在SD-Access上配置中央Web身份驗證

目錄

簡介

本文檔介紹配置中央Web身份驗證(CWA)的逐步指南，並概述所有元件的驗證過程。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Catalyst Center
- 思科身分識別服務引擎(ISE)
- Catalyst 9800無線控制器架構
- 驗證、授權及記帳(AAA)

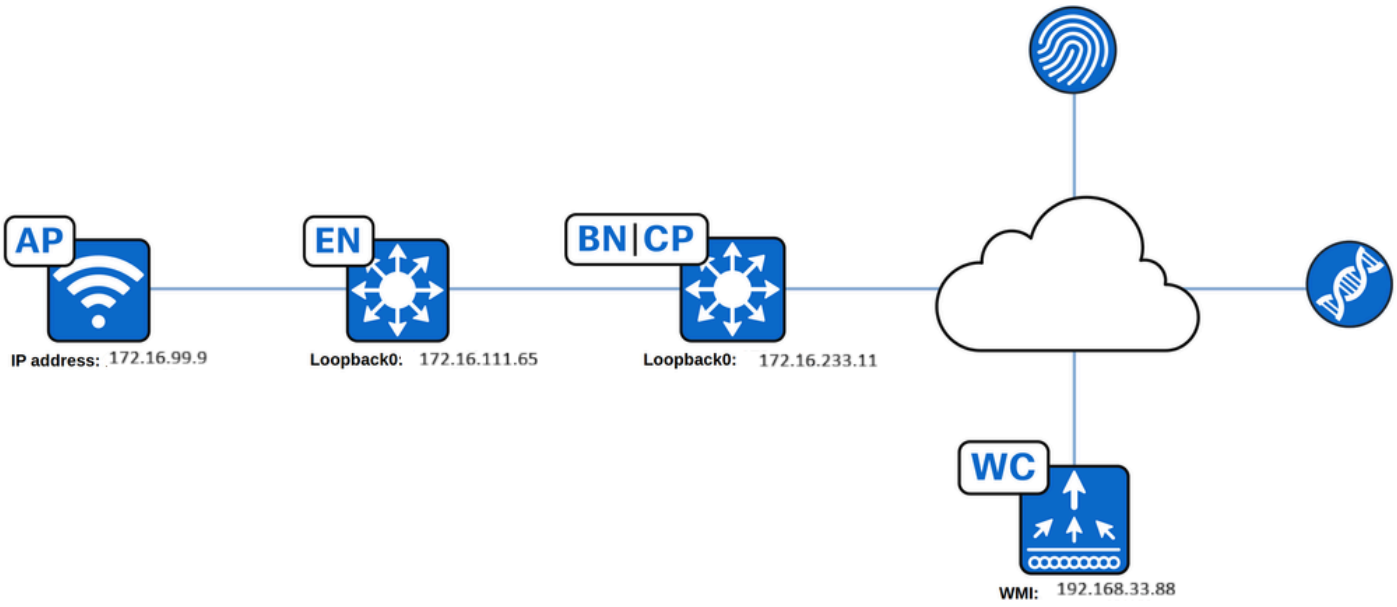
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco無線LAN控制器(WLC)- C9800-CL、Cisco IOS® XE 17.12.04
- Cisco Catalyst中心 — 2.3.7.7版
- 思科身份服務引擎(ISE)- 3.0.0.458版
- SDA邊緣節點 — C9300-48P,Cisco IOS® XE 17.12.05
- SDA邊界節點/控制平面 — C9500-48P,Cisco IOS® XE17.12.05
- 思科存取點 — C9130AXI-A，版本17.9.5.47

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。

拓撲



概觀

中央Web驗證(CWA)使用訪客型別SSID將使用者的Web瀏覽器重定向至由思科ISE託管的強制網路門戶（使用配置的重定向ACL）。強制網路門戶允許使用者註冊和身份驗證，身份驗證成功後，無線LAN控制器(WLC)應用適當的授權以授予完整網路訪問許可權。本指南提供使用Cisco Catalyst Center配置CWA的逐步說明。

在Cisco Catalyst Center上配置CWA

建立網路配置檔案

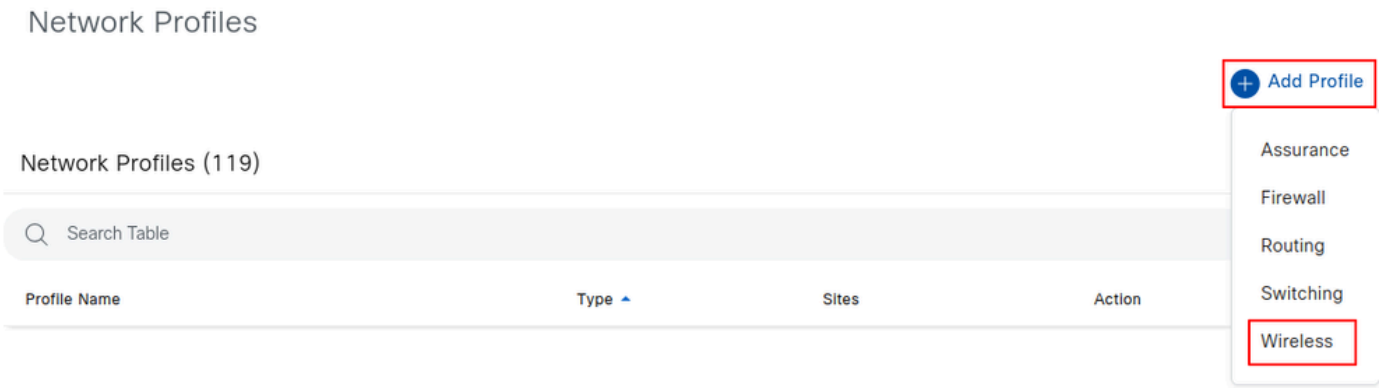
網路配置檔案允許配置可應用於特定站點的設定。可以為Cisco Catalyst Center中的各種元素建立網路配置檔案，包括：

