設定無線區域網路控制器中的有線訪客驗證和疑難排解

目錄

簡介

本文說明如何使用外部Web驗證在9800和IRCM中設定、驗證和疑難排解有線訪客存取。

必要條件

需求

思科建議您瞭解以下主題：

9800 WLC

AireOS WLC

行動通道

ISE

假設在設定有線訪客存取之前，已在兩個WLC之間建立行動通道。

此方面不在本組態範例範圍內。有關詳細說明，請參閱附件標題為在9800上配置移動拓撲的檔案

採用元件

9800 WLC版本17.12.1

5520 WLC版本8.10.185.0

ISE版本3.1.0.518

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

在錨定到另一個catalyst 9800的catalyst 9800上配置有線訪客

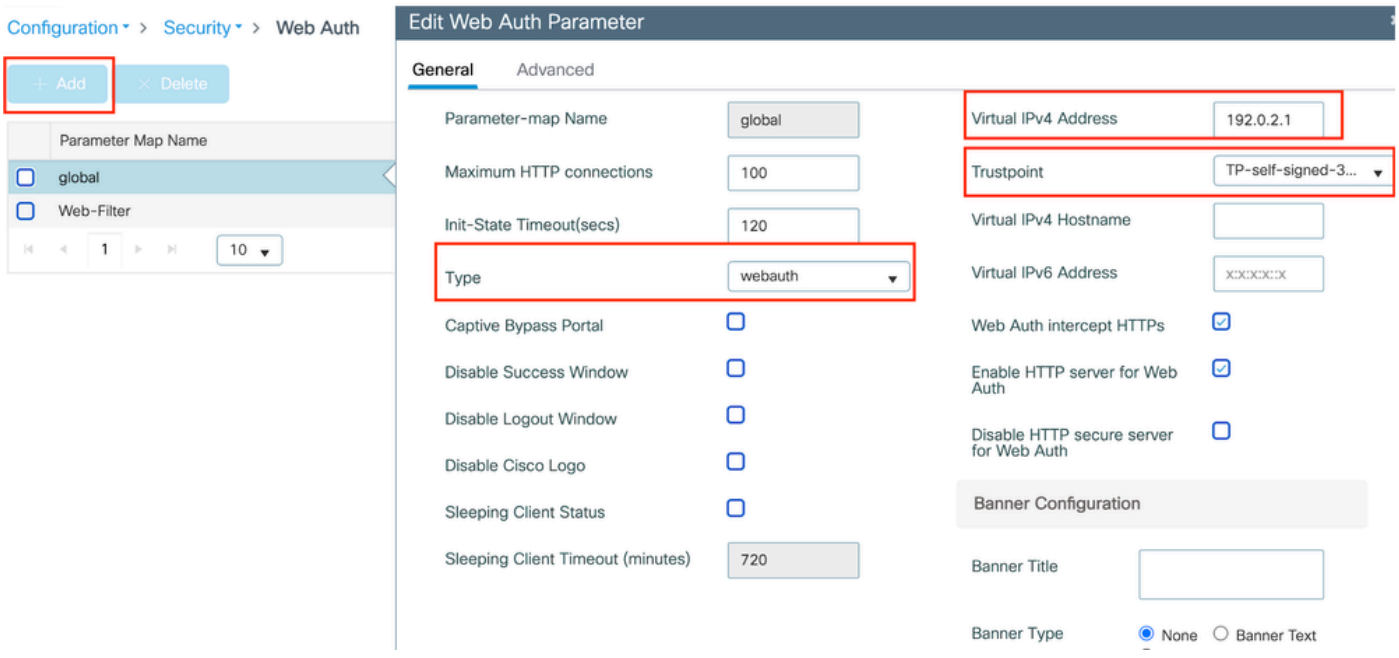
網路圖表

網路拓撲

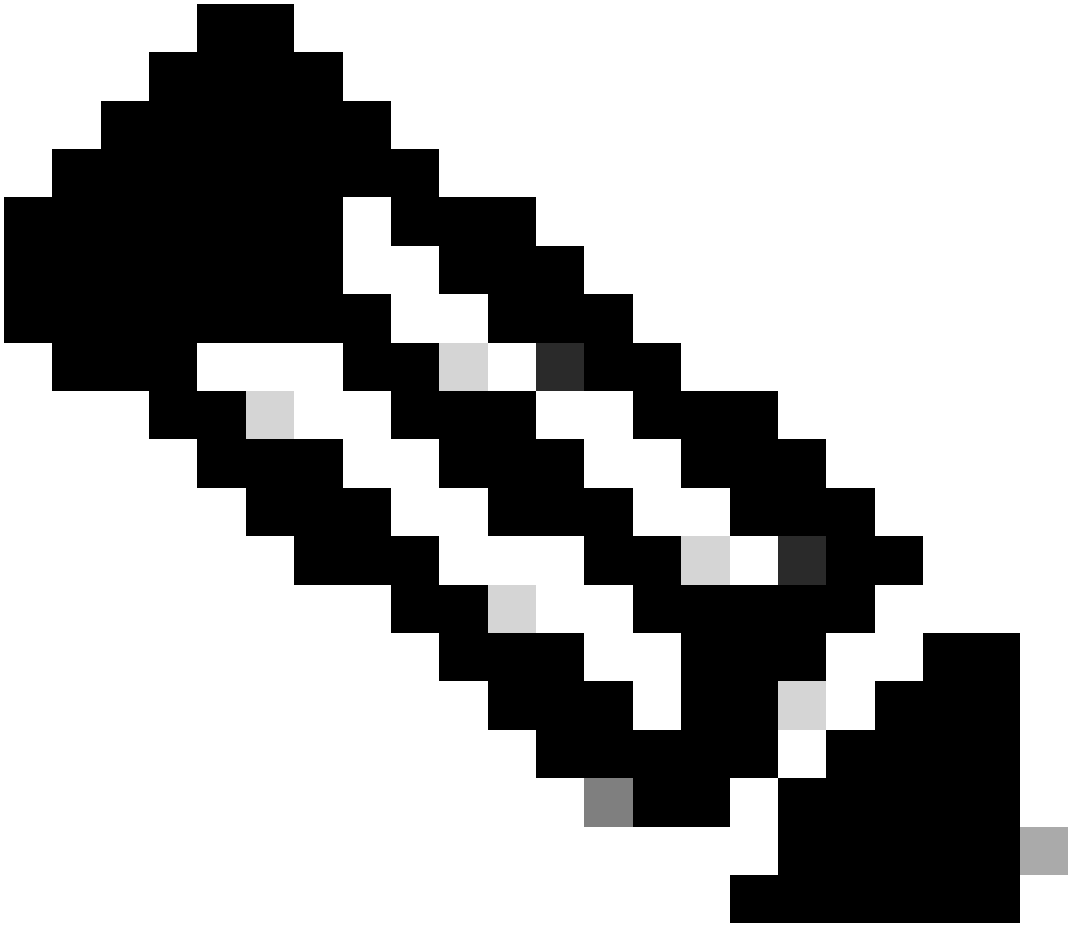
外部9800 WLC上的配置

配置Web引數對映

第1步：導航到配置>安全> Web身份驗證，選擇全局，驗證控制器的虛擬IP地址和信任點對映，並確保將型別設定為webauth。

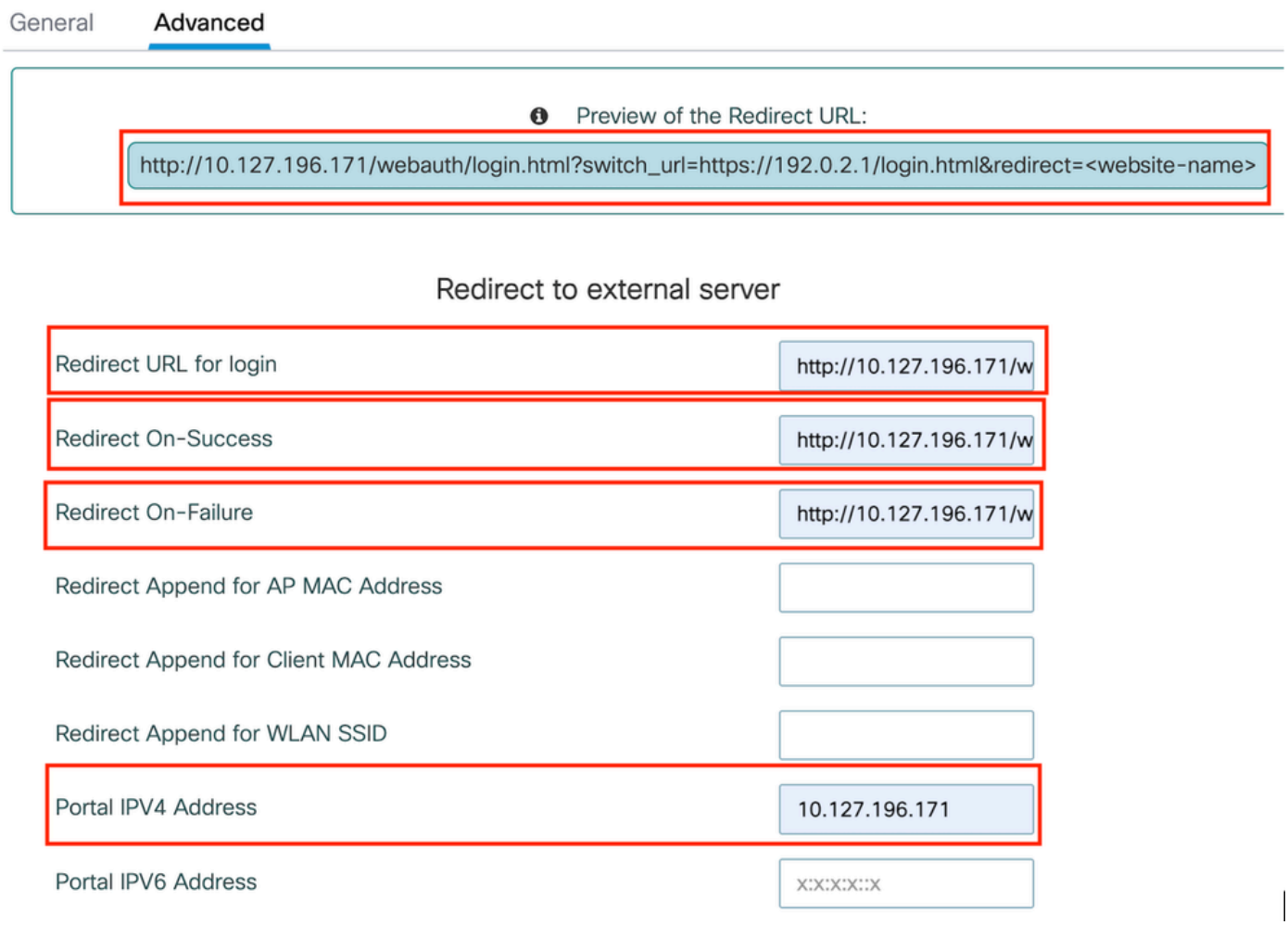


全局引數對映



附註： Web Auth intercept HTTPs是選用設定。如果需要HTTPS重新導向，則必須啟用Web Auth攔截HTTPS選項。但是，不建議使用此配置，因為它會增加CPU使用率。

第2步：在高級頁籤下，配置客戶端重定向的外部網頁URL。設定「Redirect URL for Login」和「Redirect On-Failure」；「Redirect On-Success」是選用的。設定後，重新導向URL的預覽會顯示在Web Auth設定檔上。



進階標籤

CLI配置

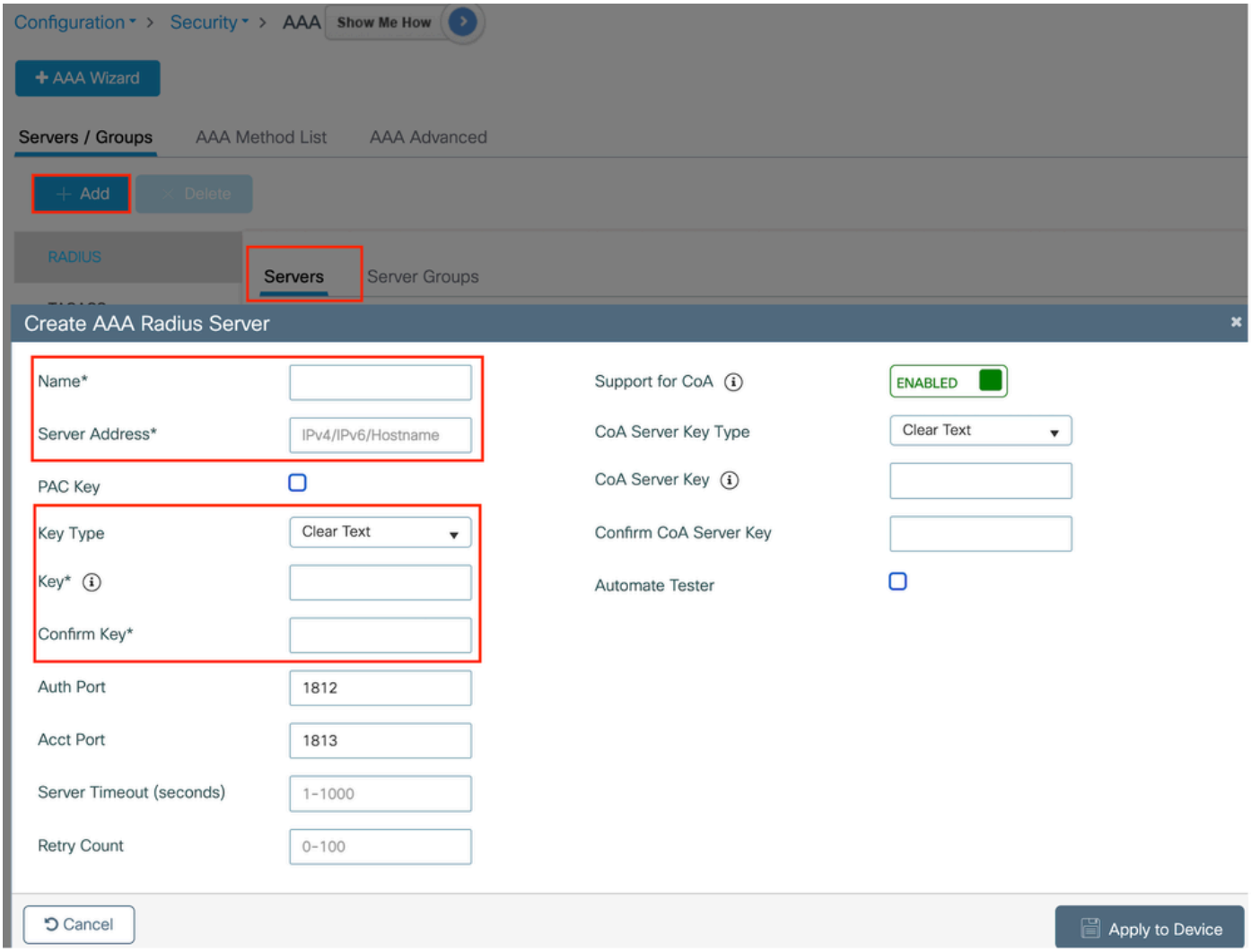
```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171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

附註：在此案例中，會使用全域引數對應。根據要求，選取新增來設定自訂Web引數對應，並在「進階」標籤下設定重新導向URL。信任點和虛擬IP設定從全局配置檔案繼承。

AAA設定：

步驟1：建立Radius伺服器：

導航到Configuration > Security > AAA，按一下Server/Group部分下的「Add」，然後在「Create AAA Radius Server」頁中輸入伺服器名稱、IP地址和共用金鑰。

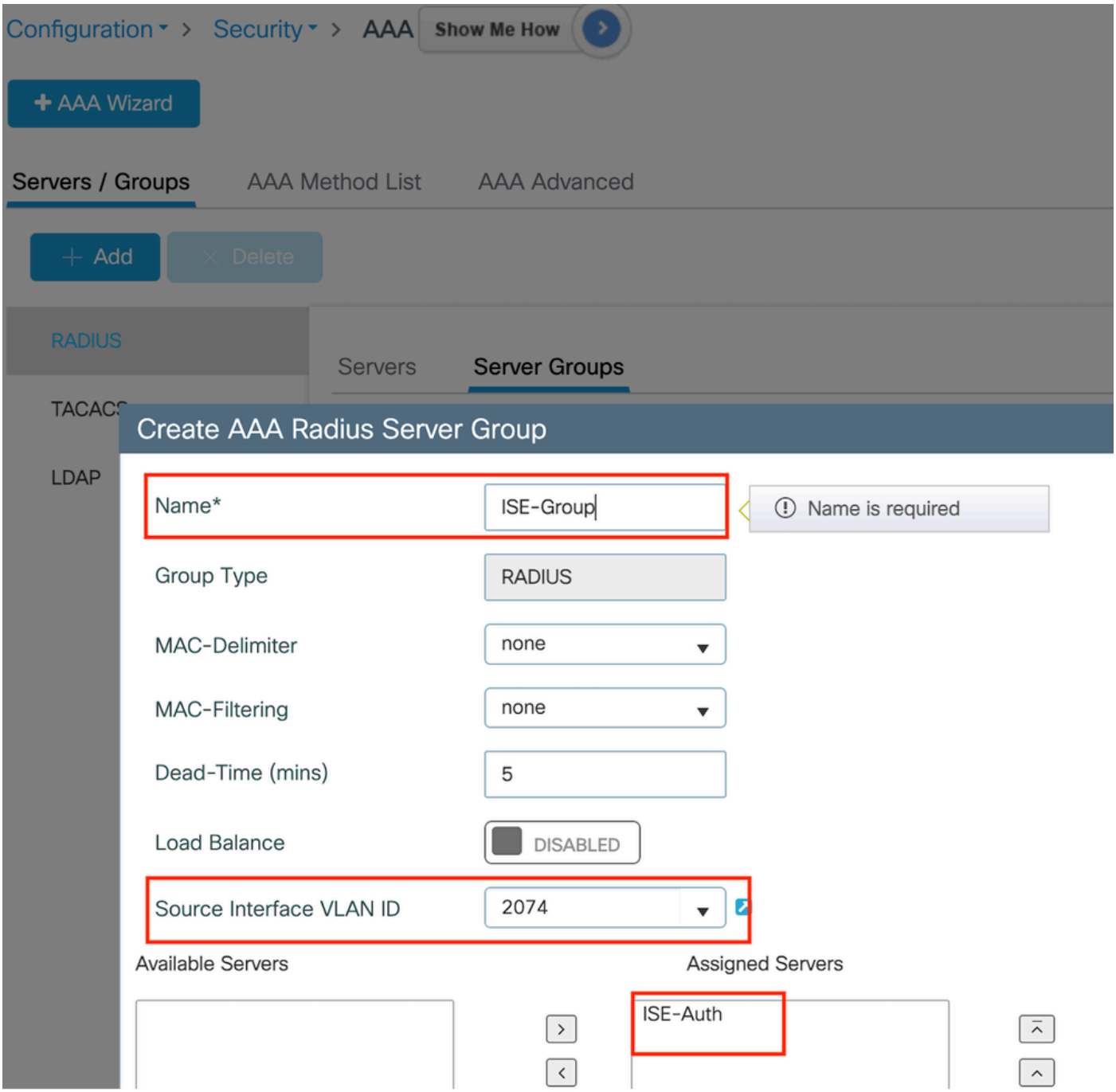


Radius伺服器配置

CLI配置

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

第2步：建立RADIUS伺服器組：
在「伺服器群組」段落下選取「新增」以定義伺服器群組，並切換要包含在群組組態中的伺服器。



Radius伺服器組

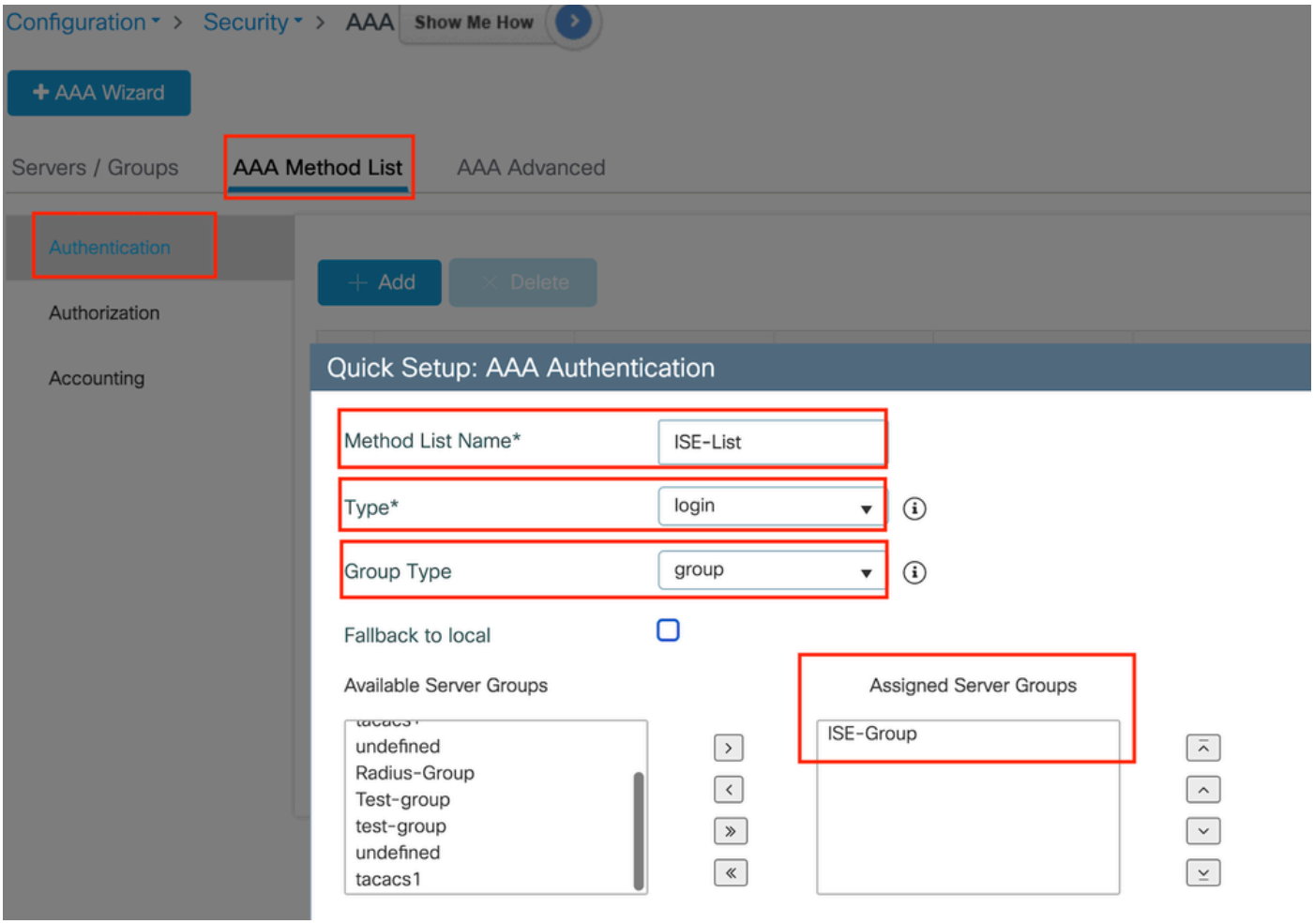
CLI配置

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

第3步：配置AAA方法清單：

導航到AAA Method List頁籤，選擇Authentication下的Add，定義Type為「login」且Group type為

「Group」的方法清單名稱，並在Assigned Server Group部分下對映配置的身份驗證伺服器組。



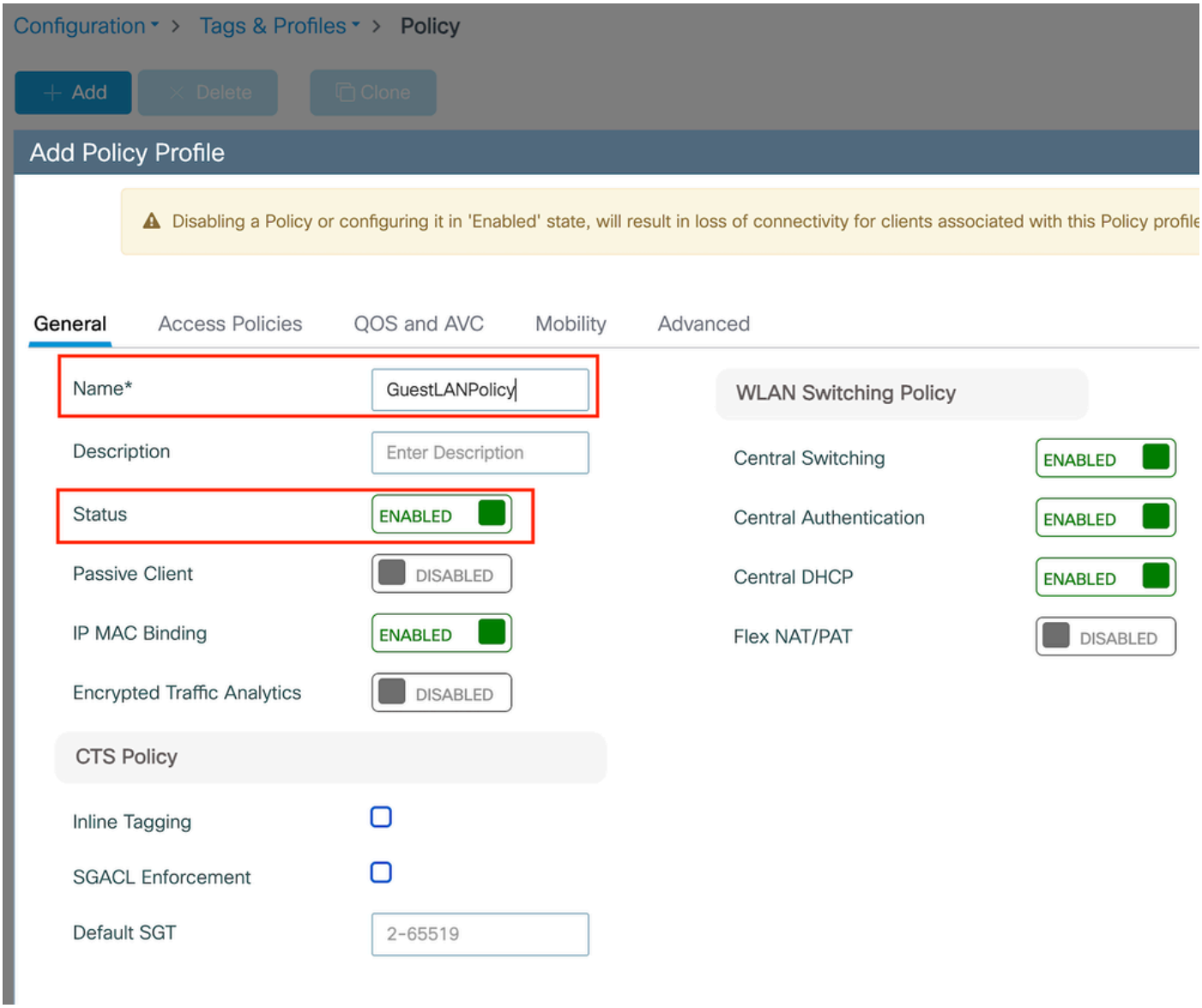
驗證方法清單

CLI配置

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

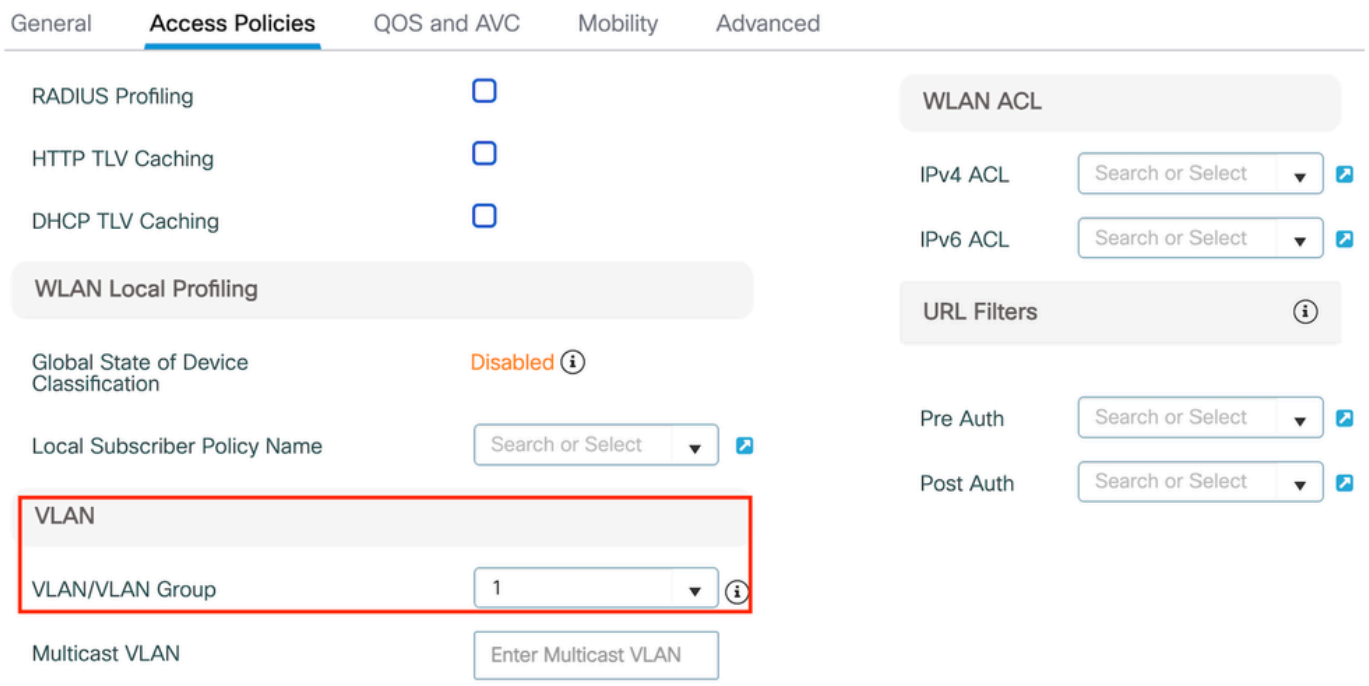
配置策略配置檔案

第1步：導航到配置>標籤和配置檔案>策略，在常規頁籤中命名您的新配置檔案，並使用狀態切換啟用它。



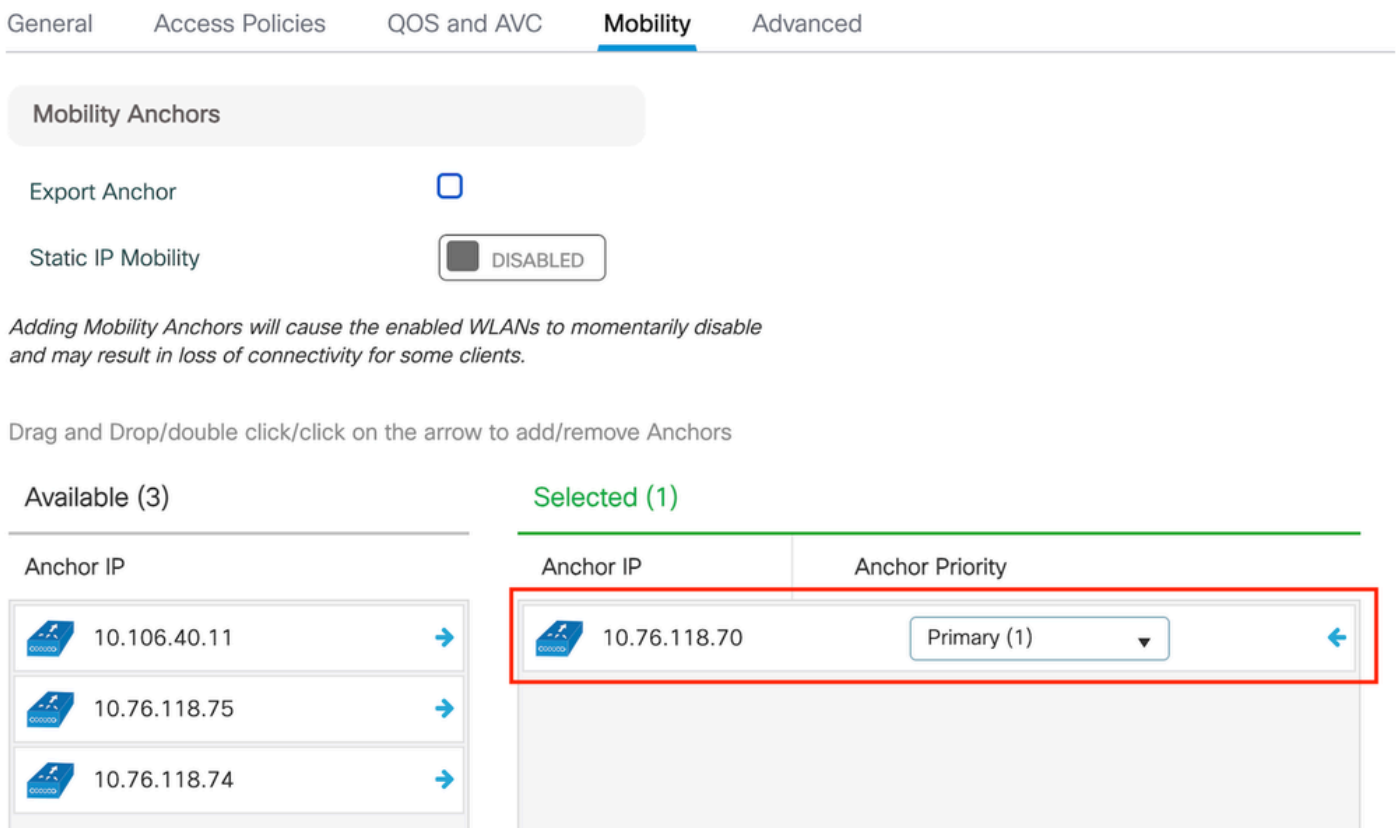
策略配置檔案

第2步：在訪問策略頁籤下，在錨點控制器上完成vlan對映時分配隨機vlan。在本例中，配置了vlan 1



訪問策略頁籤

第3步：在移動頁籤下，將錨點控制器切換到主(1)，並根據冗餘要求配置輔助和第三移動隧道



移動圖

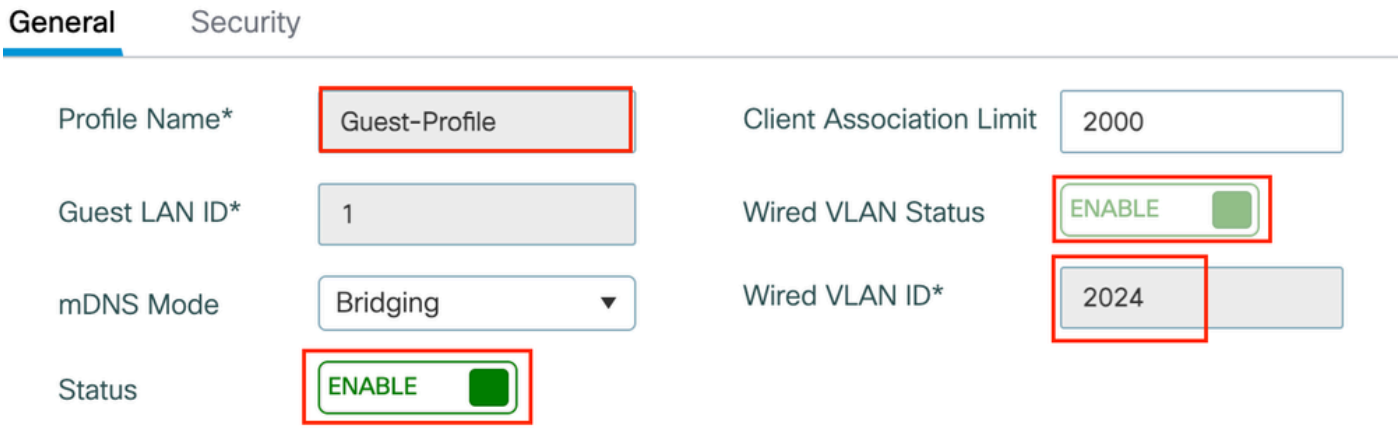
CLI配置

