Catalyst 9800 WLCを使用したDNAスペースキャプティブポータルの設定

内容

概要

このドキュメントでは、Cisco DNA Spaceでキャプティブポータルを設定する方法について説明

します。

前提条件

このドキュメントでは、Catalyst 9800ワイヤレスLANコントローラ(C9800 WLC)上のクライアントが外部Web認証ログインページとしてDNAスペースを使用できるようにします。

要件

次の項目に関する知識があることが推奨されます。

- 9800ワイヤレスコントローラへのコマンドラインインターフェイス(CLI)またはグラフィックユーザインターフェイス(GUI)アクセス
- Cisco DNA Spaces

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。

- 9800-Lコントローラバージョン16.12.2s

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

Web認証は、サプリカントやクライアントユーティリティを必要としないシンプルなレイヤ3認証方式です。これは可能です

a) C9800 WLCの内部ページを現状のまま、または変更をポストして

b)カスタマイズされたログインバンドルをC9800 WLCにアップロードする

c)外部サーバでホストされるカスタムログインページ

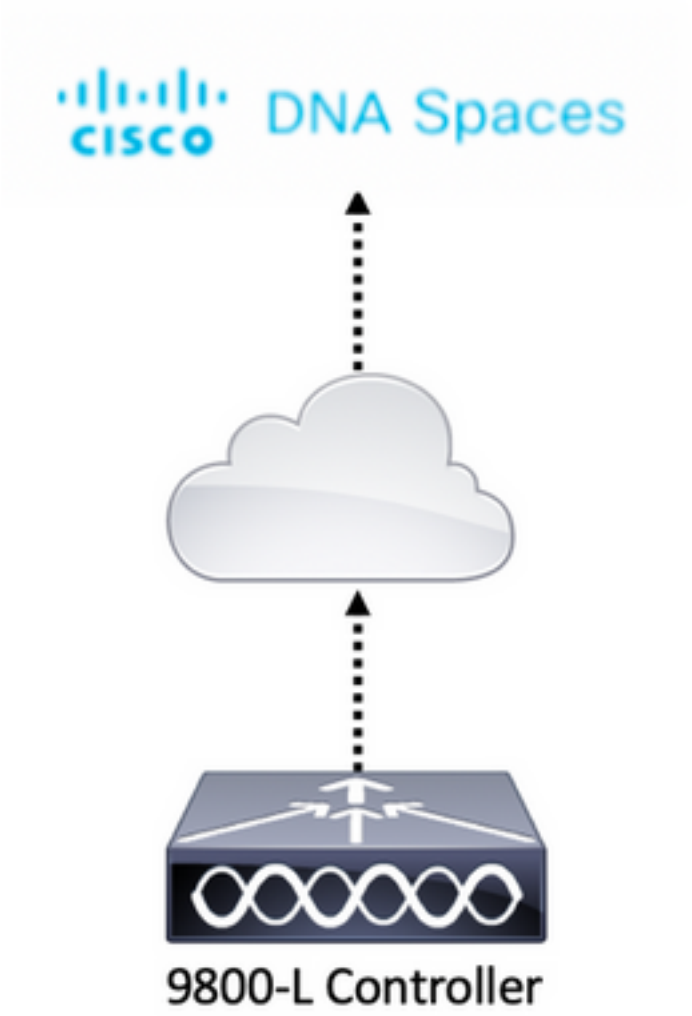
DNA Spacesが提供するキャプティブポータルを活用することは、基本的にC9800 WLC上のクライアントに外部Web認証を実装する方法です。

外部webauthプロセスの詳細については、次のサイトを参照してください。
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/web-authentication/b-configuring-web-based-authentication-on-cisco-catalyst-9800-series-controllers/m-external-web-authentication-configuration.html

C9800 WLCでは、仮想IPアドレスはグローバルパラメータマップで定義され、通常は192.0.2.1です

設定

ネットワーク図



9800コントローラをCisco DNA Spaceに接続する

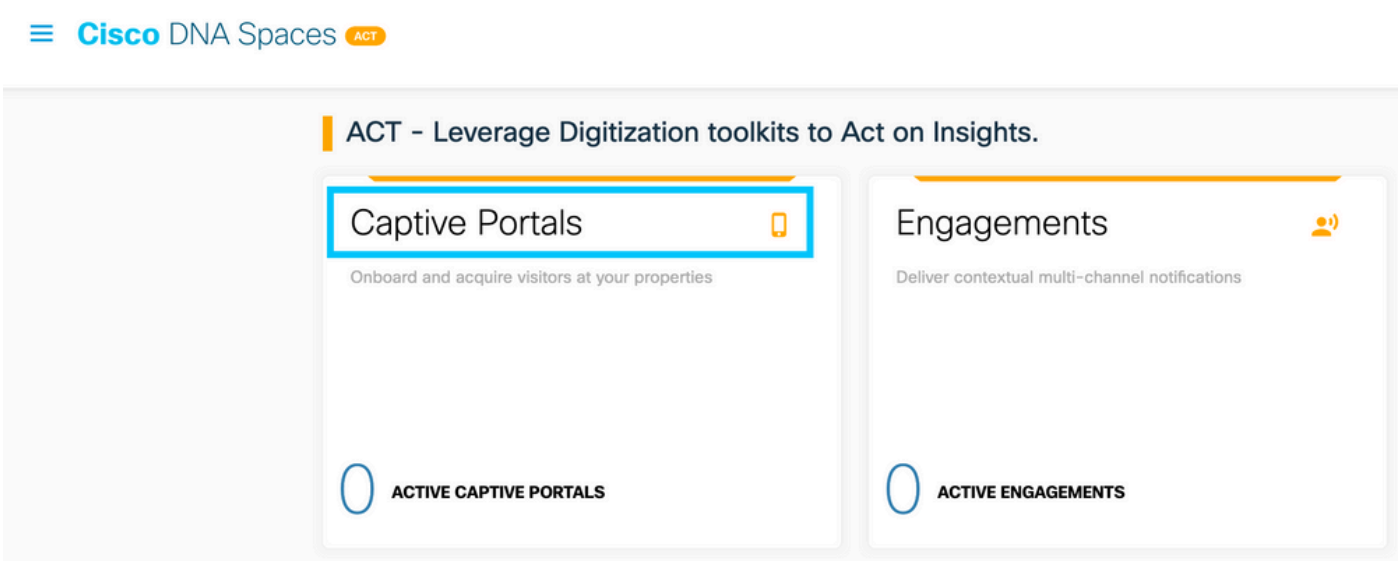
コントローラは、DNAスペースコネクタを介して、またはCMXテザリングを使用して、Direct Connectのいずれかのオプションで DNAスペースに接続する必要があります。

この例では、[Direct Connect]オプションが使用されていますが、キャプティブポータルはすべての設定に対して同じ方法で設定されています。

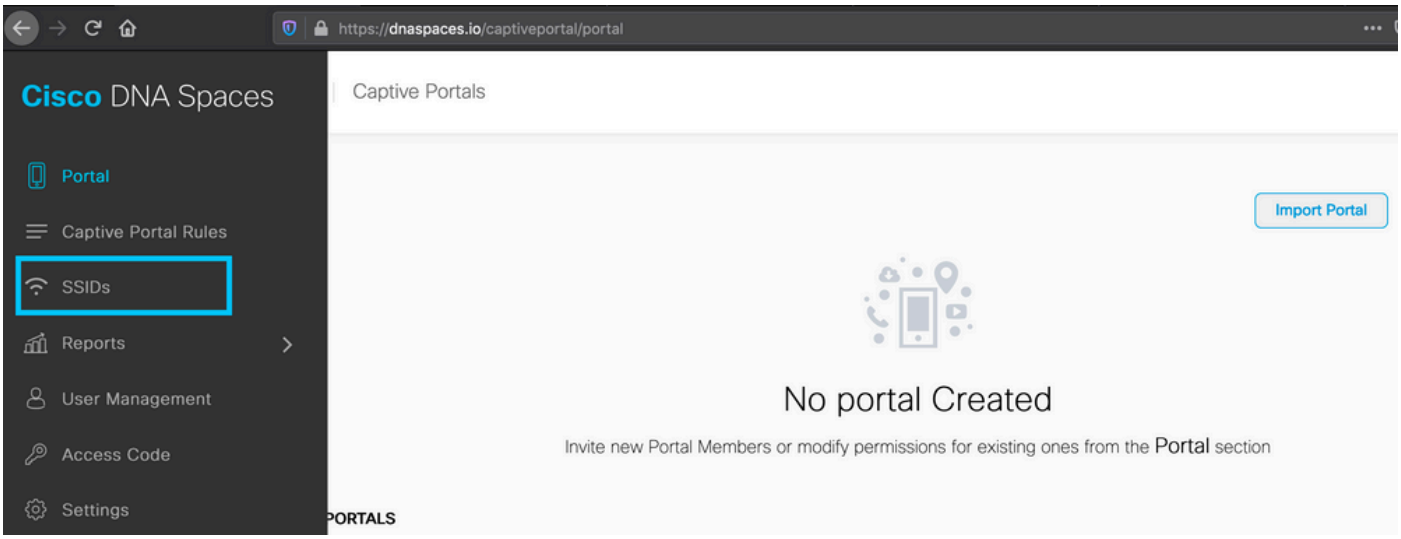
コントローラをCisco DNA Spacesに接続するには、HTTPS経由でCisco DNA Spaces Cloudに到達できる必要があります。9800コントローラをDNAスペースに接続する方法の詳細については、次のリンクを参照してください。DNA Spaces - 9800 Controller Direct Connect

DNAスペースでのSSIDの作成

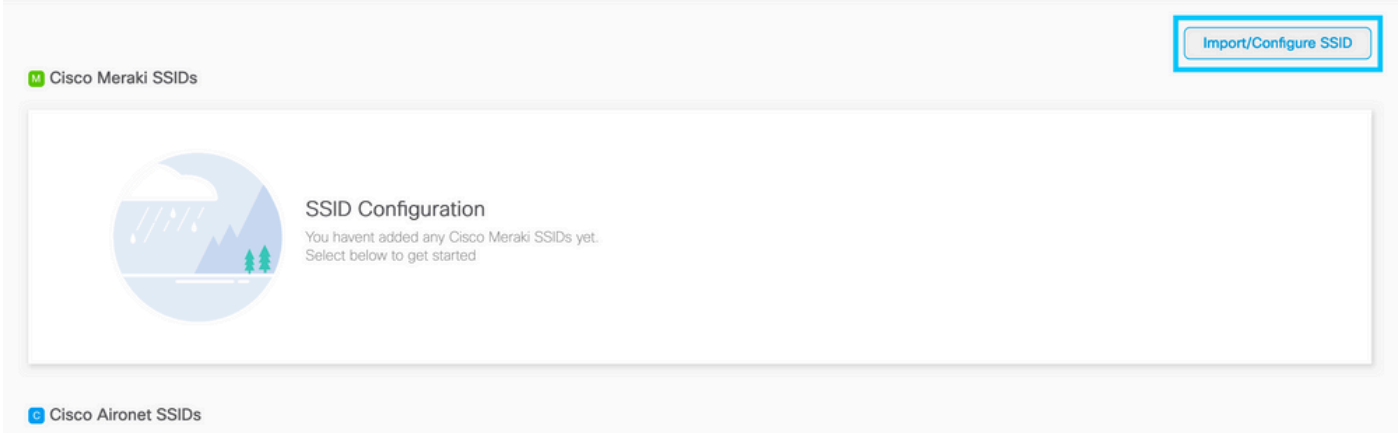
ステップ 1：DNA Spacesのダッシュボードで[Captive Portals] をクリックします。



ステップ 2：キャプティブポータルの特定のメニューを開き、ページの左上隅にある3行のアイコンをクリックし、[**SSIDs:**



ステップ 3：[Import/Configure SSID] をクリックし、[Wireless Network]タイプとして[CUWN (CMX/WLC)] を選択し、SSID名を入力します。



9800コントローラでのACLおよびURLフィルタの設定

ワイヤレスクライアントからのトラフィックは、認証が完了するまでネットワーク上で許可されません。Web認証の場合、これを完了するために、ワイヤレスクライアントはこのSSIDに接続し

、IPアドレスを受け取り、クライアントポリシーマネージャの状態はWebauth_reqd状態に移行します。クライアントはまだ認証されていないため、クライアントIPアドレスから発信されるすべてのトラフィックは、DHCP、DNS、およびHTTP（代行受信され、リダイレクトされる）を除いて廃棄されます。

デフォルトでは、Web認証WLANを設定すると、9800はハードコードされた事前認証ACLを作成します。これらのハードコードACLにより、DHCP、DNS、および外部Web認証サーバへのトラフィックが許可されます。残りはすべて、HTTPトラフィックと同様にリダイレクトされます。ただし、特定の非HTTPトラフィックタイプの通過を許可する必要がある場合は、事前認証ACLを設定できます。次に、既存のハードコードされた事前認証ACL（このセクションのステップ1で説明）の内容を模倣し、必要に応じて拡張する必要があります。

ステップ 1：現在のハードコードされたACLの確認

CLI による設定：

```
Andressi-9800L#show ip access list

Extended IP access list WA-sec-34.235.248.212
10 permit tcp any host 34.235.248.212 eq www
20 permit tcp any host 34.235.248.212 eq 443
30 permit tcp host 34.235.248.212 eq www any
40 permit tcp host 34.235.248.212 eq 443 any
50 permit tcp any any eq domain
60 permit udp any any eq domain
70 permit udp any any eq bootpc
80 permit udp any any eq bootps
90 deny ip any any

Extended IP access list WA-v4-int-34.235.248.212
10 deny tcp any host 34.235.248.212 eq www
20 deny tcp any host 34.235.248.212 eq 443
30 permit tcp any any eq www
40 permit tcp any host 192.0.2.1 eq 443
```

WA-sec-34.235.248.212は、自動Web認証(WA)セキュリティ(sec)ACLまたはポータルIP「34.235.248.212」であるため、そのように呼ばれます。セキュリティACLは、許可(permit)またはドロップ(deny)を定義します。

Wa-v4-intは代行受信ACLです。これはパントACLまたはリダイレクトACLであり、リダイレクト用に（permitで）CPUに送信される内容または（denyで）データプレーンに送信される内容を定義します。

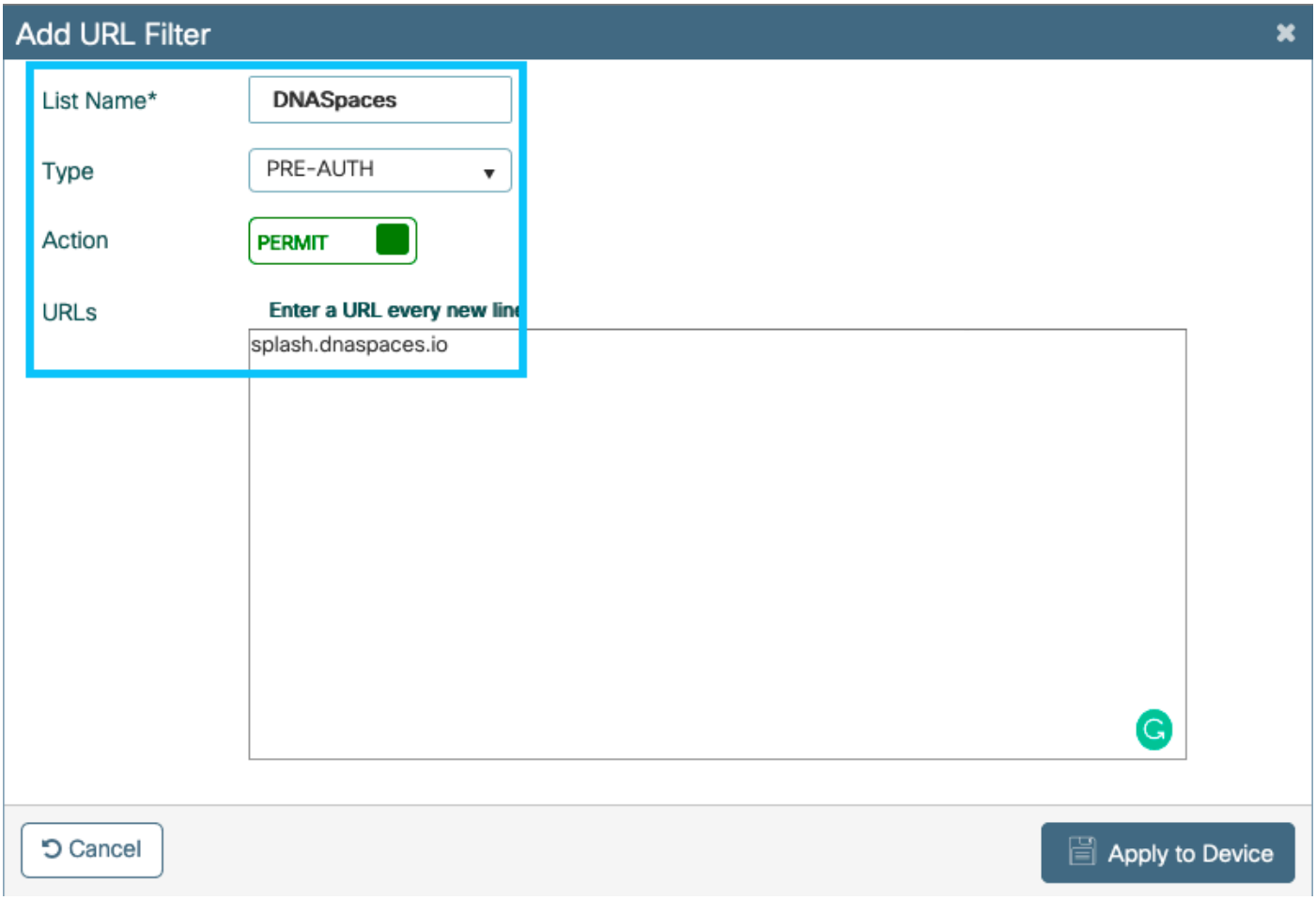
WA-v4-int34.235.248.212は、クライアントから送信されるトラフィックに最初に適用され、データプレーン上のDNA SpacesポータルIP 34.235.248.212に向かうHTTP(s)トラフィックを保持します（ドロップまたは転送アクションはまだ行われず、データプレーンに渡すだけです）。Webサーバによって処理される仮想IPトラフィックを除くリダイレクション用に、すべてのHTTPトラフィックをCPUに送信します。データプレーンには、他のタイプのトラフィックが与えられます。

WA-sec-34.235.248.212は、Web認証パラメータマップで設定したDNA空間IP 34.235.248.212へのHTTPおよびHTTPSトラフィックを許可し、DNSおよびDHCPトラフィックも許可し、残りはドロップします。代行受信されるHTTPトラフィックは、このACLに到達する前にすでに代行受信されているため、このACLでカバーされる必要はありません。

注:ACLで許可されるDNAスペースのIPアドレスを取得するには、「ACL設定」セクションの「**DNAスペースでのSSIDの作成**」セクションのステップ3で作成したSSIDから、[Configure Manually] オプションをクリックします。例は、このドキュメントの最後にある「DNAスペースが使用するIPアドレスは何ですか」の項にあります。

DNAスペースは2つのIPアドレスを使用し、手順1のメカニズムでは1つのポータルIPのみを許可します。より多くのHTTPリソースへの事前認証アクセスを許可するには、URLフィルタを使用する必要があります。このURLフィルタは、URLフィルタに入力したURLを持つWebサイトに関連するIPに対して、インターセプト（リダイレクト）ACLとセキュリティ（事前認証）ACLに動的にホールを形成します。DNS要求は9800に対して動的にスヌーピングされ、これらのURLのIPアドレスが学習されてACLに動的に追加されます。