- 保證
- 防火牆
- 路由
- 交換
- 遙測裝置

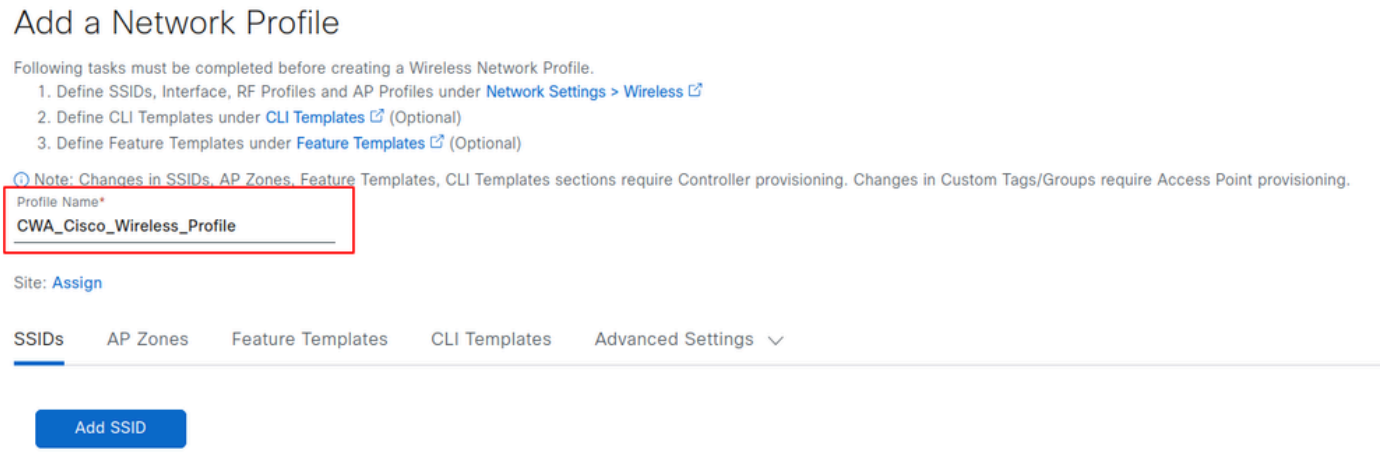
- 無線

對於CWA，必須配置無線配置檔案。

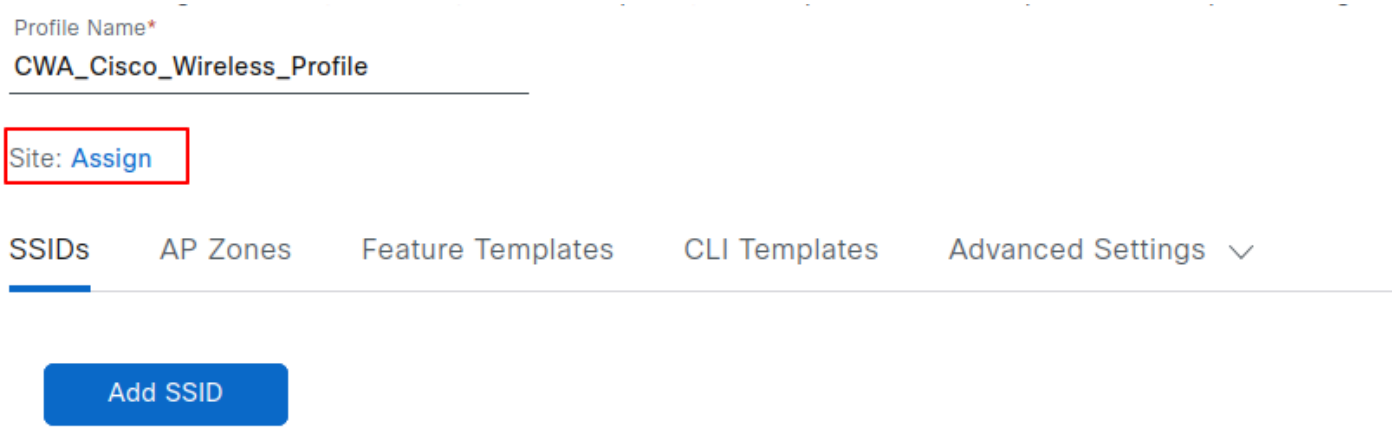
要配置無線配置檔案，請導航到設計>網路配置檔案，按一下新增配置檔案，然後選擇無線。



根據需要為配置檔案命名。在本示例中，無線配置檔案命名為CWA_Cisco_Wireless_Profile。您可以通過選擇Add SSID將任何現有SSID新增到此配置檔案。下一節將介紹SSID的建立。