```
wireless profile policy GuestLANPolicy
```

```
mobility anchor 10.76.118.70 priority 1
no shutdown
```

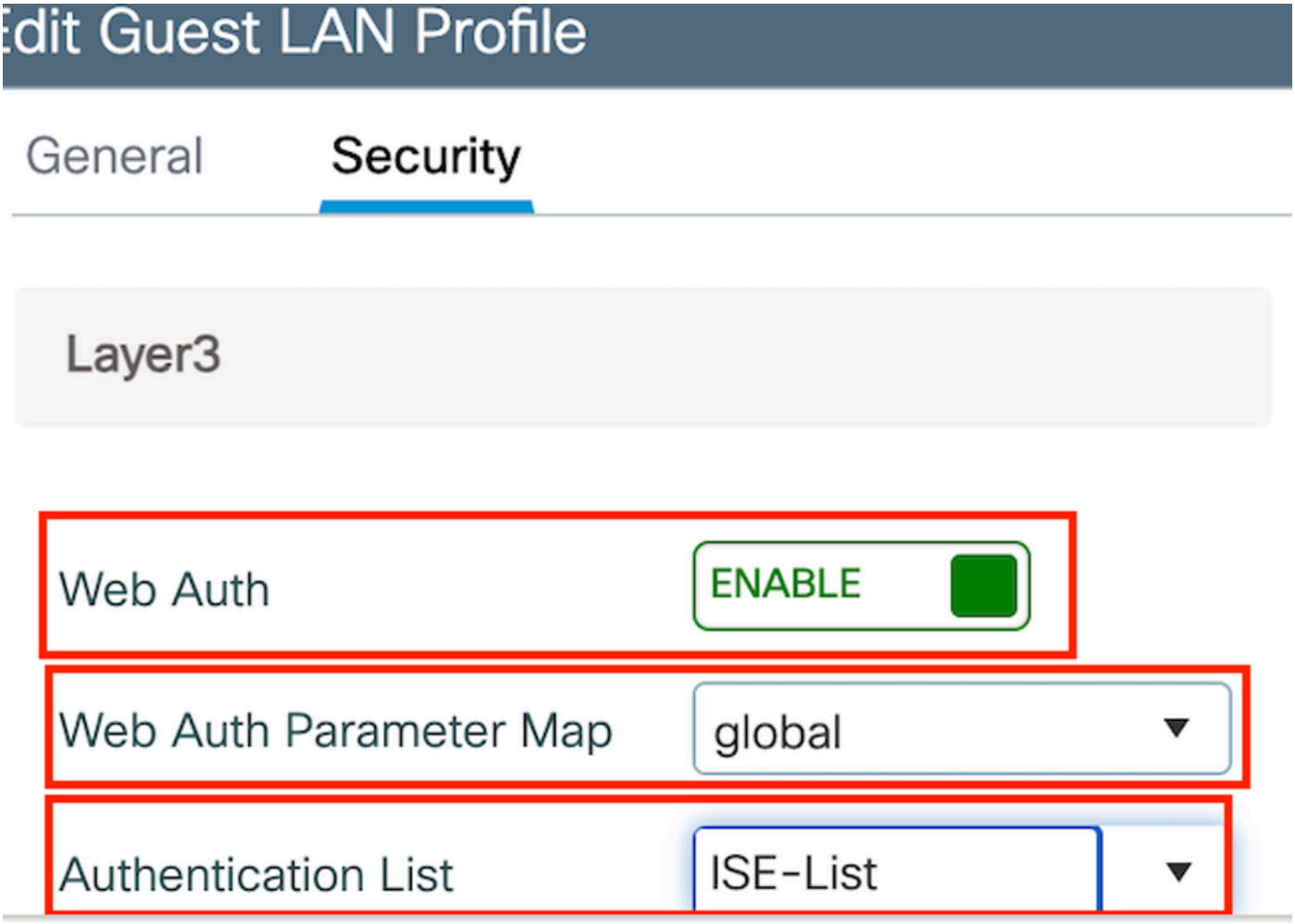
設定訪客LAN設定檔

第1步：導航到配置>無線>訪客LAN，選擇增加，配置唯一的配置檔名稱，啟用有線VLAN，輸入有線訪客使用者的VLAN ID，並將配置檔案狀態切換為啟用。



訪客LAN配置檔案

第2步：在Security頁籤下，啟用Web Auth，對映Web Auth引數對映，然後從Authentication下拉選單中選擇Radius伺服器。



訪客LAN安全頁籤

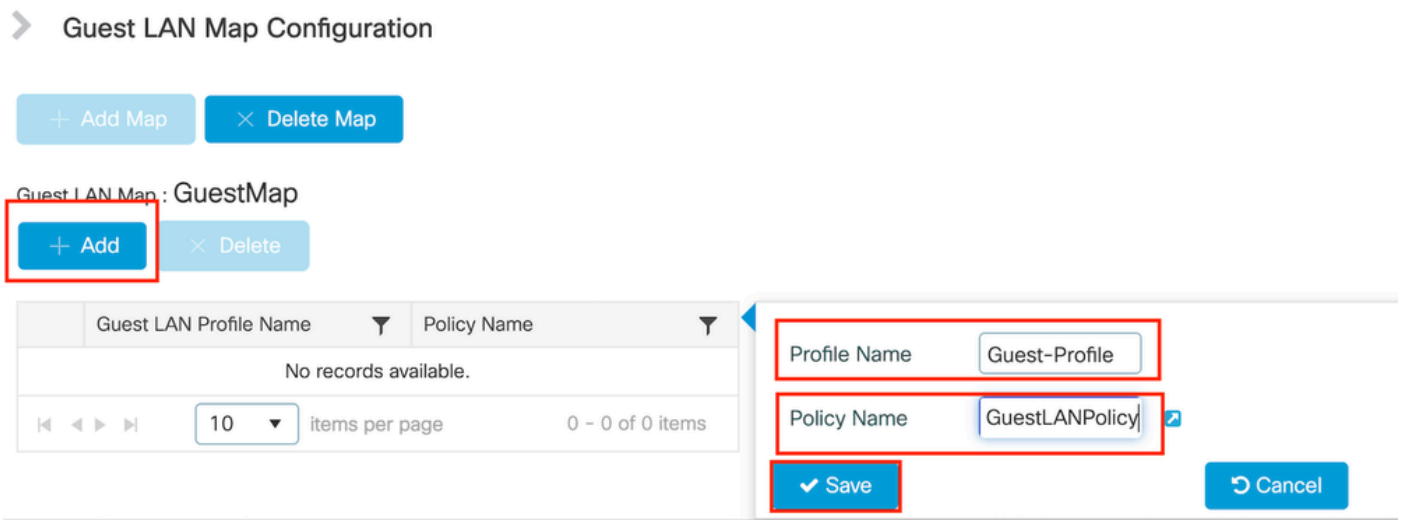
CLI配置

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

訪客LAN對映

導航到Configuration > Wireless > Guest LAN。

在訪客LAN對映配置部分，選擇增加並對映策略配置檔案和訪客LAN配置檔案



訪客LAN對映

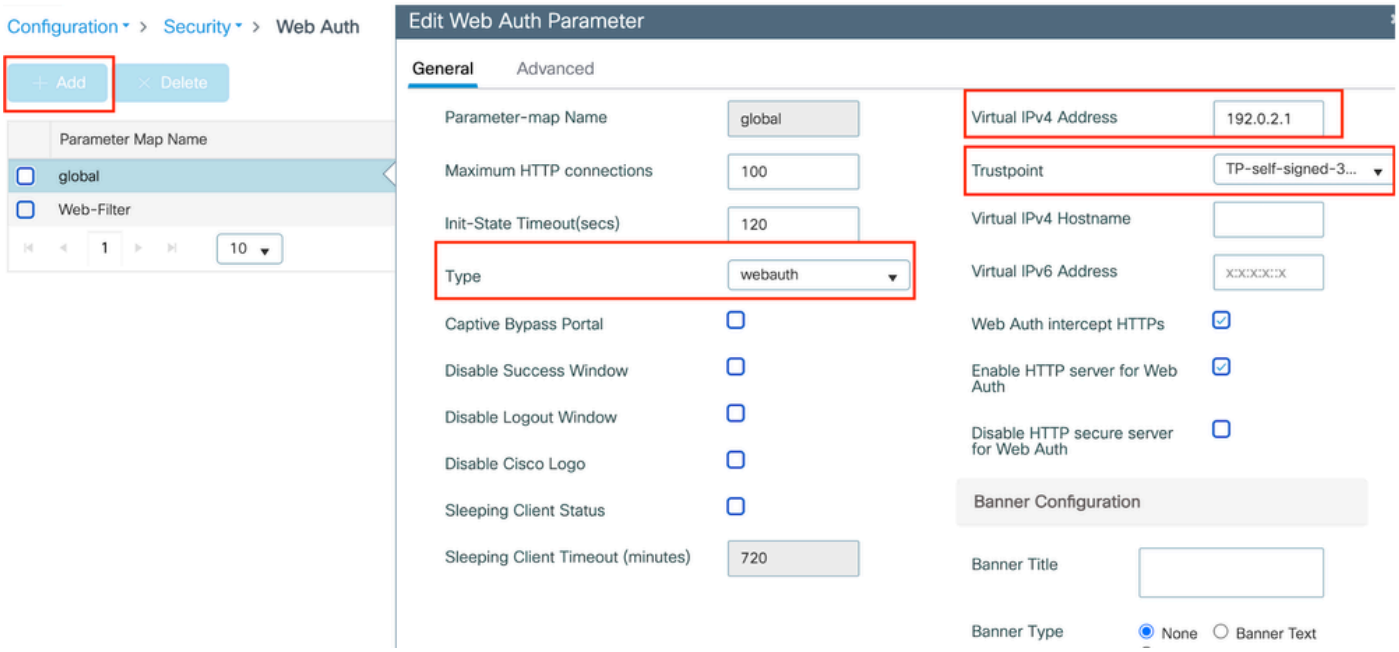
CLI配置

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

錨點9800 WLC上的組態

配置Web引數對映

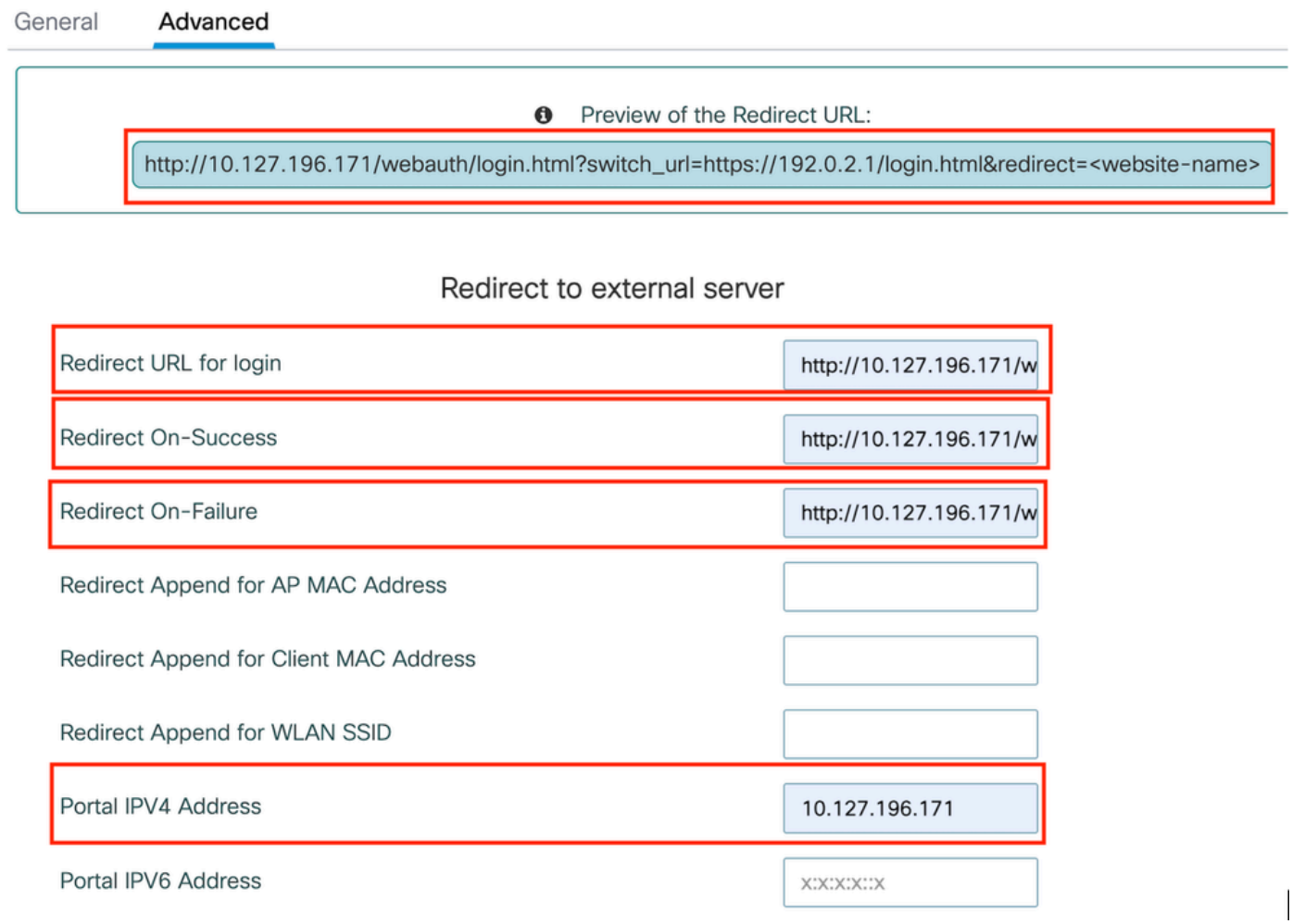
第1步：導航到配置>安全> Web身份驗證，選擇全局，驗證控制器的虛擬IP地址和信任點對映，並確保將型別設定為webauth。



全局引數對映

第2步：在高級頁籤下，配置客戶端重定向的外部網頁URL。設定「Redirect URL for Login」和「Redirect On-Failure」；「Redirect On-Success」是選用的。

設定後，重新導向URL的預覽會顯示在Web Auth設定檔上。



進階標籤

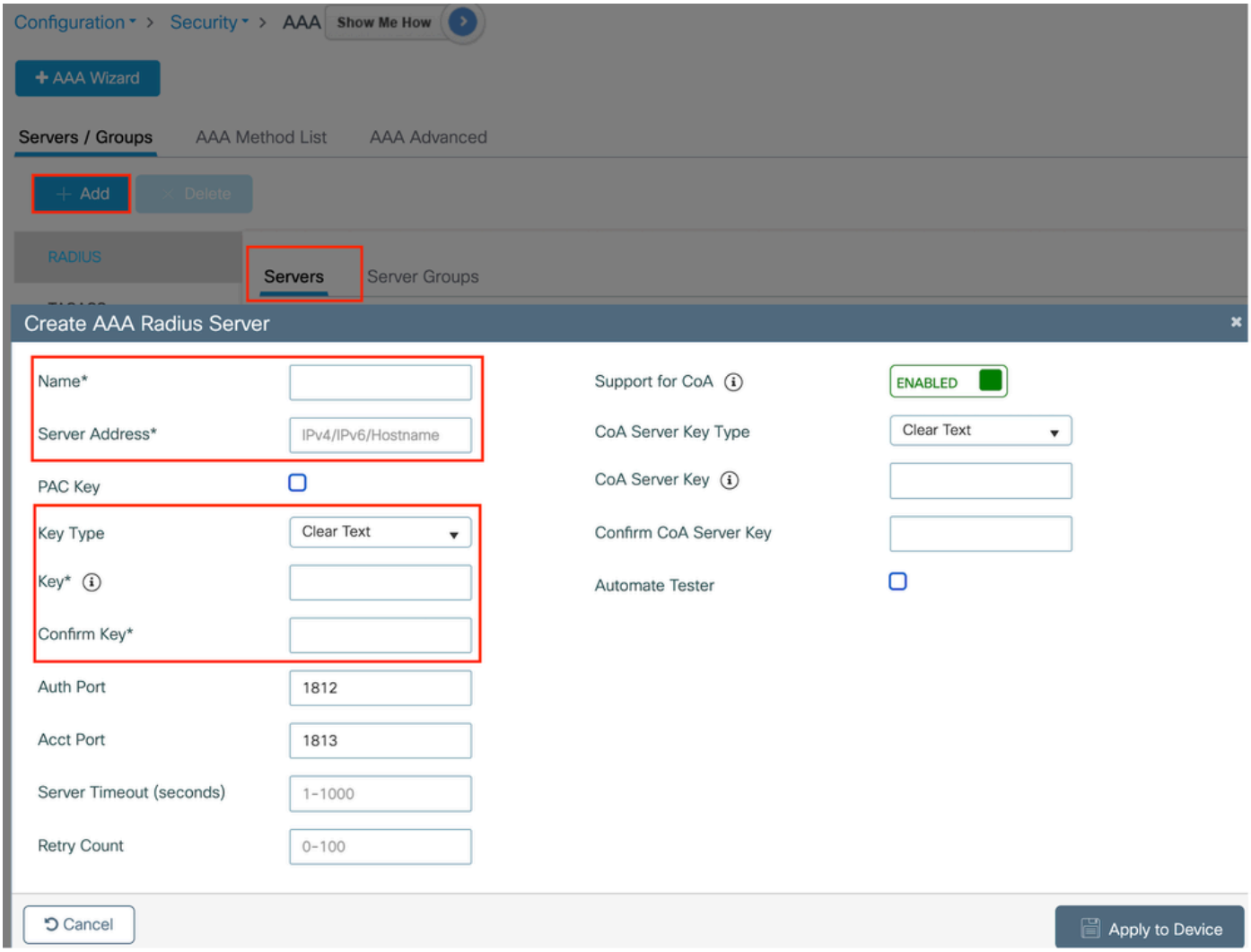
CLI配置

```
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：

步驟1：建立Radius伺服器：

導航到Configuration > Security > AAA，按一下Server/Group部分下的Add，然後在「Create AAA Radius Server」頁上，輸入伺服器名稱、IP地址和共用金鑰。

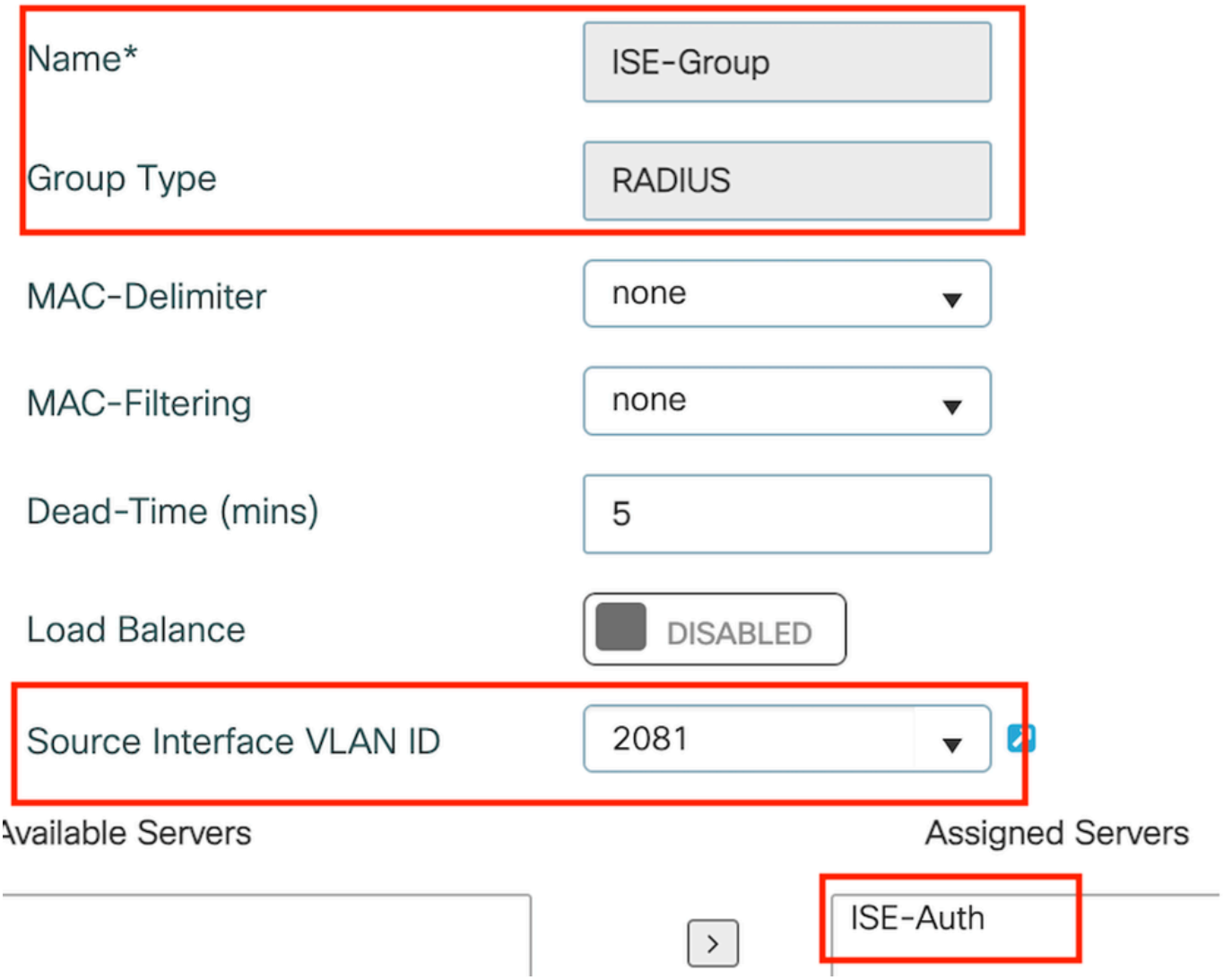


Radius伺服器配置

CLI配置

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

第2步：建立RADIUS伺服器組：
在「Server Groups」部分下選擇Add以定義伺服器組，並切換要包括在組配置中的伺服器。



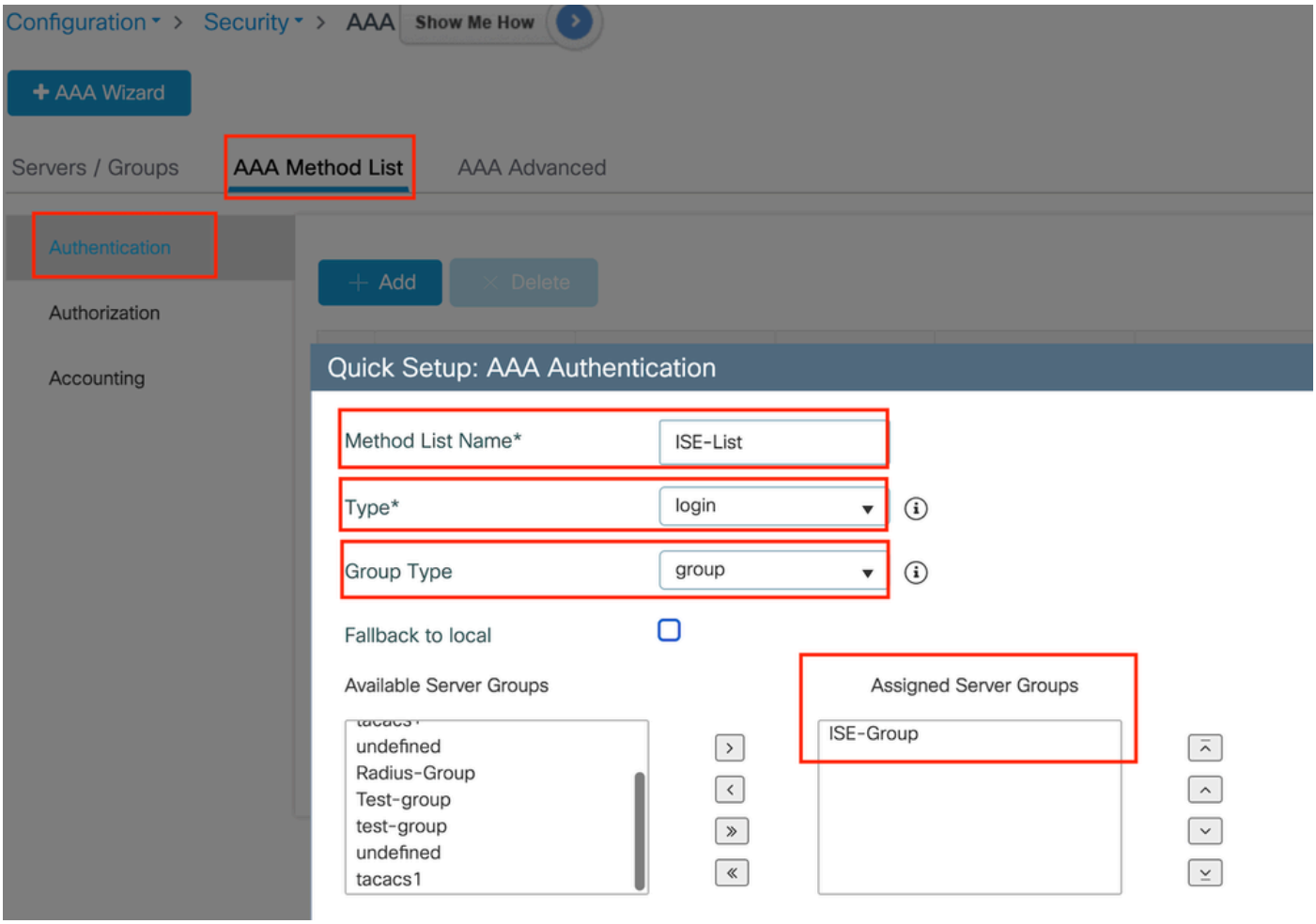
錨點半徑組

CLI配置

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

第3步：配置AAA方法清單：

導航到AAA Method List頁籤，選擇Authentication下的Add，使用「Type」作為「login」定義「Type」並將「Group type」作為「Group」定義「method list name」，然後在「Assigned Server Group」部分下對映配置的身份驗證伺服器組。



