ワイヤレスLANコントローラの有線ゲストの設定、確認、トラブルシューティング

内容

はじめに

このドキュメントでは、外部Web認証を使用した9800およびIRCMでの有線ゲストアクセスの設定、確認、およびトラブルシューティングの方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

9800 WLC

AireOS WLC

モビリティトンネル

ISE

有線ゲストアクセスを設定する前に、2つのWLC間にモビリティトンネルが確立されていることを前提としています。

この点は、この設定例の範囲外です。詳細な手順については、添付資料の『9800でのモビリティトポロジの設定』を参照してください。

使用するコンポーネント

9800 WLCバージョン17.12.1

5520 WLCバージョン8.10.185.0

ISEバージョン3.1.0.518

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

別のCatalyst 9800にアンカーされたCatalyst 9800での有線ゲストの設定

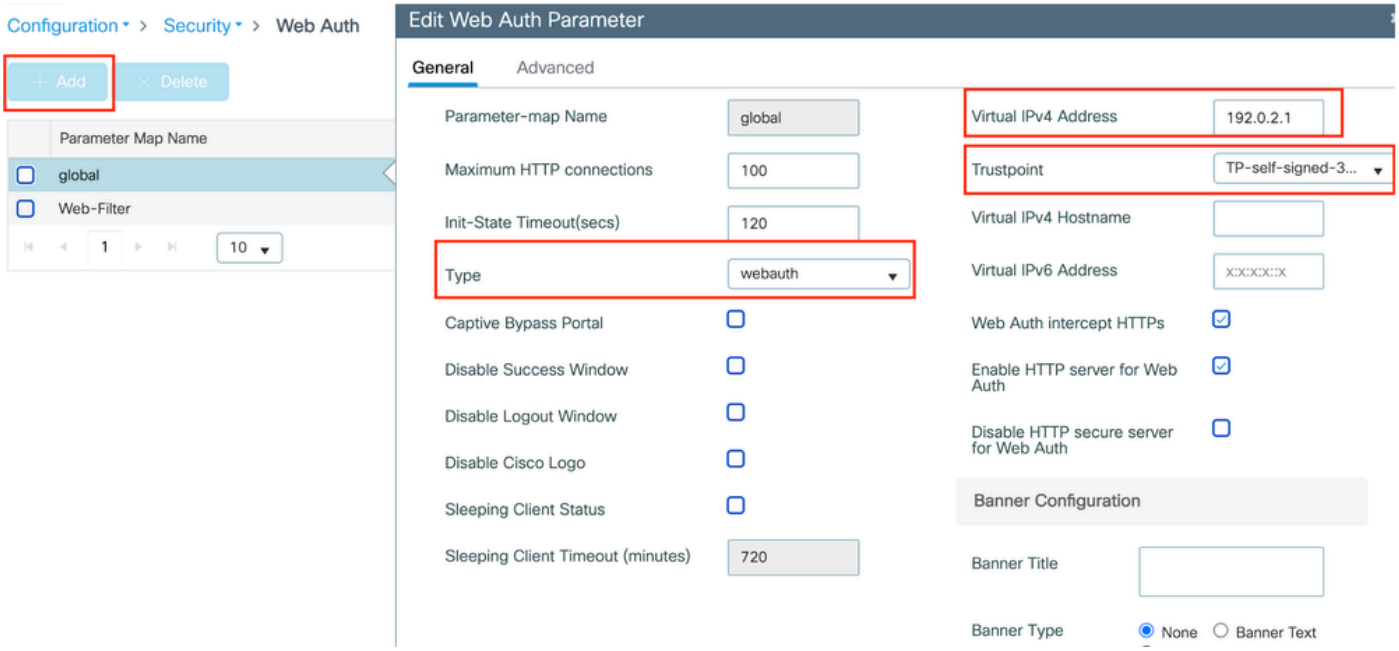
ネットワーク図

Network Topology

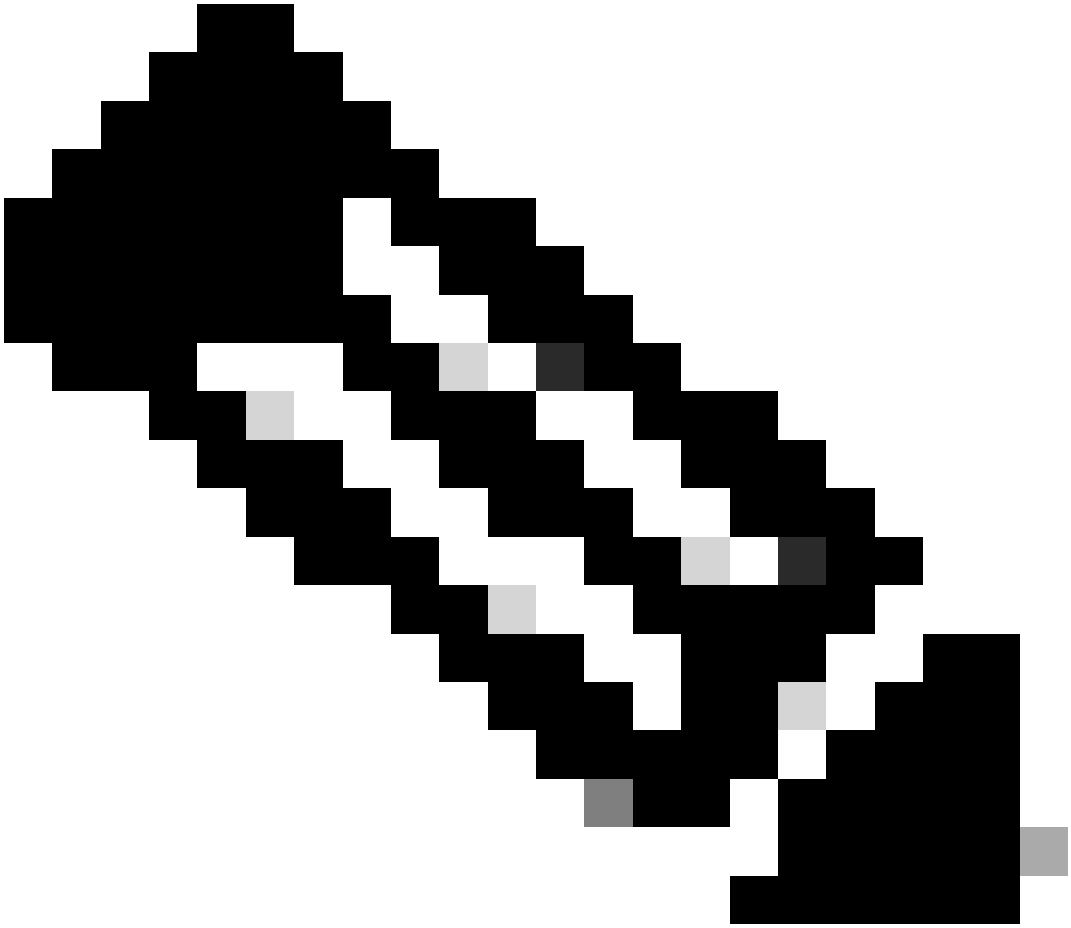
外部9800 WLC上の設定

Webパラメータマップの設定

ステップ1:Configuration > Security > Web Authの順に移動し、Globalを選択して、コントローラとトラストポイントマッピングの仮想IPアドレスを確認し、タイプがwebauthに設定されていることを確認します。

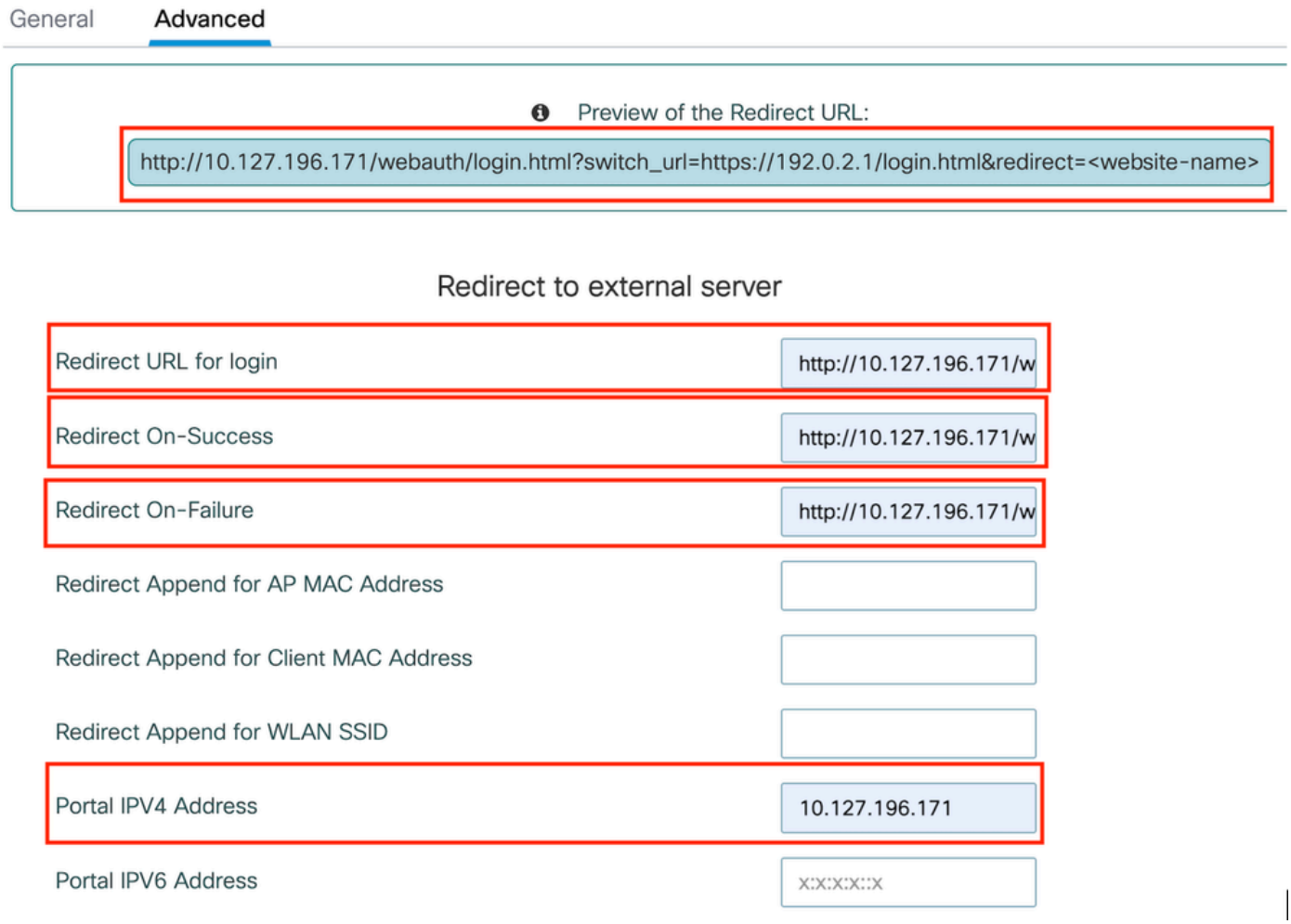


グローバルパラメータマップ



注:Web Auth intercept HTTPsはオプション設定です。HTTPSリダイレクションが必要な場合、Web Auth intercept HTTPSオプションを有効にする必要があります。ただし、この設定はCPU使用率を増加させるため、推奨されません。

ステップ2:Advancedタブで、クライアントリダイレクション用の外部WebページのURLを設定します。「Redirect URL for Login」と「Redirect On-Failure」を設定します。「Redirect On-Success」はオプションです。設定が完了すると、リダイレクトURLのプレビューがWeb認証プロファイルに表示されます。



[詳細設定]タブ

CLI での設定

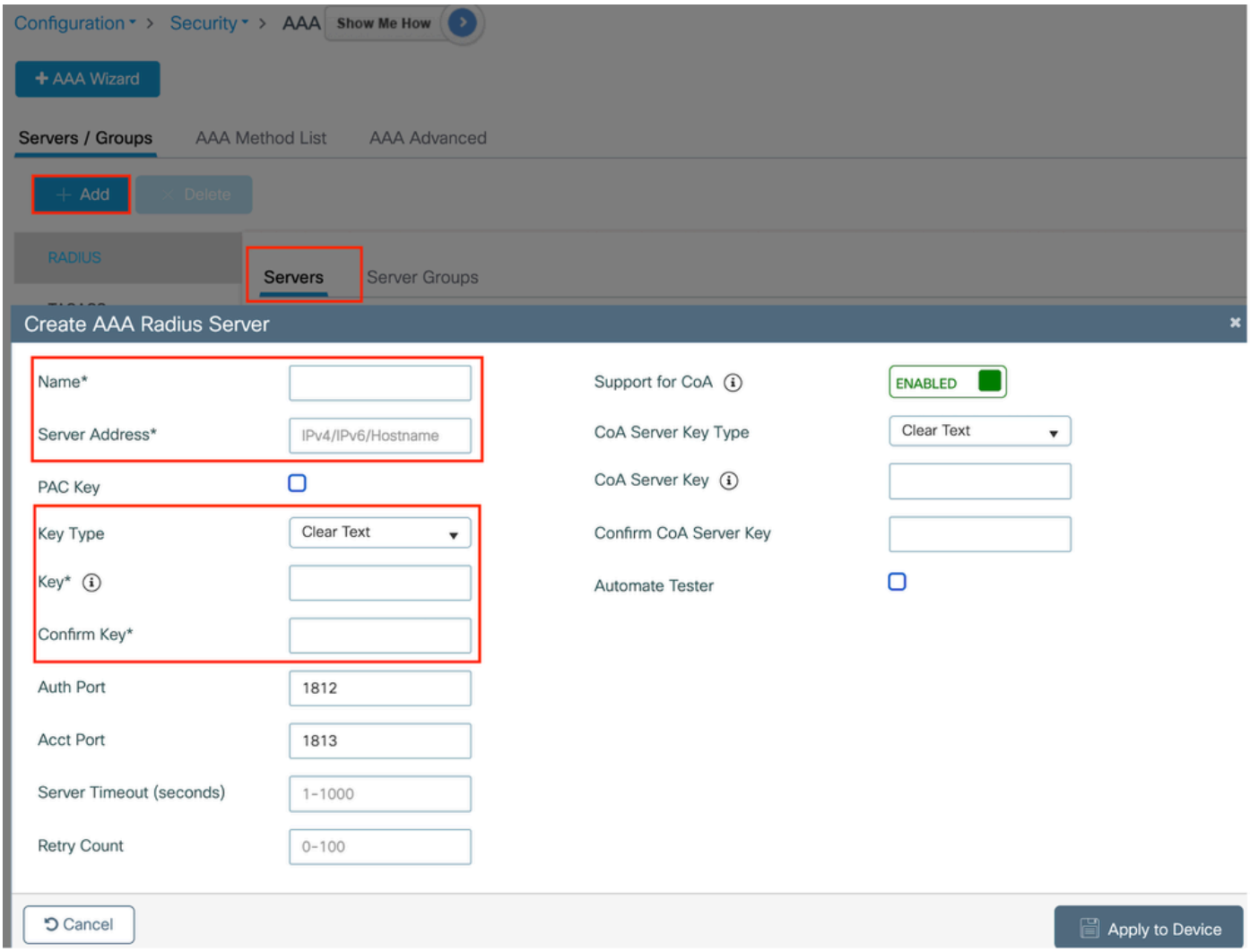
```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171
 intercept-https-enable
 trustpoint TP-self-signed-3915430211
 webauth-http-enable
```

注：このシナリオでは、グローバルパラメータマップが使用されます。要件に従って、[追加]を選択してカスタムWebパラメータマップを設定し、[詳細設定]タブでリダイレクトURLを設定します。トラストポイントと仮想IP(VIP)の設定は、グローバルプロファイルから継承されます。

AAA設定：

ステップ1:RADIUSサーバを作成します。

Configuration > Security > AAAの順に移動し、Server/Groupセクションの下のAddをクリックして、Create AAA Radius Serverページで、サーバ名、IPアドレス、およびShared Secretを入力します。

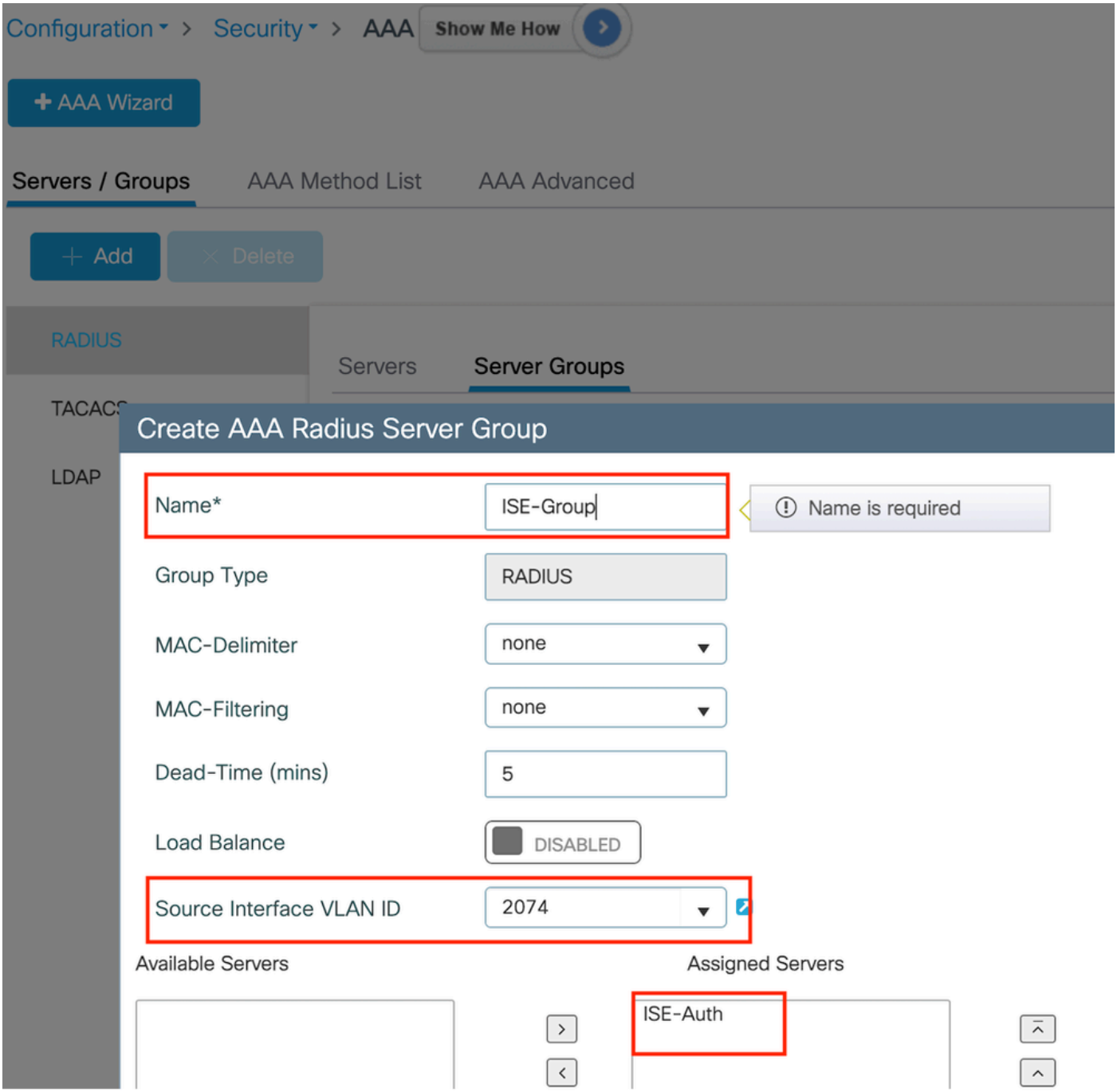


RADIUS サーバの設定

CLI での設定

```
radius server ISE-Auth
 address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
 key *****
 server name ISE-Auth
```

ステップ2:RADIUSサーバグループを作成します。
サーバグループを定義し、グループ設定に含めるサーバを切り替えるには、Server Groupsセクションの下のAddを選択します。



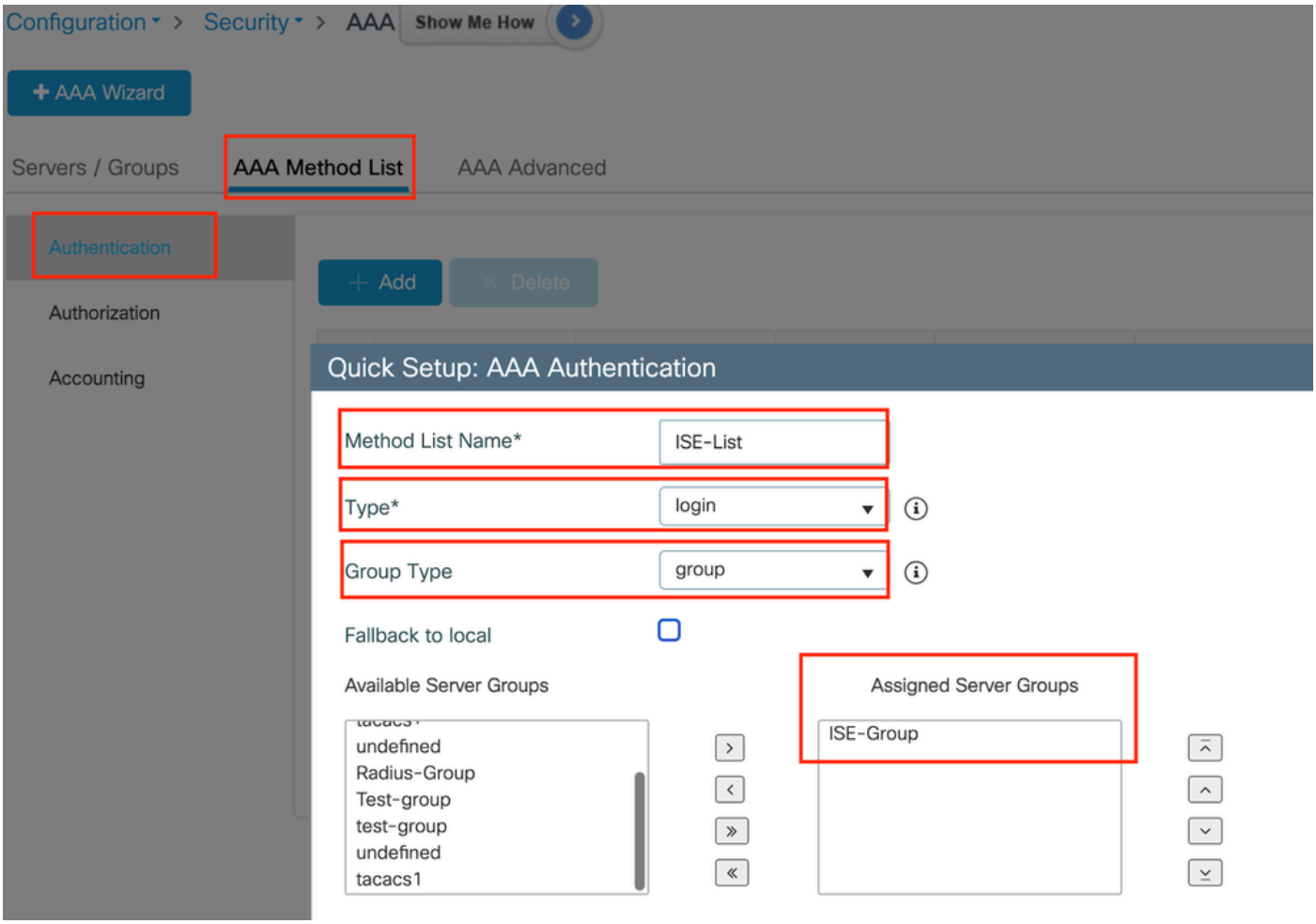
RADIUSサーバグループ

CLI での設定

```
aaa group server radius ISE-Group
 server name ISE-Auth
 ip radius source-interface Vlan2074
 deadtime 5
```

ステップ3:AAA方式リストを設定します。

AAA Method Listタブに移動し、Authenticationの下でAddを選択し、Typeに「login」、Group typeに「Group」を指定した方式リスト名を定義し、Assigned Server Groupセクションで設定した認証サーバグループをマッピングします。



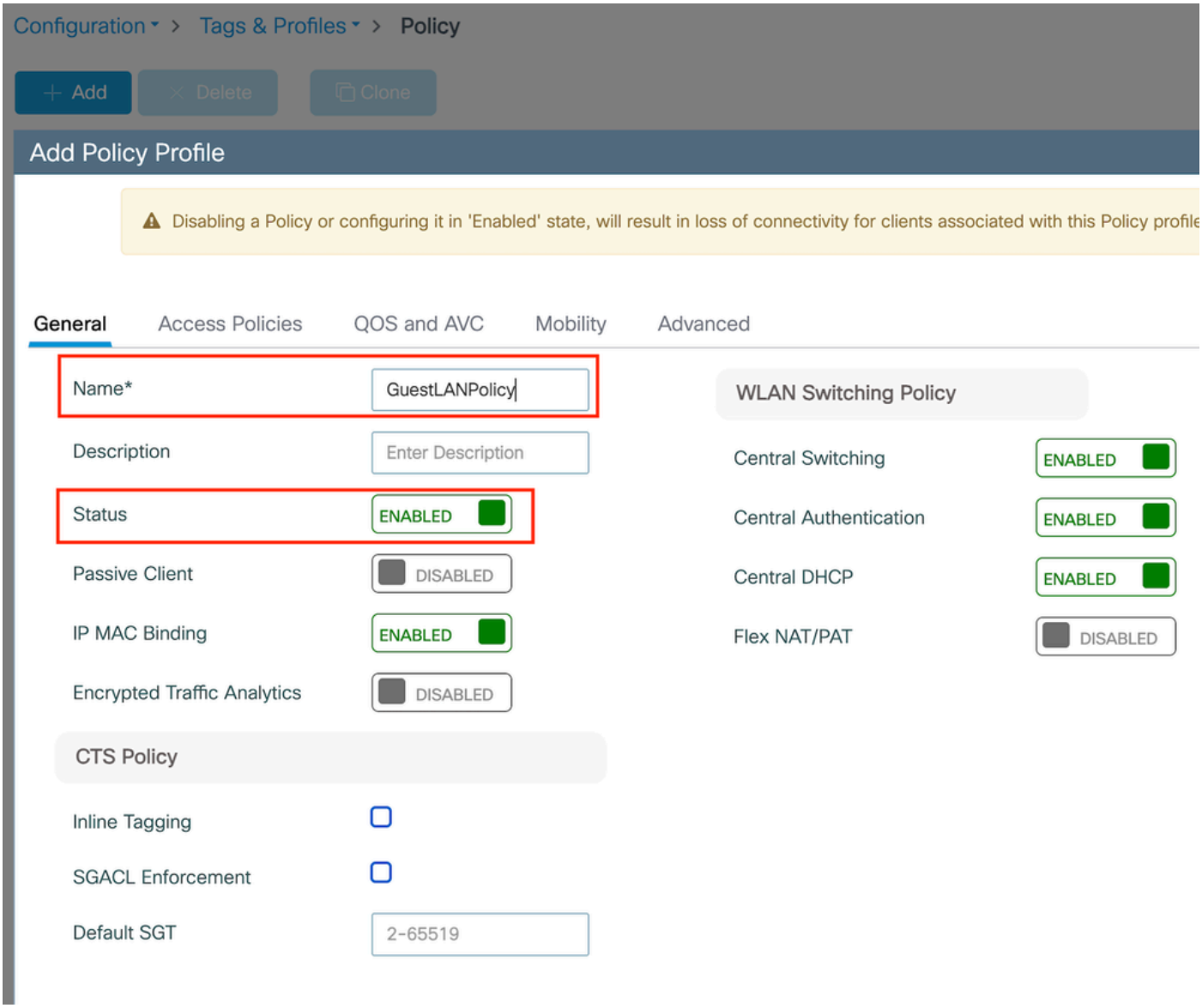
認証方式リスト

CLI での設定

```
aaa authentication login ISE-List group ISE-Group
```

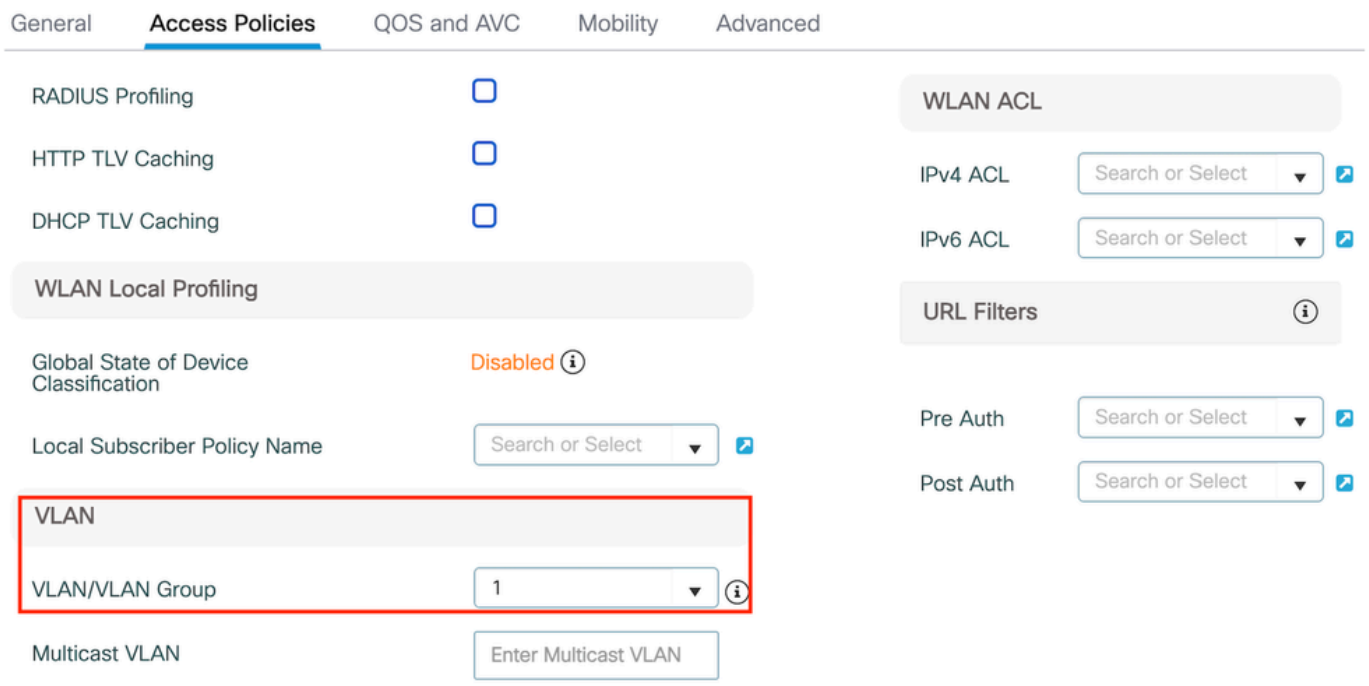
ポリシープロファイルの設定

ステップ1:Configuration > Tags & Profiles > Policyの順に移動し、Generalタブで新しいプロファイルに名前を付け、ステータス切り替えを使用して有効にします。



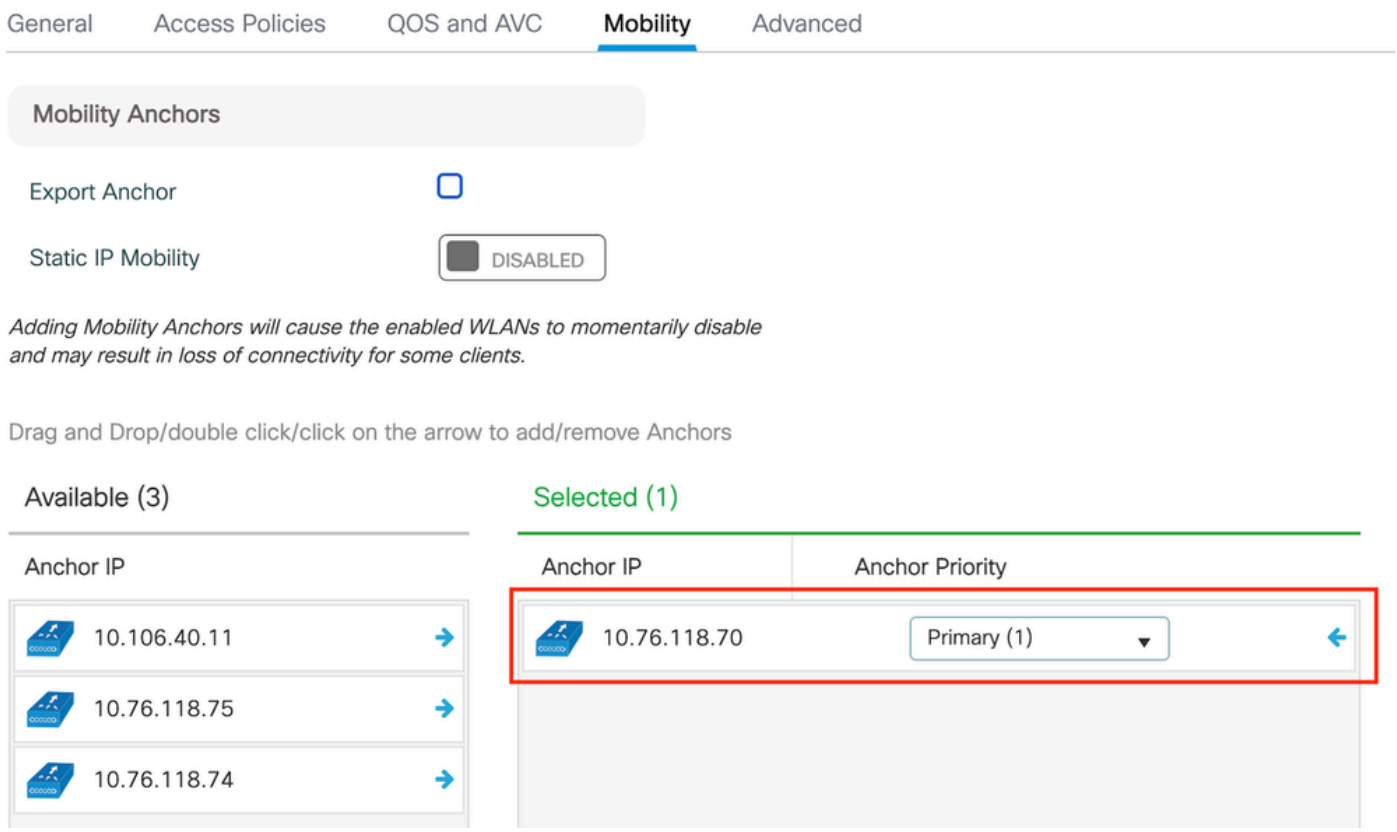
ポリシー プロファイル

ステップ2:Access Policiesタブで、VLANマッピングが完了したアンカーコントローラにランダムVLANを割り当てます。この例では、vlan 1が設定されています