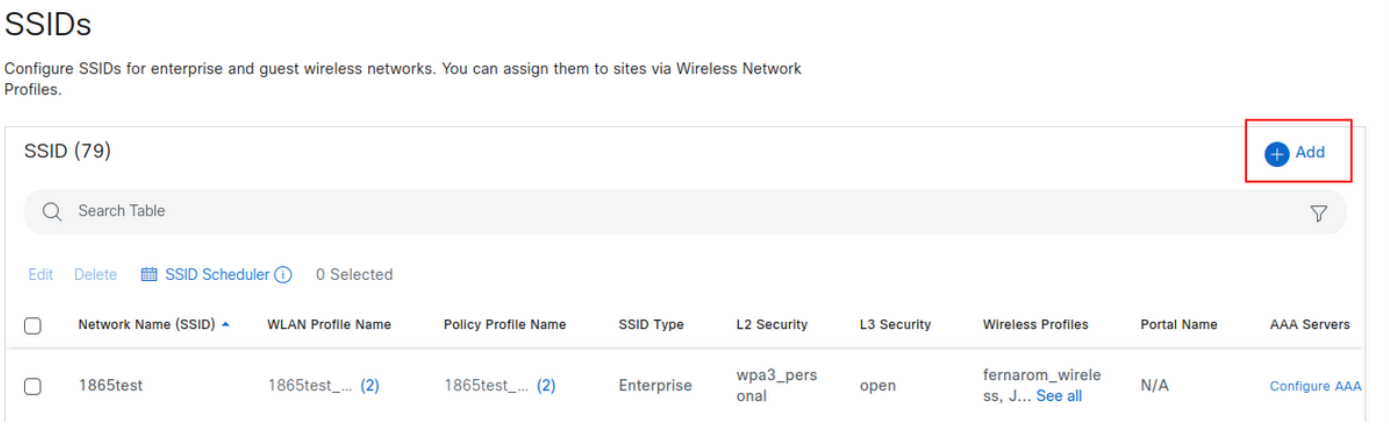


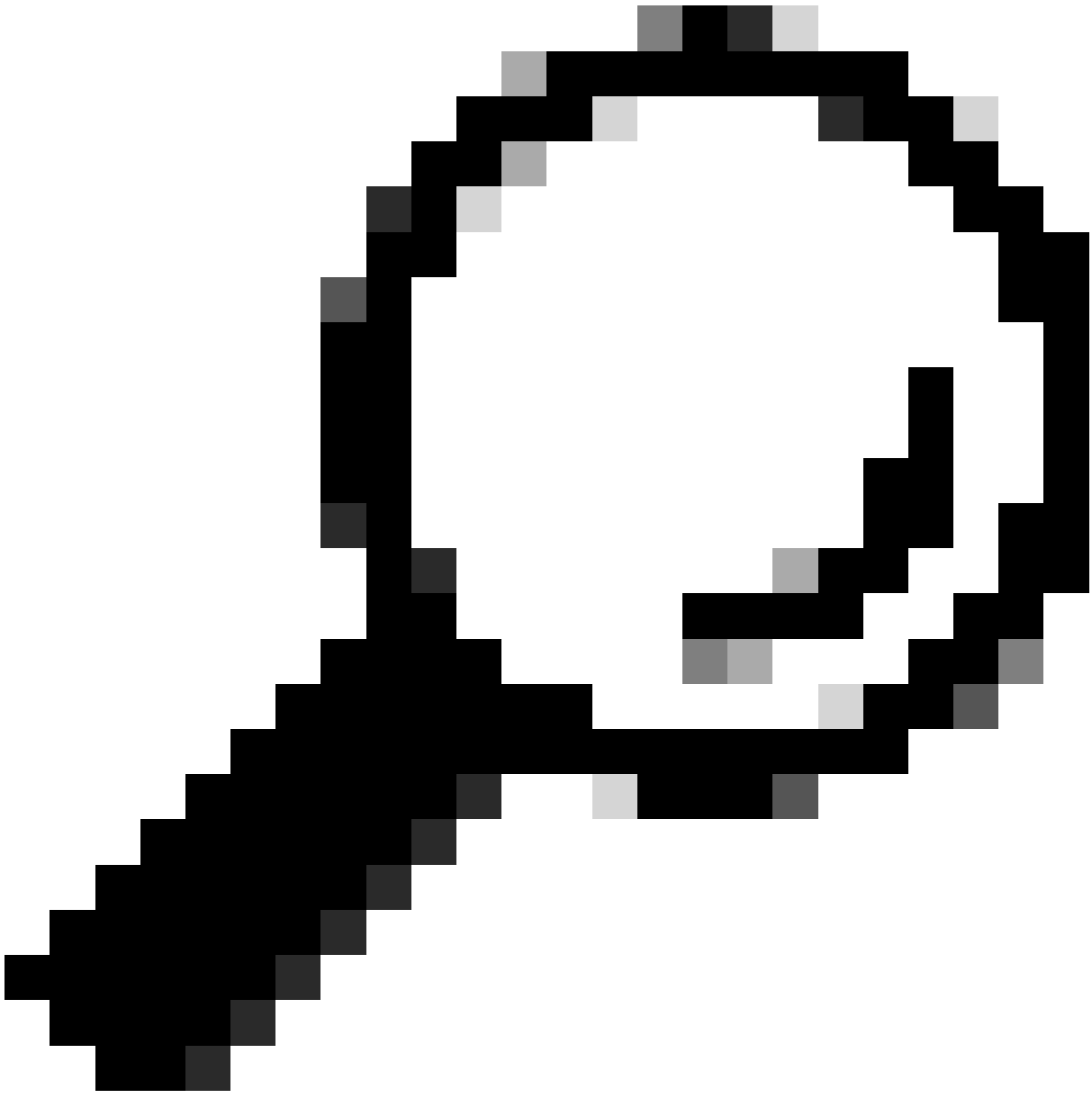
選擇Assign以選擇要應用此配置檔案的站點，然後選擇所需的站點。選擇站點後，按一下Save。



建立SSID

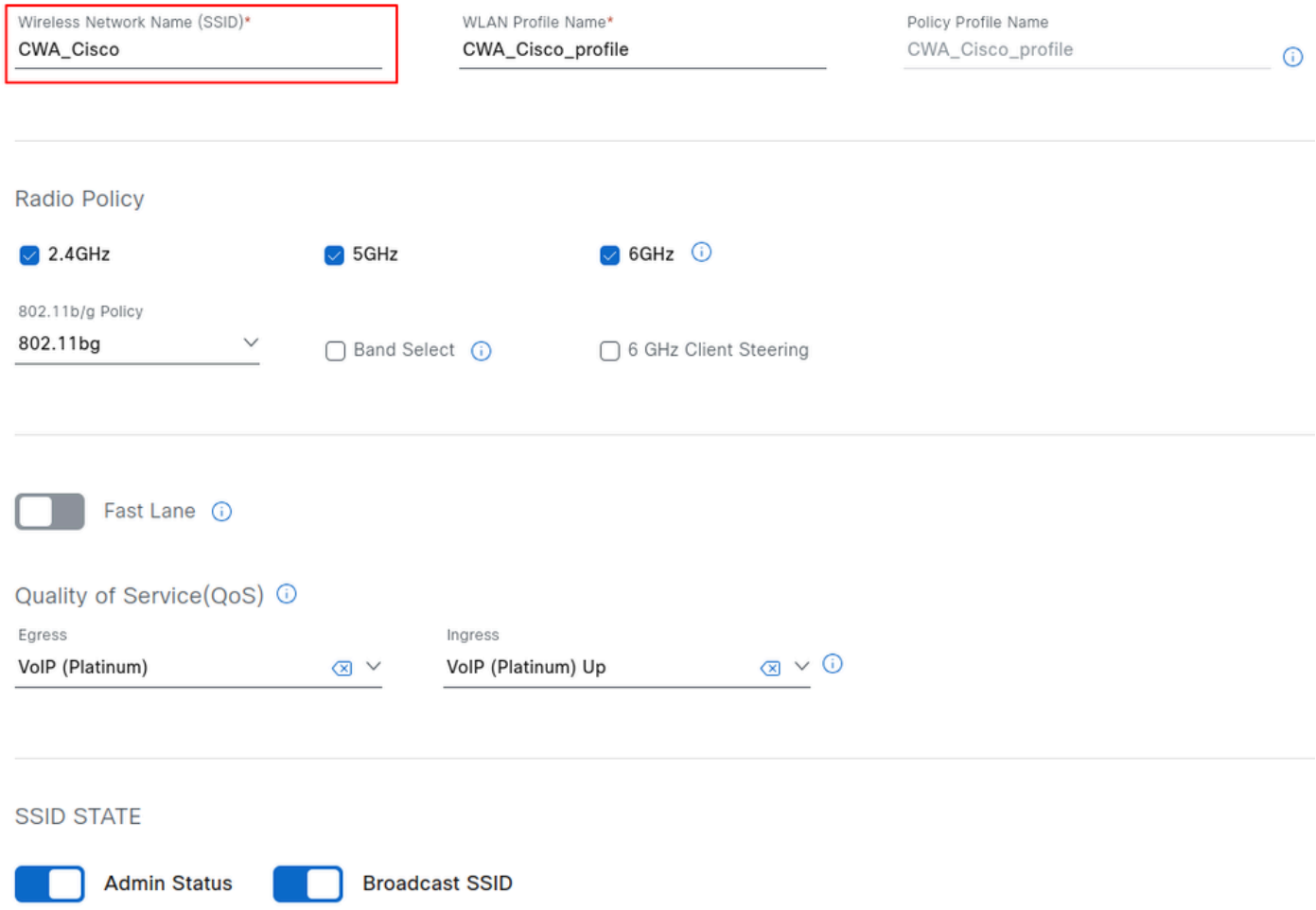
導航至Design > Network Settings > Wireless > SSIDs，然後點選Add。