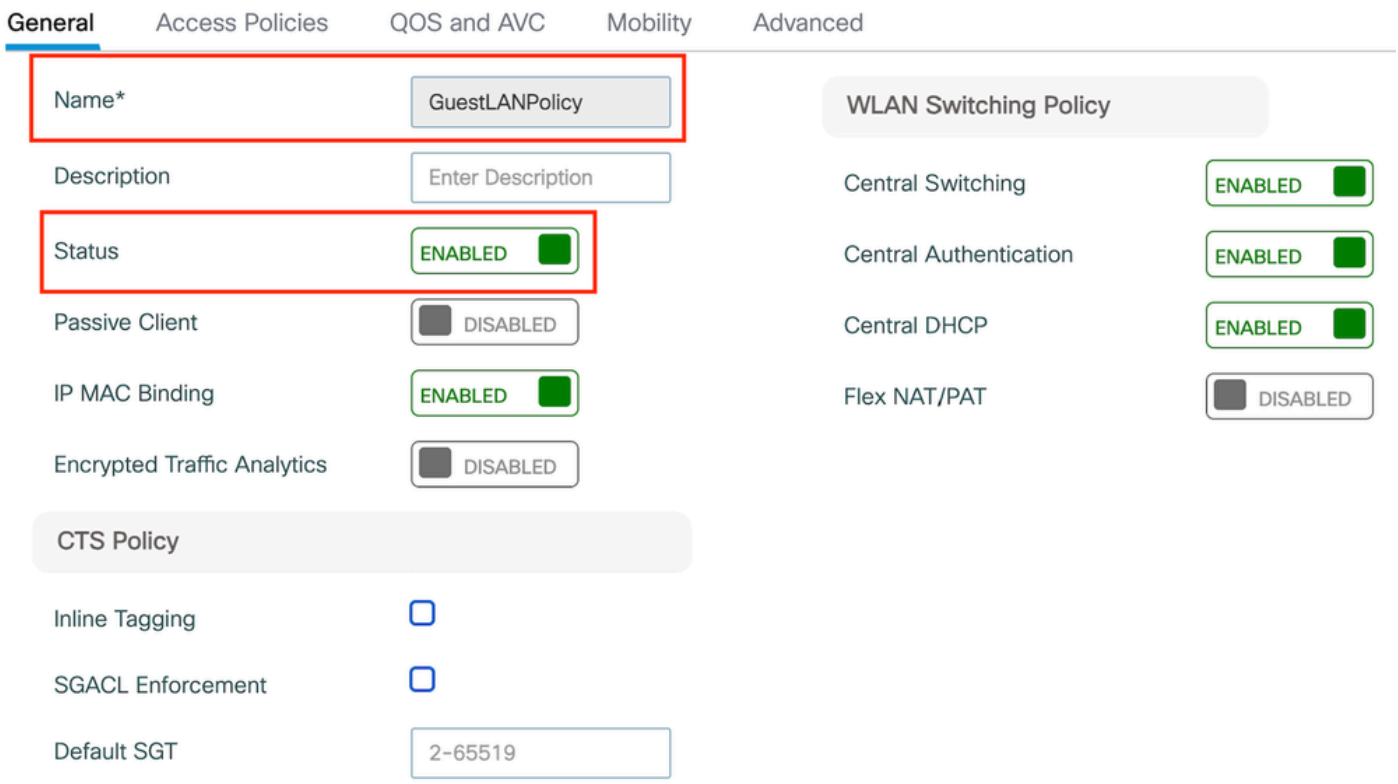
驗證方法清單

CLI配置

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

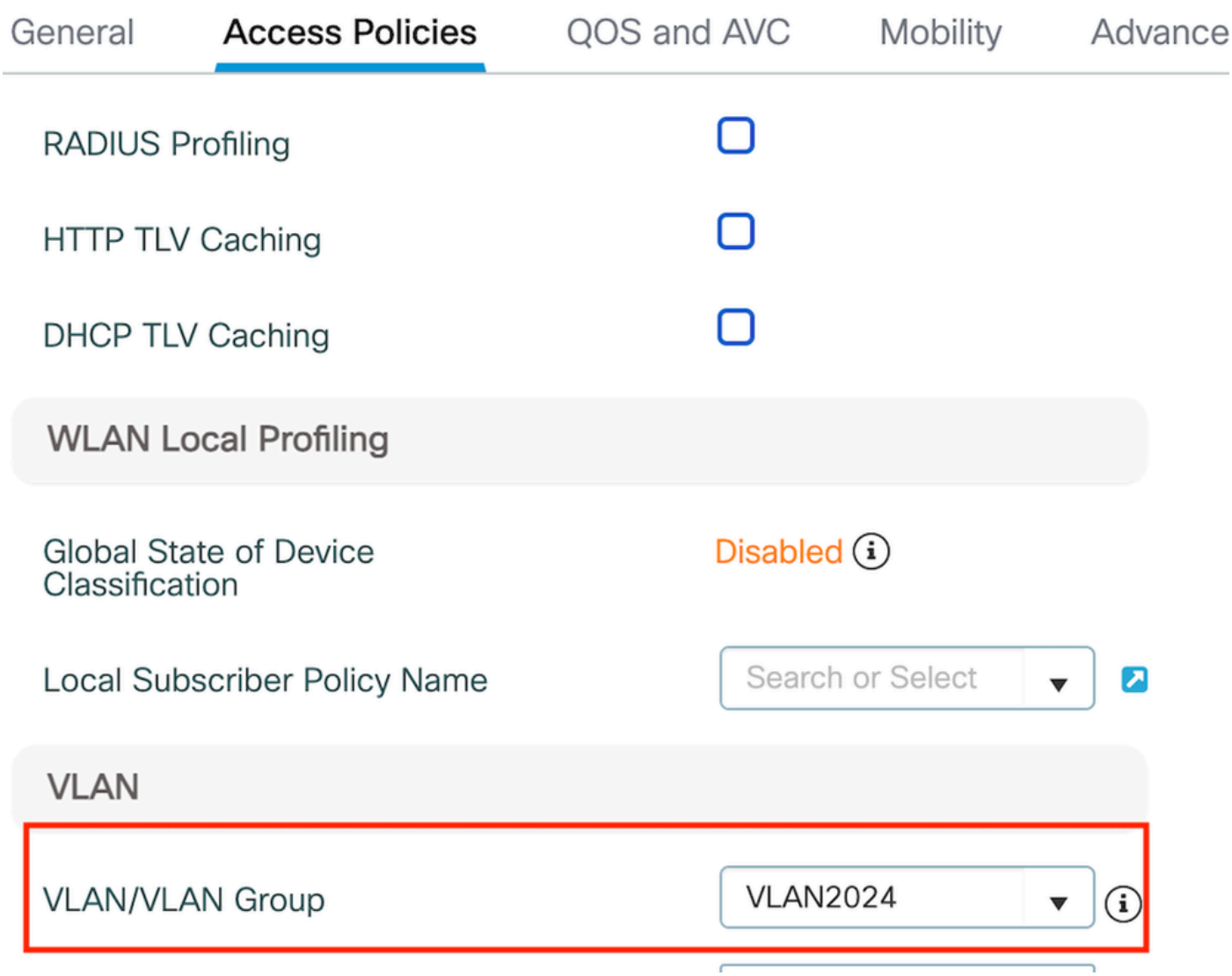
配置策略配置檔案

第1步：導航到配置>標籤和配置檔案>策略，使用與外部控制器上的名稱配置策略配置檔案並啟用配置檔案。

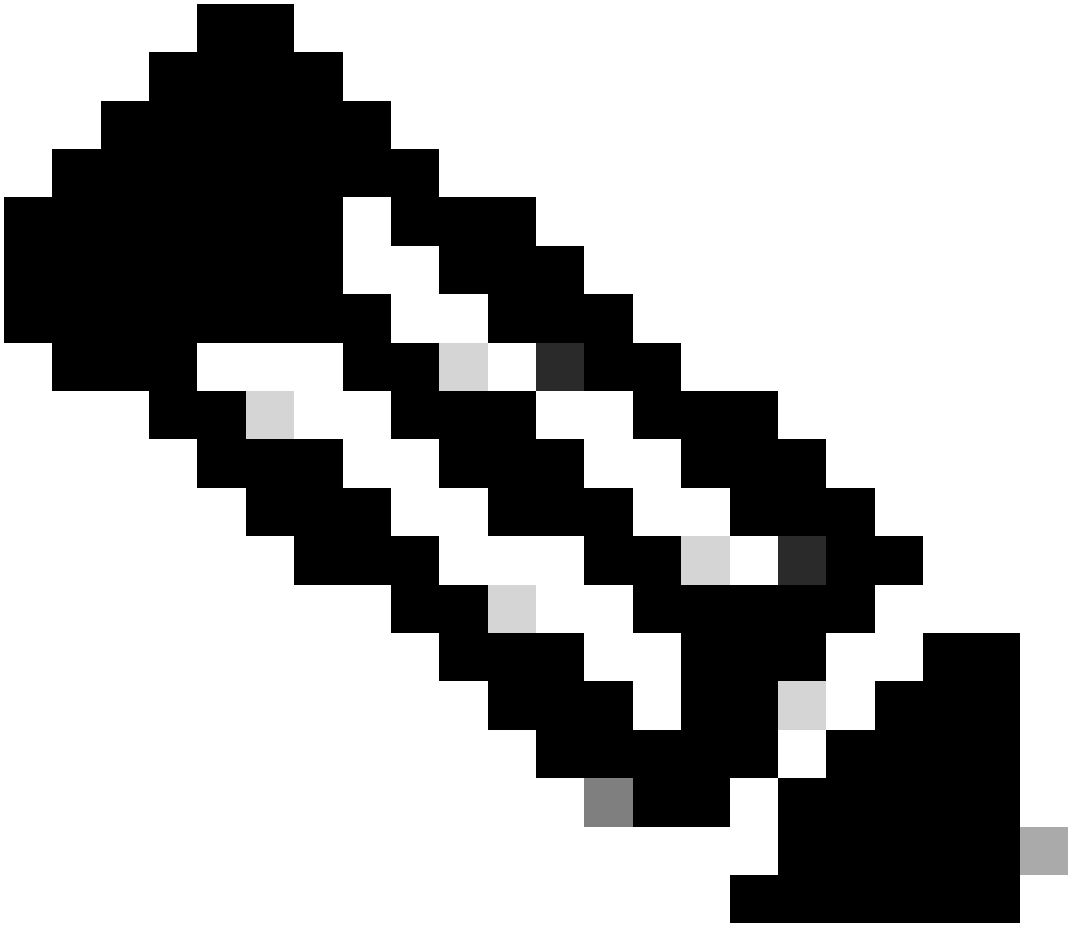


錨點策略配置檔案

第2步：在訪問策略下，從下拉選單中對映有線客戶端VLAN

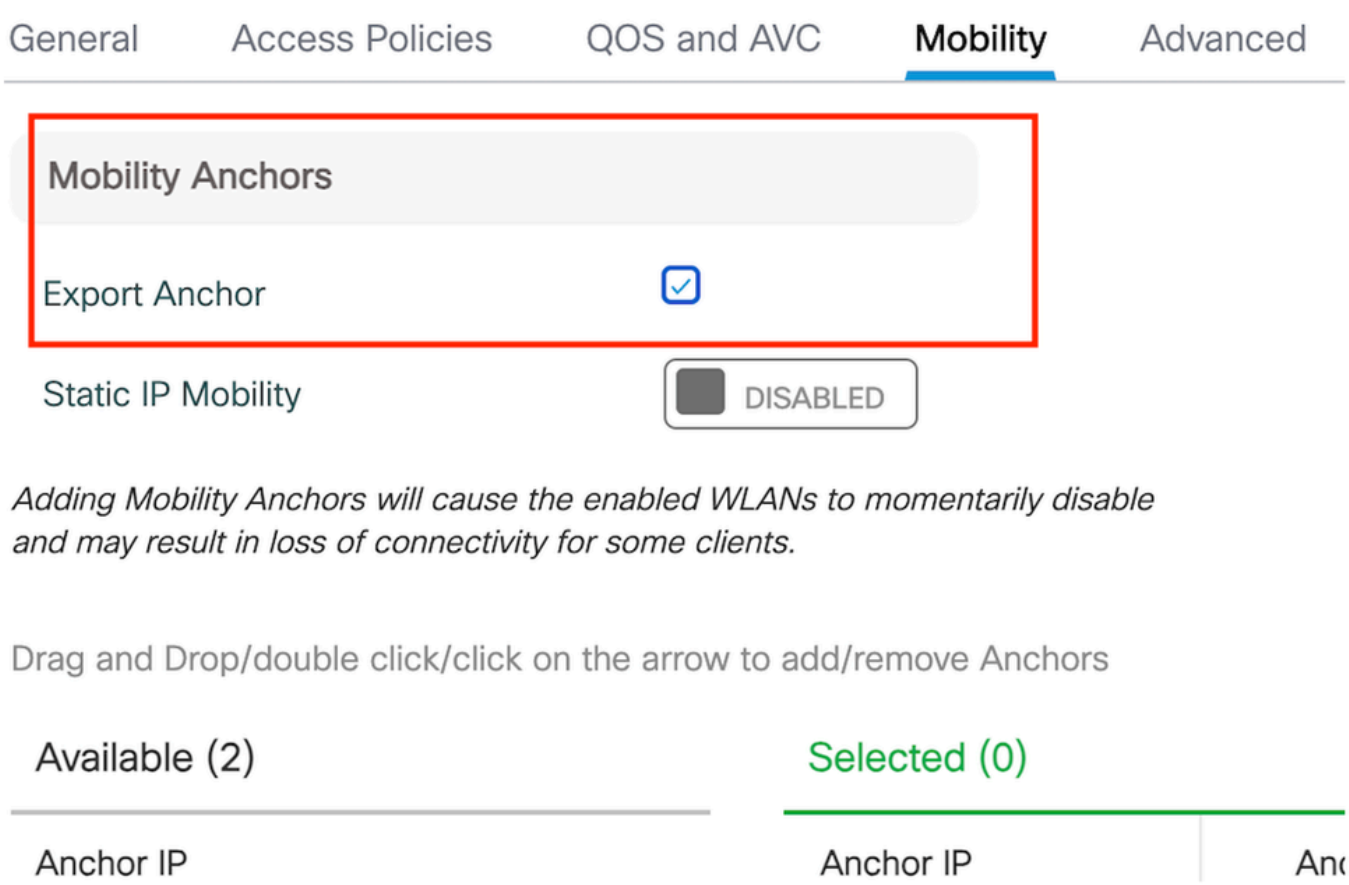

General
Access Policies
QOS and AVC
Mobility
Advance
RADIUS Profiling
HTTP TLV Caching
DHCP TLV Caching
WLAN Local Profiling
Global State of Device Classification
Disabled
Local Subscriber Policy Name
Search or Select
VLAN
VLAN/VLAN Group
VLAN2024

訪問策略頁籤

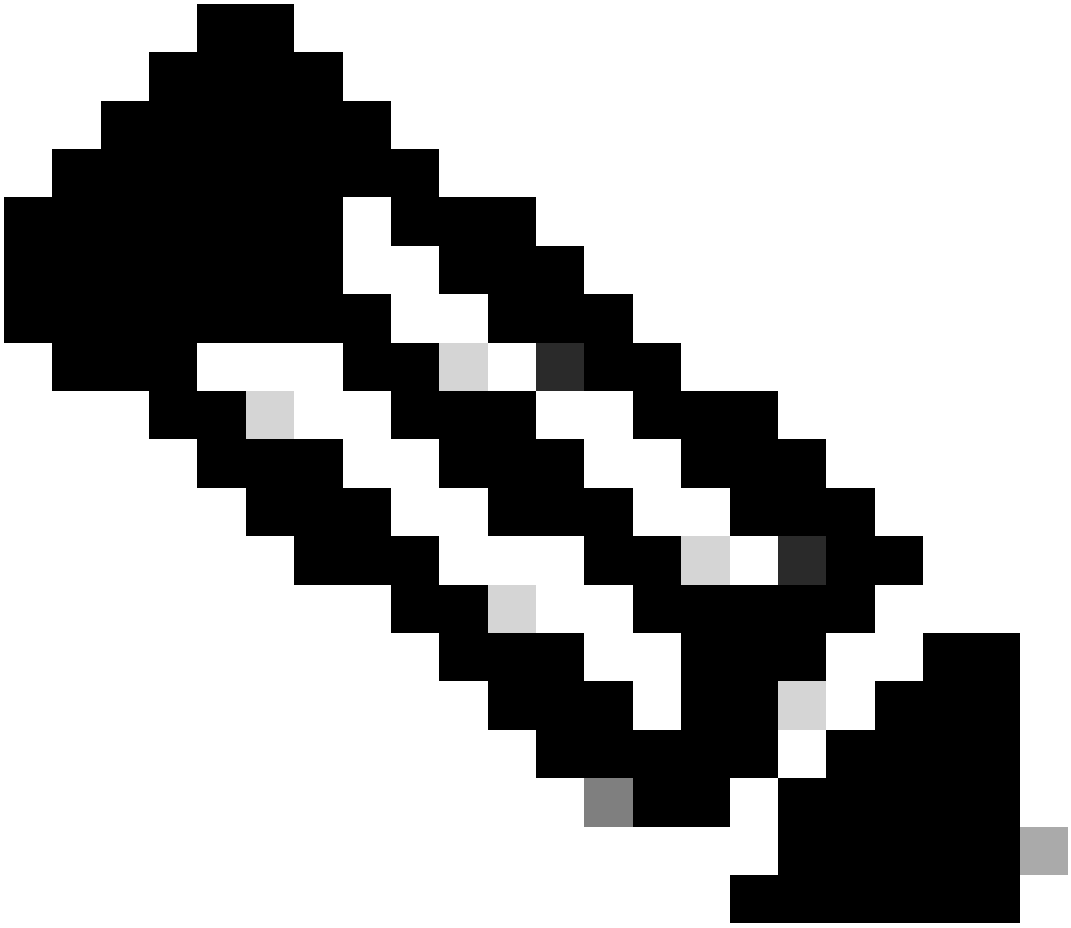


注意：除VLAN外，其他控制器和錨點控制器上的策略配置檔案配置必須匹配。

第3步：在移動頁籤下，選中導出錨點覈取方塊。


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

匯出錨點



注意：此組態會指定9800無線LAN控制器(WLC)為與指定原則設定檔關聯任何WLAN的錨點WLC。當外部9800 WLC將客戶端重定向到錨點WLC時，它提供有關分配給客戶端的WLAN和策略配置檔案的詳細資訊。這使錨點WLC能夠根據收到的資訊應用適當的本地策略配置檔案。

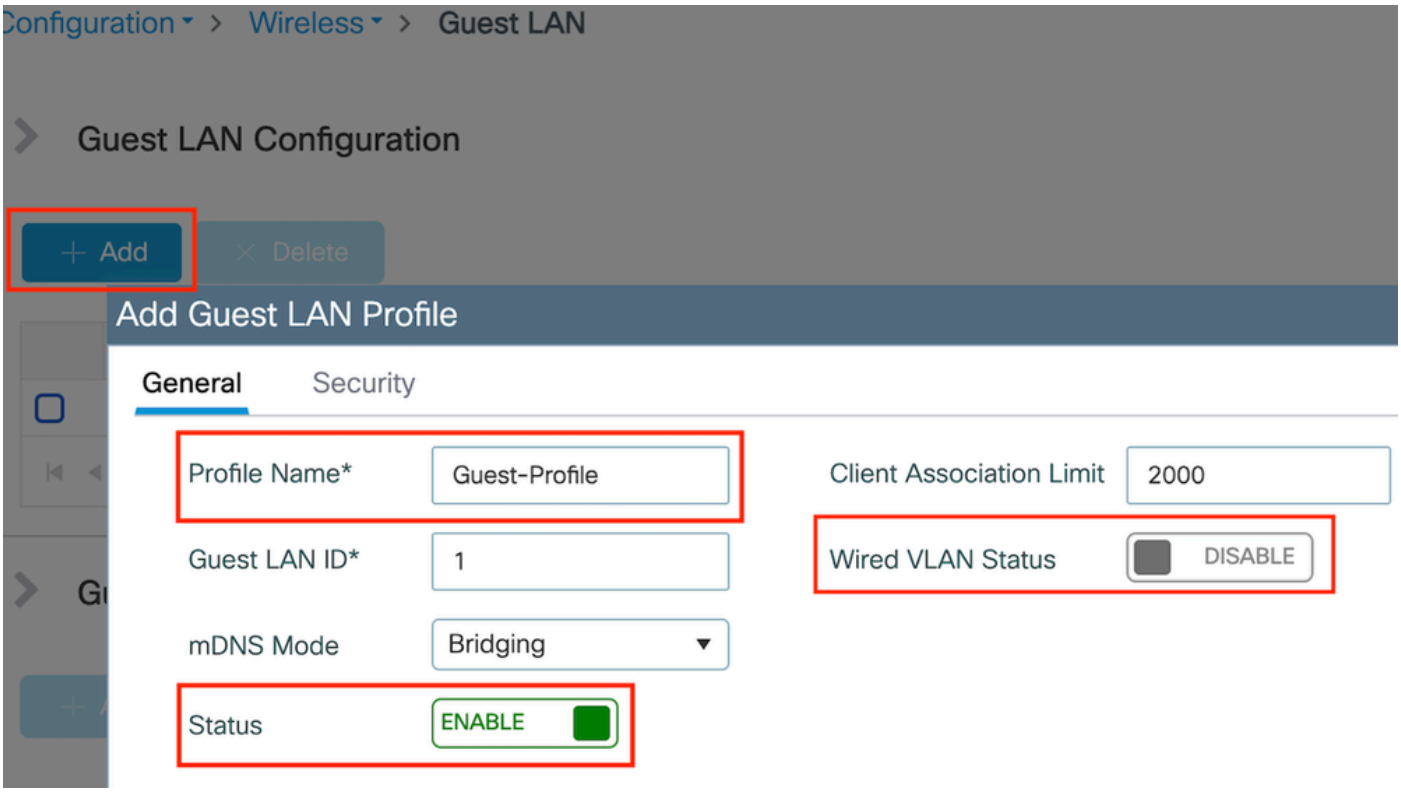
CLI配置

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

設定訪客LAN設定檔

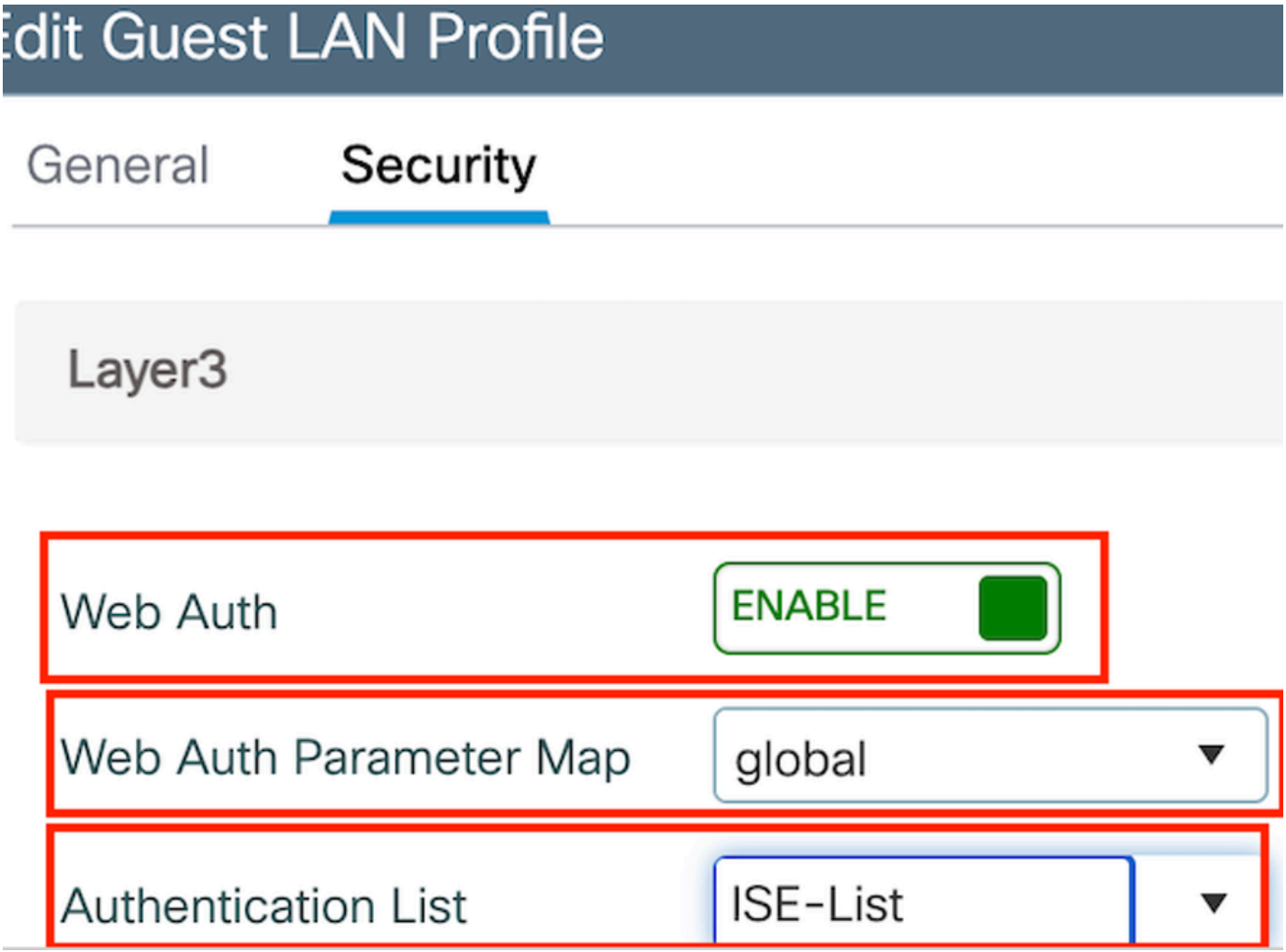
第1步：導航到配置>無線>訪客LAN，然後選擇增加建立和配置訪客LAN配置檔案。確定設定檔名

