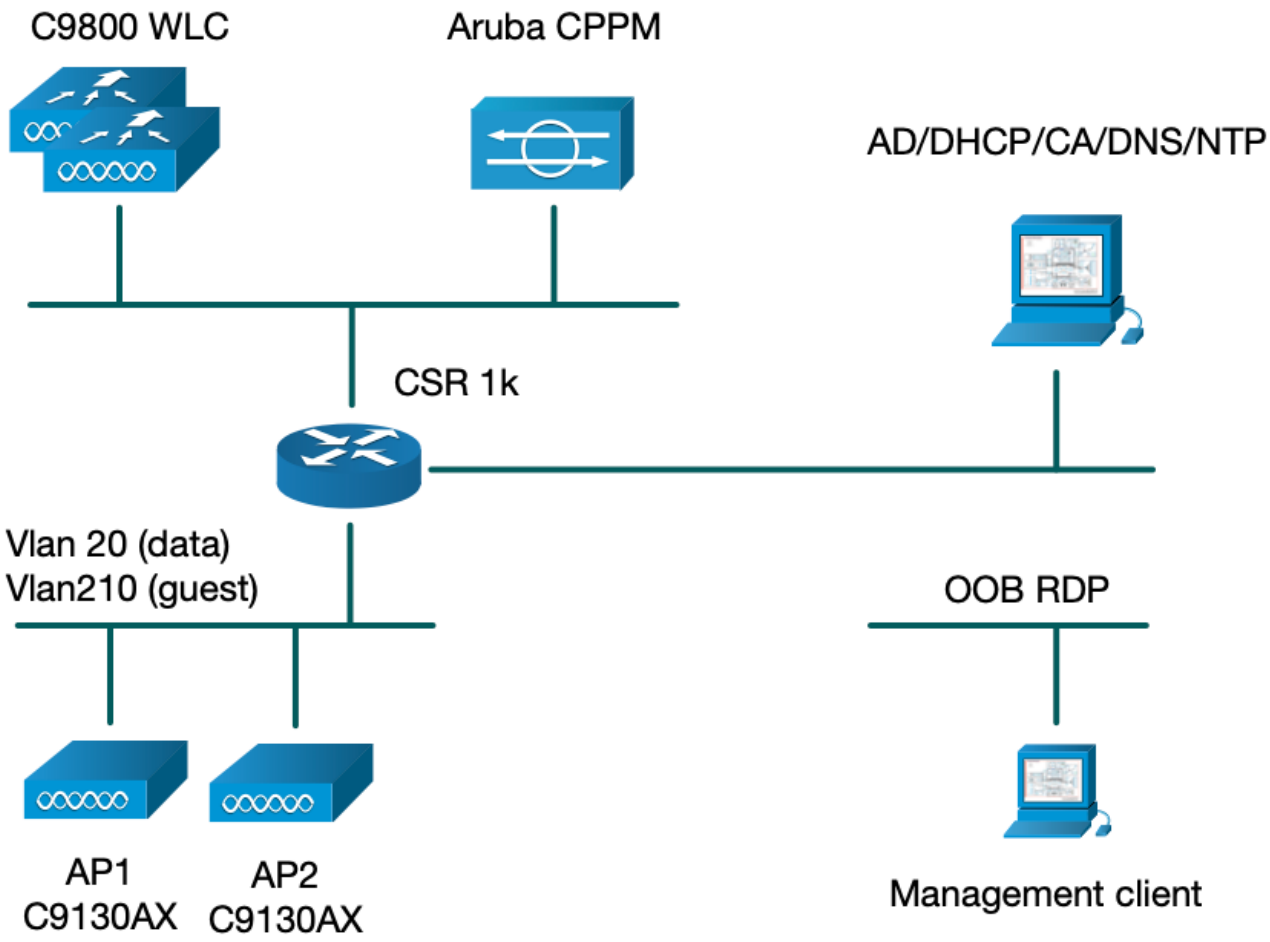
3.ゲストポータルでゲストがEULAを受け入れると、RADIUS CoA再認証がCPPMから9800 WLCに発行されます

4.ゲストはインターネットへのアクセスを許可される



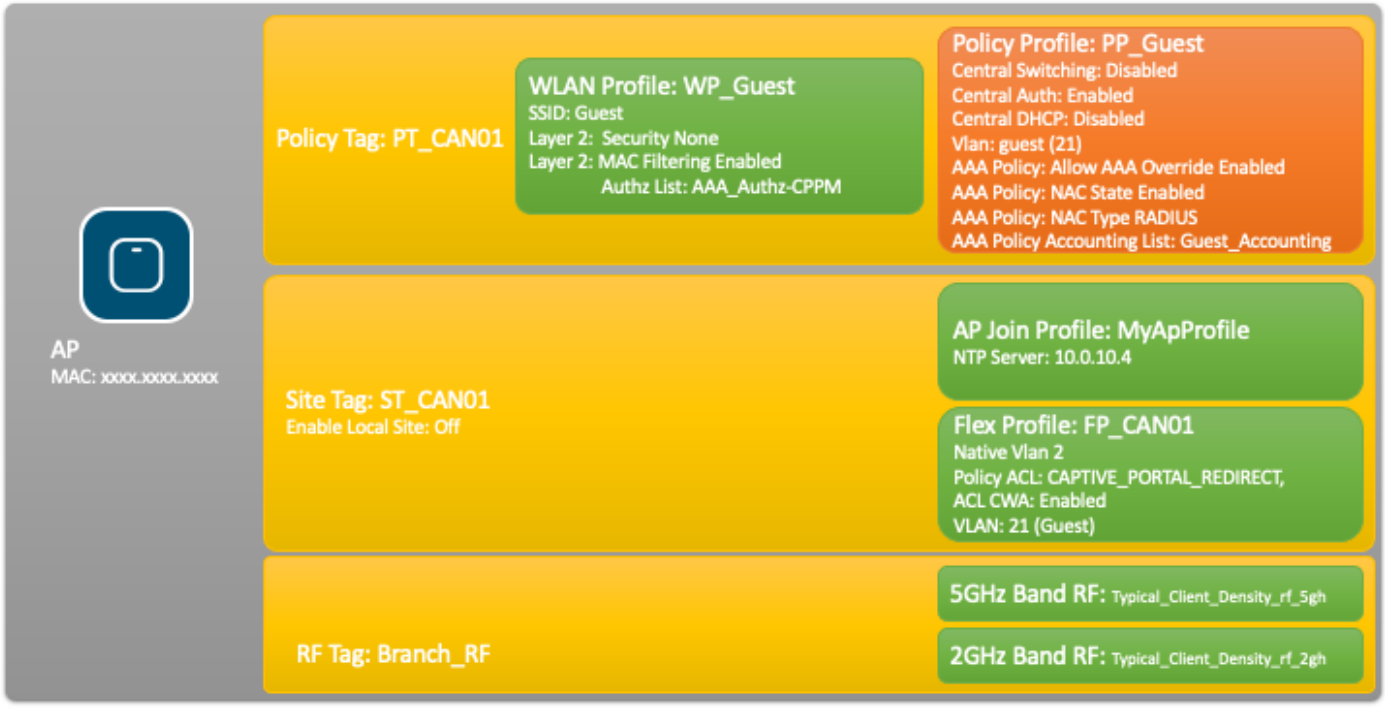
ネットワーク図

注：ラボのデモ目的では、単一または組み合わされた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。

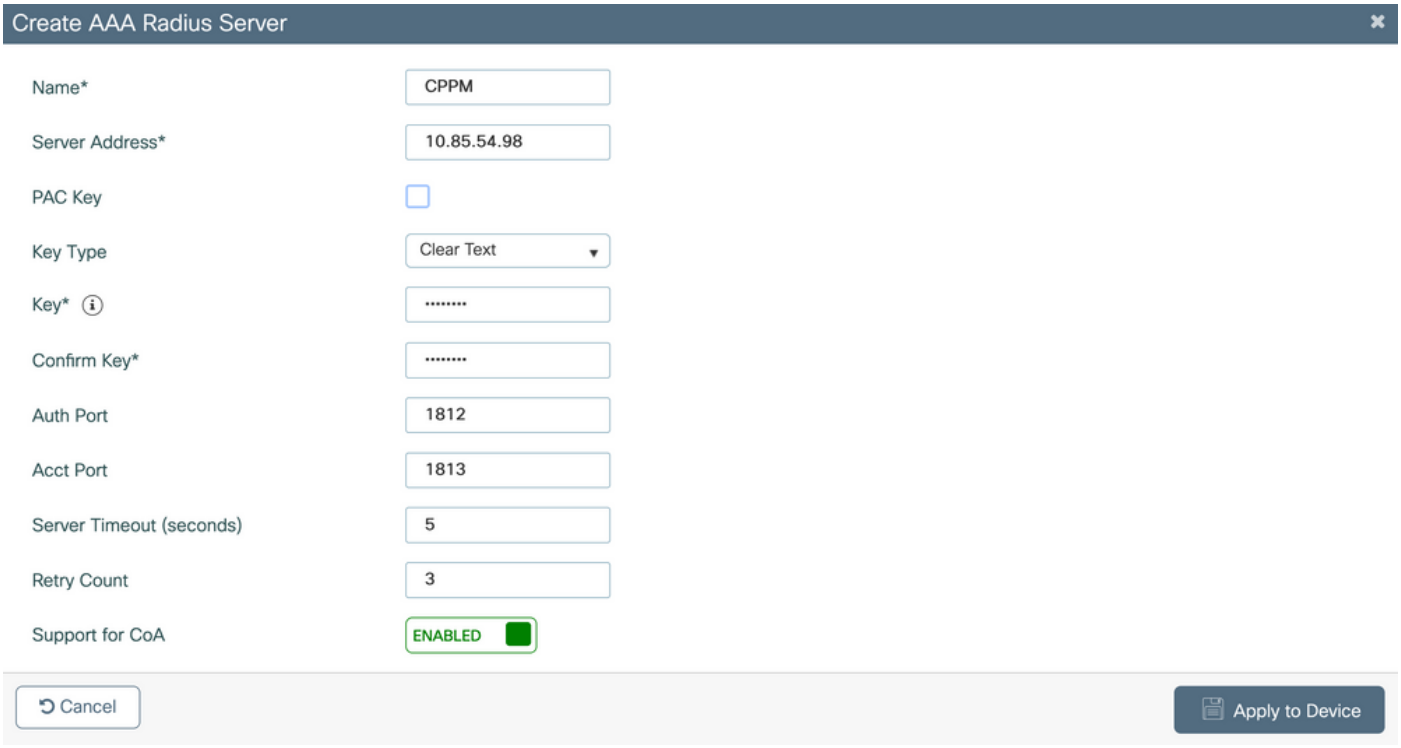


ゲストワイヤレスアクセスC9800パラメータの設定

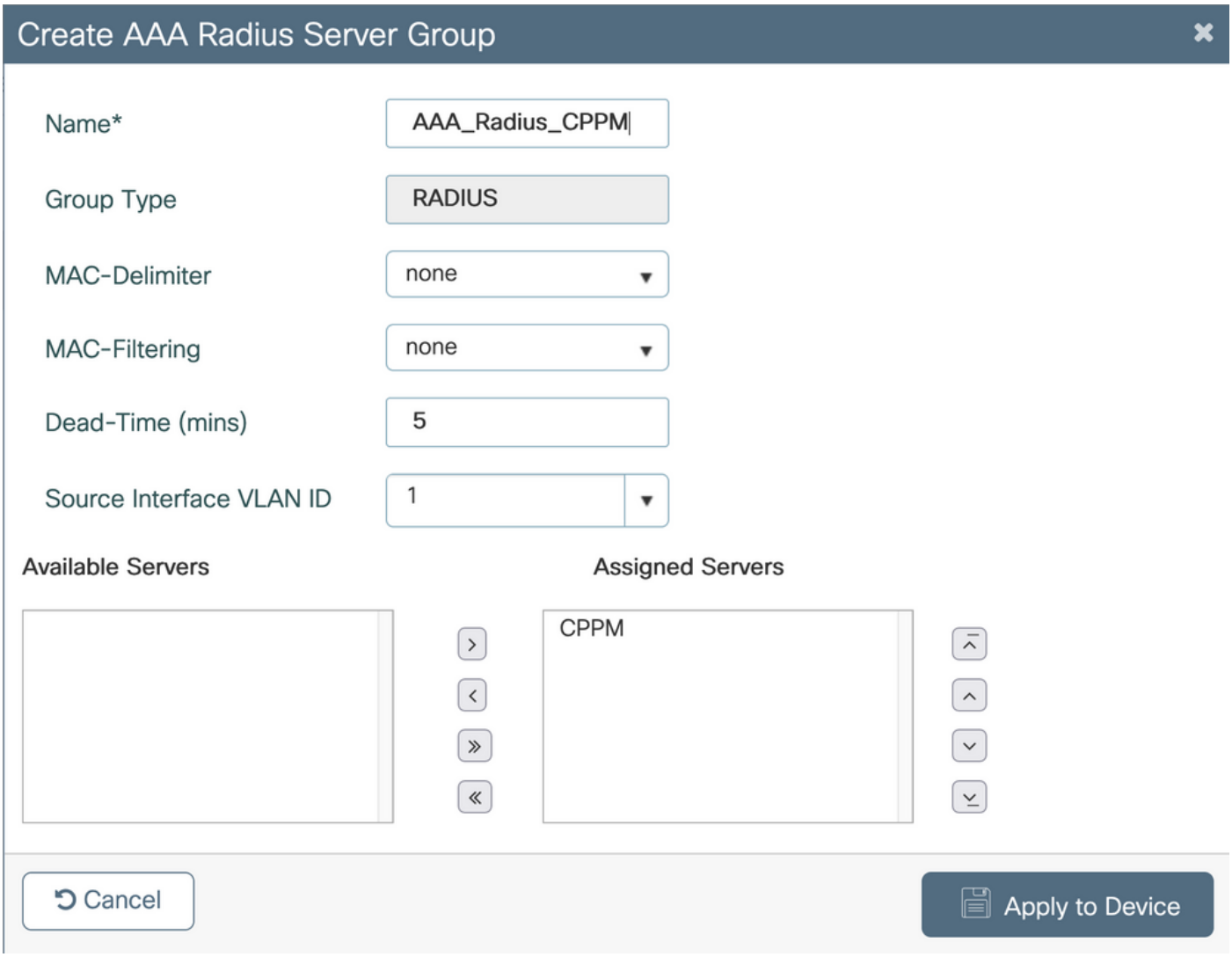
C9800：ゲスト用AAA設定

> **注**：Cisco Bug ID CSCvh03827について、定義された認証、許可、アカウンティング(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。

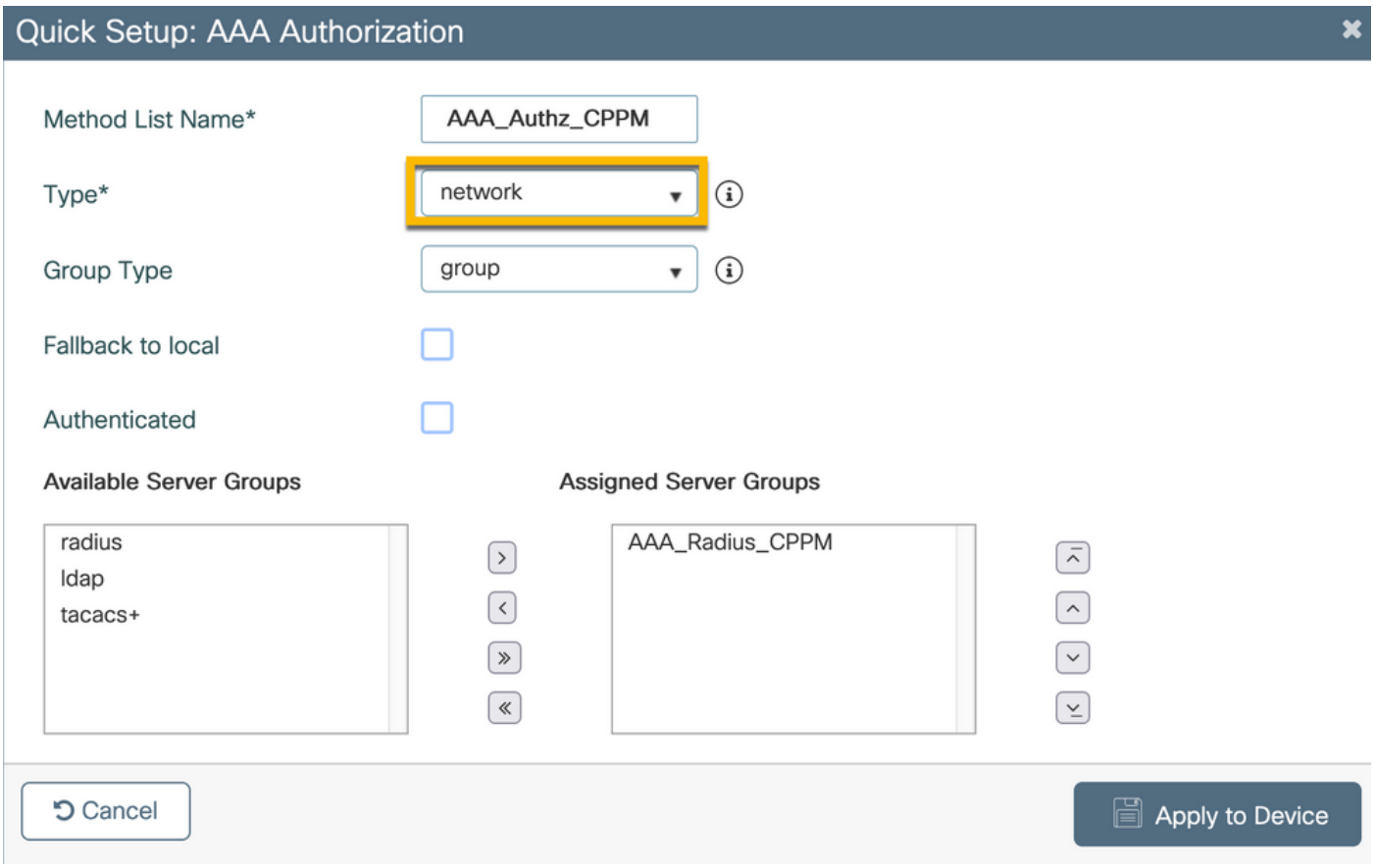
ステップ1:Aruba ClearPass DMZサーバを9800 WLC設定に追加し、認証方式リストを作成します。[Configuration] > [Security] > [AAA] > [Servers/Groups] > [RADIUS] > [Servers] > [+Add] に移動し、RADIUSサーバ情報を入力します。



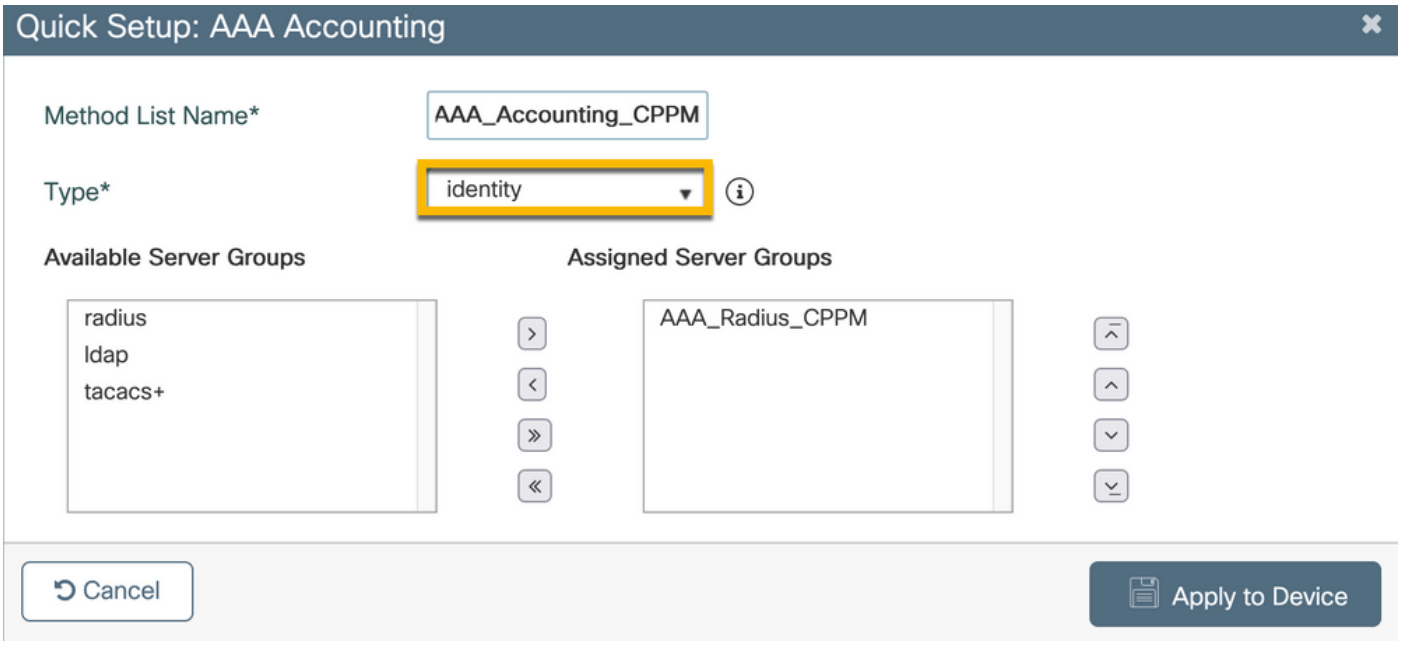
ステップ2：ゲスト用のAAAサーバグループを定義し、ステップ1.で設定したサーバをこのサーバグループに割り当てます。[Configuration] > [Security] > [AAA] > [Servers/Groups] > [RADIUS] > [Groups] > [+Add] に移動します。