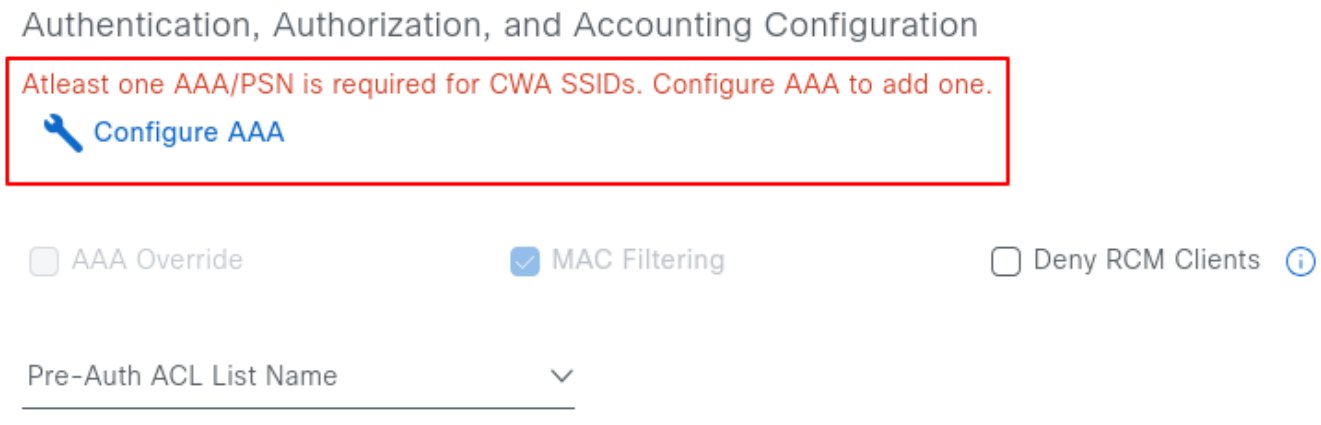


提示：為CWA建立SSID時，選擇Guest type至關重要。此選擇向WLC上的SSID無線策略配置檔案新增命令 — nac命令 — 允許使用者在強制網路門戶上註冊後使用CoA進行重新身份驗證。如果沒有此配置，使用者可能會遇到無休止的循環：註冊並反複重定向到門戶。

選擇Add後，繼續執行SSID配置工作流。在第一頁上，配置SSID名稱，您還可以選擇radio policy band，並定義SSID狀態，包括管理狀態和廣播設定。在本配置指南中，SSID名稱為CWA_Cisco。

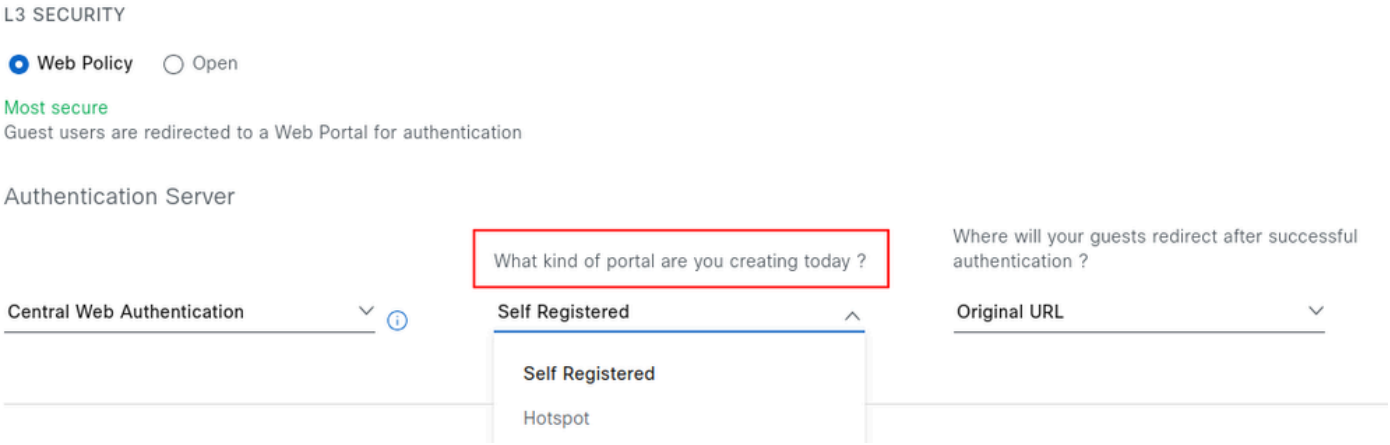


輸入SSID名稱后，將自動生成WLAN配置檔名稱和策略配置檔名稱。選擇Next繼續。
必須至少為CWA SSID配置一個AAA/PSN。如果沒有配置任何地址，請選擇Configure AAA並從下拉選單中選擇PSN IP address。

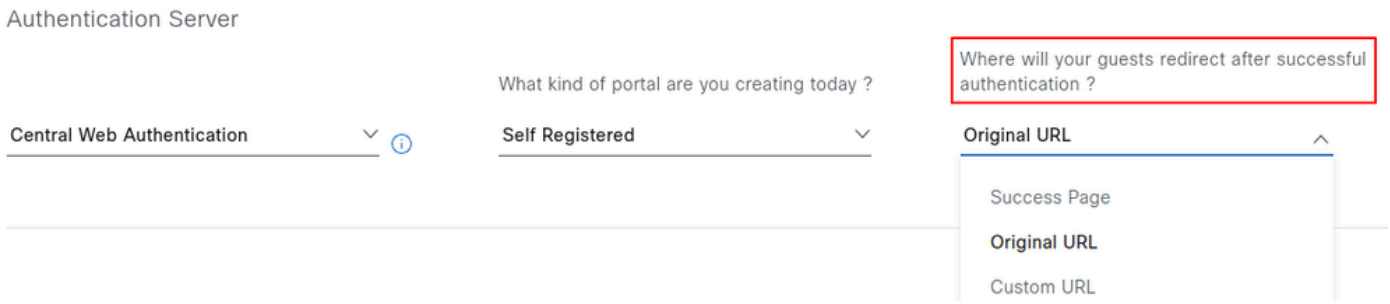


選擇AAA伺服器後，設定第3層安全引數並選擇入口型別：Self-Registered or Hotspot。

熱點訪客門戶：熱點訪客門戶為訪客提供網路訪問，無需使用者名稱和密碼。在此，使用者必須接受可接受的使用策略(AUP)才能訪問網路，進而訪問後續的Internet。提供憑證的訪客門戶：通過具有憑證的訪客門戶進行訪問，需要訪客具有使用者名稱和密碼。