ステップ 2：DNAスペースドメインを許可するようにURLフィルタを設定します。[Configuration] > [Security] > [URL Filters] に移動し、[**+Add**]をクリックしてリスト名を設定し、タイプとして**PRE-AUTH**を選択し、**PERMIT**としてアクションを選択し、URLとして**splash.dnaspaces.io**（EMEAポータルを使用する場合は.eu）を選択します。



CLI による設定：

```
Andressi-9800L(config)#urlfilter list
```

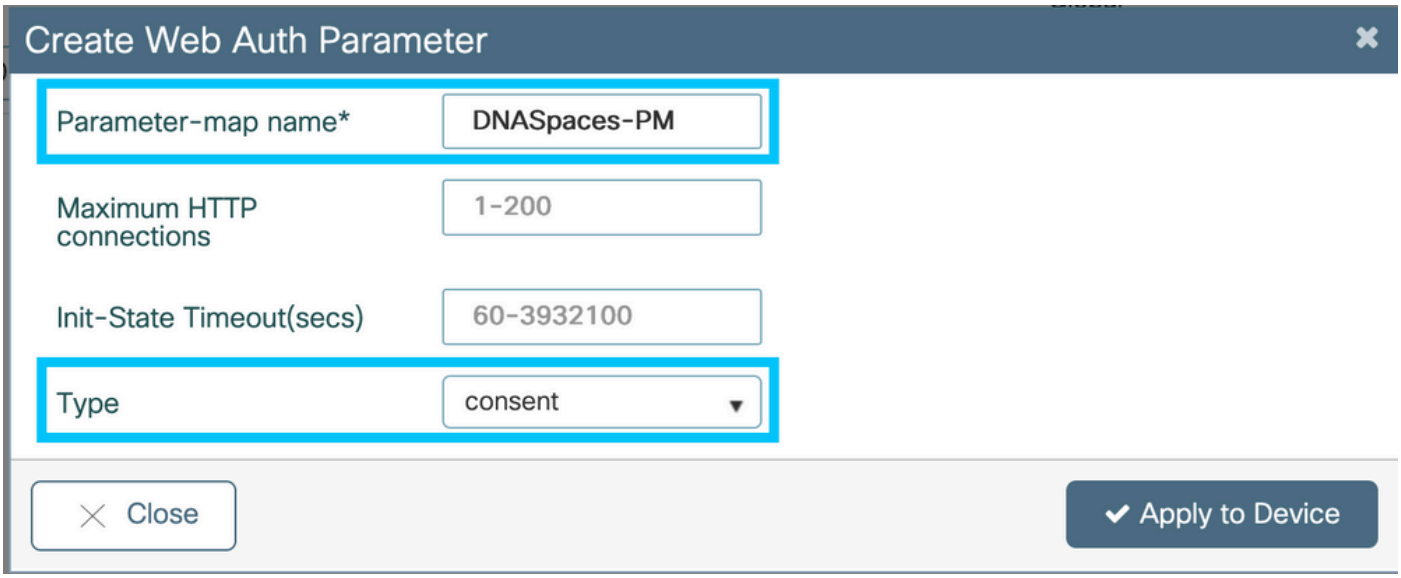
```
Andressi-9800L(config-urlfilter-params)#action permit
Andressi-9800L(config-urlfilter-params)#url splash.dnaspaces.io
```

SSIDは、RADIUSサーバを使用するように設定することも、使用せずに設定することもできます。キャプティブポータルルール設定の[Actions] セクションで[Session Duration]、[Bandwidth Limit]、または[Seamently Provision Internet]が設定されている場合は、SSIDをRADIUSサーバで設定する必要があります。そうでない場合は、RADIUSサーバを使用する必要はありません。DNAスペース上のすべての種類のポータルは、両方の構成でサポートされています。

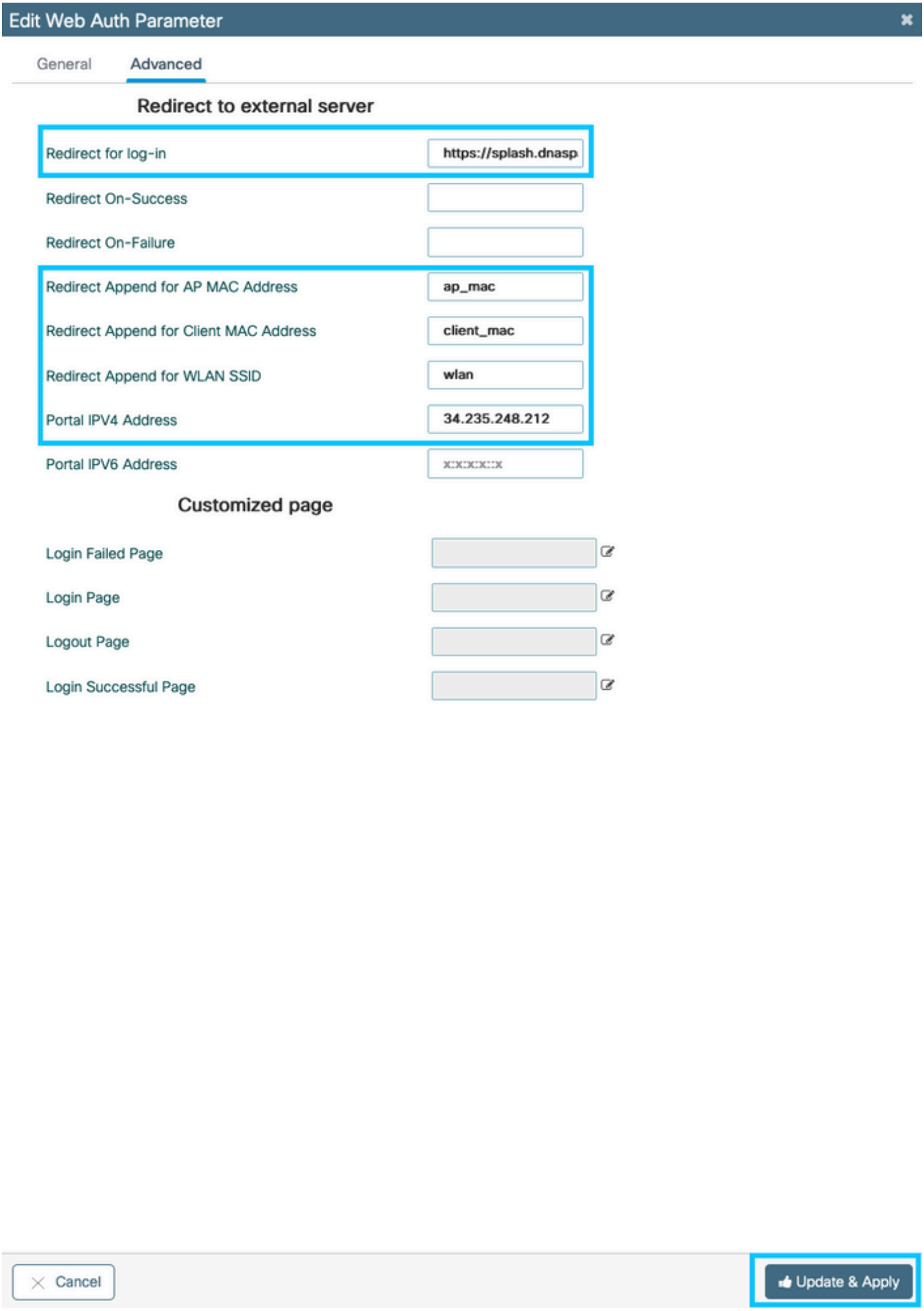
DNAスペース上のRADIUSサーバを使用しないキャプティブポータル

9800コントローラでのWeb認証パラメータマップの設定

ステップ 1：[Configuration] > [Security] > [Web Auth] に移動し、[Add] をクリックして新しいパラメータマップを作成します。ポップアップウィンドウで、パラメータマップ名を設定し、タイプとして[Consent] を選択します。



ステップ 2：前のステップで設定したパラメータマップをクリックし、[Advanced] タブに移動して、ログインURLの[Redirect]、[Append for AP MAC Address] 、[Append for Client MAC Address] 、[Append for WLAN SSID and portal IPv4 Address] を入力します（ 図を参照 ）。[Update & Apply] をクリックします。


Edit Web Auth Parameter
General
Advanced
Redirect to external server
Redirect for log-in
https://splash.dnasp
Redirect On-Success
Redirect On-Failure
Redirect Append for AP MAC Address
ap_mac
Redirect Append for Client MAC Address
client_mac
Redirect Append for WLAN SSID
wlan
Portal IPV4 Address
34.235.248.212
Portal IPV6 Address
X:X:X:X::X
Customized page
Login Failed Page
Login Page
Logout Page
Login Successful Page
Cancel
Update & Apply

注：スプラッシュページのURLとIPv4リダイレクトアドレスを取得するには、[DNA Spaces]の[SSID]ページで[Configure Manually] オプションをクリックします。これは、このドキュメントの最後にある「DNAスペースポータルが使用するURLは何ですか？」で説明されています

注:Cisco DNA Spacesポータルは2つのIPアドレスに解決できますが、9800コントローラでは1つのIPアドレスしか設定できません。これらのIPアドレスのいずれかを選択し、ポータルのIPv4アドレスとしてパラメータマップで設定します。

注：次の点を確認します。 仮想IPv4アドレスと仮想IPv6アドレスの両方が、グローバルWeb認証パラメータマップで設定されます。Virtual IPv6が設定されていない場合、クライアントは設定されたDNAスペースポータルではなく、内部ポータルにリダイレクトされることがあります。このため、仮想IPは常に設定する必要があります。「192.0.2.1」は仮想IPv4として、FE80:0:0:0:903A::11E4は仮想IPV6として設定できます。それ以外のIPを使用する理由はほとんどまたはまったくありません。

CLI による設定：

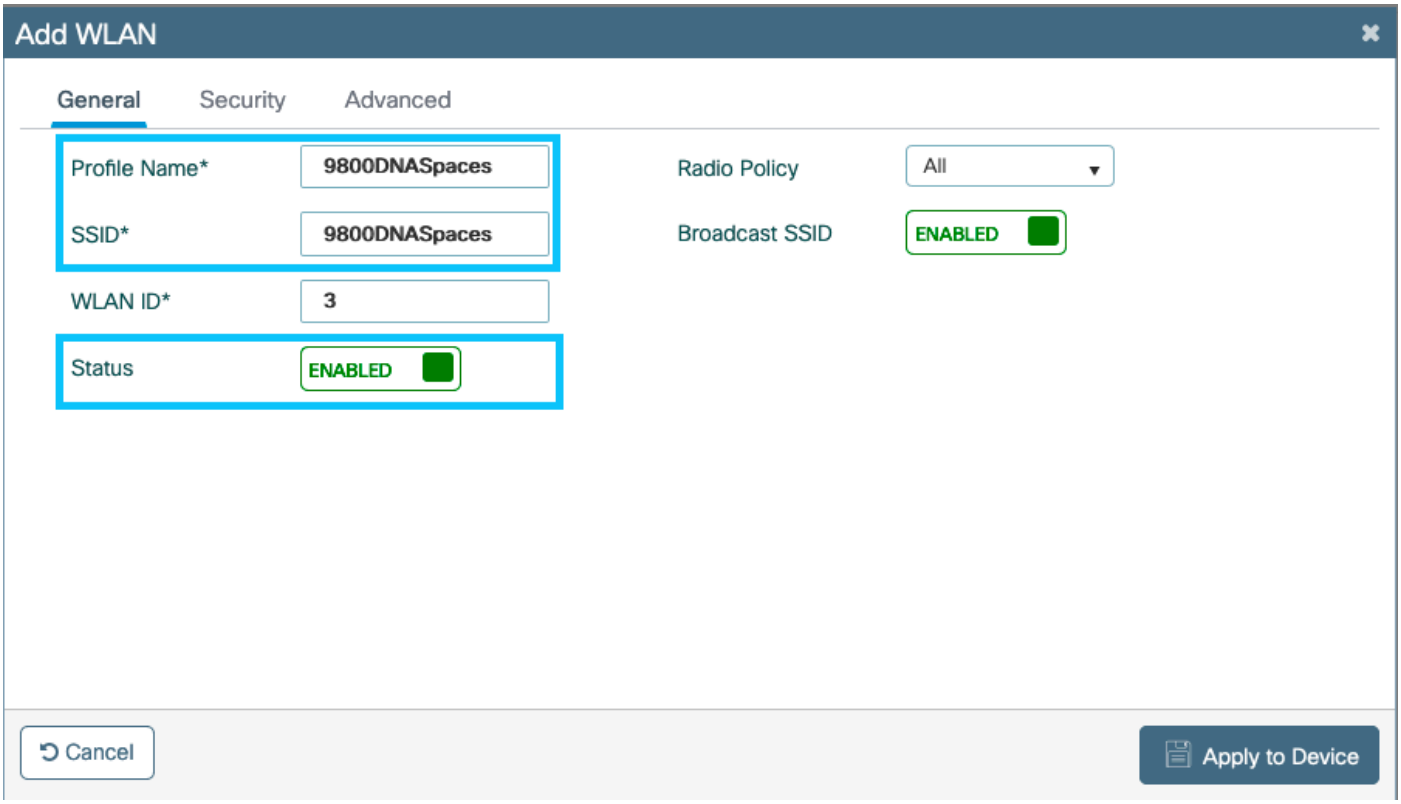
```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type consent
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
Andressi-9800L(config-params-parameter-map)#redirect append ap-mac tag ap_mac
Andressi-9800L(config-params-parameter-map)#redirect append wlan-ssid tag wlan
Andressi-9800L(config-params-parameter-map)#redirect append client-mac tag client_mac
Andressi-9800L(config-params-parameter-map)#redirect portal ipv4
```