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。



ステップ4：ゲストアクセス用のアカウンティング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。



C9800：リダイレクションACLの設定

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。

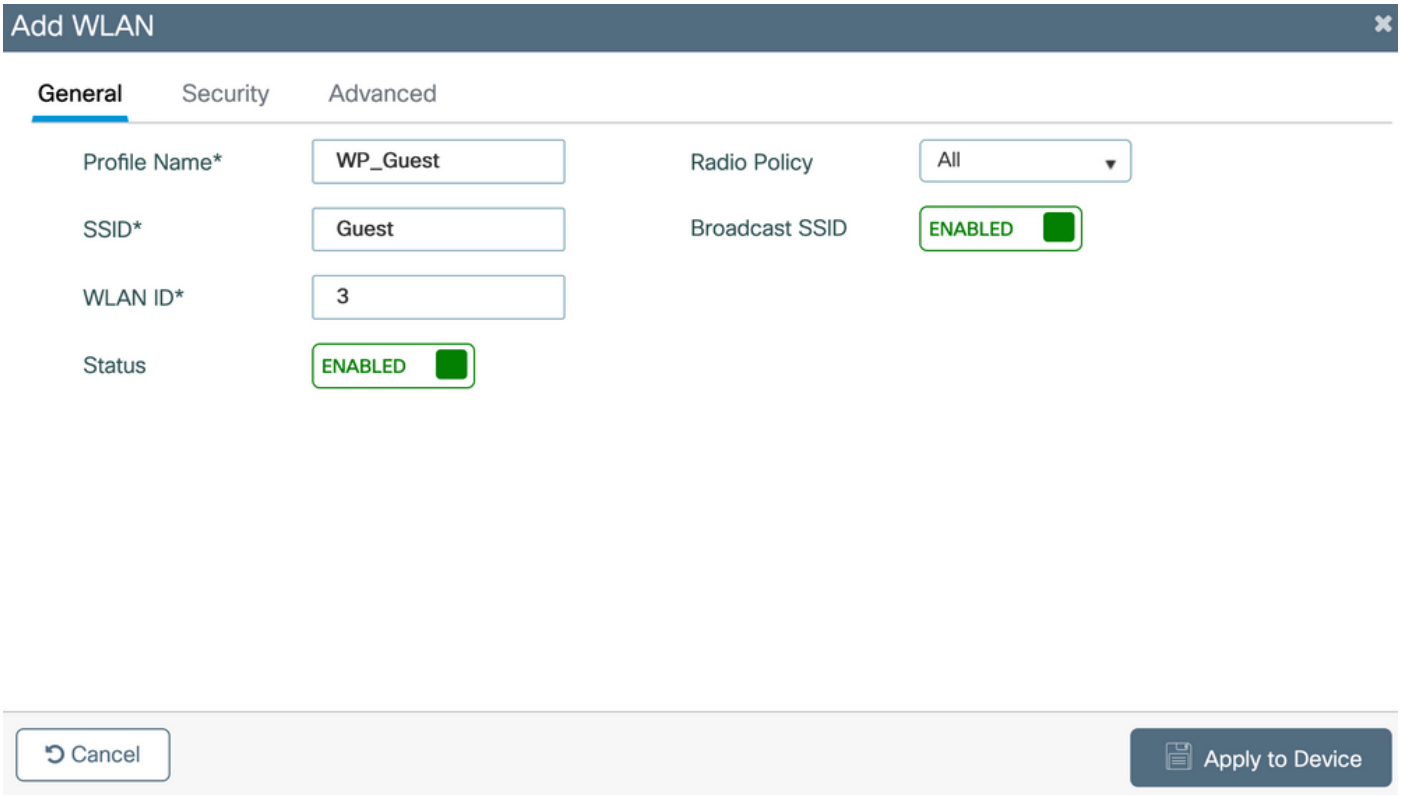
[Configuration] > [Security] > [ACL] に移動し、**CAPTIVE_PORTAL_REDIRECT**という名前の新しいACLを定義します。次のACEでACLを設定します。

- 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」のブ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。

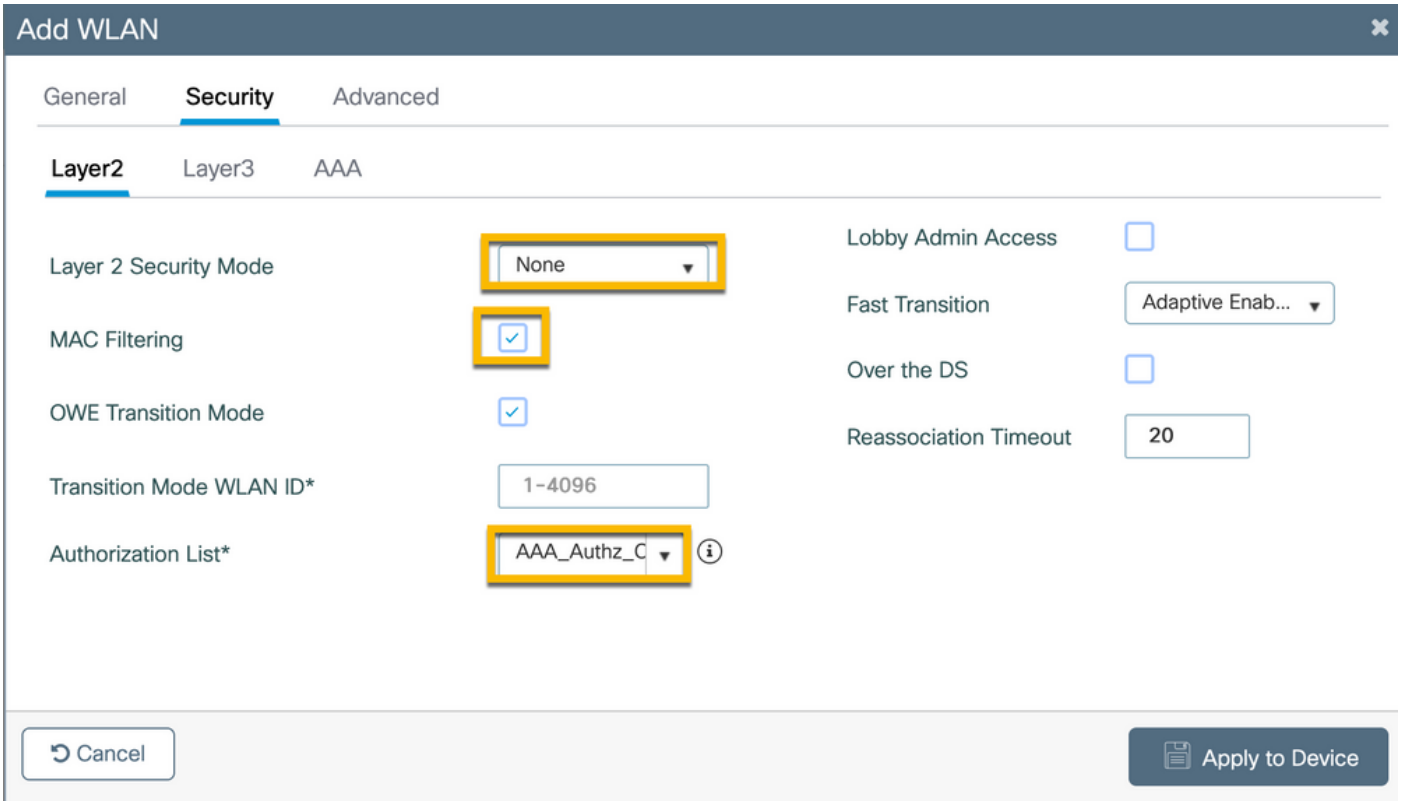


同じ[Add WLAN] ダイアログで、[Security] > [Layer 2] タブに移動します。

– 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）



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

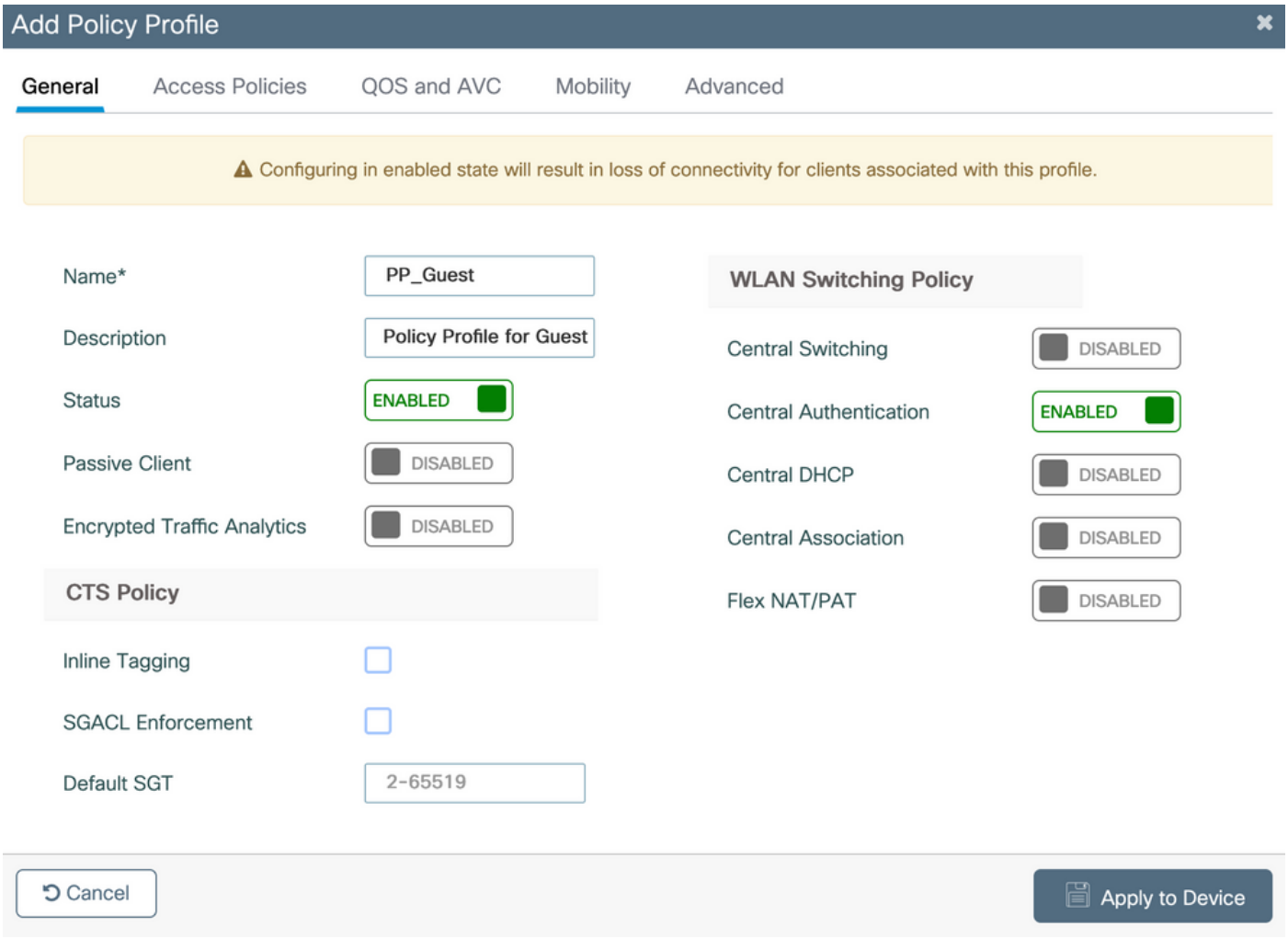
ステータス：有効

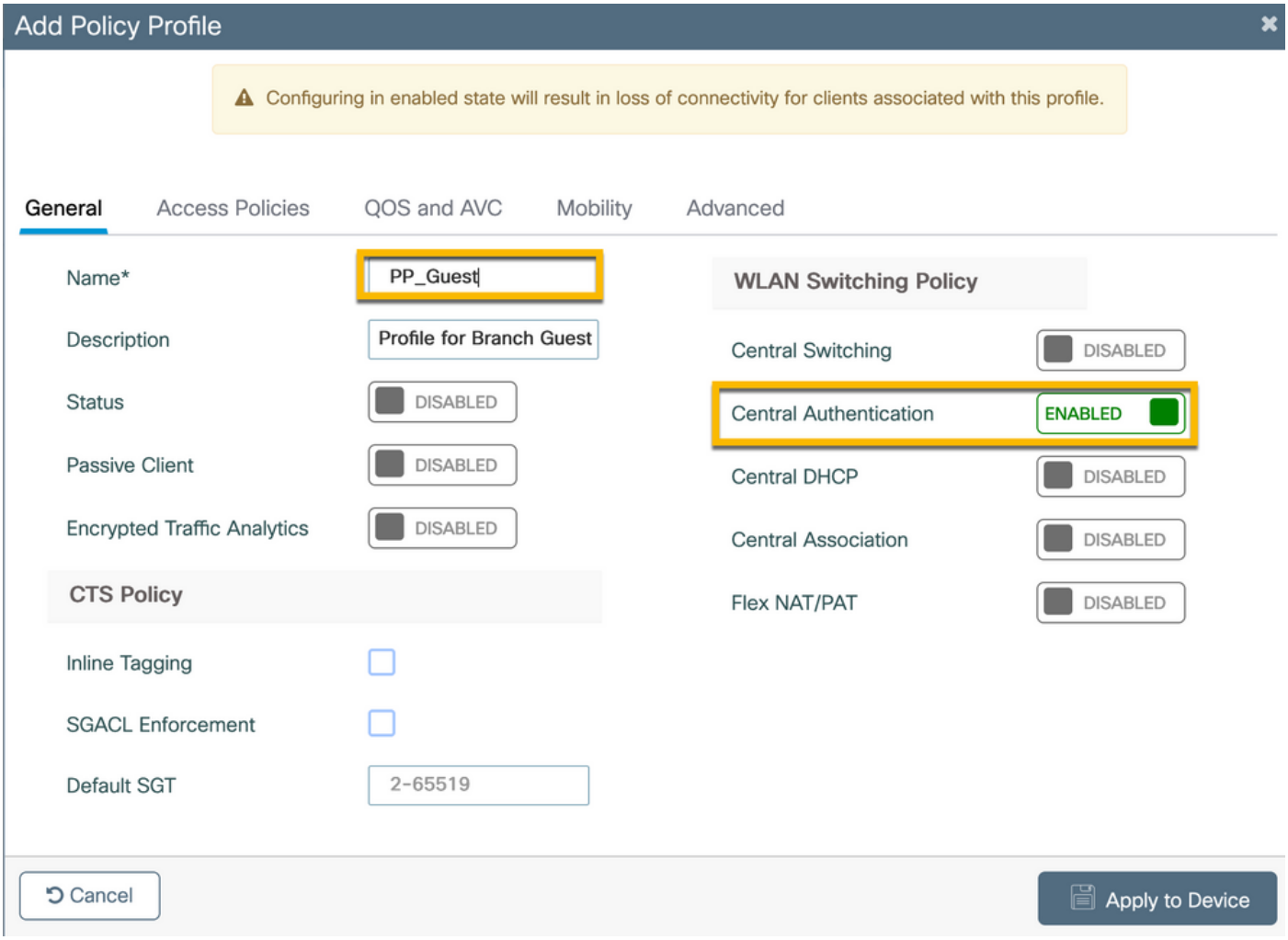
中央スイッチング：Disabled

中央認証：有効

中央DHCP:Disabled

中央関連付け：Disabled





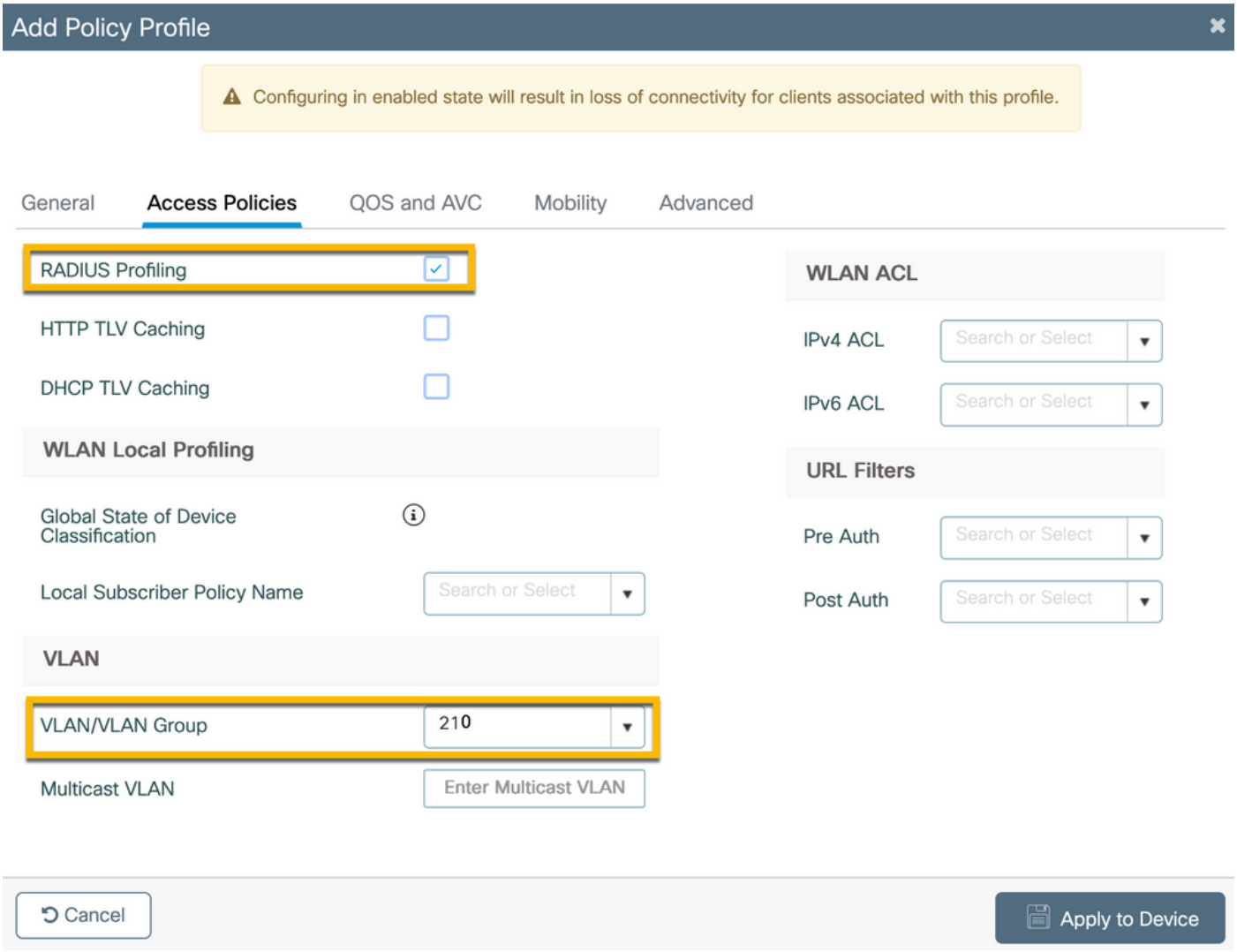
同じ[Add Policy Profile] ダイアログの[Access Policies] タブに移動します。