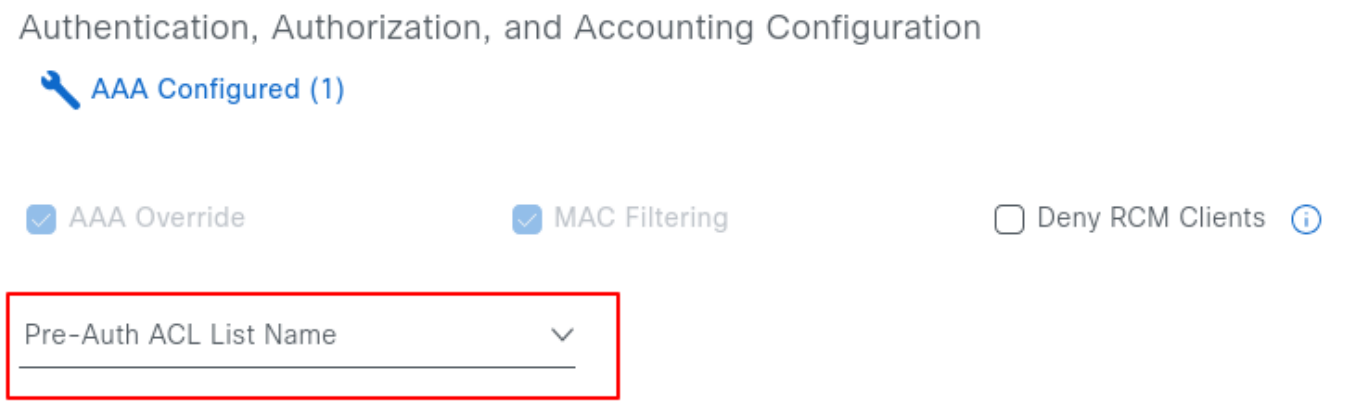
還可以配置在使用者註冊或接受使用策略後發生的操作。有三個可用選項：Success Page、Original URL和Custom URL。



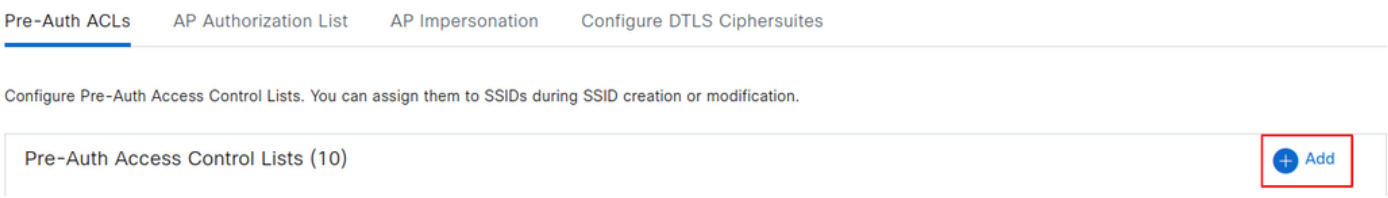
以下說明每個選項的行為：

「成功」頁：將使用者重定向到指示身份驗證成功的確認頁。
原始URL：將使用者重定向到在被強制網路門戶截獲之前請求的原始URL。
自定義URL：將使用者重定向到指定的自定義URL。選擇此選項可啟用其他欄位來定義目標URL

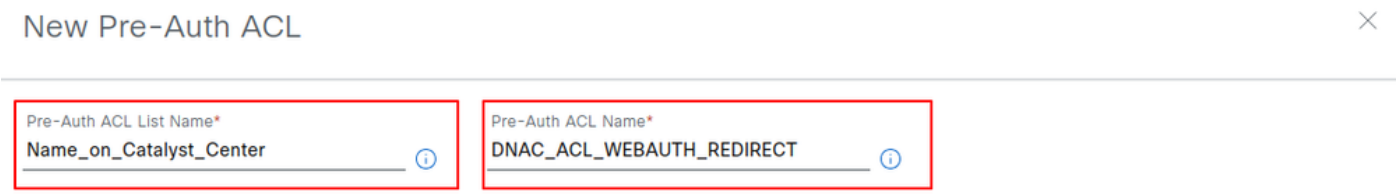
在同一頁面上，在驗證、授權和計費組態下，您還可以設定預先驗證ACL。此ACL允許為DHCP、DNS或PSN IP位址以外的通訊協定新增額外專案，這些專案是從網路設定中取得，並在布建期間追加到重新導向ACL中。Cisco Catalyst Center 2.3.3.x版及更高版本提供此功能。