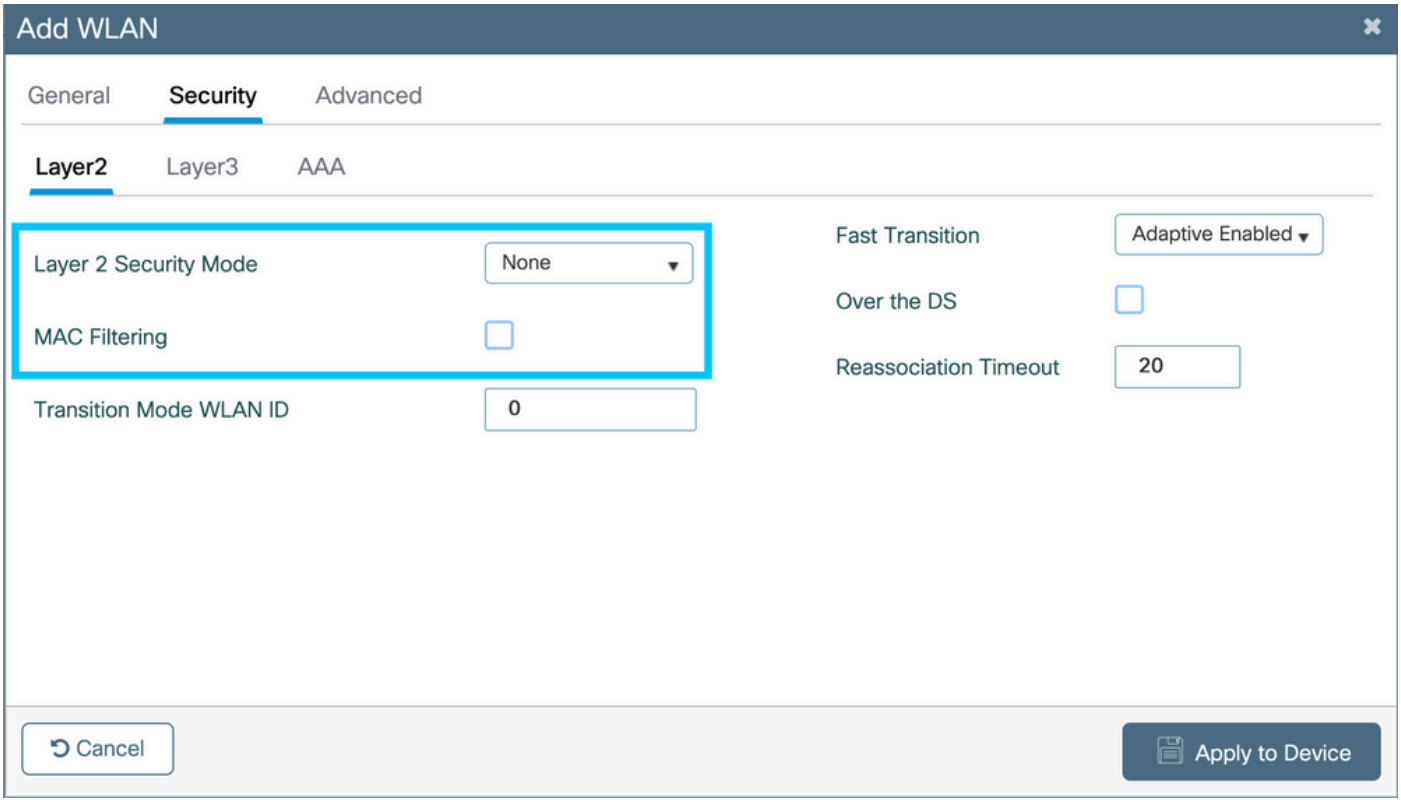
```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

9800コントローラでSSIDを作成します

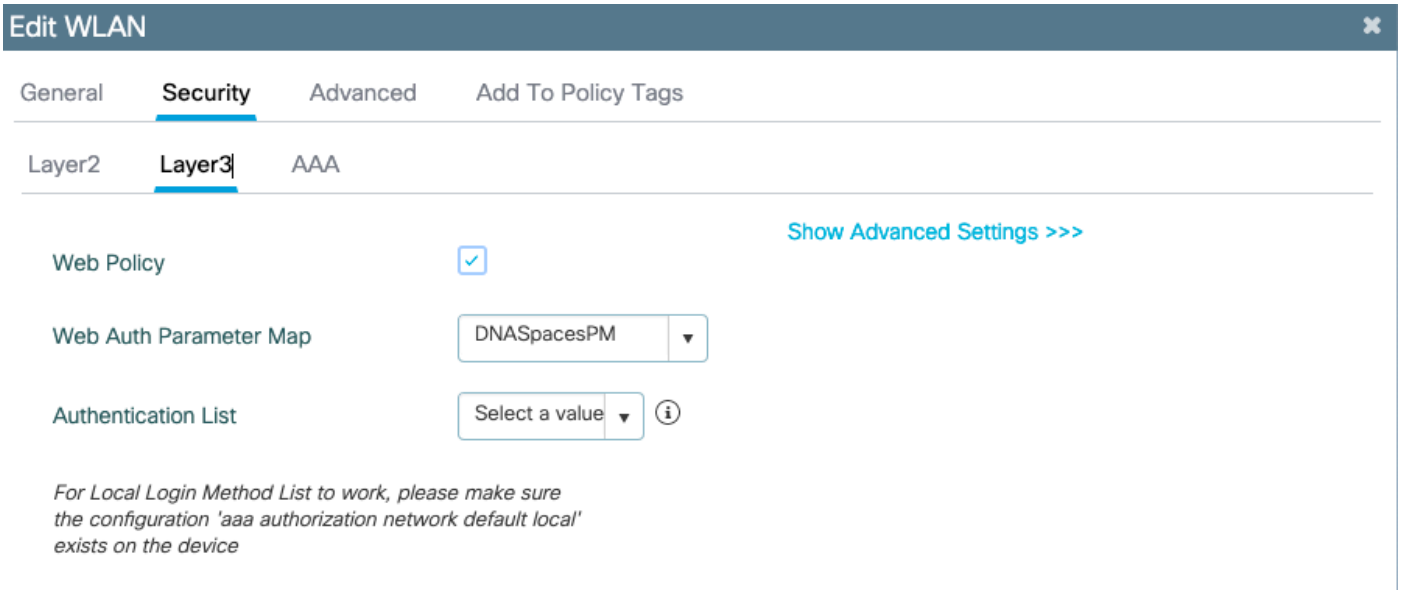
ステップ 1：[Configuration] > [Tags & Profiles] > [WLANs] に移動し、[+Add] をクリックします。プロファイル名とSSIDを設定し、WLANを有効にします。SSID名が、「**DNAスペースでのSSIDの作成**」セクションのステップ3で設定した名前と同じであることを確認します。



ステップ 2：[Security] > [Layer2] に移動します。**[Layer 2 Security Mode]を[None]** に設定し、[MAC Filtering]が無効になっていることを確認します。

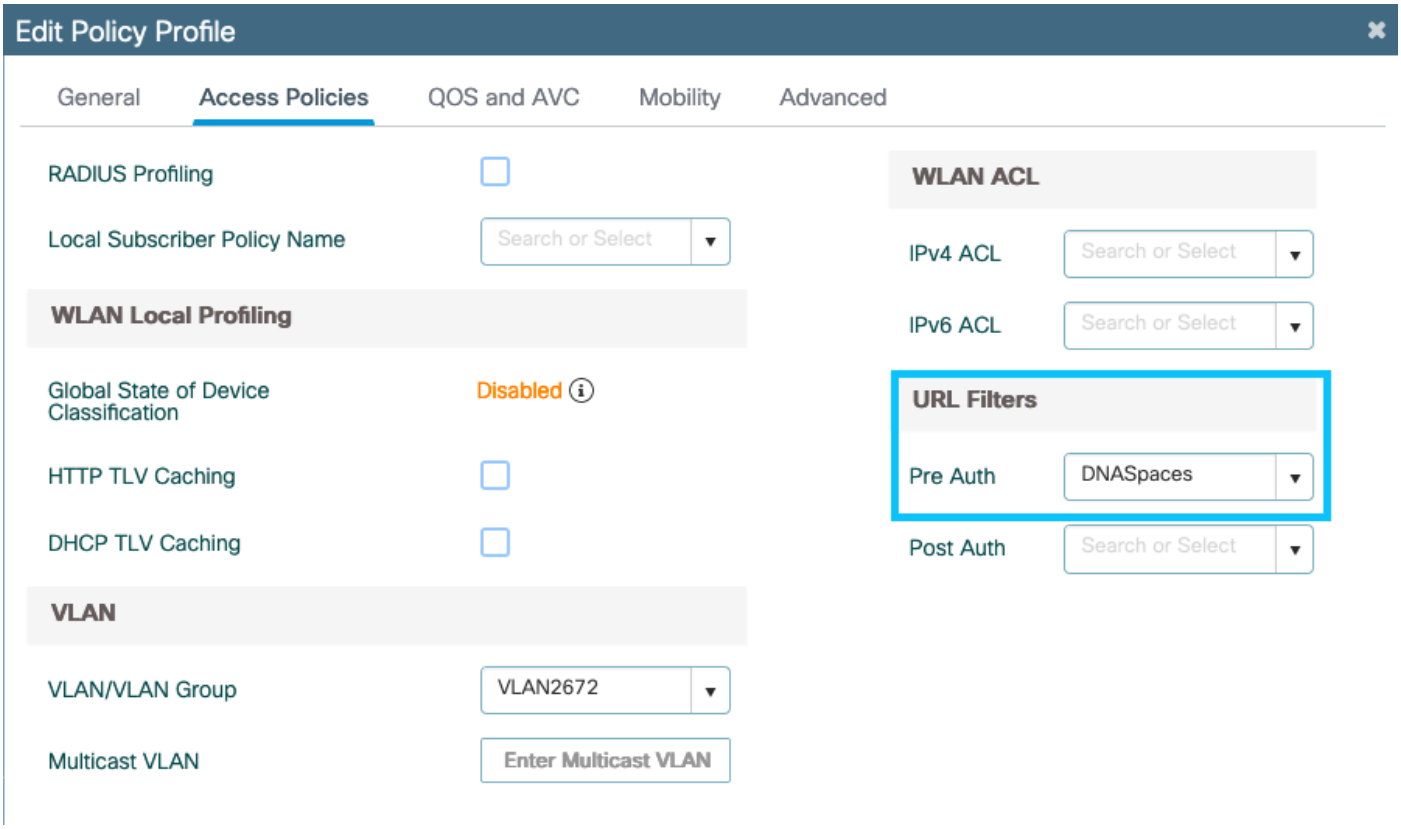


ステップ 3：[Security] > [Layer3] に移動します。Webポリシーを有効にし、Web認証パラメータマップを設定します。[Apply to Device] をクリックします。



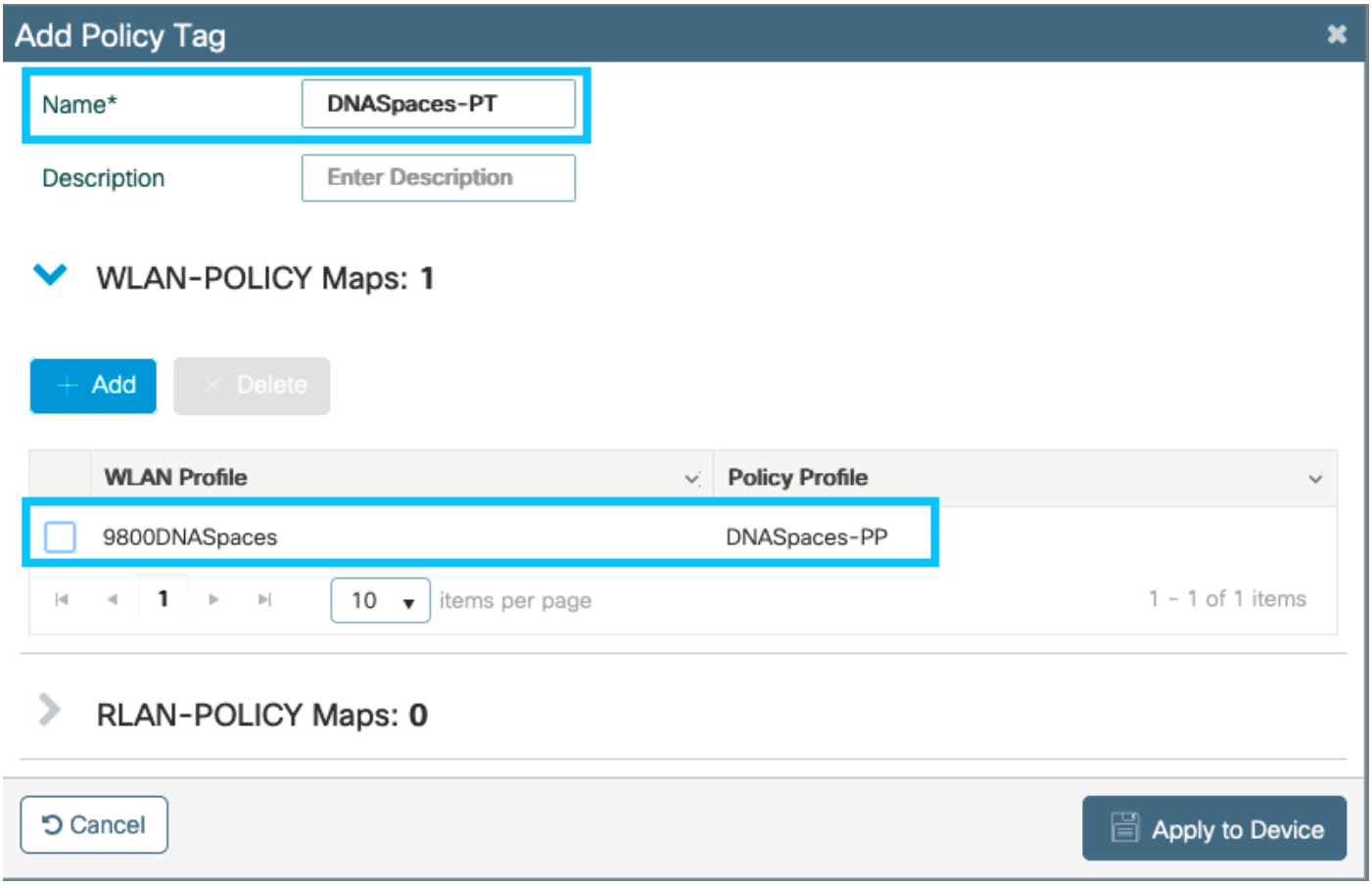
9800コントローラでのポリシープロファイルの設定

ステップ 1：[Configuration] > [Tags & Profiles] > [Policy] に移動し、新しいポリシープロファイルを作成するか、デフォルトのポリシープロファイルを使用します。[access Policies]タブで、クライアントVLANを設定し、URLフィルタを追加します。

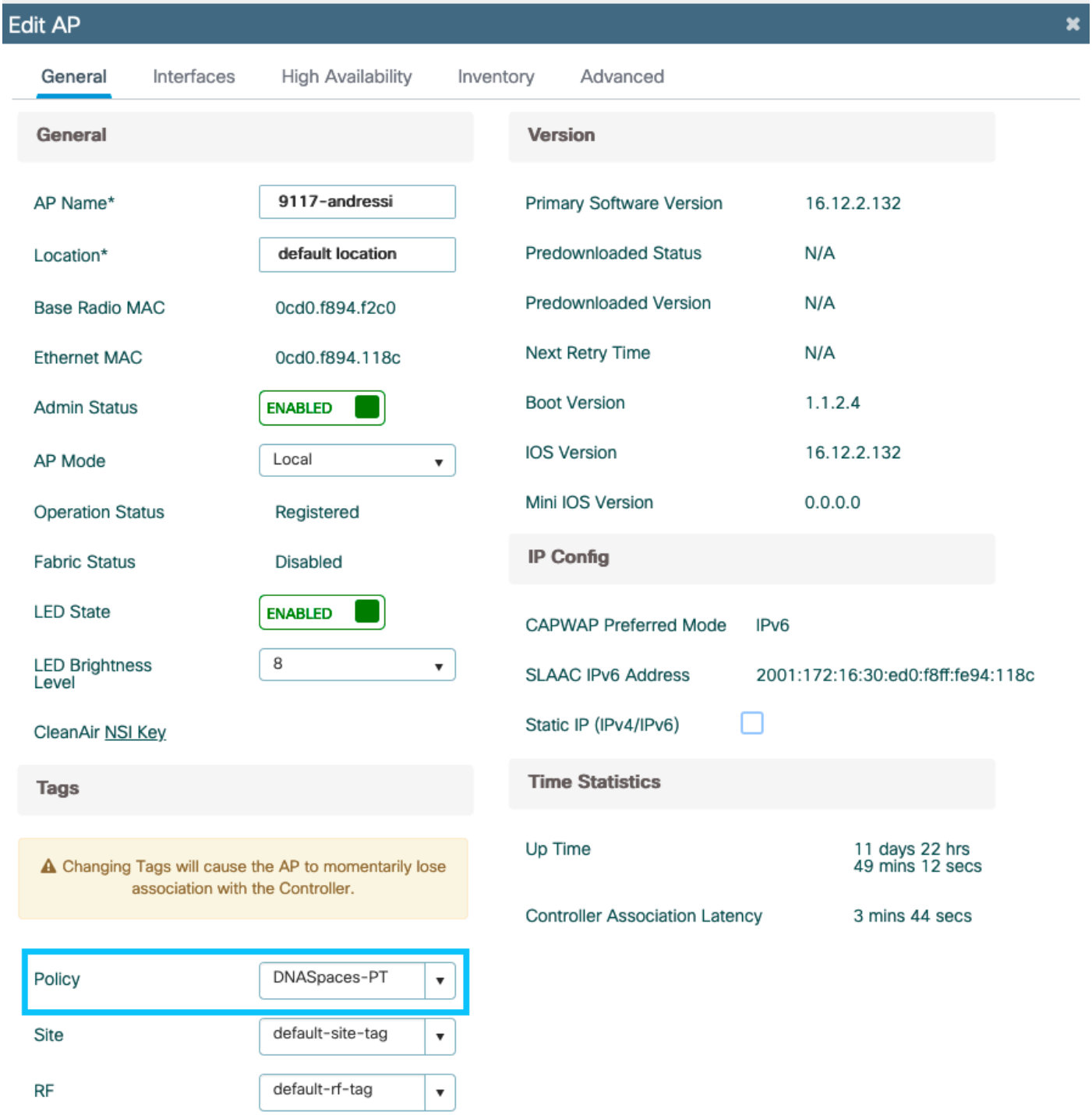


9800コントローラでのポリシータグの設定

ステップ 1：[Configuration] > [Tags & Profiles] > [Policy] に移動します。新しいポリシータグを作成するか、デフォルトのポリシータグを使用します。WLANをポリシータグのポリシープロファイルにマッピングします。



ステップ 2：SSIDをブロードキャストするためにAPにポリシータグを適用します。[Configuration] > [Wireless] > [Access Points] に移動し、対象のAPを選択してポリシータグを追加します。これにより、APはCAPWAPトンネルを再起動し、9800コントローラに戻ります。



CLI による設定：

```
Andressi-9800L(config)#wlan
```

```
Andressi-9800L(config-wlan)#no security wpa
Andressi-9800L(config-wlan)#no security wpa akm dot1x
Andressi-9800L(config-wlan)#no security wpa wpa2 ciphers aes
Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown

Andressi-9800L(config)#wireless profile policy
```

```
Andressi-9800L(config-wireless-policy)#vlan <id>
Andressi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter
```