Access Policyタブ

手順3:[モビリティ]タブで、アンカーコントローラをプライマリ(1)に切り替え、オプションで冗長性の要件に合わせてセカンダリおよびターシャリモビリティトンネルを設定します



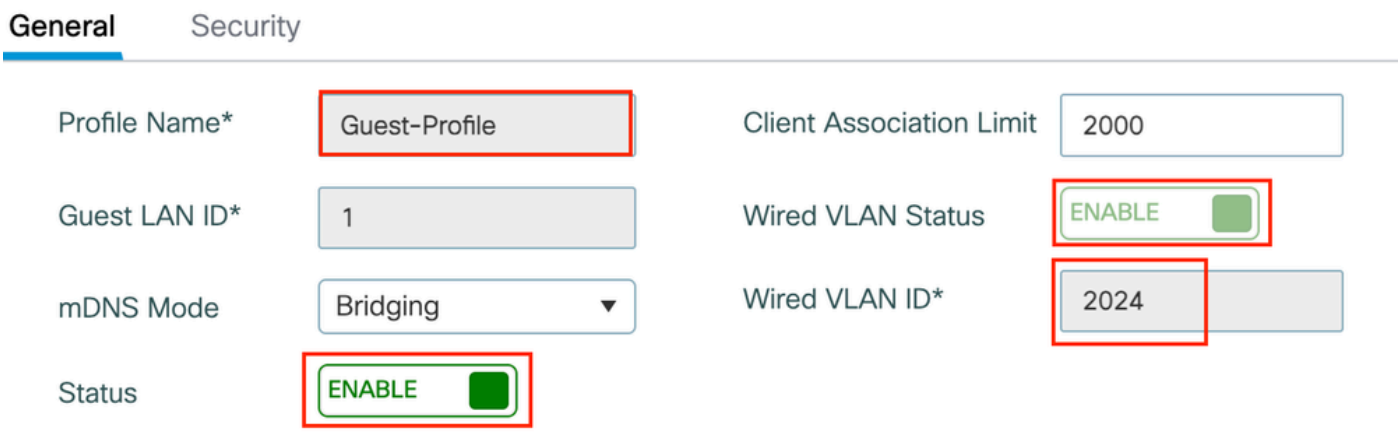
モビリティマップ

CLI での設定

```
wireless profile policy GuestLANPolicy
 mobility anchor 10.76.118.70 priority 1
 no shutdown
```

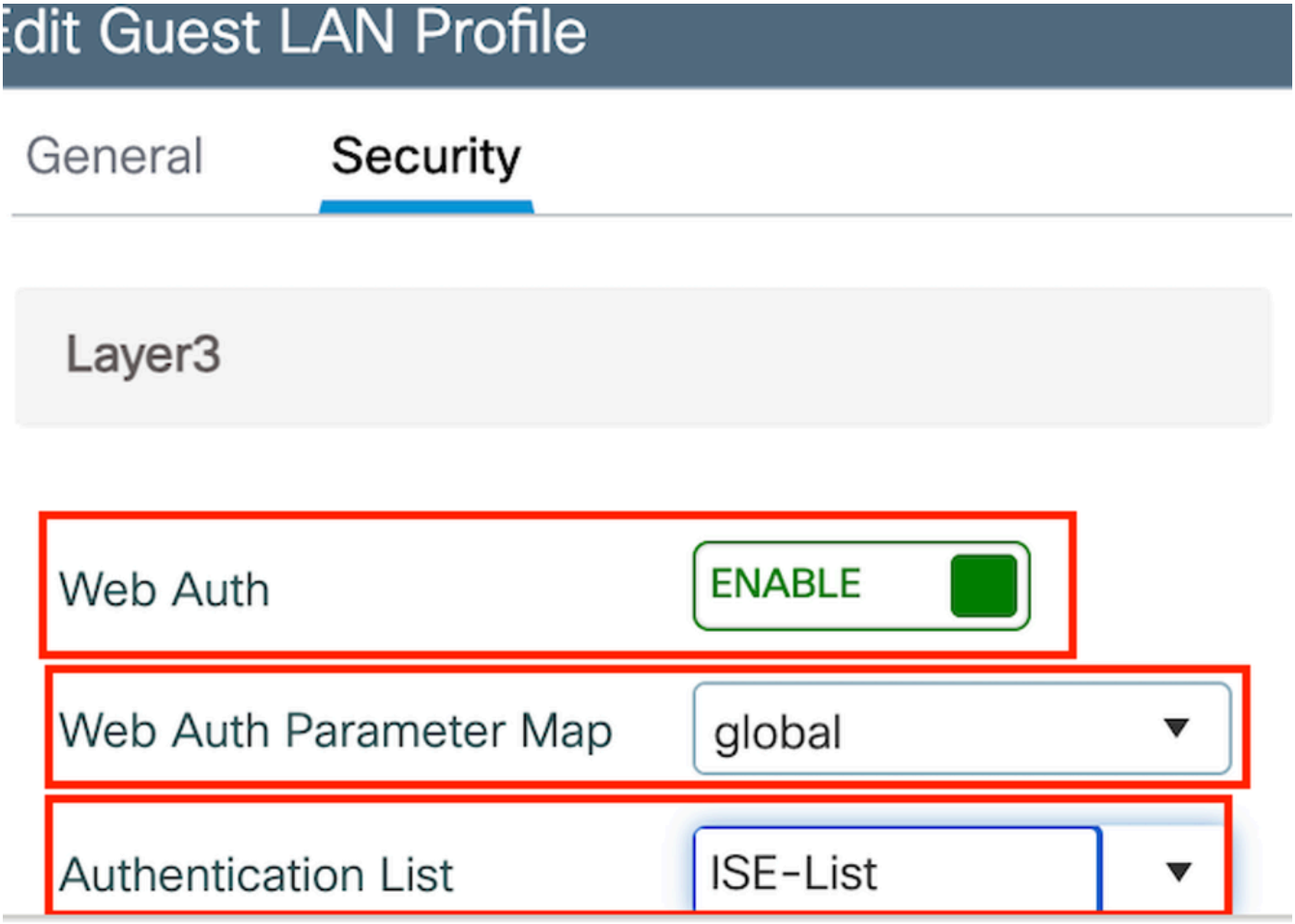
ゲストLANプロファイルの設定

ステップ1:Configuration > Wireless > Guest LANの順に移動し、Addを選択して、一意のプロファイル名を設定し、有線VLANを有効にします。次に、有線ゲストユーザのVLAN IDを入力し、プロファイルステータスをEnabledに切り替えます。



ゲストLANプロファイル

ステップ2: Securityタブで、Web Authを有効にし、Web Authパラメータマップをマッピングし、Authenticationドロップダウンリストから Radiusサーバを選択します。



Guest LAN Securityタブ

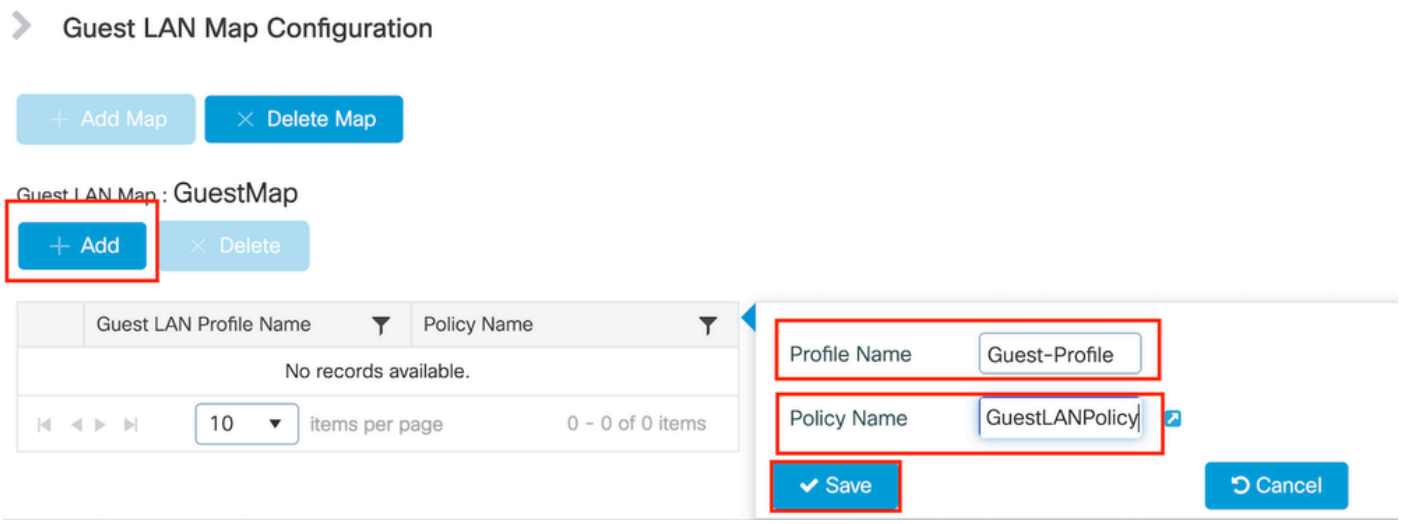
CLI での設定

```
guest-lan profile-name Guest-Profile 1 wired-vlan 2024
 security web-auth authentication-list ISE-List
 security web-auth parameter-map global
```

ゲストLANマップ

Configuration > Wireless > Guest LANの順に移動します。

Guest LAN MAP設定セクションで、Addを選択し、ポリシープロファイルとゲストLANプロファイルをマッピングします



ゲストLANマップ

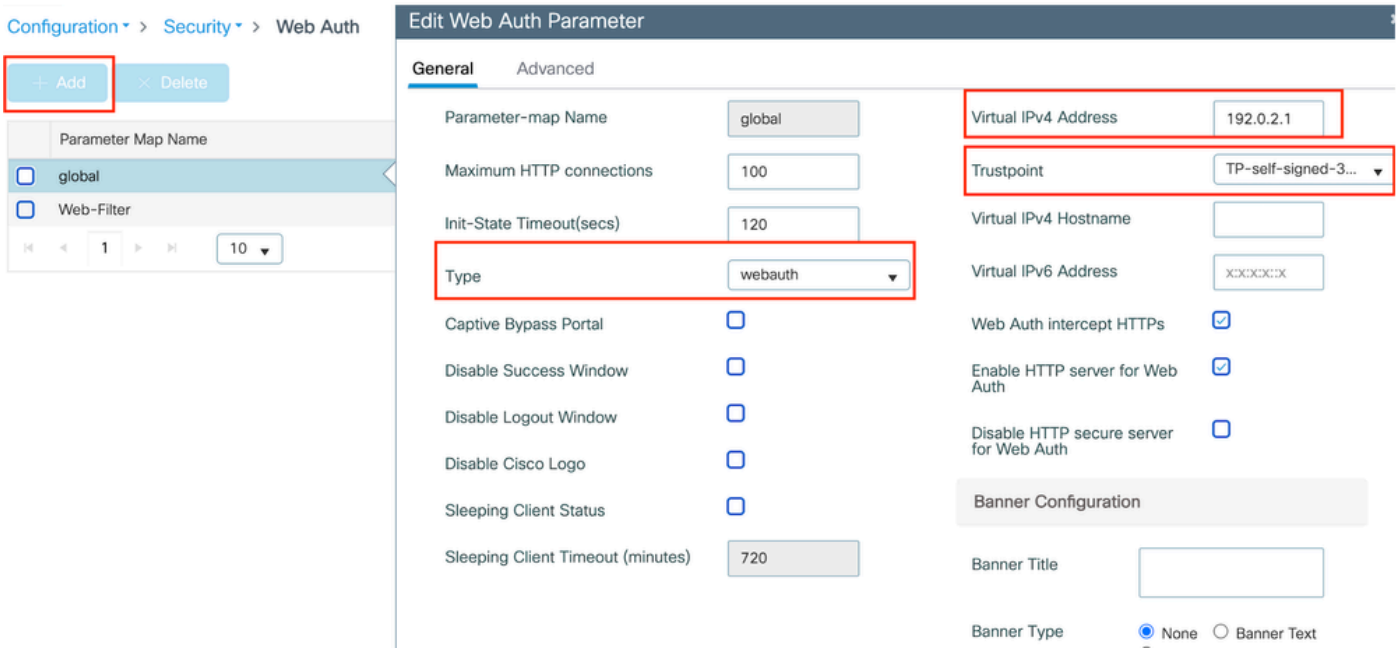
CLI での設定

```
wireless guest-lan map GuestMap
guest-lan Guest-Profile policy GuestLANPolicy
```

アンカー9800 WLCでの設定

Webパラメータマップの設定

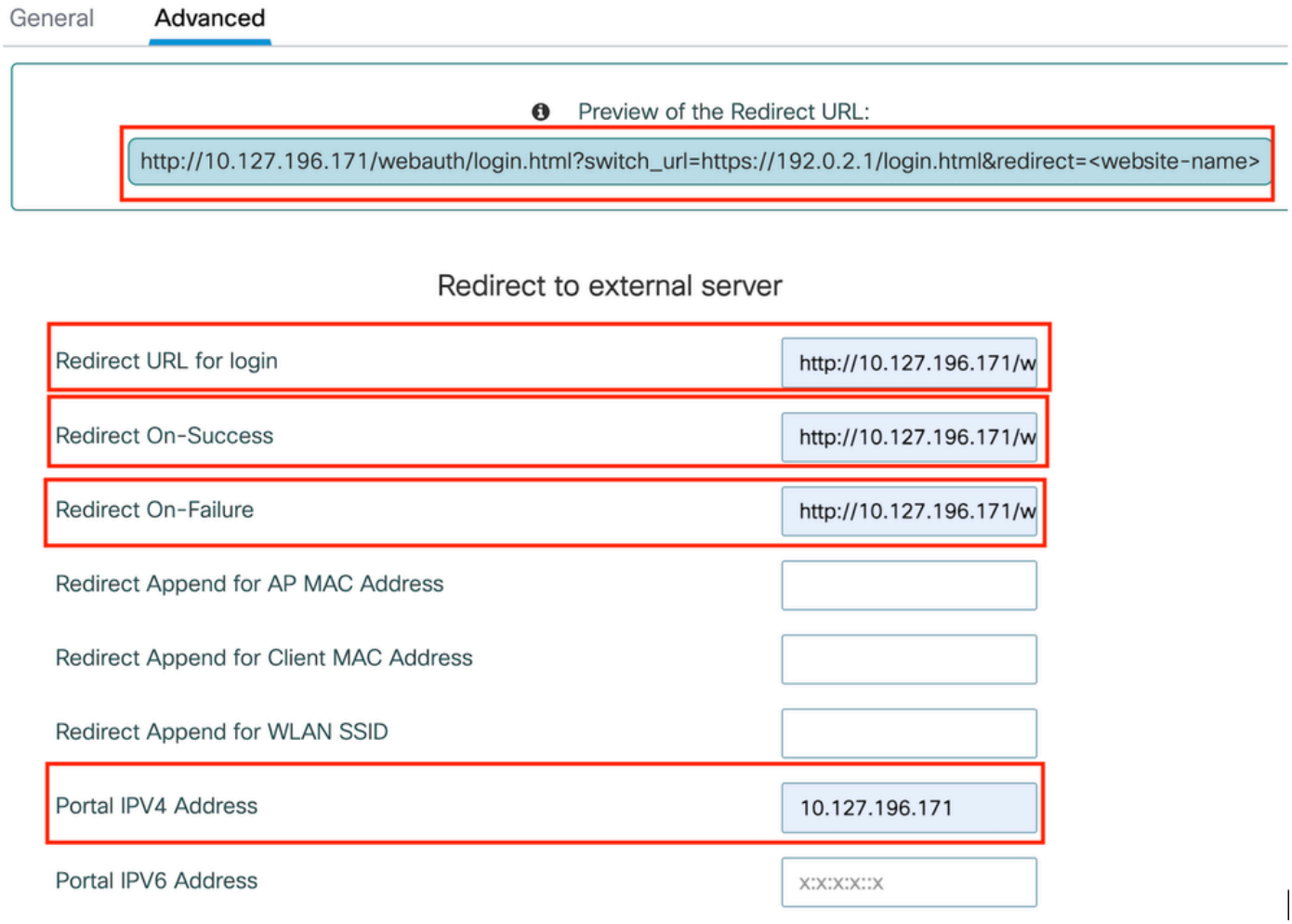
ステップ1:Configuration > Security > Web Authの順に移動し、Globalを選択して、コントローラとトラストポイントマッピングの仮想IPアドレスを確認し、タイプがwebauthに設定されていることを確認します。



グローバルパラメータマップ

ステップ2:Advancedタブで、クライアントリダイレクション用の外部WebページのURLを設定します。「Redirect URL for Login」と「Redirect On-Failure」を設定します。「Redirect On-Success」はオプションです。

設定が完了すると、リダイレクトURLのプレビューがWeb認証プロファイルに表示されます。



[詳細設定]タブ

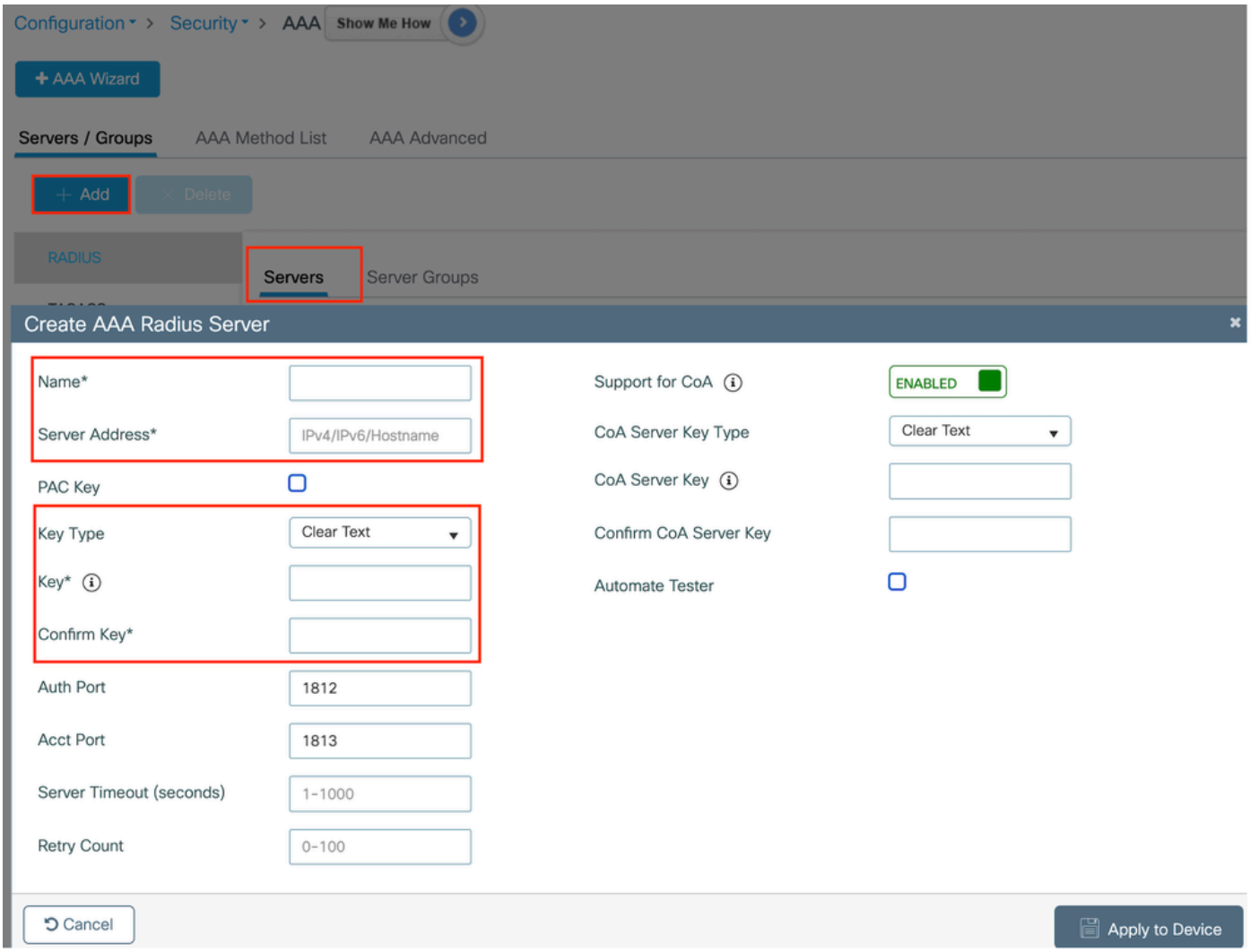
CLI での設定

```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171
 intercept-https-enable.
 trustpoint TP-self-signed-3915430211
 webauth-http-enable
```

AAA設定：

ステップ1:RADIUSサーバを作成します。

Configuration > Security > AAAの順に移動し、Server/Groupセクションにあ るAddをクリックし、Create AAA Radius Serverページで、サーバ名、IPアドレス、およびShared Secretを入力します。

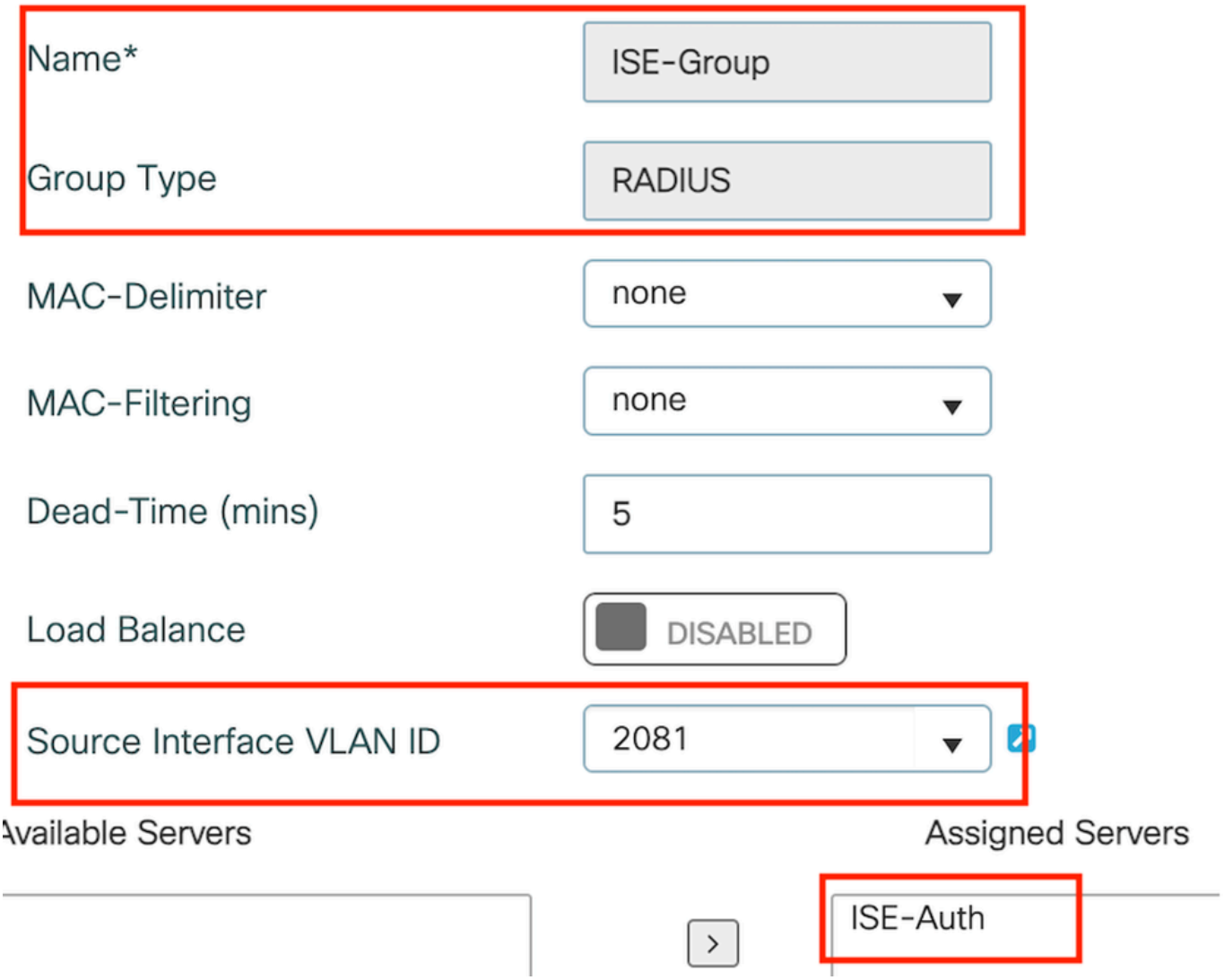


RADIUS サーバの設定

CLI での設定

```
radius server ISE-Auth
 address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
 key *****
 server name ISE-Auth
```

ステップ2:RADIUSサーバグループを作成します。
Server Groupsセクションにあ るAddを選択してサーバグループを定義し、グループ設定に含めるサーバを切り替えます。



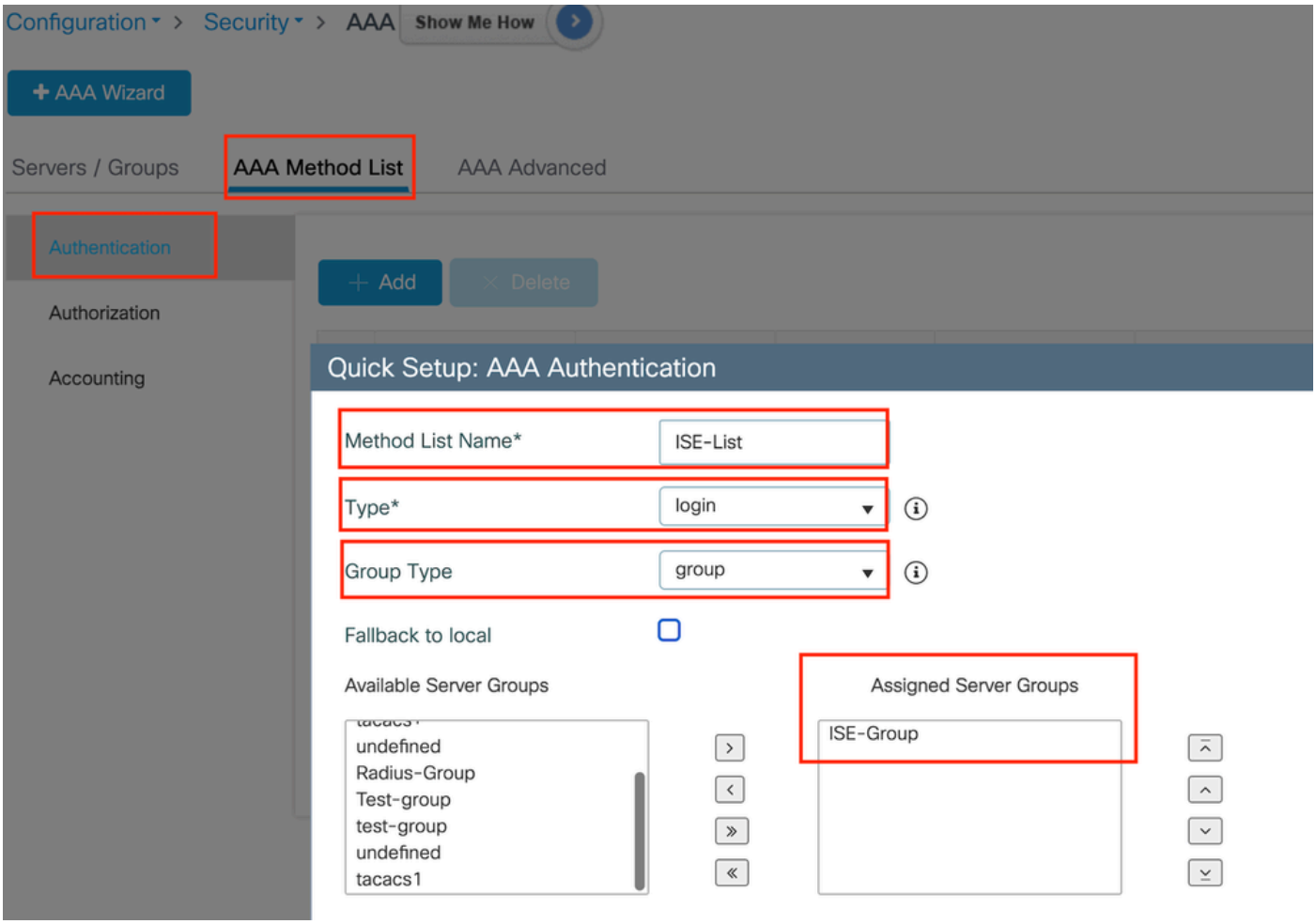
[アンカー半径]領域

CLI での設定

```
aaa group server radius ISE-Group
 server name ISE-Auth
 ip radius source-interface Vlan2081
 deadtime 5
```

ステップ3:AAA方式リストを設定します。

AAA Method Listタブに移動し、Authenticationの下でAddを選択し、Typeに「login」、Group typeに「Group」を指定した方式リスト名を定義し、Assigned Server Groupセクションで設定した認証サーバグループをマッピングします。



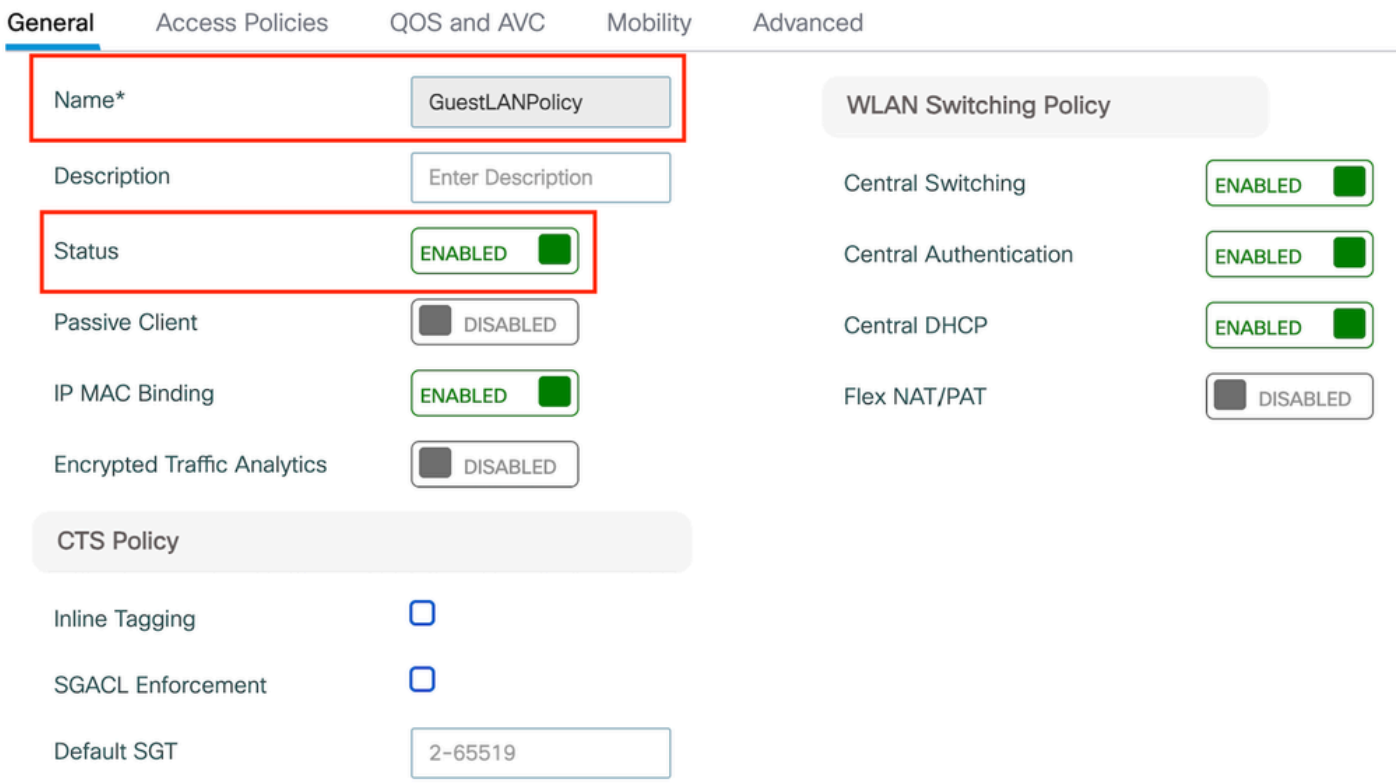
認証方式リスト

CLI での設定

```
aaa authentication login ISE-List group ISE-Group
```

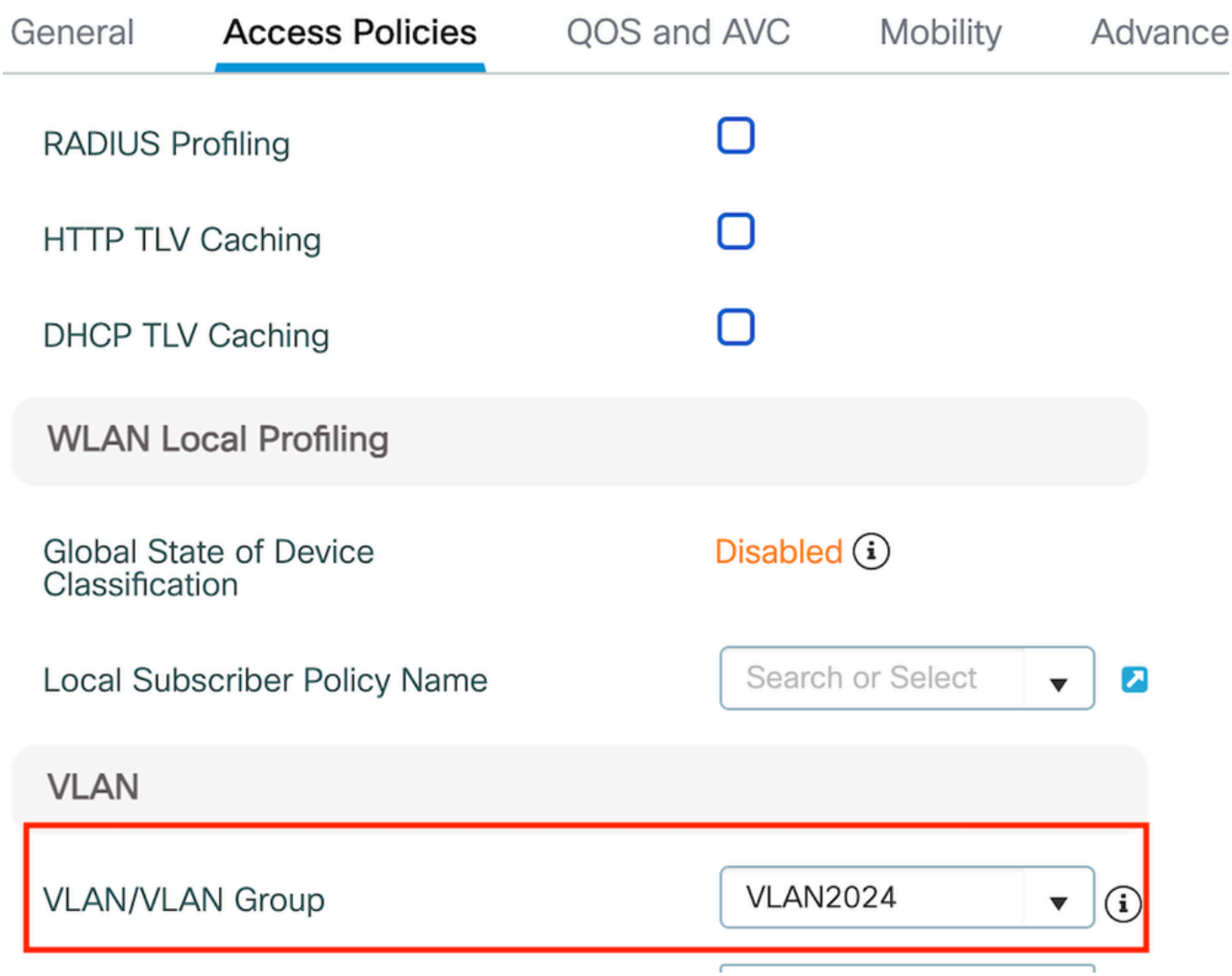
ポリシープロファイルの設定

ステップ1:Configuration > Tag & Profiles > Policyの順に移動し、外部コントローラと同じ名前でポリシープロファイルを設定し、プロファイルを有効にします。