- 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。



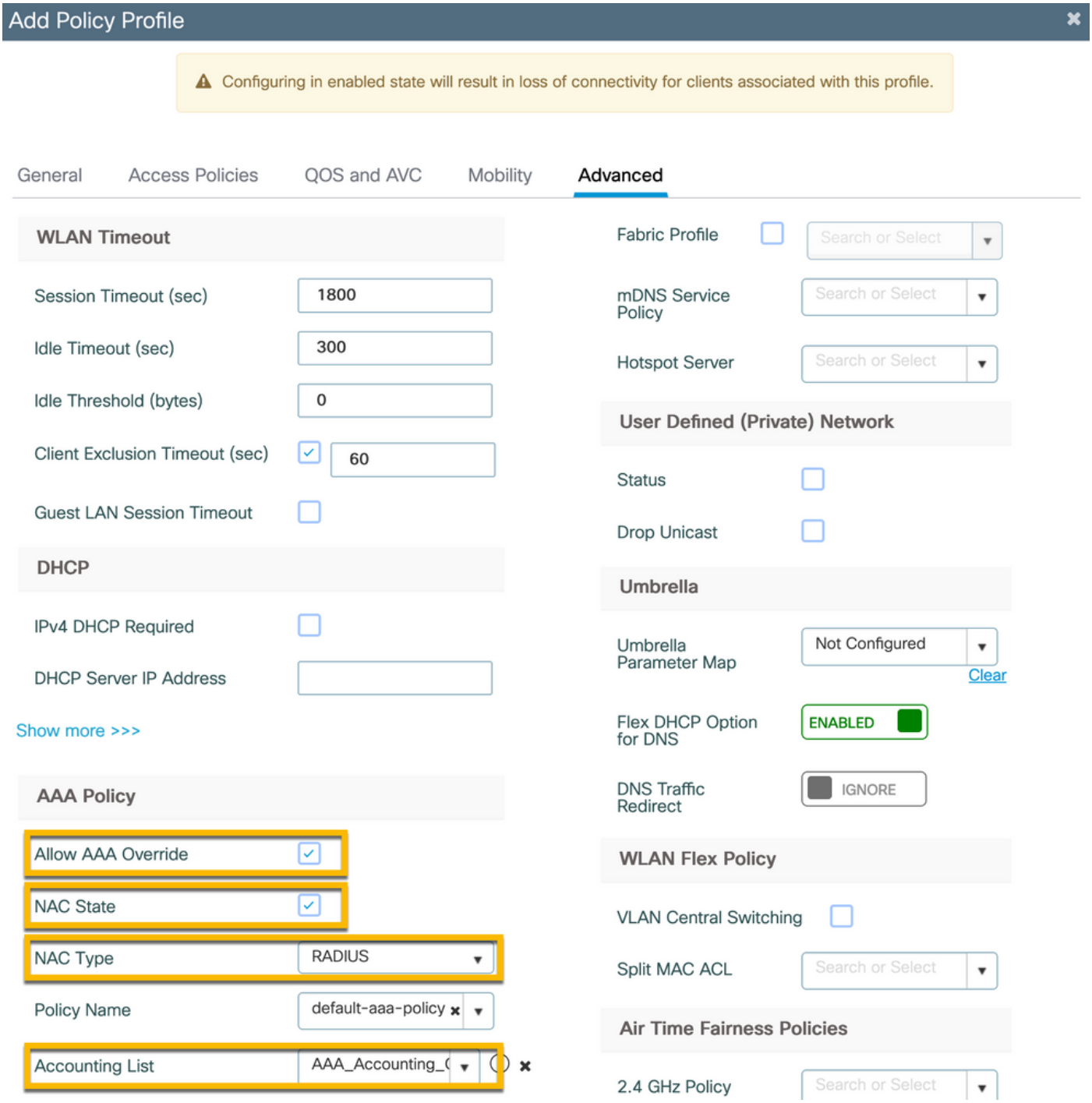
同じ[Add Policy Profile] ダイアログで、[Advanced] タブに移動します。

-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）



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。

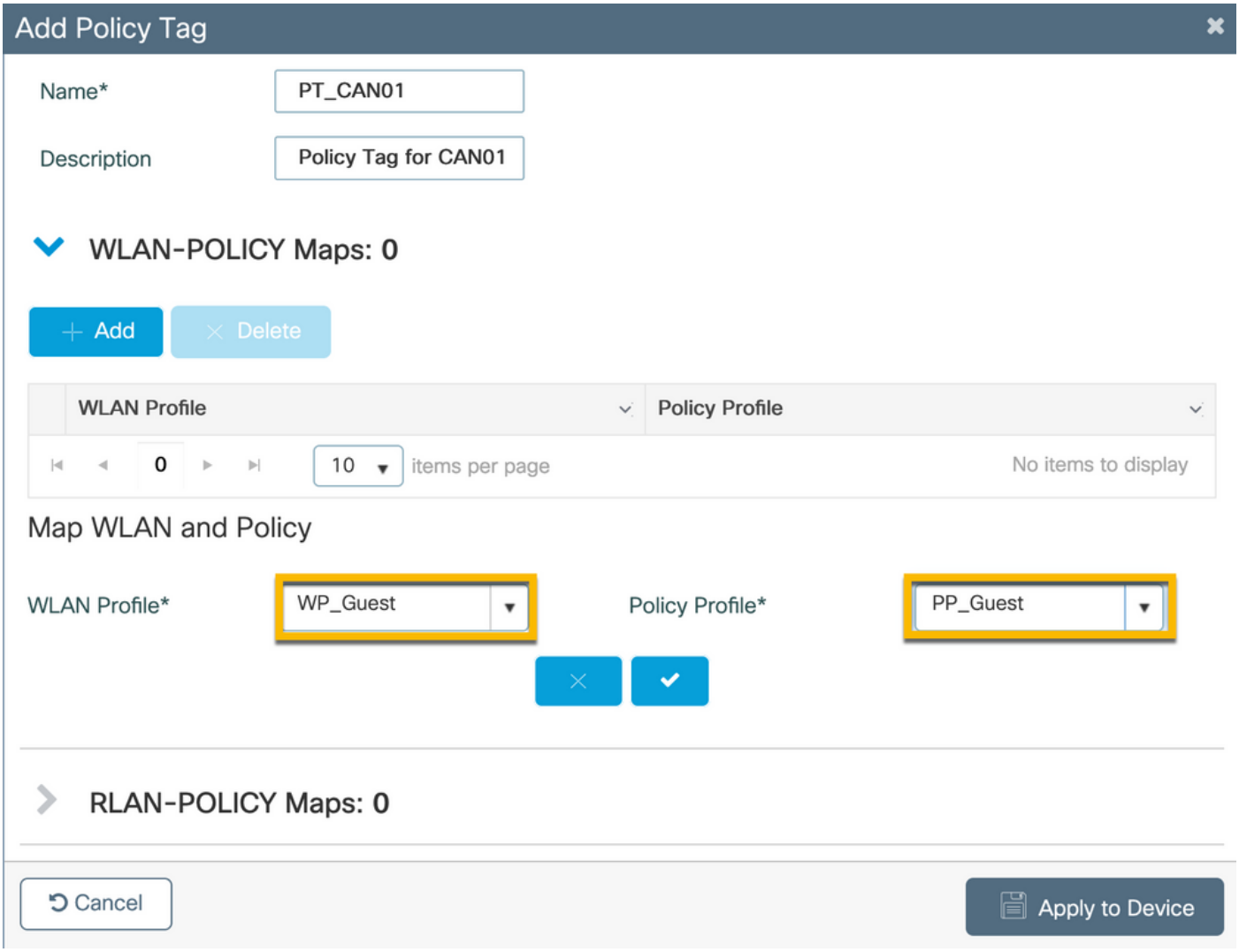
-Name：PT_CAN01

-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] の下の[Add] をクリックし、以前に作成したWLANプロファイルをポリシープロファイルにマッピングします。

- WLANプロファイル：WP_Guest

– ポリシープロファイル：PP_Guest

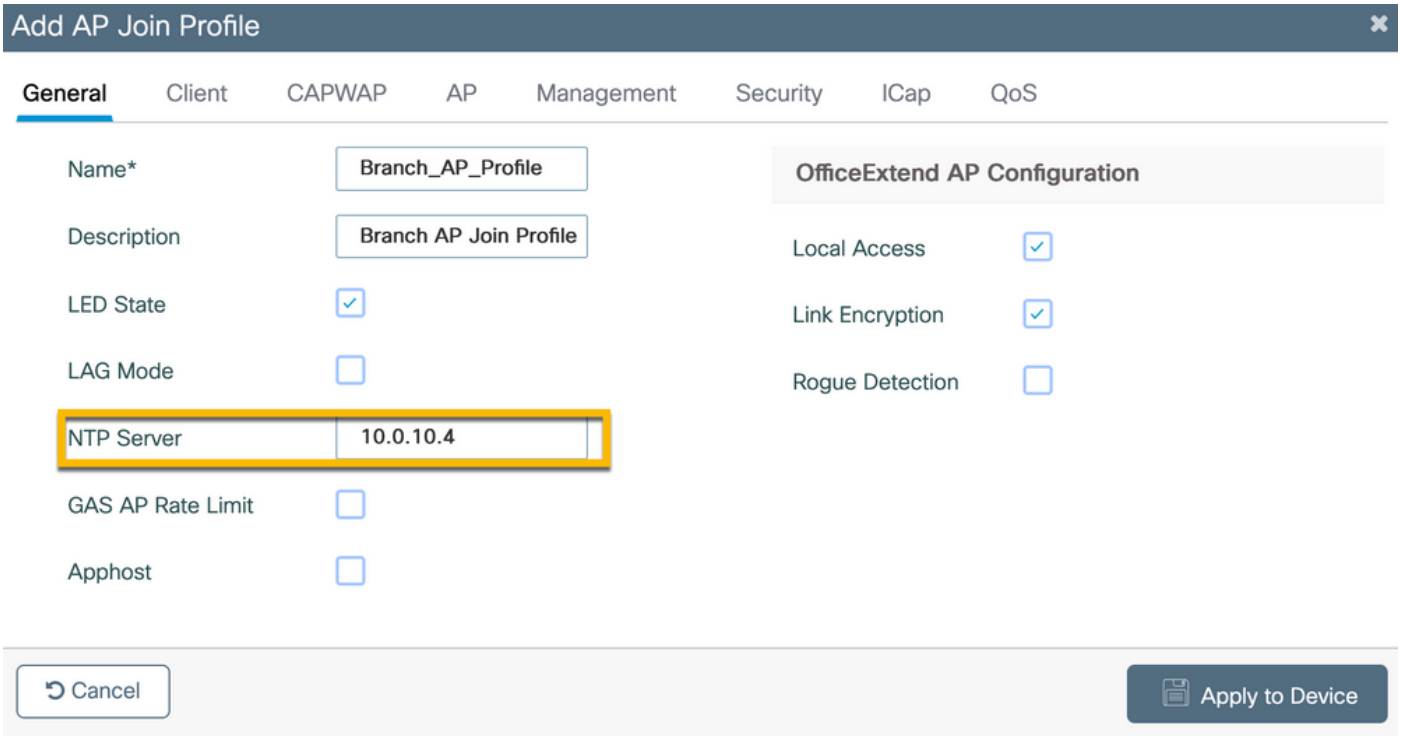


C9800:AP加入プロファイル

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。



C9800:Flexプロファイル

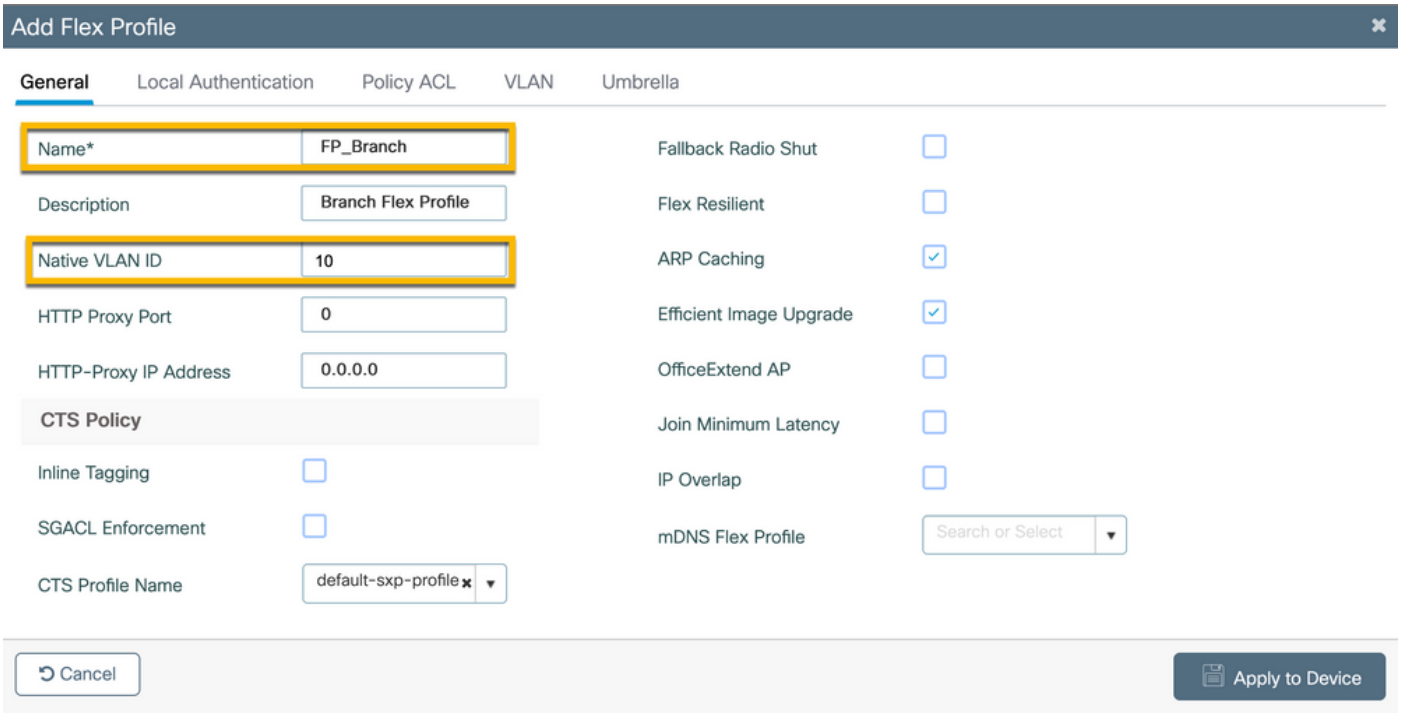
プロファイルとタグはモジュール化されており、複数のサイトで再利用できます。

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プロファイ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）

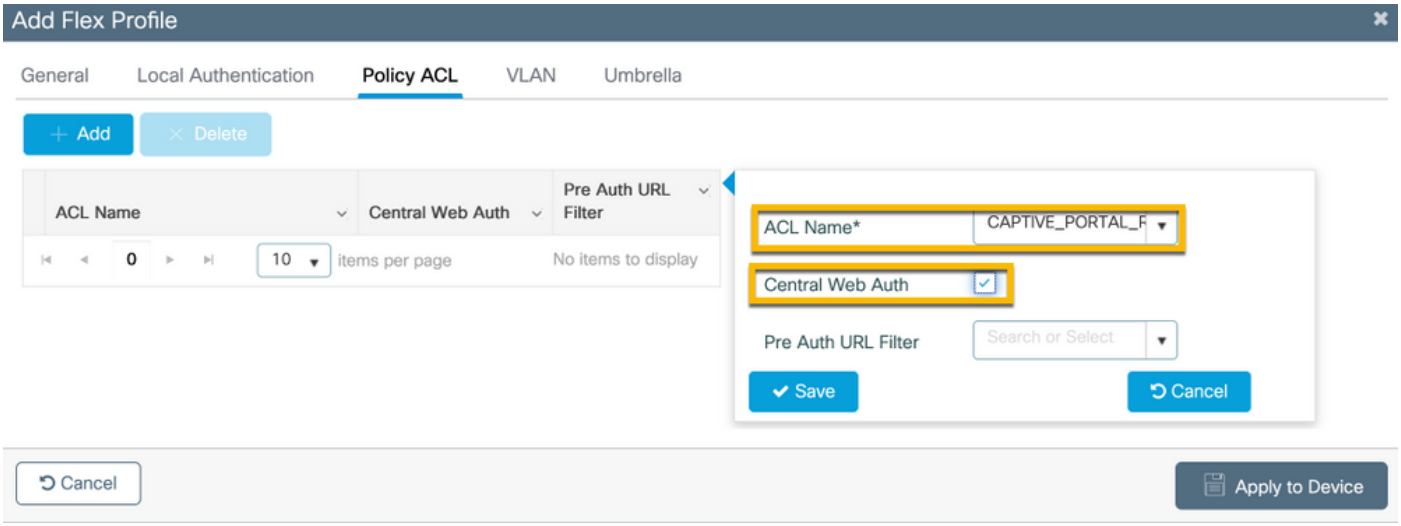


同じ[Add Flex Profile] ダイアログで、[Policy ACL] タブに移動し、[Add] をクリックします。

-ACL 名:CAPTIVE_PORTAL_REDIRECT

– 中央Web認証：有効

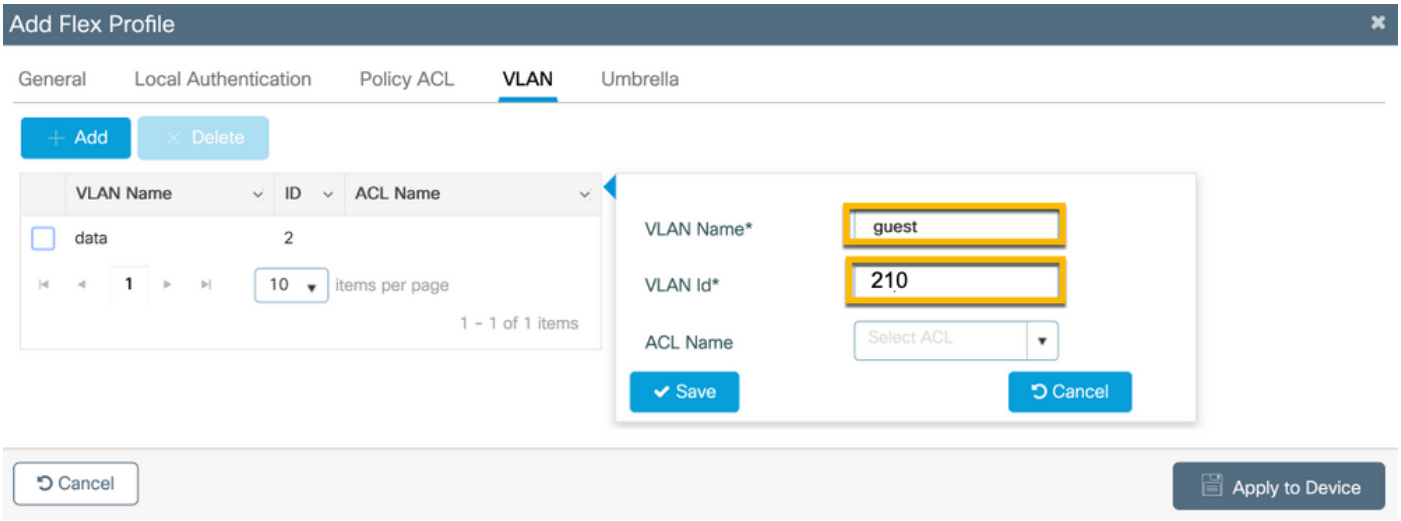
Flexconnect導入では、C9800ではなくAPでリダイレクションが発生するため、管理対象の各APはローカルにリダイレクトACLをダウンロードすることが想定されます。