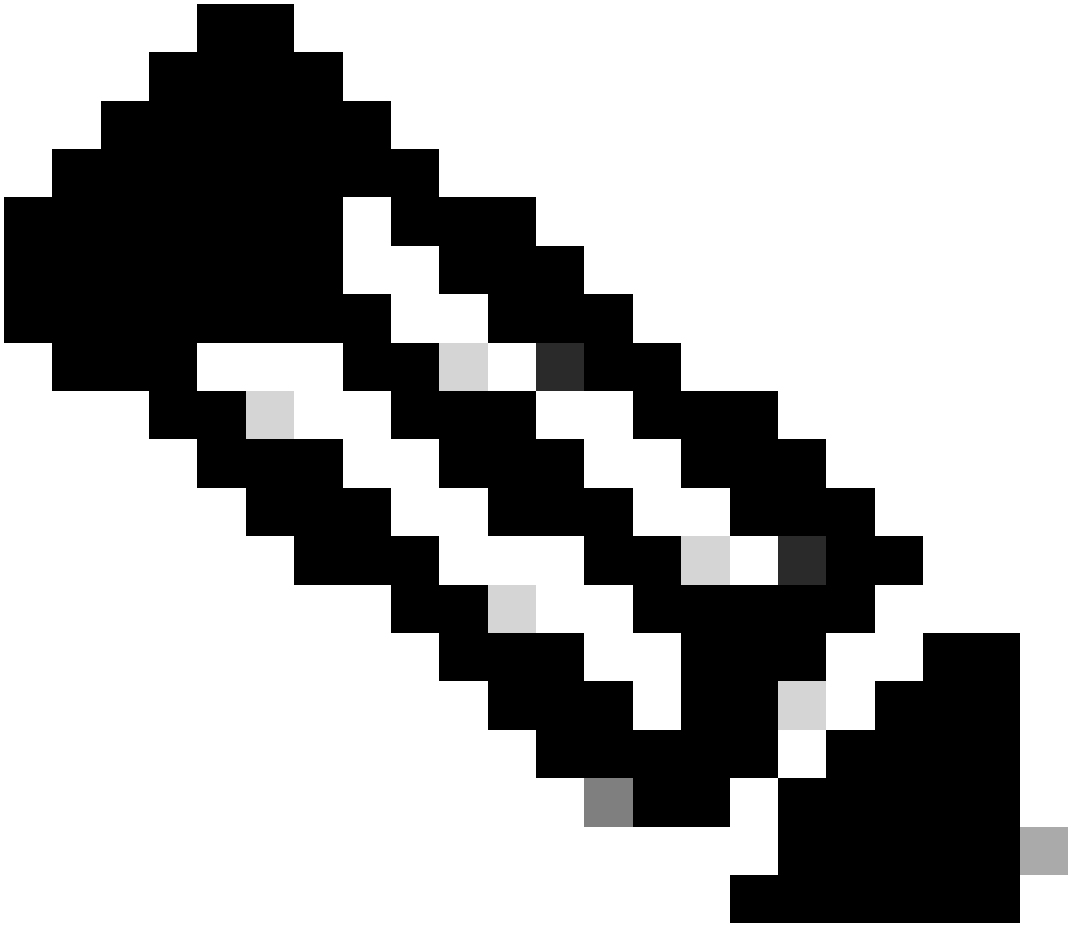
稱與外部控制器的名稱相符。請注意，必須在錨點控制器上停用有線VLAN。



訪客LAN配置檔案

第2步：在安全設定中，啟用Web Auth，然後配置Web Auth引數對映和身份驗證清單。


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



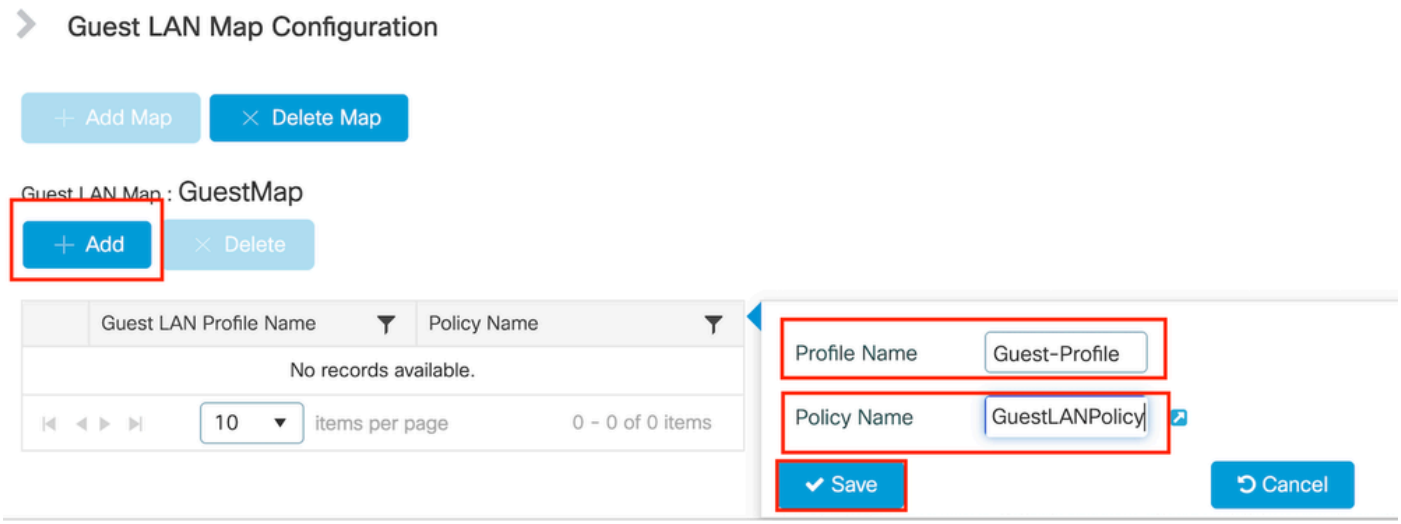
注意：除了有線VLAN狀態外，外部控制器和錨點控制器之間的訪客LAN配置檔案配置必須相同

CLI配置

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

訪客LAN對映

第1步：導航到配置>無線>訪客LAN。在Guest LAN MAP configuration部分，選擇Add並將策略配置檔案對映到訪客LAN配置檔案。



訪客LAN對映

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

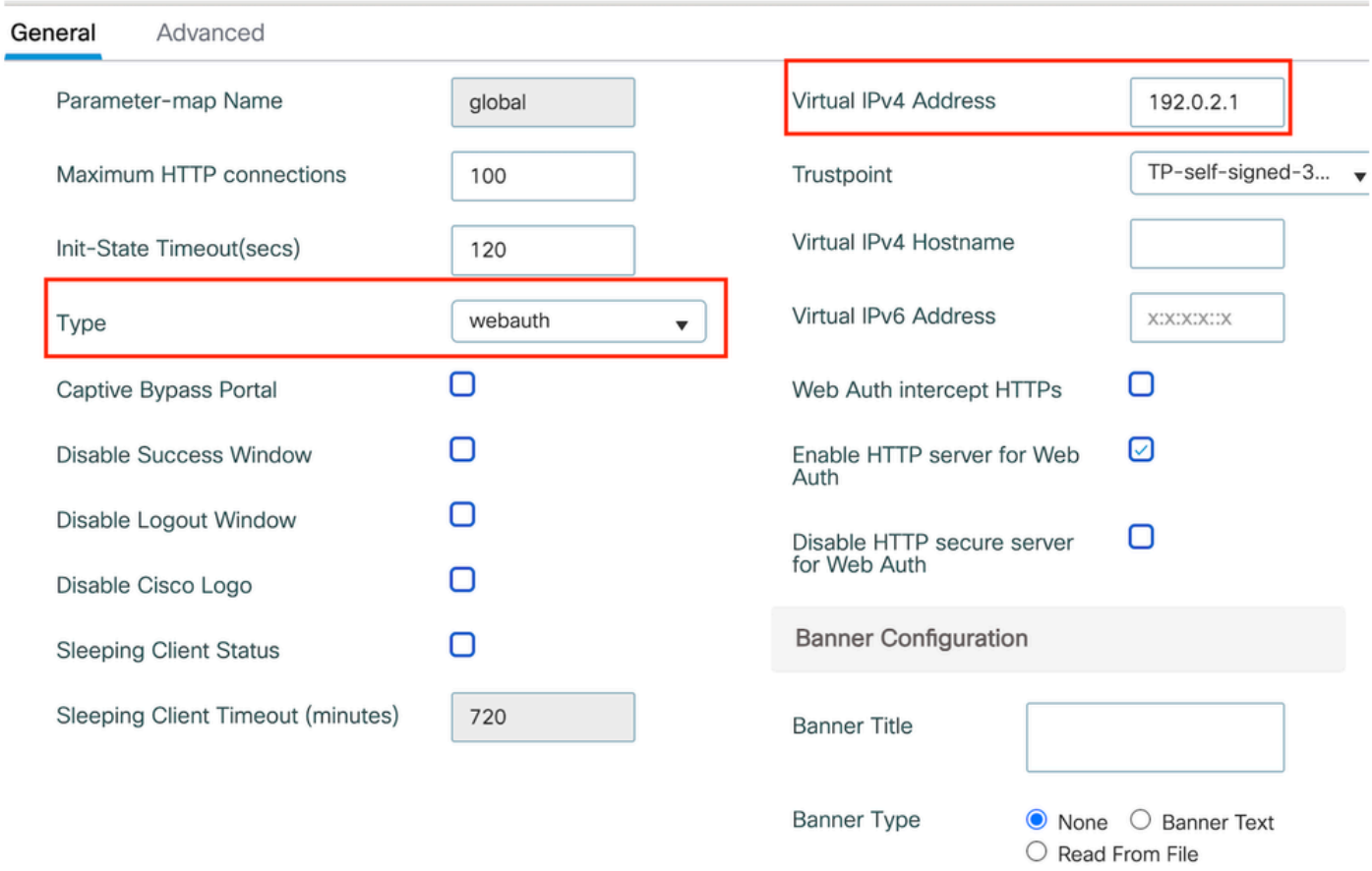
在Catalyst 9800上配置錨定到AireOS 5520控制器的有線訪客

網路拓撲

外部9800 WLC上的配置

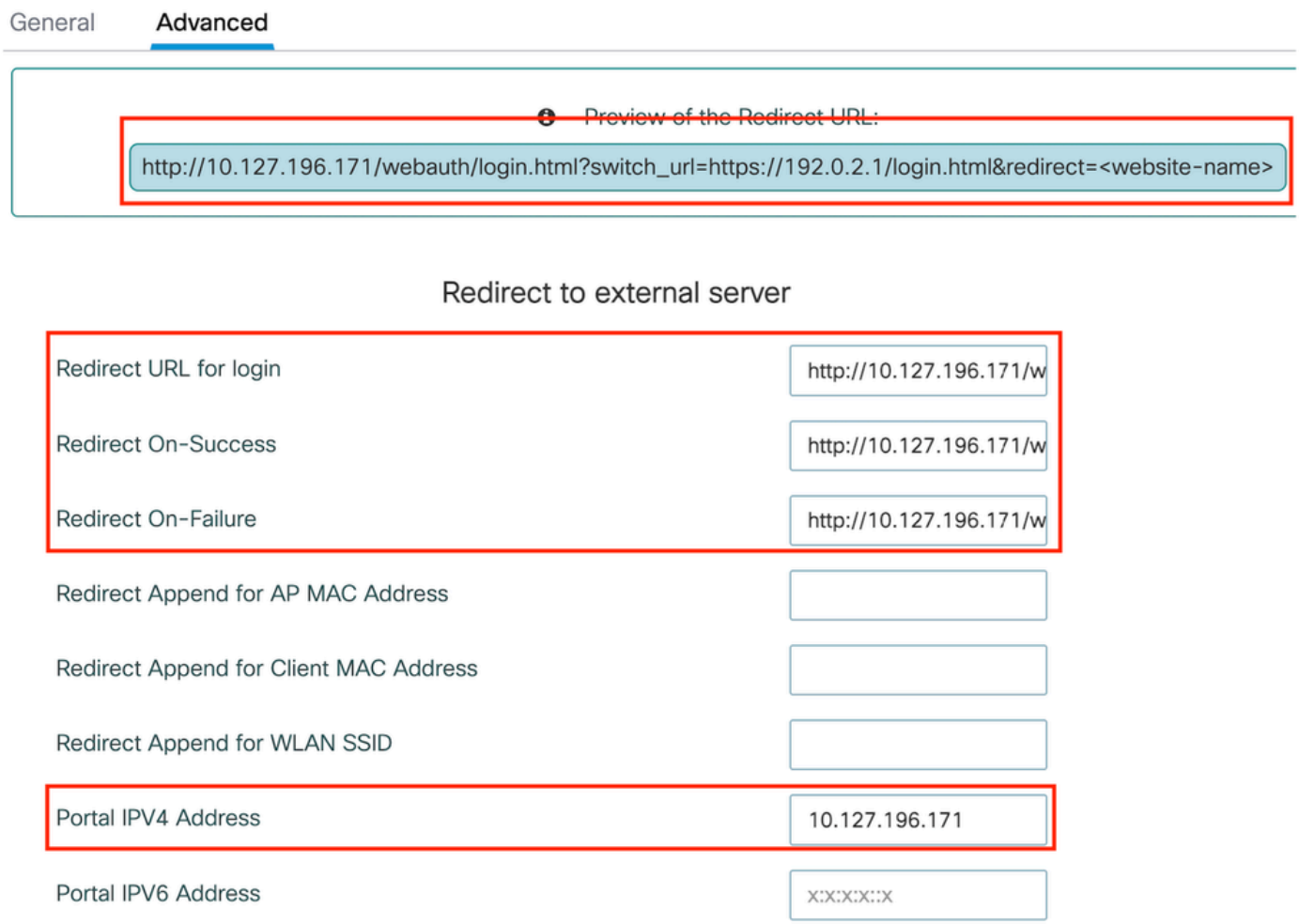
配置Web引數對映

第1步：導航到配置>安全> Web身份驗證，然後選擇全局。驗證控制器的虛擬IP地址和信任點是否已正確對映到配置檔案上，並且型別設定為webauth。



Web引數對映

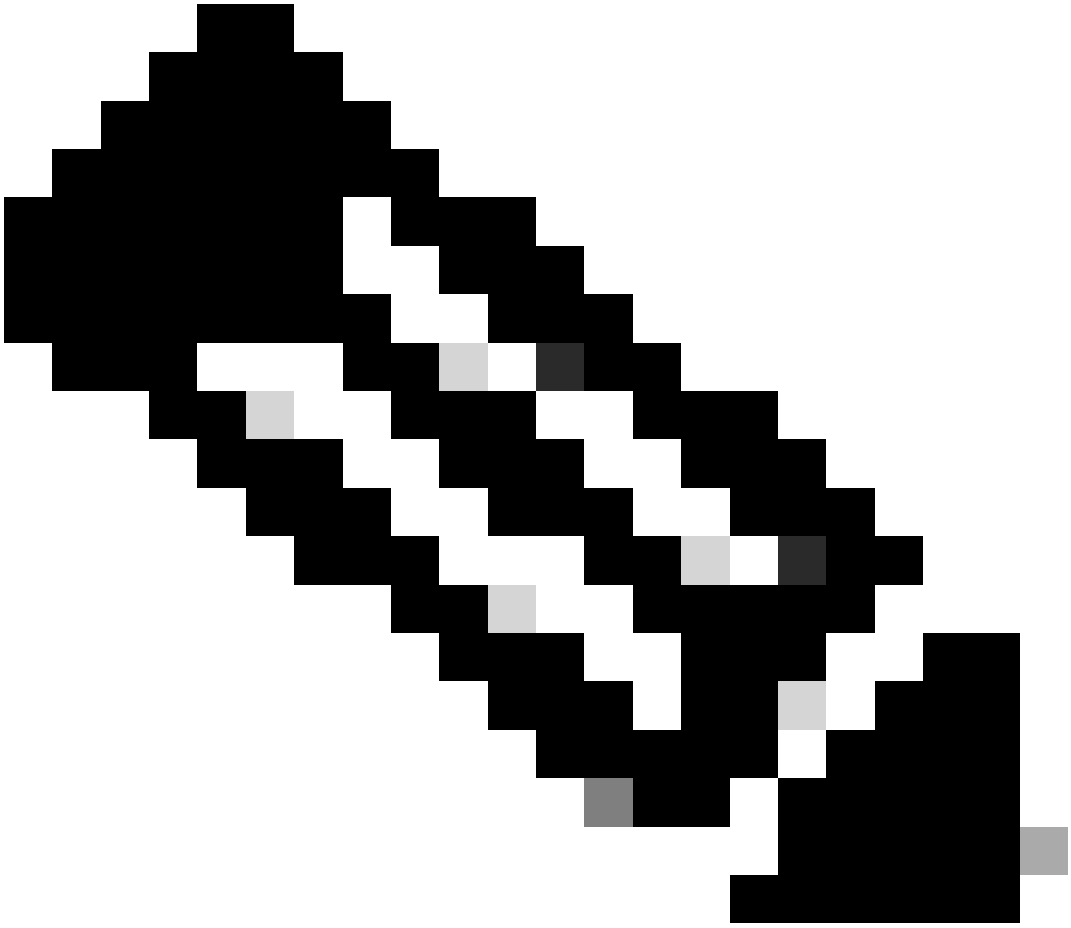
第2步：在高級頁籤下，指定客戶端必須重定向到的外部網頁URL。配置Redirect URL for Login和Redirect On-Failure。Redirect On-Success設定是可選配置。



進階標籤

CLI配置

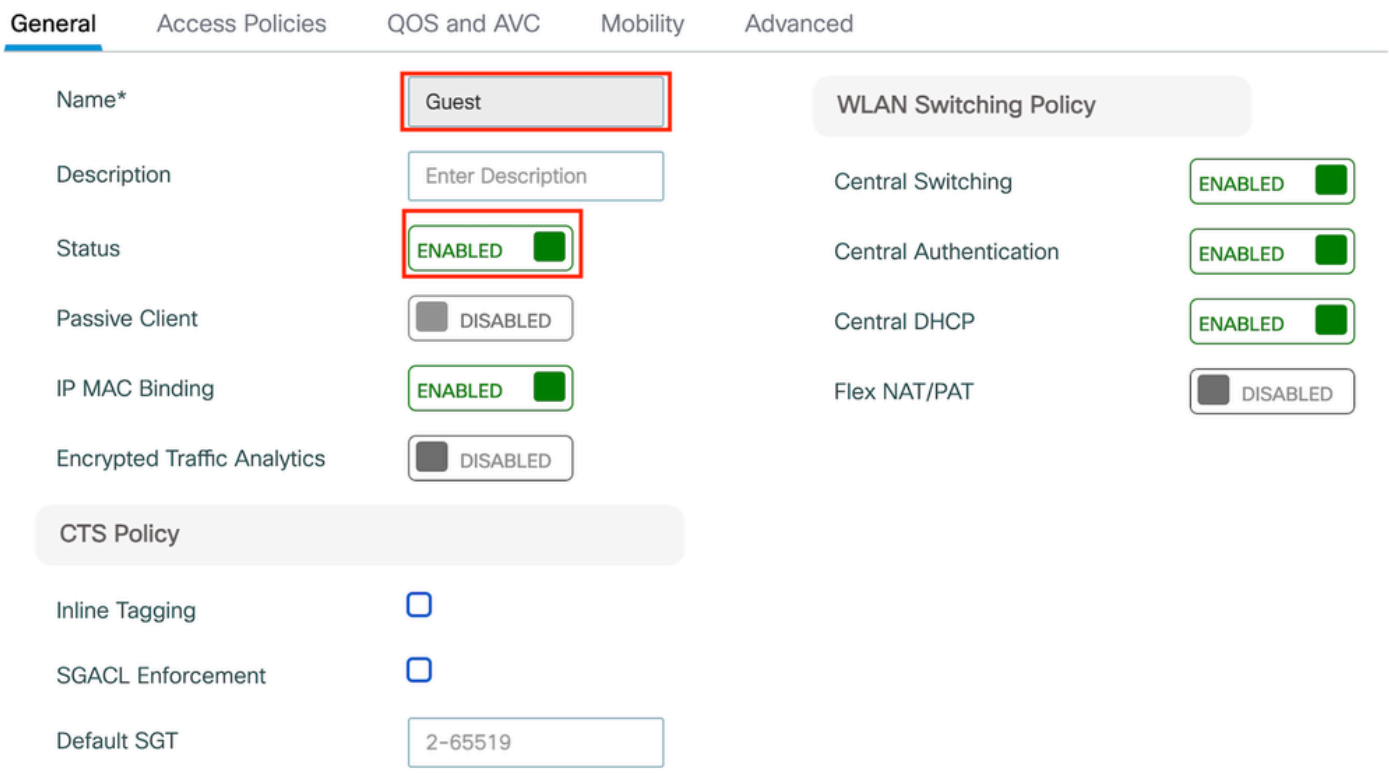
```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171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



注意：有關AAA配置，請參閱外部9800 WLC的「」部分中提供的配置詳細資訊。

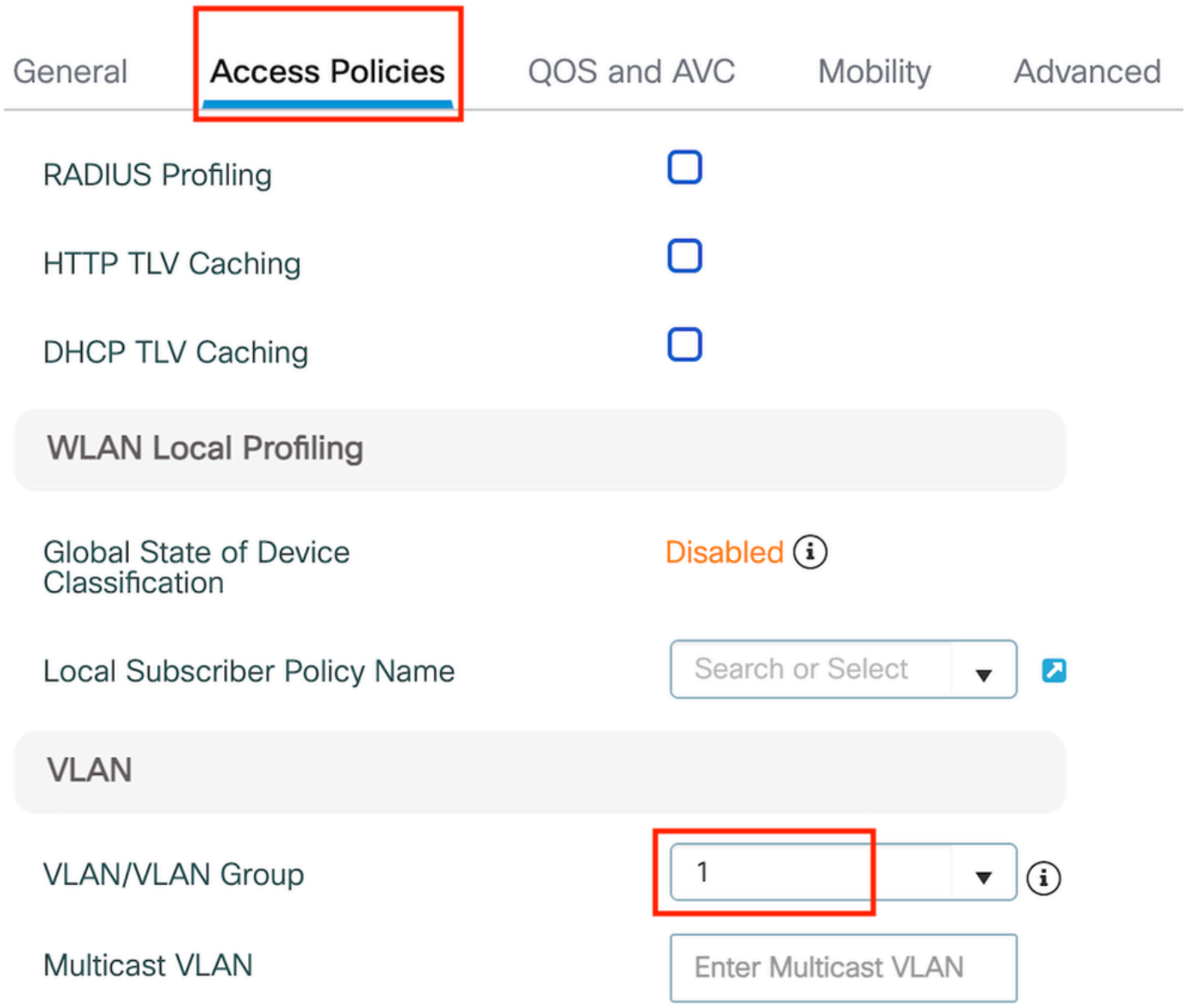
配置策略配置檔案

第1步：導航到配置>標籤和配置檔案>策略。選擇Add，並在General頁籤中為配置檔案提供一個名稱並啟用狀態切換。



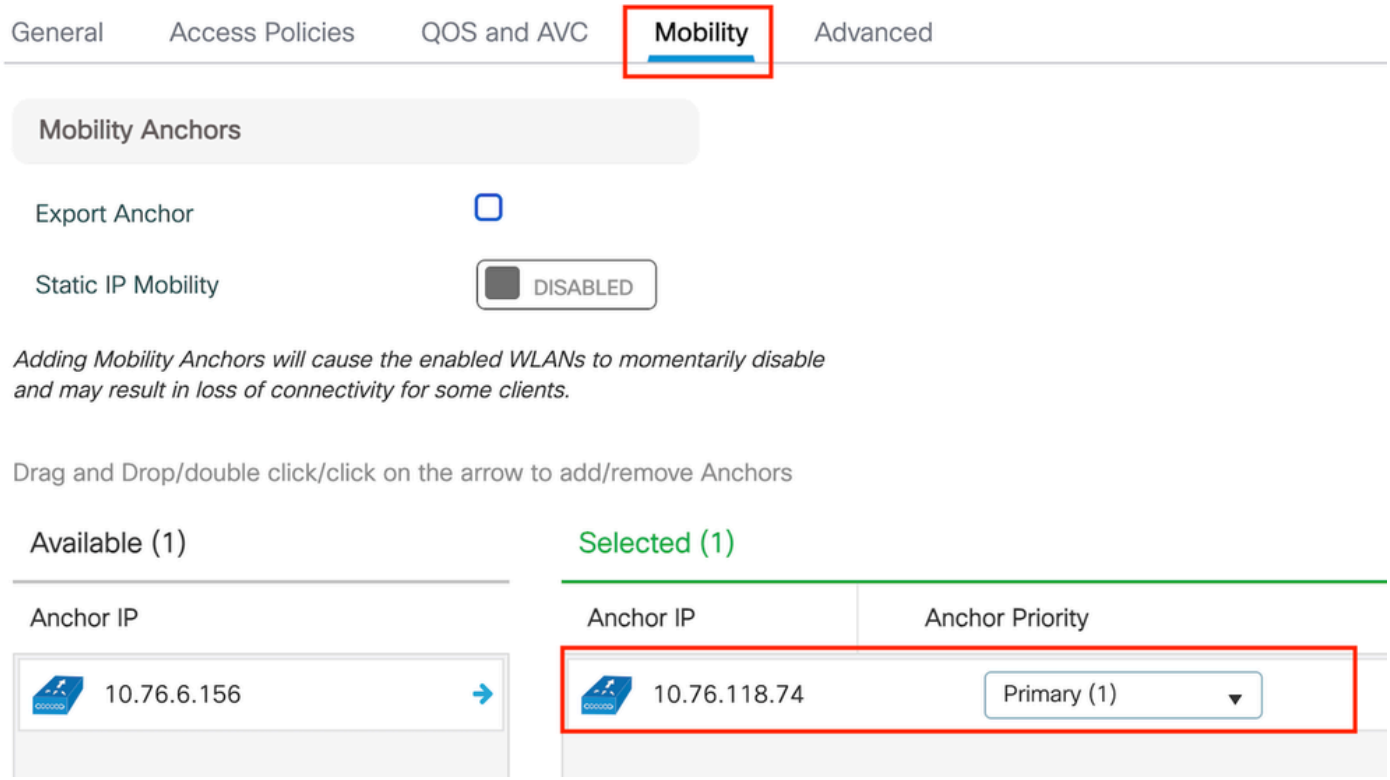
策略配置檔案

第2步：在訪問策略頁籤中，分配隨機VLAN。

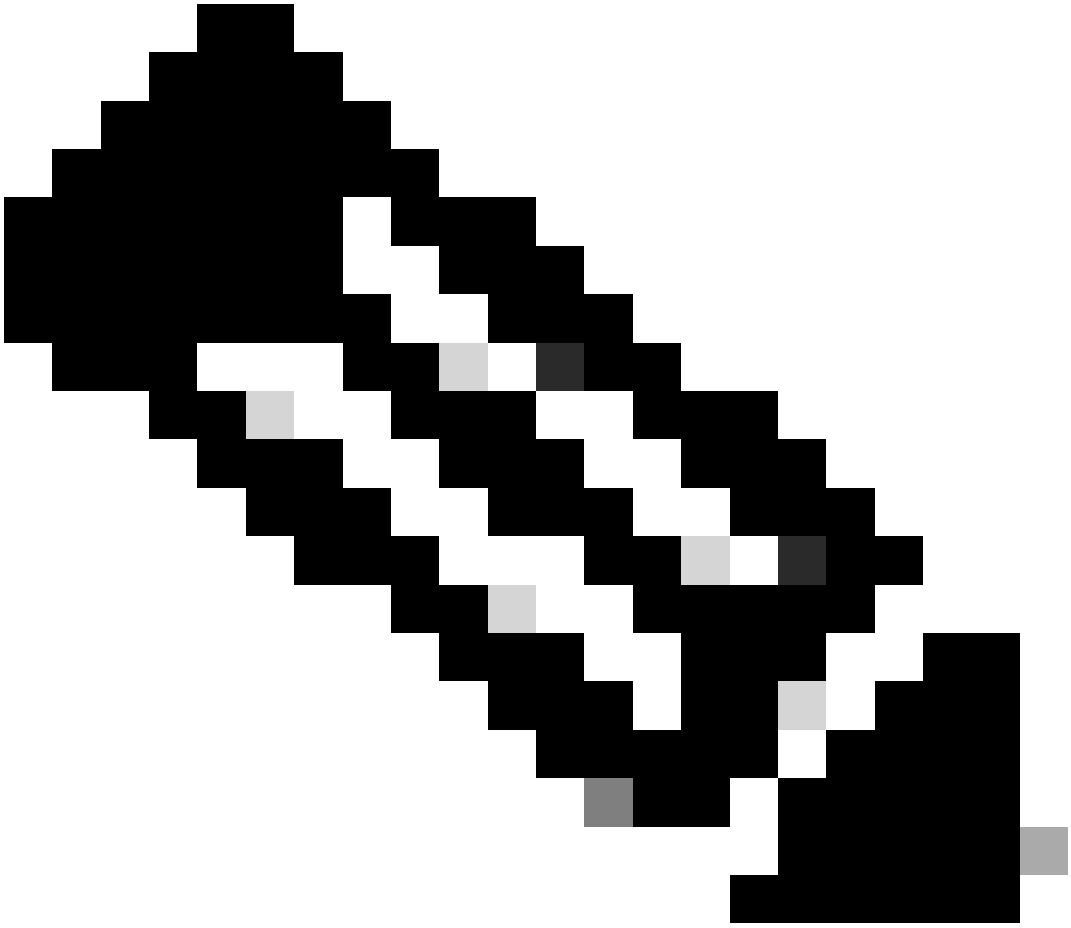


訪問策略

第3步：在移動性頁籤中，切換錨點控制器並將其優先順序設定為主(1)


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頁籤



注意： 9800外部WLC的策略配置檔案必須與5520錨點WLC的訪客LAN配置檔案匹配，但vlan配置除外

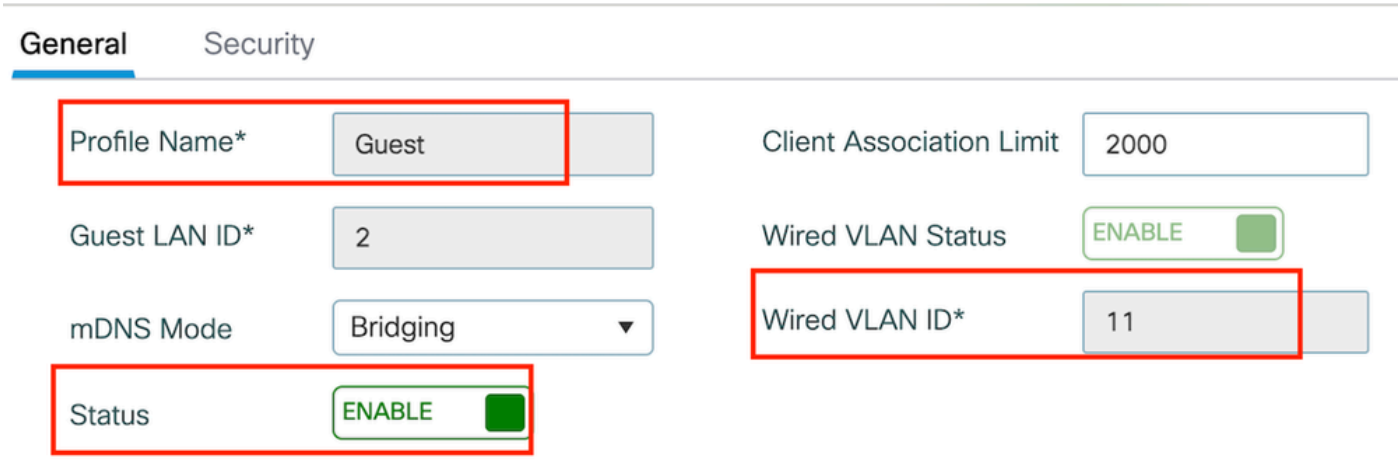
CLI配置