```
Andressi-9800L(config-wireless-policy)#no shutdown
```

```
Andressi-9800L(config)#wireless tag policy
```

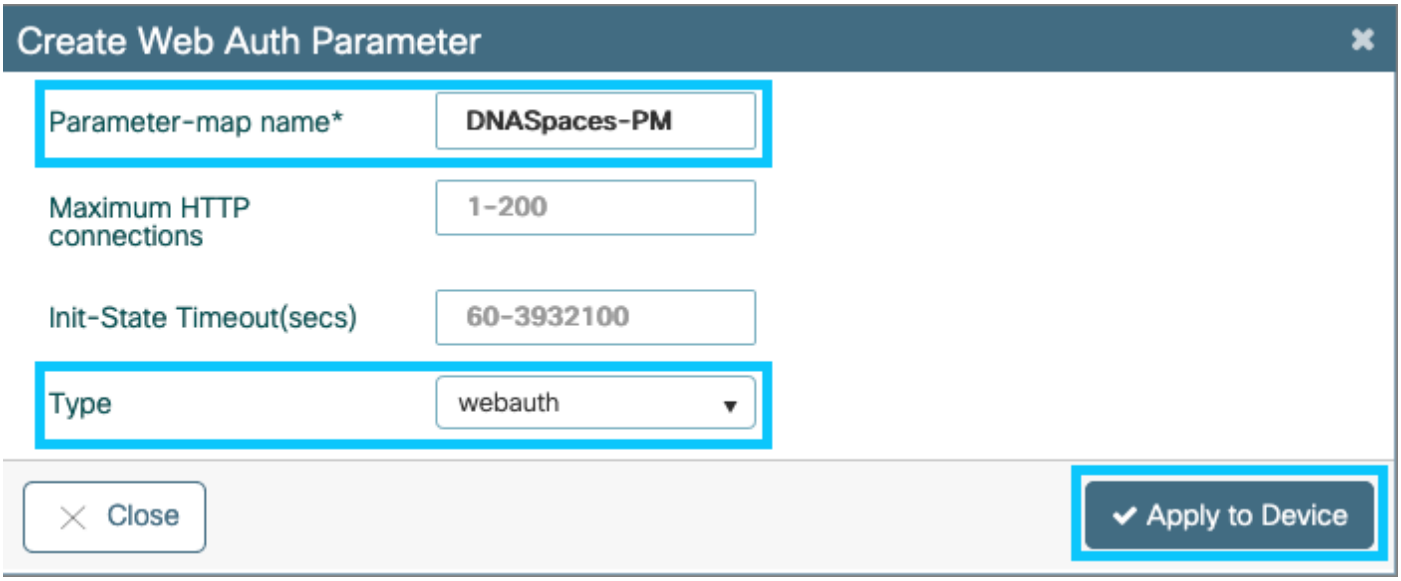
```
Andressi-9800L(config-policy-tag)#wlan
```

DNAスペース上のRADIUSサーバを使用したキャプティブポータル

注:DNAスペースRADIUSサーバは、コントローラからのPAP認証のみをサポートします。

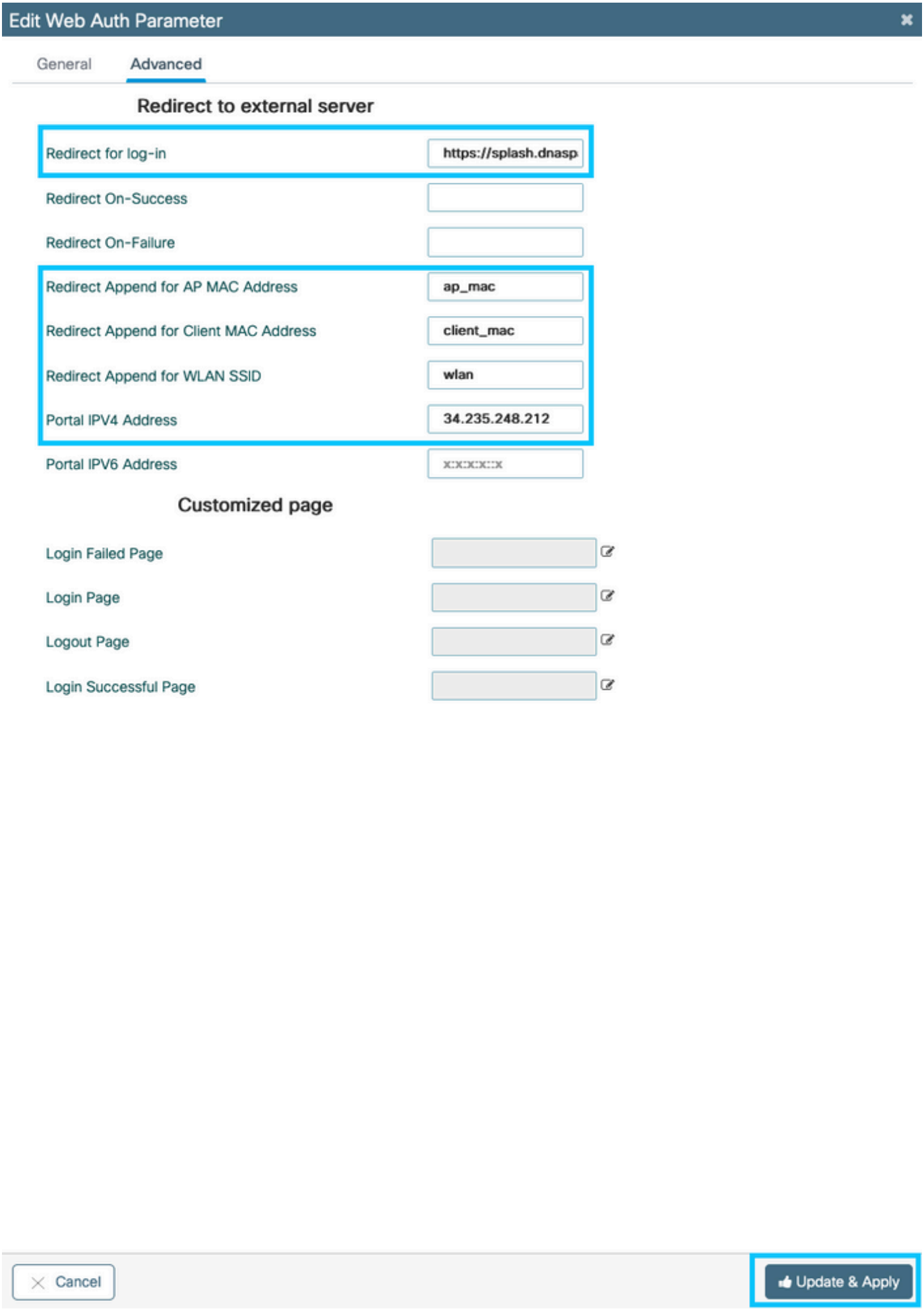
9800コントローラでのWeb認証パラメータマップの設定

ステップ 1：Web認証パラメータマップを作成します。[Configuration] > [Security] > [Web Auth] に移動し、[+Add] をクリックしてパラメータマップ名を設定し、タイプとして[webauth] を選択します。



ステップ 2：ステップ1で設定したパラメータマップをクリックし、[Advanced] をクリックして

、ログインのリダイレクト、AP MACアドレスの追加、クライアントMACアドレスの追加、WLAN SSIDとポータルIPv4アドレスの追加を入力します。[Update & Apply] をクリックします。


Edit Web Auth Parameter
General
Advanced
Redirect to external server
Redirect for log-in
https://splash.dnasp
Redirect On-Success
Redirect On-Failure
Redirect Append for AP MAC Address
ap_mac
Redirect Append for Client MAC Address
client_mac
Redirect Append for WLAN SSID
wlan
Portal IPV4 Address
34.235.248.212
Portal IPV6 Address
X:X:X:X::X
Customized page
Login Failed Page
Login Page
Logout Page
Login Successful Page
Cancel
Update & Apply

注：スプラッシュページのURLとIPv4リダイレクトアドレスを取得するには、「**WLC直接接続でのSSIDの作成**」セクションの「**アクセスコントロールリストの作成**」セクションの「**DNAスペースでのSSIDの作成**」セクションのステップ3で作成したSSIDから、「**手動で設定**」オプションをクリックします。

注：Cisco DNA Spacesポータルは2つのIPアドレスに解決できますが、9800コントローラでは1つのIPアドレスしか設定できません。1つのケースでは、これらのIPアドレスのいずれかを選択して、ポータルのIPv4アドレスとしてパラメータマップに設定します。

注： 仮想IPv4アドレスとIPv6アドレスの両方がグローバルWeb認証パラメータマップで設定されていることを確認します。仮想IPv6が設定されていない場合、クライアントは設定されているDNAスペースポータルではなく内部ポータルにリダイレクトされることがあります。このため、仮想IPは常に設定する必要があります。「192.0.2.1」は仮想IPv4として、FE80:0:0:0:903A::11E4は仮想IPV6として設定できます。それ以外のIPを使用する理由はほとんどまたはまったくありません。

CLI による設定：

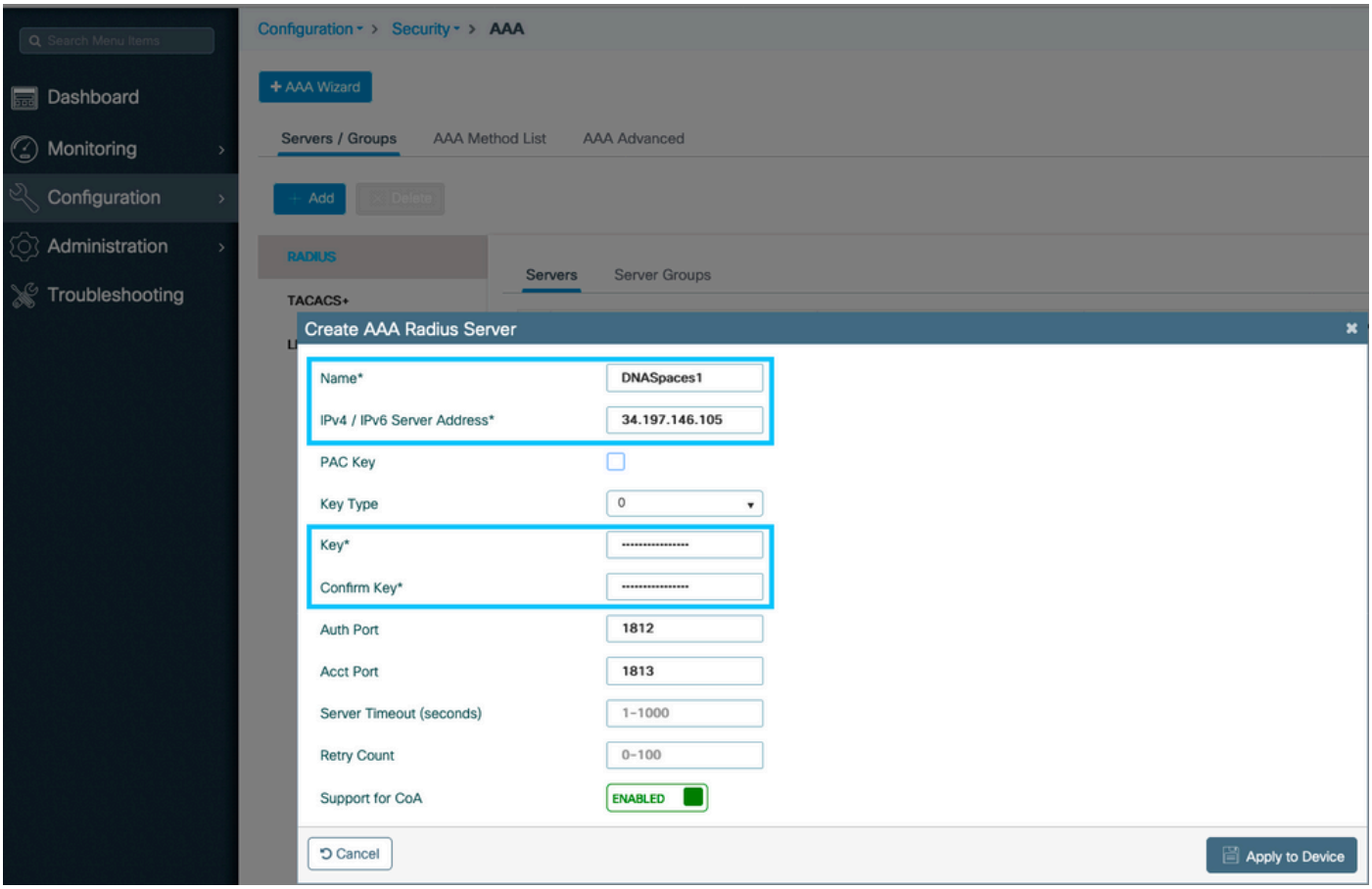
```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type webauth
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
Andressi-9800L(config-params-parameter-map)#redirect append ap-mac tag ap_mac
Andressi-9800L(config-params-parameter-map)#redirect append wlan-ssid tag wlan
Andressi-9800L(config-params-parameter-map)#redirect append client-mac tag client_mac
Andressi-9800L(config-params-parameter-map)#redirect portal ipv4
```

```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

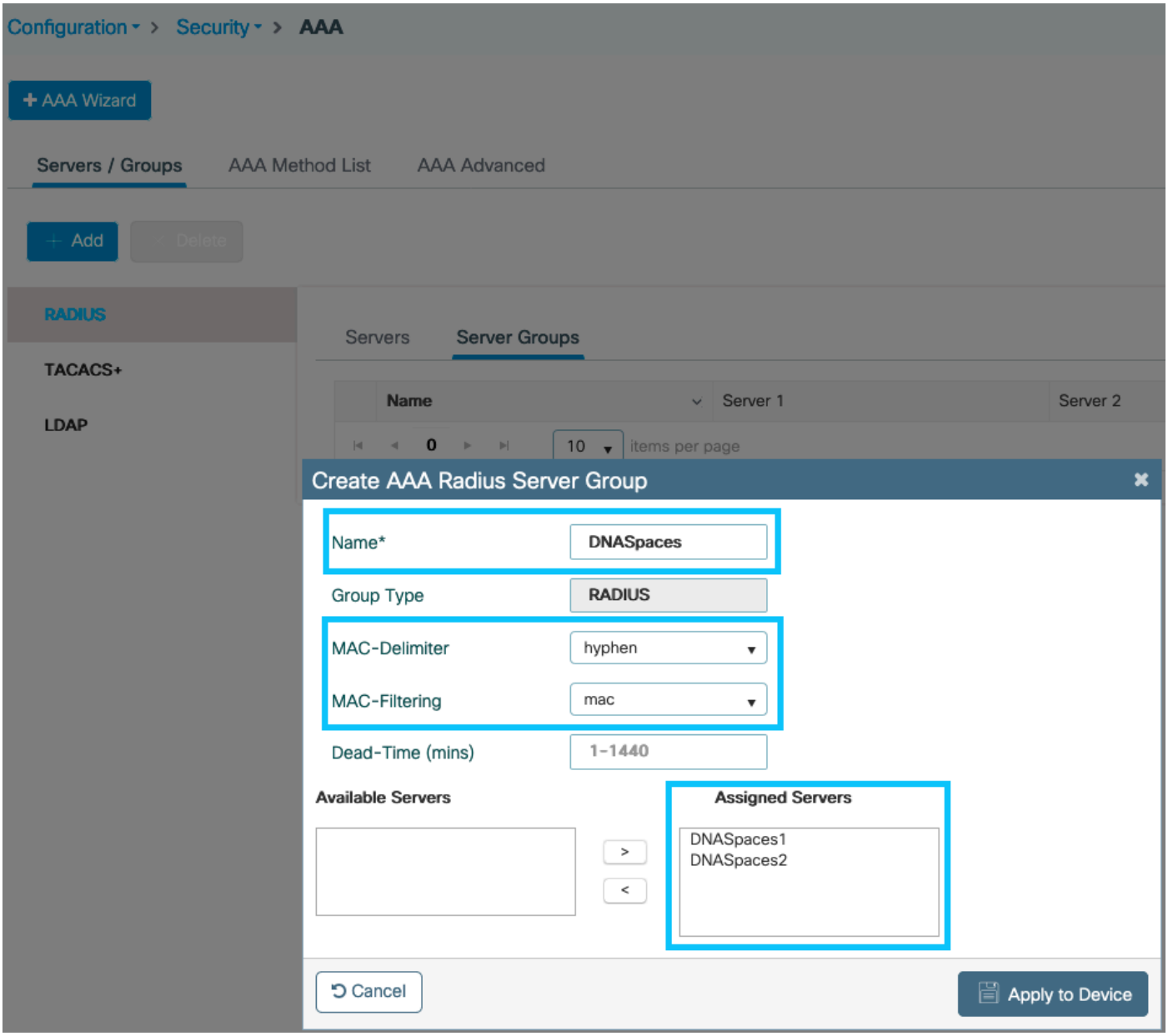
9800コントローラでのRADIUSサーバの設定

ステップ 1：RADIUSサーバを設定します。Cisco DNA Spacesは、ユーザ認証のためにRADIUSサーバとして機能し、2つのIPアドレスで応答できます。[Configuration] > [Security] > [AAA] に移動し、[Add] をクリックして両方のRADIUSサーバを設定します。

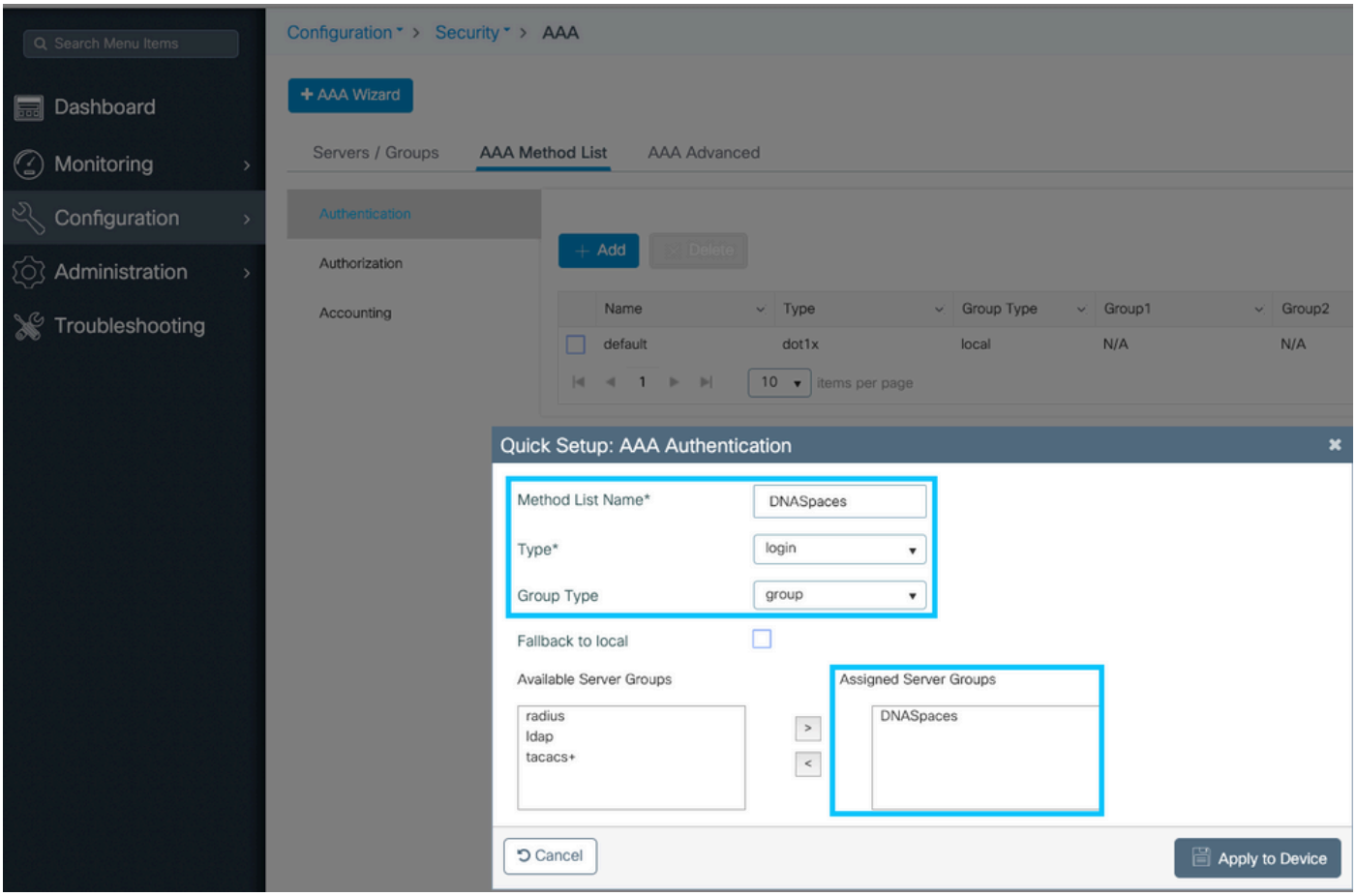


注：プライマリサーバとセカンダリサーバの両方のRADIUS IPアドレスと秘密キーを取得するには、「**DNAスペースでのSSIDの作成**」セクションのステップ3で作成したSSIDから [Configure Manually] オプションをクリックし、[RADIUS Server Configuration] セクションに移動します。

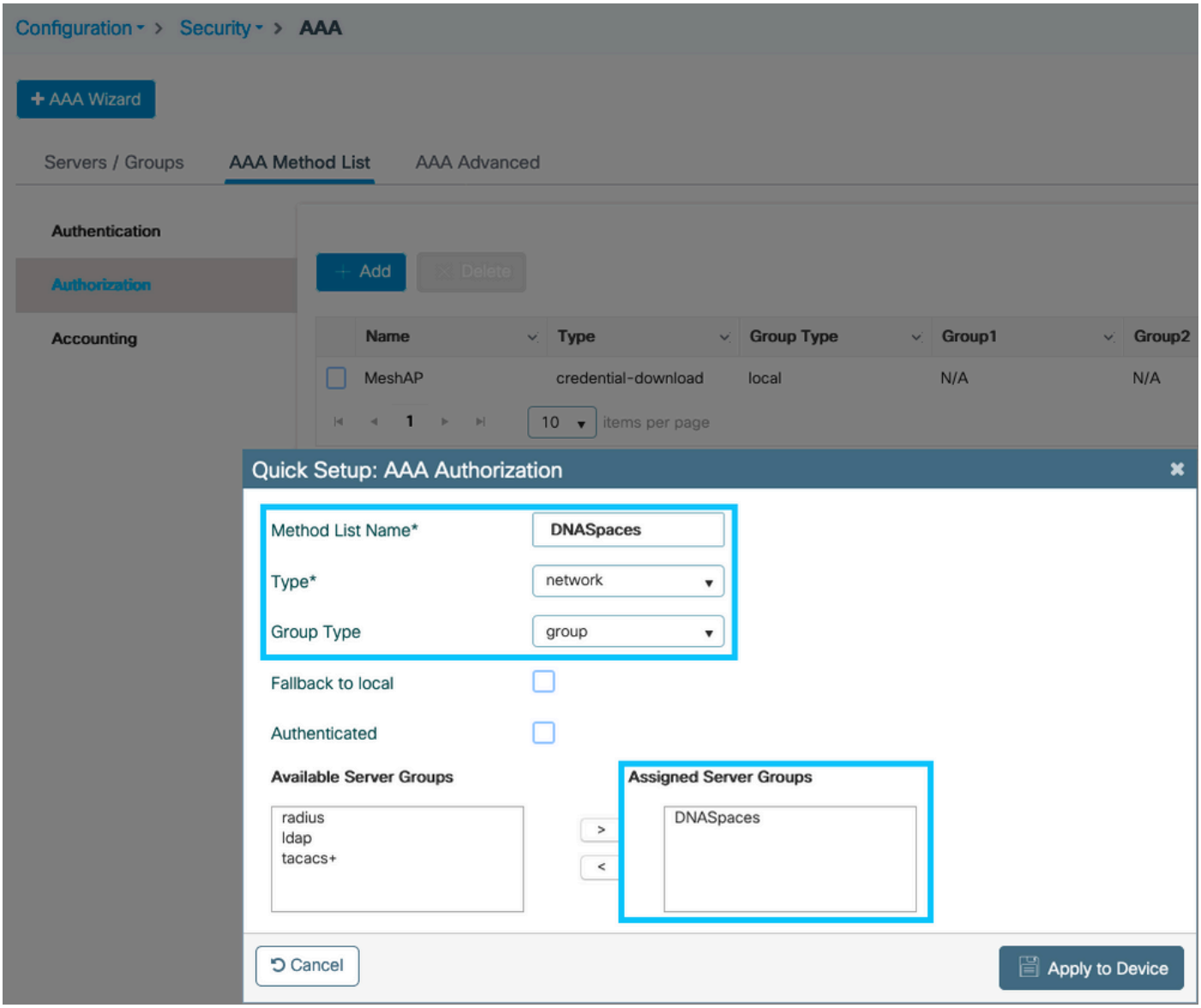
ステップ 2：RADIUSサーバグループを設定し、両方のRADIUSサーバを追加します。[Configuration] > [Security] > [AAA] > [Servers / Groups] > [RADIUS] > [Server Groups] に移動し、[+add] をクリックして、サーバグループ名、MAC-DelimiterをHyphen、MAC-FilteringをMACとして設定し、2つのRADIUSサーバを割り当てます。