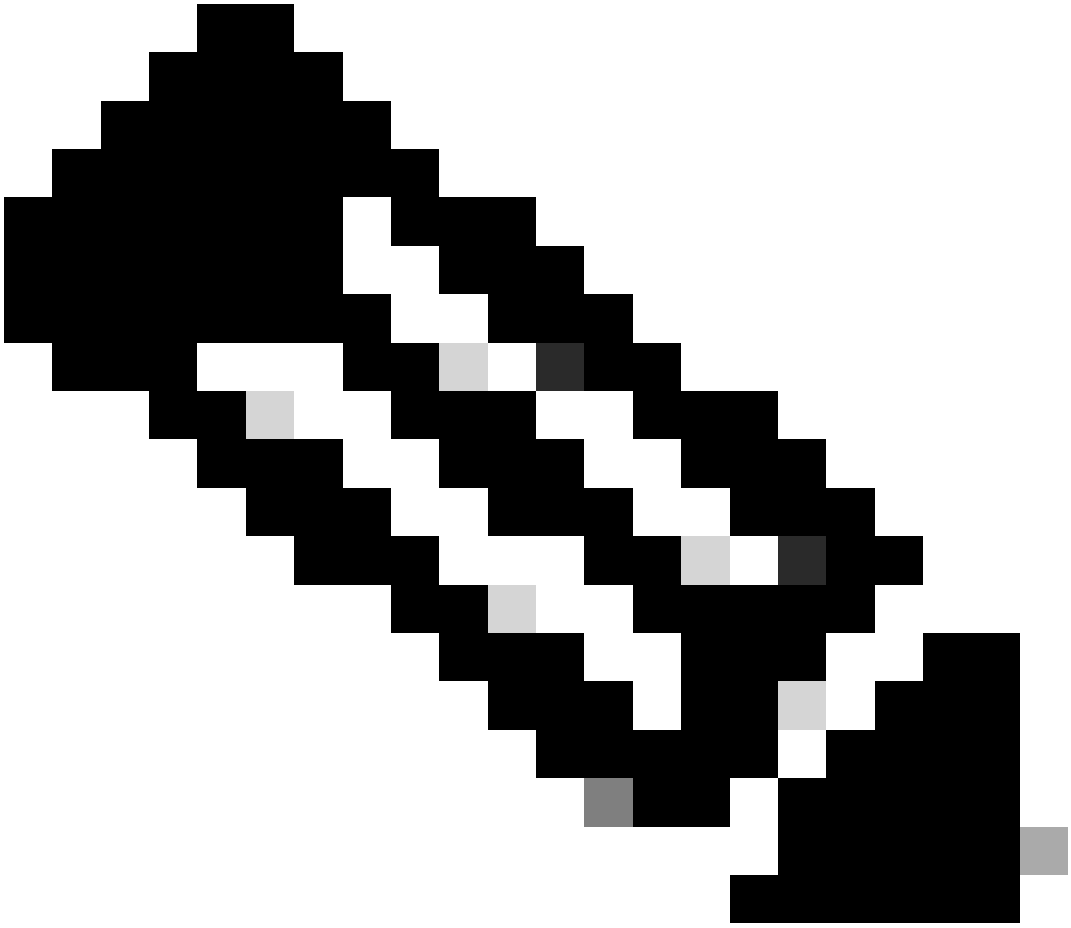


アンカーポリシープロファイル

ステップ2:アクセスポリシーで、ドロップダウンリストから有線クライアントVLANをマッピングします

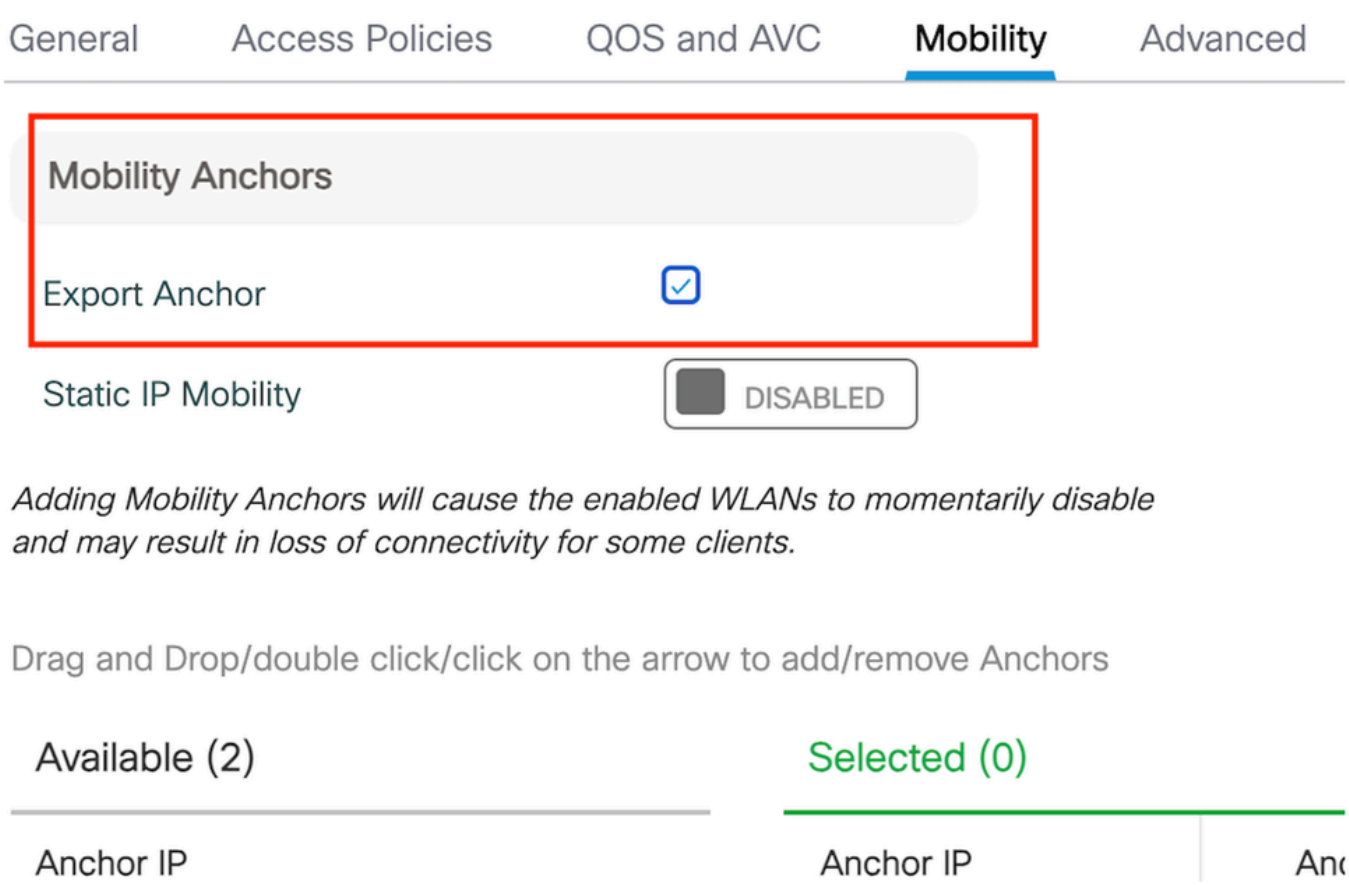


Access Policiesタブ

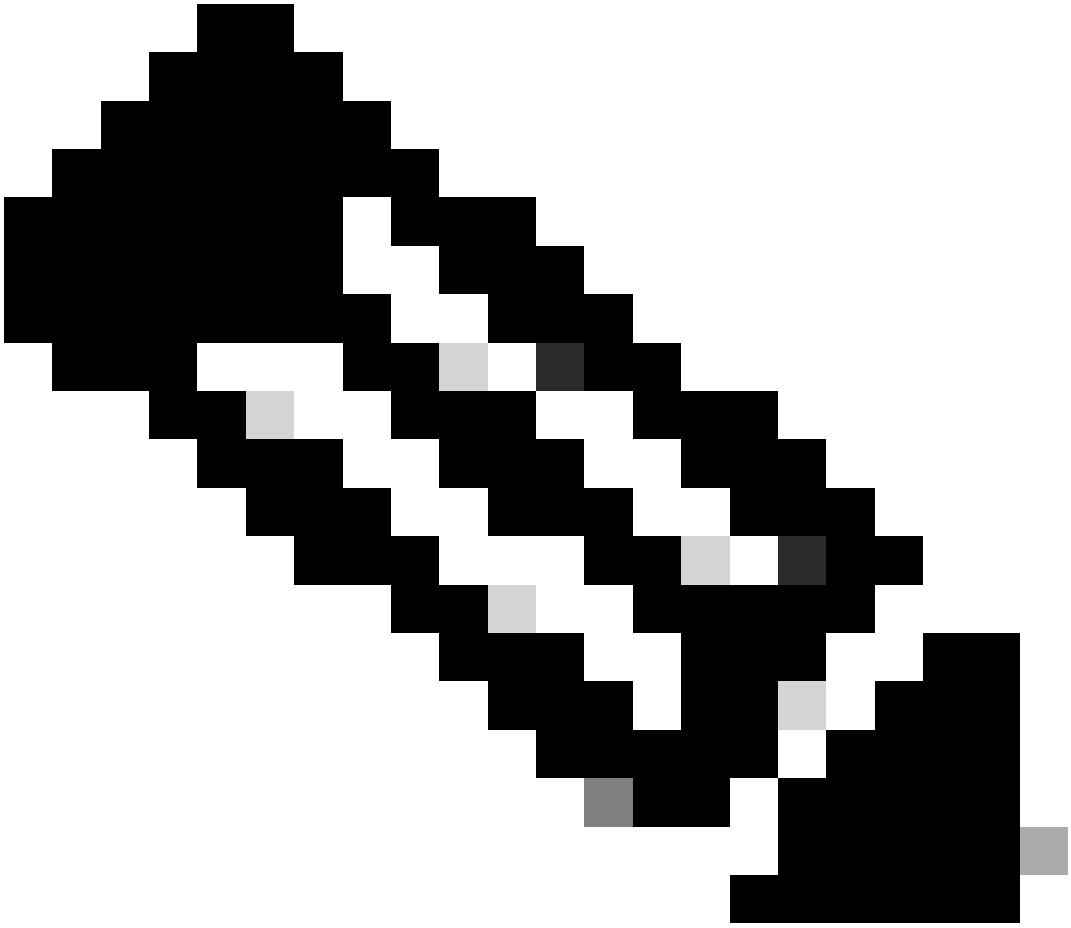


注：ポリシープロファイルの設定は、VLANを除き、外部コントローラとアンカーコントローラの両方で一致している必要があります。

ステップ3:Mobilityタブで、Export Anchorチェックボックスをオンにします。


General
Access Policies
QOS and AVC
Mobility
Advanced
Mobility Anchors
Export Anchor
Static IP Mobility
DISABLED
Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.
Drag and Drop/double click/click on the arrow to add/remove Anchors
Available (2)
Selected (0)
Anchor IP
Anchor IP
Anc

アンカーを書き出し



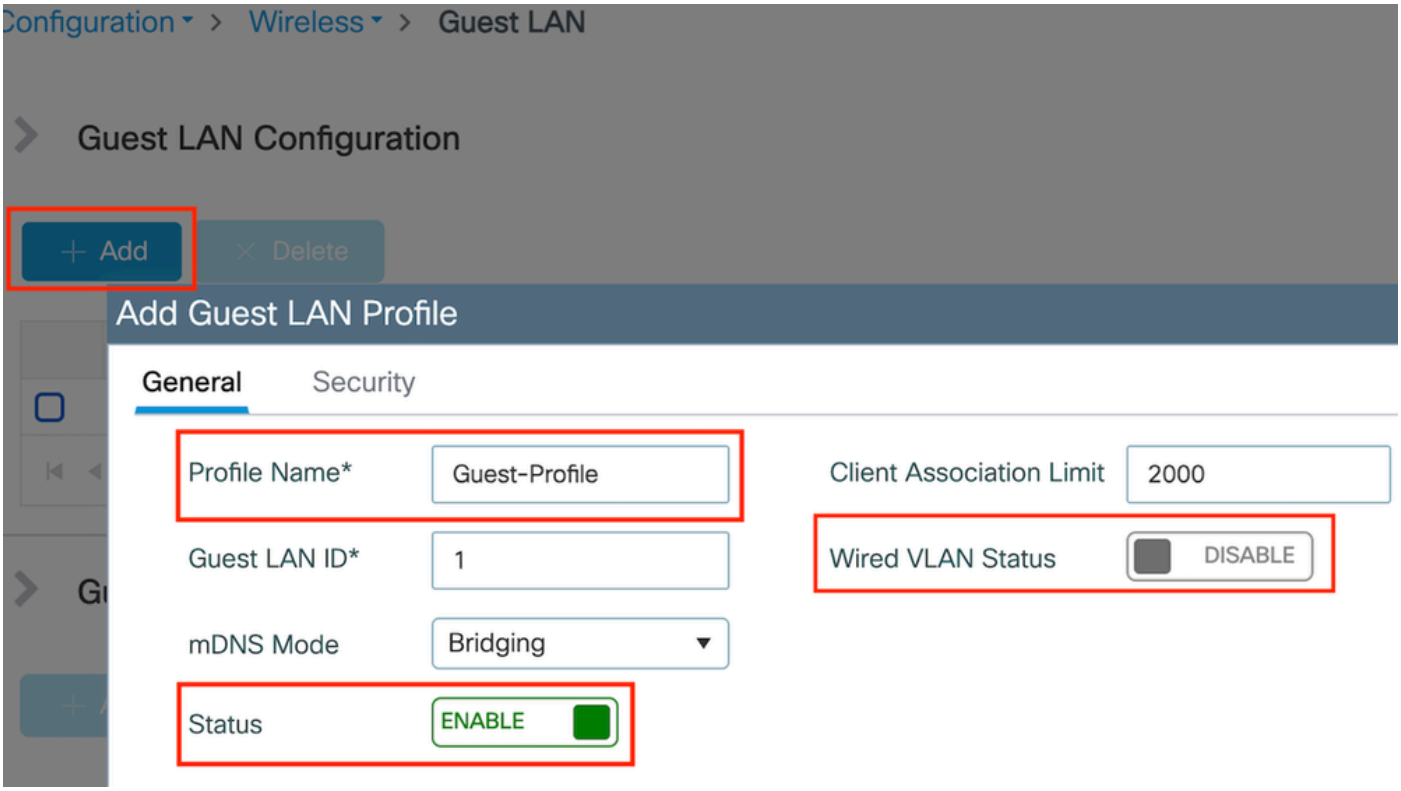
注：この設定では、9800ワイヤレスLANコントローラ(WLC)を、指定したポリシープロファイルに関連付けられたすべてのWLANのアンカーWLCとして指定します。外部9800 WLCがクライアントをアンカーWLCにリダイレクトする場合、クライアントに割り当てられたWLANとポリシープロファイルに関する詳細が提供されます。これにより、アンカーWLCは、受信した情報に基づいて適切なローカルポリシープロファイルを適用できます。

CLI での設定

```
wireless profile policy GuestLANPolicy
 mobility anchor
 vlan VLAN2024
 no shutdown
```

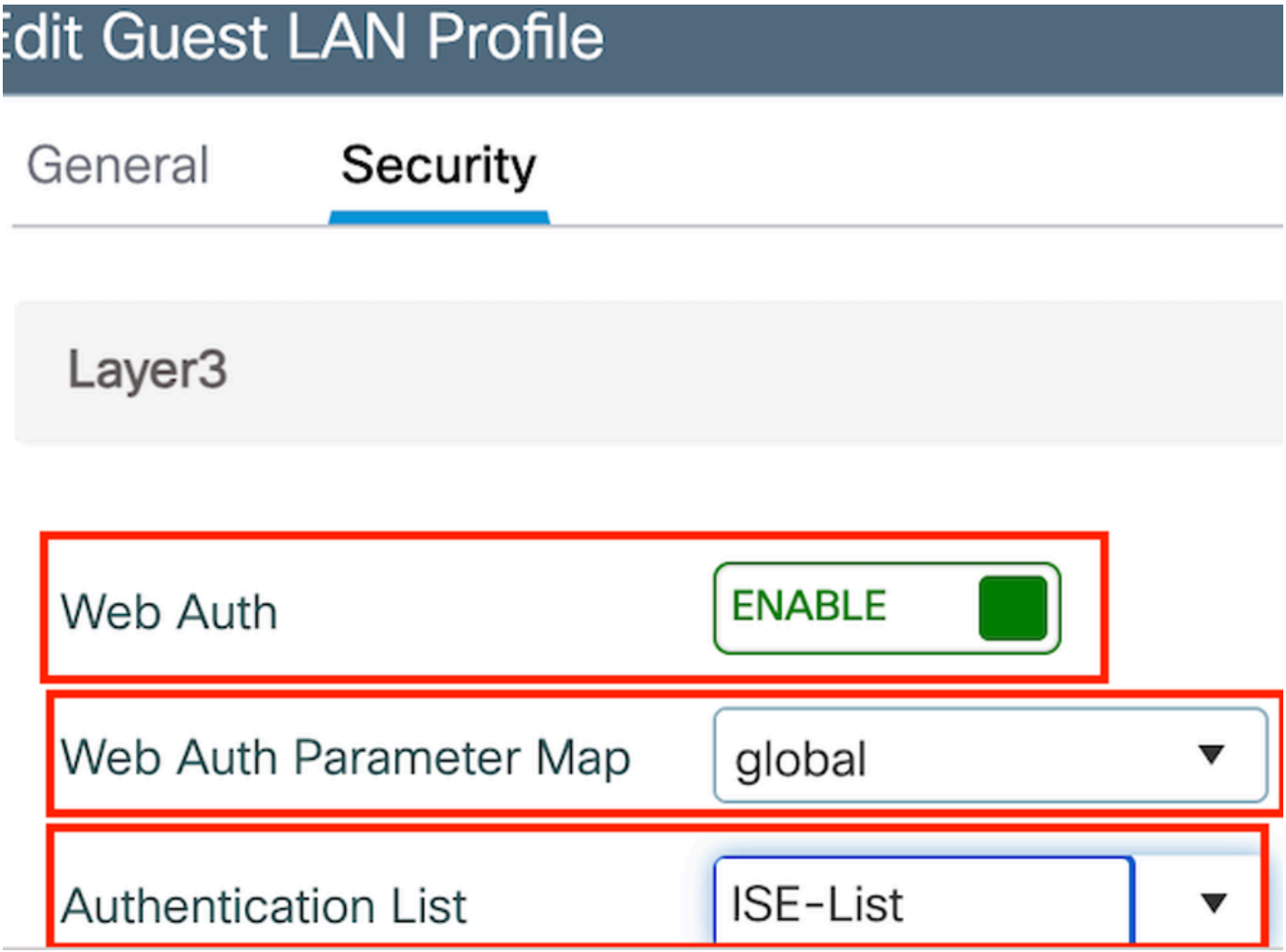
ゲストLANプロファイルの設定

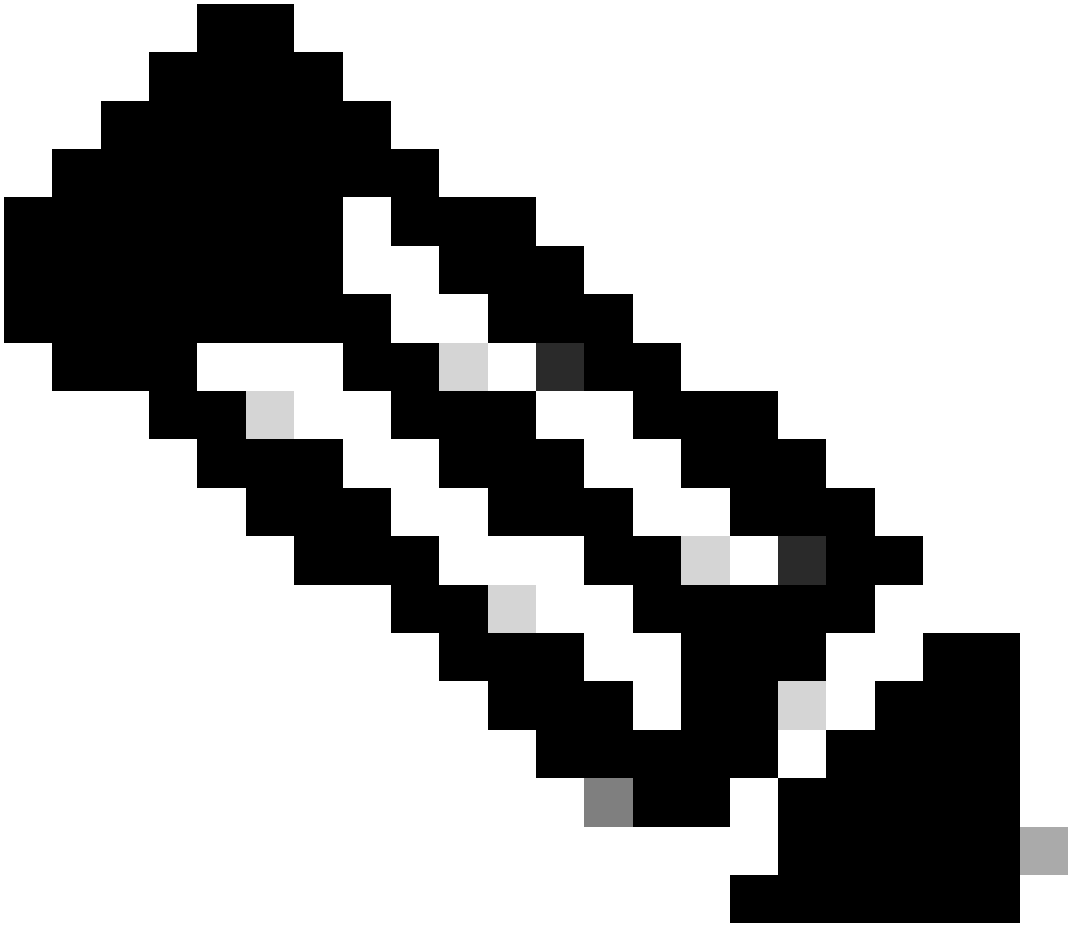
ステップ1:Configuration > Wireless > Guest LANの順に移動し、Addを選択して、ゲストLANプロファイルを作成し、設定します。プロファイル名が外部コントローラのプロファイル名と一致することを確認します。アンカーコントローラでは有線VLANを無効にする必要があります。



ゲストLANプロファイル

ステップ2：セキュリティ設定で、Web Authを有効にし、Web Authパラメータマップと認証リストを設定します。


Edit Guest LAN Profile
General
Security
Layer3
Web Auth
ENABLE
Web Auth Parameter Map
global
Authentication List
ISE-List



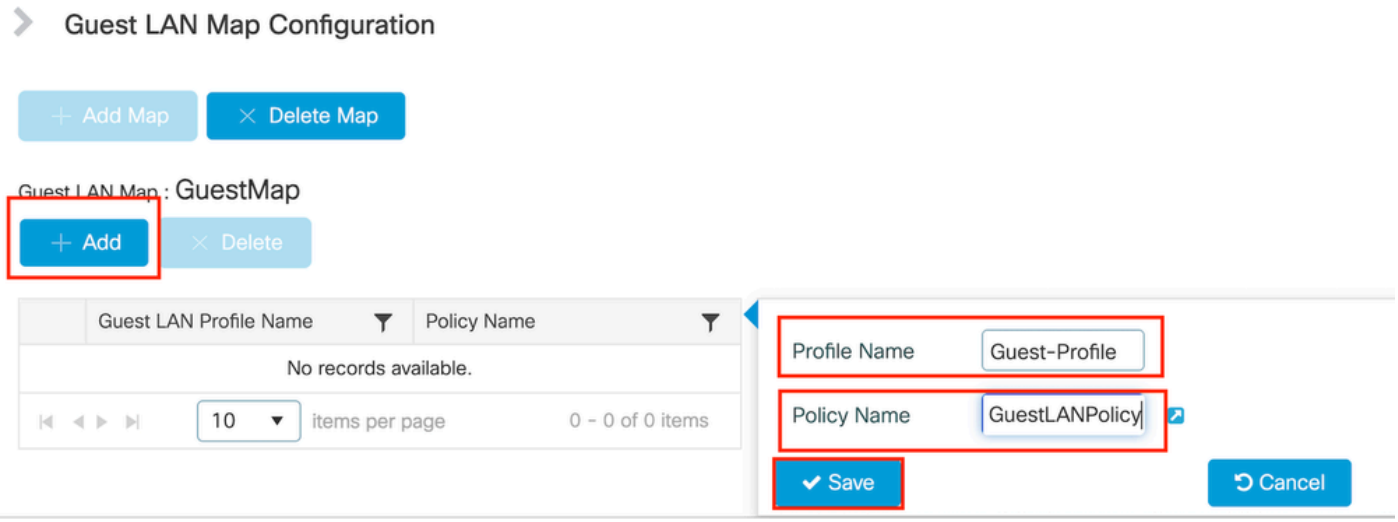
注：ゲストLANプロファイルの設定は、有線VLANステータスを除き、外部コントローラとアンカーコントローラで同じである必要があります

CLI での設定

```
guest-lan profile-name Guest-Profile 1
 security web-auth authentication-list ISE-List
 security web-auth parameter-map global
```

ゲストLANマップ

ステップ1:Configuration > Wireless > Guest LANの順に移動します。Guest LAN MAP configurationセクションでAddを選択し、ポリシープロファイルをゲストLANプロファイルにマッピングします。



ゲストLANマップ

```
wireless guest-lan map GuestMap
guest-lan Guest-Profile policy GuestLANPolicy
```

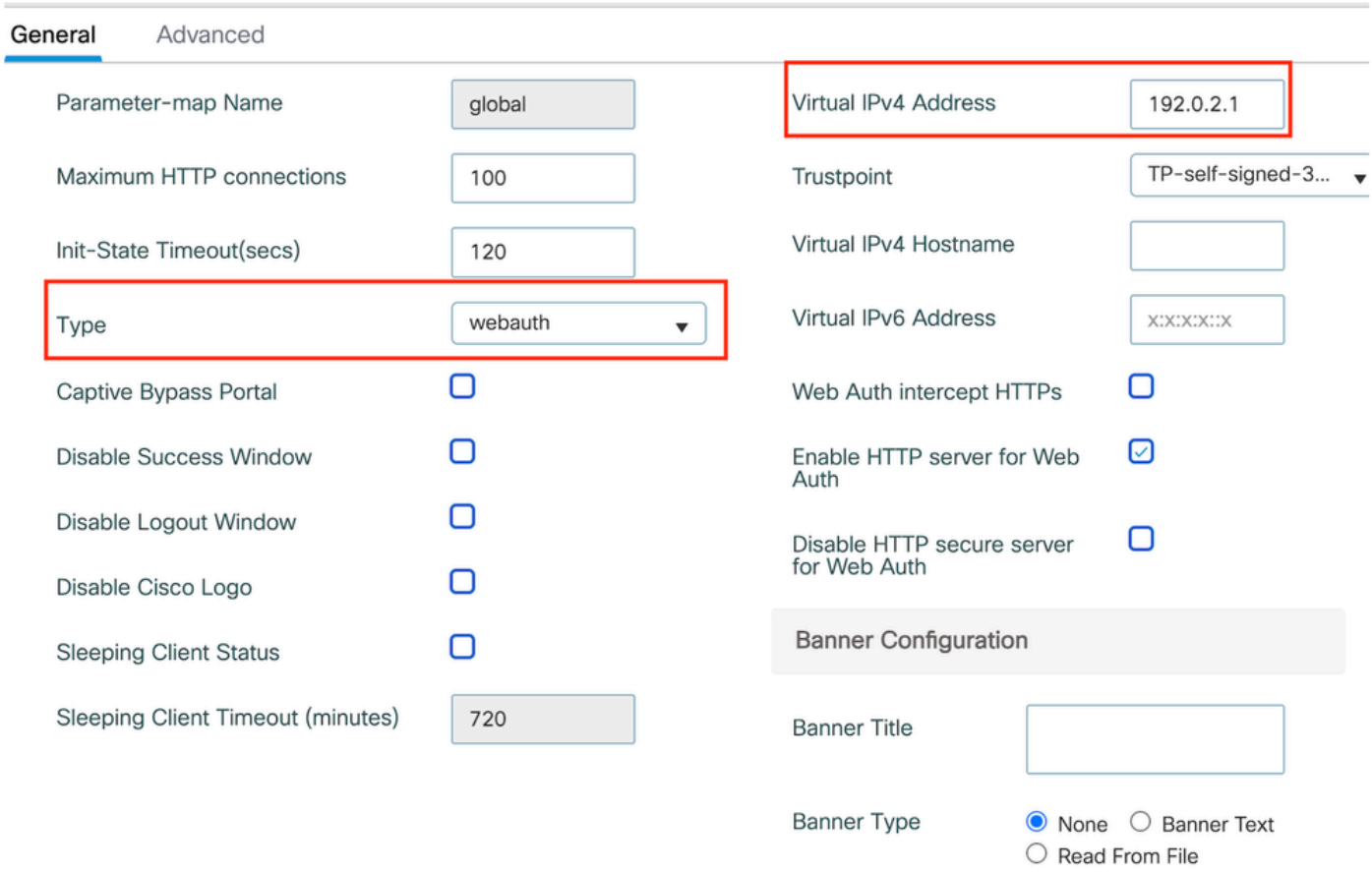
AireOS 5520コントローラにアンカーされたCatalyst 9800での有線ゲストの設定

Network Topology

外部9800 WLC上の設定

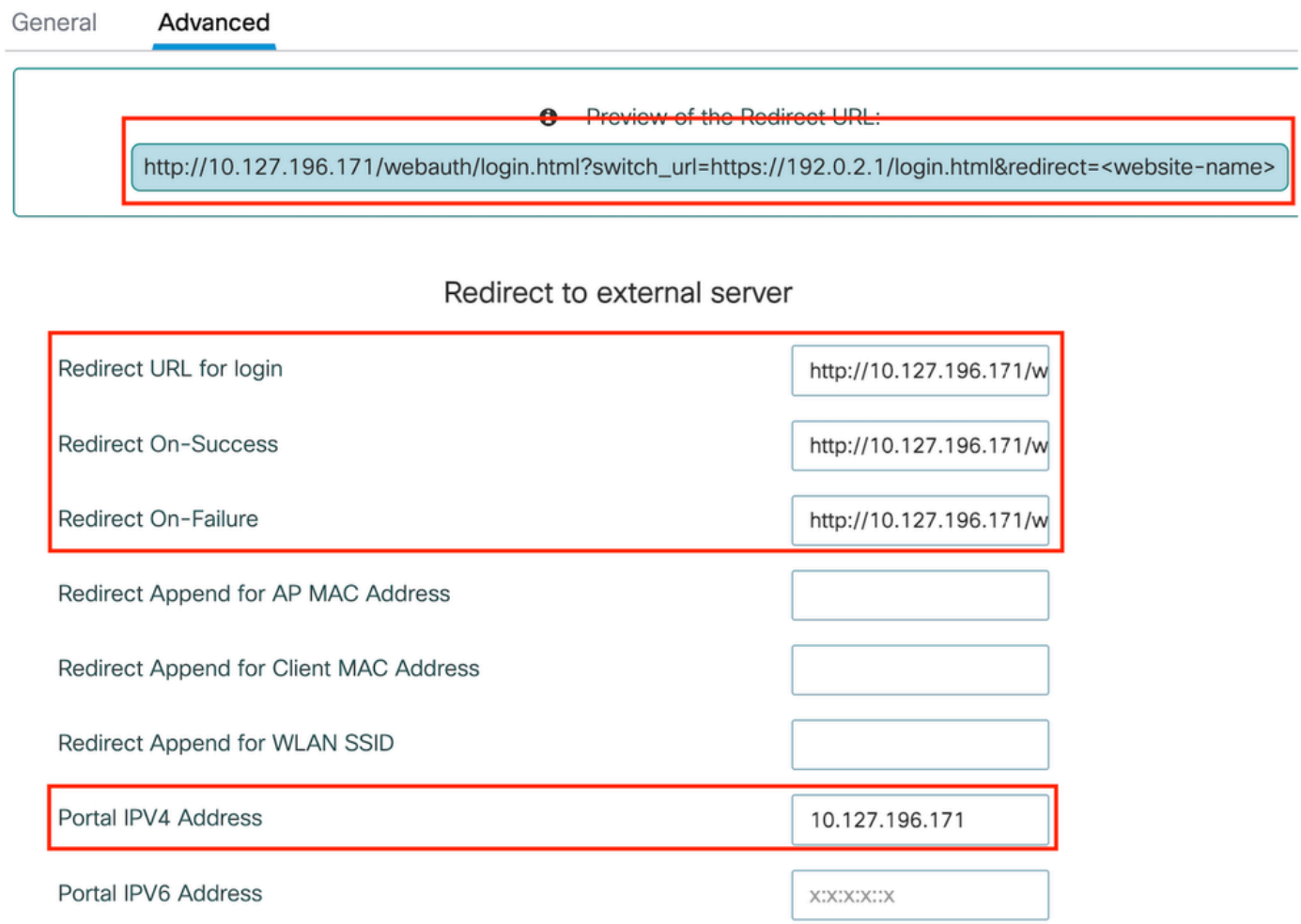
Webパラメータマップの設定

ステップ1:Configuration > Security > Web Authの順に移動し、Globalを選択します。コントローラの仮想IPアドレスとトラストポイントがプロファイル上で正しくマッピングされ、タイプがwebauthに設定されていることを確認します。