```
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
```

設定訪客LAN設定檔

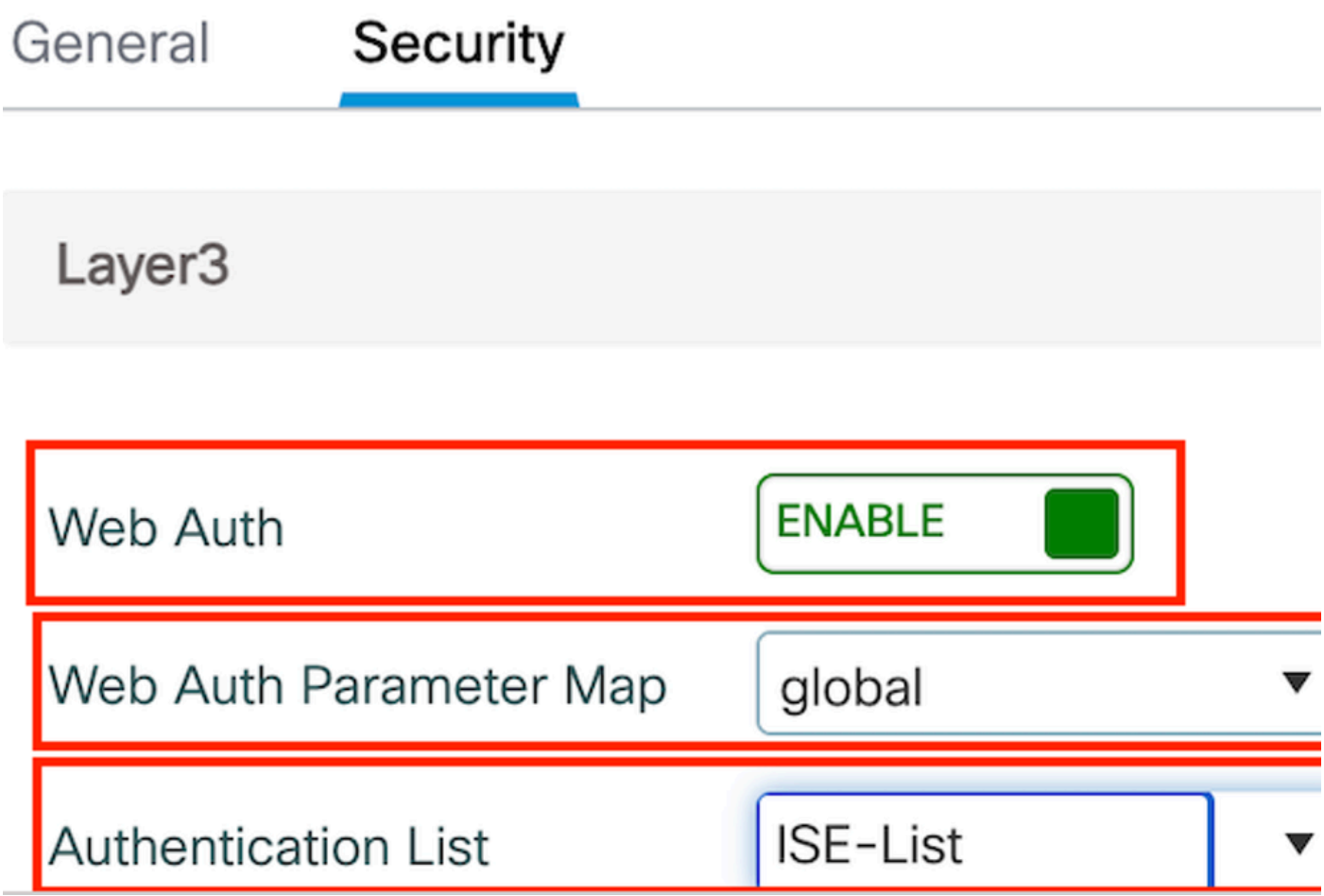
第1步：導航到配置>無線>訪客LAN，選擇增加。配置一個唯一的配置檔名稱並啟用Wired

VLAN，指定專用於有線訪客使用者的VLAN ID。最後，將配置檔案狀態切換為Enabled。

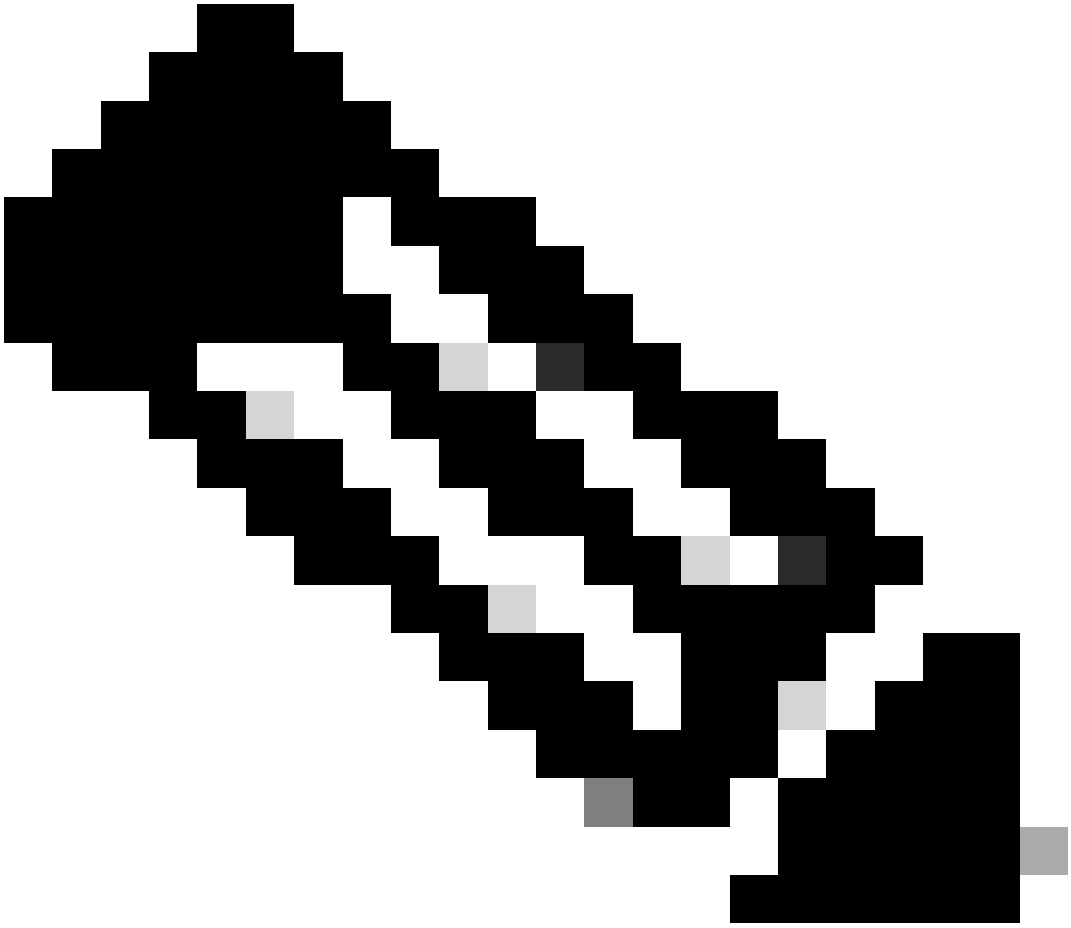


訪客LAN策略

第2步：在安全頁籤下，啟用Web身份驗證，對映Web身份驗證引數對映，然後從身份驗證下拉選單中選擇RADIUS伺服器。



「安全」頁籤



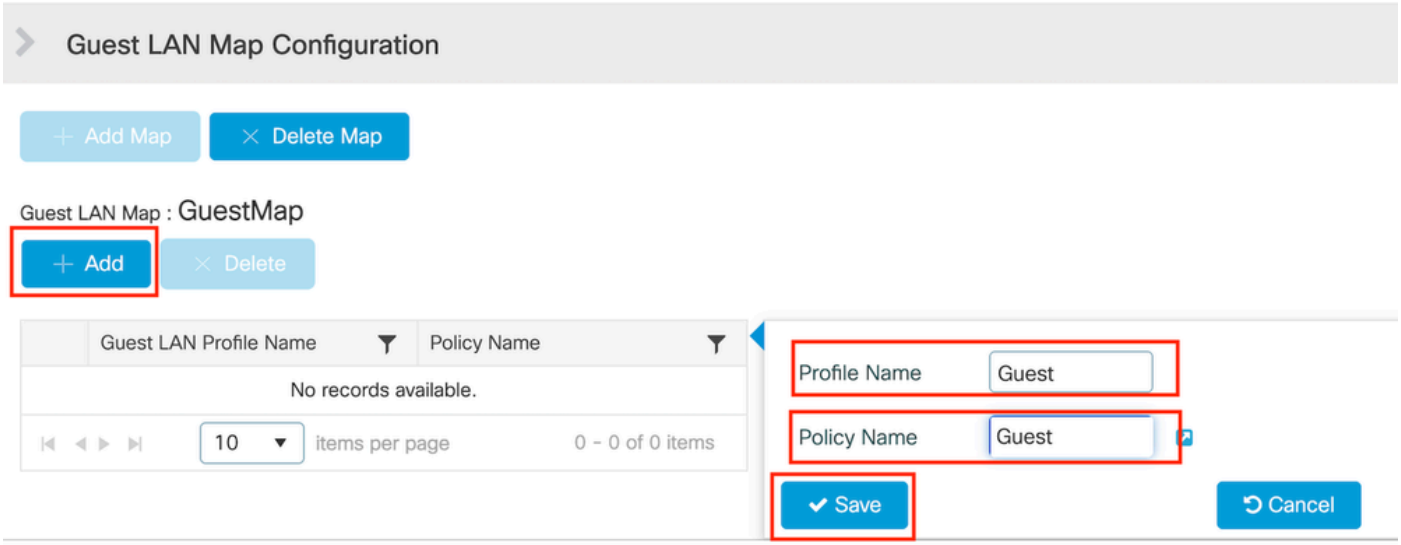
注意：9800外部和5520錨點控制器的訪客LAN配置檔名稱必須相同

CLI配置

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

訪客LAN對映

第1步：導航到配置>無線>訪客LAN。在訪客LAN對映配置部分，選擇增加，並將策略配置檔案對映到訪客LAN配置檔案。



訪客LAN對映

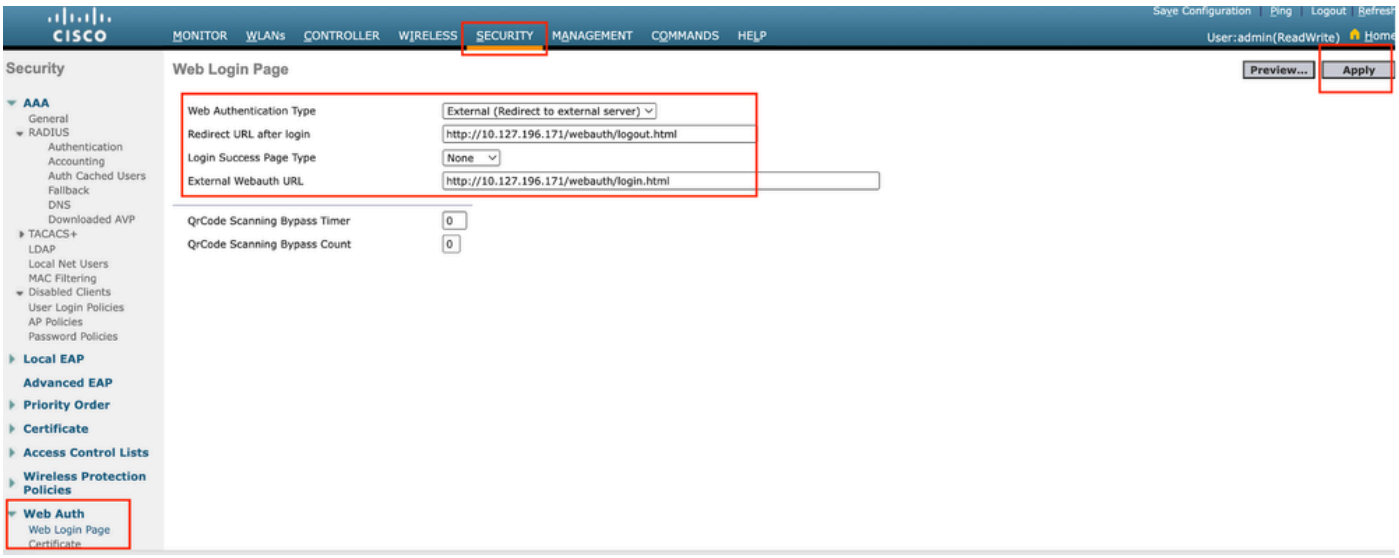
CLI配置

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

錨點5520 WLC上的組態

設定Web驗證

第1步：導航到安全> Web身份驗證> Web登入頁。將Web身份驗證型別設定為External（重定向到外部伺服器），並配置外部Web Auth URL。登入後重定向URL是可選的，並且如果客戶端在身份驗證成功之後需要重定向到專用頁，則可以配置此項。

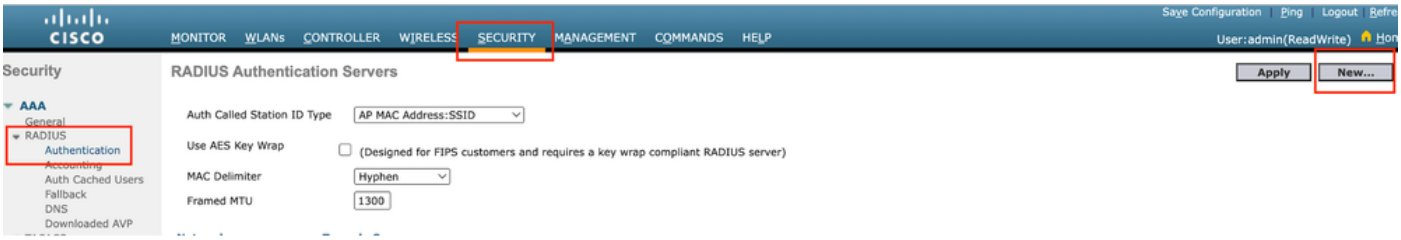


Web身份驗證設定

AAA設定：

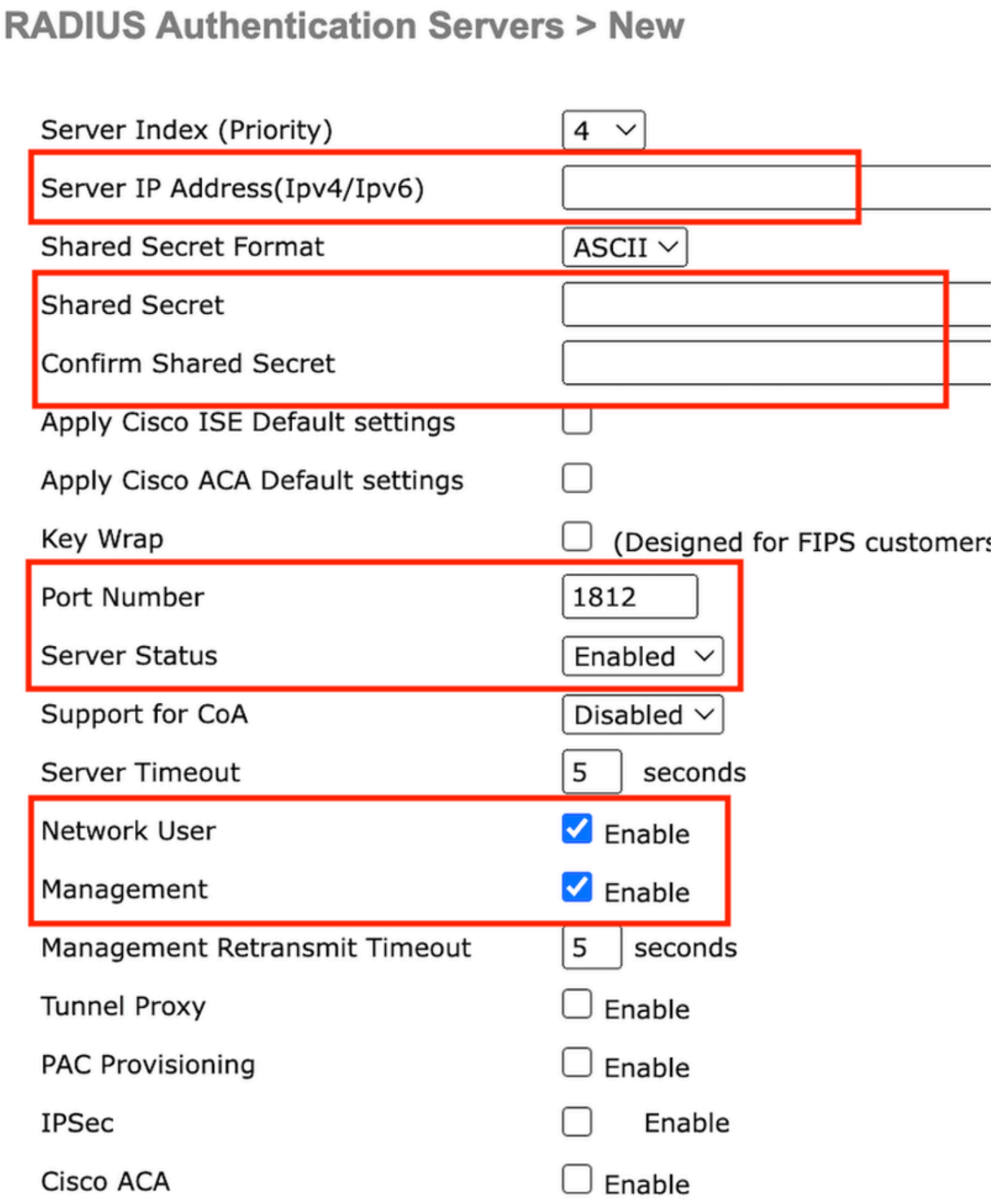
步驟1：配置RADIUS伺服器

導航到Security > Radius > Authentication > New。



Radius伺服器

第2步：在控制器上配置RADIUS伺服器IP和共用金鑰。將伺服器狀態切換為Enabled，並選中Network User覈取方塊。

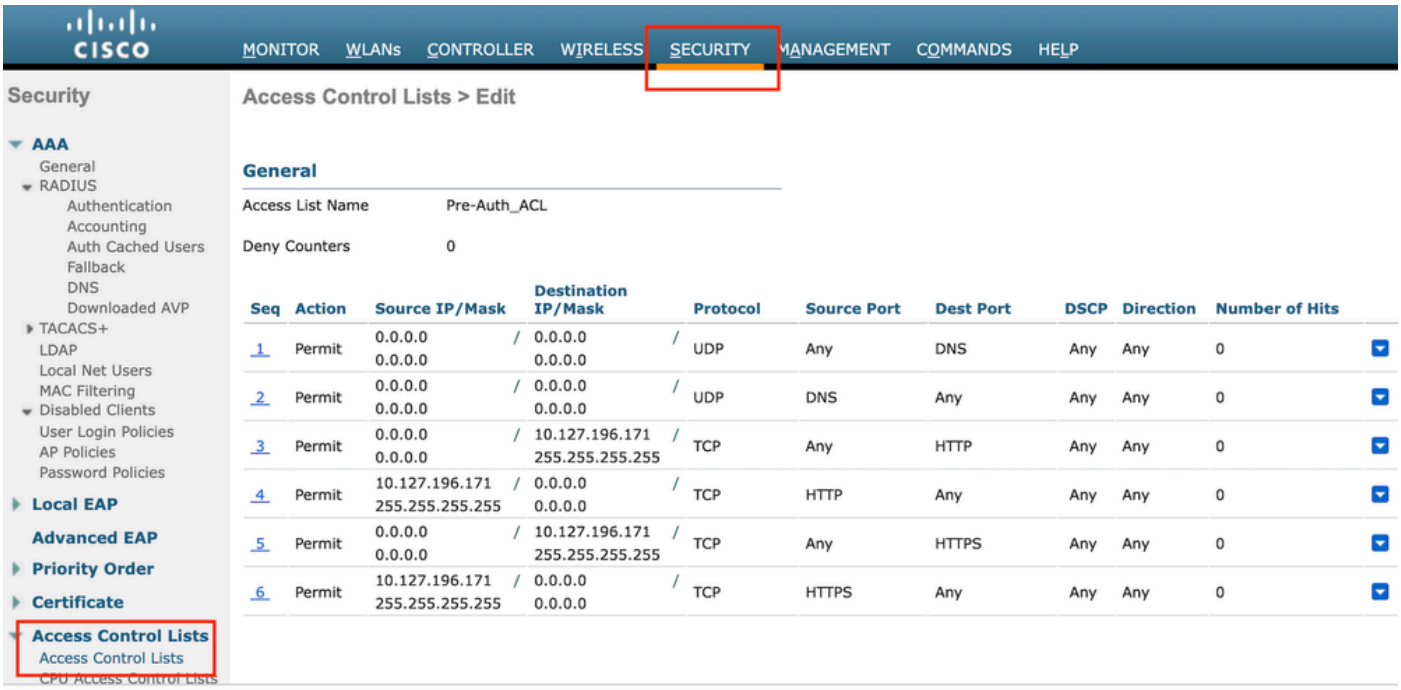


伺服器配置

配置訪問控制清單

第1步：導航到安全>訪問控制清單，選擇新建。建立允許流量到達DNS和外部Web伺服器的預先驗

證ACL。



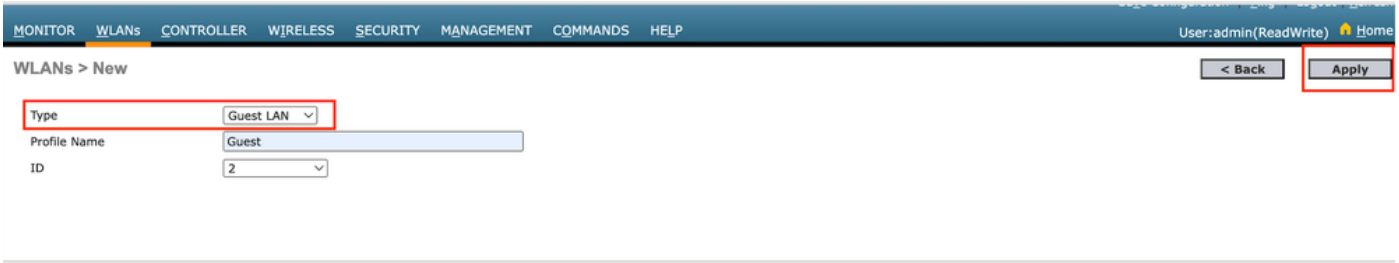
允許流量進入Web伺服器的訪問清單

設定訪客LAN設定檔

第1步：導航到WLAN >，選擇Create New。

選擇Type作為Guest LAN，並配置與9800外部控制器的策略配置檔案相同的名稱。

建立訪客LAN

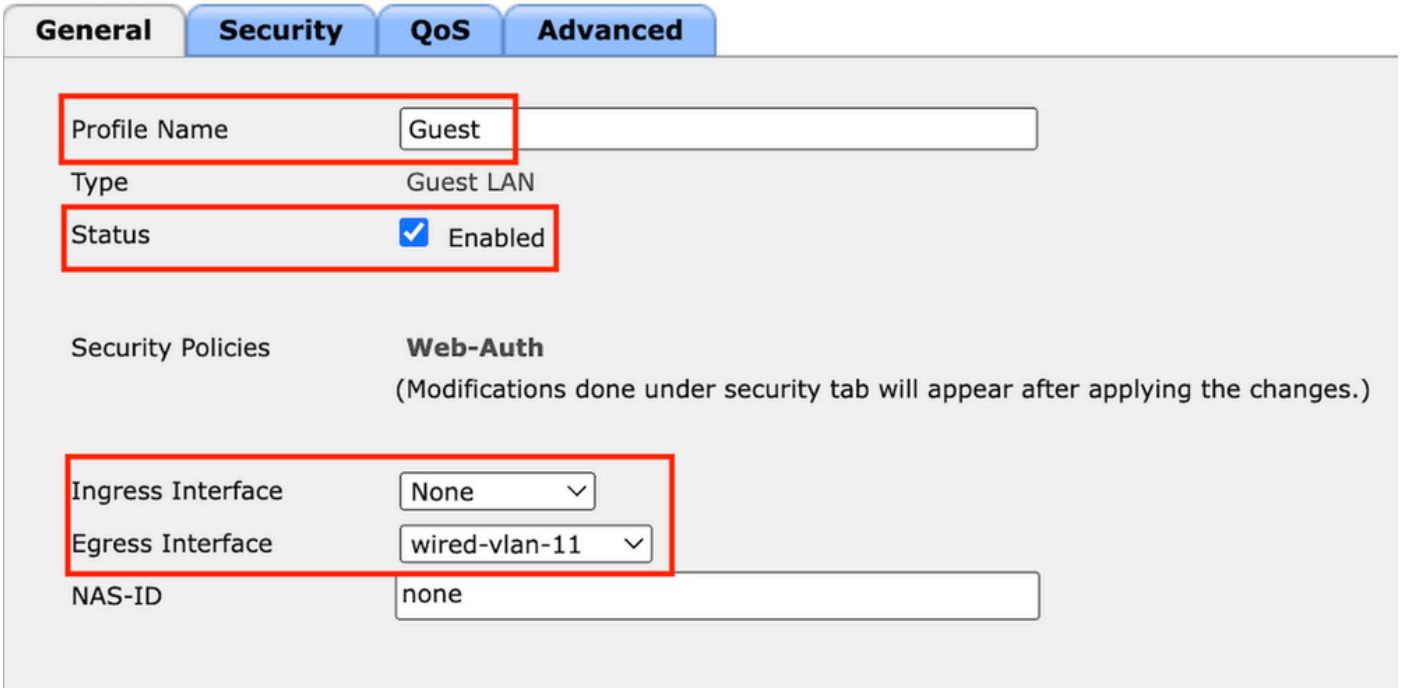


訪客LAN配置檔案

第2步：在訪客LAN配置檔案上對映入口和出口介面。

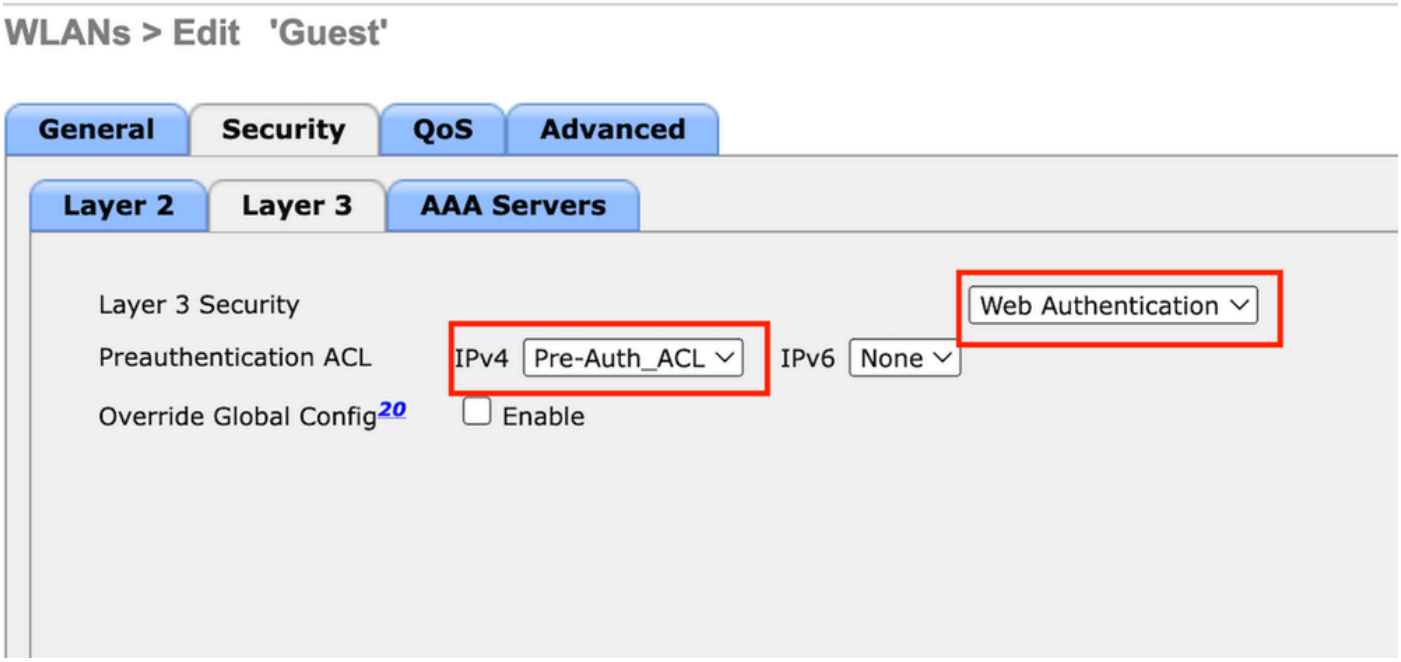
在此案例中，輸入介面是無，因為輸入介面是來自外部控制器的EoIP通道。

Egress介面是有線客戶端物理連線的VLAN。



訪客LAN配置檔案

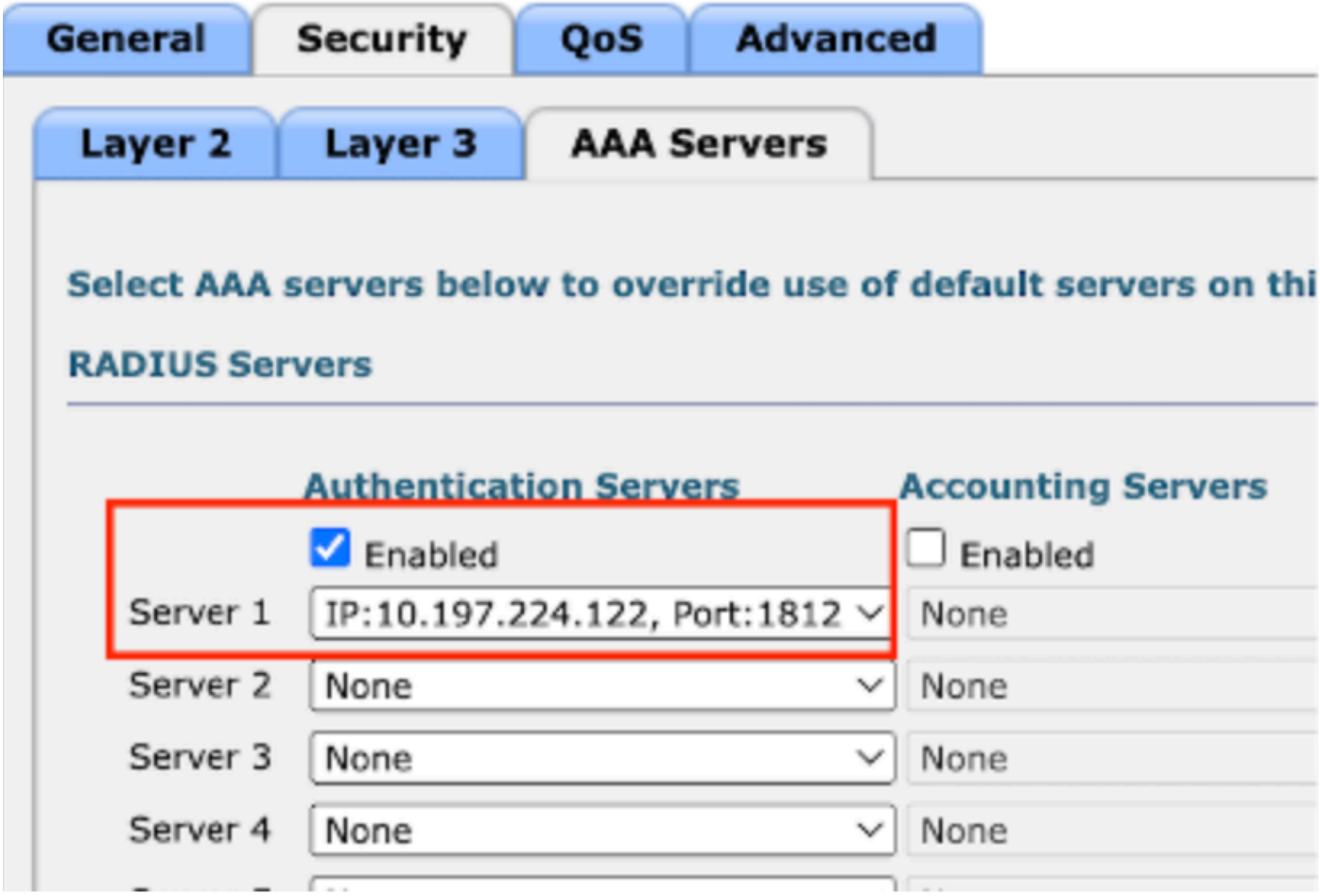
第3步：在Security頁籤下，選擇第3層安全作為Web Authentication，並對映預身份驗證ACL。



訪客LAN安全頁籤

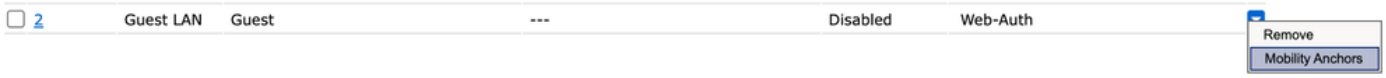
第4步：導航到安全> AAA伺服器。

選取下拉式清單，將RADIUS伺服器對應到訪客LAN設定檔。



將RADIUS伺服器對映到訪客LAN配置檔案

第5步：導航到WLAN。將滑鼠懸停在訪客LAN配置檔案的下拉圖示上，然後選擇移動錨點。



第6步：選擇Mobility Anchor Create為此訪客LAN配置檔案將控制器配置為導出錨點。

移動錨點建立

在AireOS 5520上配置錨定到Catalyst 9800的有線訪客

網路拓撲

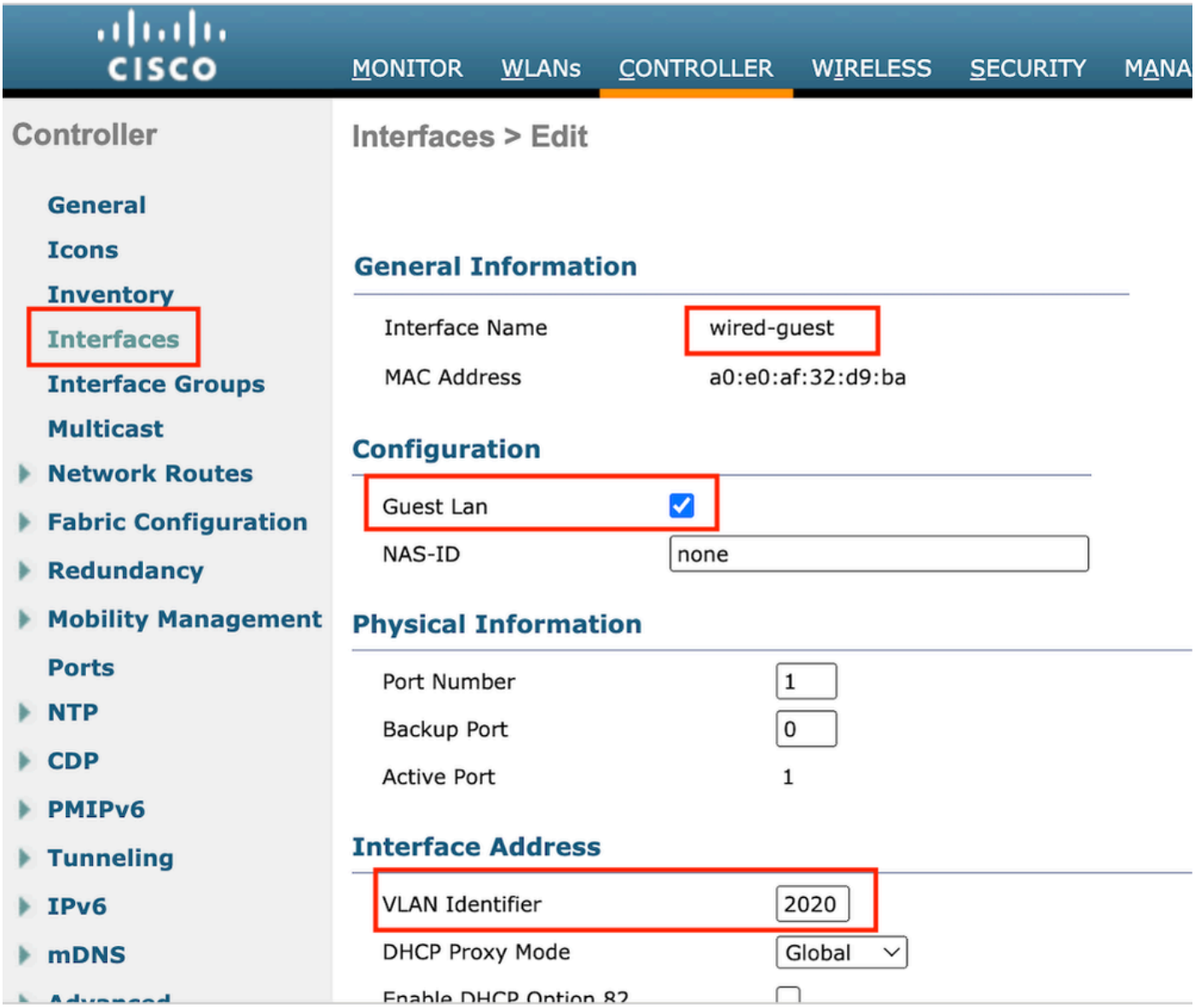
外部5520 WLC上的設定

控制器介面配置

第1步：導航到Controller > Interfaces > New。配置介面名稱、VLAN ID並啟用訪客LAN。

有線訪客需要兩個動態介面。

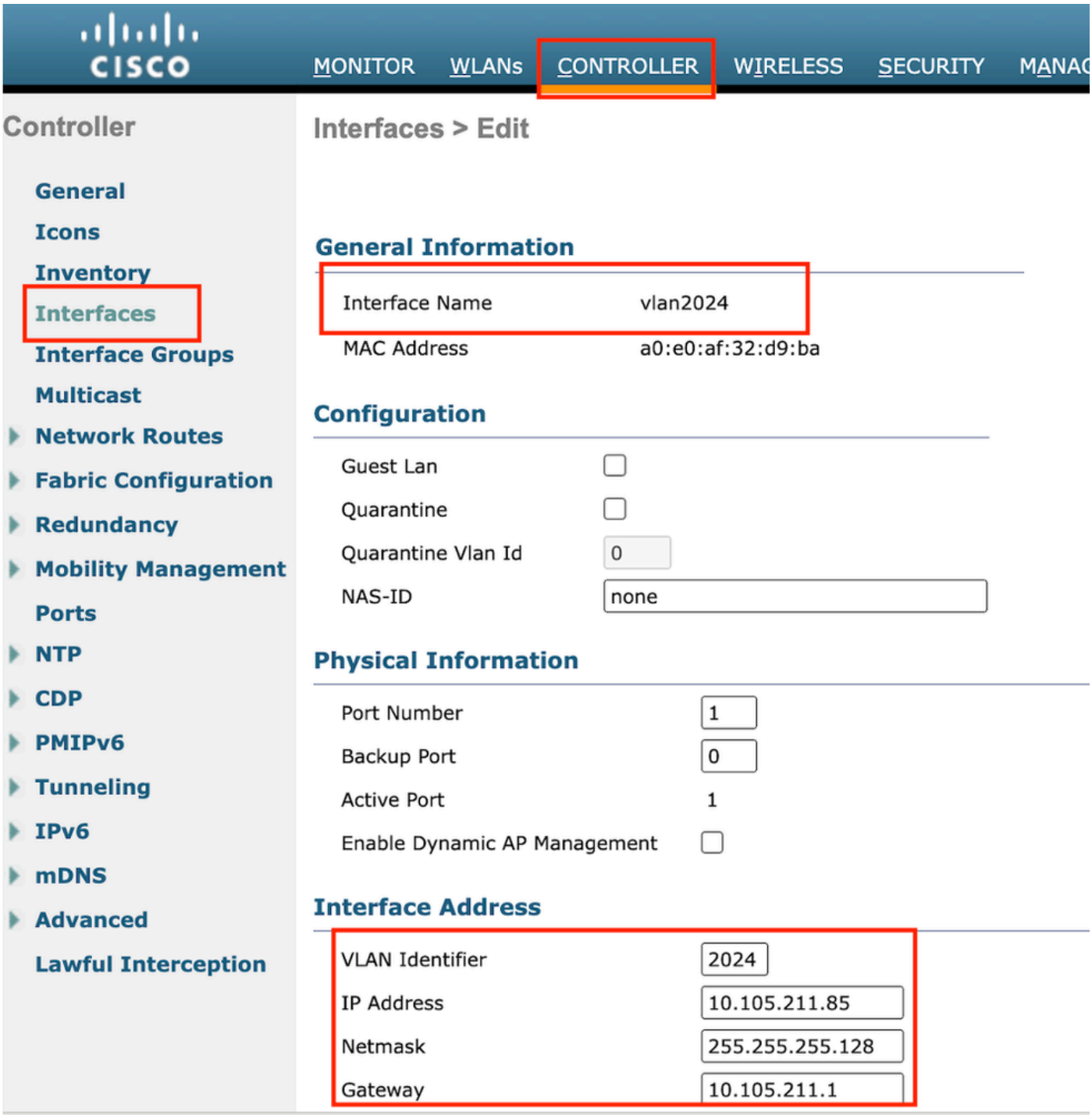
首先，建立一個第2層動態介面並將其指定為Guest LAN。此介面可作為訪客LAN的輸入介面，有線使用者端可在此處進行實體連線。



輸入介面

第2步：導航到Controller > Interfaces > New。配置介面名稱、VLAN ID。