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



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。

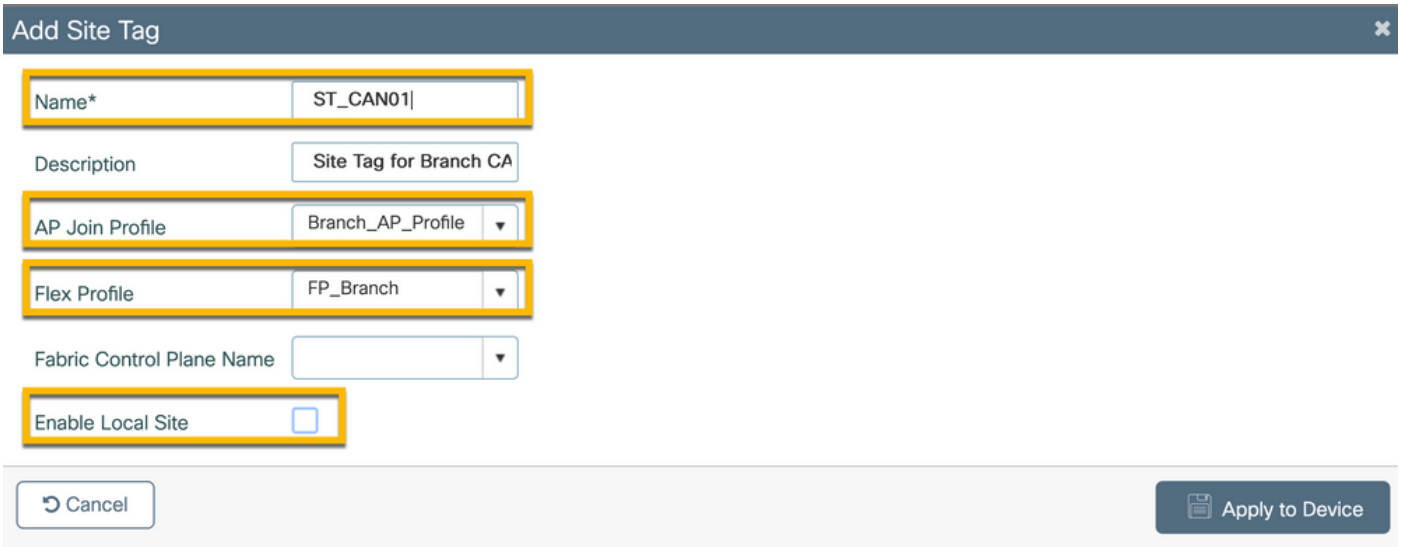
Flex Connectサイトには、Flex Connectプロファイルが関連付けられている必要があります。
Flex Connectサイトごとに最大100のアクセスポイントを設定できます。

-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



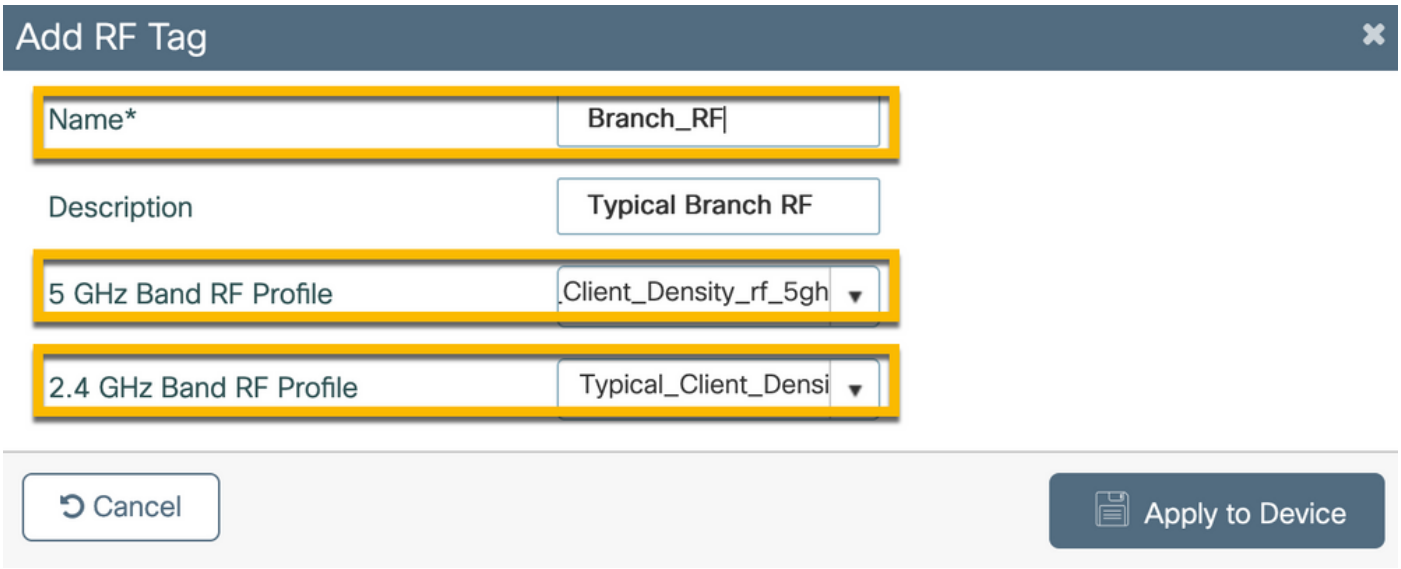
C9800:RFプロファイル

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）



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)。

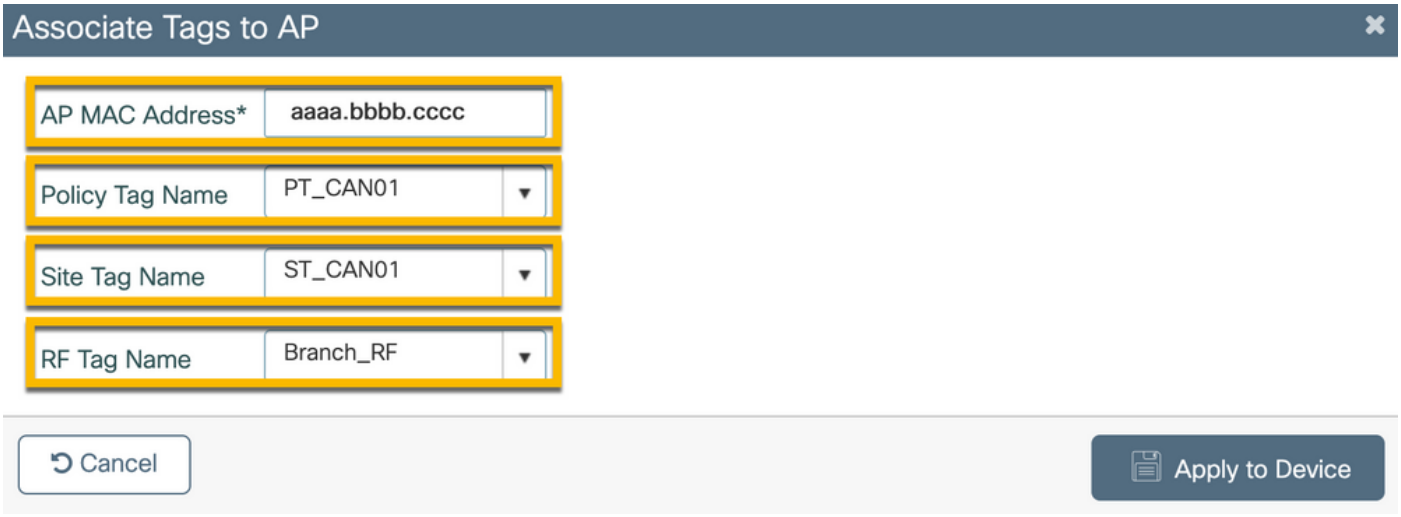
-AP MACアドレス:<AP_ETHERNET_MAC>

– 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。



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

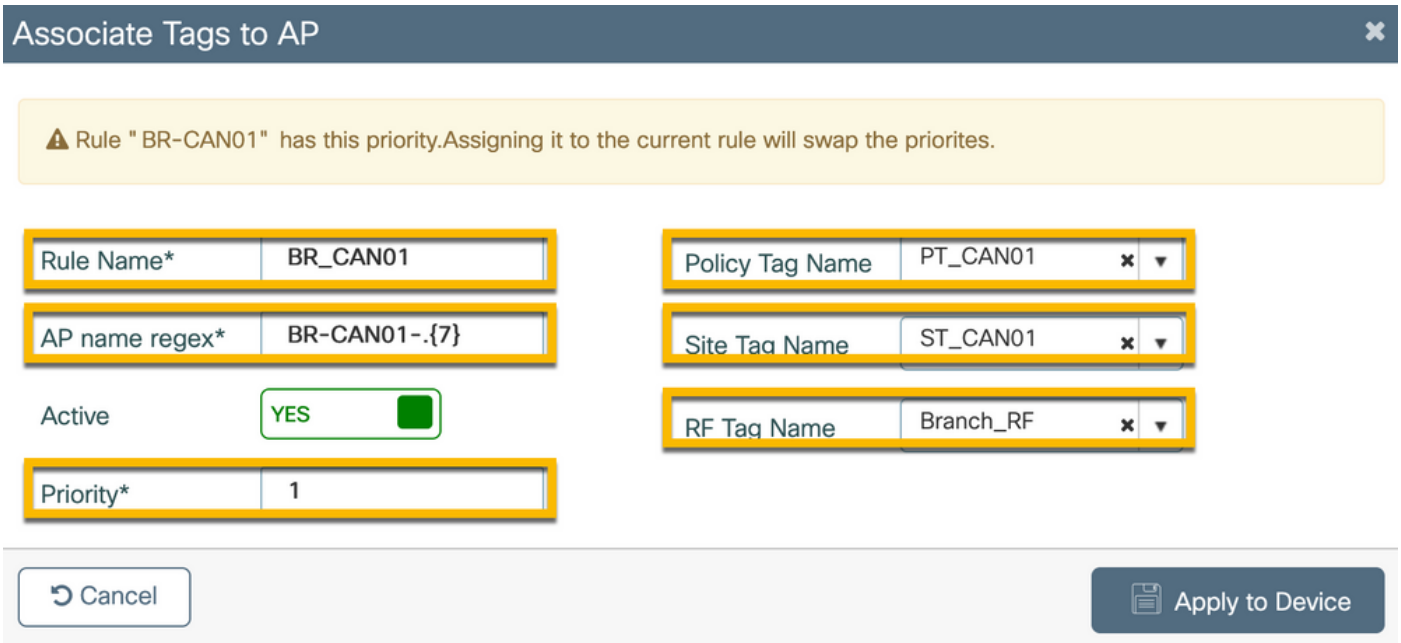
- AP名regex:BR-CAN01-.(7)(このルールは、組織内で採用されているAP名の表記法に一致します。この例では、タグは、「BR_CAN01 – 」の後に7文字が続くAP名フィールドを持つAPに割り当てられます)。

-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



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。

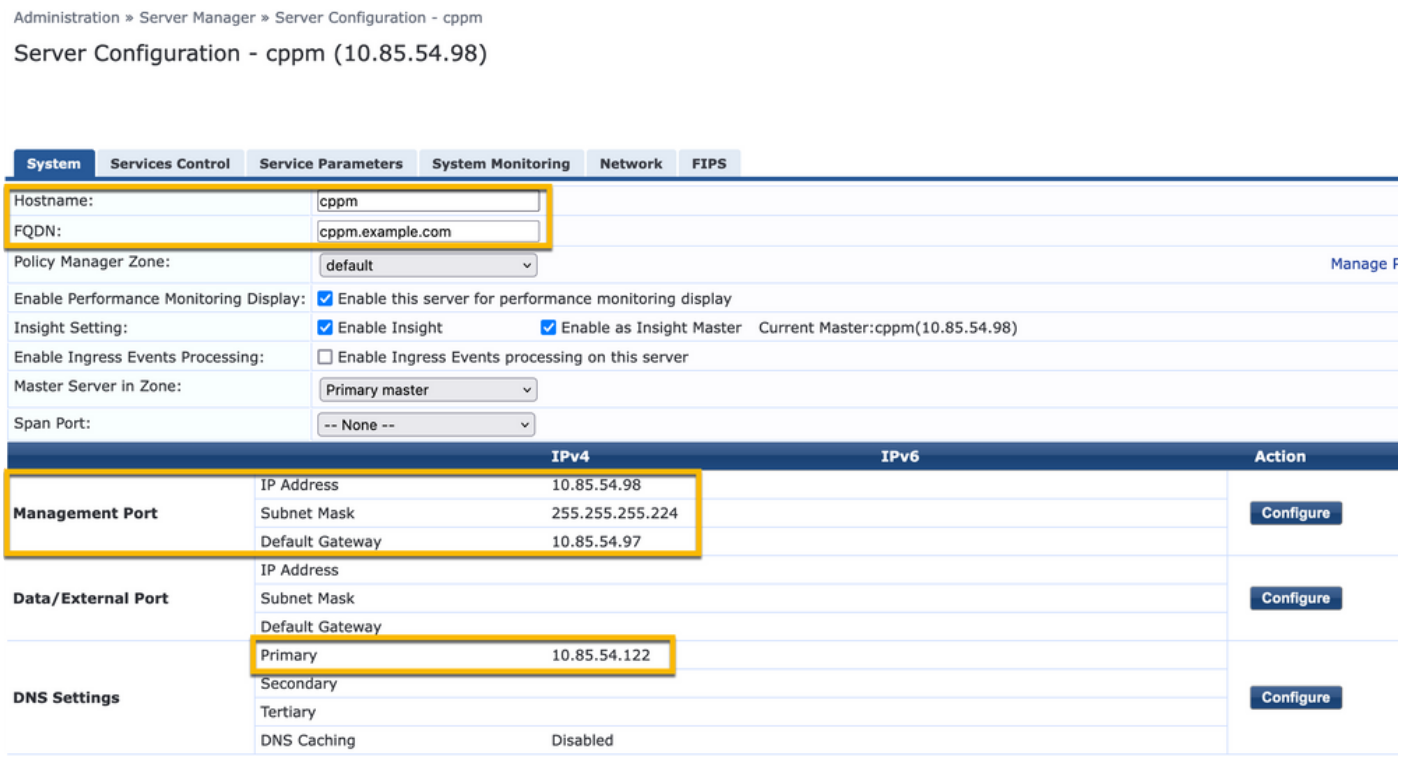
サーバホスト名

[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



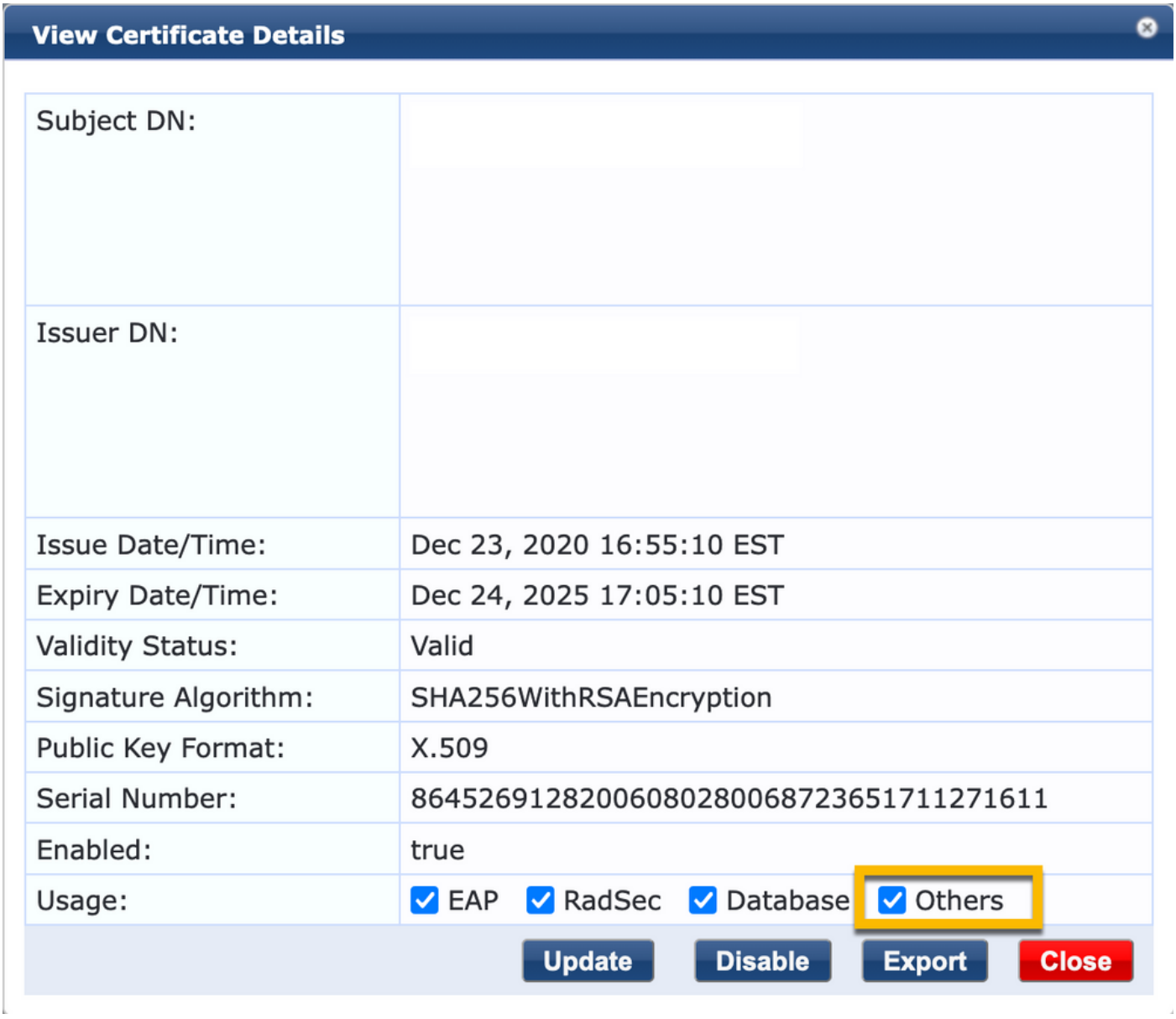
CPPM Webサーバ証明書(HTTPS)の生成

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



ステップ2：証明書署名要求を作成します。

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

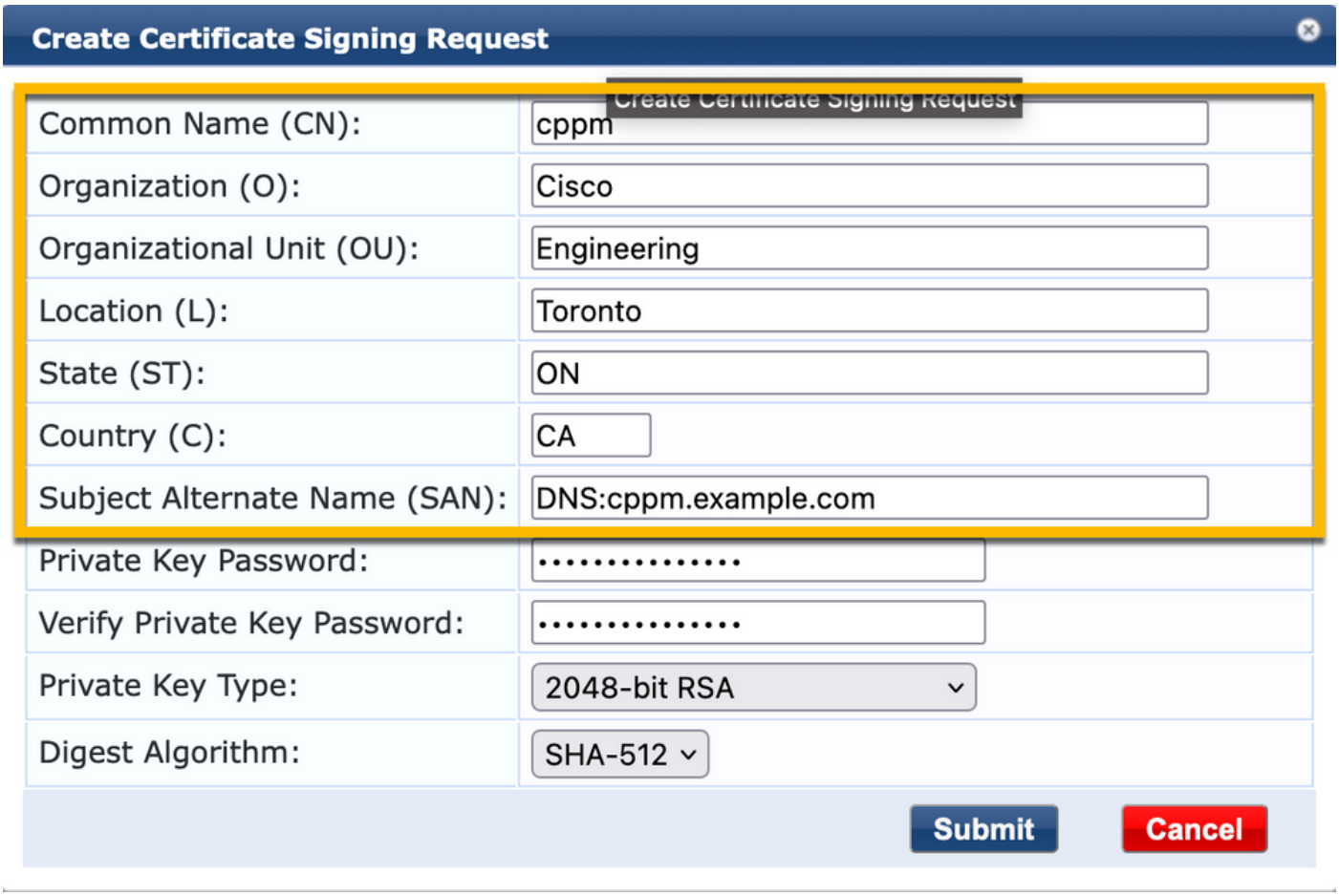
- [Create] [Certificate Signing Request]をクリックします