Webパラメータマップ

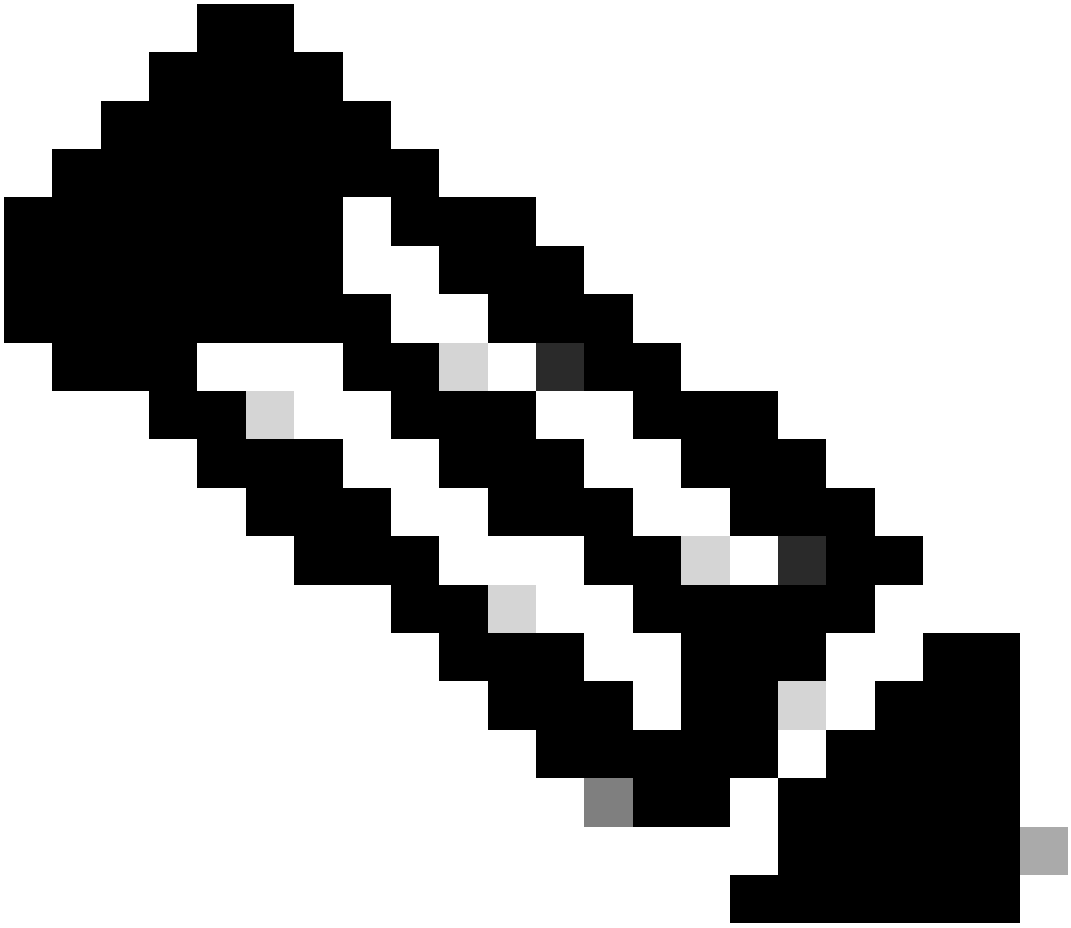
ステップ2:Advancedタブで、クライアントのリダイレクト先となる外部WebページのURLを指定します。ログイン用のリダイレクトURLおよび障害時のリダイレクトを設定します。Redirect On-Success設定はオプションの設定です。



[詳細設定]タブ

CLI での設定

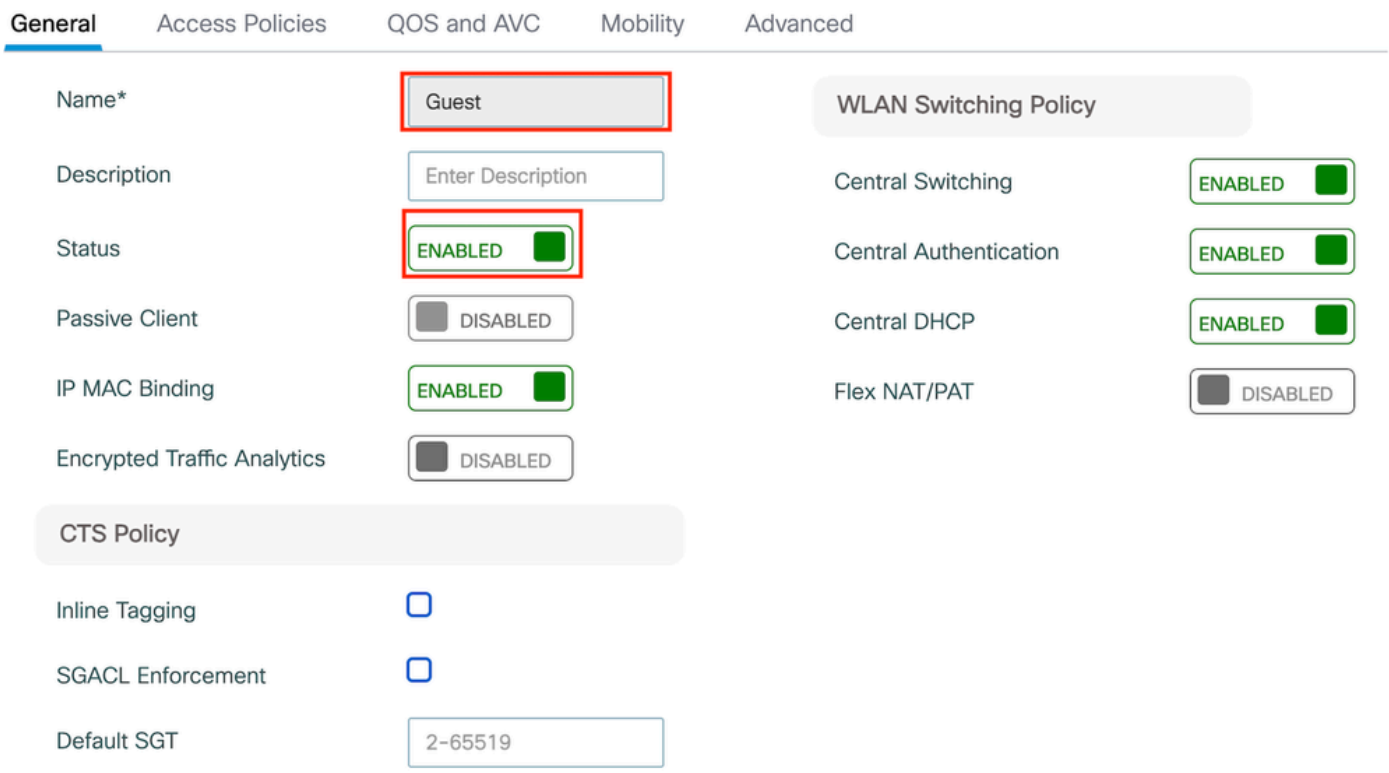
```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171
 trustpoint TP-self-signed-3010594951
 webauth-http-enable
```



注:AAAの設定については、外部9800 WLCの「」セクションの設定の詳細を参照してください。

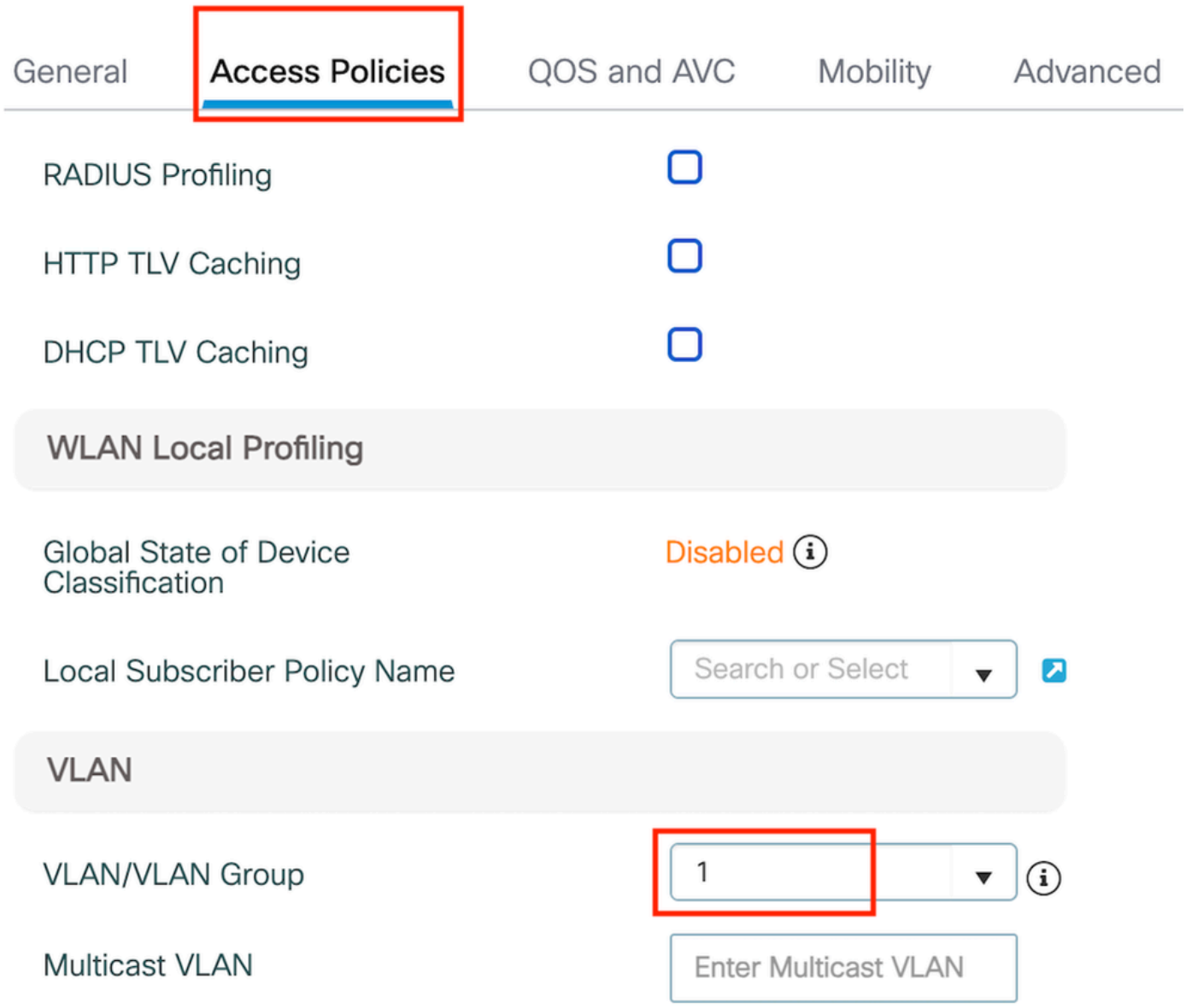
ポリシープロファイルの設定

ステップ1:Configuration > Tags & Profiles > Policyの順に移動します。Addを選択し、Generalタブでプロファイルの名前を指定し、ステータスの切り替えを有効にします。



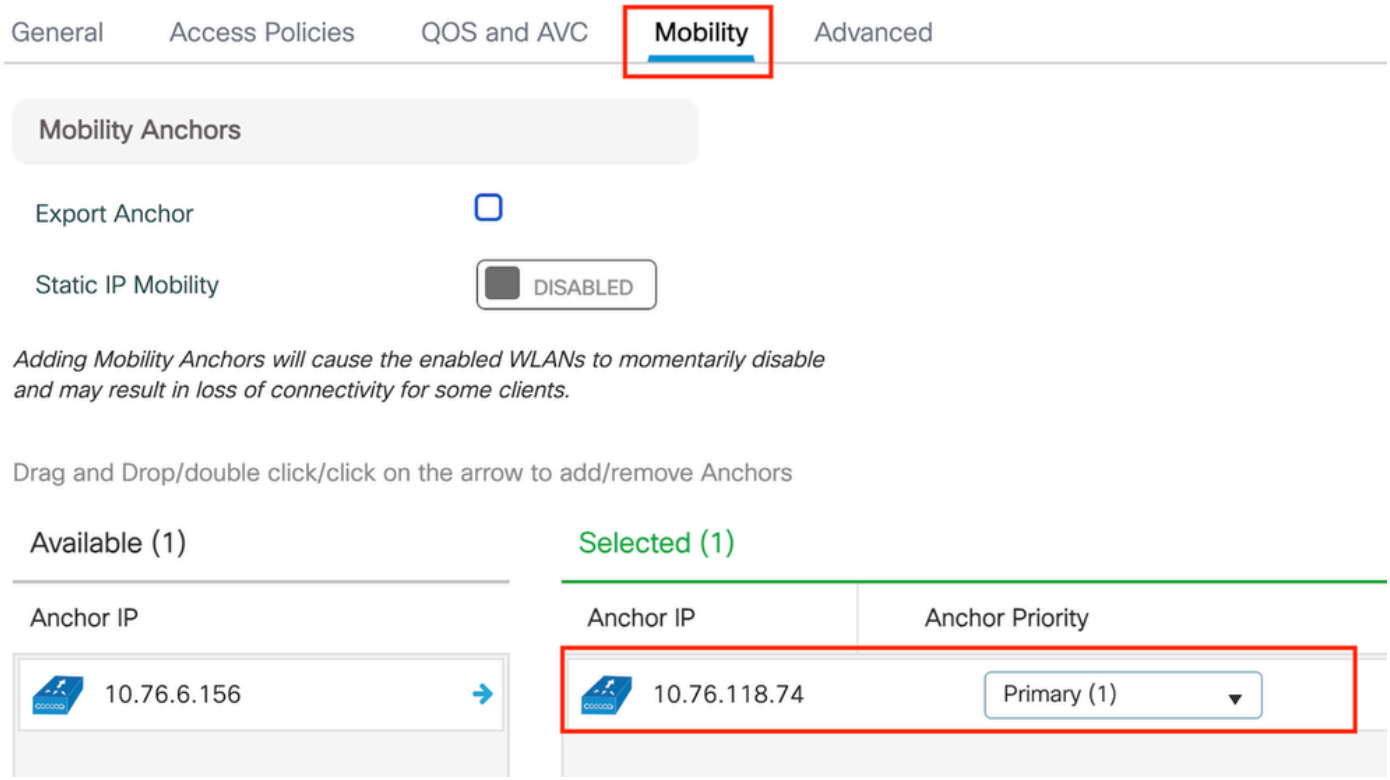
ポリシー プロファイル

ステップ2:Access Policiesタブで、ランダムVLANを割り当てます。

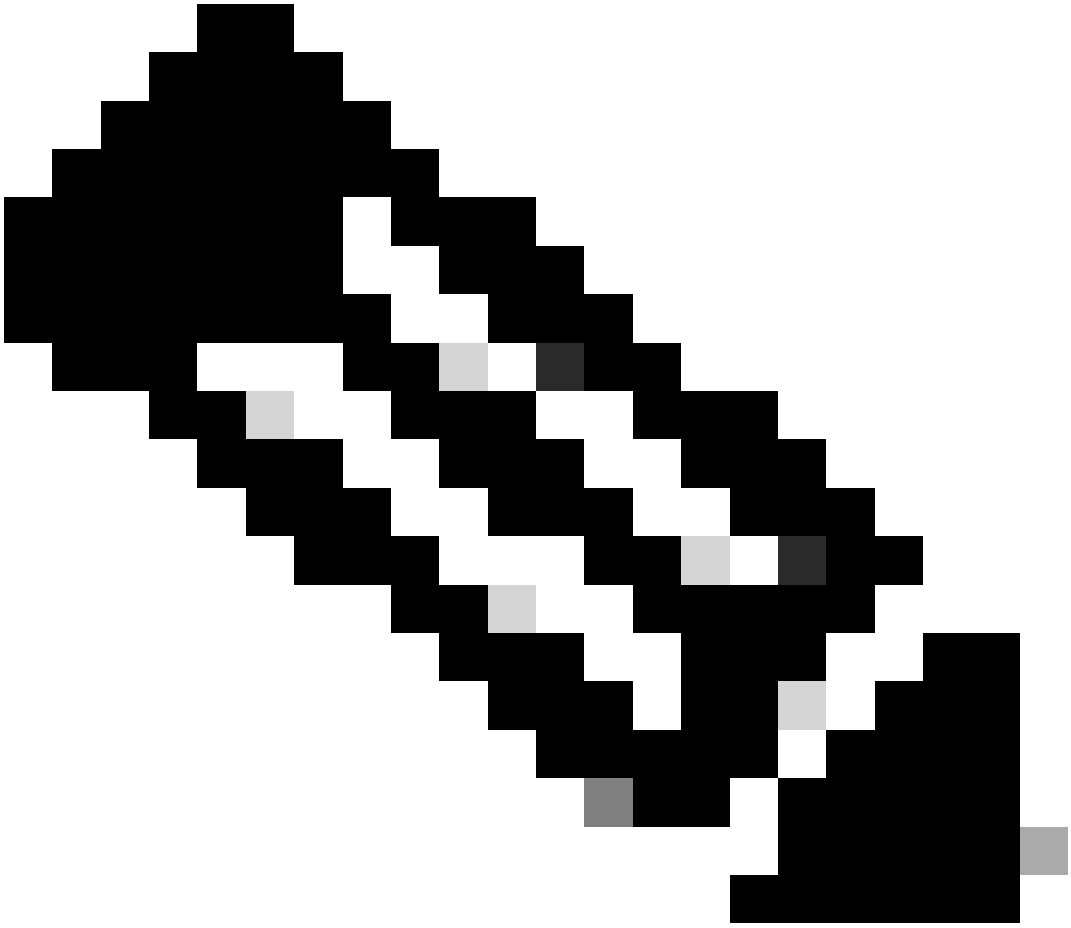


アクセスポリシー

ステップ3:Mobilityタブで、アンカーコントローラを切り替えて優先度をPrimary (1)に設定します。


General
Access Policies
QOS and AVC
Mobility
Advanced
Mobility Anchors
Export Anchor
Static IP Mobility
DISABLED
Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.
Drag and Drop/double click/click on the arrow to add/remove Anchors
Available (1)
Anchor IP
10.76.6.156
Selected (1)
Anchor IP
Anchor Priority
10.76.118.74
Primary (1)

Mobilityタブ



注:9800外部WLCのポリシープロファイルは、VLAN設定を除き、5520アンカーWLCのゲストLANプロファイルと一致する必要があります

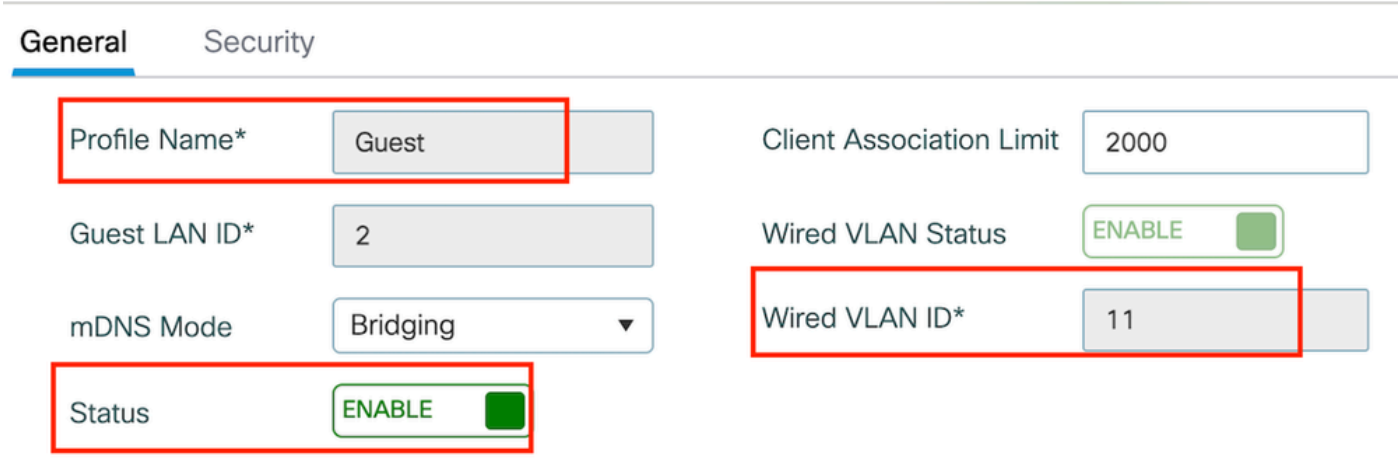
CLI での設定

```
wireless profile policy Guest
 no accounting-interim
 exclusionlist timeout 180
 no flex umbrella dhcp-dns-option
 mobility anchor 10.76.118.74 priority 1
 no shutdown
```

ゲストLANプロファイルの設定

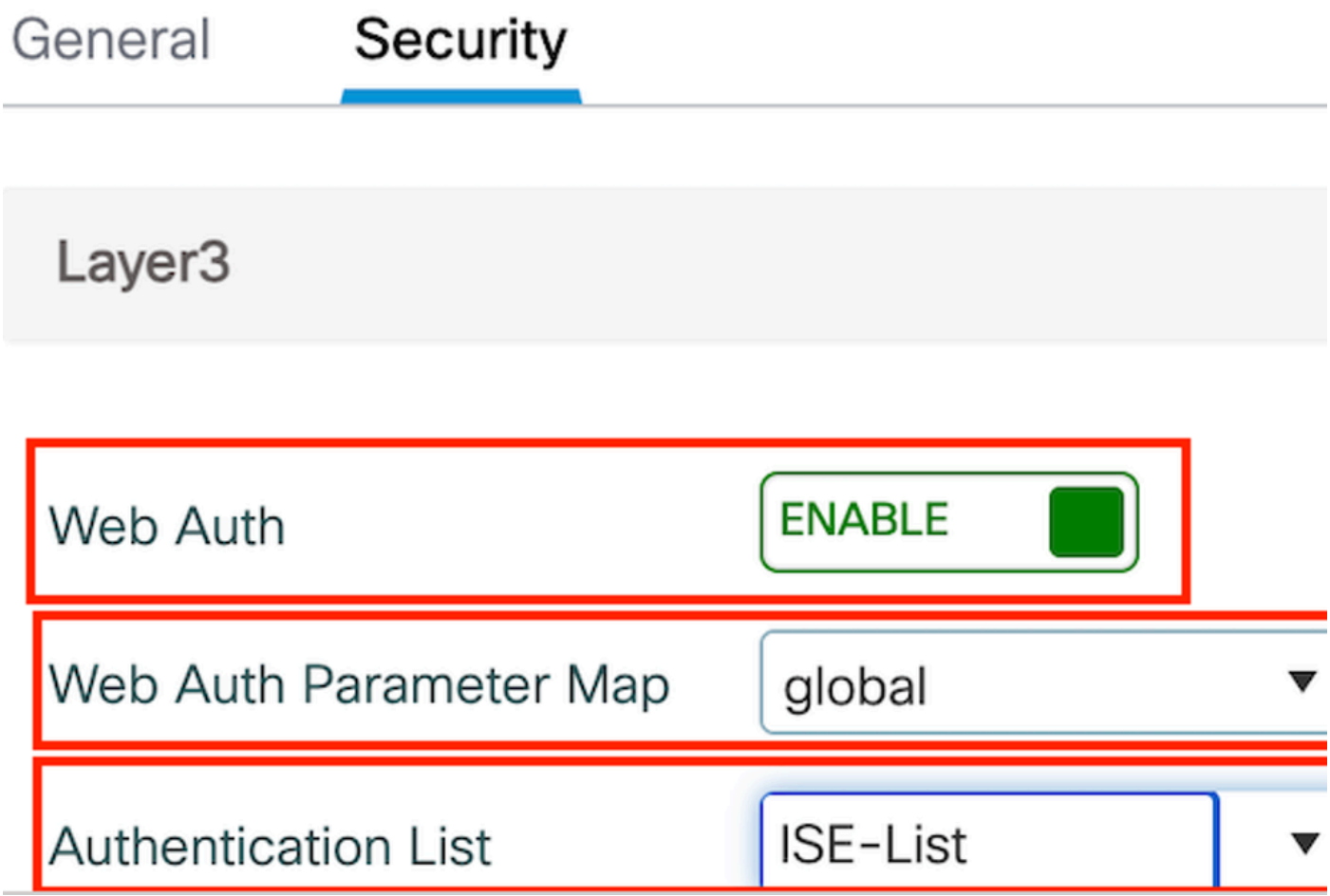
ステップ1:Configuration > Wireless > Guest LANの順に移動し、Addを選択します。一意のプロフ

ァイル名を設定して有線VLANを有効にし、有線ゲストユーザ専用のVLAN IDを指定します。最後に、プロファイルステータスをEnabledに切り替えます。

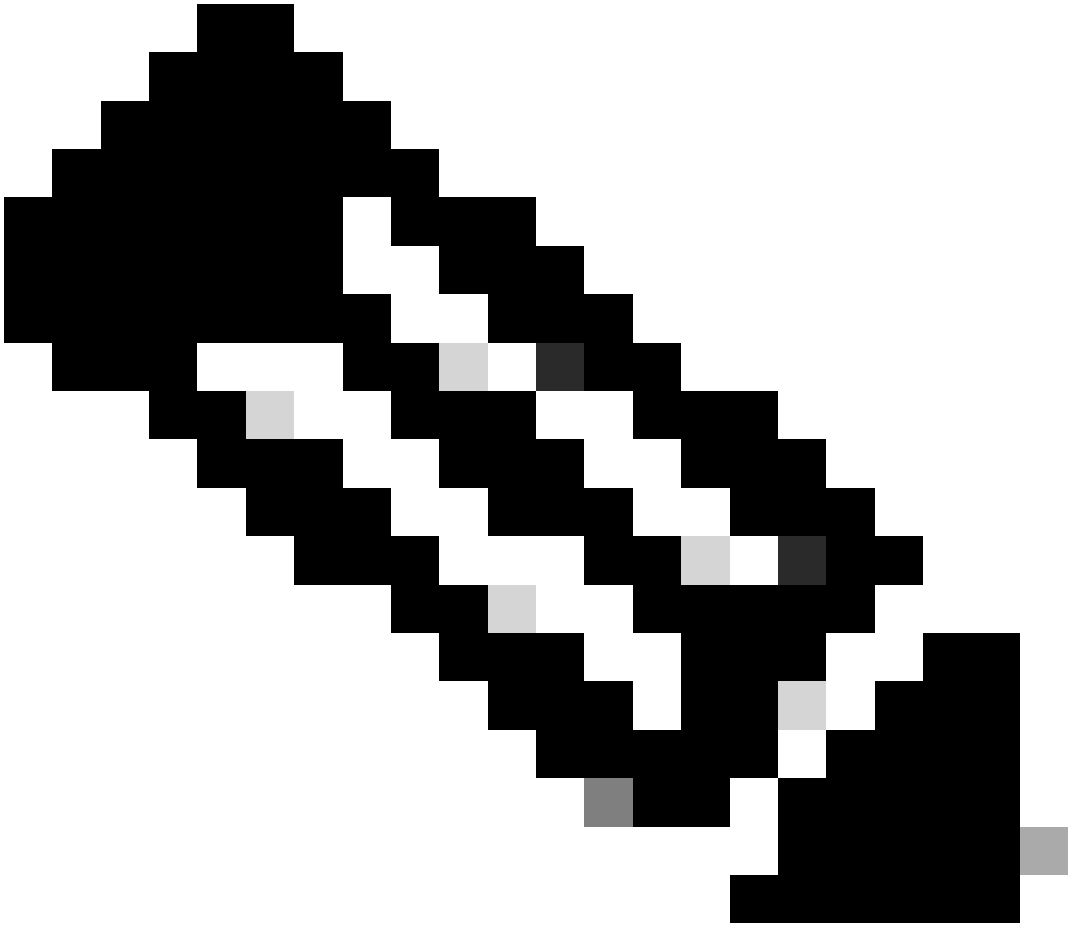


ゲストLANポリシー

ステップ2:Securityタブで、Web Authを有効にし、Web Authパラメータマップをマップして、AuthenticationドロップダウンリストからRADIUSサーバを選択します。



Securityタブ



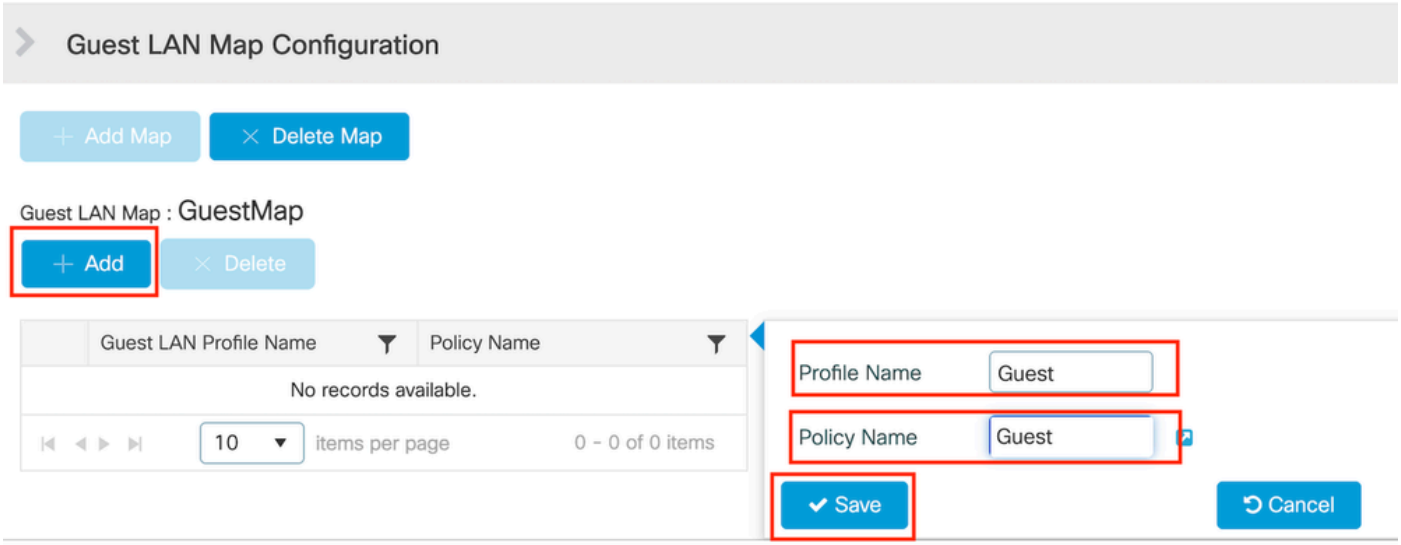
注：ゲストLANプロファイル名は、9800外部コントローラと5520アンカーコントローラで同じである必要があります

CLI での設定

```
guest-lan profile-name Guest 2 wired-vlan 11
 security web-auth authentication-list ISE-List
 security web-auth parameter-map global
```

ゲストLANマップ

ステップ1:Configuration > Wireless > Guest LANの順に移動します。Guest LAN MAP設定セクションで、Addを選択し、ポリシープロファイルをゲストLANプロファイルにマッピングします。