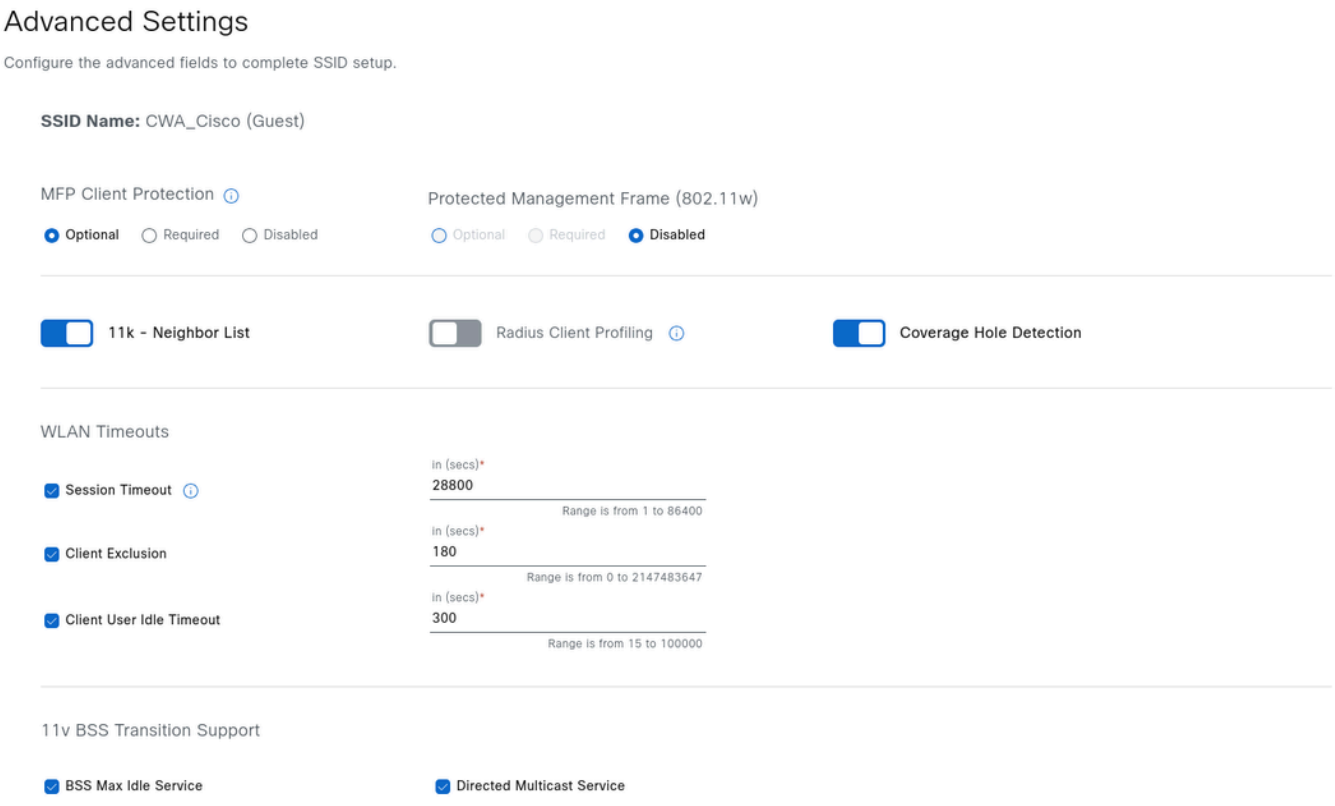
若要設定預先驗證ACL，請導覽至Design > Network Settings > Wireless > Security Settings，然後按一下Add。



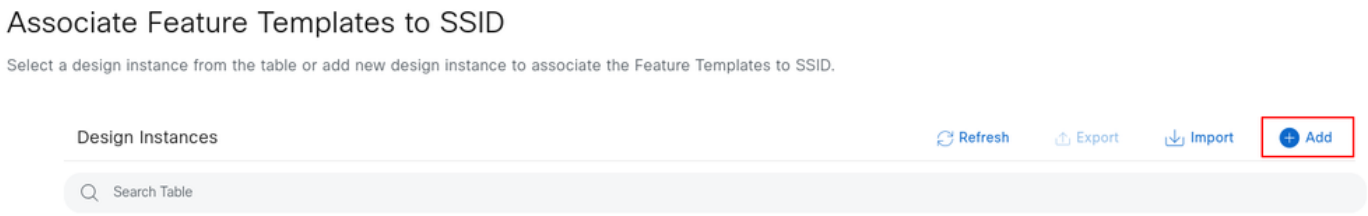
第一個名稱識別Catalyst Center中的ACL，而第二個名稱對應於WLC上的ACL名稱。第二個名稱可與WLC上設定的現有重新導向ACL相符。作為參考，Catalyst Center將名稱Cisco DNA_ACL_WEBAUTH_REDIRECT設定為WLC。預先驗證ACL中的專案會在現有專案之後附加。



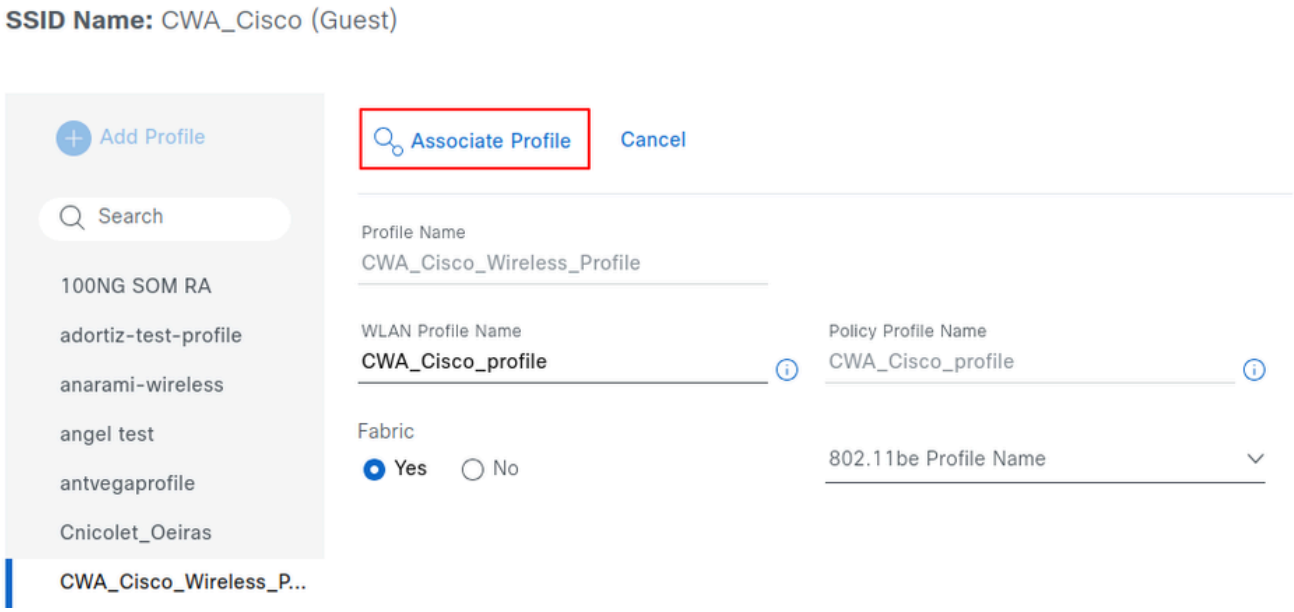
返回SSID建立工作流，選擇下一步將顯示高級設定，包括快速轉換、會話超時、客戶端使用者超時和速率限制。根據需要調整引數，然後選擇下一步以繼續。出於本配置指南的目的，該示例保留預設設定。