– 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>。



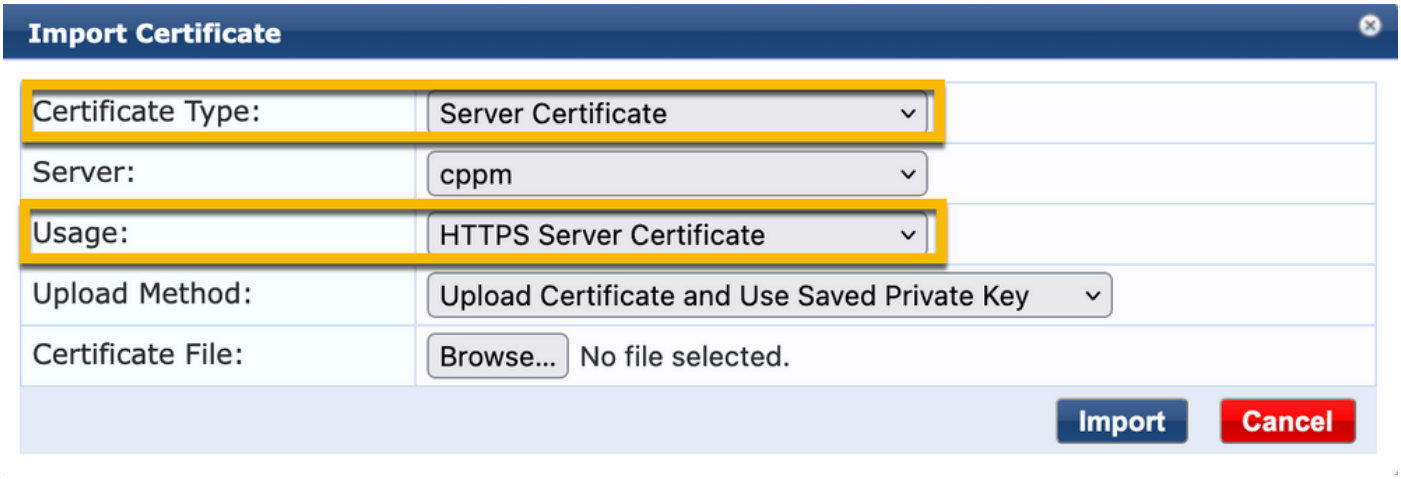
ステップ3：選択したCAで、新しく生成されたCPPM HTTPSサービスCSRに署名します。

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



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。

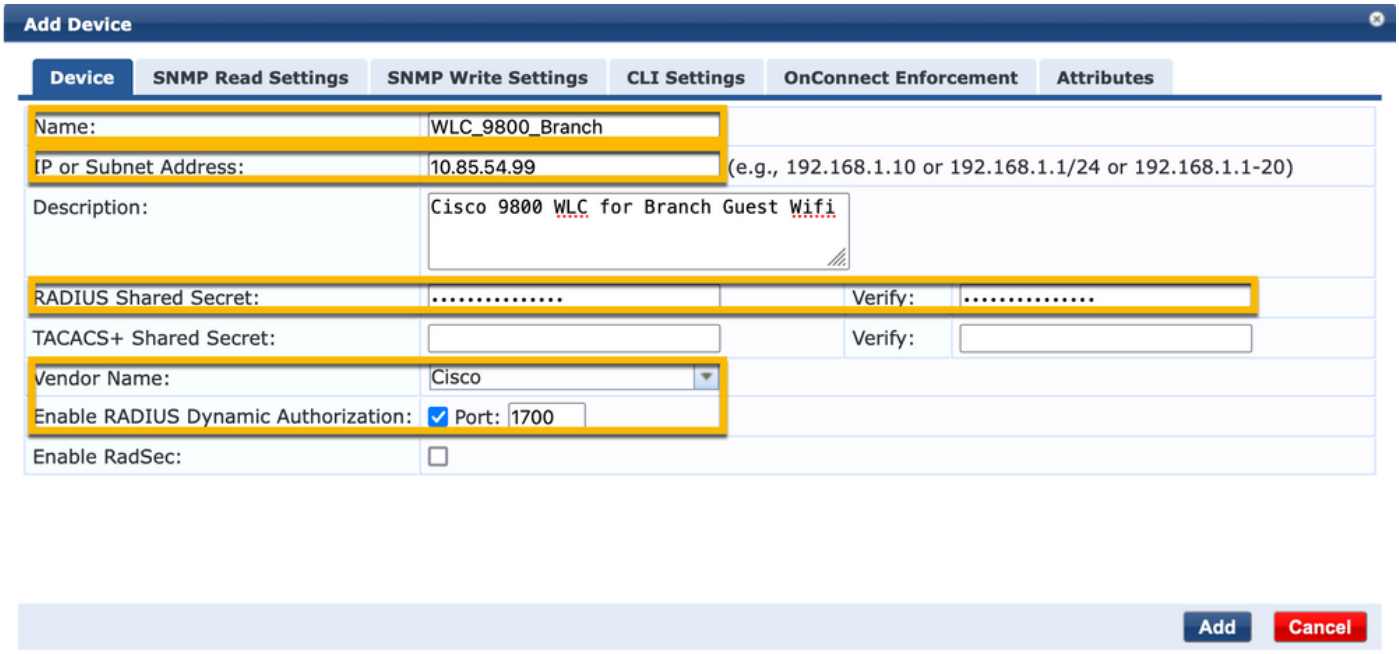
-Name：WLC_9800_Branch

- 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



ゲストポータルページとCoAタイマー

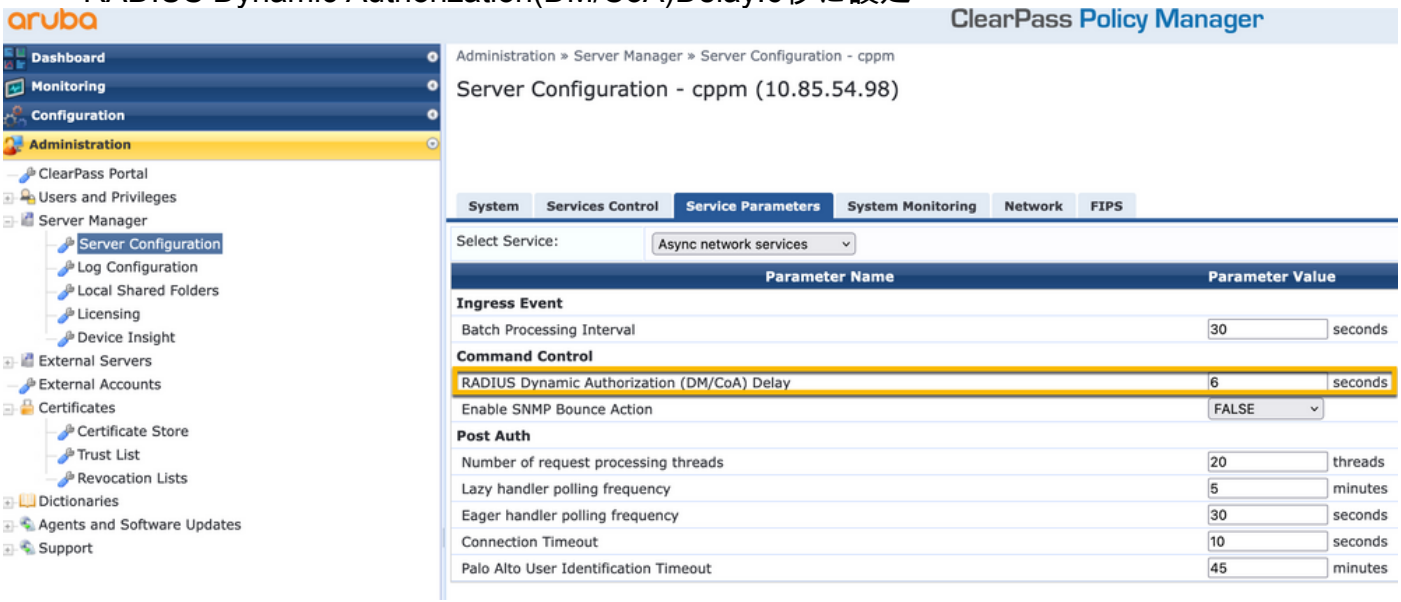
設定全体を通して正しいタイマー値を設定することが非常に重要です。タイマーが調整されていない場合は、クライアントが「実行状態」でない状態で、循環するWebポータルリダイレクトが発生する可能性があります。
注意すべきタイマー：

- 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

- 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-Inter** TRUEの場合は、ネットワーク 接続を許可します。それ以外の は、**Redirect**をトリガーし、**C** **認証**。
2.ゲスト	Webログイン	匿名ログインAUPページを表 す。 Post-auth set custom attribute **Allow-Guest-Internet** = TRUE。
3.ポリシーマネージャ	Service（サービス）：Web ベース の認証	エンドポイントを既知に**更新** カスタム属性**Allow-Guest-Inter** 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。

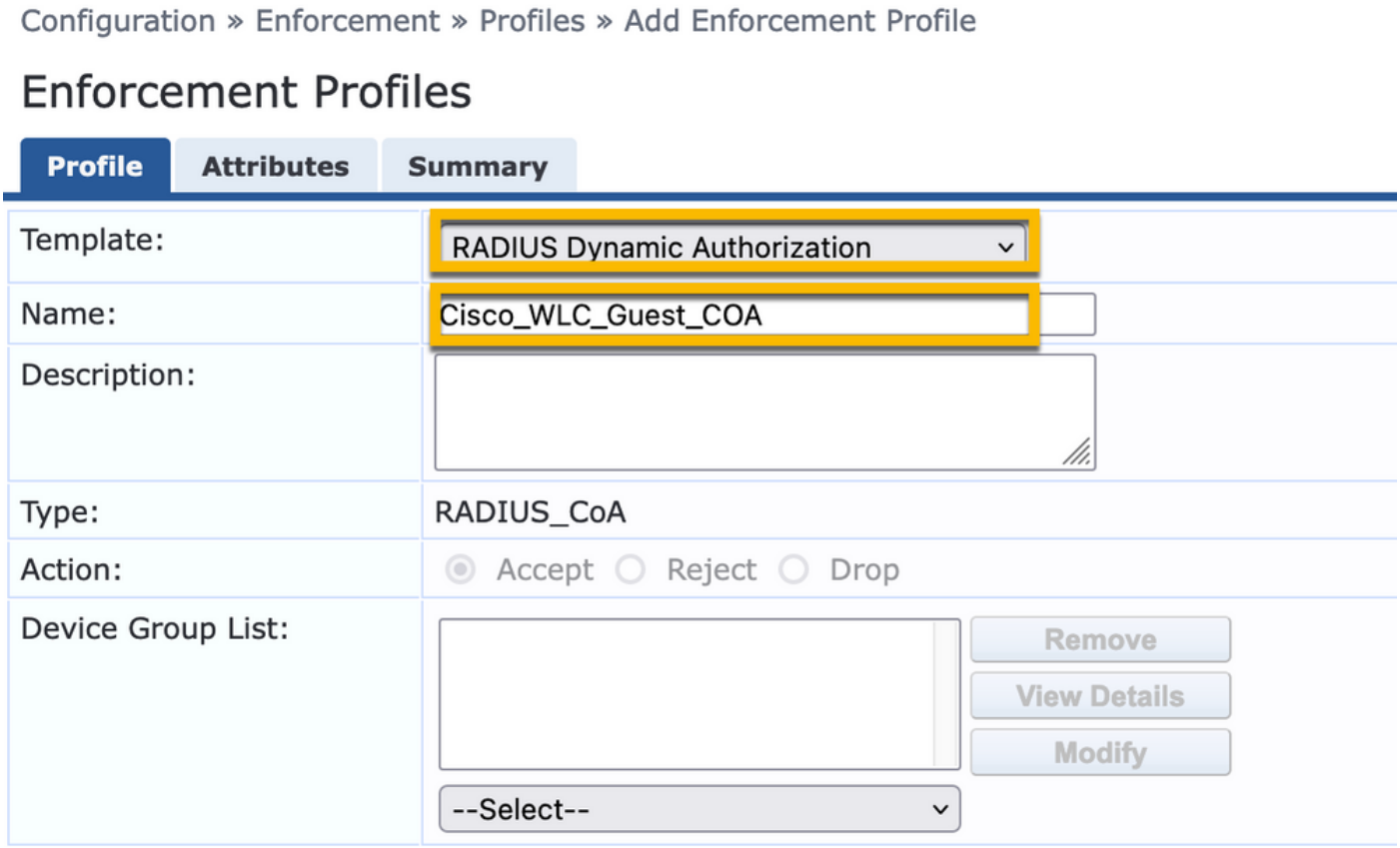
ClearPass再認証適用ポリシー設定

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



半径：IETF	Calling-Station-Id	%{Radius:IETF:Calling-Station
半径：Cisco	Cisco-AVPair	subscriber:command=reauther e
半径：Cisco	Cisco-AVPair	%{Radius:Cisco:Cisco-AVPair:subscriber:audit-sessio
半径：Cisco	Cisco-AVPair	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。

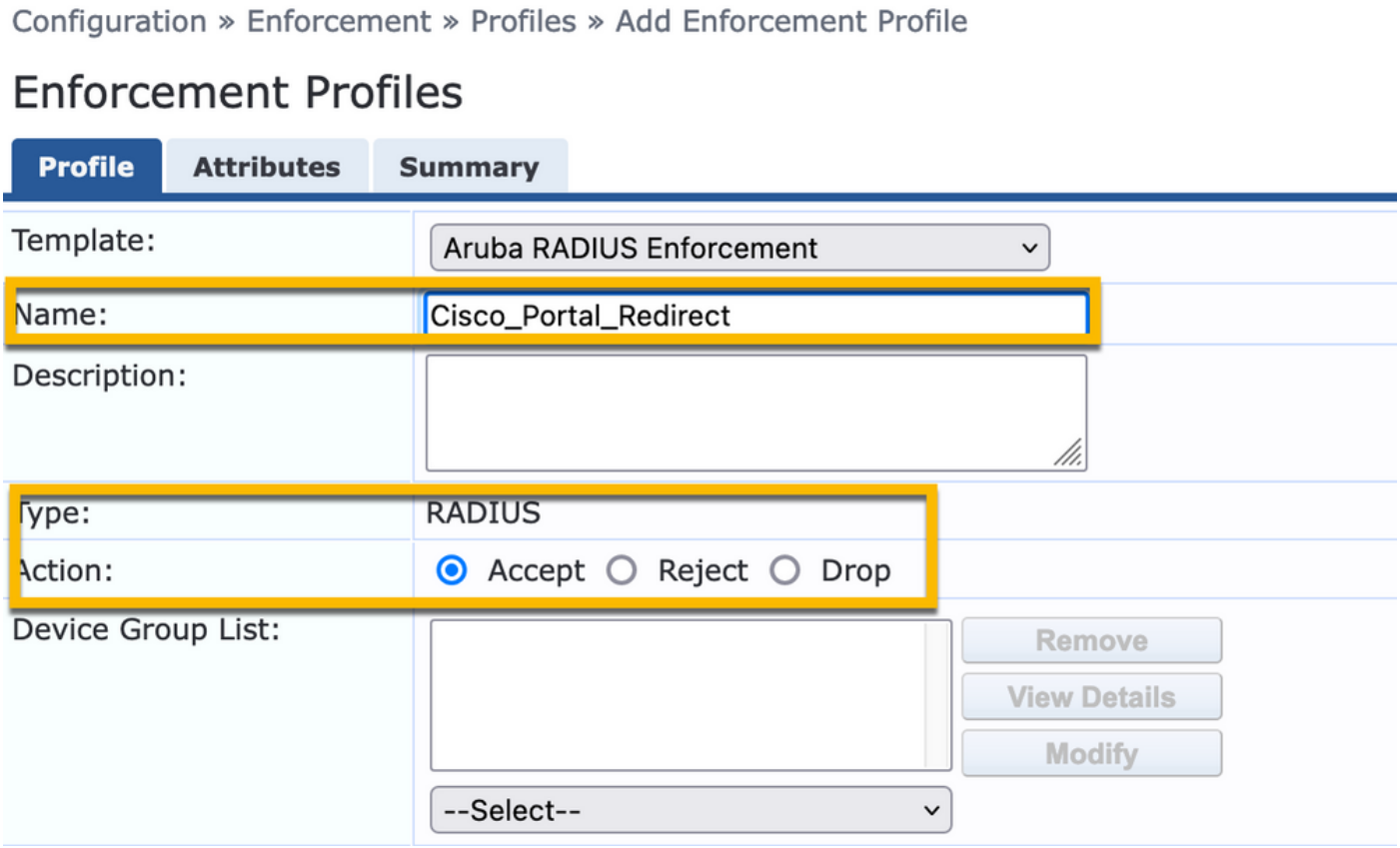
これにより、9800 WLCは外部認証のためにゲストクライアントをCPPMゲストポータルにリダイレクトします。