ステップ 3：[Authentication Method]リストを設定します。[Configuration] > [Security] > [AAA] > [AAA Method List] > [Authentication] に移動し、[+add] をクリックします。方式リスト名を設定し、タイプとして**login**を選択し、サーバグループを割り当てます。

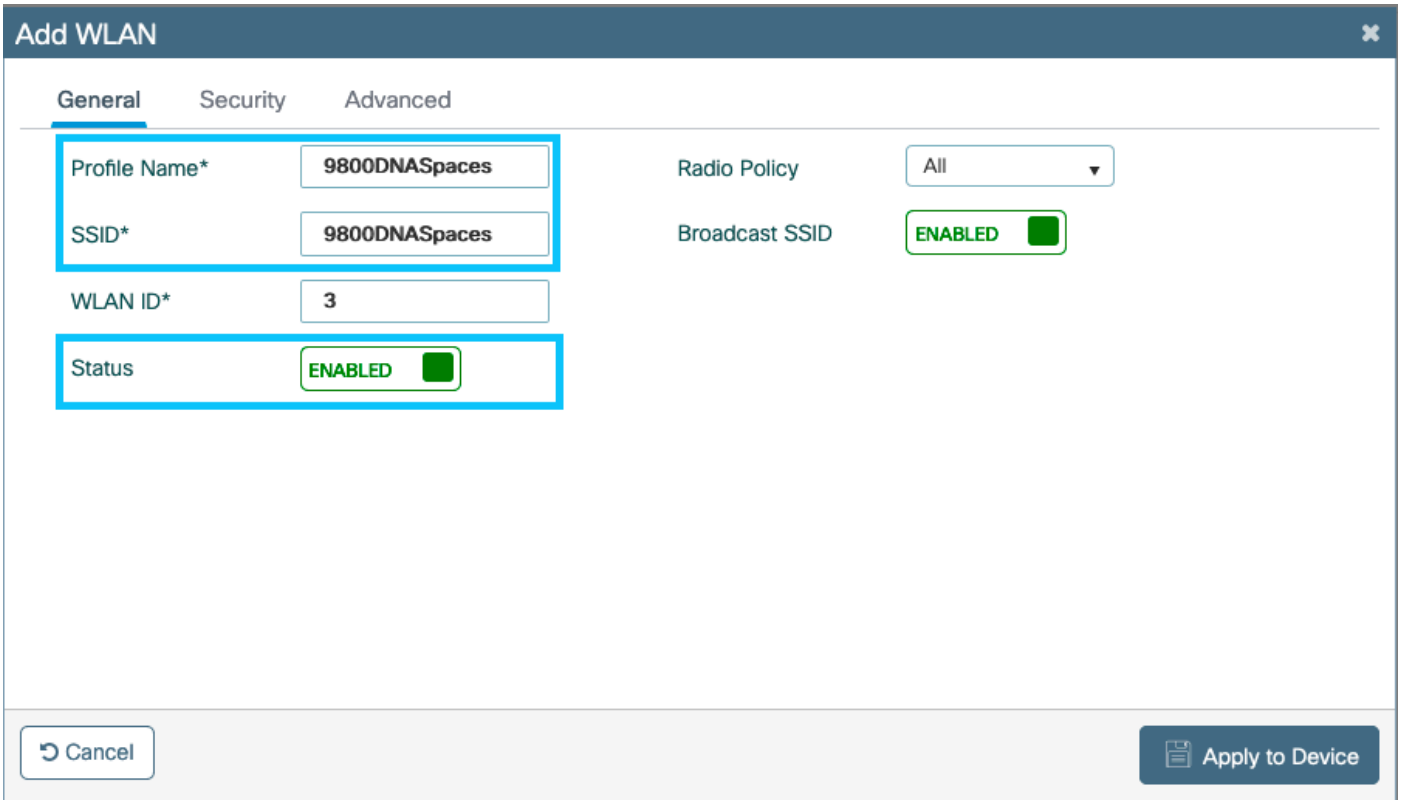


ステップ 4：[Authorization Method]リストを設定します。[Configuration] > [Security] > [AAA] > [AAA Method List] > [Authorization] に移動し、[+add] をクリックします。方式リスト名を設定し、タイプとして**network**を選択し、サーバグループを割り当てます。

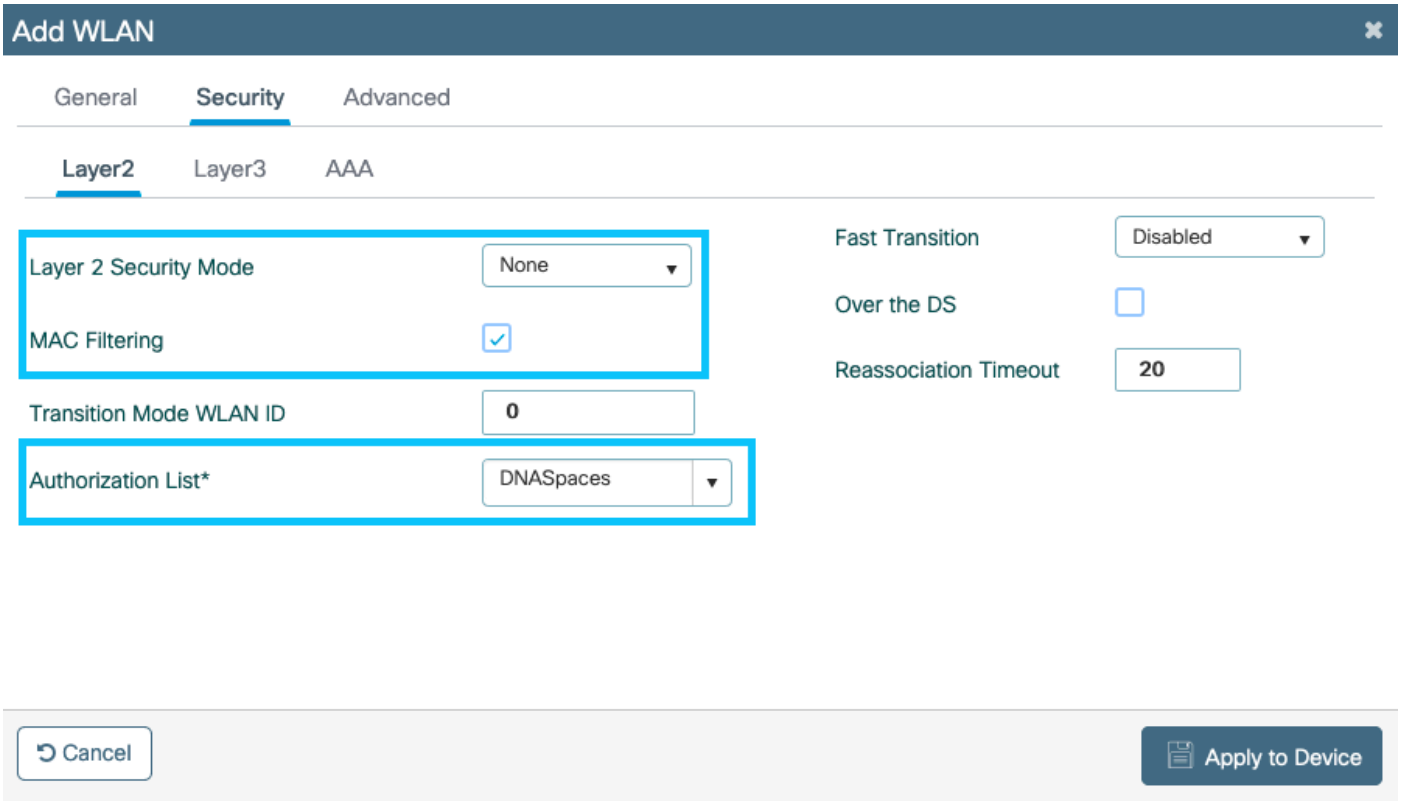


9800コントローラでSSIDを作成します

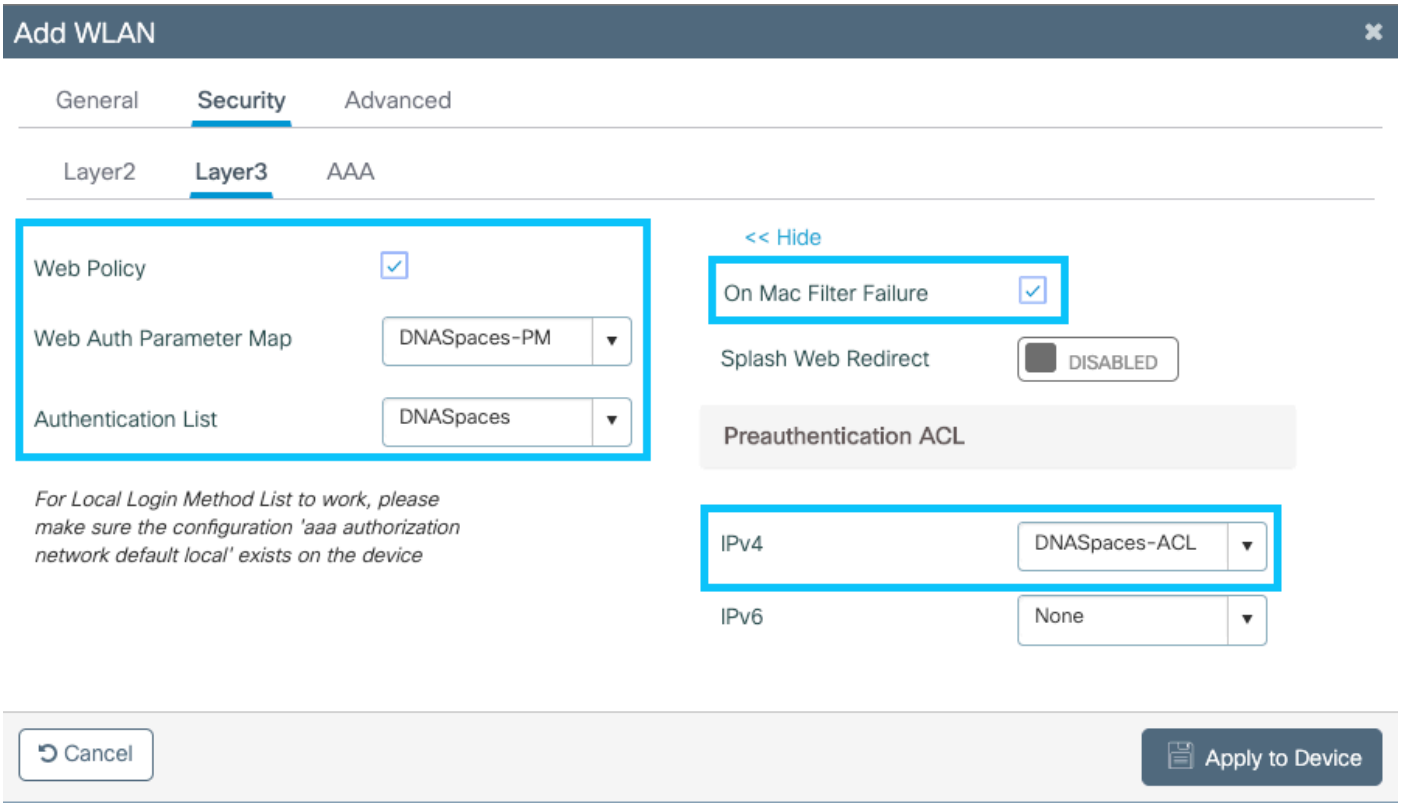
ステップ 1：[Configuration] > [Tags & Profiles] > [WLANs] に移動し、[+Add] をクリックします。プロファイル名とSSIDを設定し、WLANを有効にします。SSID名が、「**DNAスペースでのSSIDの作成**」セクションのステップ3で設定した名前と同じであることを確認します。



ステップ 2：[Security] > [Layer2] に移動します。**[Layer 2 Security Mode]を[None]** に設定し、MACフィルタリングを有効にして、許可リストを追加します。

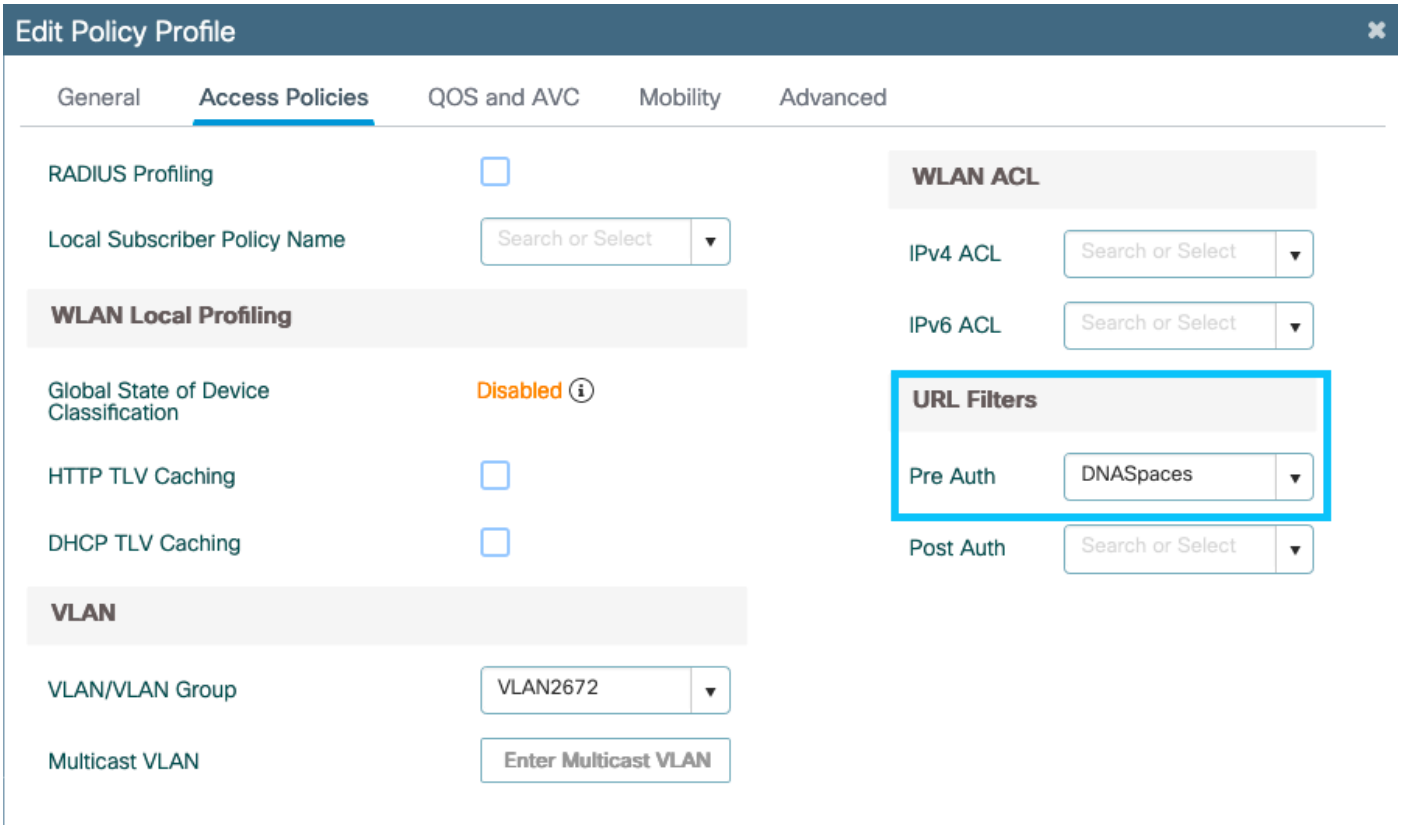


ステップ 3：[Security] > [Layer3] に移動します。Webポリシーを有効にし、Web認証パラメータマップと認証リストを設定します。On Mac Filter Failureを有効にし、事前認証ACLを追加します。[Apply to Device] をクリックします。

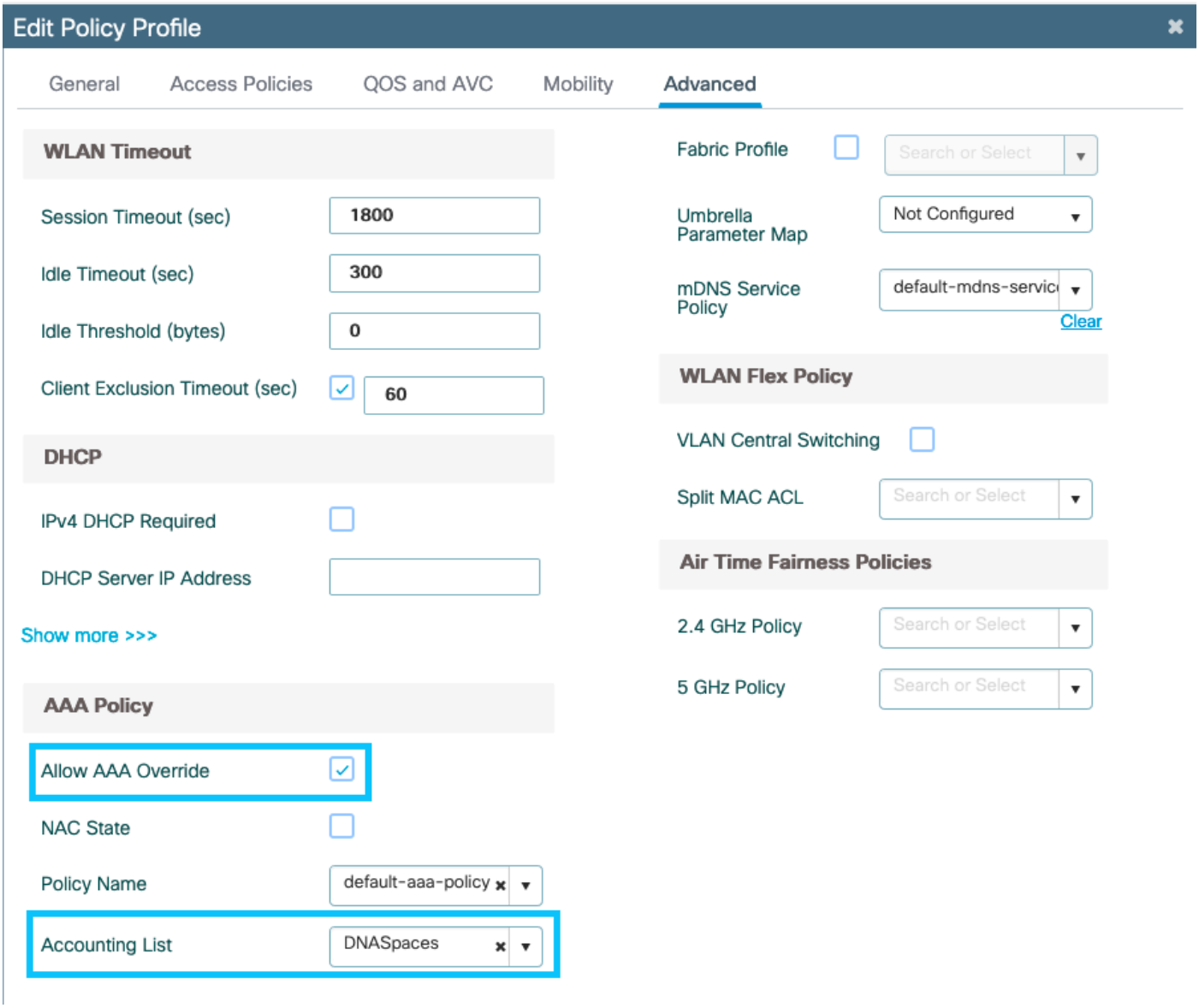


9800コントローラでのポリシープロファイルの設定

ステップ 1：[Configuration] > [Tags & Profiles] > [Policy] に移動し、新しいポリシープロファイルを作成するか、デフォルトのポリシープロファイルを使用します。[access Policies]タブで、クライアントVLANを設定し、URLフィルタを追加します。