選擇Next後，系統將顯示提示以將任何功能模板與SSID關聯。如果適用，通過按一下Add選擇所需的模板，並在完成後按一下Next。



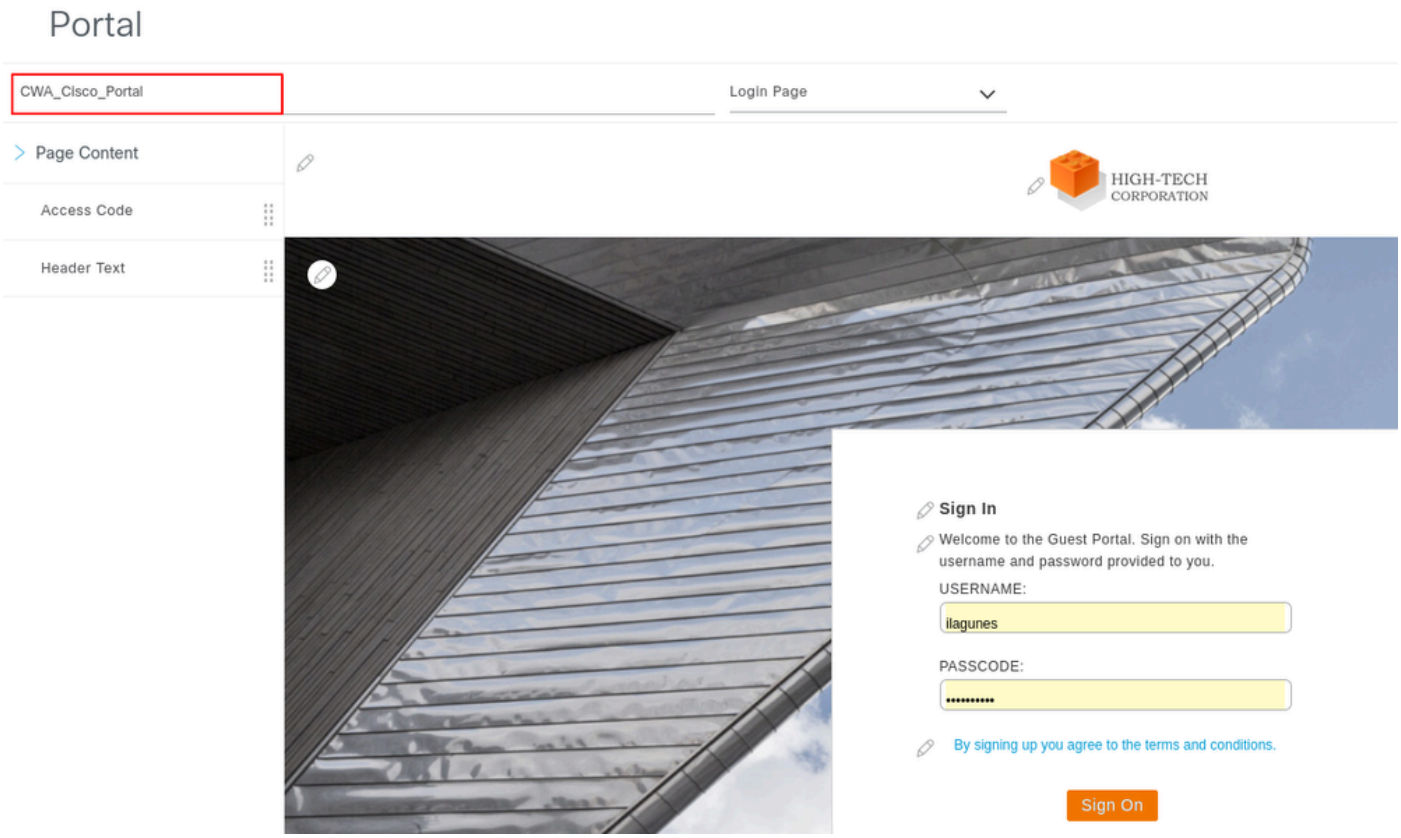
將SSID與先前建立的無線配置檔案相關聯。有關參考，請參閱建立無線網路配置檔案部分。在此部分中，您還可以選擇是否啟用了SSID交換矩陣。完成後，按一下關聯配置檔案。