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

-Name：Cisco_Portal_Redirect

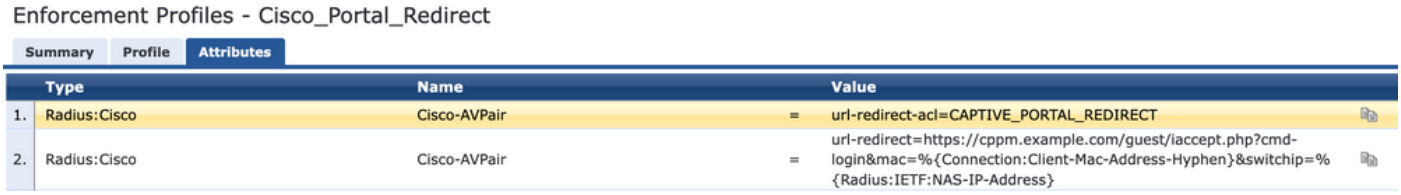
-タイプ:RADIUS

-Action:Accept



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。



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。

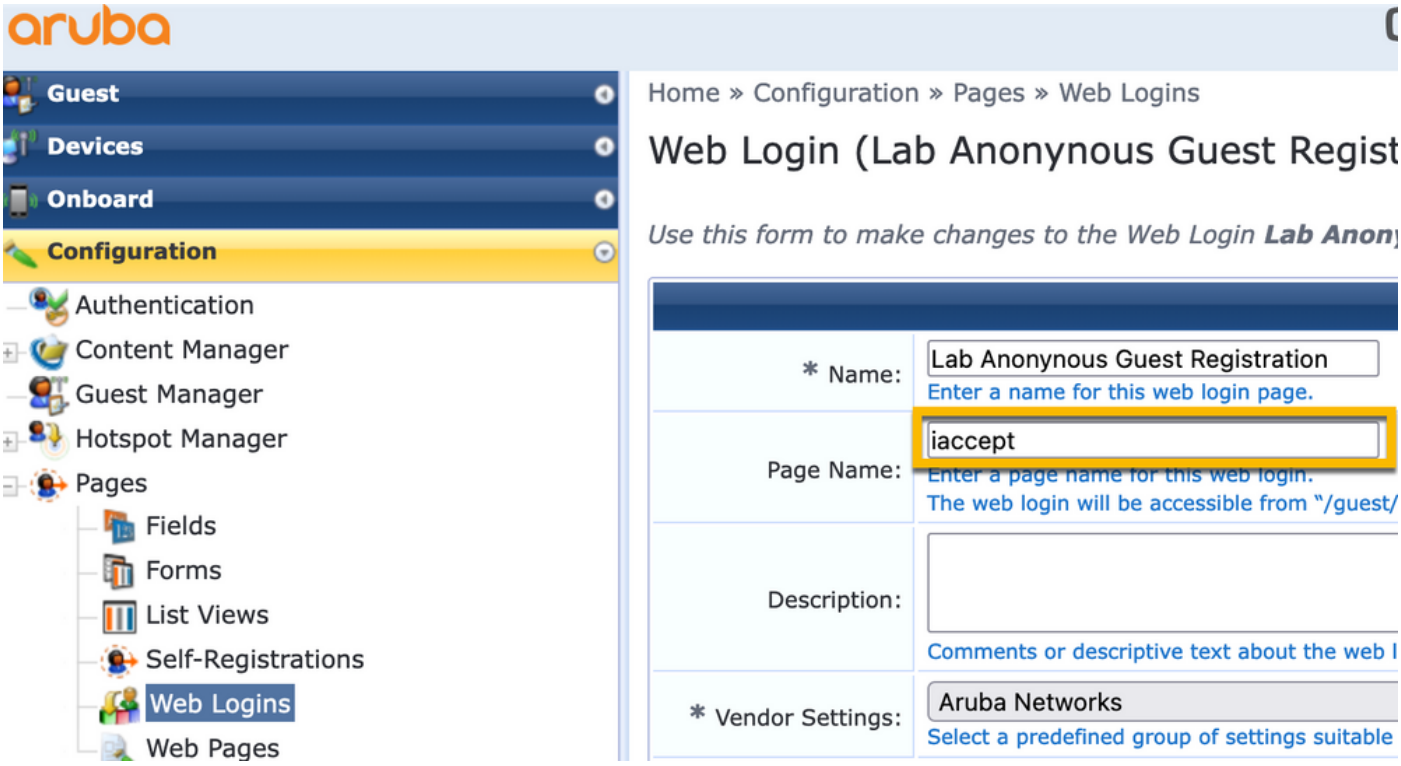
url-redirect属性は、複数のパラメータで構成されます。

- **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。



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

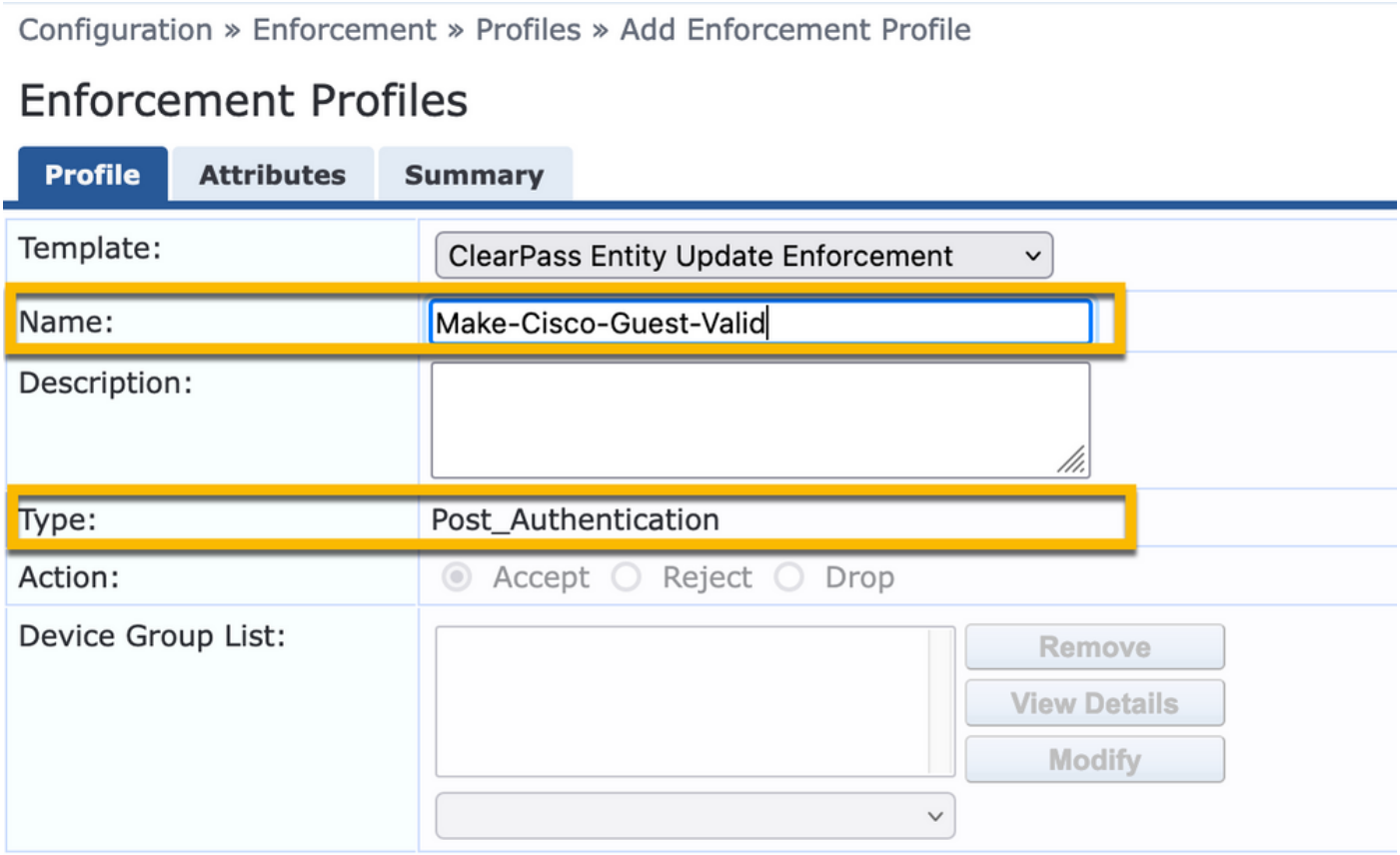
CPPMによる状態遷移の追跡に使用されるEndpointメタデータ属性を更新するように、強制プロファイルを構成します。

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



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

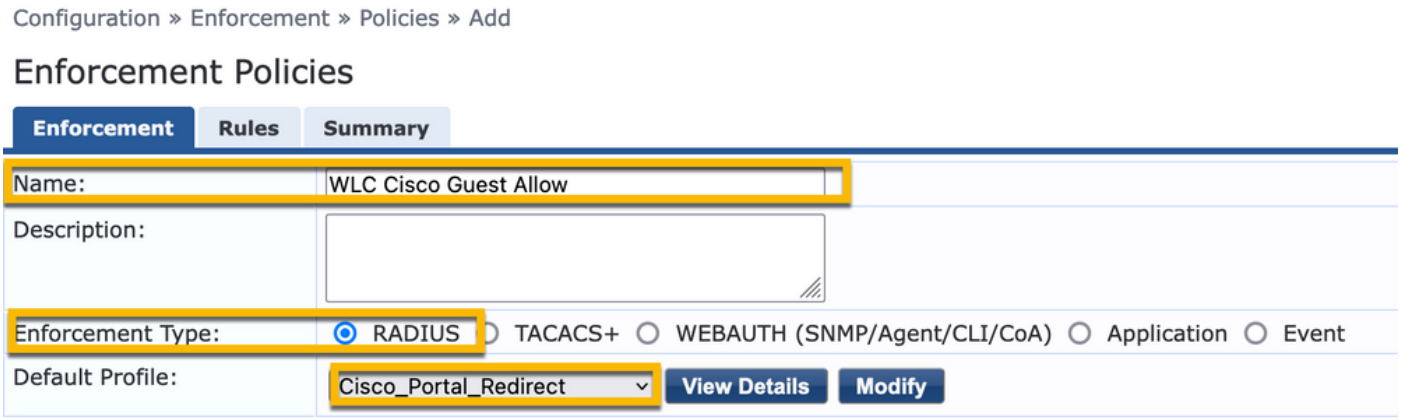
ClearPassゲストインターネットアクセス適用ポリシーの設定

[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



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。

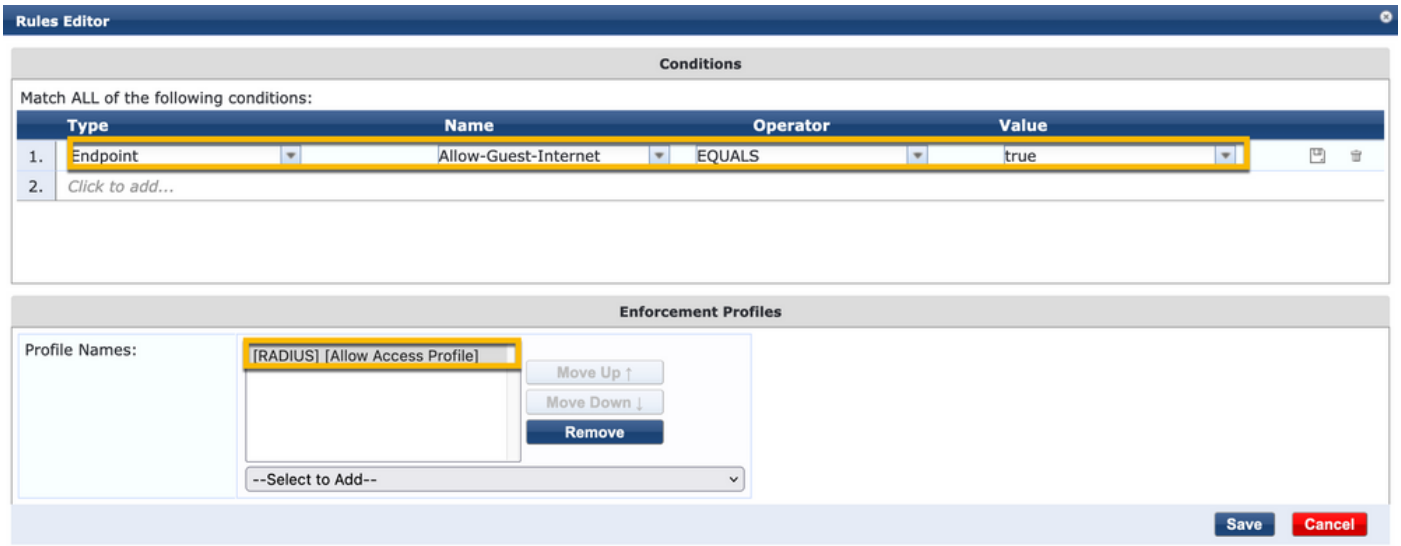
-タイプ:エンドポイント

-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]



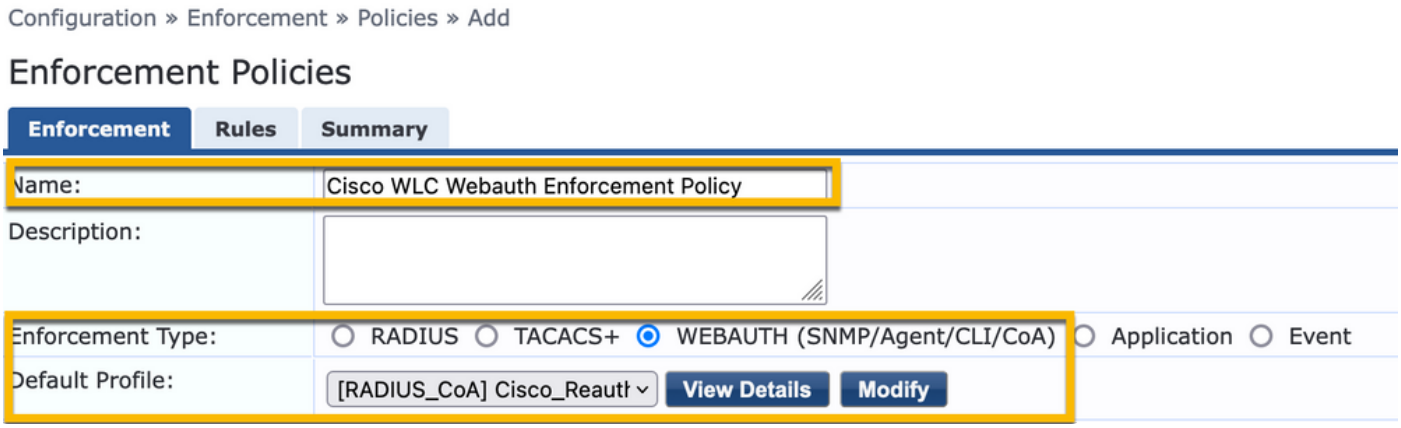
ClearPassゲストのAUP後の適用ポリシーの設定

[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



同じダイアログで、[Rules] > [Add] に移動します。

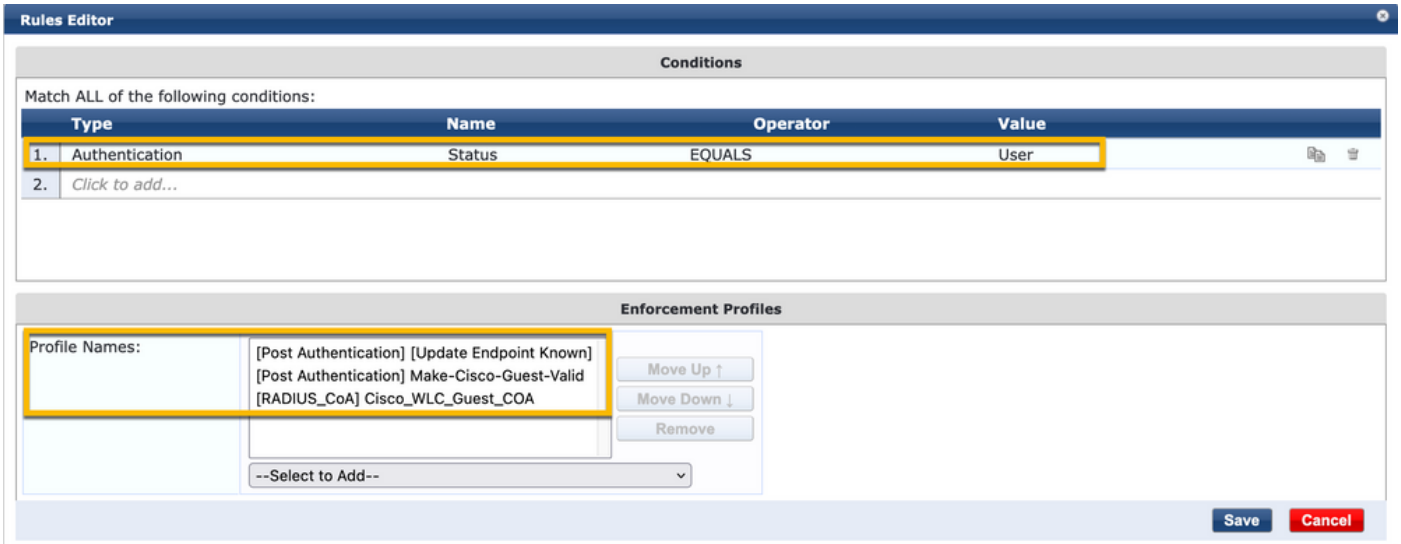
-条件：[Authentication]

-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]



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：

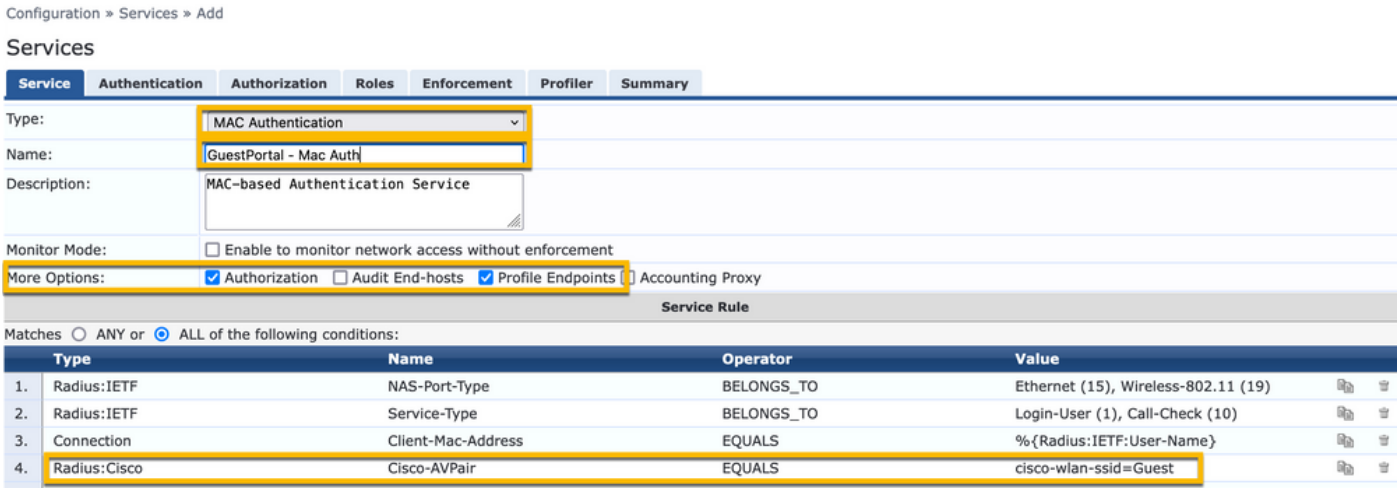
-タイプ:Radius:『シスコ

-Name：Cisco-AVPair

-Operator：[Equals]

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

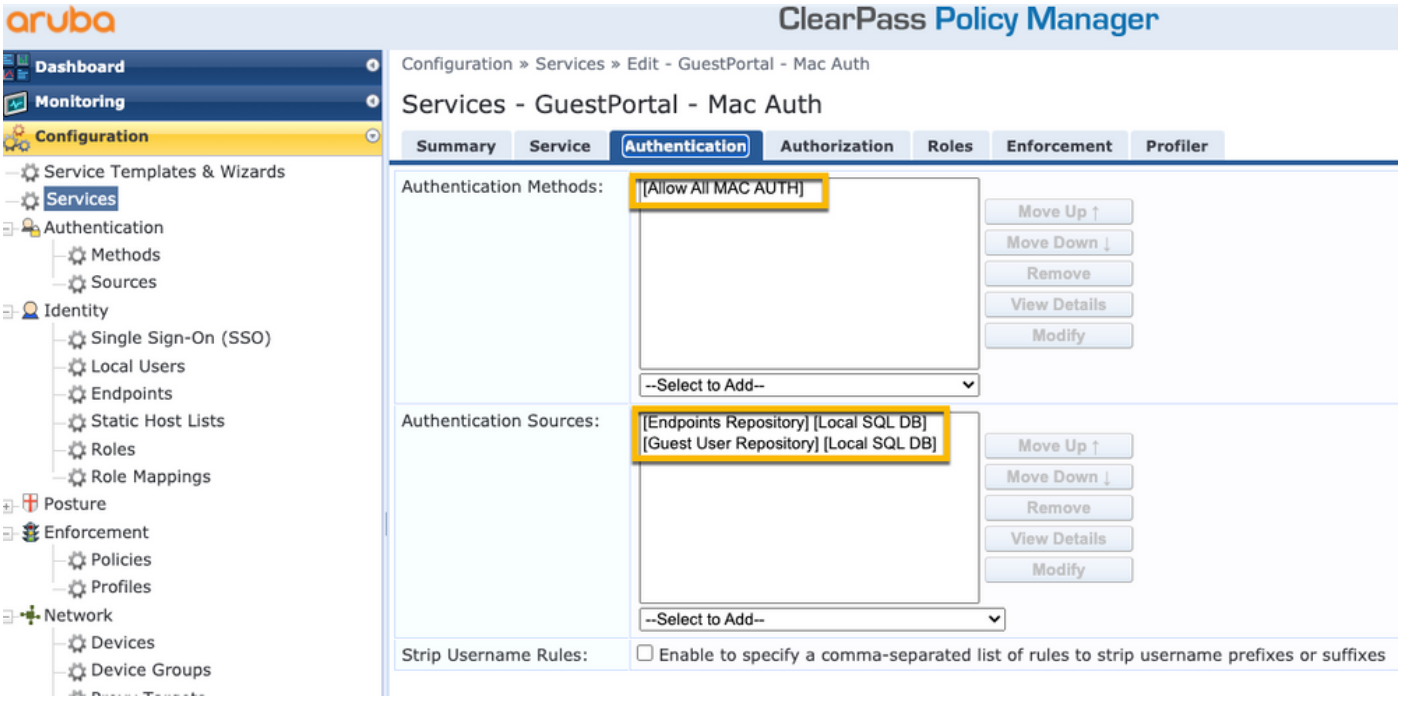
> **注：**「Guest」は、9800 WLCによってブロードキャストされるゲストSSIDの名前です。