ゲストLANマップ

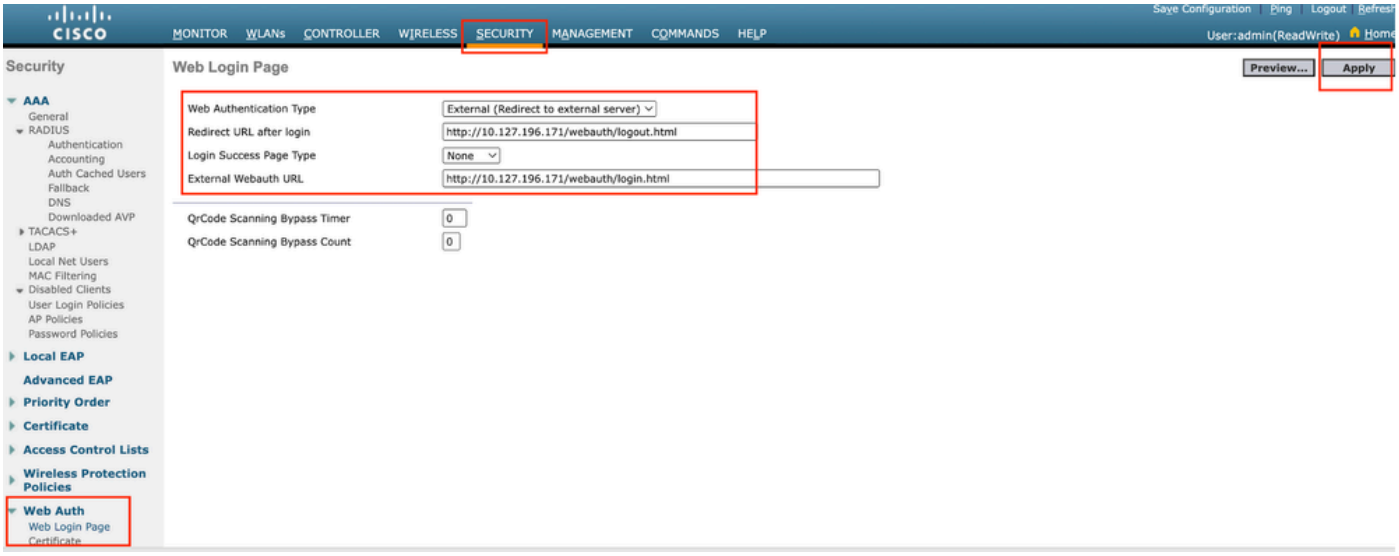
CLI での設定

```
wireless guest-lan map GuestMap
 guest-lan Guest policy Guest
```

アンカー5520 WLCでの設定

Web認証の設定

ステップ1:Security > Web Auth > Web Login Pageの順に移動します。Web認証タイプをExternal（外部サーバへのリダイレクト）に設定し、外部Web認証URLを設定します。Redirect URL after loginはオプションであり、認証が成功した後にクライアントを専用ページにリダイレクトする必要がある場合に設定できます。

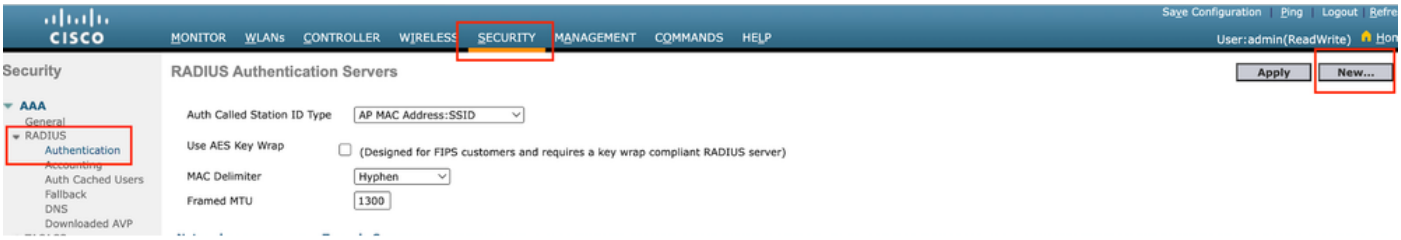


Web認証の設定

AAA設定：

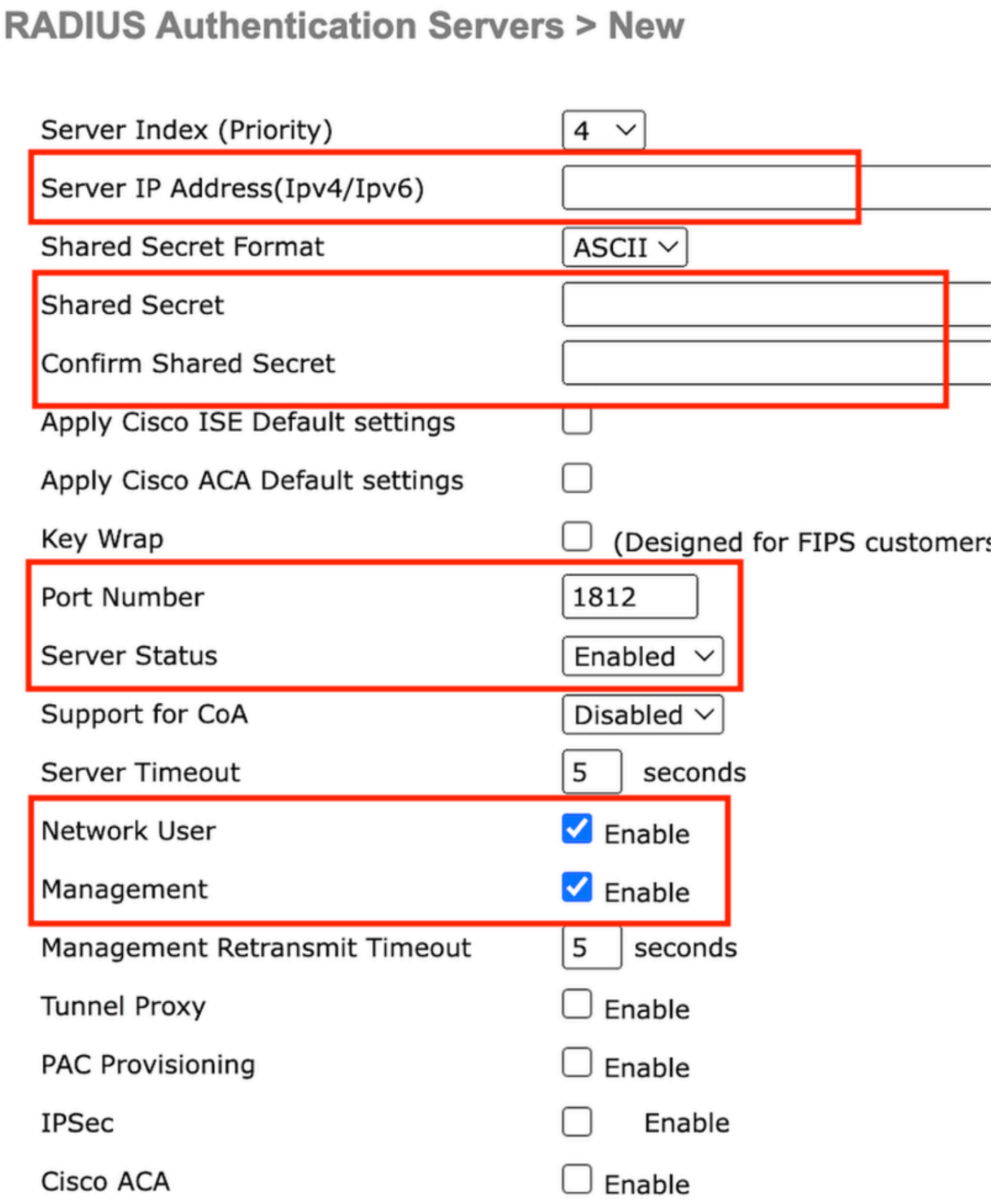
ステップ1:RADIUSサーバを設定します。

Security > Radius > Authentication > Newの順に移動します。



RADIUS サーバ

ステップ2：コントローラでRADIUSサーバのIPと共有秘密を設定します。サーバステータスをEnabledに切り替え、Network Userチェックボックスにチェックマークを付けます。

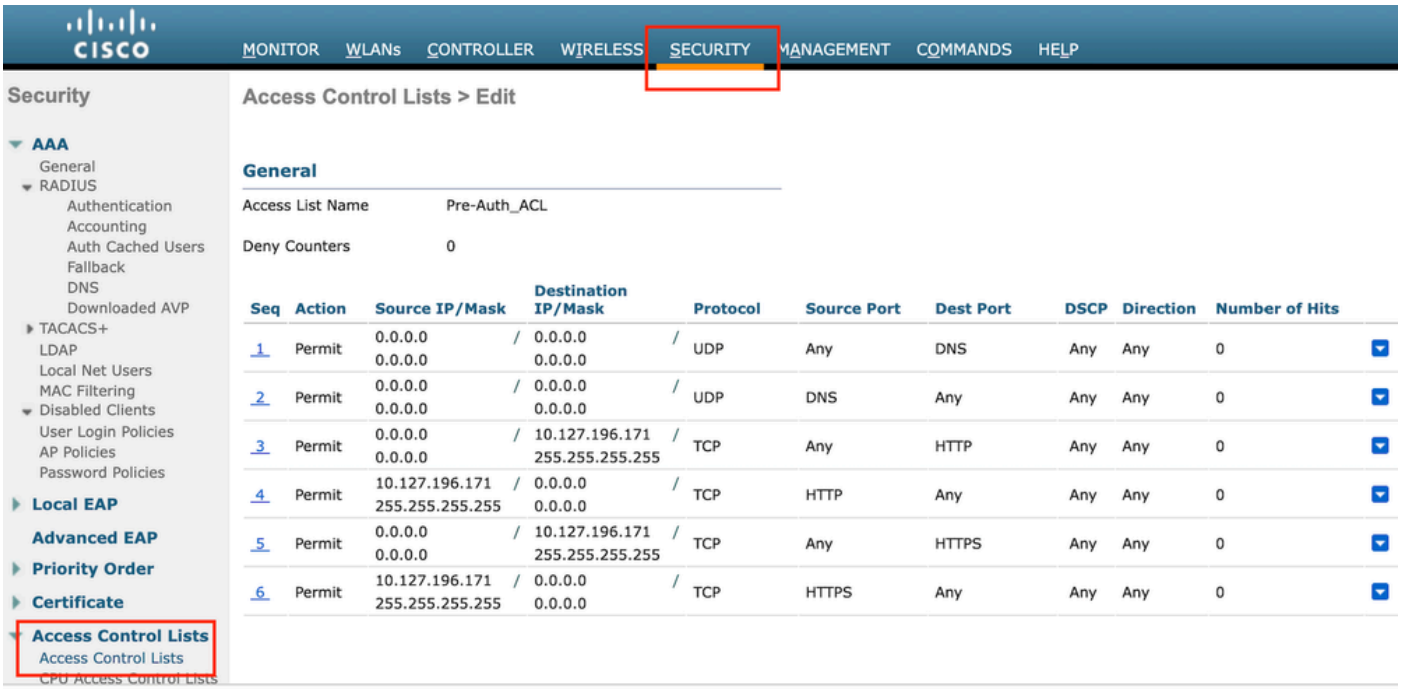


サーバ設定

アクセスコントロールリストの設定

ステップ1:Security > Access Control Listの順に移動し、Newを選択します。DNSおよび外部

Webサーバへのトラフィックを許可する事前認証ACLを作成します。



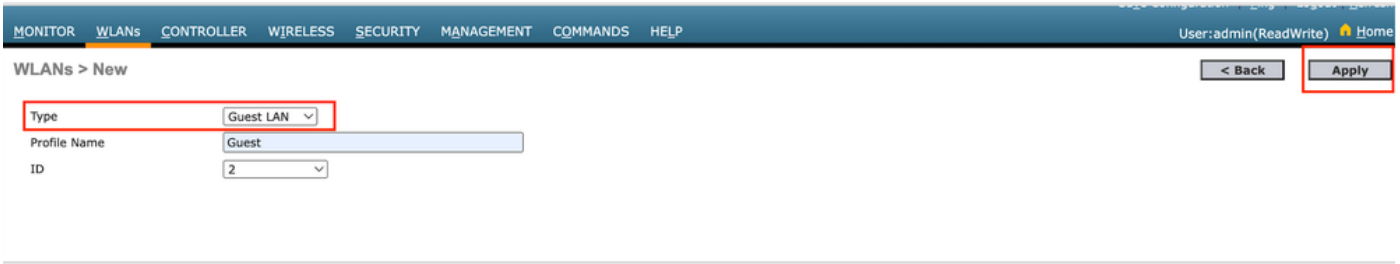
Webサーバへのトラフィックを許可するアクセスリスト

ゲストLANプロファイルの設定

ステップ1:WLANs >に移動し、Create Newを選択します。

Type as Guest LANを選択し、9800外部コントローラのポリシープロファイルと同じ名前を設定します。

ゲストLANの作成



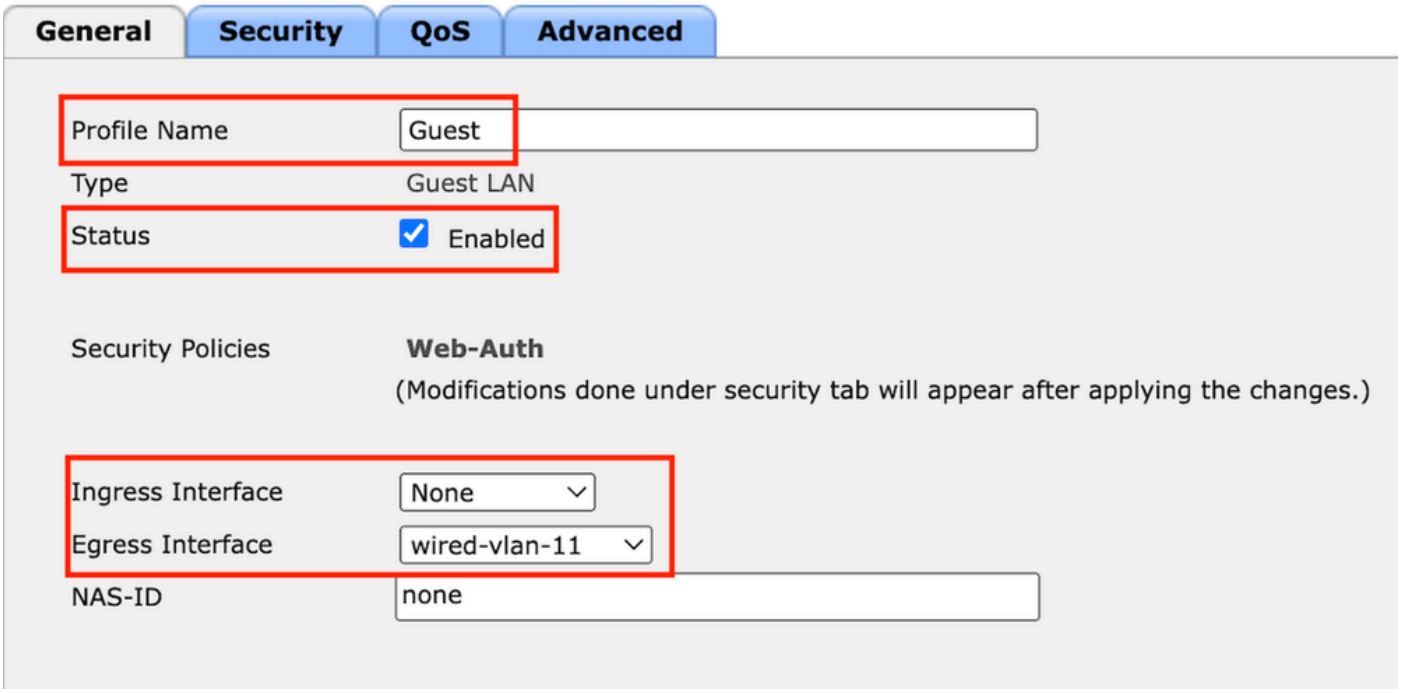
ゲストLANプロファイル

ステップ2：ゲストLANプロファイルの入力および出力インターフェイスをマッピングします。

この場合、入力インターフェイスはnoneです。これは、入力インターフェイスが外部コントロー

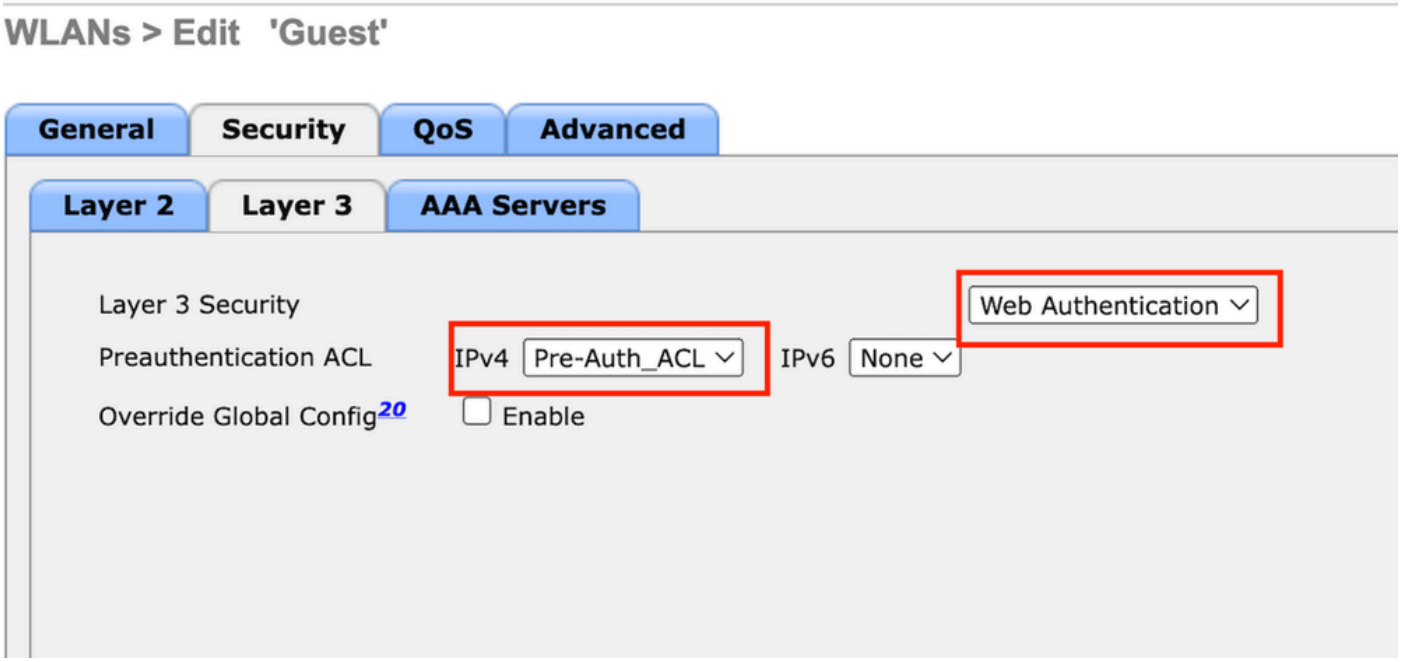
ラからのEoIPトンネルであるためです。

出力インターフェイスは、有線クライアントが物理的に接続するVLANです（ローカルVLANの場合はPVLAN）。



ゲストLANプロファイル

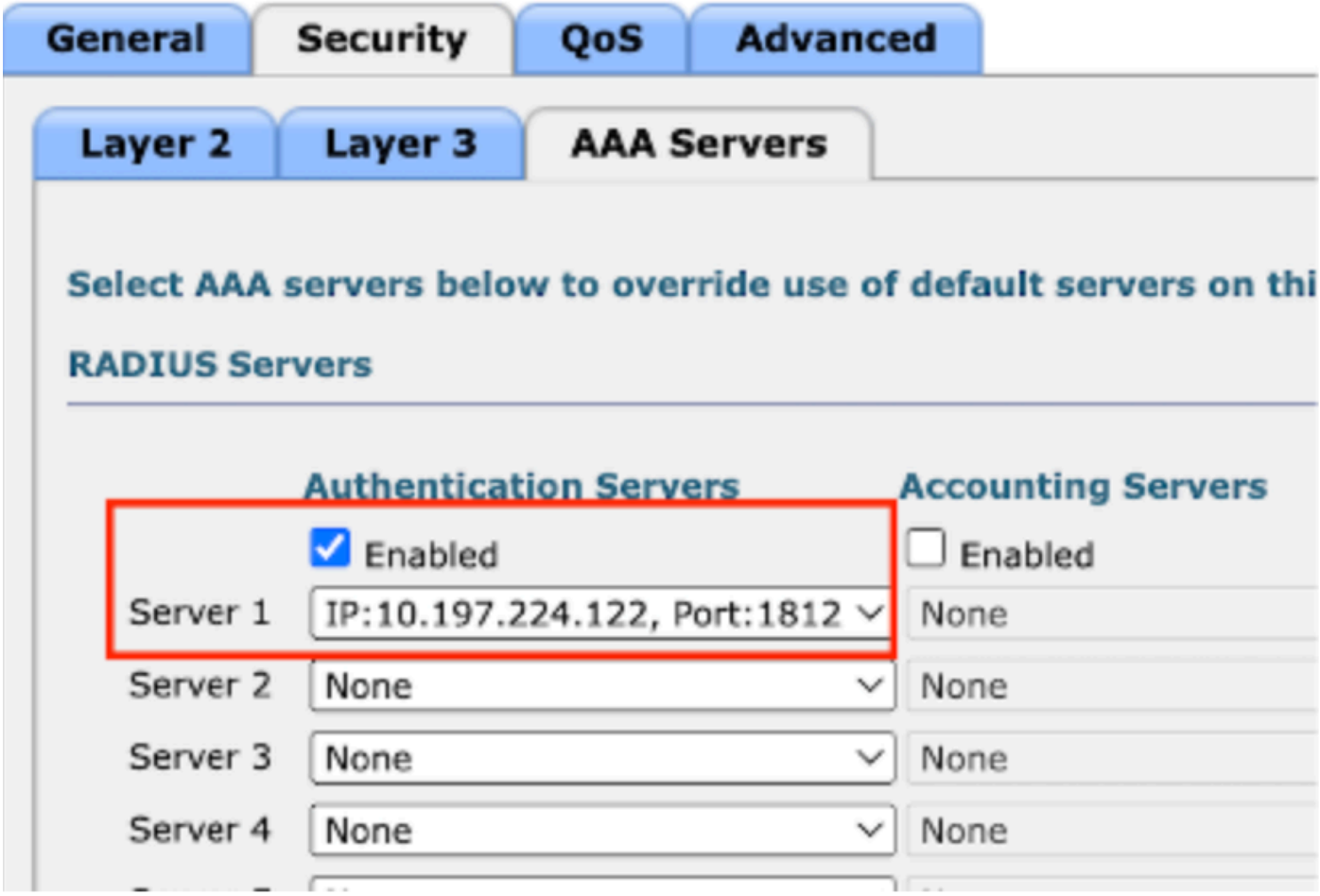
ステップ3:Securityタブで、レイヤ3セキュリティとしてWeb Authenticationを選択し、事前認証ACLをマッピングします。



Guest LAN Securityタブ

ステップ4:Security > AAA Serverの順に移動します。

ドロップダウンを選択し、RADIUSサーバをゲストLANプロファイルにマッピングします。



ゲストLANプロファイルへのRADIUSサーバのマッピング

ステップ5:WLANに移動します。ゲストLANプロファイルのドロップダウンアイコンにカーソルを合わせ、Mobility Anchorsを選択します。

ステップ6:Mobility Anchor Createを選択して、コントローラをこのゲストLANプロファイルのエクスポートアンカーとして設定します。

モビリティアンカーの作成

Catalyst 9800にアンカーされたAireOS 5520で有線ゲストを設定

Network Topology

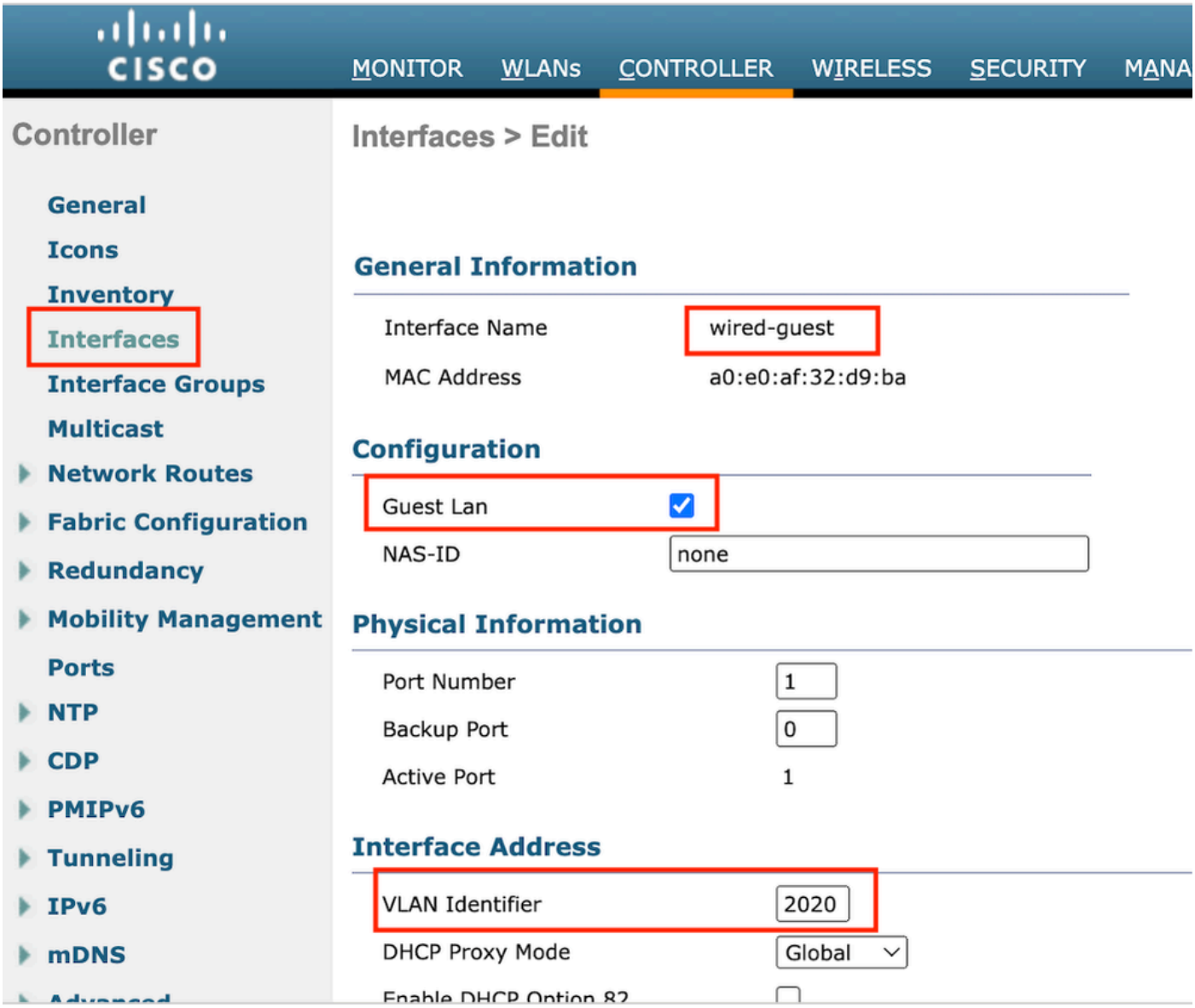
外部5520 WLC上の設定

コントローラインターフェイスの設定

ステップ1:Controller > Interfaces > Newの順に移動します。インターフェイス名、VLAN IDを設定し、ゲストLANを有効にします。

有線ゲストには2つのダイナミックインターフェイスが必要です。

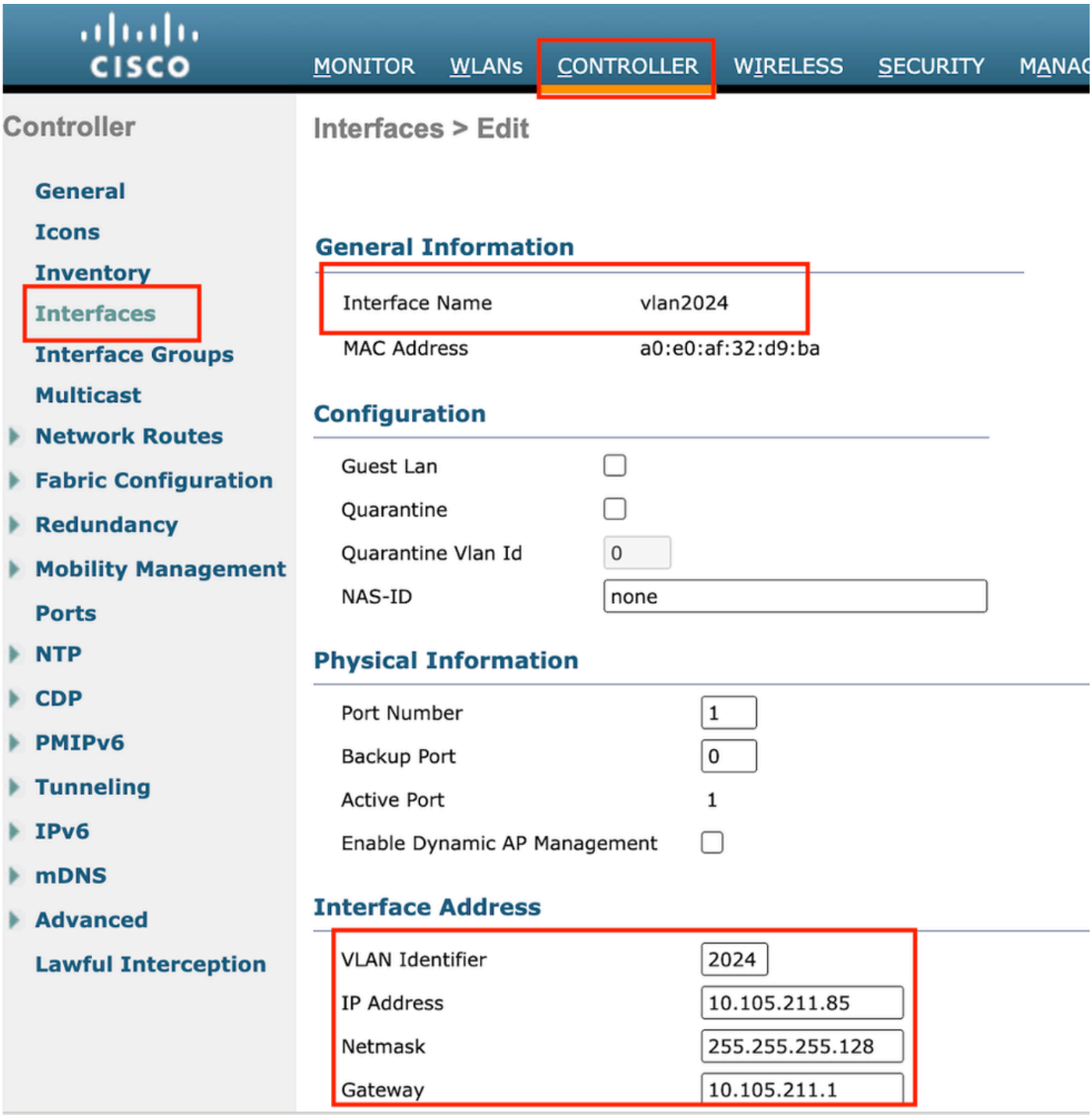
最初に、レイヤ2ダイナミックインターフェイスを作成し、ゲストLANとして指定します。このインターフェイスは、有線クライアントが物理的に接続するゲストLANの入力インターフェイスとして機能します。



入力インターフェイス

ステップ2:Controller > Interfaces > Newの順に移動します。インターフェイス名とVLAN IDを設定します。

2番目のダイナミックインターフェイスはコントローラ上のレイヤ3インターフェイスである必要があり、有線クライアントはこのVLANサブネットからIPアドレスを受信します。このインターフェイスは、ゲストLANプロファイルの出力インターフェイスとして機能します。



出力インターフェイス

スイッチポートの設定

有線ゲストユーザはアクセスレイヤスイッチに接続します。これらの指定ポートは、コントローラでゲストLANが有効になっているVLANで設定する必要があります

アクセスレイヤスイッチポートの設定

インターフェイスギガビットイーサネット<x/x/x>

説明：有線ゲストアクセス

switchport access vlan 2020

switchport mode access

最後

外部コントローラアップリンクポートの設定

インターフェイスTenGigabitEthernet<x/x/x>

説明：外部WLCへのトランクポート

switchport mode trunk

switchport trunk native vlan 2081

switchport trunk allowed vlan 2081,2020

最後

アンカーコントローラアップリンクポートの設定

インターフェイスTenGigabitEthernet<x/x/x>

説明アンカーWLCへのトランクポート

switchport mode trunk

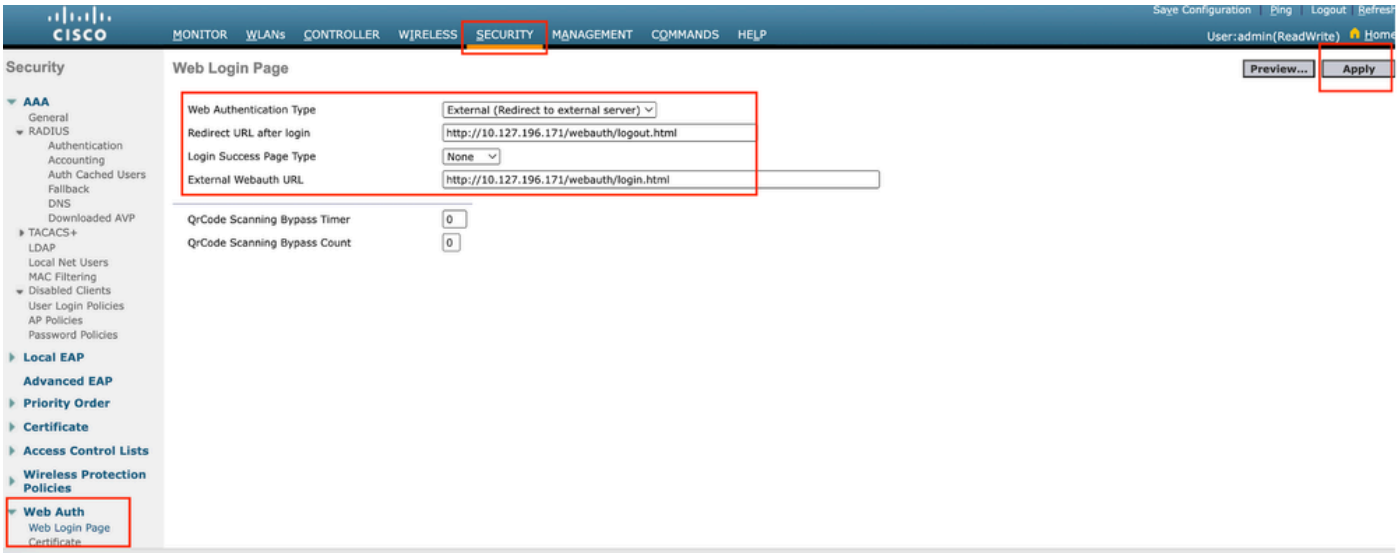
switchport trunk native vlan 2081

switchport trunk allowed vlan 2081,2024

最後

Web認証の設定

ステップ1:Security > Web Auth > Web Login Pageの順に移動します。Web認証タイプをExternal（外部サーバへのリダイレクト）に設定し、外部Web認証URLを設定します。Redirect URL after loginはオプションであり、認証が成功した後にクライアントを専用ページにリダイレクトする必要がある場合に設定できます。