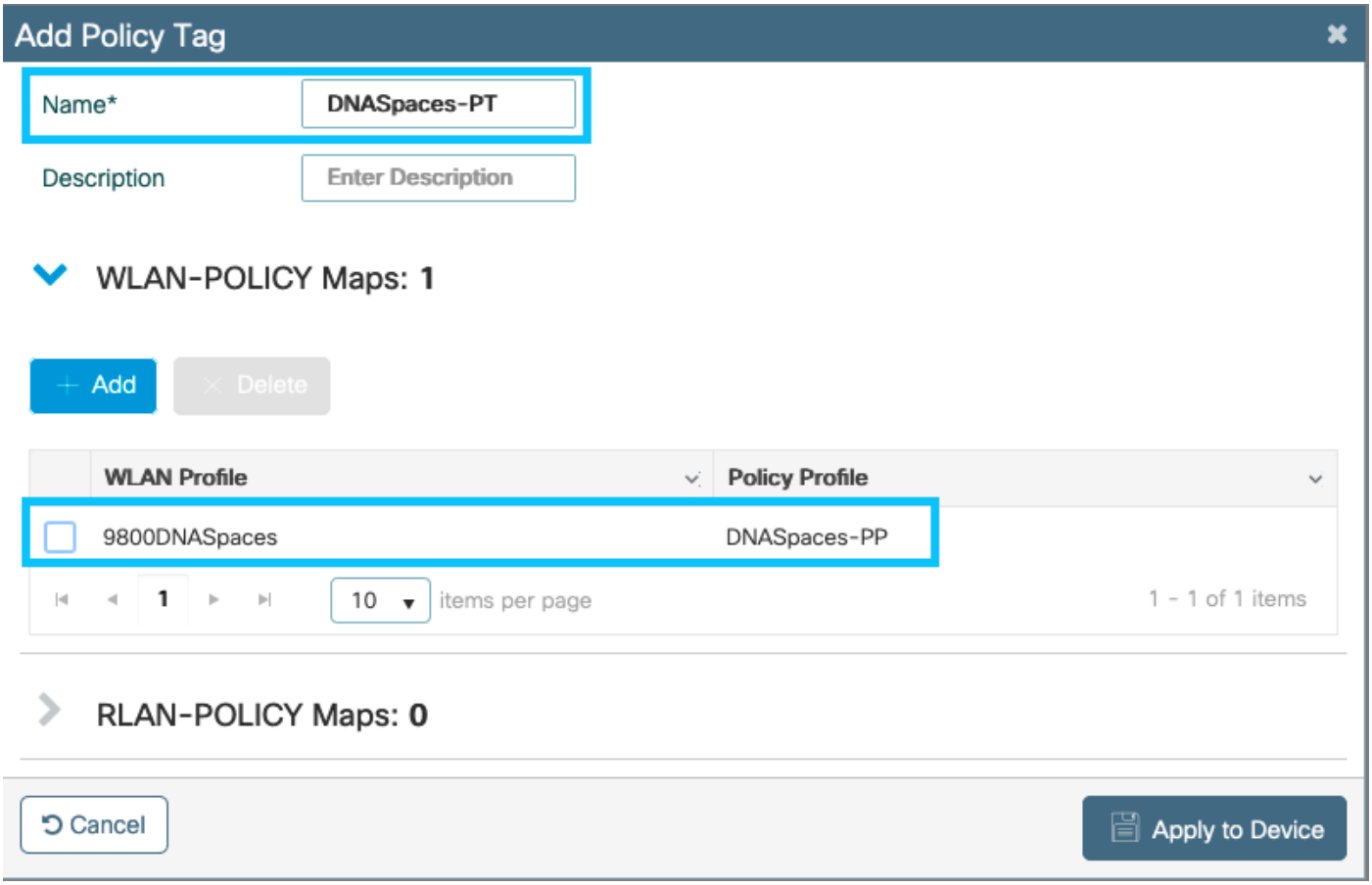


ステップ 2：[Advanced]タブで、[AAA Override]を有効にし、オプションでアカウンティング方式リストを設定します。

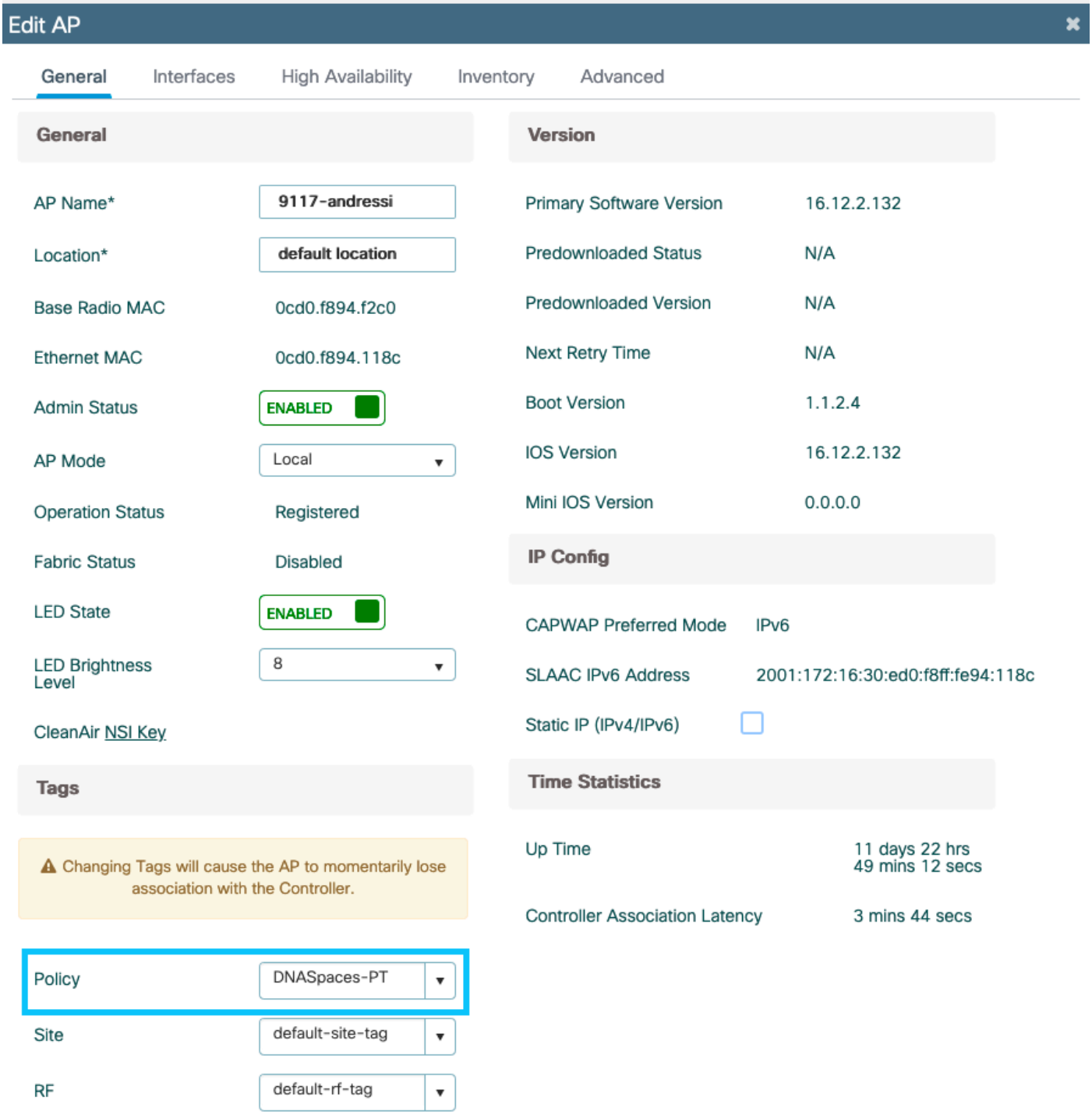


9800コントローラでのポリシータグの設定

ステップ 1：[Configuration] > [Tags & Profiles] > [Policy] に移動します。新しいポリシータグを作成するか、デフォルトのポリシータグを使用します。WLANをポリシータグのポリシープロファイルにマッピングします。



ステップ 2：SSIDをブロードキャストするためにAPにポリシータグを適用します。[Configuration] > [Wireless] > [Access Points] に移動し、対象のAPを選択してポリシータグを追加します。これにより、APはCAPWAPトンネルを再起動し、9800コントローラに戻ります。



CLI による設定：

```
Andressi-9800L(config)#wlan
```

```
Andressi-9800L(config-wlan)#ip access-group web
```

```
Andressi-9800L(config-wlan)#no security wpa
Andressi-9800L(config-wlan)#no security wpa akm dot1x
```

```
Andressi-9800L(config-wlan)#no security wpa wpa2 ciphers aes
Andressi-9800L(config-wlan)#mac-filtering




Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth authentication-list




Andressi-9800L(config-wlan)#security web-auth on-macfilter-failure
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown

Andressi-9800L(config)#wireless profile policy




Andressi-9800L(config-wireless-policy)#aaa-override
Andressi-9800L(config-wireless-policy)#accounting-list




Andressi-9800L(config-wireless-policy)#vlan <id>
Andressi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter




Andressi-9800L(config-wireless-policy)#no shutdown

Andressi-9800L(config)#wireless tag policy




Andressi-9800L(config-policy-tag)#wlan
```

グローバルパラメータマップの設定

推奨されない手順：次のコマンドを実行してHTTPSリダイレクションを許可します。ただし、クライアントのオペレーティングシステムでキャプティブポータルの検出が行われ、CPU使用率が高くなり、常に証明書の警告がスローされる場合、クライアントのHTTPSトラフィックでのリダイレクションは必要ありません。そのため、特定の使用例で必要な場合を除き、この設定は避けることをお勧めします。

```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#intercept-https-enable
```

> **注**:Cisco Catalyst 9800シリーズワイヤレスコントローラにインストールされた仮想IP用の有効なSSL証明書が必要です。

ステップ 1：拡張子が.p12の署名付き証明書ファイルをTFTPサーバにコピーし、次のコマンドを実行して、証明書を9800コントローラに転送してインストールします。

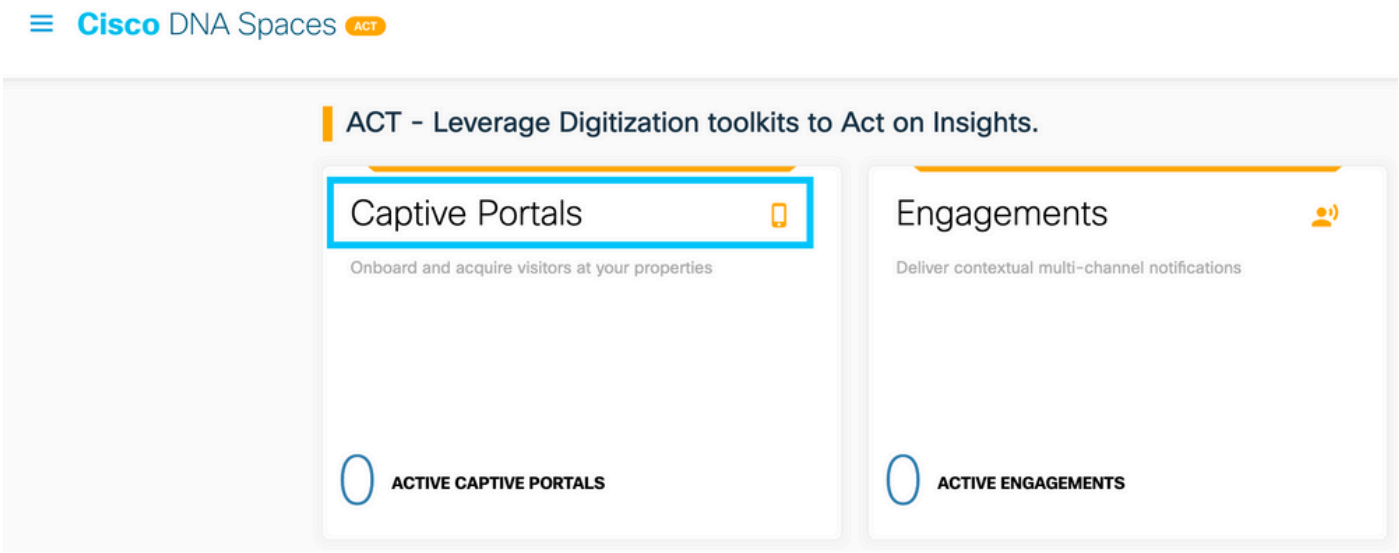
```
Andressi-9800L(config)#crypto pki import
```

ステップ 2：インストールされた証明書をWeb認証パラメータマップにマップするには、次のコマンドを実行します。

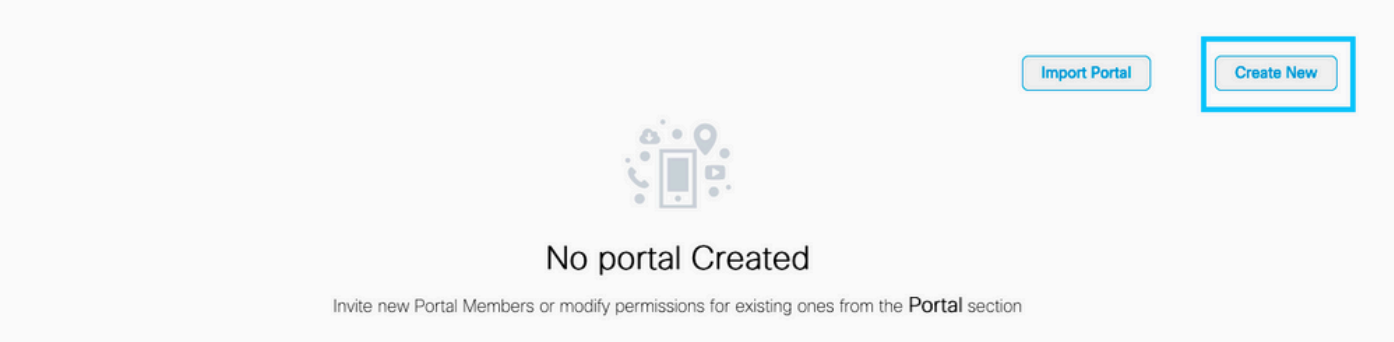
```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#trustpoint
```

DNAスペースにポータルを作成する

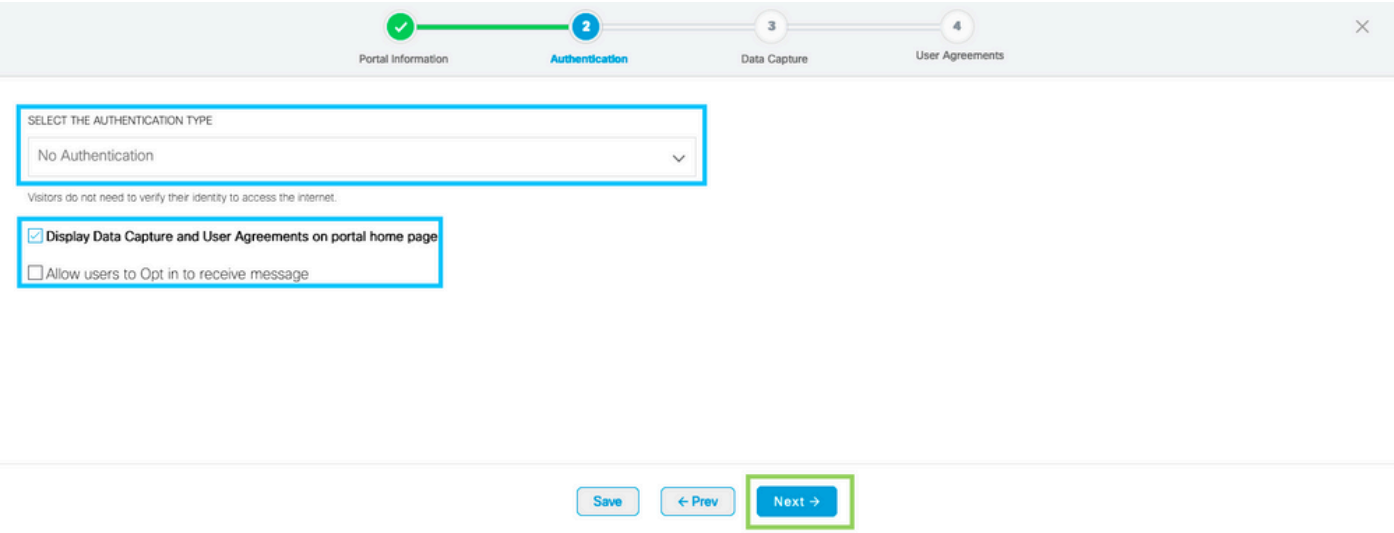
ステップ 1：DNA Spacesのダッシュボードで[Captive Portals] をクリックします。



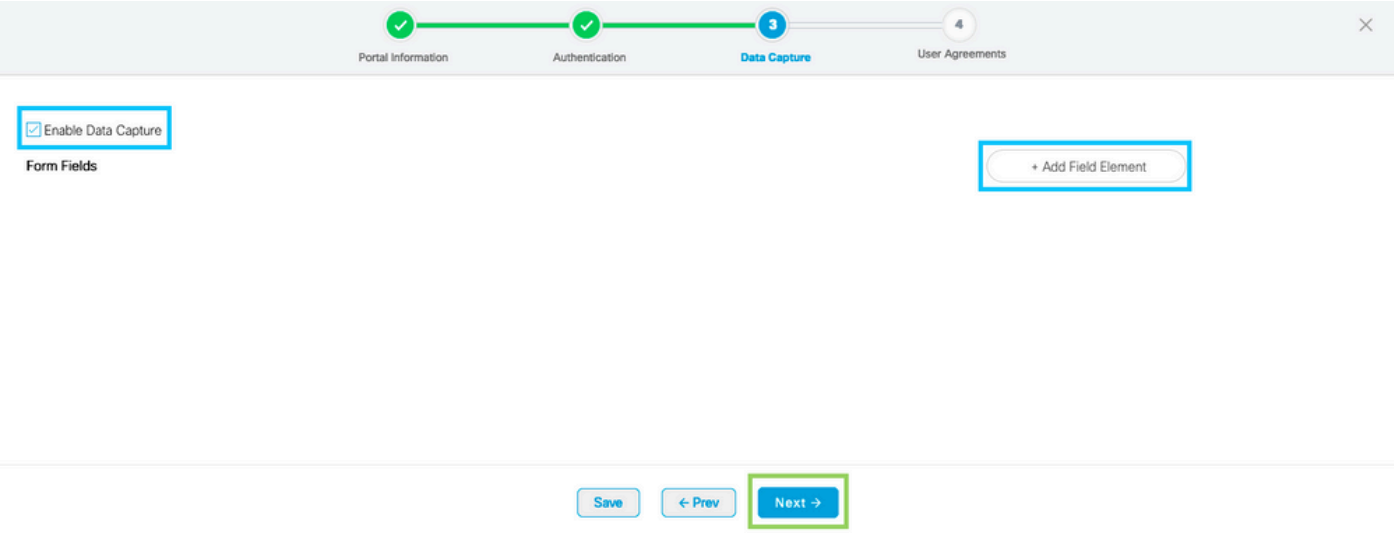
ステップ 2：[Create New] をクリックし、ポータル名を入力して、ポータルを使用できる場所を選択します。