第二個動態介面必須是控制器上的第3層介面，有線客戶端從此vlan子網接收IP地址。此介面可作為訪客LAN設定檔的輸出介面。



輸出介面

交換機埠配置

有線訪客使用者連線到接入層交換機，這些指定埠必須配置有在控制器上啟用訪客LAN的VLAN

接入層交換機埠配置

interface gigabitEthernet <x/x/x>

說明有線訪客訪問

switchport access vlan 2020

switchport mode access

end

外部控制器上行鏈路埠配置

interface TenGigabitEthernet<x/x/x>

說明到外部WLC的中繼埠

switchport mode trunk

switchport trunk native vlan 2081

switchport trunk allowed vlan 2081,2020

end

錨點控制器上行鏈路埠配置

interface TenGigabitEthernet<x/x/x>

描述連線到錨點WLC的中繼埠

switchport mode trunk

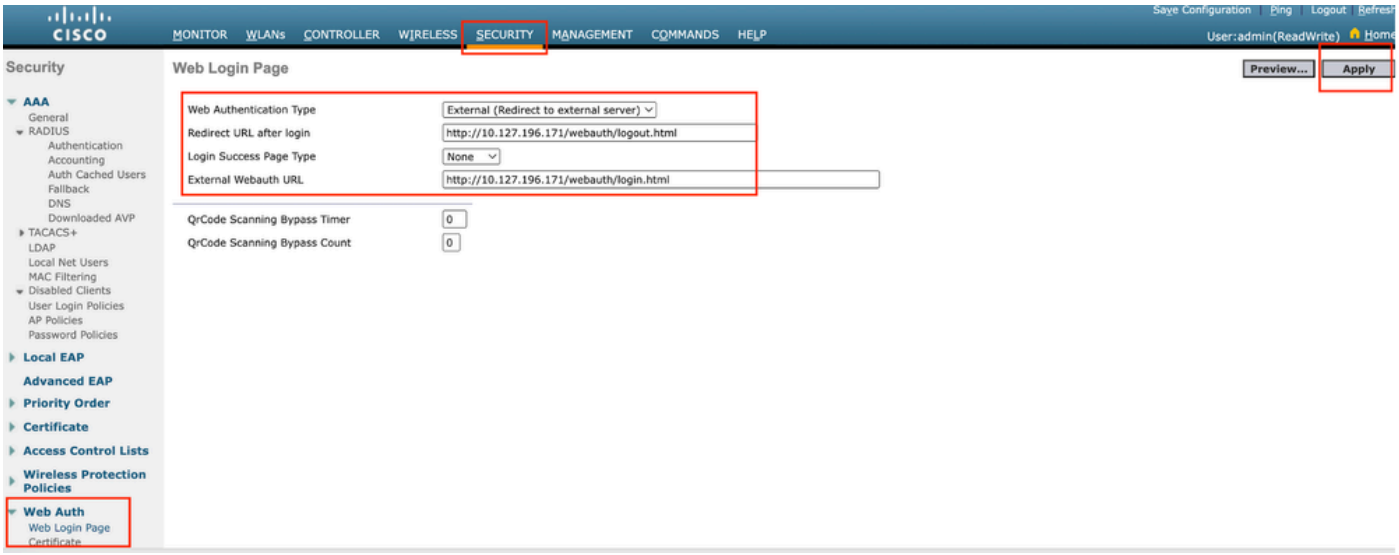
switchport trunk native vlan 2081

switchport trunk allowed vlan 2081,2024

end

設定Web驗證

第1步：導航到安全> Web身份驗證> Web登入頁。將Web身份驗證型別設定為External（重定向到外部伺服器），並配置外部Web Auth URL。登入後重定向URL是可選的，並且如果客戶端在身份驗證成功之後需要重定向到專用頁，則可以配置此項。

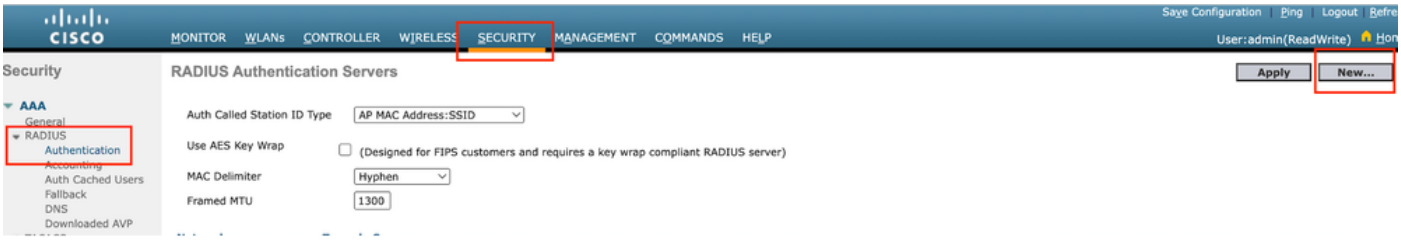


Web身份驗證設定

AAA設定：

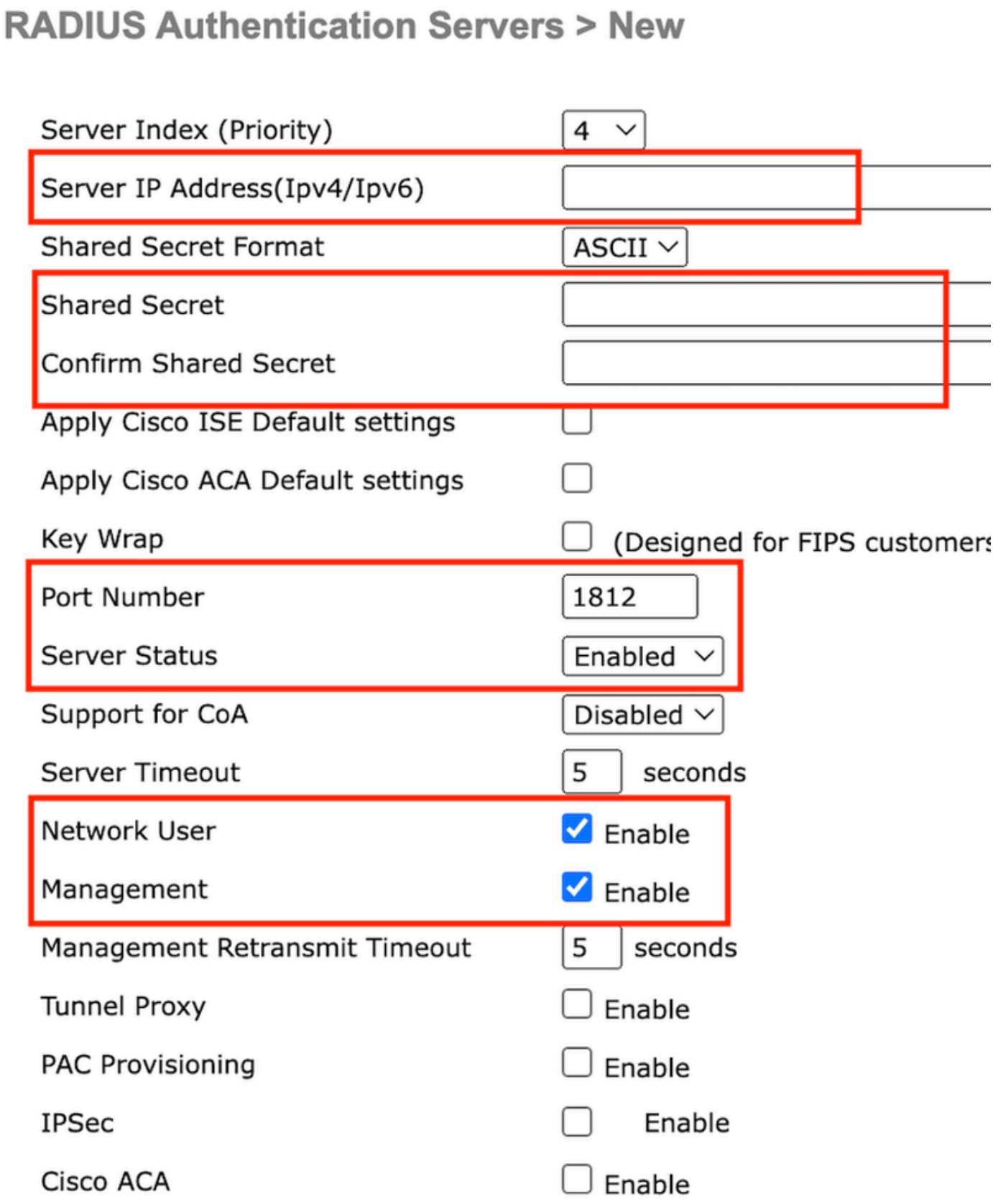
步驟1：配置RADIUS伺服器

導航到Security > Radius > Authentication > New。



Radius伺服器

第2步：在控制器上配置RADIUS伺服器IP和共用金鑰。將伺服器狀態切換為Enabled，並選中Network User覈取方塊。

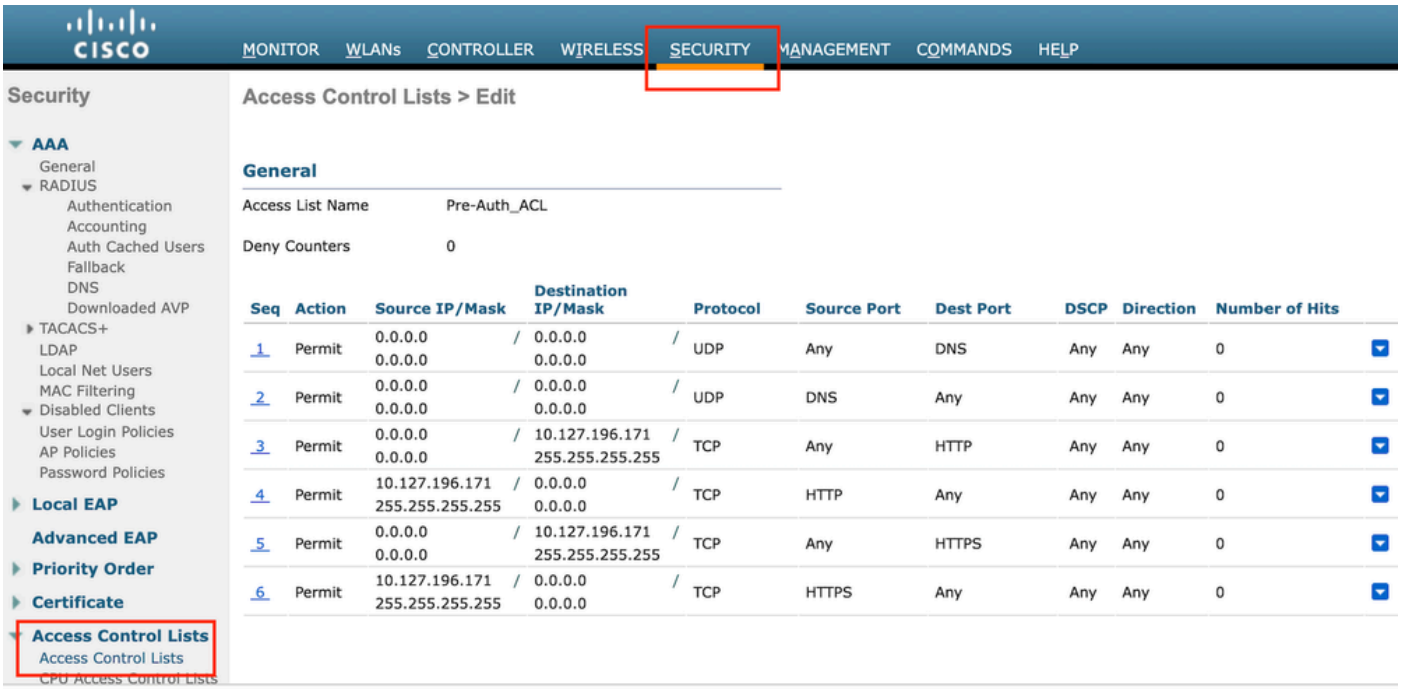


伺服器配置

配置訪問控制清單

第1步：導航到安全>訪問控制清單，選擇新建。建立允許流量到達DNS和外部Web伺服器的預先驗

證ACL。



允許流量進入Web伺服器的訪問清單

設定訪客LAN設定檔

第1步：導航到WLAN > Create New > Go。

訪客LAN配置檔案

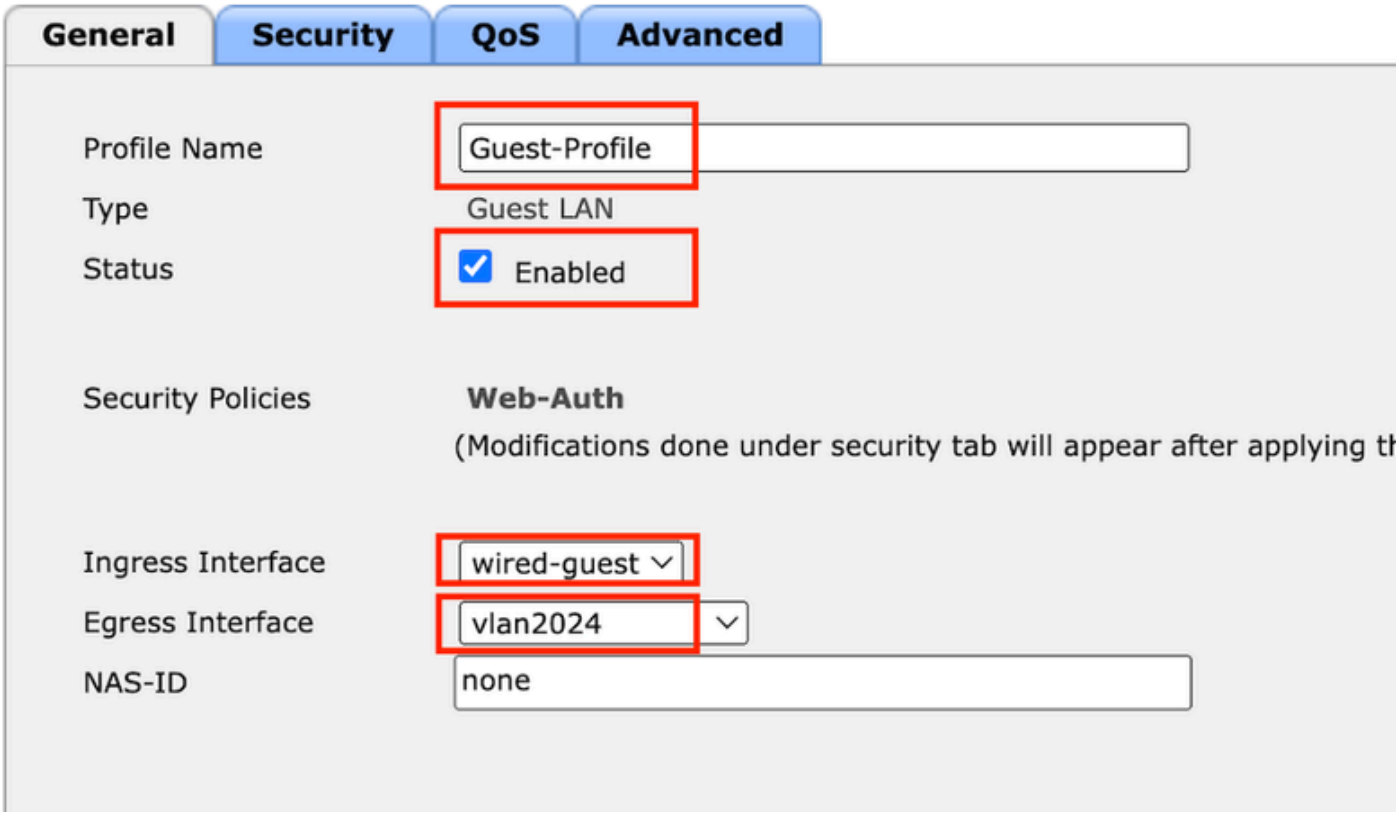
選擇Type as Guest LAN並配置配置檔名稱。必須在9800錨點控制器的原則設定檔和訪客LAN設定檔上設定相同的名稱。

訪客LAN配置檔案

第2步：在General頁籤下，在訪客LAN配置檔案上對映入口和出口介面。

輸入介面是有線使用者端實際連線的vlan。

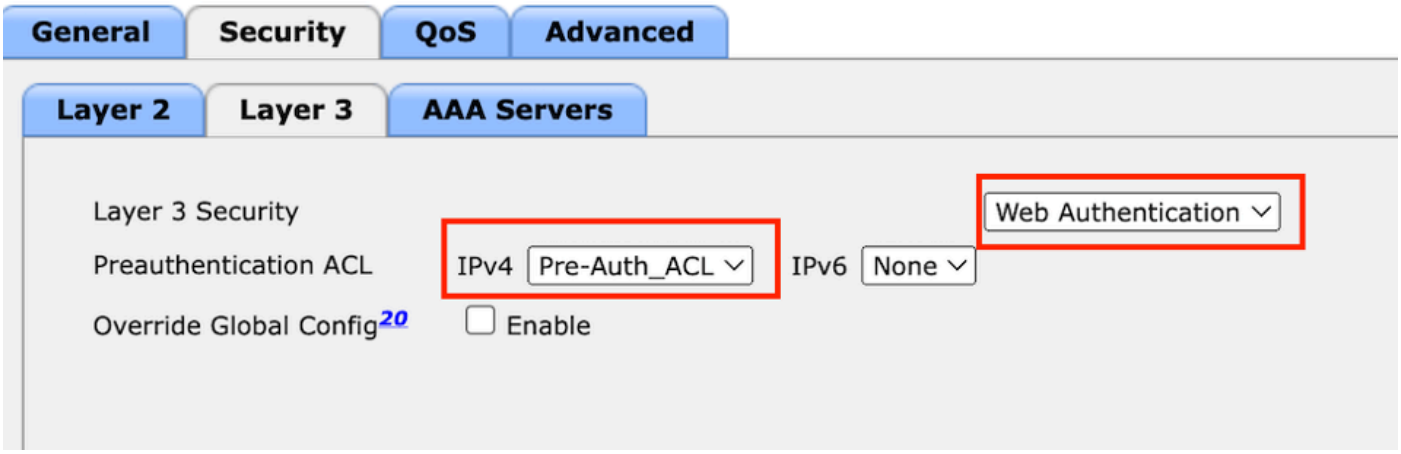
輸出介面是客戶端請求的IP地址的VLAN子網。



訪客LAN配置檔案

第3步：導航到安全>第3層。

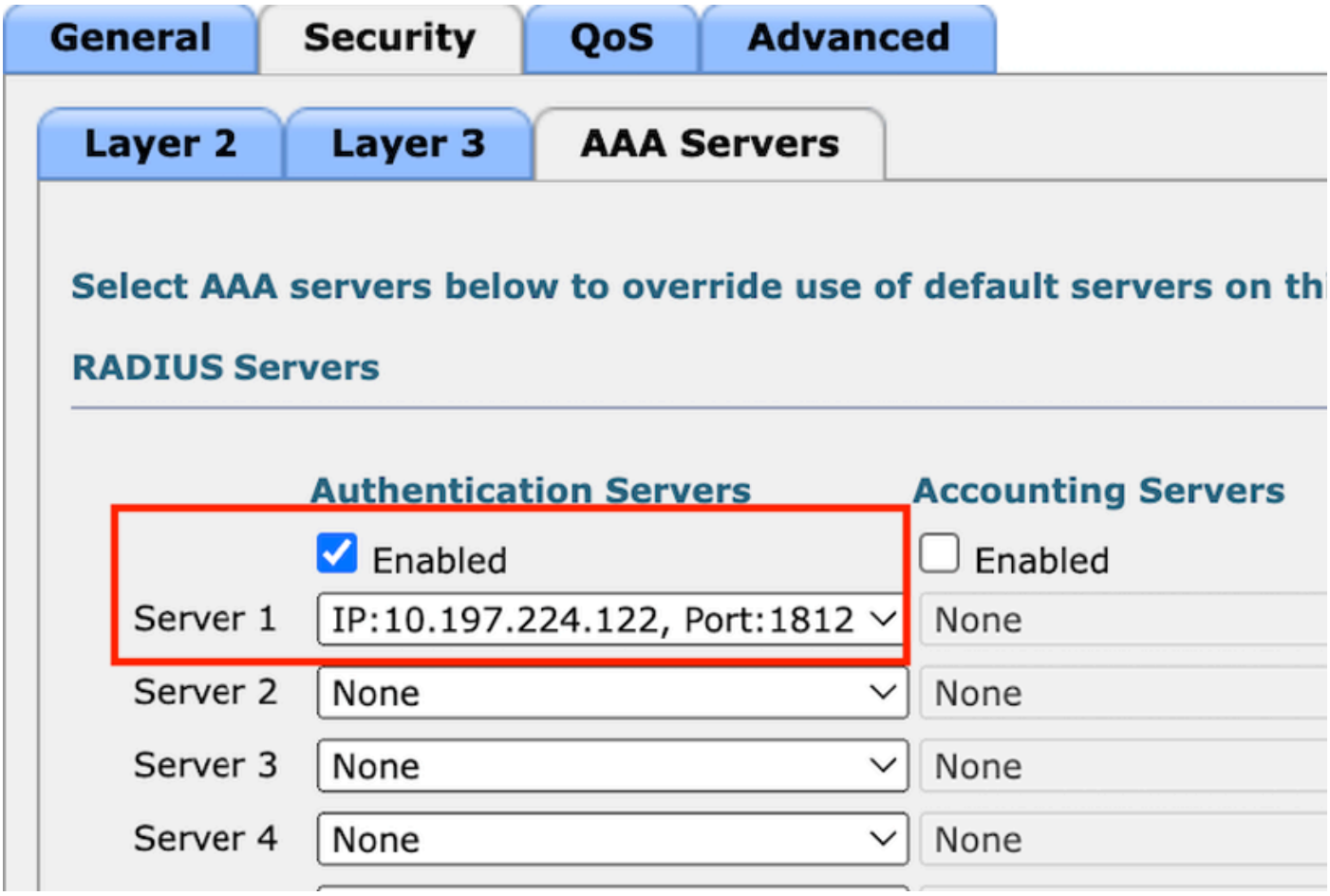
選擇Layer 3 Security作為Web Authentication，並對映預身份驗證ACL。



第3層安全頁籤

步驟4：

在AAA servers頁籤下，對映RADIUS伺服器和Enabled覈取方塊。



將RADIUS伺服器對應到訪客LAN設定檔

第5步：導航到WLAN頁面，將滑鼠懸停在訪客LAN配置檔案的下拉圖示上，然後選擇移動錨點。

行動錨點

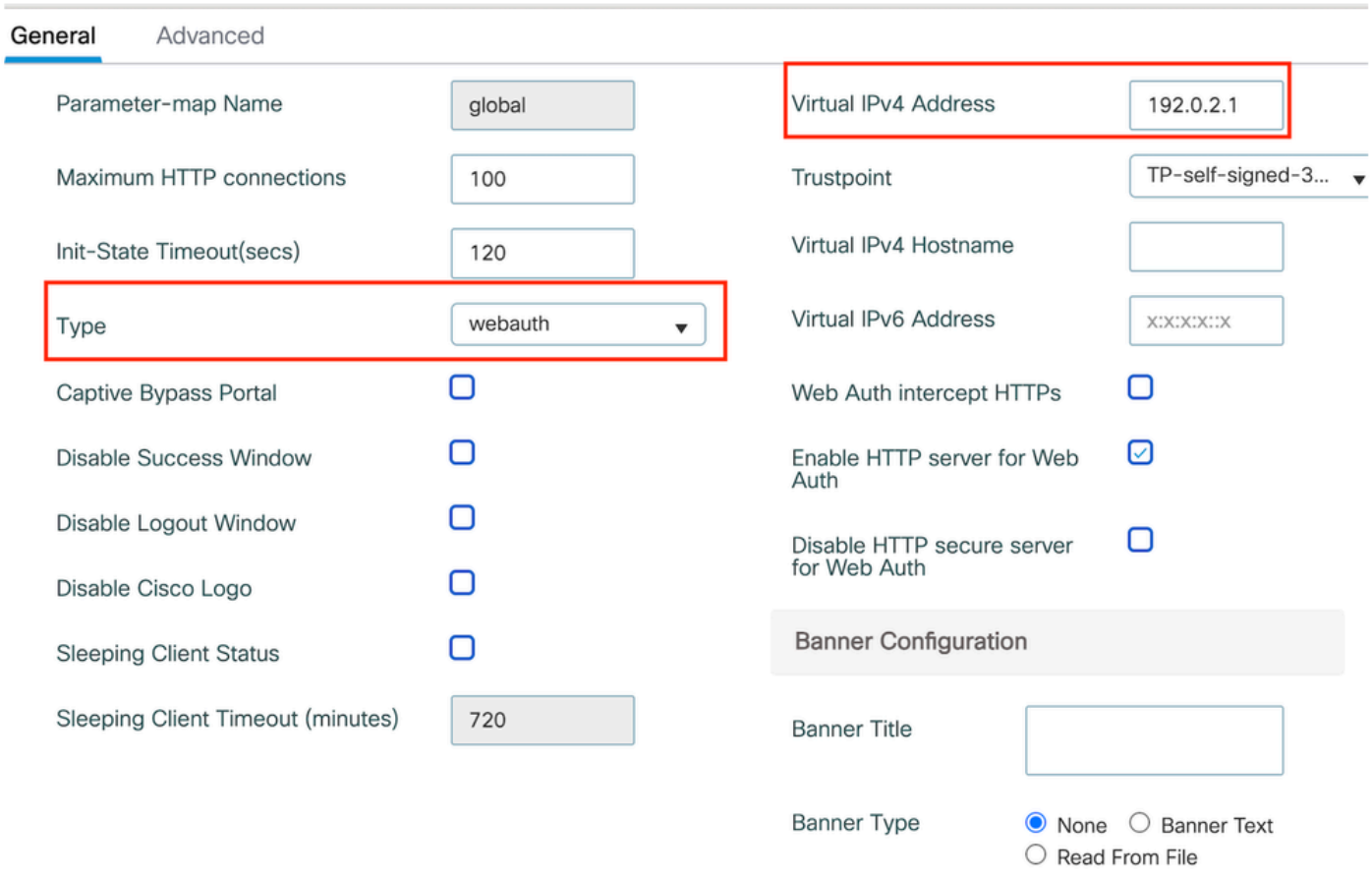
第6步：將移動錨點從下拉選單對映到訪客LAN配置檔案。

將移動錨點對映到訪客LAN

錨點9800 WLC上的組態

配置Web引數對映

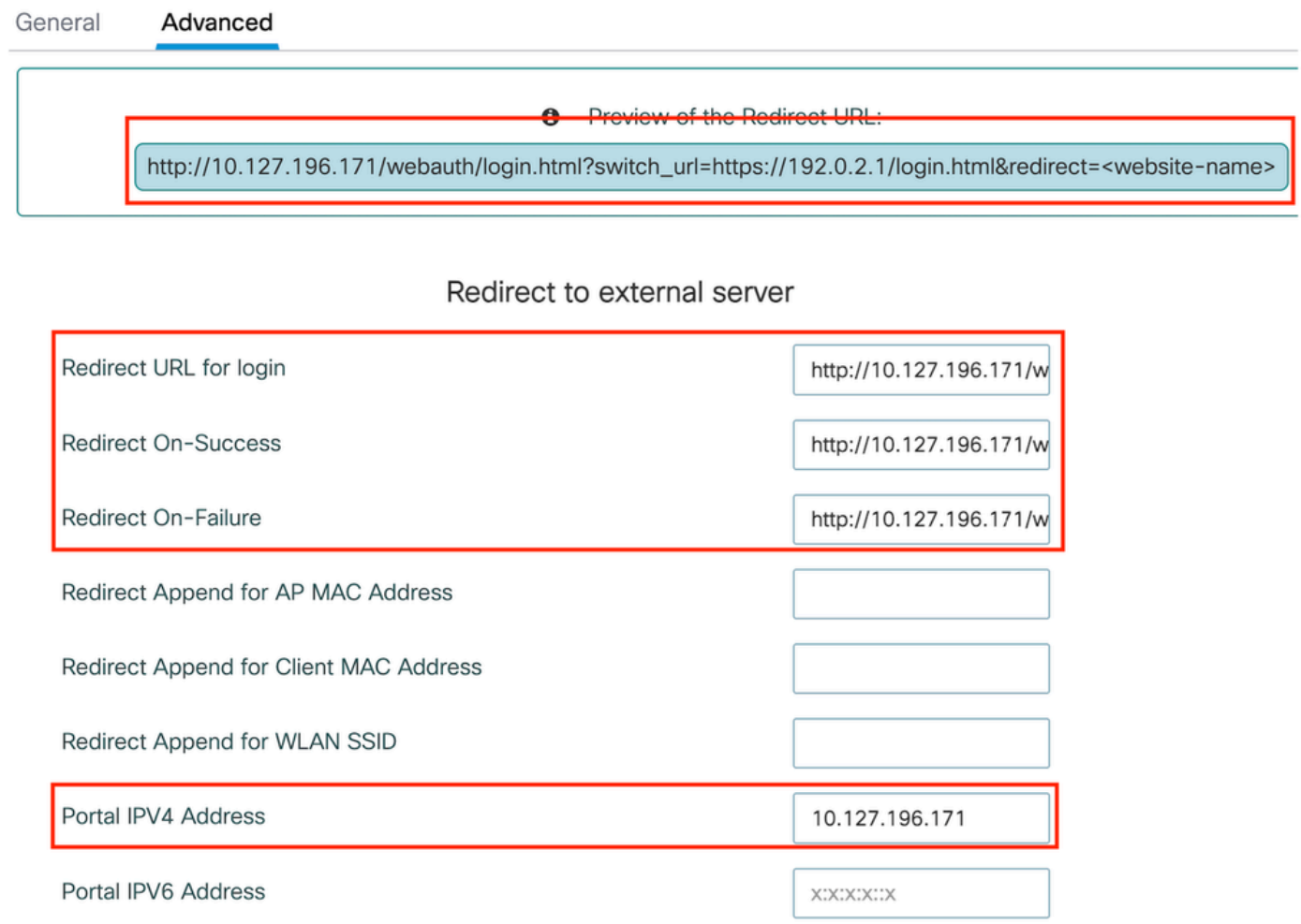
第1步：導航到配置>安全> Web身份驗證，然後選擇全局。驗證控制器的虛擬IP地址和信任點是否已正確對映到配置檔案上，並且型別設定為webauth。



Web引數對映

第2步：在高級頁籤下，指定客戶端必須重定向到的外部網頁URL。配置Redirect URL for Login和

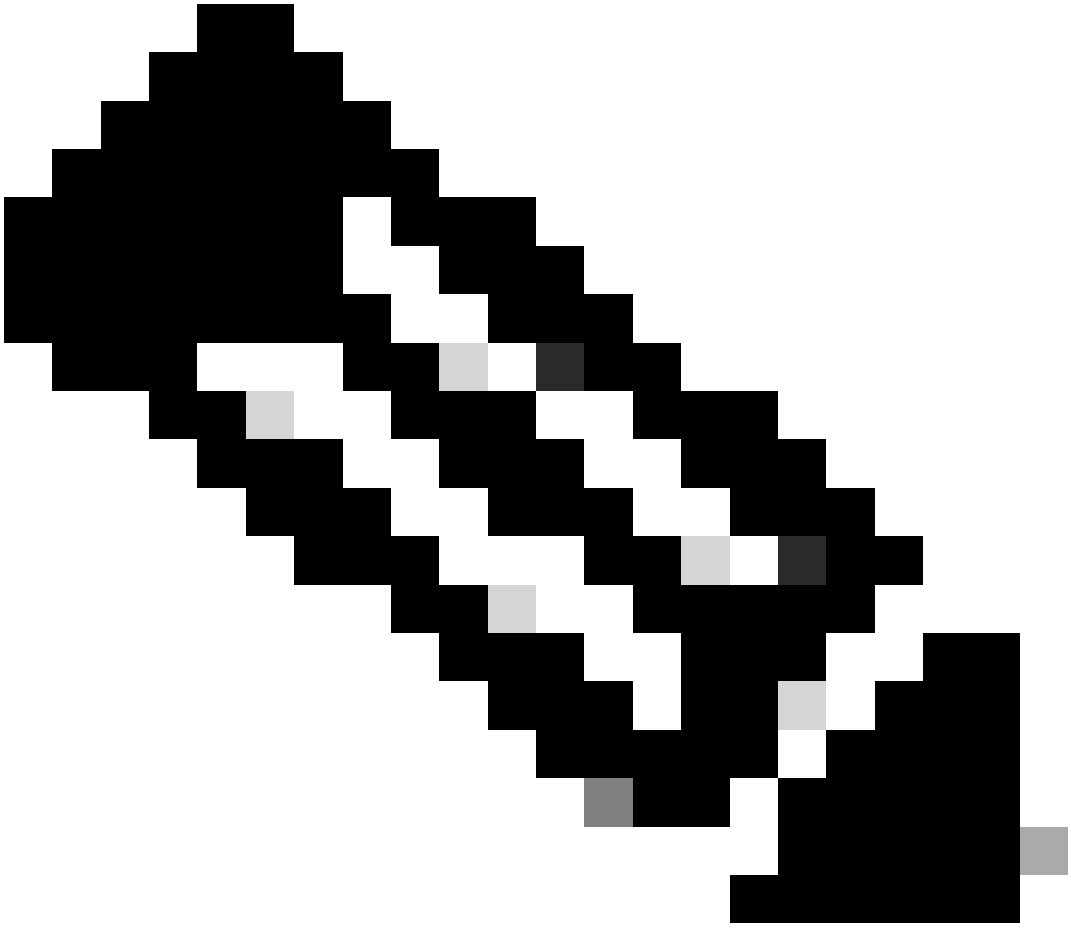
Redirect On-Failure。Redirect On-Success設定是可選配置。



進階標籤

CLI配置

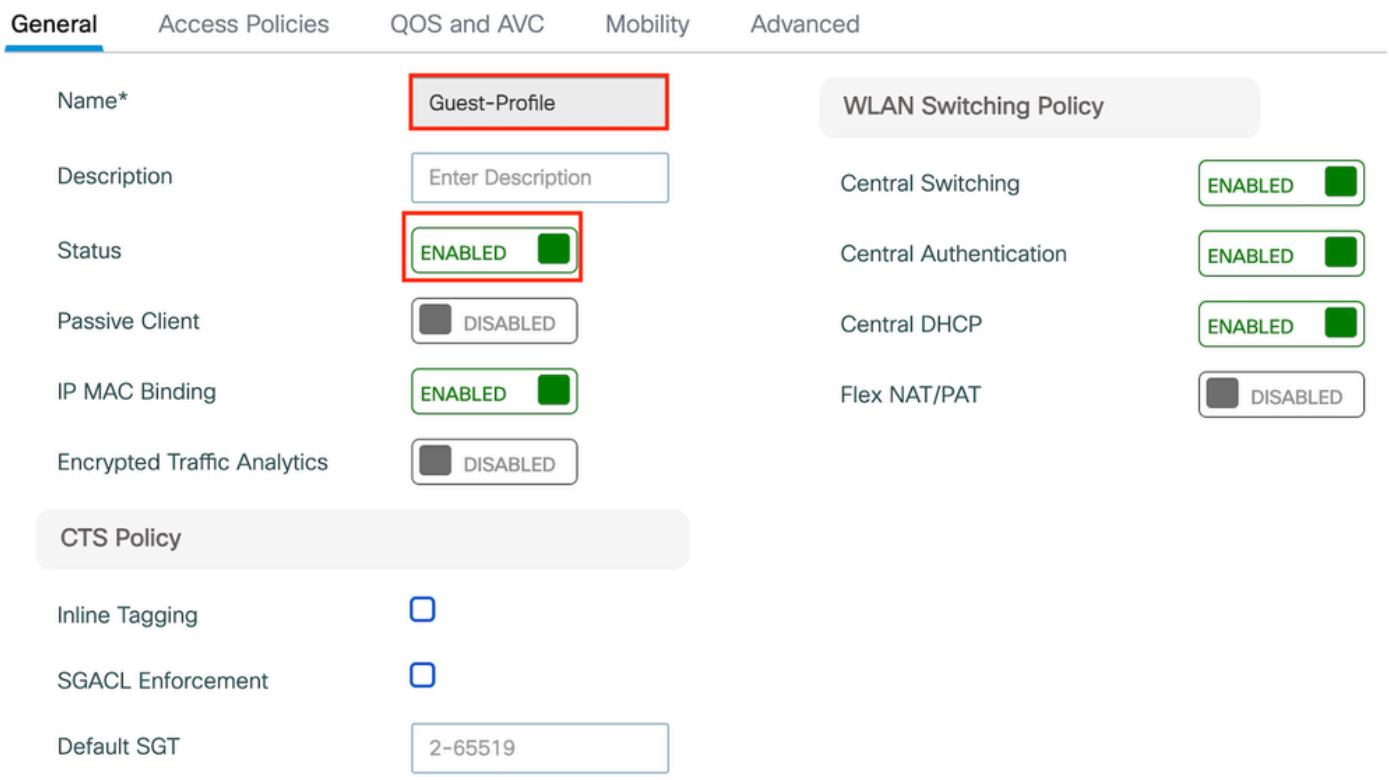
```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171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