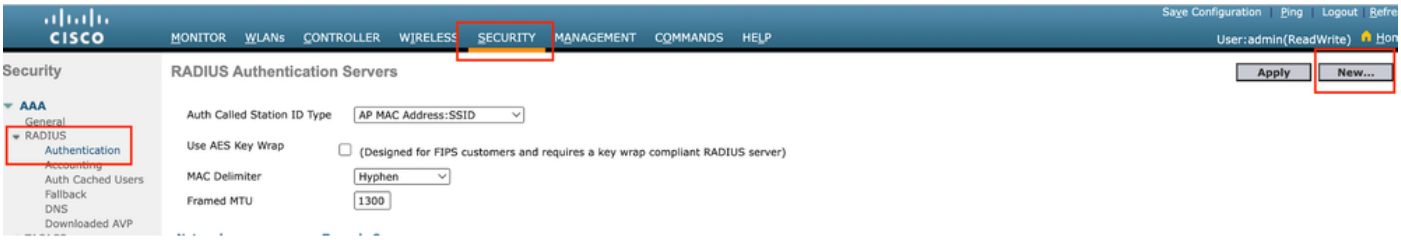


Web認証の設定

AAA設定：

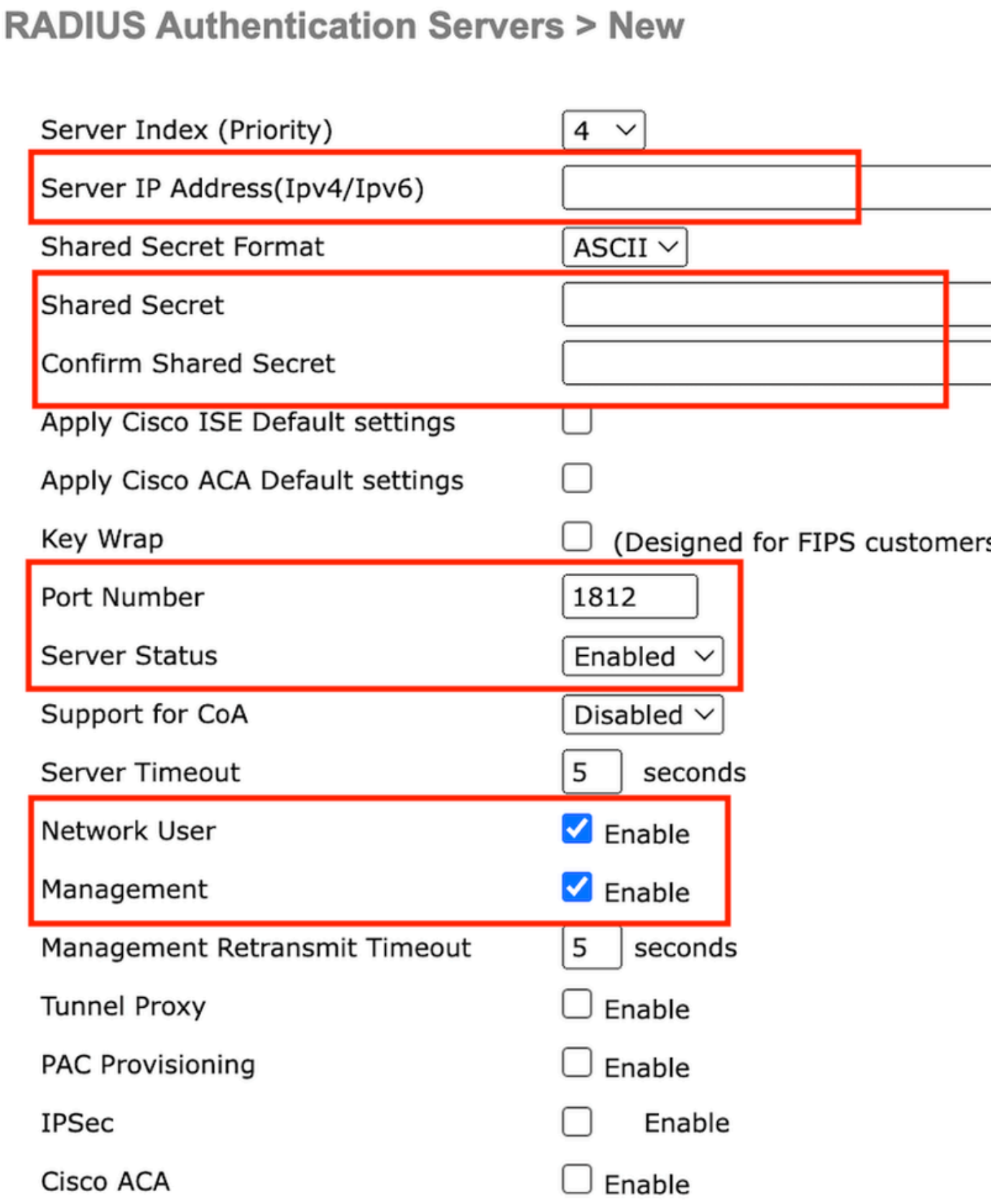
ステップ1:RADIUSサーバを設定します。

Security > Radius > Authentication > Newの順に移動します。



RADIUS サーバ

ステップ2：コントローラでRADIUSサーバのIPと共有秘密を設定します。サーバステータスをEnabledに切り替え、Network Userチェックボックスにチェックマークを付けます。

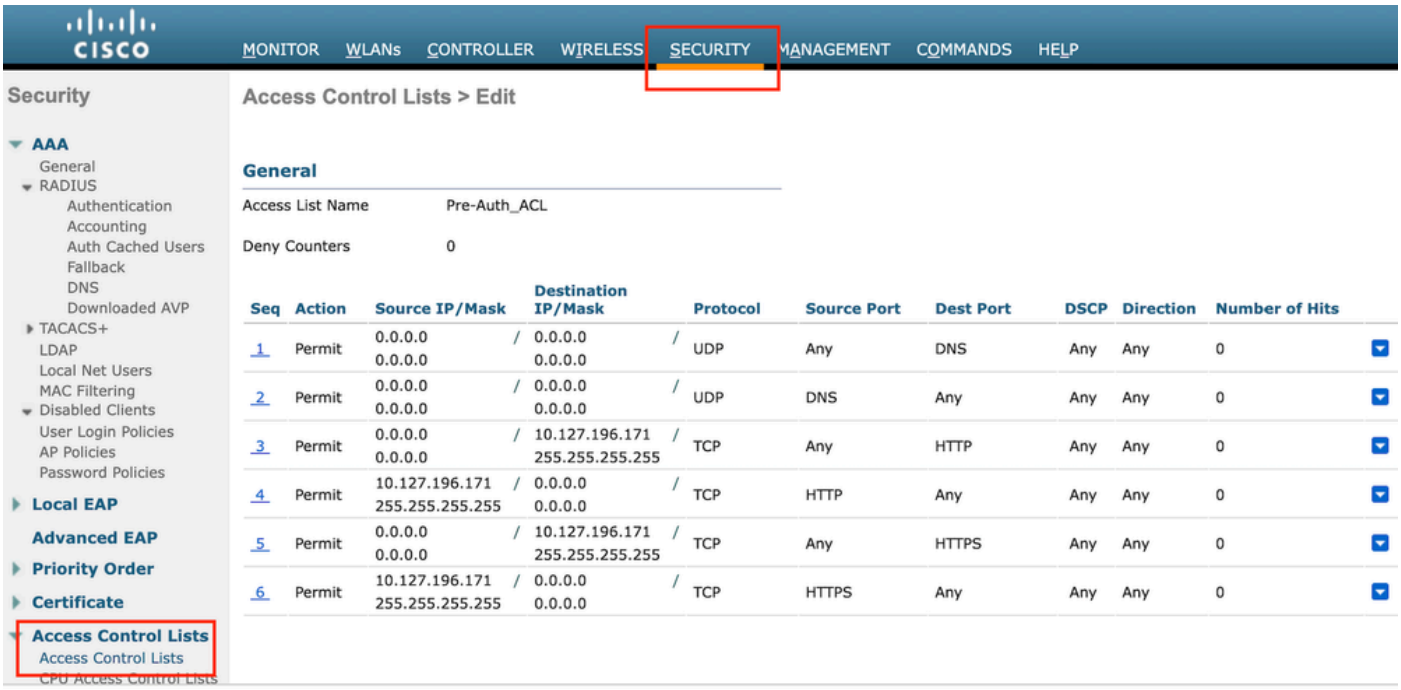


サーバ設定

アクセスコントロールリストの設定

ステップ1:Security > Access Control Listの順に移動し、Newを選択します。DNSおよび外部

Webサーバへのトラフィックを許可する事前認証ACLを作成します。



Webサーバへのトラフィックを許可するアクセスリスト

ゲストLANプロファイルの設定

ステップ1:WLAN > Create New > Goの順に移動します。

ゲストLANプロファイル

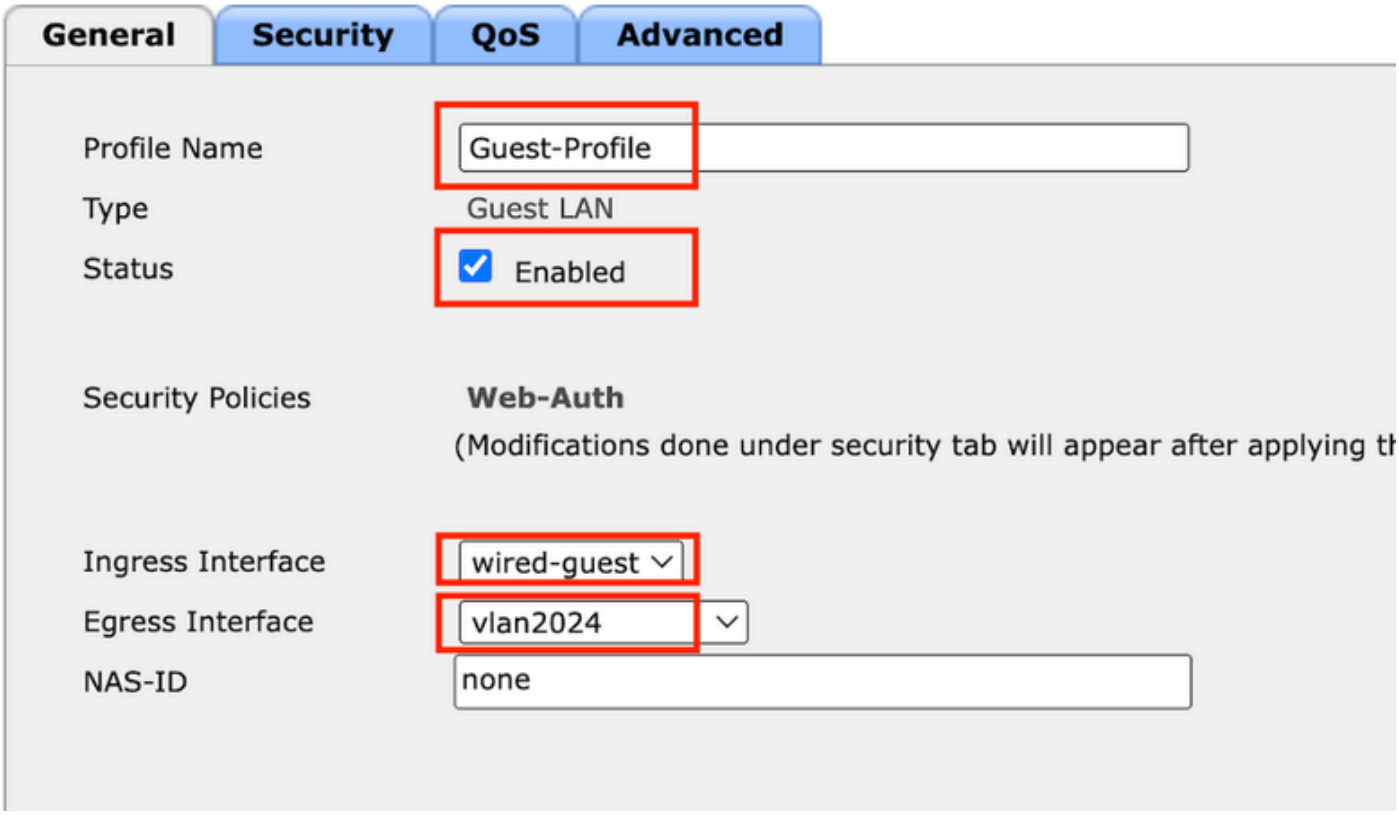
Type as Guest LANを選択して、プロファイル名を設定します。9800アンカーコントローラのポリシープロファイルとゲストLANプロファイルで同じ名前を設定する必要があります。

ゲストLANプロファイル

ステップ2:Generalタブで、入力インターフェイスと出力インターフェイスをゲストLANプロファイルにマッピングします。

入力インターフェイスは、有線クライアントが物理的に接続するVLANです。

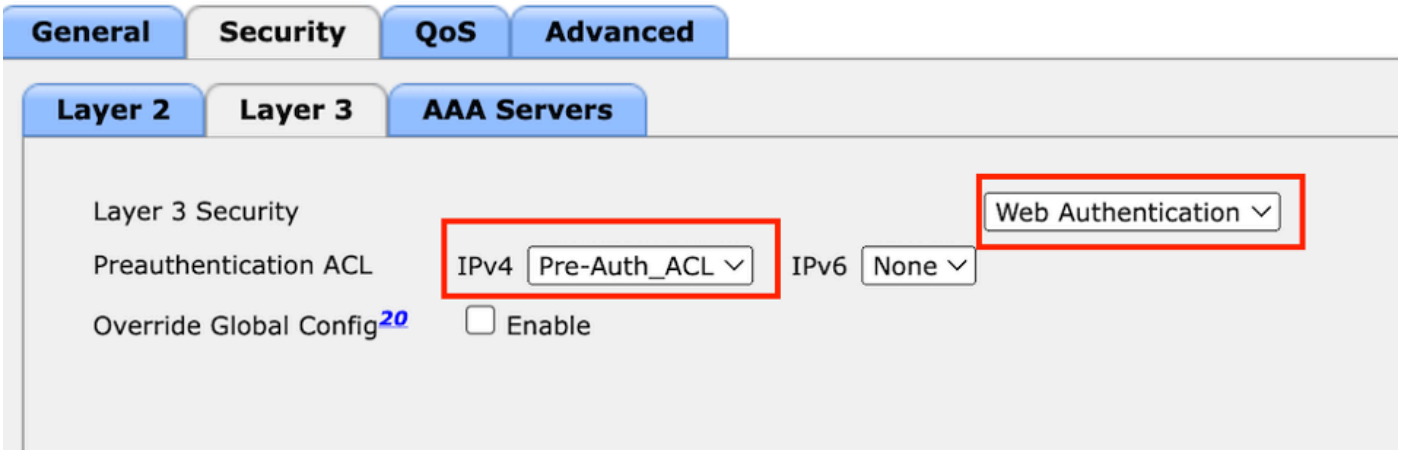
出力インターフェイスは、クライアントがIPアドレスを要求するVLANサブネットです。



ゲストLANプロファイル

ステップ3:Security > Layer 3の順に移動します。

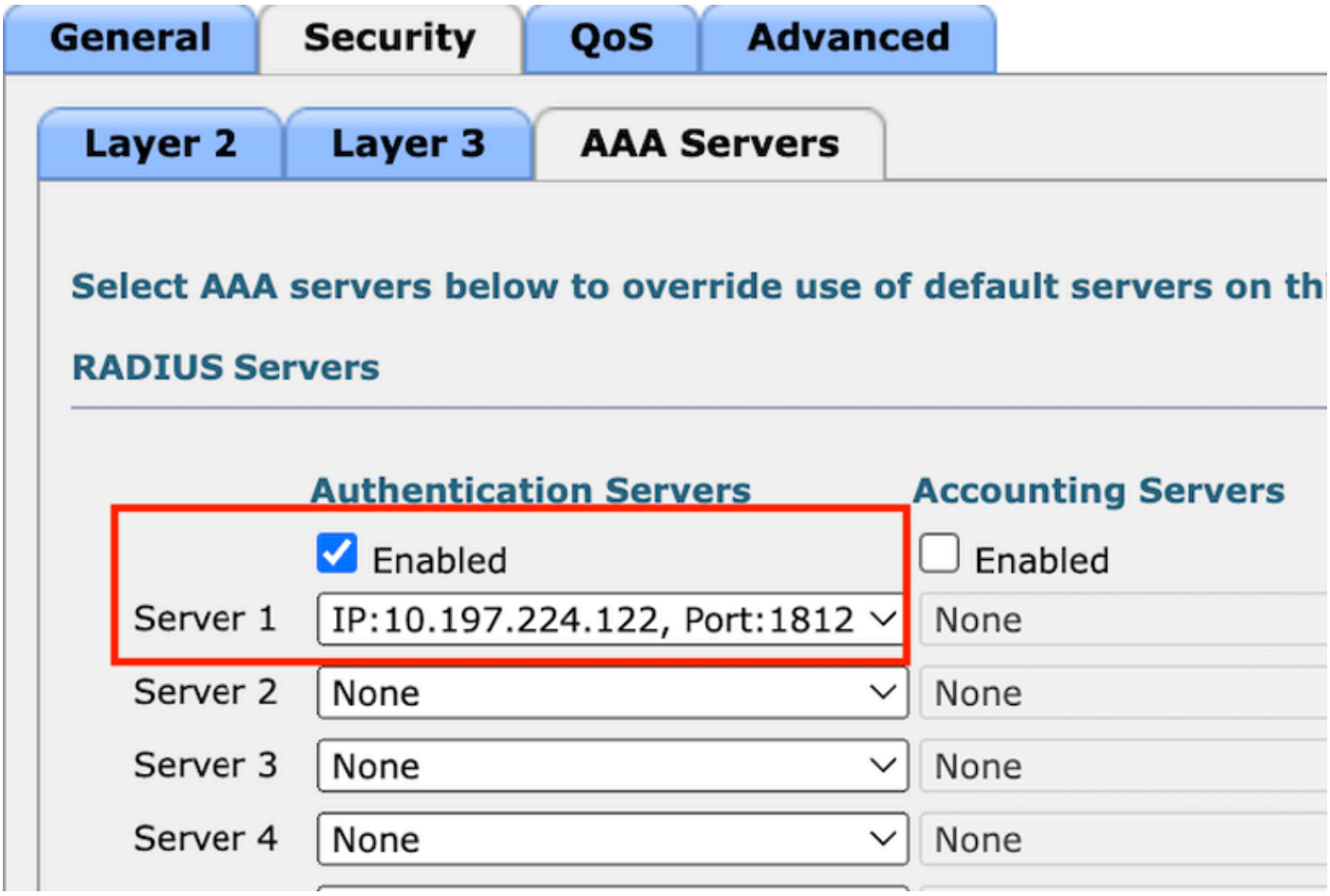
Web AuthenticationとしてLayer 3 Securityを選択し、事前認証ACLをマッピングします。



Layer 3 Securityタブ

ステップ4:

AAA serversタブで、RADIUSサーバとチェックボックスEnabledをマッピングします。



ゲストLANプロファイルへのRADIUSサーバのマッピング

ステップ5:WLANページに移動し、ゲストLANプロファイルのダウンダウンアイコンにカーソルを合わせて、モビリティアンカーを選択します。

モビリティアンカー

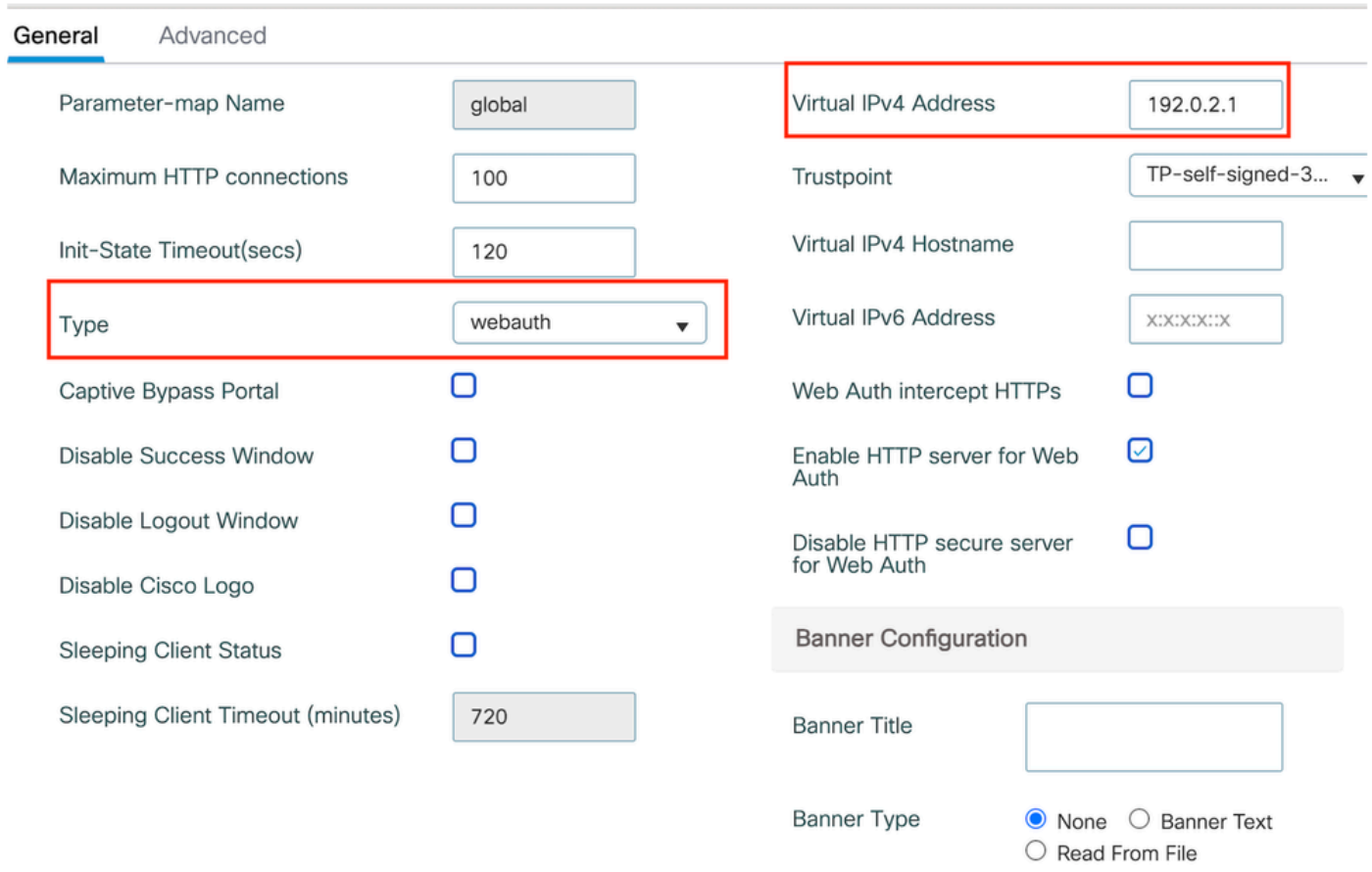
ステップ6：モビリティアンカーをドロップダウンリストからゲストLANプロファイルにマッピングします。

モビリティアンカーのゲストLANへのマッピング

アンカー9800 WLCでの設定

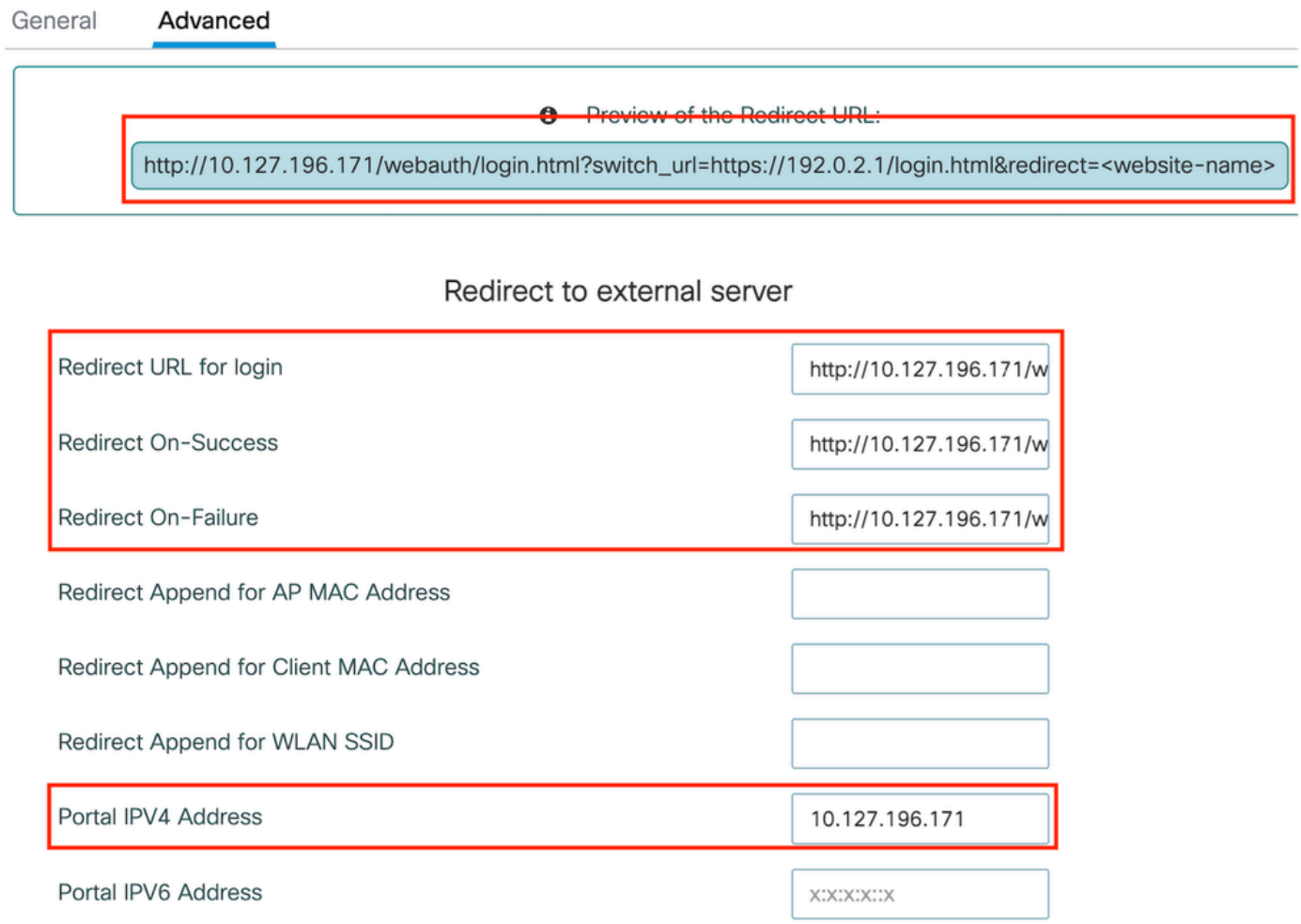
Webパラメータマップの設定

ステップ1:Configuration > Security > Web Authの順に移動し、Globalを選択します。コントローラの仮想IPアドレスとトラストポイントがプロファイル上で正しくマッピングされ、タイプがwebauthに設定されていることを確認します。



Webパラメータマップ

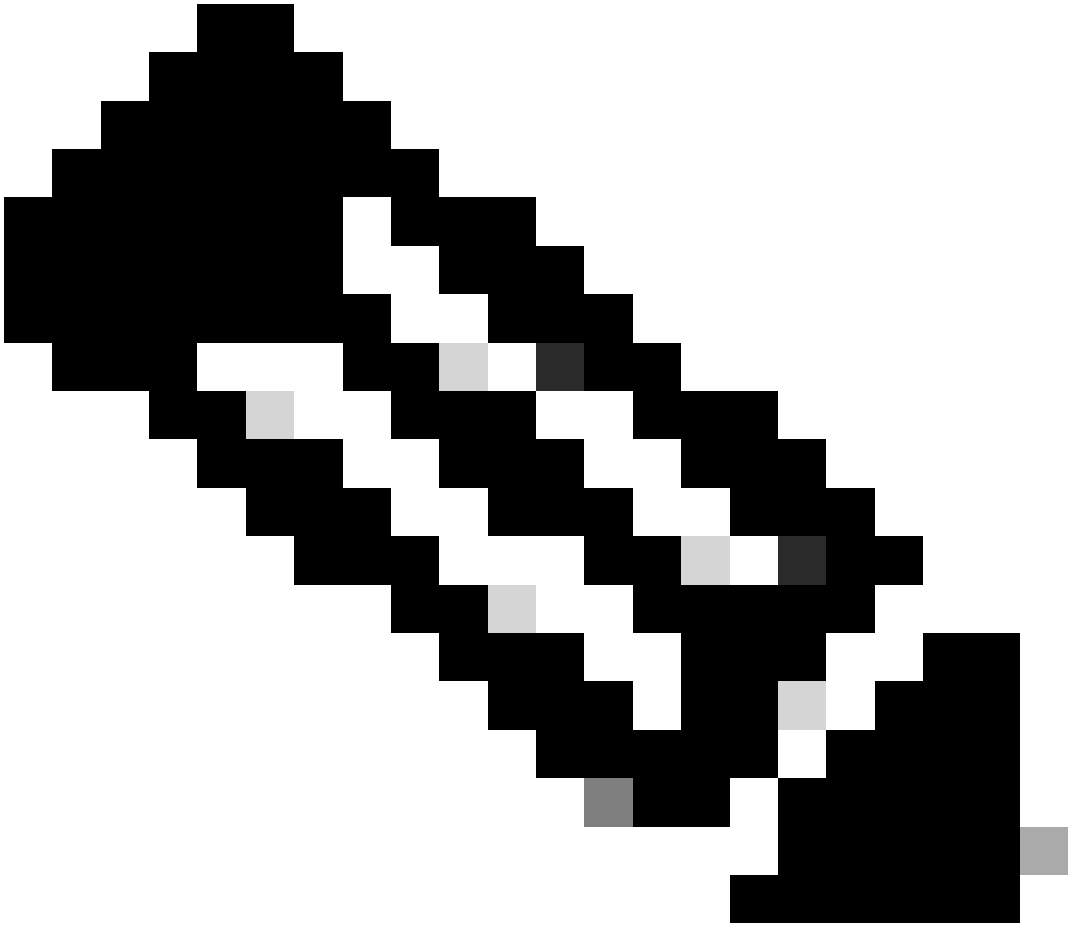
ステップ2:Advancedタブで、クライアントのリダイレクト先となる外部WebページのURLを指定します。ログイン用のリダイレクトURLおよび障害時のリダイレクトを設定します。Redirect On-Success設定はオプションの設定です。



[詳細設定]タブ

CLI での設定

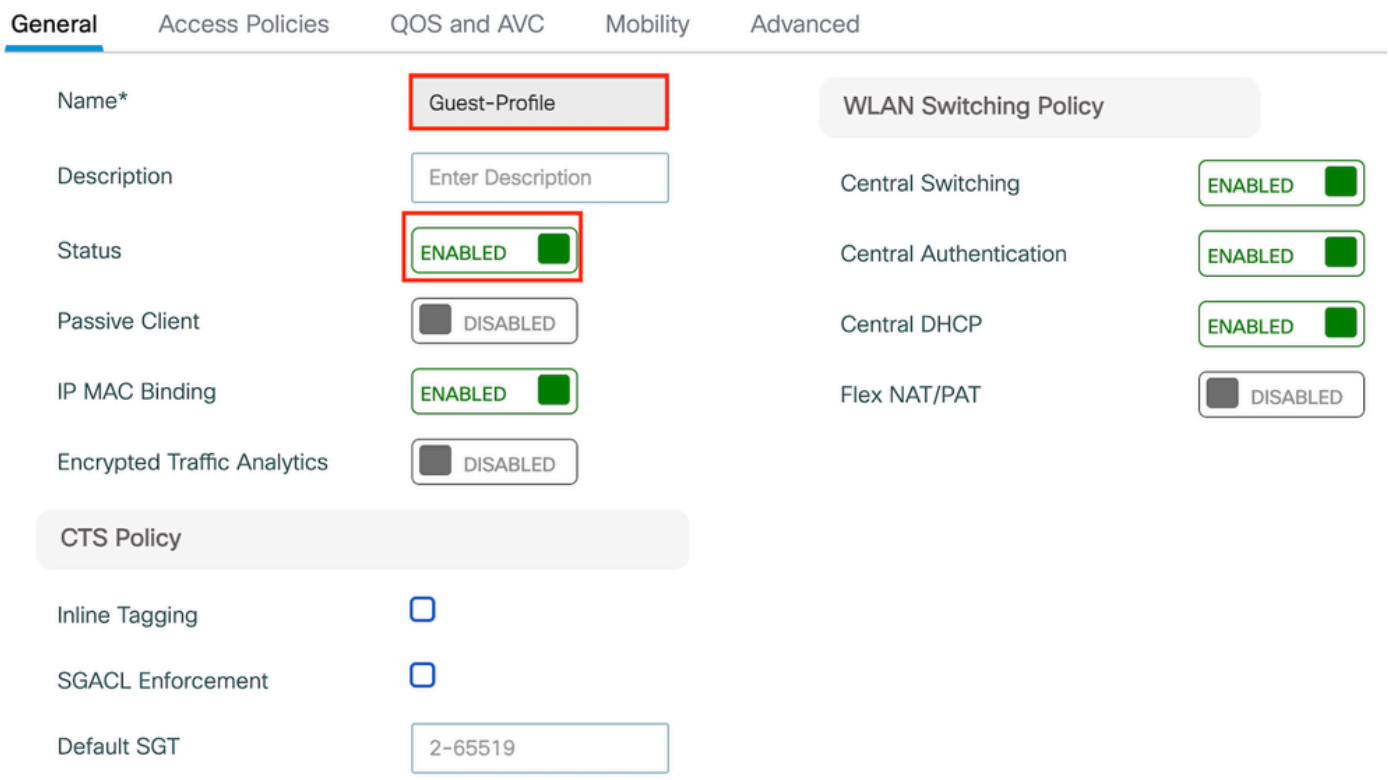
```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171
 trustpoint TP-self-signed-3010594951
 webauth-http-enable
```