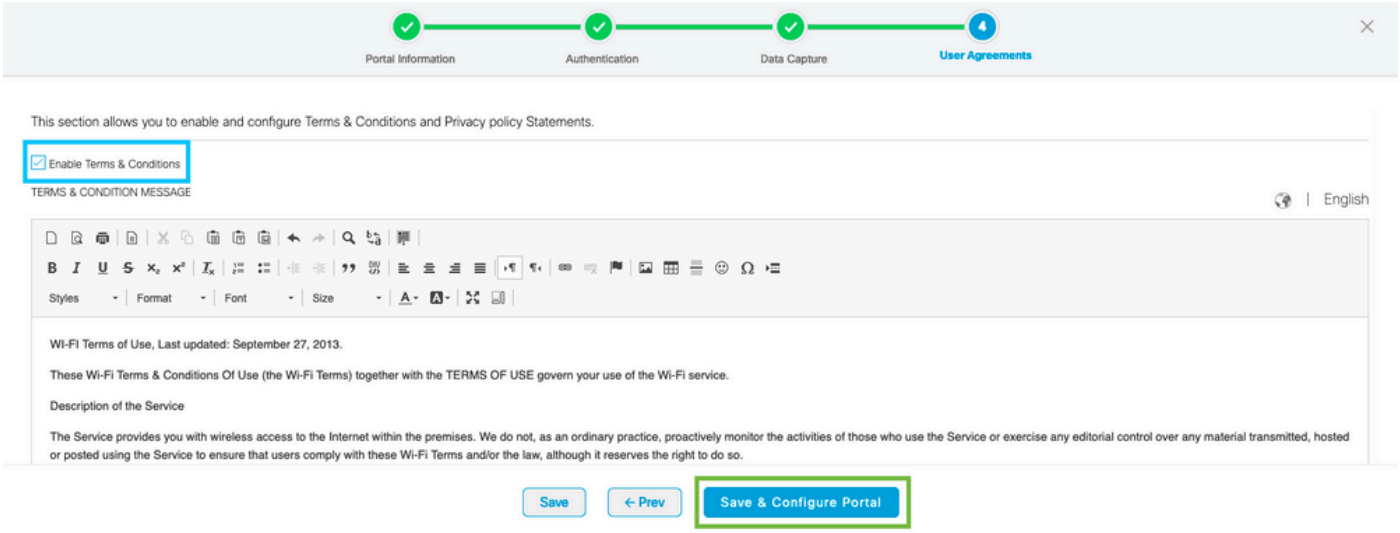
ステップ 3：認証タイプを選択し、ポータルホームページにデータの取り込みとユーザ契約を表示するかどうか、およびユーザがメッセージを受信することを許可するかどうかを選択します。[Next] をクリックします。



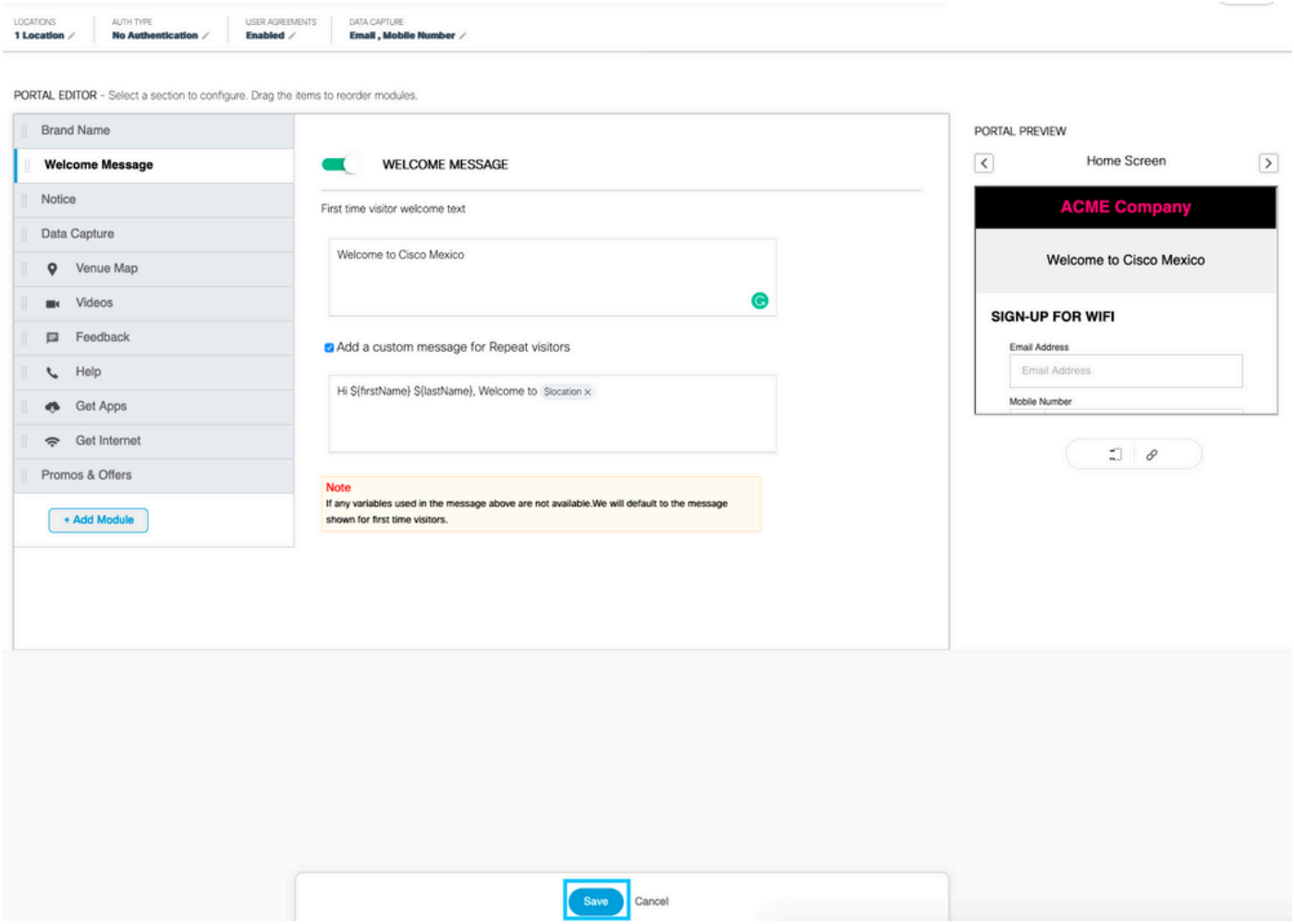
ステップ 4：データキャプチャ要素を構成します。ユーザからデータをキャプチャする場合は、[Enable Data Capture] ボックスをオンにし、[Add Field Element] をクリックして目的のフィールドを追加します。[Next] をクリックします。



ステップ 5：[Enable Terms & Conditions] にチェックマークを入れ、[Save & Configure Portal] をクリックします。

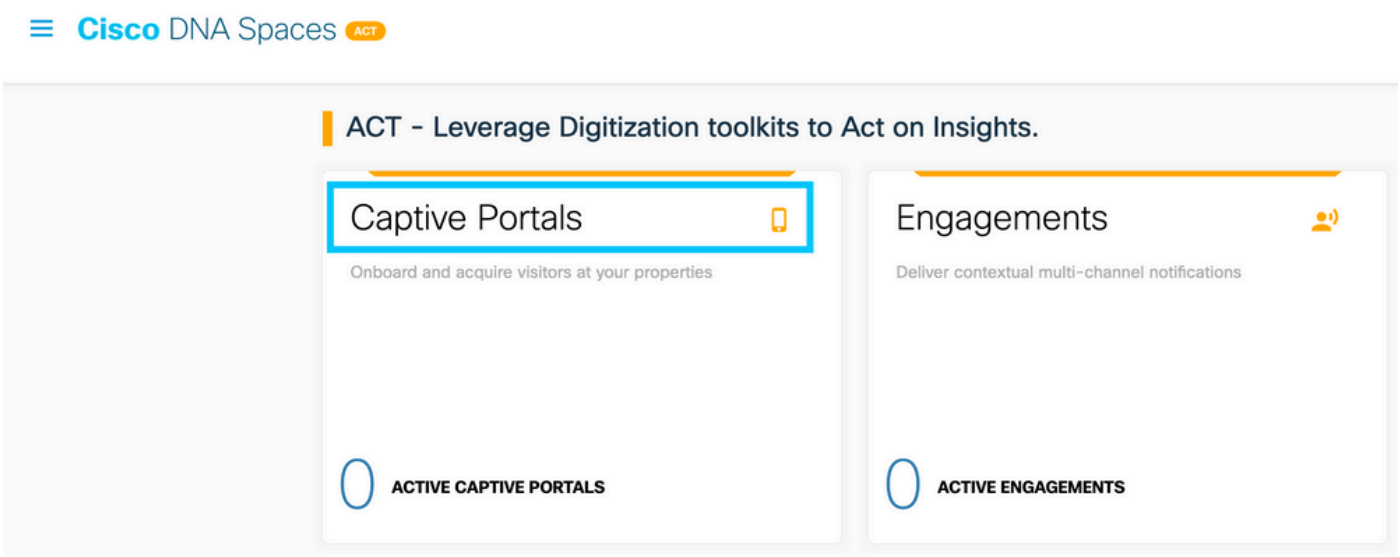


手順 6：必要に応じてポータルを編集し、[Save] をクリックします。

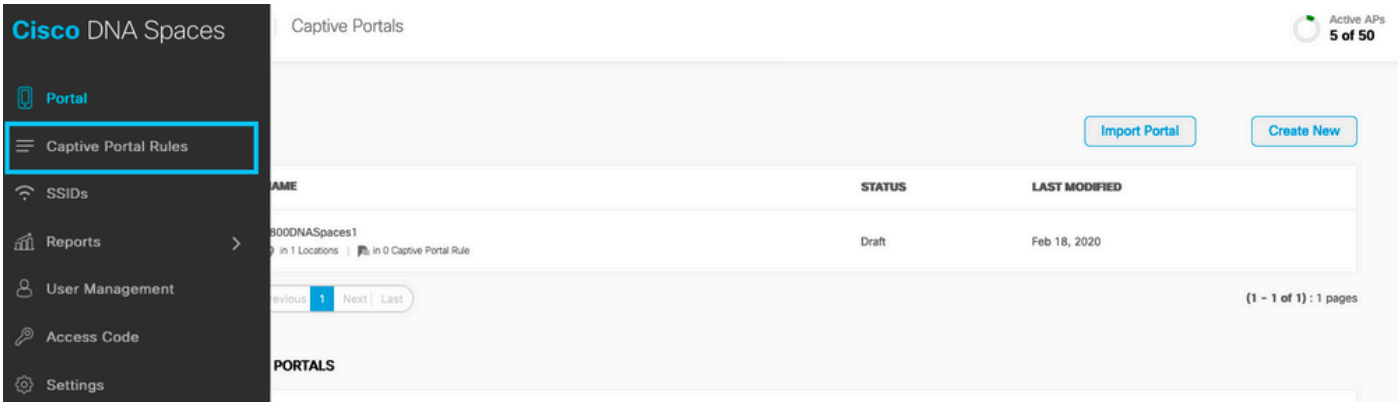


DNAスペースでのキャプティブポータルルールの設定

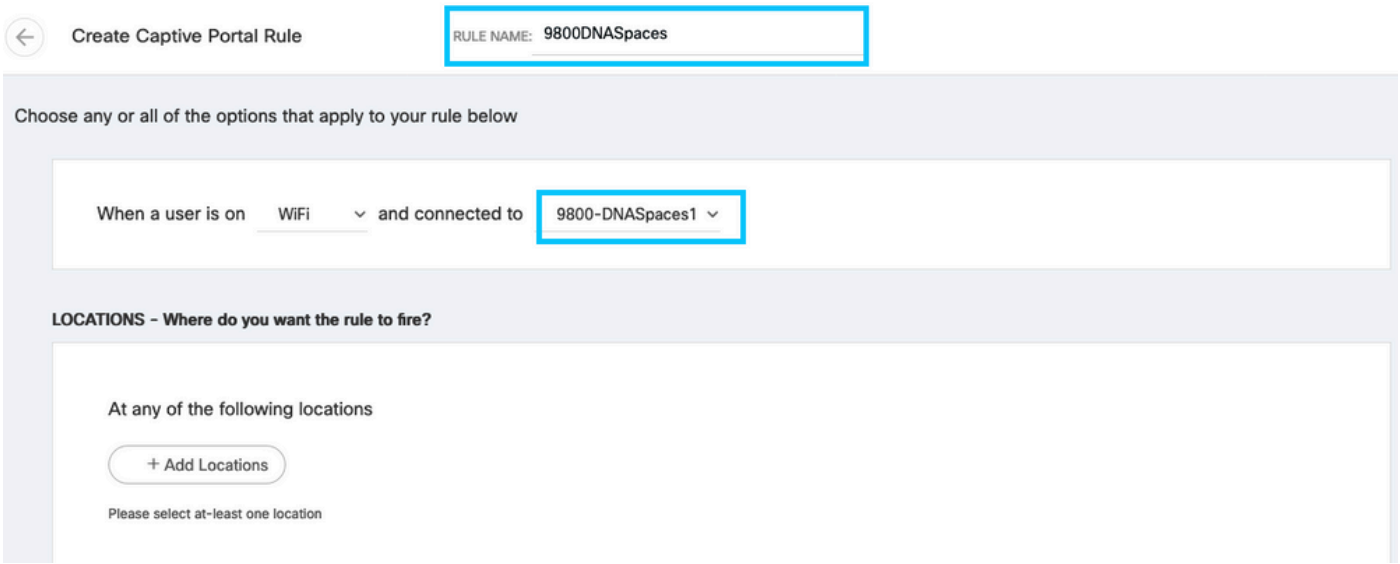
ステップ 1：DNA Spacesのダッシュボードで[Captive Portals] をクリックします。



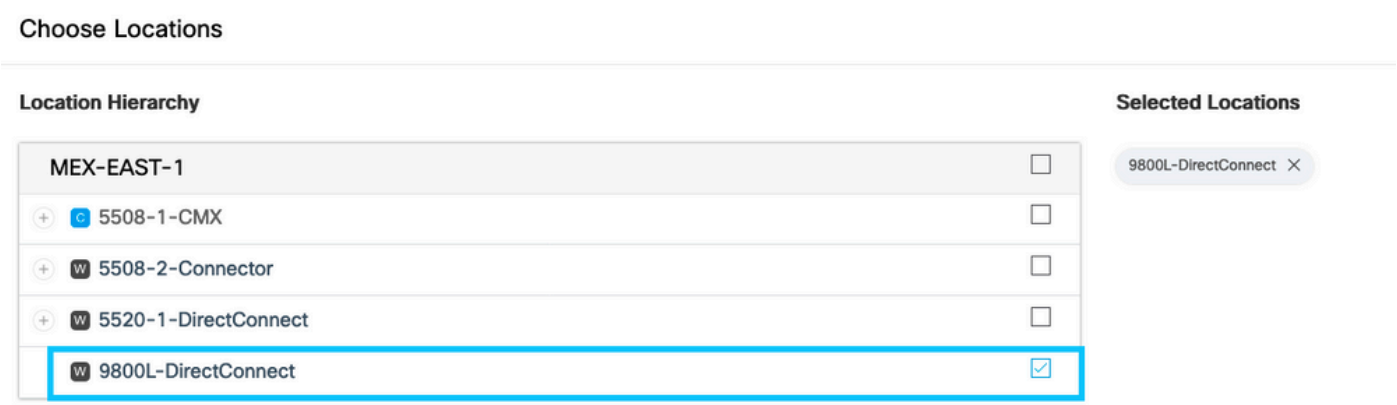
ステップ 2：キャプティブポータルメニューを開き、[Captive Portal Rules] をクリックします。



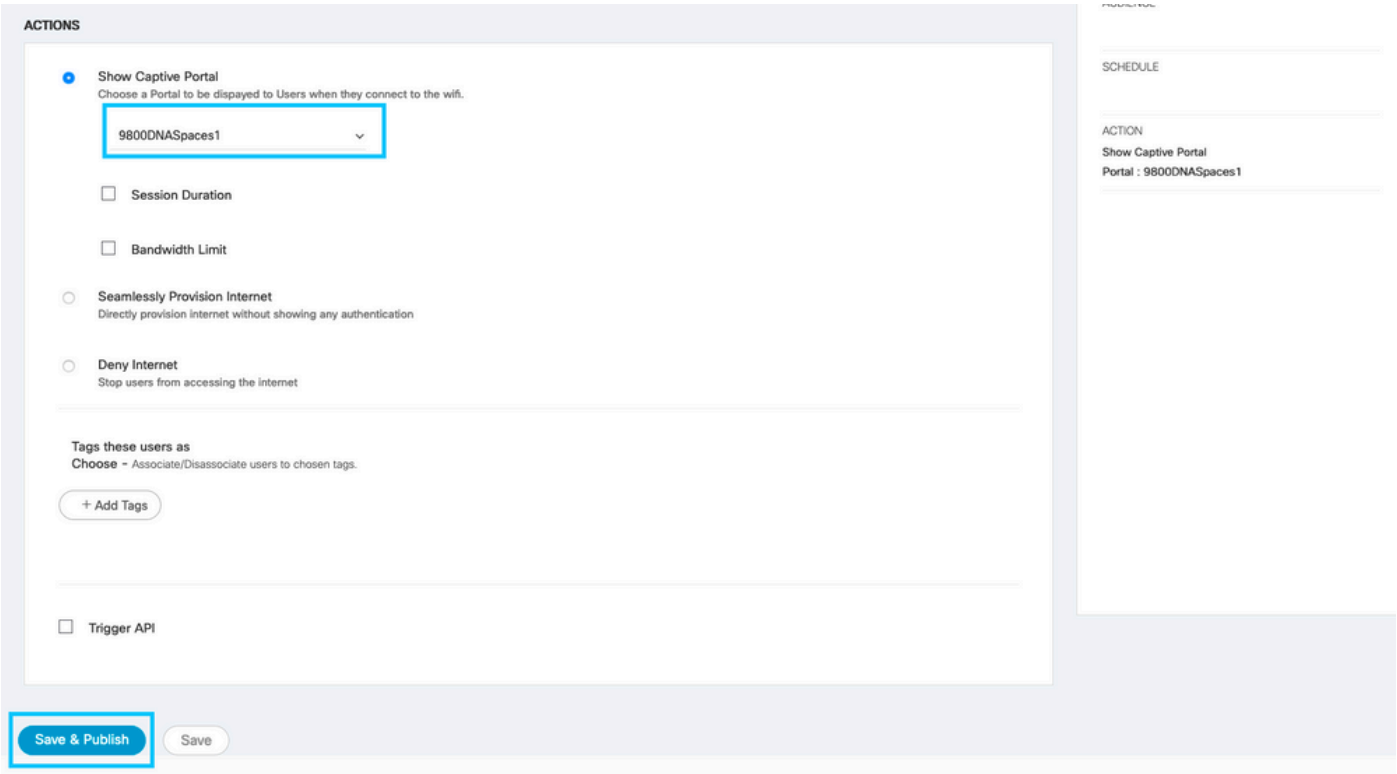
ステップ 3：+ [Create New Rule]をクリックします。ルール名を入力し、以前に設定したSSIDを選択します。