注意：有關AAA配置，請參閱外部9800 WLC的「在Catalyst 9800上配置錨定到其他Catalyst 9800的有線訪客」部分中提供的配置詳細資訊。

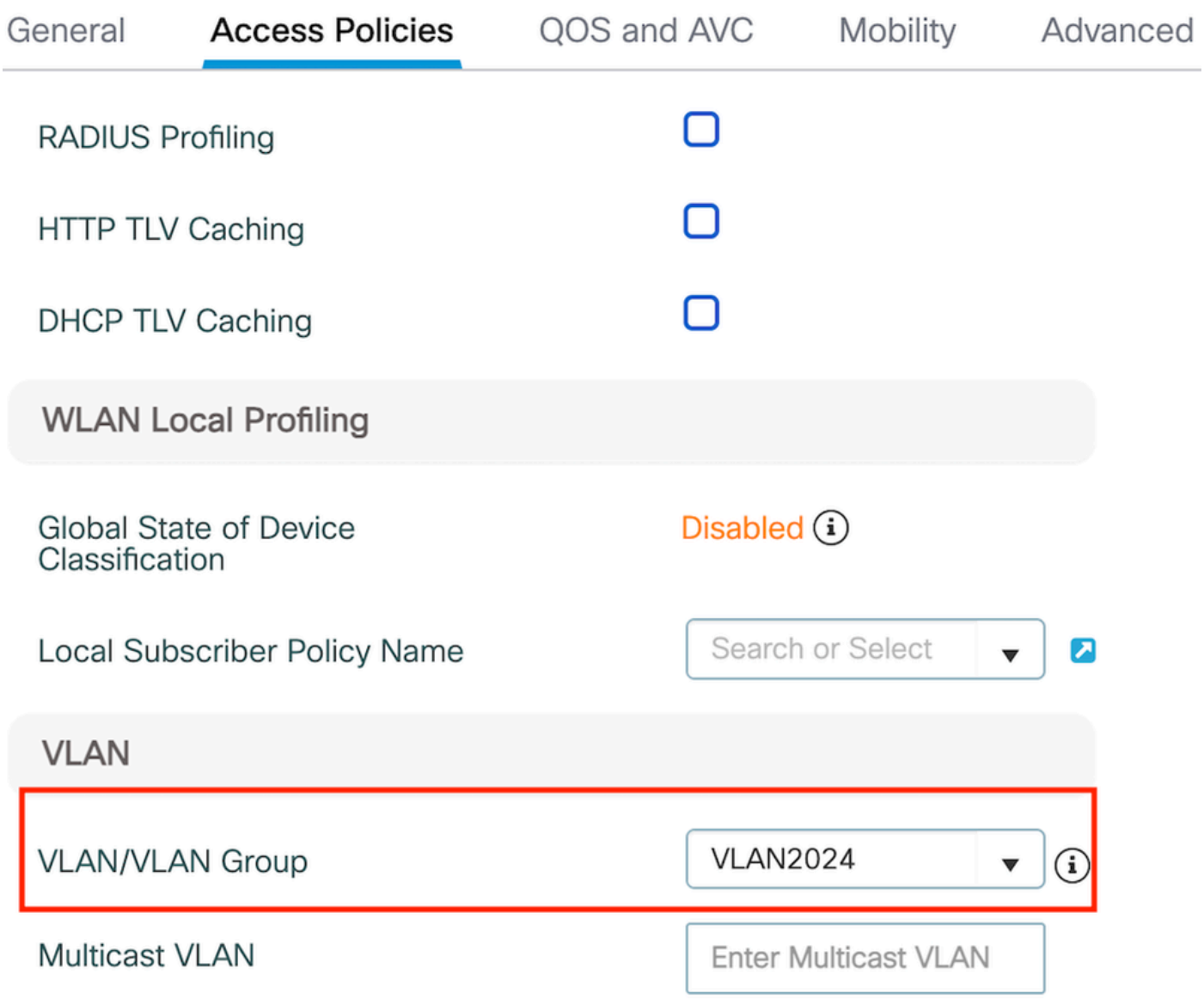
配置策略配置檔案

第1步：導航到配置>標籤和配置檔案>策略。使用與外部控制器的訪客LAN配置檔案相同的名稱配置策略配置檔案。



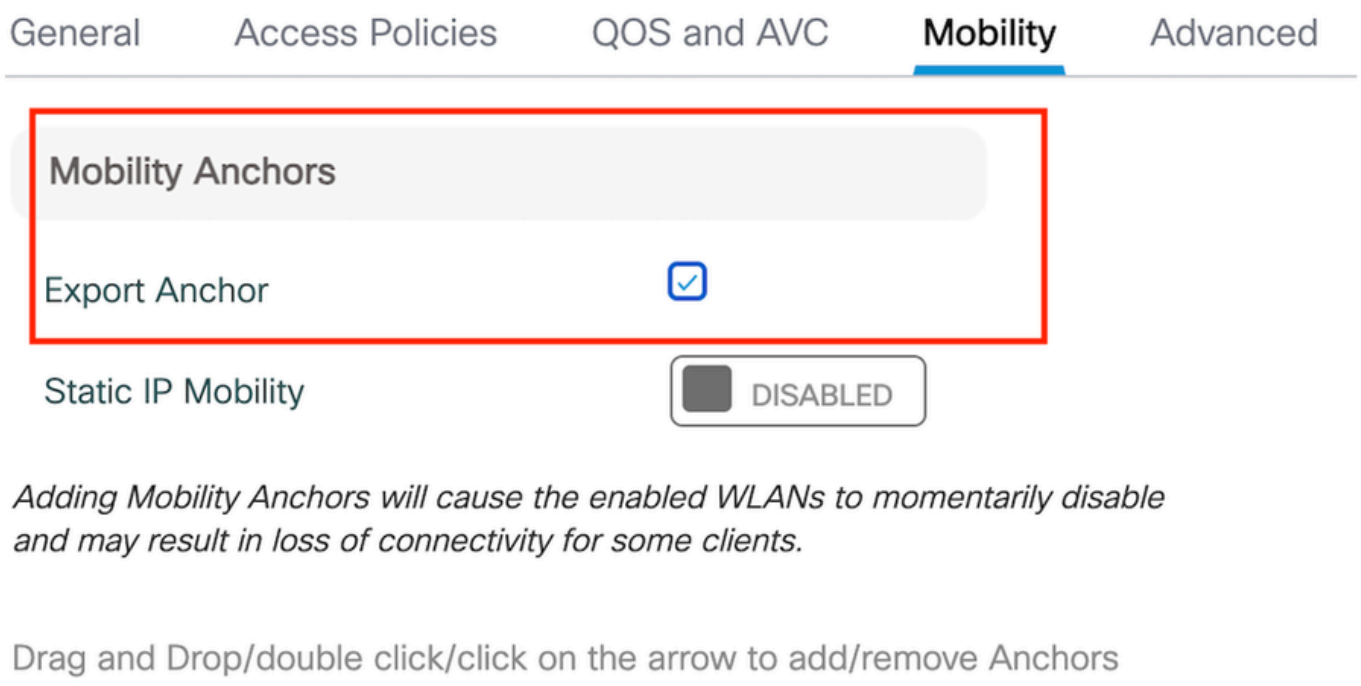
策略配置檔案

第2步：在Access Policies頁籤下，從下拉選單中對映有線客戶端VLAN



訪問策略

第3步：在移動頁籤下，選中導出錨點覈取方塊。



移動性頁籤

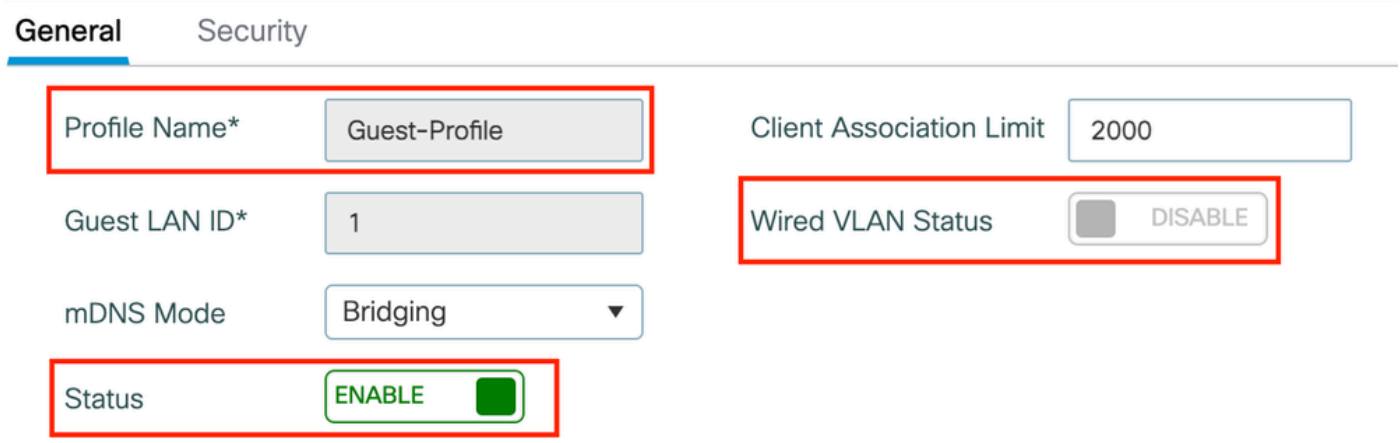
CLI配置

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

設定訪客LAN設定檔

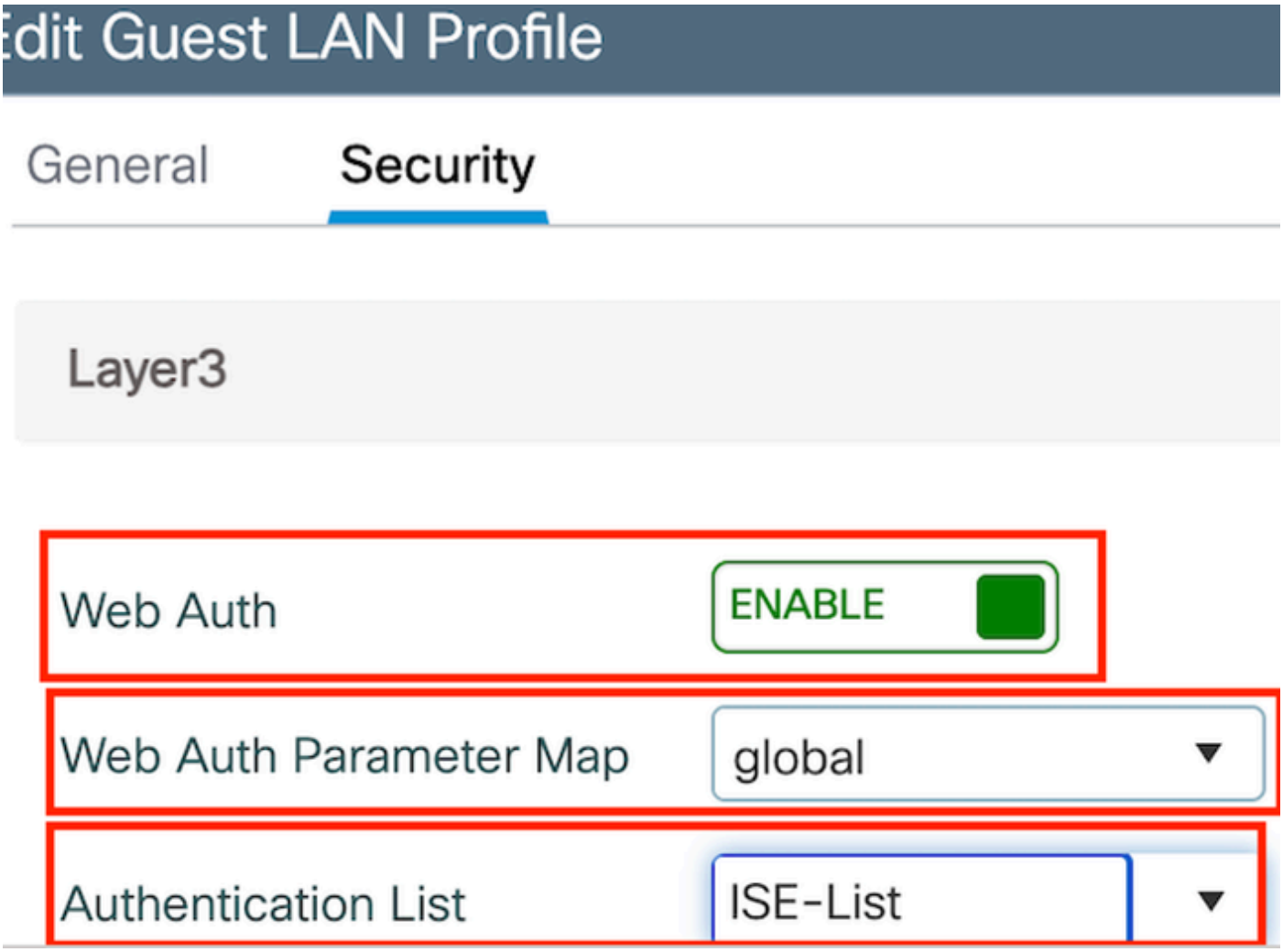
第1步：導航到配置>無線>訪客LAN，選擇增加配置訪客LAN配置檔案並停用有線VLAN狀態。