注：AAA設定の詳細については、外部9800 WLCの「別のCatalyst 9800にアンカーされたCatalyst 9800での有線ゲストの設定」セクションを参照してください。

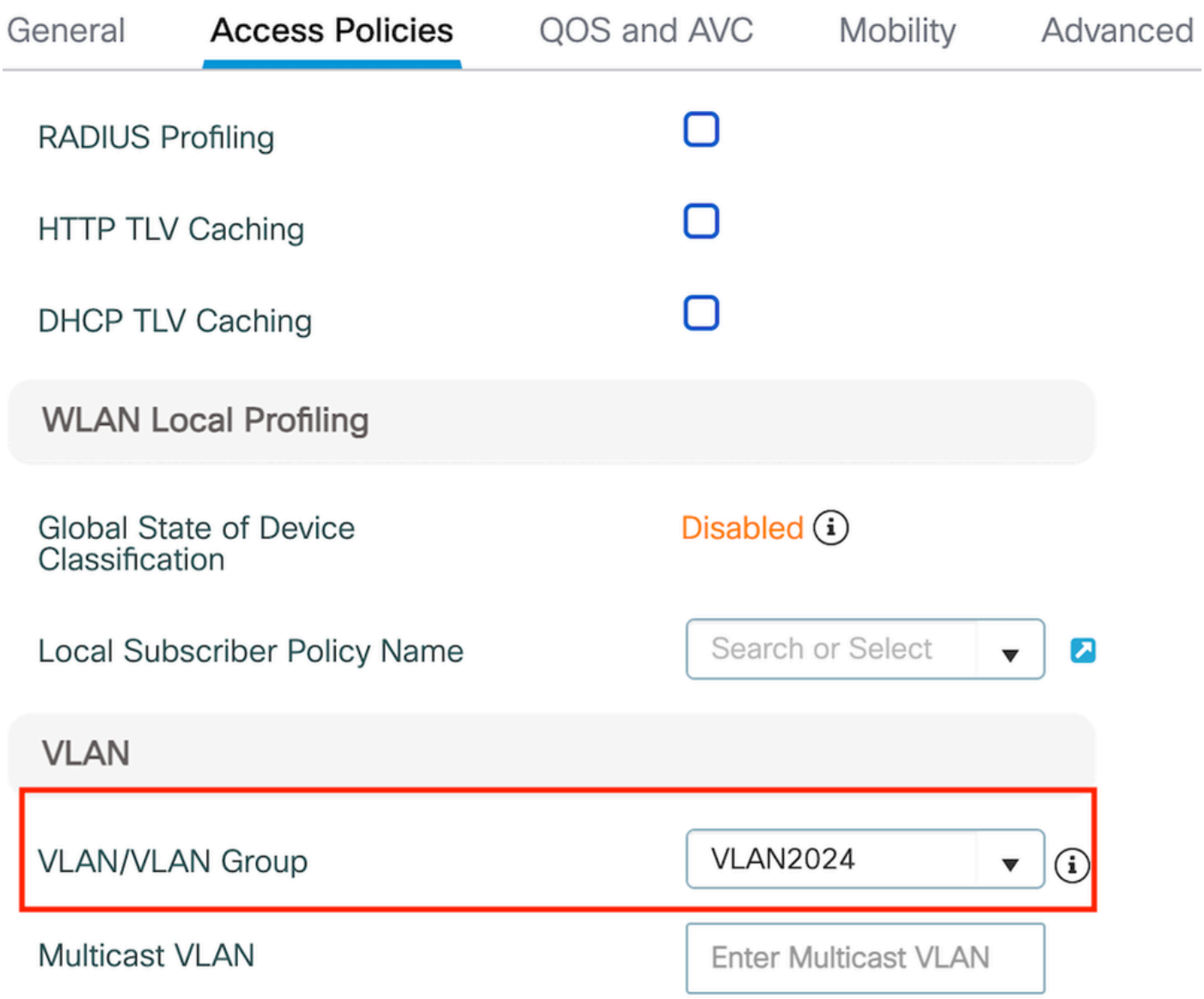
ポリシープロファイルの設定

手順1:Configuration > Tags & Profiles > Policyの順に移動します。外部コントローラのゲストLANプロファイルに使用したのと同じ名前で、ポリシープロファイルを設定します。



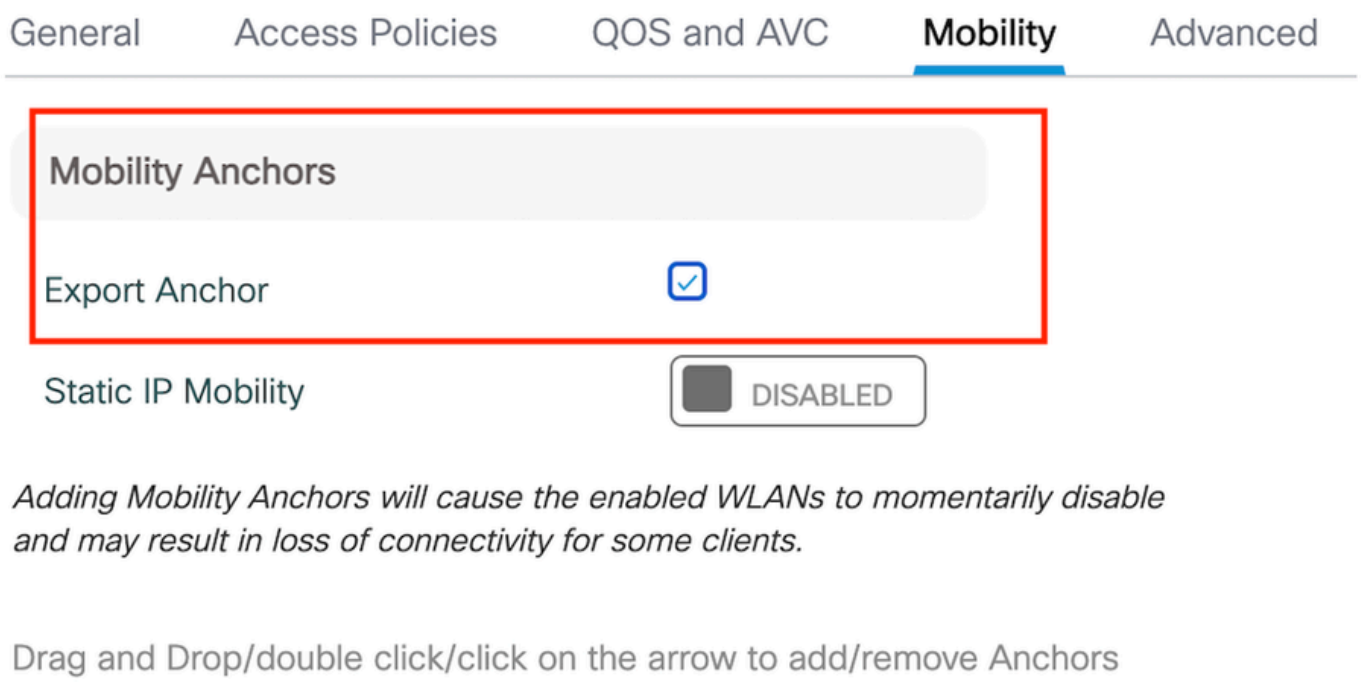
ポリシー プロファイル

ステップ2:Access Policiesタブで、ドロップダウンリストから有線クライアントvlanをマッピングします



アクセスポリシー

ステップ3:Mobilityタブで、Export Anchorチェックボックスをオンにします。



Mobilityタブ

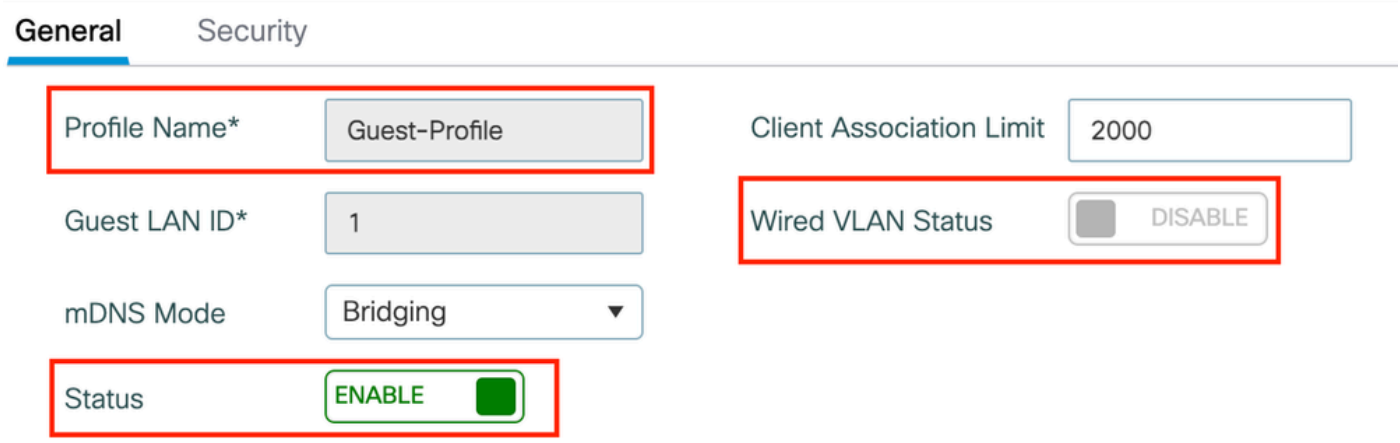
CLI での設定

```
wireless profile policy Guest-Profile
 no accounting-interim
 exclusionlist timeout 180
 no flex umbrella dhcp-dns-option
 mobility anchor
 vlan VLAN2024
 no shutdown
```

ゲストLANプロファイルの設定

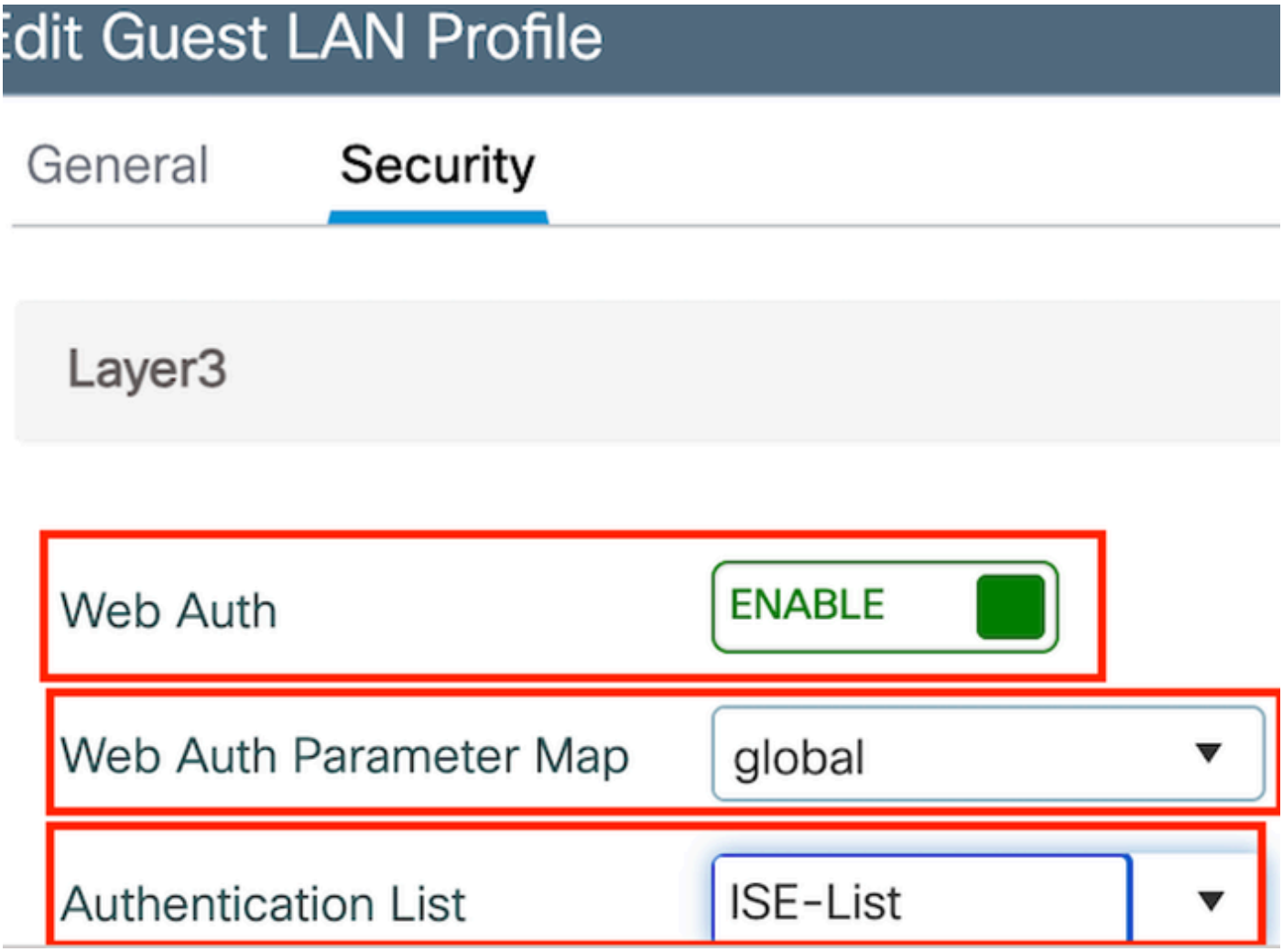
ステップ1:Configuration > Wireless > Guest LANの順に移動し、Addを選択してゲストLANプロファイルを設定し、有線VLANステータスを無効にします。

アンカー上のゲストLANプロファイル名は、外部WLC上のゲストLANプロファイルと同じにする必要があります。



ゲストLANプロファイル

ステップ2:Securityタブで、Web Authを有効にします。 Web Authパラメータマップと認証リストをドロップダウンリストから選択します



Guest LAN Securityタブ

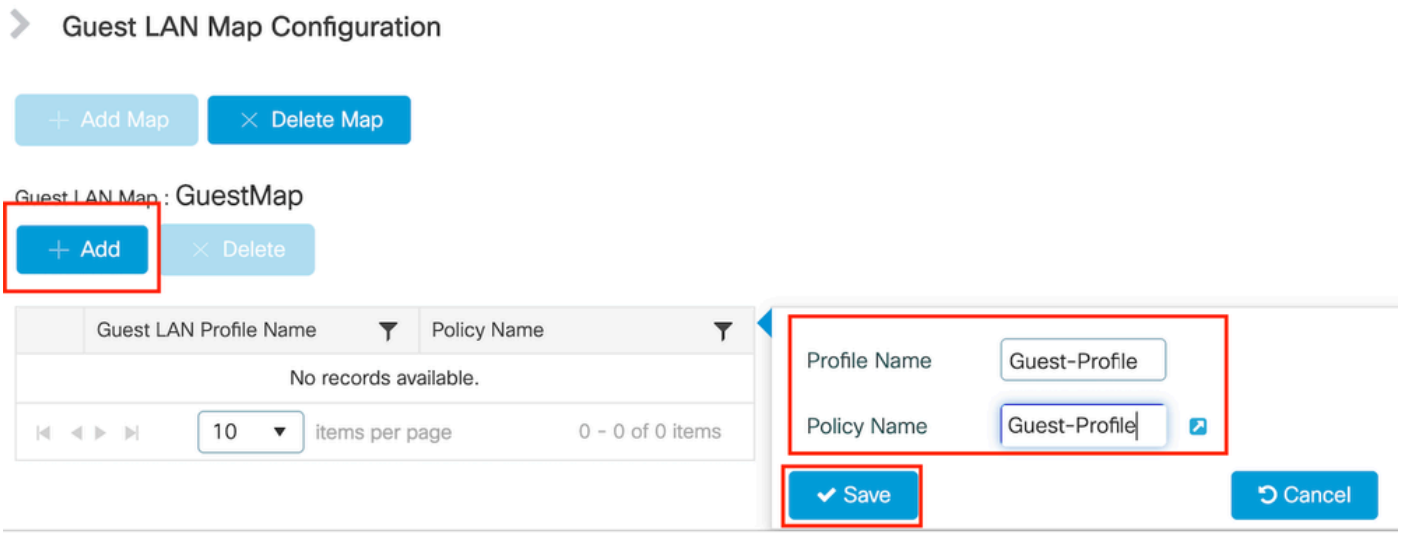
CLI での設定

```
guest-lan profile-name Guest-Profile 1
```

```
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

ゲストLANマップ

ステップ1:Configuration > Wireless > Guest LANの順に移動します。Guest LAN MAP設定セクションで、Addを選択し、ポリシープロファイルをゲストLANプロファイルにマッピングします。



ゲストLANマップ

確認

コントローラ設定の検証

#showゲストLANの概要

```
GLAN  GLAN Profile Name                  Status
-----------------------------------------------
1     Guest-Profile                      UP
2     Guest                              UP
```

#showゲストLAN ID 1

<#root>

```
Guest-LAN Profile Name     : Guest
================================================
Guest-LAN ID                                 : 2
Wired-Vlan                                   :

11

Status                                       :
```

```
Enabled

Number of Active Clients                      : 0
Max Associated Clients                        : 2000
Security
    WebAuth                                   :

Enabled

    Webauth Parameter Map                     : global
    Webauth Authentication List               :

ISE-List

    Webauth Authorization List                : Not configured
mDNS Gateway Status                           : Bridge
```

#showパラメータマップタイプwebauthグローバル

<#root>

```
Parameter Map Name               : global
  Type                           :

webauth

  Redirect:
    For Login                    :

http://10.127.196.171/webauth/login.html

    On Success                   :

http://10.127.196.171/webauth/logout.html

    On Failure                   :

http://10.127.196.171/webauth/failed.html

    Portal ipv4                  :

10.127.196.171

        Virtual-ipv4                  :

192.0.2.1
```

#show parameter-map type webauth name <profile name>（カスタムWebパラメータプロファイルを使用する場合）

#show wireless guest-lan-mapの要約

```
GLAN Profile Name                  Policy Name
------------------------------------------------------------------------
Guest                              Guest
```

#show wireless mobility summary

```
IP                                          Public Ip                                       MAC Address
-----------------------------------------------------------------------------------------------------------
10.76.118.70                                10.76.118.70                                    f4bd.9e59.314b
```

#show ip httpサーバステータス

```
HTTP server status: Enabled
HTTP server port: 80
HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local

HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server trustpoint: TP-self-signed-3010594951
```

>show guest-lan summary (ゲストLANの概要を表示)

```
Number of Guest LANs.............................. 1

GLAN ID  GLAN Profile Name                      Status    Interface Name
-------  -------------------------------------  --------  --------------------
2        Guest                                  Enabled  wired-vlan-11
```

>ゲストLAN 2を表示

```
Guest LAN Identifier.............................. 2
Profile Name...................................... Guest
Status............................................ Enabled
Interface......................................... wired-vlan-11
Radius Servers
   Authentication................................. 10.197.224.122 1812 *
    Web Based Authentication...................... Enabled
   Web Authentication Timeout..................... 300
        IPv4 ACL..................................... Pre-Auth_ACL
               Mobility Anchor List
 GLAN ID     IP Address            Status
 -------     ---------------       ------
 2           10.76.118.74          Up
```

>カスタムWebをすべて表示

```
Radius Authentication Method..................... PAP
Cisco Logo....................................... Enabled
CustomLogo....................................... None
Custom Title..................................... None
Custom Message................................... None
Custom Redirect URL.............................. http://10.127.196.171/webauth/logout.html
Web Authentication Login Success Page Mode....... None
Web Authentication Type.......................... External
Logout-popup..................................... Enabled
External Web Authentication URL.................. http://10.127.196.171/webauth/login.html
QR Code Scanning Bypass Timer.................... 0
QR Code Scanning Bypass Count.................... 0
```

>show custom-web guest-lan 2（カスタムwebゲストlan 2を表示）

```
Guest LAN Status............................... Enabled
Web Security Policy............................ Web Based Authentication
WebAuth Type................................... External
Global Status.................................. Enabled
```

クライアントポリシーの状態の検証

海外では –

#showワイヤレスクライアントの概要

外部コントローラのクライアントポリシーマネージャの状態は、クライアントが正常に関連付けられた後でRUNになります。

<#root>

```
MAC Address    AP Name                                          Type ID   State             Protocol Meth
-------------------------------------------------------------------------------------------------------
a0ce.c8c3.a9b5 N/A

GLAN 1

    Run

802.3

    Web Auth

Export Foreign
```

>show client detail a0ce.c8c3.a9b5

<#root>

```
Client MAC Address.............................. a0:ce:c8:c3:a9:b5
Client Username ................................ N/A
Client Webauth Username ........................ N/A
Client State.................................... Associated
User Authenticated by .......................... None
Client User Group.............................
Client NAC OOB State............................ Access
guest-lan....................................... 1
Wireless LAN Profile Name....................... Guest-Profile
Mobility State..................................

Export Foreign

Mobility Anchor IP Address.....................

10.76.118.70

Security Policy Completed.......................

Yes

Policy Manager State............................

RUN

Pre-auth IPv4 ACL Name.......................... Pre-Auth_ACL
EAP Type........................................ Unknown
Interface.......................................

wired-guest-egress

VLAN............................................ 2024
Quarantine VLAN................................. 0
```

アンカー時

アンカーコントローラでクライアントの状態遷移を監視する必要があります。

クライアントポリシーマネージャの状態がWeb Auth pending(WAUTH)です。

<#root>

```
MAC Address    AP Name                                          Type ID   State             Protocol Meth
-------------------------------------------------------------------------------------------------------
a0ce.c8c3.a9b5 10.76.6.156

GLAN 1

    Webauth Pending

802.3

    Web Auth

Export Anchor
```

クライアントが認証されると、ポリシーマネージャの状態はRUN状態に移行します。

```
MAC Address    AP Name                                              Type ID   State             Protocol Meth
-------------------------------------------------------------------------------------------------------------
a0ce.c8c3.a9b5 10.76.6.156                                          GLAN 1    Run               802.3    Web
```

#show wireless client mac-address a0ce.c8c3.a9b5 detail

<#root>

```
Client MAC Address : a0ce.c8c3.a9b5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :
```

10.105.211.69

```
Client State : Associated
Policy Profile : Guest-Profile
Flex Profile : N/A
Guest Lan:
  GLAN Id: 1
  GLAN Name: Guest-Profile

Mobility:
  Foreign IP Address          :
```

10.76.118.74

```
  Point of Attachment         : 0xA0000003
  Point of Presence           : 0
  Move Count                  : 1
  Mobility Role               :
```

Export Anchor

```
  Mobility Roam Type          :
```

L3 Requested

```
Policy Manager State:
```

Webauth Pending

```
Last Policy Manager State :
```

IP Learn Complete

```
Client Entry Create Time : 35 seconds

VLAN : VLAN2024

Session Manager:
  Point of Attachment : mobility_a0000003
  IIF ID              : 0xA0000003
  Authorized          : FALSE
  Session timeout     : 28800
  Common Session ID: 4a764c0a0000008ea0285466
```

```
  Acct Session ID  : 0x00000000
  Auth Method Status List
        Method : Web Auth
                Webauth State    :
```

Login

```
                Webauth Method   :
```

Webauth

```
Server Policies:
  Resultant Policies:
                URL Redirect ACL :
```

WA-v4-int-10.127.196.171

```
                Preauth ACL      :
```

WA-sec-10.127.196.171

```
                VLAN Name        : VLAN2024
                VLAN             :
```

2024

```
                Absolute-Timer   : 28800
```

Web認証が成功すると、クライアントはRUN状態に移行します。

show wireless client mac-address a0ce.c8c3.a9b5 detail

<#root>

```
Client MAC Address : a0ce.c8c3.a9b5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :
```

10.105.211.69

```
Client Username :
```

testuser

```
Client State : Associated
Policy Profile : Guest-Profile
Flex Profile : N/A
Guest Lan:
  GLAN Id: 1
  GLAN Name: Guest-Profile
Wireless LAN Network Name (SSID) : N/A
BSSID : N/A
Connected For : 81 seconds
Protocol : 802.3

Policy Manager State:
```

Run

Last Policy Manager State :

Webauth Pending

Client Entry Create Time : 81 seconds
VLAN : VLAN2024

Last Tried Aaa Server Details:
Server IP :

10.197.224.122

Auth Method Status List
Method : Web Auth
Webauth State : Authz
Webauth Method : Webauth

Resultant Policies:
URL Redirect ACL :

IP-Adm-V4-LOGOUT-ACL

VLAN Name : VLAN2024
VLAN :

2024

Absolute-Timer : 28800

>show client detail a0:ce:c8:c3:a9:b5

<#root>

Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username ..... N/A
Client Webauth Username ..... N/A
Client State..... Associated
Wireless LAN Profile Name..... Guest
WLAN Profile check for roaming..... Disabled
Hotspot (802.11u)..... Not Supported
Connected For ..... 90 secs
IP Address..... 10.105.211.75
Gateway Address..... 10.105.211.1
Netmask..... 255.255.255.128
Mobility State.....

Export Anchor

Mobility Foreign IP Address.....

10.76.118.70

Security Policy Completed..... No
Policy Manager State.....

WEBAUTH_REQD

Pre-auth IPv4 ACL Name.....

Pre-Auth_ACLPre-auth

```
IPv4 ACL Applied Status.................. Yes
Pre-auth IPv4 ACL Applied Status.................
```

Yes

認証の後、クライアントはRUN状態に移行します。

<#root>

```
show client detail a0:ce:c8:c3:a9:b5
Client MAC Address.............................. a0:ce:c8:c3:a9:b5
Client Username .................................
```

testuser

```
Client Webauth Username .........................
```

testuser

```
Client State.....................................
```

Associated

```
User Authenticated by ...........................
```

RADIUS Server

```
Client User Group............................... testuser
Client NAC OOB State............................ Access
Connected For .................................. 37 secs
IP Address.....................................
```

10.105.211.75

```
Gateway Address................................. 10.105.211.1
Netmask......................................... 255.255.255.128
Mobility State..................................
```

Export Anchor

```
Mobility Foreign IP Address..................... 10.76.118.70
Security Policy Completed....................... Yes
Policy Manager State............................
```

RUN

```
Pre-auth IPv4 ACL Name.......................... Pre-Auth_ACL
Pre-auth IPv4 ACL Applied Status................ Yes
EAP Type........................................ Unknown
Interface.......................................
```

wired-vlan-11

```
VLAN............................................
```

11

```
Quarantine VLAN................................. 0
```

トラブルシュート

AireOSコントローラデバッグ

クライアントデバッグの有効化

>debug client <H.H.H>

デバッグが有効かどうかを確認するには

>デバッグの表示

デバッグを無効にするには

debug disable-all（ディセーブルに設定）

9800放射性微量

CLIで指定したMACアドレスのクライアントデバッグトレースを生成するには、無線アクティブトレースをアクティブにします。

放射性トレースを有効にする手順：

すべての条件付きデバッグが無効になっていることを確認します。

```
clear platform condition all
```

指定したMACアドレスのデバッグを有効にします。

```
debug wireless mac <H.H.H> monitor-time <Time is seconds>
```

問題を再現したら、デバッグを無効にしてRAトレース収集を停止します。

```
no debug wireless mac <H.H.H>
```

RAトレースが停止すると、デバッグファイルがコントローラのブートフラッシュに生成されます。

```
show bootflash: | include ra_trace
2728        179 Jul 17 2024 15:13:54.0000000000 +00:00 ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_Da
```

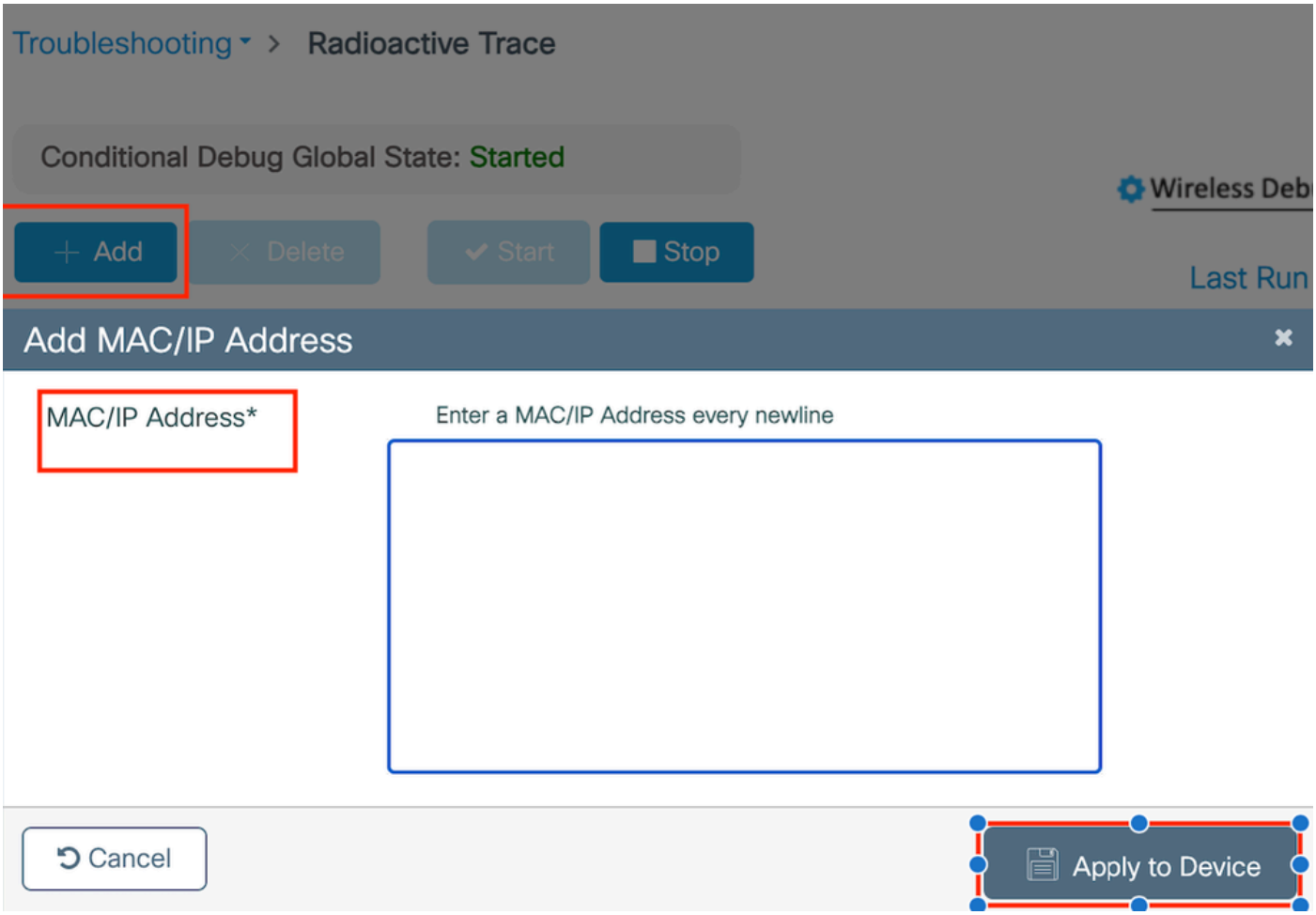
ファイルを外部サーバにコピーします。