ステップ 4：ポータルを使用できる場所を選択します。[LOCATIONS] セクションで[Add Locations] をクリックします。「ロケーション階層」から目的のロケーションを選択します。



ステップ 5：キャプティブポータルのアクションを選択します。この場合、ルールがヒットすると、ポータルが表示されます。[Save & Publish] をクリックします。

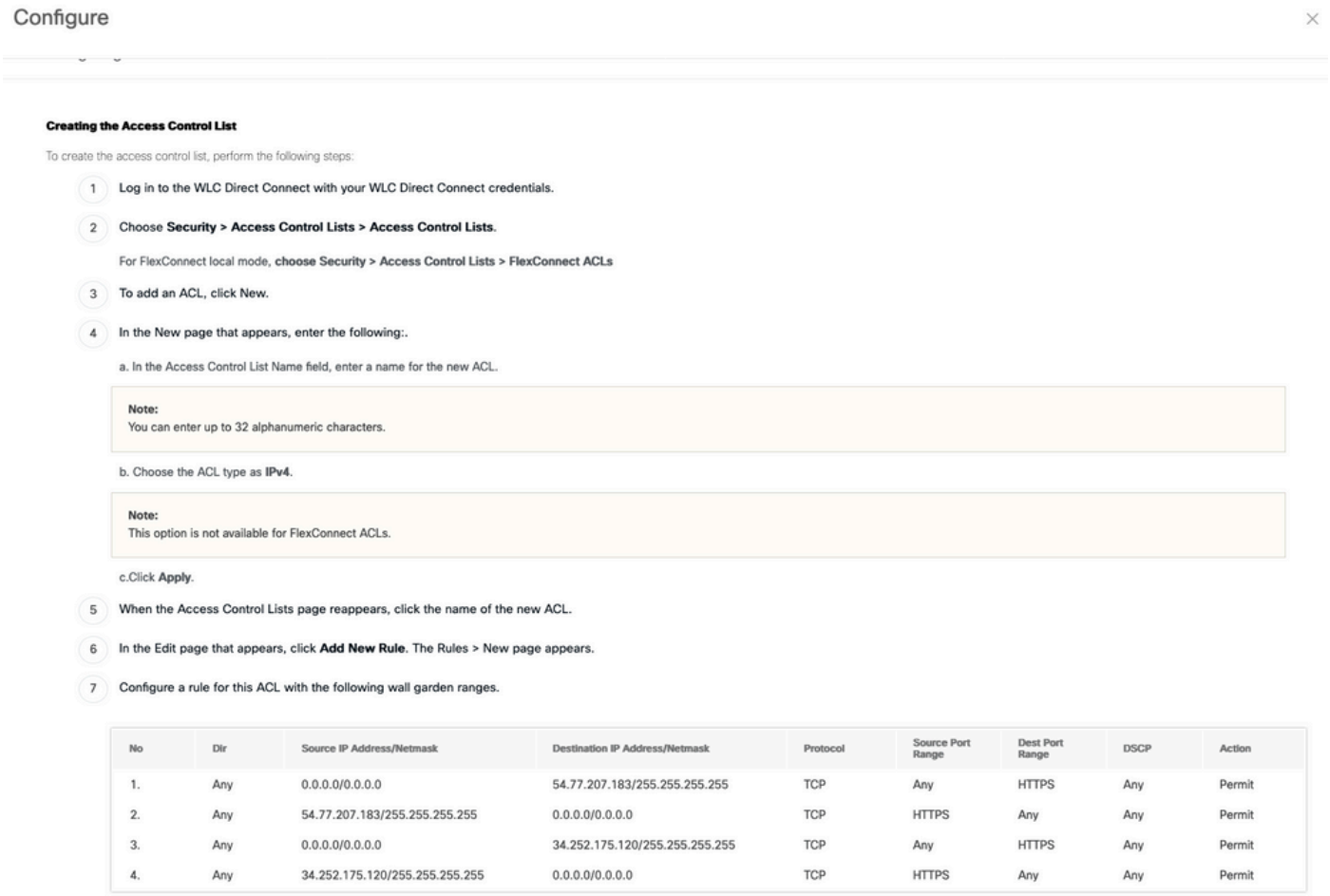


DNA空間から具体的な情報を得る

DNA空間が使用するIPアドレスは何ですか。

DNA Spaceが地域のポータルに使用するIPアドレスを確認するには、DNA Spaceホームの Captival Portalページに移動します。左側のメニューで**SSID**をクリックし、次にSSIDの下で **Configure manually**をクリックします。IPアドレスはACLの例で説明されています。これらは、ACLおよびwebauthパラメータマップで使用するポータルのIPアドレスです。DNA空間は、コントロールプレーンのNMSP/クラウド接続全体に対して他のIPアドレスを使用します。

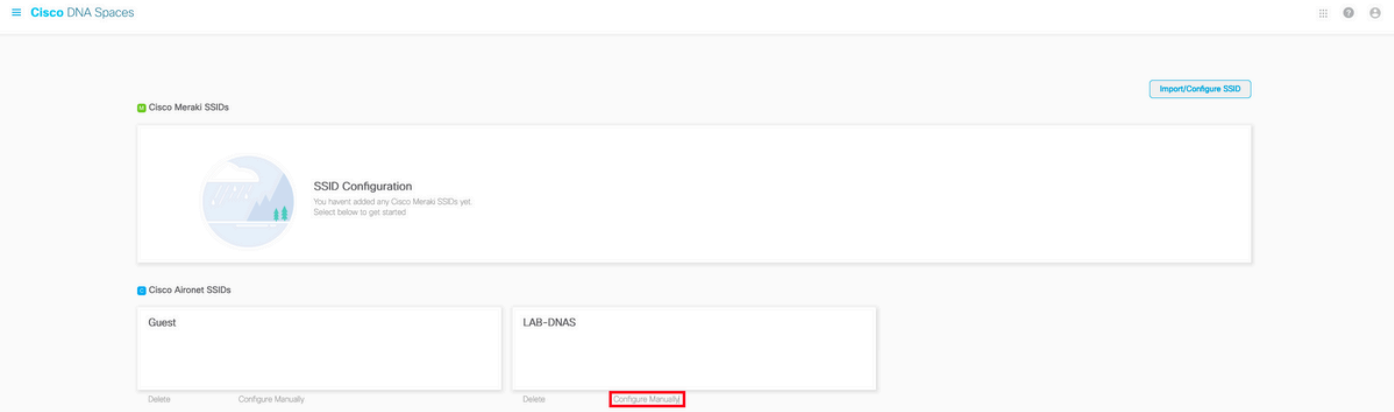
表示されるポップアップの最初のセクションで、手順7にACL定義で指定されたIPアドレスが表示されます。これらの手順を実行してACLを作成する必要はありません。IPアドレスを書き留めておくだけです。これらは、お客様の地域のポータルで使用されるIPです



No	Dir	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP	Action
1.	Any	0.0.0.0/0.0.0.0	54.77.207.183/255.255.255.255	TCP	Any	HTTPS	Any	Permit
2.	Any	54.77.207.183/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit
3.	Any	0.0.0.0/0.0.0.0	34.252.175.120/255.255.255.255	TCP	Any	HTTPS	Any	Permit
4.	Any	34.252.175.120/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit

DNAスペースログインポータルが使用するURLは何ですか。

お住まいの地域のポータルで使用されているログインポータルURL DNA Spacesを確認するには、DNA SpaceホームのCaptival Portalページに移動します。左側のメニューで**SSID**をクリックし、次にSSIDの下で**Configure manually**をクリックします。



表示されるポップアップで下にスクロールし、2番目のセクションのステップ7に、9800のパラメータマップで設定する必要があるURLが表示されます。

Creating the SSIDs in WLC Direct Connect

To create the SSIDs in the WLC Direct Connect, perform the following steps:

1. In the WLC Direct Connect main window, click the **WLANs** tab.
2. To create a WLAN, choose **Create New** from the drop-down list at the right side of the page, and click **Go**.
3. In the New page that appears, enter the WLAN details like Type, Profile Name, SSID, and so on.
4. Click **Apply**.

   The WLAN added appears in the WLANs page.
5. Click the WLAN you have newly created.
6. Choose **Security > Layer 2** , and configure the Layer 2 Security as **None** .
7. In the **Layer 3 tab** , do the following configurations:

   a.From the Layer 3 security drop-down list, choose **Web Policy** .

   b.Choose the **Passthrough** radio button.

   c.In the Preauthentication ACL area, from the IPv4 drop-down list, choose the ACL created earlier.

   d.Select the Enable check box for the Sleeping Client.

   e.Select the Enable check box for the Override Global Config.

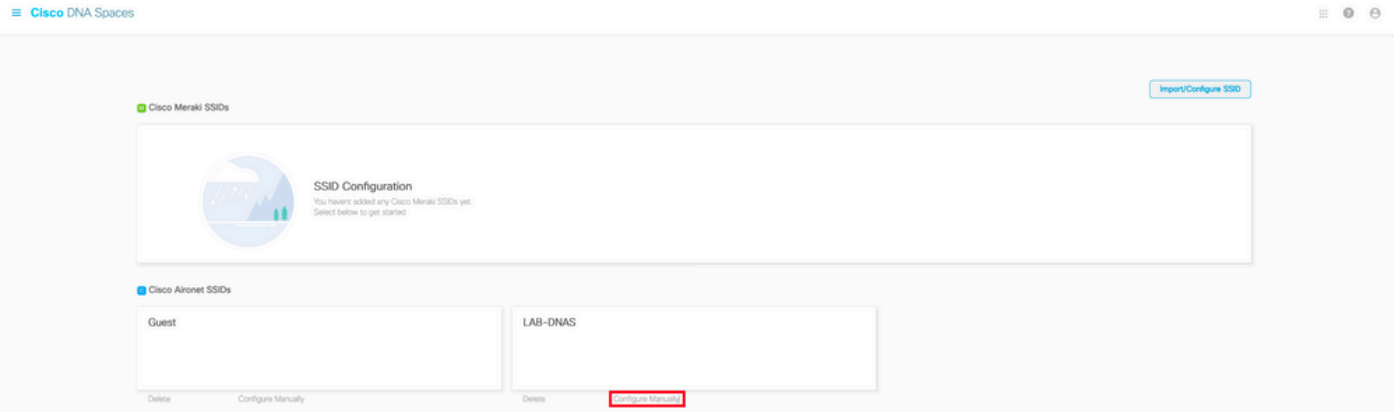
   f.From the Web Auth Type drop-down list, choose **External** .

   g.In the URL field that appears, enter the Cisco DNA Spaces splash URL.

https://splash.dnaspaces.eu/p2/emeabru2

DNAスペースのRADIUSサーバの詳細は何ですか。

使用する必要があるRADIUSサーバのIPアドレスと共有秘密を確認するには、DNA Spaceホームのページに移動します。左側のメニューで**SSID**をクリックし、次にSSIDの下で**Configure manually**をクリックします。



表示されるポップアップで、3番目のセクション(RADIUS)を下にスクロールすると、ステップ7にRADIUS認証のIP/ポートと共有秘密が表示されます。アカウンティングはオプションで、手順12で説明します。

7 In the New page that appears, enter the details of the radius server for authentication, such as server IP address, port number, and secret key, select the Server Status as **Enabled** , and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1812
Secret Key: emeab1299E2PqvUK

8 Choose **Radius > Accounting**.

The Radius Accounting Servers page appears.

9 From the Acct Called Station ID Type, choose **AP MAC Address:SSID**.

10 From the MAC Delimiter drop-down list, choose **Hyphen**.

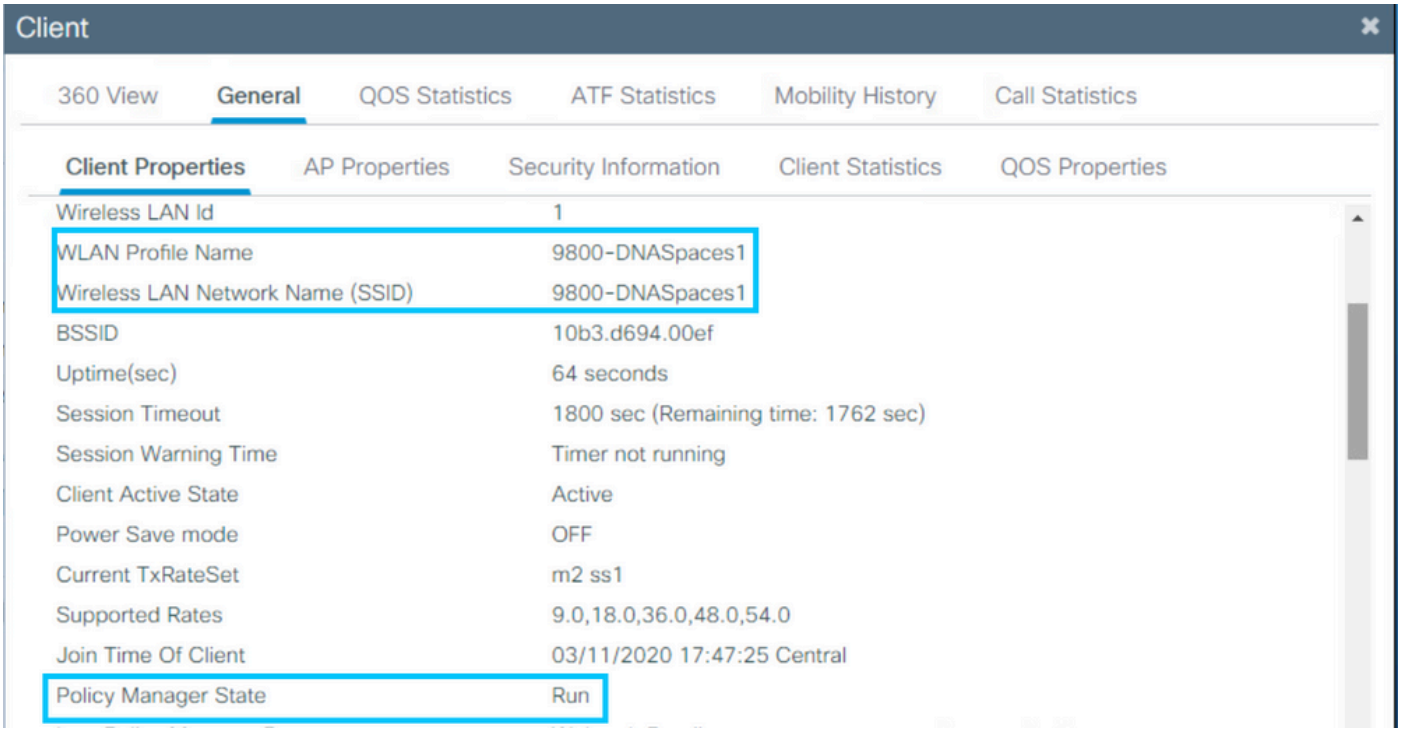
11 Click **New**.

12 In the New page that appears, enter the details of the radius server for accounting, such as server IP address, port number, and secret key, select the Server Status as **Enabled** , and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1813
Secret Key: emeab1299E2PqvUK

確認

SSIDに接続されているクライアントのステータスを確認するには、[Monitoring] > [Clients] に移動し、デバイスのMACアドレスをクリックして[Policy Manager State]を探します。



トラブルシュート

一般的な問題

1.コントローラの仮想インターフェイスにIPアドレスが設定されていない場合、クライアントはパラメータマップで設定されているリダイレクトポータルではなく、内部ポータルにリダイレクトされます。

2.クライアントがDNAスペースのポータルにリダイレクトされている間に*503*エラーを受信する場合は、コントローラがDNAスペースの**ロケーション階層**で設定されていることを確認します。

常時オンのトレース

WLC 9800 では、ALWAYS-ON トレース機能を利用できます。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、発生後にインシデントまたは障害状態のログを表示できます。

> **注**：生成されるログの量に応じて、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。

```
# 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、システムの状態とエラー（ある場合）を簡単に確認できます。

```
# 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。

```
# show debugging
Cisco IOS-XE Conditional Debug Configs:

Conditional Debug Global State: Stop

Cisco IOS-XE Packet Tracing Configs:


Packet Infra debugs:

Ip Address                                            Port
------------------------------------------------------|----------
```

> **注：**リストされている条件が表示される場合は、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ていない場合は、特定のMACアドレスのalways-on notice levelトレースを収集します。

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

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。

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

条件付きデバッグとラジオアクティブトレース

常時オンのトレースでは、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、無線アクティブ(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が提供されます。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 1：デバッグ条件が有効になっていないことを確認します。

```
# clear platform condition all
```

ステップ 2：モニタ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。

次のコマンドは、指定された MAC アドレスの 30 分間（1800 秒）のモニターを開始します。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。

```
# 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：ターミナルセッションでは、クライアントアクティビティの出力は表示されません。これは、後で表示できるように内部でバッファされているためです。

ステップ 3：監視する問題または動作を再現します。

ステップ 4：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された場合は、デバッグを停止します。

```
# 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 5： 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

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

ファイルを外部サーバーにコピーします。

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://a.b.c.d/ra-FILENAME.txt
```

内容を表示します。

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

手順 6：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。クライアントを再度デバッグする必要はありません。すでに収集され、内部で保存されているデバッグログをさらに詳しく調べるだけです。

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

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、非常に膨大です。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。

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

内容を表示します。

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

手順 7：デバッグ条件を削除します。

```
# 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。

成功した試行の例

これは、RADIUSサーバを使用せずにSSIDに接続しているときに、アソシエーション/認証プロセス中に各フェーズの識別に成功した場合のRA_tracesからの出力です。

802.11アソシエーション/認証：

```
Association received. BSSID 10b3.d694.00ee, WLAN 9800DNASpaces, Slot 1 AP 10b3.d694.00e0,
2802AP-9800L
Received Dot11 association request. Processing started,SSID: 9800DNASpaces1, Policy profile:
DNASpaces-PP, AP Name: 2802AP-9800L, Ap Mac Address: 10b3.d694.00e0 BSSID MAC0000.0000.0000 wlan
ID: 1RSSI: 0, SNR: 32
Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
dot11 send association response. Sending association response with resp_status_code: 0
dot11 send association response. Sending assoc response of length: 144 with resp_status_code: 0,
DOT11_STATUS: DOT11_STATUS_SUCCESS
Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False
DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED
Station Dot11 association is successful
```

IP Learnプロセス：

```
IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
Client IP learn successful. Method: ARP IP: 10.10.30.42
IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
Received ip learn response. method: IPLEARN_METHOD_AR
```

レイヤ3認証：

```
Triggered L3 authentication. status = 0x0, Success
Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
L3 Authentication initiated. LWA
Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING
```

```
Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in
INIT state
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]HTTP GET request
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Parse GET, src
[10.10.30.42] dst [13.107.4.52] url [http://www.msftconnecttest.com/connecttest.txt]
```

```
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-
agent = Microsoft NCSI
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in
LOGIN state
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]HTTP GET request
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Parse GET, src
[10.10.30.42] dst [151.101.24.81] url [http://www.bbc.com/]
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-
agent = Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]POST rcvd when in
LOGIN state
```

レイヤ3認証に成功し、クライアントをRUN状態に移行します。

```
[34e1.2d23.a668:capwap_90000005] Received User-Name 34E1.2D23.A668 for client 34e1.2d23.a668
L3 Authentication Successful. ACL:[]
Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE
%CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: Username entry (34E1.2D23.A668) joined with ssid
(9800DNASpaces) for device with MAC: 34e1.2d23.a668
Managed client RUN state notification: 34e1.2d23.a668
Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RU
```

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。