錨點上的訪客LAN配置檔名稱必須與外部WLC上的訪客LAN配置檔案相同。



訪客LAN配置檔案

第2步：在安全頁籤下，啟用Web身份驗證。 從下拉選單中選擇Web身份驗證引數對映和身份驗證清單



訪客LAN安全頁籤

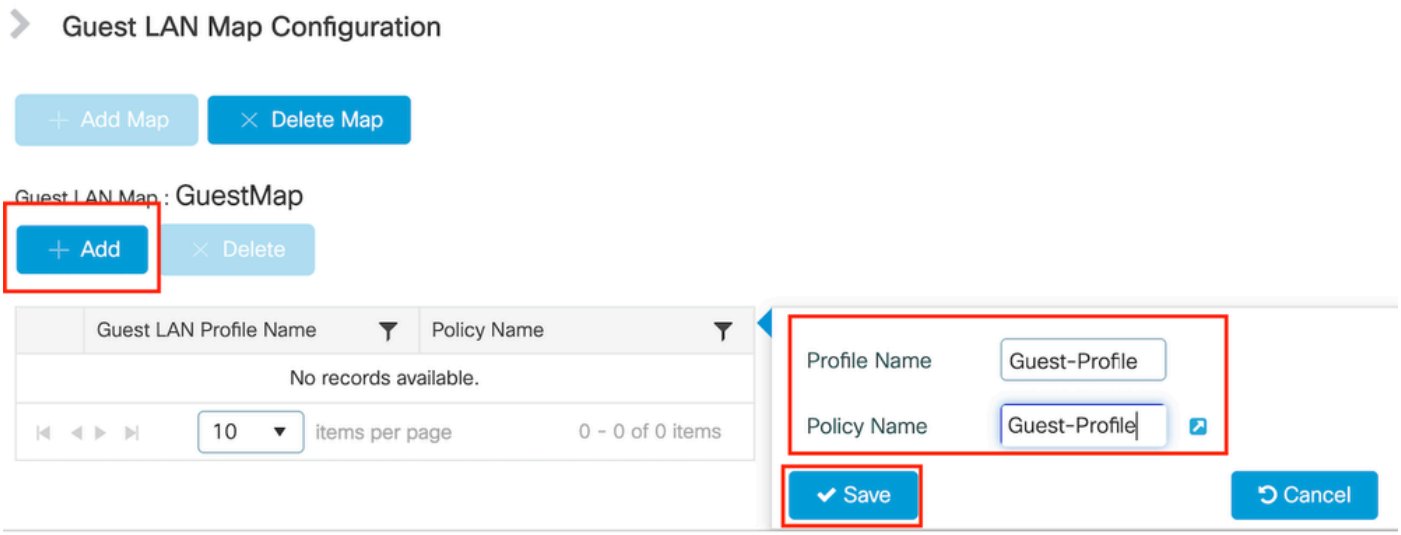
CLI配置

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

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

訪客LAN對映

第1步：導航到配置>無線>訪客LAN。在訪客LAN對映配置部分，選擇增加，並將策略配置檔案對映到訪客LAN配置檔案。



訪客LAN對映

驗證

驗證控制器配置

#show guest-lan summary

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

#show guest-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 parameter-map type webauth global

<#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>（如果使用自定義web引數配置檔案）

#show wireless guest-lan-map summary

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

#show無線移動性摘要

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

#show ip http伺服器狀態

```
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

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

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

>show guest-lan 2

```
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
```

>show custom-web all

```
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

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

驗證客戶端策略狀態

關於外國，

#show無線客戶端摘要

在客戶端成功關聯後，外部控制器上的客戶端策略管理器狀態為RUN。

<#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
```

在錨點上，

必須在錨點控制器上監視客戶端狀態轉換。

客戶端策略管理器狀態為Web Auth pending（Web身份驗證掛起）。

<#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
```

一旦客戶端進行身份驗證，策略管理器狀態將轉換為RUN狀態。

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

#show無線客戶端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
```

客戶端在成功Web身份驗證後進入RUN狀態。

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

在身份驗證客戶端轉換到RUN狀態之後。

<#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
```

疑難排解

AireOS控制器調試

啟用客戶端調試

>debug client <H.H.H>

驗證是否已啟用除錯

>show debugging

若要停用除錯，請執行下列動作

debug disable-all

9800放射性痕跡

啟用無線電活動跟蹤以在CLI中為指定的MAC地址生成客戶端調試跟蹤。

啟用放射性追蹤的步驟：

確定所有條件式偵錯都已停用。

```
clear platform condition all
```

為指定的MAC地址啟用調試。

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

重現問題後，請停用調試以停止RA跟蹤收集。

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

一旦RA跟蹤停止，調試檔案將在控制器的bootflash中生成。

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

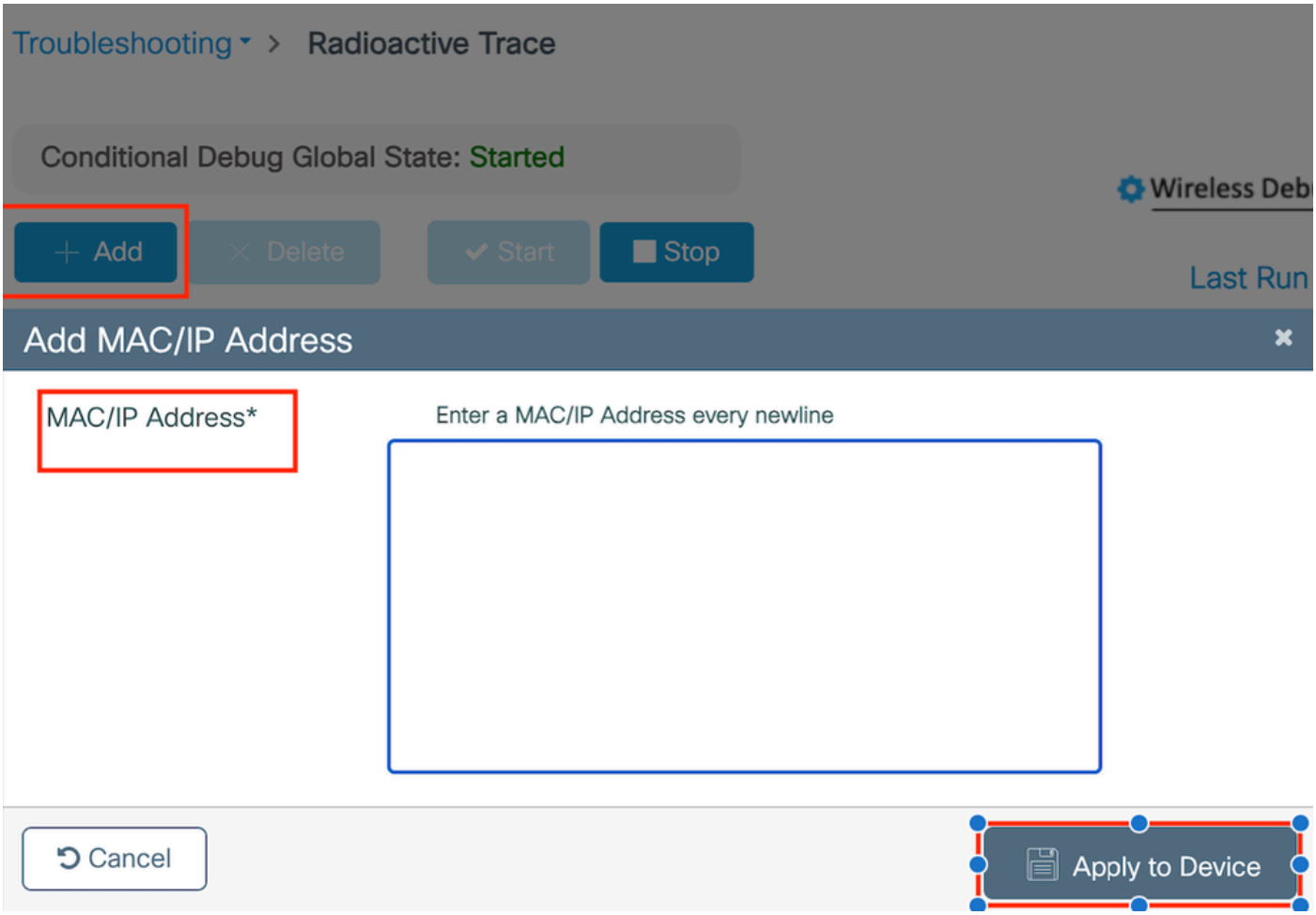
將檔案複製到外部伺服器。

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

顯示調試日誌：

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

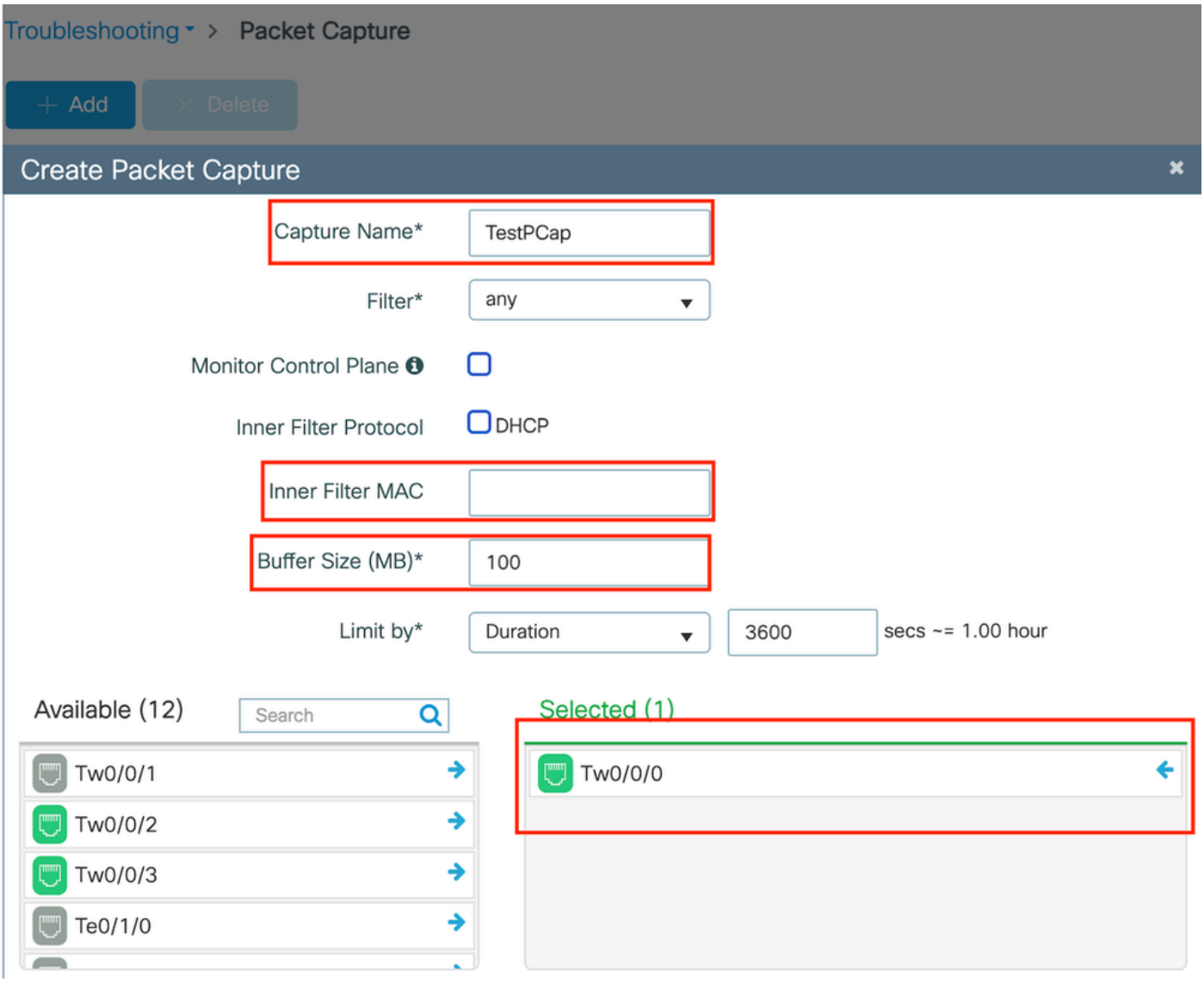
在GUI中啟用RA跟蹤，



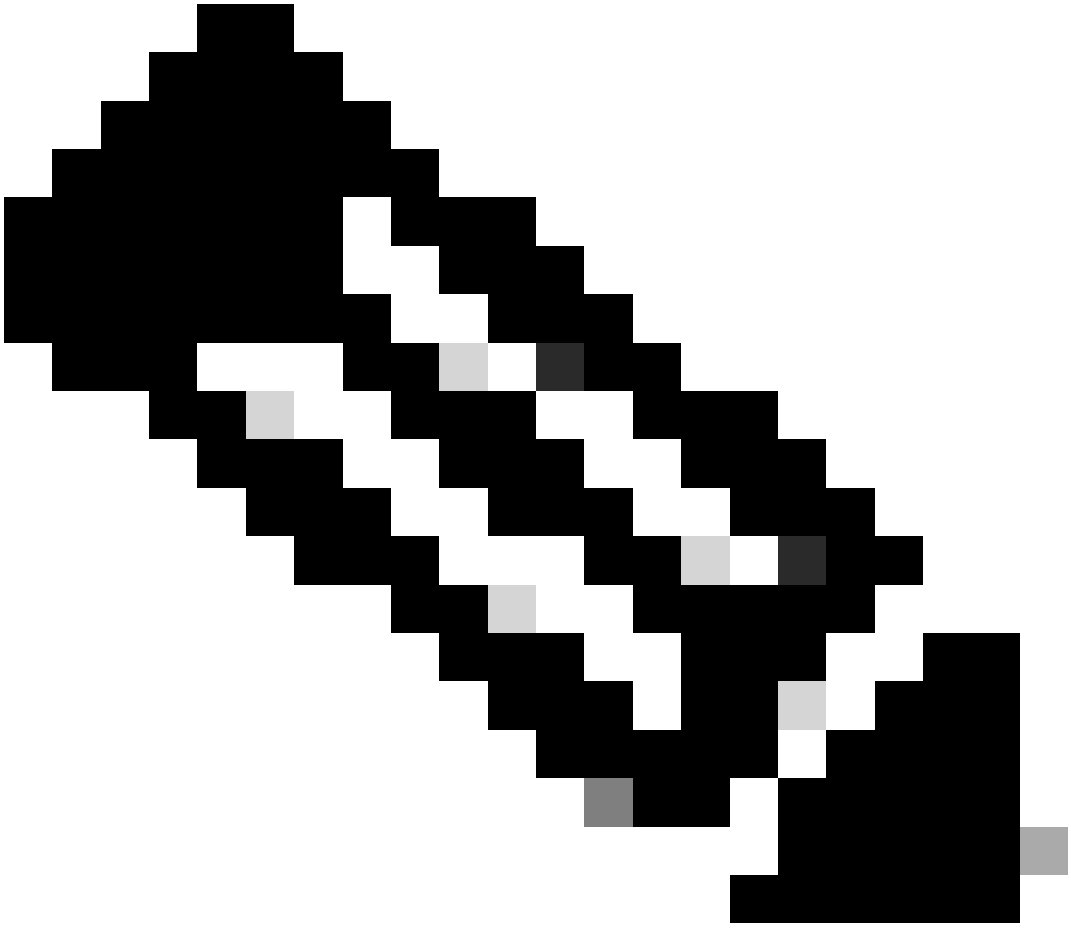
在WebUI上啟用RA追蹤

內嵌式封包擷取

導航到故障排除>資料包捕獲。輸入捕獲名稱並指定客戶端的MAC地址作為內部過濾器MAC。將緩衝區大小設定為100，並選擇上行鏈路介面來監控傳入和傳出的資料包。

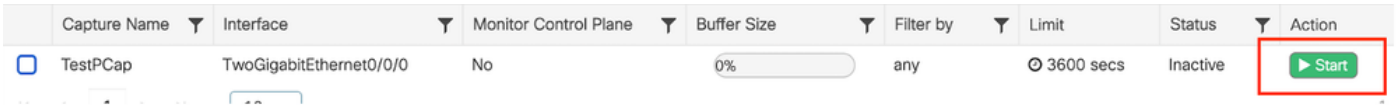

Troubleshooting
Packet Capture
Add
Delete
Create Packet Capture
Capture Name*
TestPCap
Filter*
any
Monitor Control Plane
Inner Filter Protocol
DHCP
Inner Filter MAC
Buffer Size (MB)*
100
Limit by*
Duration
3600
secs ~= 1.00 hour
Available (12)
Search
Tw0/0/1
Tw0/0/2
Tw0/0/3
Te0/1/0
Selected (1)
Tw0/0/0

內嵌式封包擷取



注意：選擇「監控控制流量」選項以檢視重定向到系統CPU並重新注入資料平面的流量。

導航到故障排除>資料包捕獲，選擇開始捕獲資料包。



開始資料包捕獲

CLI配置

```
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
```

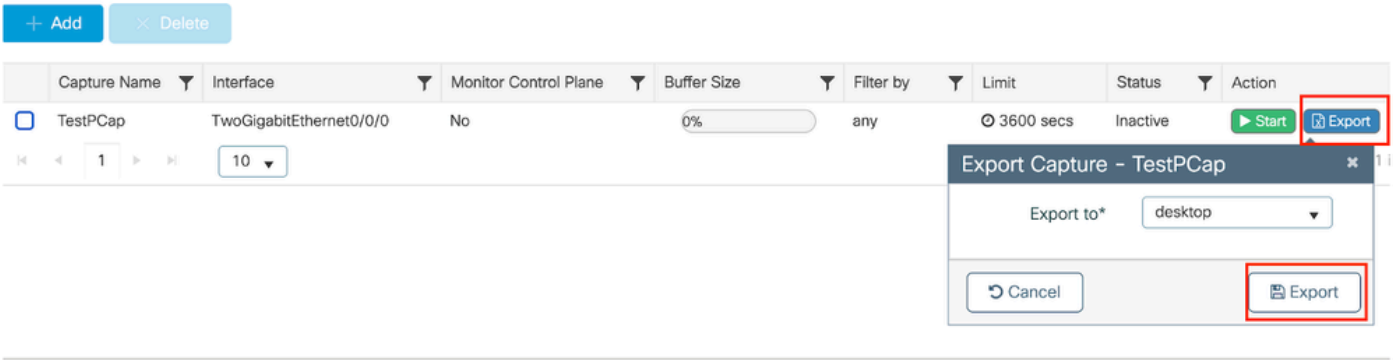
```
show monitor capture TestPCap

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)
```

將資料包捕獲導出到外部TFTP伺服器。

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

導航到故障排除>資料包捕獲，選擇導出以將捕獲檔案下載到本地電腦上。



下載EPC

工作日誌片段

AireOS外部控制器客戶端調試日誌

從有線客戶端接收的有線資料包

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

外部控制器建立匯出錨點要求

```
*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
```

外部控制器向錨點控制器傳送導出錨點請求。

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

錨點控制器為客戶端傳送錨點請求的確認

```
*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
```

外部控制器上客戶端的移動角色已更新為導出外部。

```
*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
```

客戶端轉換到RUN狀態。

```
*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放射性示蹤劑

使用者端與控制器關聯。

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

關聯後移動性發現正在進行中。

```
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
```

處理移動性發現後，客戶端漫遊型別是請求的L3更新。

```
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
```

外部控制器正在將導出錨點請求傳送到錨點WLC。

```
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 Forw
```

從錨點控制器接收導出錨點響應，並從使用者配置檔案應用vlan。

```
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:
```

處理導出錨點請求後，客戶端移動角色將更新為導出外部。

```
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
```

客戶端轉換到IP學習狀態。

```
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
```

在IP獲知後，客戶端在外部WLC上進入RUN狀態。

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

AireOS錨點控制器客戶端調試日誌

從外部控制器接收匯出錨點要求。

```
*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
```

本地橋接VLAN應用於客戶端。

```
*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
```

移動角色更新為「導出錨點」，客戶端狀態轉換為「關聯」。

```
*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
```

移動已完成，客戶端狀態已關聯，移動角色為導出錨點。

```
*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
```

使用者端IP位址是在控制器上得知的，且狀態已從所需的DHCP轉換至所需的Web驗證。

```
*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是透過增加外部重定向URL和控制器虛擬IP地址來形成的。

```
*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://
```

已將客戶端MAC地址和WLAN增加到URL。

```
*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
```

剖析主機10.105.211.1的HTTP GET後的最終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.
```

重定向URL傳送到200 OK響應資料包中的客戶端。

```
*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
```

客戶端與重定向url主機建立TCP連線。一旦使用者端在入口端提交登入使用者名稱和密碼，控制器就會將radius要求傳送到radius伺服器

控制器收到Access-Accept後，客戶端關閉TCP會話並進入RUN狀態。

```
*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錨點控制器放射性跟蹤

來自外部控制器的客戶端移動通告消息。

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

當客戶端正在關聯時，從外部控制器接收導出錨點請求，該客戶端的導出錨點響應由錨點控制器傳送，可在外部控制器RA跟蹤上驗證。

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

客戶端已移至關聯狀態，移動角色已轉換為導出錨點。

```
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學習完成，客戶端IP透過ARP學習。

```
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
```

客戶端策略狀態為web auth pending。

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

TCP握手被控制器偽裝。當客戶端傳送HTTP GET時，會傳送200 OK響應幀，其中包含重定向URL。

使用者端必須與重新導向URL建立TCP交握並載入頁面。

```
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
```

使用者端在Web入口頁面上提交登入認證時，會向RADIUS伺服器傳送存取要求封包以進行驗證。

```
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
```

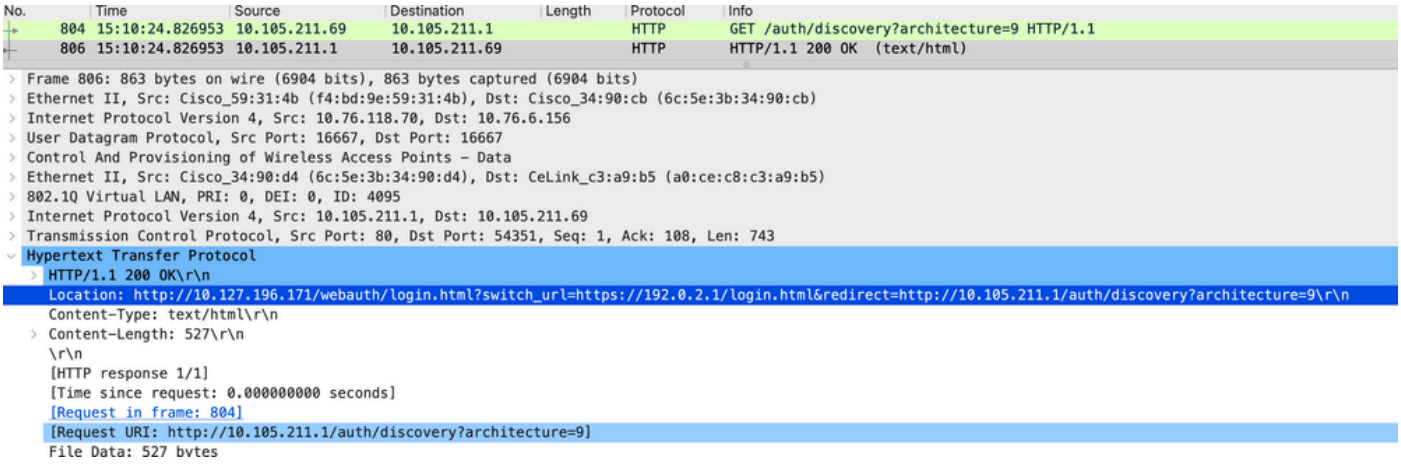
從RADIUS伺服器收到Access-Accept，webauth成功。

```
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
```

身份驗證成功，客戶端策略狀態為RUN。

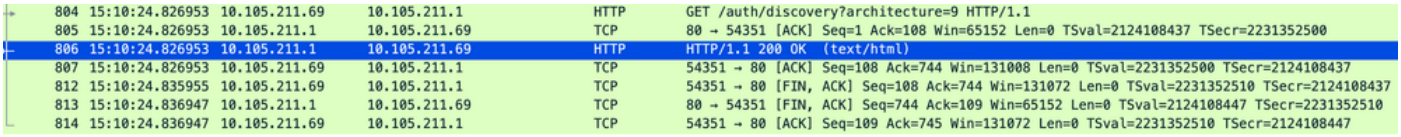
```
2024/07/15 15:12:04.683901842 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:12:04.690643388 {wncd_x_R0-0}{1}: [errmsg] [14709]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/15 15:12:04.690726966 {wncd_x_R0-0}{1}: [aaa-attr-inf] [14709]: (info): [ Applied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

嵌入式資料包捕獲分析



使用者端已重新導向至入口網站頁面

收到重定向URL後，會話關閉。

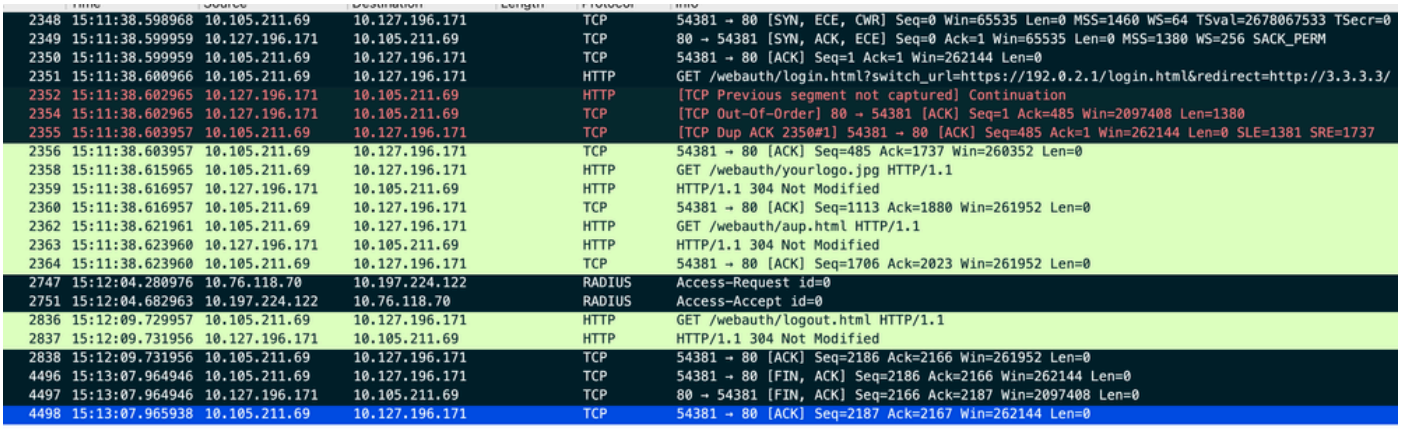


收到重新導向URL後，TCP作業階段關閉

客戶端發起到重定向URL主機的TCP 3次握手，並傳送HTTP GET請求。

頁面載入後，登入憑證會提交到入口網站，控制器會向radius伺服器傳送存取要求，以驗證使用者端。

身份驗證成功後，與Web伺服器的TCP會話關閉，並在控制器上將客戶端策略管理器狀態轉換為RUN。



客戶端向門戶頁面傳送HTTP GET請求並成功完成身份驗證

Radius存取要求封包

```
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
RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 363
    Authenticator: e3018f5d8e52fccbe0d703dac1a209e6
    [The response to this request is in frame 2751]
  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)
```

訪問請求資料包

Radius存取接受封包

```
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]
 Attribute Value Pairs
    AVP: t=User-Name(1) l=10 val=testuser
    AVP: t=Class(25) l=57 val=434143533a3030303030303030303030303733423542433434374 23a697365333167…
    AVP: t=Message-Authenticator(80) l=18 val=223df8645f1387d7137428b20df9e0c1
```

Access Accept packet

相關文章

[在Catalyst 9800上配置WLAN錨點移動功能]

[使用AireOS控制器的有線訪客接入配置示例]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。