```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP addr
```

デバッグログを表示します。

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

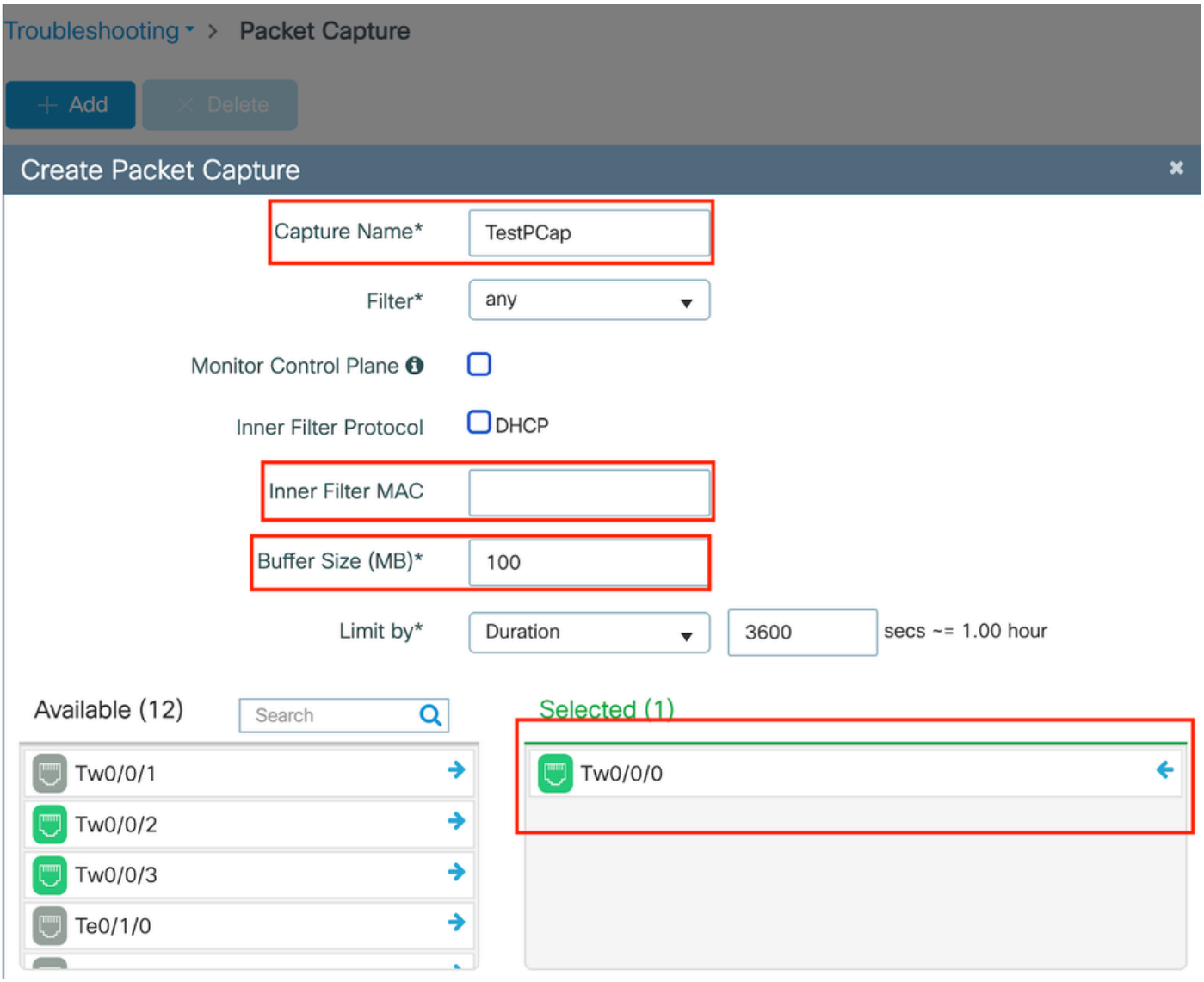
GUIでRAトレースを有効にします。



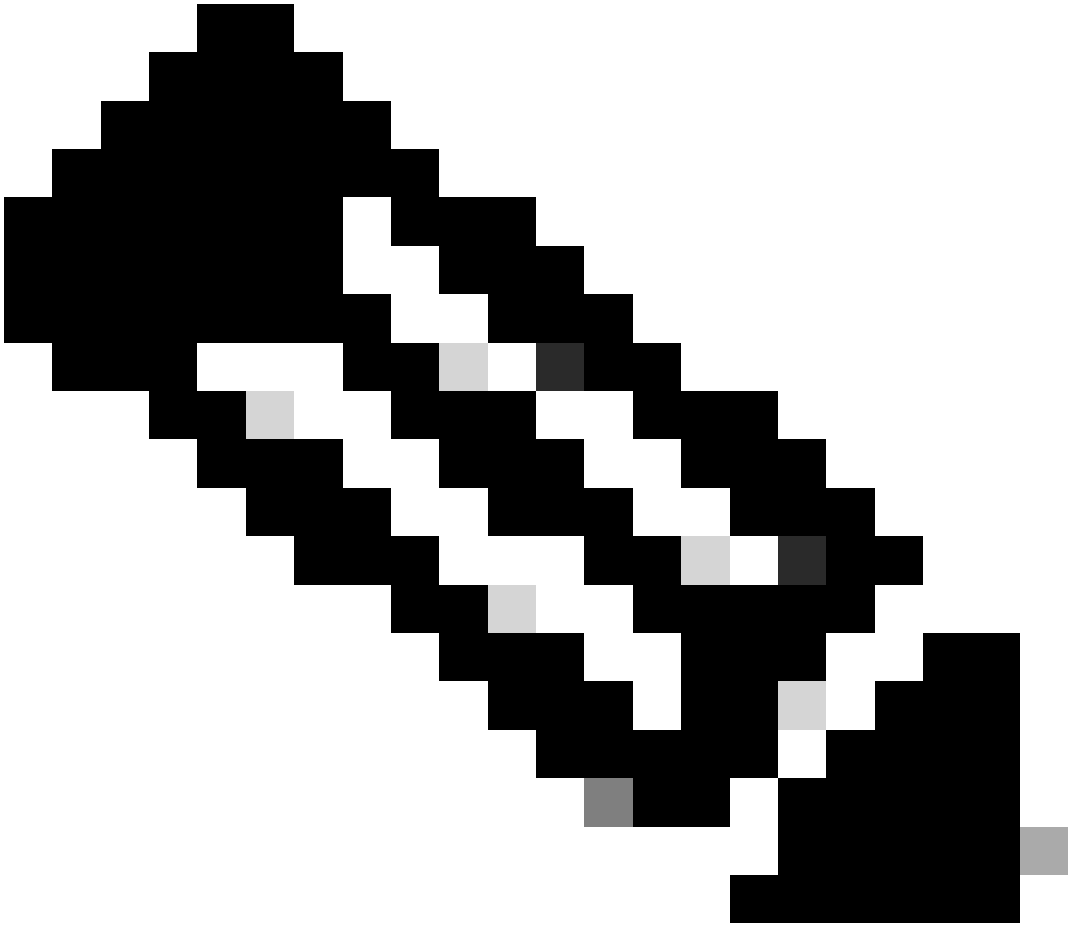
WebUIでのRAトレースの有効化

Embedded Packet Capture

トラブルシューティング>パケットキャプチャに移動します。キャプチャ名を入力し、クライアントのMACアドレスを内部フィルタMACとして指定します。バッファサイズを100に設定し、着信パケットと発信パケットを監視するアップリンクインターフェイスを選択します。

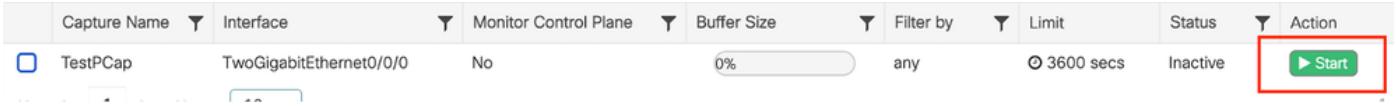


Embedded Packet Capture



注：システムCPUにリダイレクトされ、データプレーンに再注入されたトラフィックを表示するには、「コントロールトラフィックの監視」オプションを選択します。

Troubleshooting > Packet Captureの順に移動し、Startを選択してパケットをキャプチャします。



パケットキャプチャの開始

CLI での設定

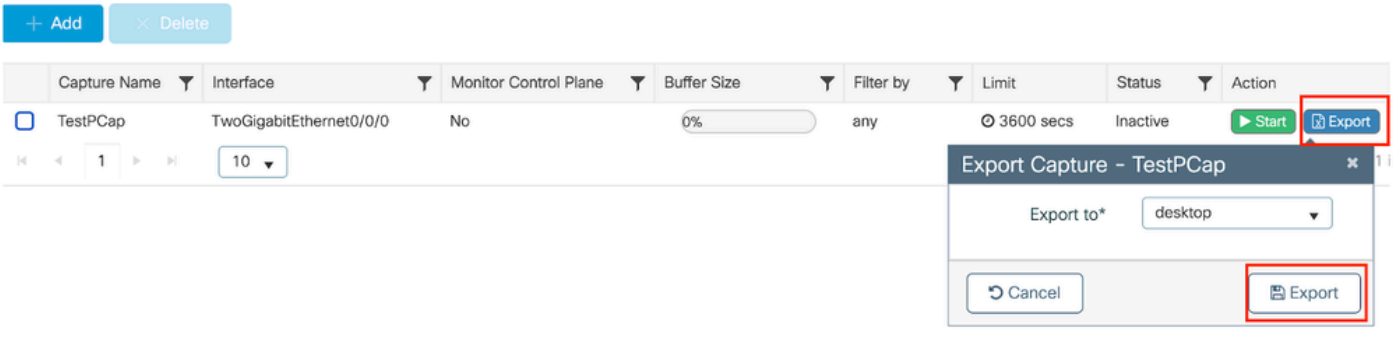
```
monitor capture TestPCap inner mac <H.H.H>
monitor capture TestPCap buffer size 100
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both
monitor capture TestPCap start
```

```
<Reporduce the issue>

monitor capture TestPCap stop



show monitor capture TestPCap

Status Information for Capture TestPCap
  Target Type:
 Interface: TwoGigabitEthernet0/0/0, Direction: BOTH
  Status : Inactive
  Filter Details:
  Capture all packets
  Inner Filter Details:
  Mac: 6c7e.67e3.6db9
  Continuous capture: disabled
  Buffer Details:
  Buffer Type: LINEAR (default)
  Buffer Size (in MB): 100
  Limit Details:
  Number of Packets to capture: 0 (no limit)
  Packet Capture duration: 3600
  Packet Size to capture: 0 (no limit)
  Maximum number of packets to capture per second: 1000
  Packet sampling rate: 0 (no sampling)
```

パケットキャプチャを外部TFTPサーバにエクスポートします。

```
monitor capture TestPCap export tftp://<IP address>/ TestPCap.pcap
```

ローカルマシンでキャプチャファイルをダウンロードするには、Troubleshooting > Packet Captureに移動してExportを選択します。



EPCのダウンロード

作業ログのスニペット

AireOS外部コントローラクライアントデバッグログ

有線クライアントから受信した有線パケット

```
*apfReceiveTask: May 27 12:00:55.127: a0:ce:c8:c3:a9:b5  Wired Guest packet from 10.105.211.69 on mobil
```

外部コントローラーのビルド書き出しアンカー要求

```
*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Attempting anchor export for mobile a0:ce:c8:c3
*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 mmAnchorExportSend: Building ExportForeignLradM
*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 SGT Payload built in Export Anchor Req 0
```

外部コントローラがアンカーコントローラにエクスポートアンカー要求を送信します。

```
*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Export Anchor request sent to 10.76.118.70
```

アンカーコントローラがクライアントのアンカー要求の確認応答を送信

```
*Dot1x_NW_MsgTask_5: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Recvd Exp Anchor Ack for mobile  a0:ce:c8:c
```

外部コントローラのクライアントのモビリティロールが更新され、外部コントローラがエクスポートされます。

```
*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) mobility role update requ
  Peer = 10.76.118.70, Old Anchor = 10.76.118.70, New Anchor = 10.76.118.70
```

クライアントがRUN状態に移行しました。

```
*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mobilit
*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Stopping deletion of Mobile Station: (callerId:
*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Moving client to run state
```

9800外部コントローラの放射性トレース

クライアントがコントローラに関連付けられます。

```
2024/07/15 04:10:29.087608331 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b
```

関連付け後にモビリティの検出が進行中です。

```
2024/07/15 04:10:29.091585813 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b
2024/07/15 04:10:29.091605761 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b
```

モビリティディスカバリが処理されると、クライアントローミングタイプはL3に対して要求されたアップデートになります。

```
2024/07/15 04:10:29.091664605 {wncd_x_R0-0}{1}: [mm-transition] [17765]: (info): MAC: a0ce.c8c3.a9b5 MM
2024/07/15 04:10:29.091693445 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Roam t
```

外部コントローラがアンカーWLCにエクスポートアンカー要求を送信しています。

```
2024/07/15 04:10:32.093245394 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex
2024/07/15 04:10:32.093253788 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Fo
2024/07/15 04:10:32.093274405 {mobilityd_R0-0}{1}: [mm-client] [18316]: (info): MAC: a0ce.c8c3.a9b5 For
```

アンカーコントローラからエクスポートアンカー応答を受信し、ユーザプロファイルからvlanが適用されます。

```
2024/07/15 04:10:32.106775213 {mobilityd_R0-0}{1}: [mm-transition] [18316]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 04:10:32.106811183 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex
2024/07/15 04:10:32.107183692 {wncd_x_R0-0}{1}: [epm-misc] [17765]: (info): [a0ce.c8c3.a9b5:Tw0/0/0] An
2024/07/15 04:10:32.107247304 {wncd_x_R0-0}{1}: [svm] [17765]: (info): [a0ce.c8c3.a9b5] Applied User Pr
2024/07/15 04:10:32.107250258 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17765]: (info): Applied User Profile:
```

アンカーのエクスポート要求が処理されると、クライアントモビリティロールがエクスポート外部に更新されます。

```
2024/07/15 04:10:32.107490972 {wncd_x_R0-0}{1}: [mm-client] [17765]: (debug): MAC: a0ce.c8c3.a9b5 Proce
2024/07/15 04:10:32.107502336 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Mobili
2024/07/15 04:10:32.107533732 {wncd_x_R0-0}{1}: [sanet-shim-translate] [17765]: (info): Anchor Vlan: 20
2024/07/15 04:10:32.107592251 {wncd_x_R0-0}{1}: [mm-client] [17765]: (note): MAC: a0ce.c8c3.a9b5 Mobili
```

クライアントがIP学習ステートに移行する。

```
2024/07/15 04:10:32.108210365 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b
2024/07/15 04:10:32.108293096 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: a0ce.c8c3.a9b5
```

IPが学習されると、クライアントは外部WLC上でRUN状態に移行します。

```
2024/07/15 04:10:32.108521618 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b
```

AireOSアンカーコントローラクライアントデバッグログ

外部コントローラから取得されたアンカー要求のエクスポート。

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Anchor Export Request Recvd for mobile a0:c
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv: Extracting mmPayloadExpo
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv  Ssid=Guest  useProfileNa
```

ローカルブリッジングVLANがクライアントに適用されます。

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Updated local bridging VLAN to 11 while app
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Applying Interface(wired-vlan-11) policy on
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 After applying Interface(wired-vlan-11) pol
```

モビリティロールが更新され、エクスポートアンカーとクライアントの状態がAssociatedに移行します。

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 0.0.0.0 START (0) mobility role update requ
  Peer = 10.76.118.70, Old Anchor = 0.0.0.0, New Anchor = 10.76.118.74
Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5
                                                    add client MAC a0:ce:c8:c3:a9:b5 IP 10.76.1
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5
                                                    Sent message to add a0:ce:c8:c3:a9:b5 on me
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv (mm_listen.c:7933) Changi
```

モビリティが完了し、クライアントの状態が関連付けられ、モビリティロールがエクスポートアンカーになります。

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mob
```

クライアントのIPアドレスはコントローラで学習され、状態はDHCP必須からWeb認証が必須に移行されます。

```
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 Static IP client associated to interface wired-vlan
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 dtlArpSetType: Changing ARP Type from 0 ---> 1 for
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 10.105.211.75 DHCP_REQD (7) Change state to WEBAUTH
```

Webauth URLは、外部リダイレクトURLとコントローラの仮想IPアドレスを追加して作成されます。

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Preparing redirect URL according to configure
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Web-auth type External, using URL:http://10.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added switch_url, redirect URL is now http://
```

URLにクライアントのMACアドレスとWLANを追加。

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added client_mac , redirect URL is now http:/
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now http://10.127
```

ホスト10.105.211.1のHTTP GETを分割した後の最終URL

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5-  parser host is 10.105.211.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser path is /auth/discovery
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5-added redirect=, URL is now http://10.127.196.
```

リダイレクトURLは、200 OK応答パケットでクライアントに送信されます。

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- 200 send_data =HTTP/1.1 200 OK
Location:http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&client_mac=a0
```

クライアントがリダイレクトURLホストとのTCP接続を確立します。クライアントがポータルでログインユーザ名とパスワードを送信すると、コントローラからradiusサーバにradius要求が送信されます

コントローラがAccess-Acceptを受信すると、クライアントはTCPセッションを閉じ、RUN状態に移行します。

```
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Sending the packet to v4 host 10.197.224.122:18
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Successful transmission of Authentication Packe

*aaaQueueReader: May 28 10:46:59:077:         AVP[01] User-Name.............................testuser
*aaaQueueReader: May 28 10:46:59:077:         AVP[03] Calling-Station-Id.....................a0-ce-c8
*aaaQueueReader: May 28 10:46:59:077:         AVP[04] Nas-Port..............................0x000000
*aaaQueueReader: May 28 10:46:59:077:         AVP[05] Nas-Ip-Address........................0x0a4c76
*aaaQueueReader: May 28 10:46:59:077:         AVP[06] NAS-Identifier........................POD1586-

*aaaQueueReader: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 radiusServerFallbackPassiveStateUpdate: RADIUS
*radiusTransportThread: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5  Access-Accept received from RADIUS serv

*Dot1x_NW_MsgTask_5: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Processing Access-Accept for mobile a0:ce:c

*apfReceiveTask: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Moving client to run state
```

9800アンカーコントローラの放射性トレース

外部コントローラからのクライアントのモビリティアナウンスメッセージ。

```
2024/07/15 15:10:20.614677358 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Re
```

外部コントローラRAトレースで検証可能なアンカーコントローラによって送信されるエクスポートアンカー応答に対して、クライアントが関連付けを行っているときに外部コントローラから受信したエクスポートアンカー要求。

```
2024/07/15 15:10:22.615246594 {mobilityd_R0-0}{1}: [mm-transition] [15259]: (info): MAC: a0ce.c8c3.a9b5
```

クライアントが関連付け状態に移行し、モビリティロールがエクスポートアンカーに移行します。

```
2024/07/15 15:10:22.616156811 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b
2024/07/15 15:10:22.627358367 {wncd_x_R0-0}{1}: [mm-client] [14709]: (note): MAC: a0ce.c8c3.a9b5 Mobili
```

```
2024/07/15 15:10:22.627462963 {wncd_x_R0-0}{1}: [dot11] [14709]: (note): MAC: a0ce.c8c3.a9b5  Client da
2024/07/15 15:10:22.627490485 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Ex
2024/07/15 15:10:22.627494963 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Fo
```

IPラーニングが完了し、クライアントIPがARPを通じて学習される。

```
2024/07/15 15:10:22.628124206 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:23.627064171 {wncd_x_R0-0}{1}: [sisf-packet] [14709]: (info): RX: ARP from interface m
2024/07/15 15:10:24.469704913 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (note): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470527056 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470587596 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470613094 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
```

クライアントポリシーの状態がWeb認証保留中です。

```
2024/07/15 15:10:24.470748350 {wncd_x_R0-0}{1}: [client-auth] [14709]: (info): MAC: a0ce.c8c3.a9b5  Cli
```

TCPハンドシェイクがコントローラによってスプーフィングされている。クライアントがHTTP GETを送信すると、リダイレクトURLを含む200 OK応答フレームが送信されます。

クライアントはリダイレクトURLを使用してTCPハンドシェイクを確立し、ページをロードする必要があります。

```
2024/07/15 15:11:37.579177010 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579190912 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579226658 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579230650 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123072893 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123082753 {wnc2024/07/15 15:12:04.280574375 {wncd_x_R0-0}{1}: [webauth-httpd] [1470
```

クライアントがWebポータルページでログインクレデンシャルを送信すると、認証のためにAccess-RequestパケットがRADIUSサーバに送信されます。

```
2024/07/15 15:12:04.281076844 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Send Access-Request t
2024/07/15 15:12:04.281087672 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS:  authenticator e3 01
2024/07/15 15:12:04.281093278 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS:  Calling-Station-Id
2024/07/15 15:12:04.281097034 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS:  User-Name
2024/07/15 15:12:04.281148298 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS:   Cisco AVpair
```

RadiusサーバからAccess-Acceptを受信し、webauthが成功しました。

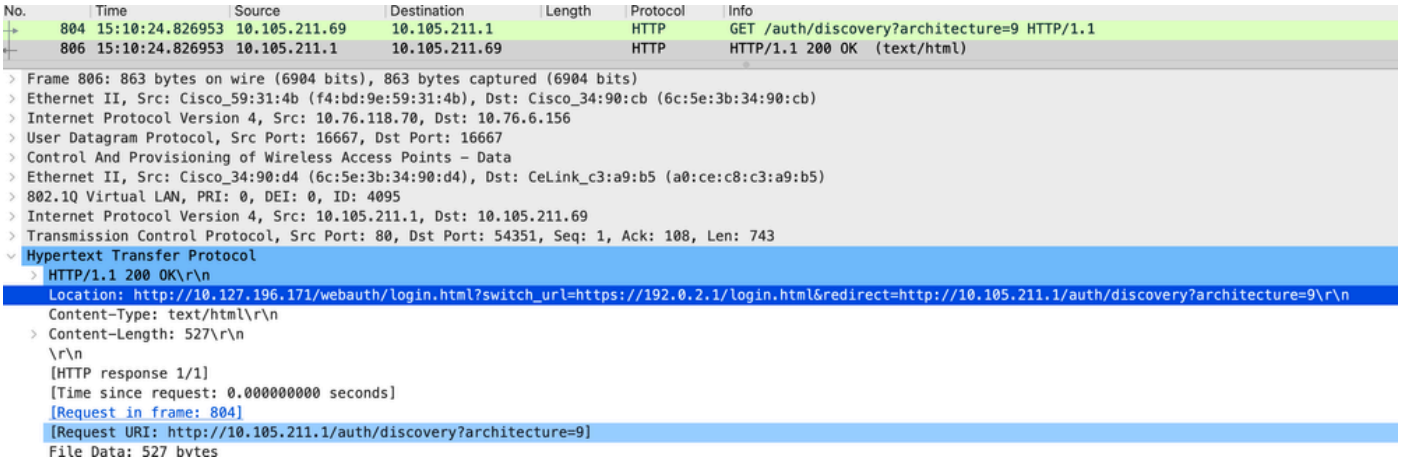
```
2024/07/15 15:12:04.683597101 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Received from id 1812
2024/07/15 15:12:04.683607762 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS:  authenticator 52 3e
```

```
2024/07/15 15:12:04.683614780 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS:  User-Name
```

認証は成功し、クライアントポリシーの状態はRUNです。

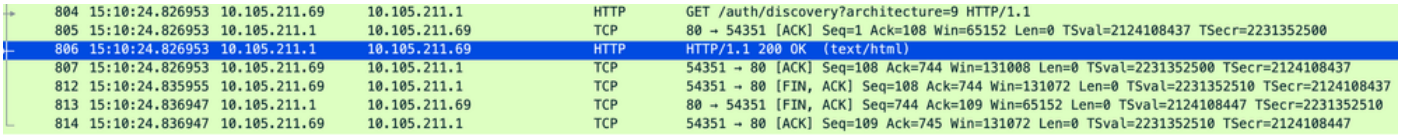
```
2024/07/15 15:12:04.683901842 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:12:04.690643388 {wncd_x_R0-0}{1}: [errmsg] [14709]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/15 15:12:04.690726966 {wncd_x_R0-0}{1}: [aaa-attr-inf] [14709]: (info): [ Applied attribute :bs
2024/07/15 15:12:04.691064276 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b
```

組み込みパケットキャプチャ分析



クライアントがポータルページにリダイレクトされる

リダイレクトURLを受信した後、セッションが閉じられます。

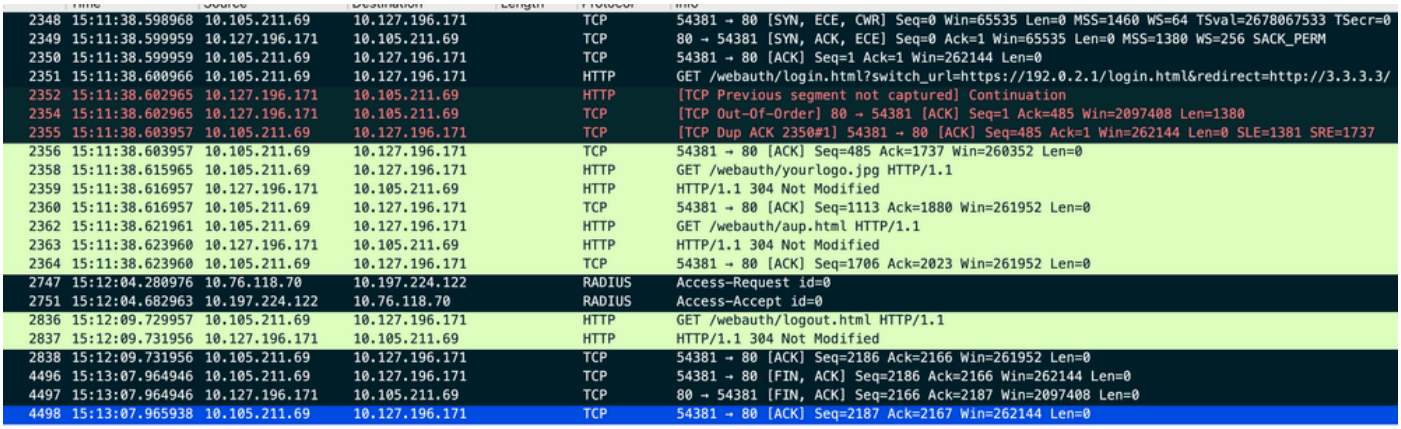


リダイレクトURLの受信後にTCPセッションが閉じられる

クライアントがリダイレクトURLホストへのTCP 3ウェイハンドシェイクを開始し、HTTP GET要求を送信します。

ページがロードされると、ログインクレデンシャルがポータルで送信され、コントローラはクライアントを認証するためにRADIUSサーバにアクセス要求を送信します。

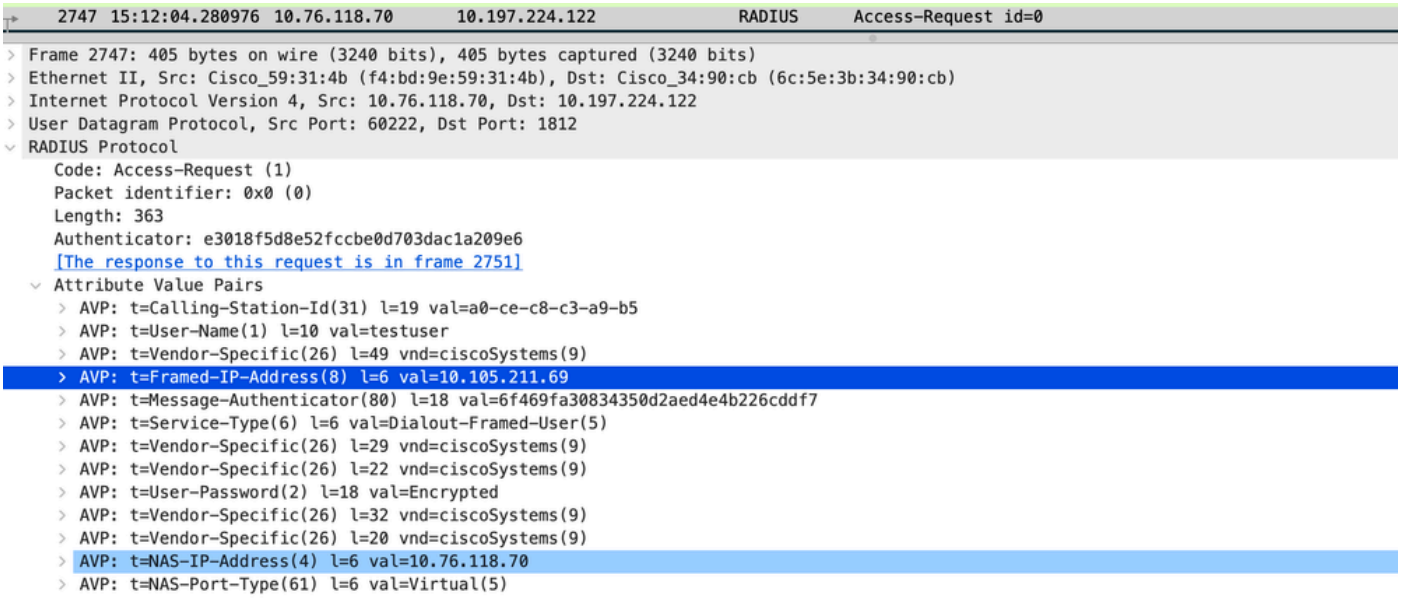
認証が成功すると、WebサーバへのTCPセッションが閉じられ、コントローラ上でクライアントポリシーマネージャの状態がRUNに移行します。



2348	15:11:38.598968	10.105.211.69	10.127.196.171	TCP	54381 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2678067533 TSecr=0
2349	15:11:38.599959	10.127.196.171	10.105.211.69	TCP	80 → 54381 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=256 SACK_PERM
2350	15:11:38.599959	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2351	15:11:38.600966	10.105.211.69	10.127.196.171	HTTP	GET /webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=http://3.3.3.3/
2352	15:11:38.602965	10.127.196.171	10.105.211.69	HTTP	[TCP Previous segment not captured] Continuation
2354	15:11:38.602965	10.127.196.171	10.105.211.69	TCP	[TCP Out-Of-Order] 80 → 54381 [ACK] Seq=1 Ack=485 Win=2097408 Len=1380
2355	15:11:38.603957	10.105.211.69	10.127.196.171	TCP	[TCP Dup ACK 2350#1] 54381 → 80 [ACK] Seq=485 Ack=1 Win=262144 Len=0 SLE=1381 SRE=1737
2356	15:11:38.603957	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=485 Ack=1737 Win=260352 Len=0
2358	15:11:38.615965	10.105.211.69	10.127.196.171	HTTP	GET /webauth/yourlogo.jpg HTTP/1.1
2359	15:11:38.616957	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2360	15:11:38.616957	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1113 Ack=1880 Win=261952 Len=0
2362	15:11:38.621961	10.105.211.69	10.127.196.171	HTTP	GET /webauth/aup.html HTTP/1.1
2363	15:11:38.623960	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2364	15:11:38.623960	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1706 Ack=2023 Win=261952 Len=0
2747	15:12:04.280976	10.76.118.70	10.197.224.122	RADIUS	Access-Request id=0
2751	15:12:04.682963	10.197.224.122	10.76.118.70	RADIUS	Access-Accept id=0
2836	15:12:09.729957	10.105.211.69	10.127.196.171	HTTP	GET /webauth/logout.html HTTP/1.1
2837	15:12:09.731956	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2838	15:12:09.731956	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=2186 Ack=2166 Win=261952 Len=0
4496	15:13:07.964946	10.105.211.69	10.127.196.171	TCP	54381 → 80 [FIN, ACK] Seq=2186 Ack=2166 Win=262144 Len=0
4497	15:13:07.964946	10.127.196.171	10.105.211.69	TCP	80 → 54381 [FIN, ACK] Seq=2166 Ack=2187 Win=2097408 Len=0
4498	15:13:07.965938	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=2187 Ack=2167 Win=262144 Len=0

クライアントがポータルページにHTTP GET要求を送信し、認証を正常に完了します

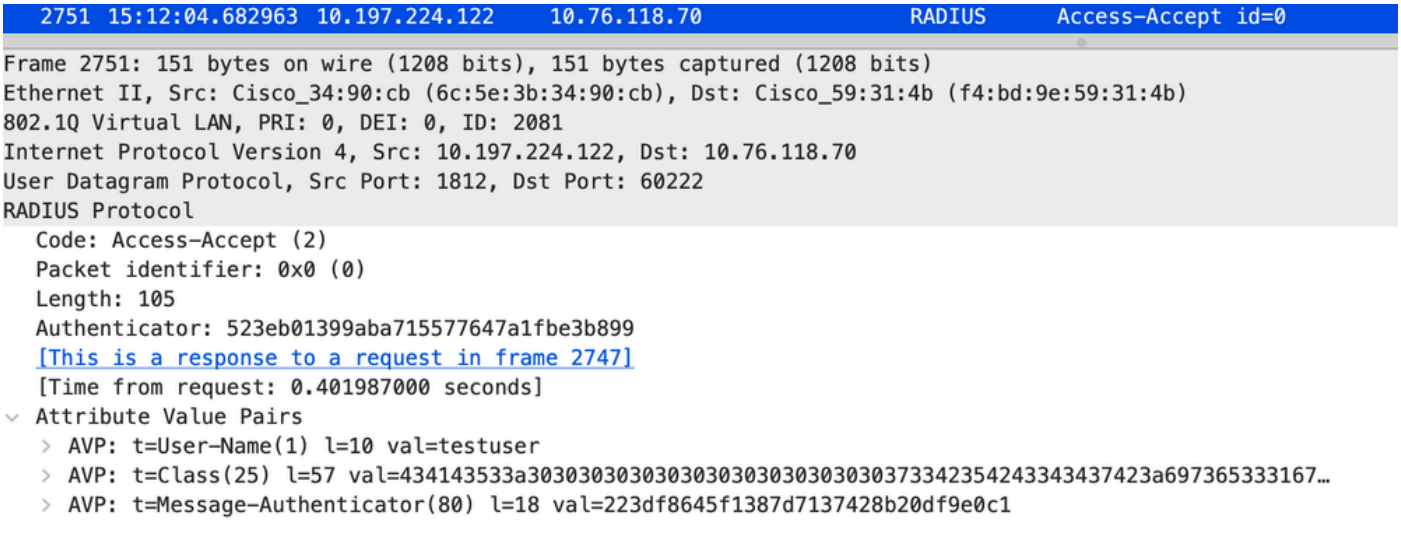
Radiusアクセス要求パケット



```
2747 15:12:04.280976 10.76.118.70 10.197.224.122 RADIUS Access-Request id=0
> Frame 2747: 405 bytes on wire (3240 bits), 405 bytes captured (3240 bits)
> Ethernet II, Src: Cisco_59:31:4b (f4:bd:9e:59:31:4b), Dst: Cisco_34:90:cb (6c:5e:3b:34:90:cb)
> Internet Protocol Version 4, Src: 10.76.118.70, Dst: 10.197.224.122
> User Datagram Protocol, Src Port: 60222, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 363
    Authenticator: e3018f5d8e52fccbe0d703dac1a209e6
    [The response to this request is in frame 2751]
  v Attribute Value Pairs
    > AVP: t=Calling-Station-Id(31) l=19 val=a0-ce-c8-c3-a9-b5
    > AVP: t=User-Name(1) l=10 val=testuser
    > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    > AVP: t=Framed-IP-Address(8) l=6 val=10.105.211.69
    > AVP: t=Message-Authenticator(80) l=18 val=6f469fa30834350d2aed4e4b226cddf7
    > AVP: t=Service-Type(6) l=6 val=Dialout-Framed-User(5)
    > AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=22 vnd=ciscoSystems(9)
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
    > AVP: t=NAS-IP-Address(4) l=6 val=10.76.118.70
    > AVP: t=NAS-Port-Type(61) l=6 val=Virtual(5)
```

アクセス要求パケット

Radius Access Acceptパケット



```
2751 15:12:04.682963 10.197.224.122 10.76.118.70 RADIUS Access-Accept id=0
Frame 2751: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
Ethernet II, Src: Cisco_34:90:cb (6c:5e:3b:34:90:cb), Dst: Cisco_59:31:4b (f4:bd:9e:59:31:4b)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2081
Internet Protocol Version 4, Src: 10.197.224.122, Dst: 10.76.118.70
User Datagram Protocol, Src Port: 1812, Dst Port: 60222
RADIUS Protocol
  Code: Access-Accept (2)
  Packet identifier: 0x0 (0)
  Length: 105
  Authenticator: 523eb01399aba715577647a1fbe3b899
  [This is a response to a request in frame 2747]
  [Time from request: 0.401987000 seconds]
v Attribute Value Pairs
  > AVP: t=User-Name(1) l=10 val=testuser
  > AVP: t=Class(25) l=57 val=434143533a3030303030303030303030303733423542433434374237a697365333167…
  > AVP: t=Message-Authenticator(80) l=18 val=223df8645f1387d7137428b20df9e0c1
```

Access Acceptパケット

関連情報

Catalyst 9800でのWLANアンカーモビリティ機能の設定

AireOSコントローラによる有線ゲストアクセスの設定例

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。