同じダイアログで、[Authentication] タブを選択します。

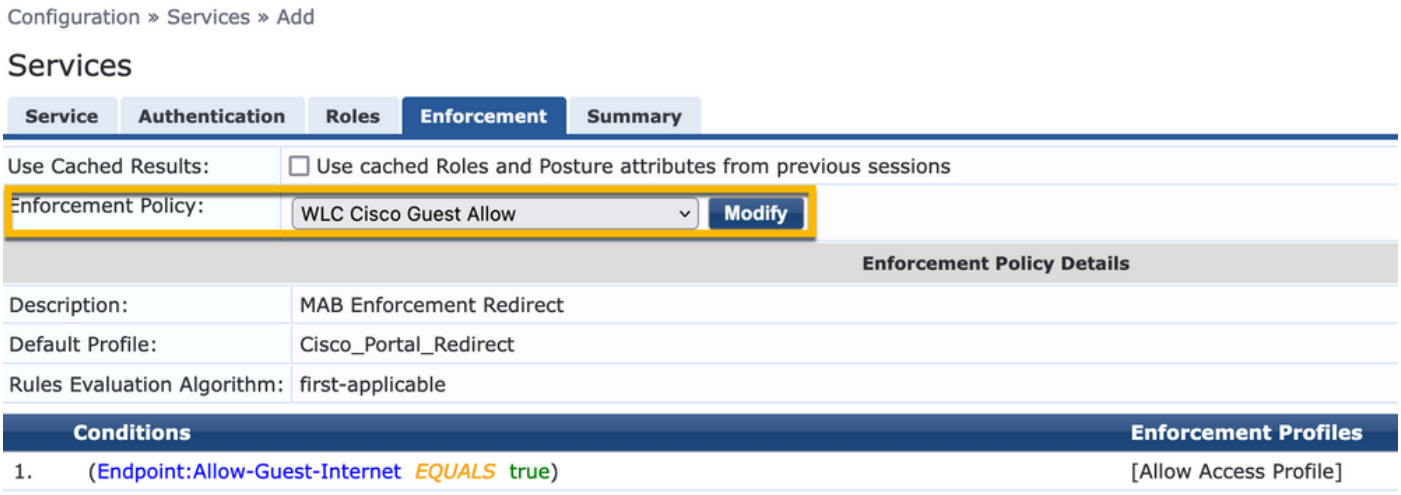
-認証方式:[MAC AUTH]を削除し、[Allow All MAC AUTH]を追加します。

– 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]

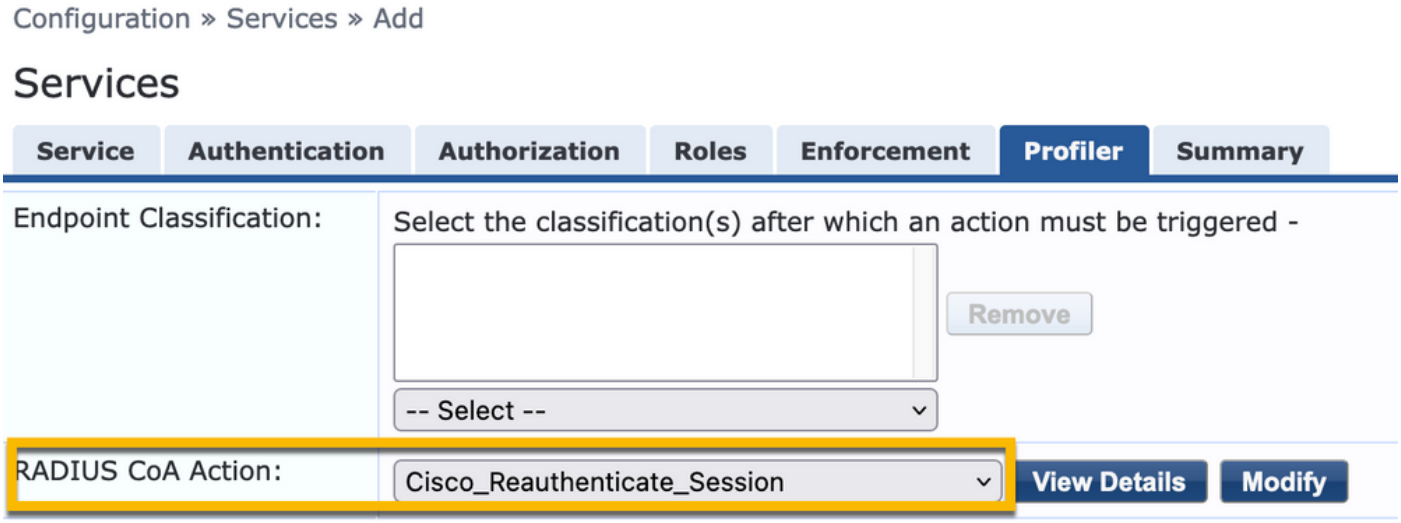


同じダイアログで、[Enforcement] タブを選択します。

– 適用ポリシー：WLCのCiscoゲスト許可



同じダイアログで、[Enforcement] タブを選択します。

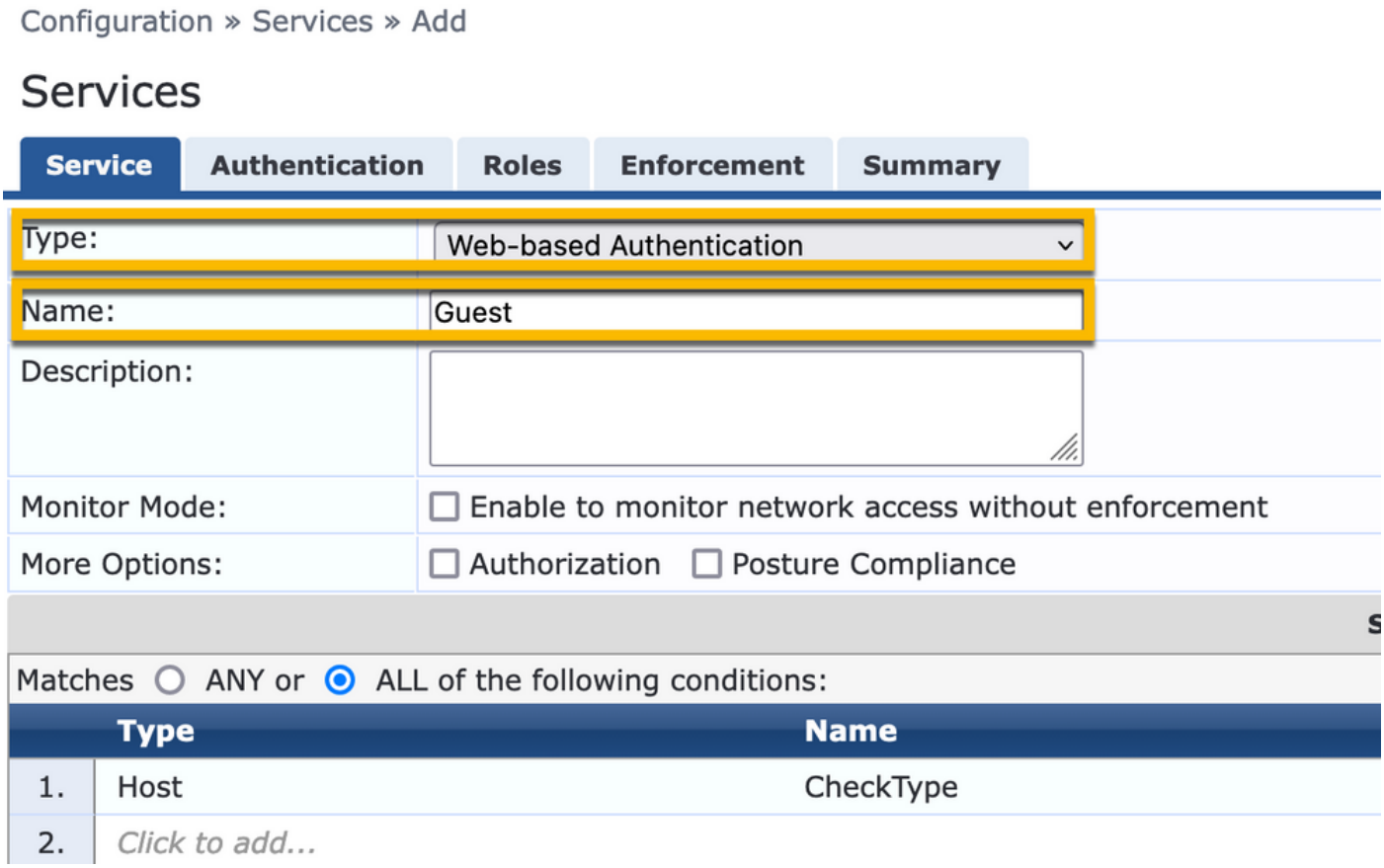


ClearPass Webauthサービスの設定

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

-Name：Guest_Portal_Webauth

-タイプ:Web ベースの認証



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

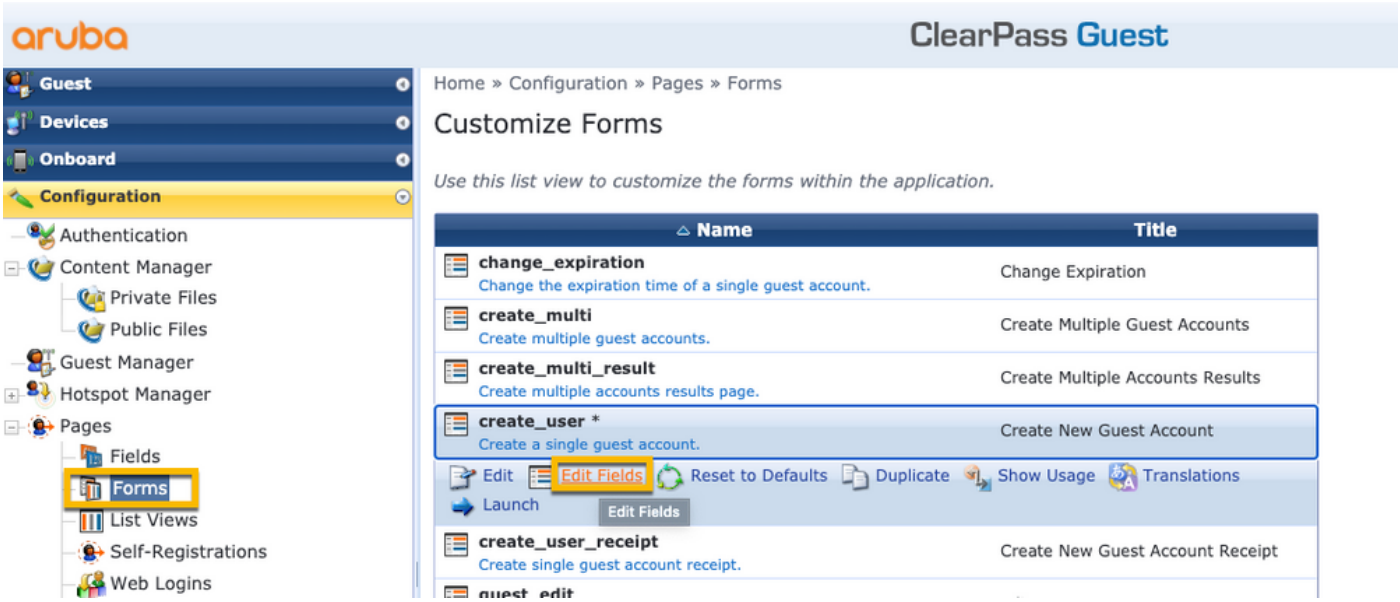
ClearPass:Webログイン

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。

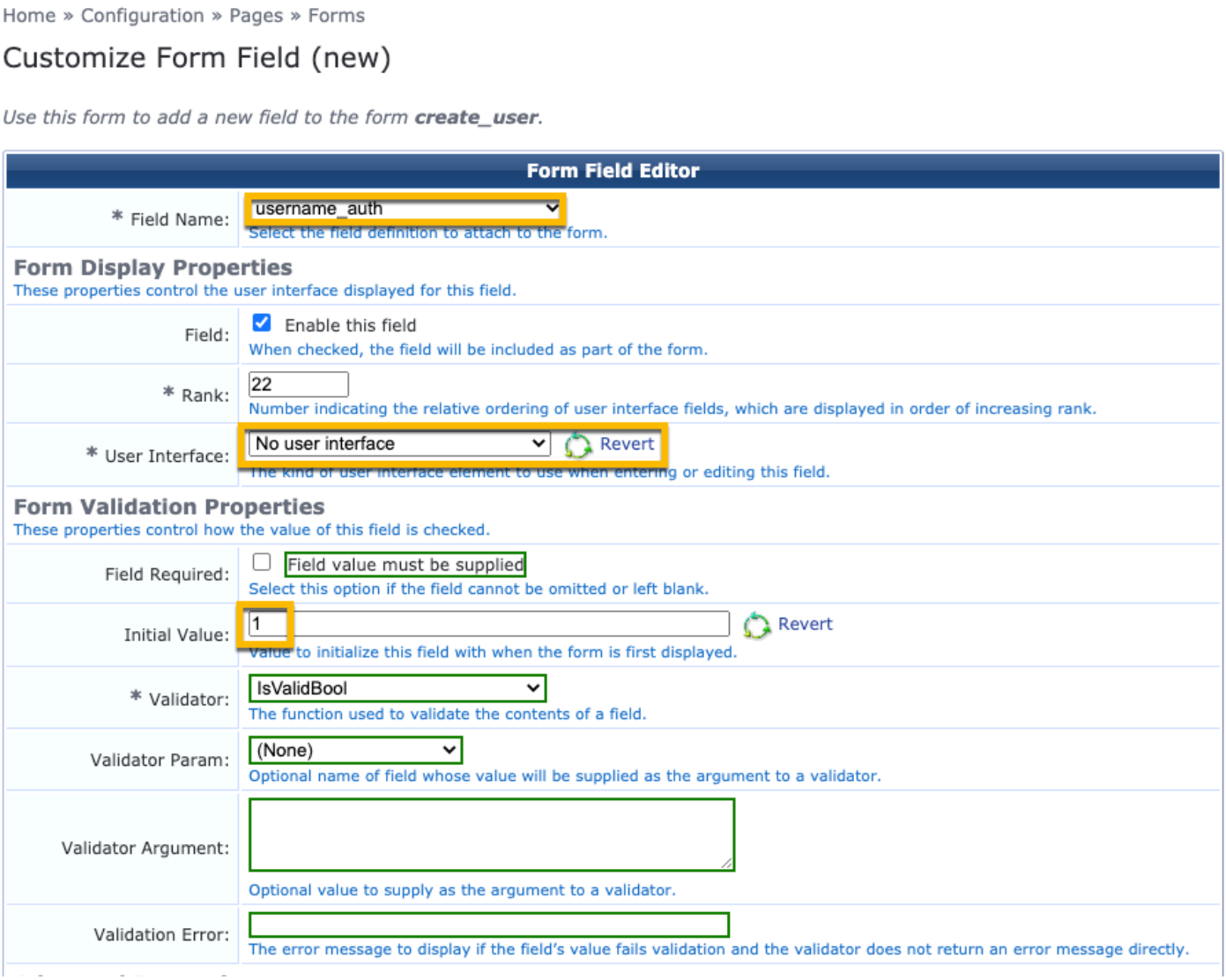
使用するユーザ名には、次のフィールドが定義または設定されている必要があります。

username_auth |ユーザー名認証： | 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。



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

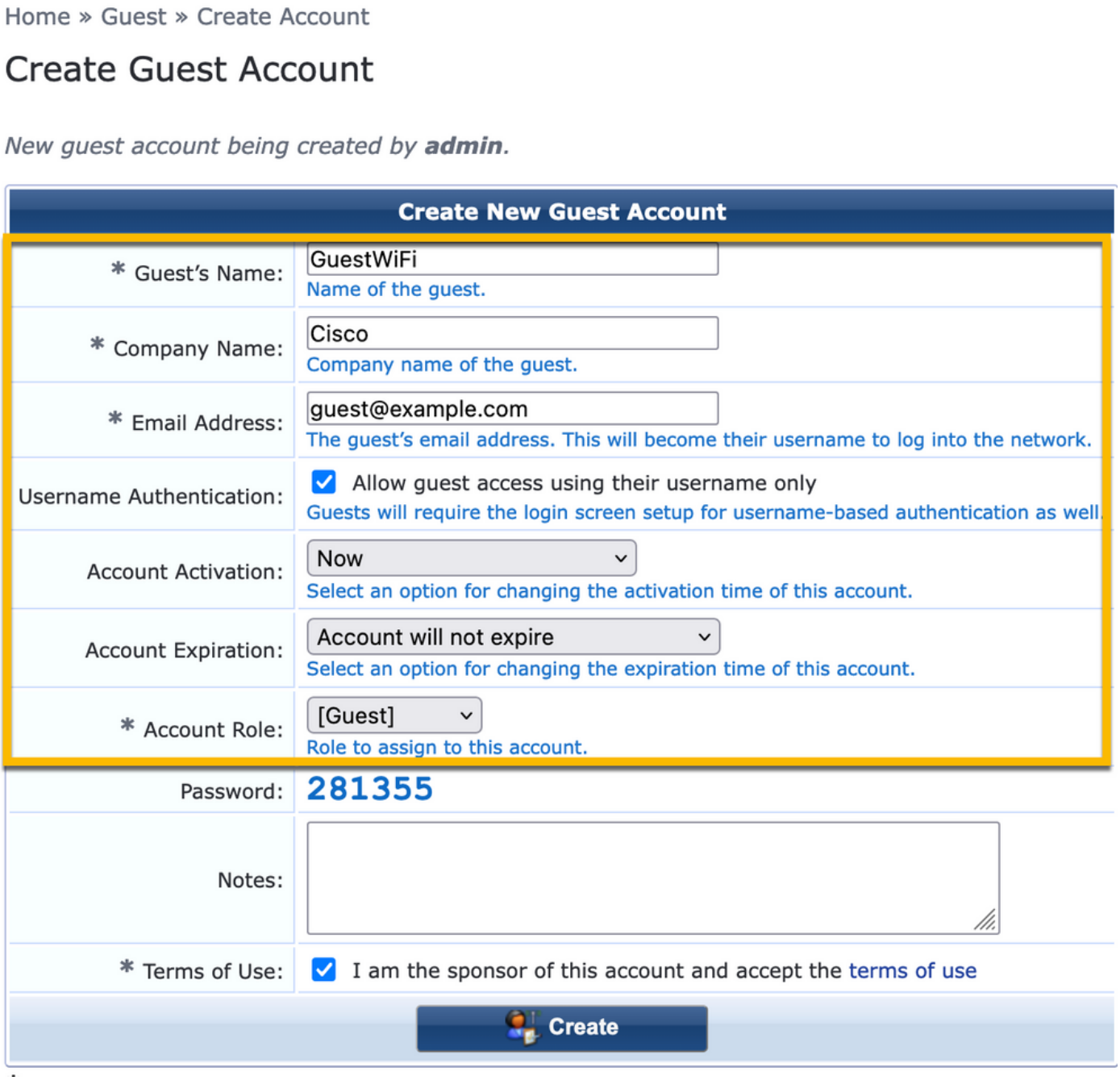
– 電子メールアドレス：guest@example.com

– 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

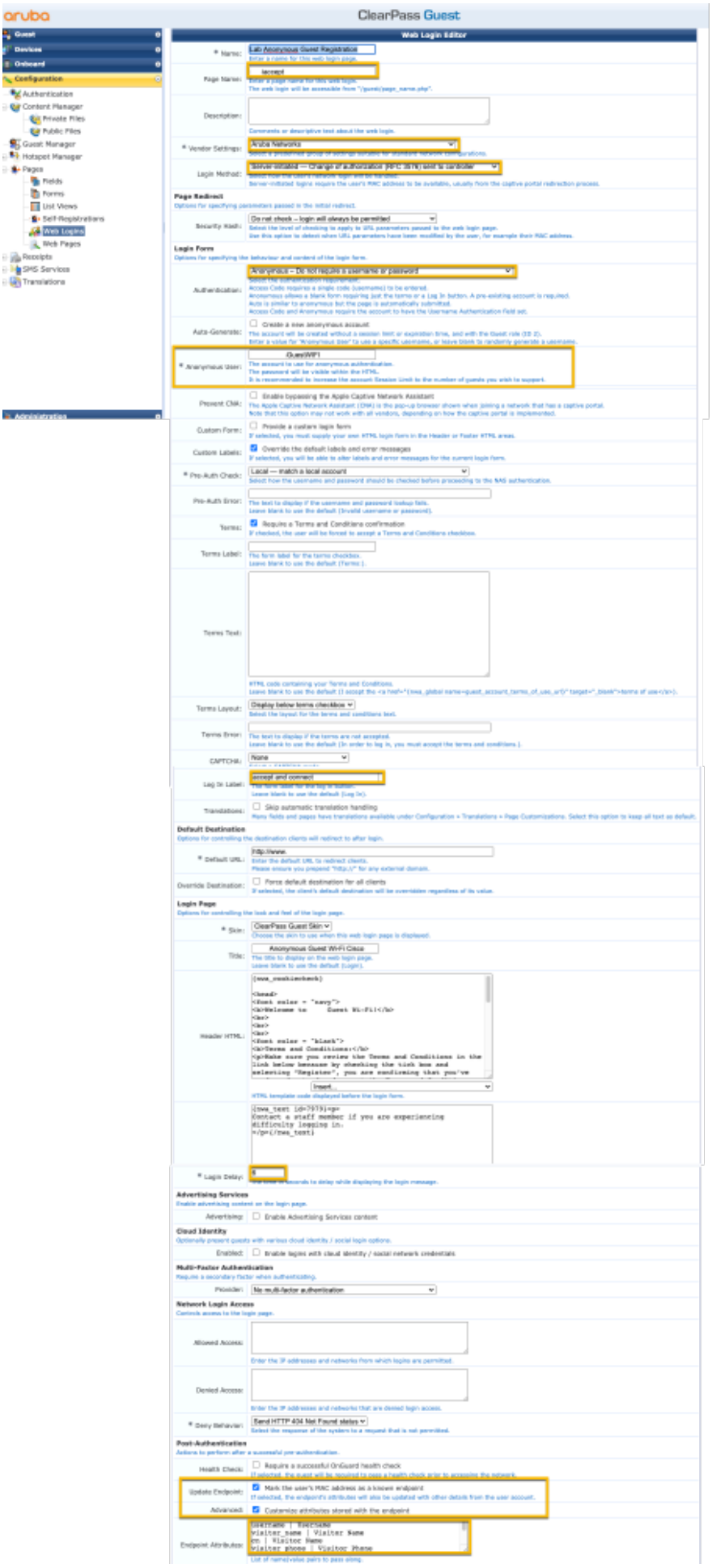
– 使用条件：私がスポンサーです。有効



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

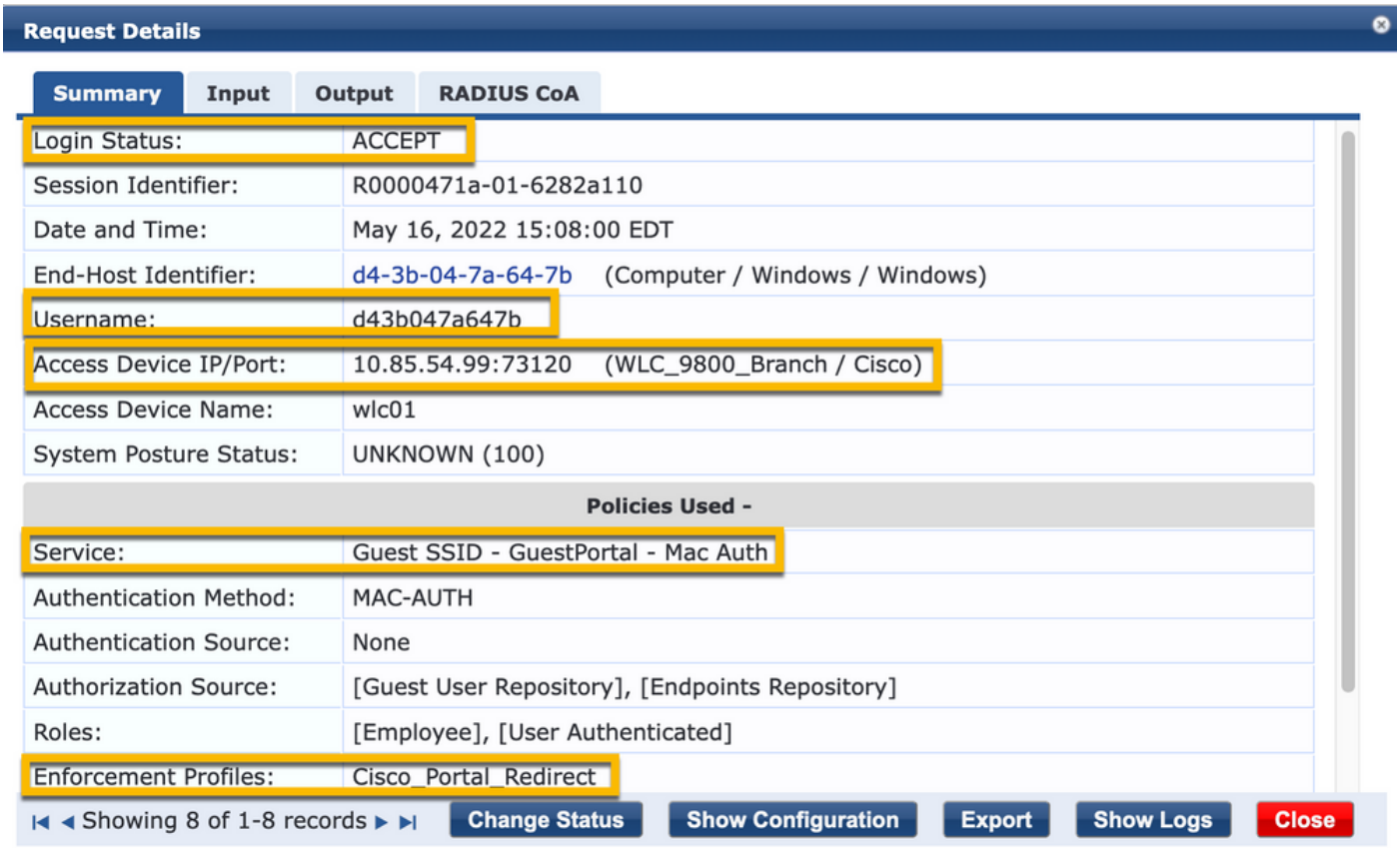

aruba
ClearPass Guest
Web Login Editor
Guest
Devices
Onboard
Configuration
Authentication
Content Manager
Private Files
Public Files
Guest Manager
Hotspot Manager
Pages
Fields
Forms
List Views
Self-Registrations
Web Logins
Web Pages
Receipts
SMS Services
Translations
Administration
* Name:
Page Name:
Description:
* Vendor Settings:
Login Method:
Page Redirect
Security Hash:
Login Form
Authentication:
Auto-Generate:
* Anonymous User:
Prevent CNA:
Custom Form:
Custom Labels:
* Pre-Auth Check:
Pre-Auth Error:
Terms:
Terms Label:
Terms Text:
Terms Layout:
Terms Error:
CAPTCHA:
Log In Label:
Translations:
Default Destination
* Default URL:
Override Destination:
Login Page
* Skin:
Title:
Header HTML:
* Login Delay:
Advertising Services
Advertising:
Cloud Identity
Enabled:
Multi-Factor Authentication
Provider:
Network Login Access
Allowed Access:
Denied Access:
* Deny Behavior:
Post-Authentication
Health Check:
Update Endpoint:
Advanced:
Endpoint Attributes:

検証：ゲストCWA認証

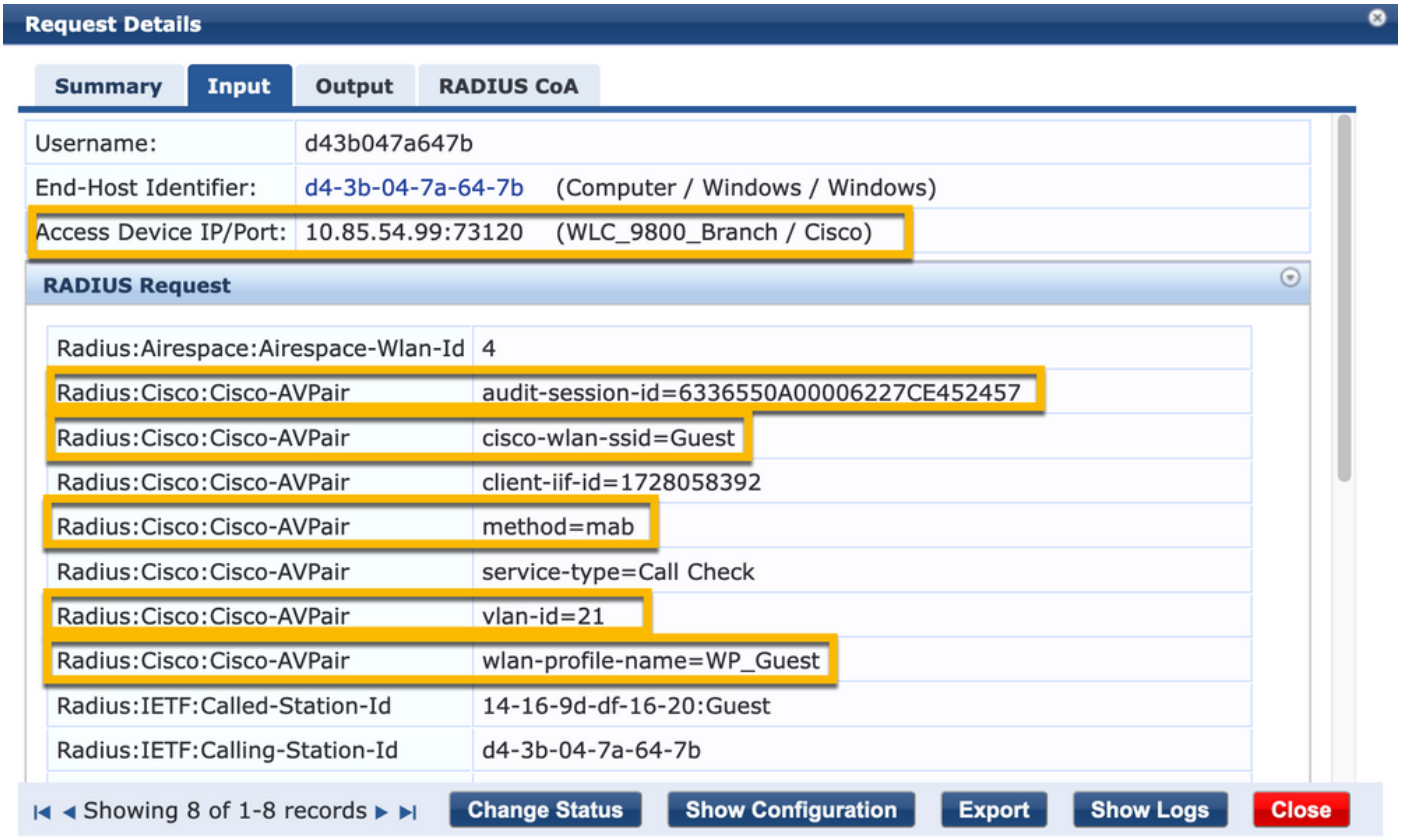
CPPMで、[Live Monitoring] > [Access Tracker] に移動します。

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。

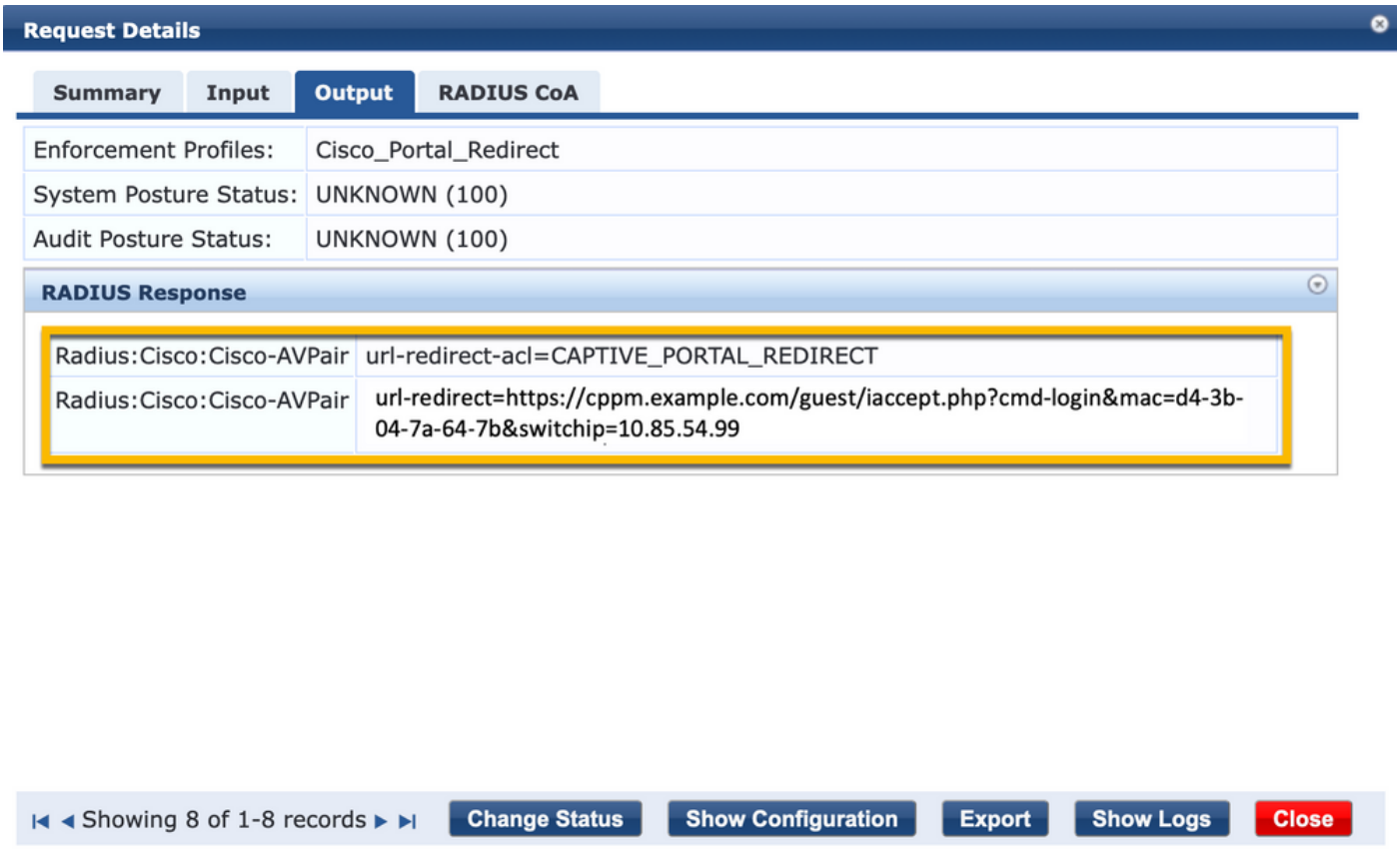
[Summary]タブ：



同じダイアログで、[Input] タブに移動します。



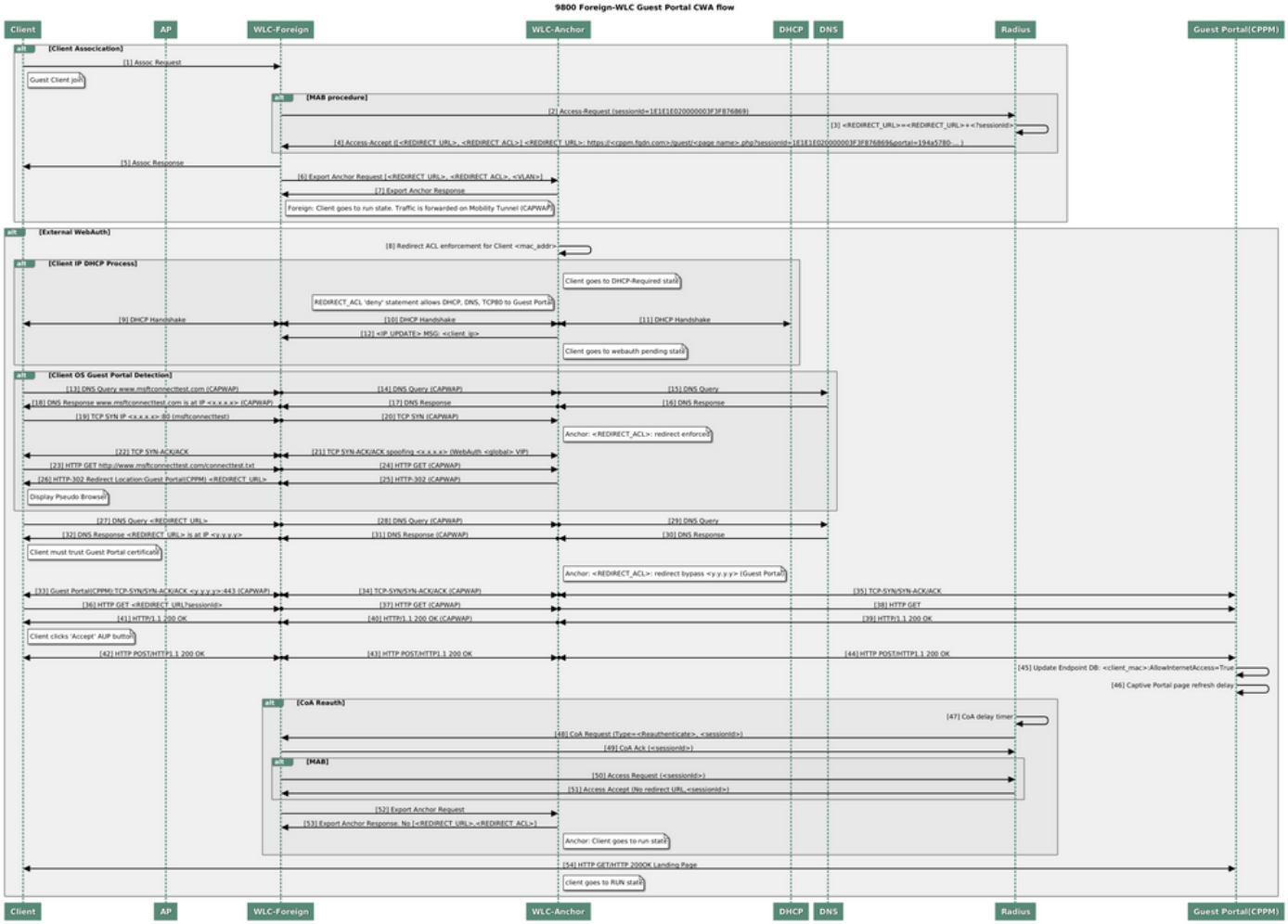
同じダイアログで、[Output] タブに移動します。



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。