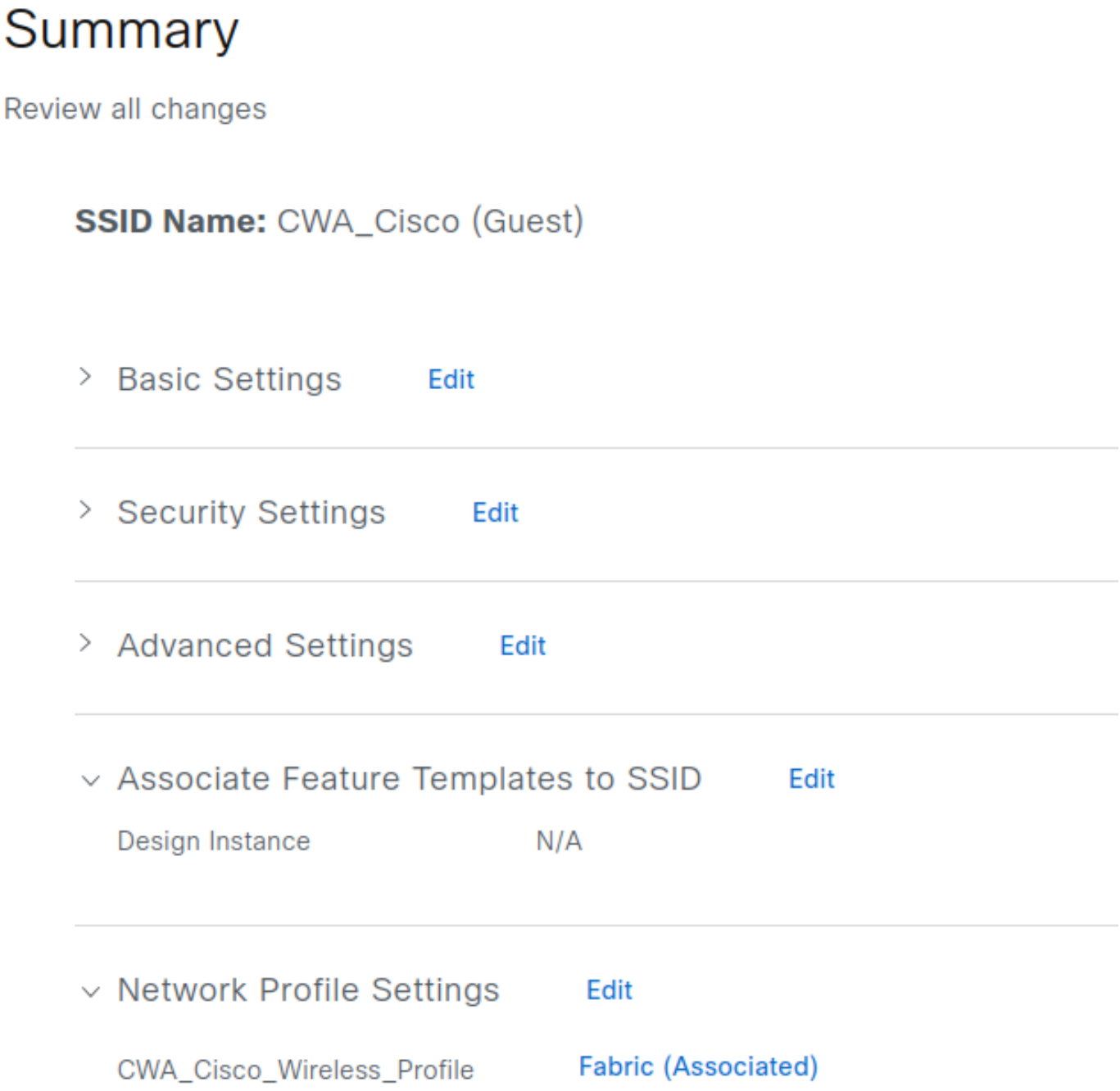
show wireless management trustpoint

配置式與SSID關聯後，按一下下一步以建立和設計強制網路門戶，要啟動，請按一下建立門戶。

門戶名稱定義FQDN中的域名和ISE上的策略集名稱。完成後按一下Save。門戶保持可編輯狀態，必要時可將其刪除。



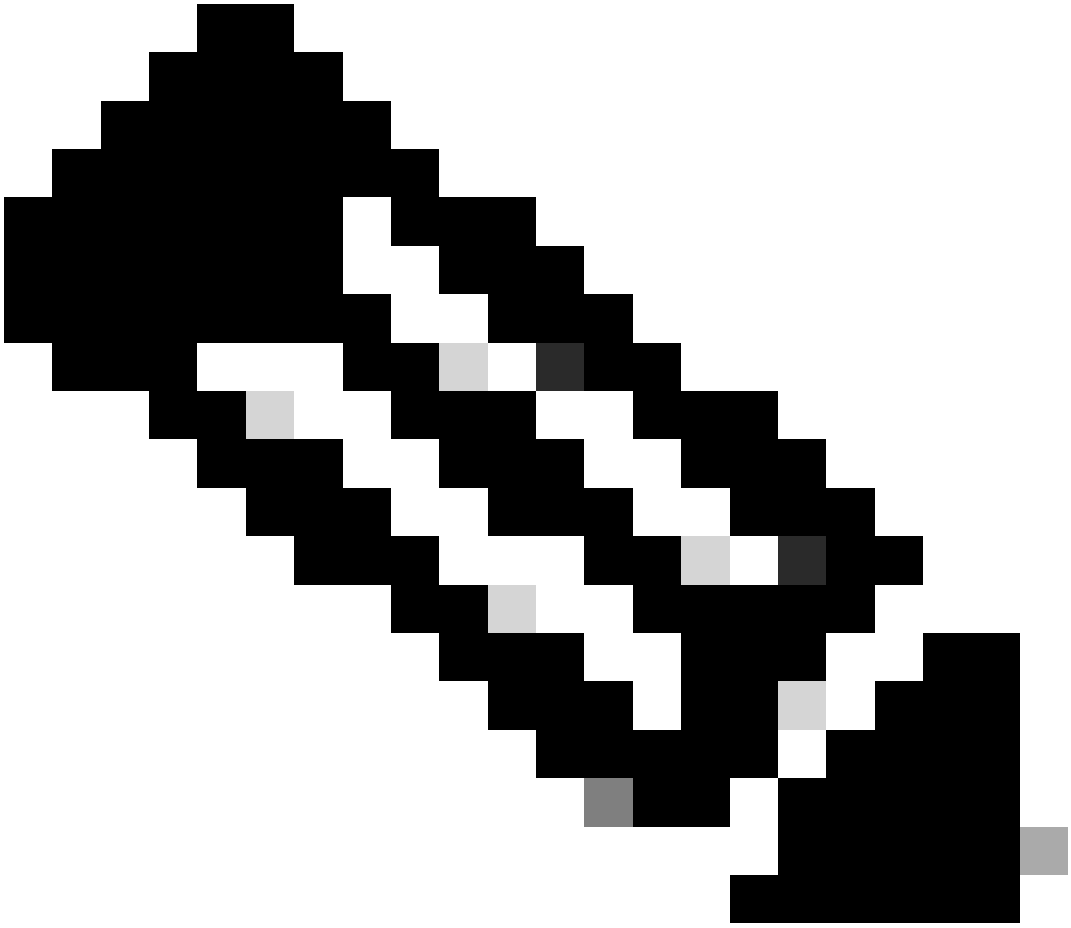
選擇下一步以顯示之前步驟中定義的所有配置引數的摘要。



確認配置詳細資訊，然後選擇Save以應用更改。

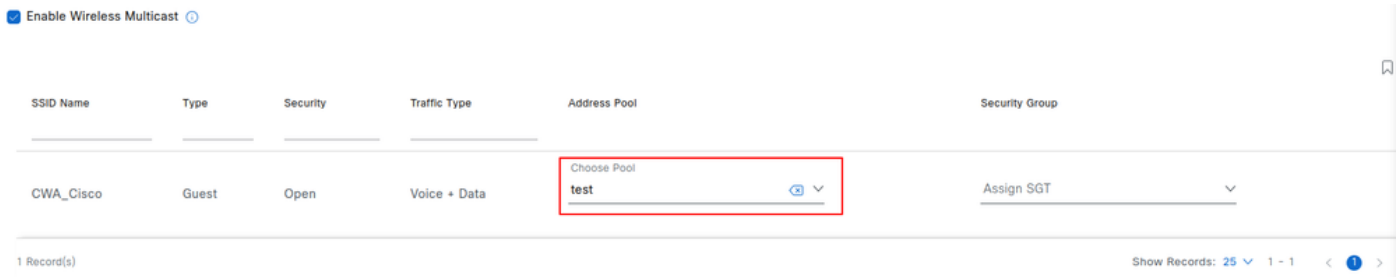
光纖布建

將無線網路配置檔案與交換矩陣站點關聯後，SSID將顯示在Provision > Fabric Sites >（您的站點）> Wireless SSIDs下。

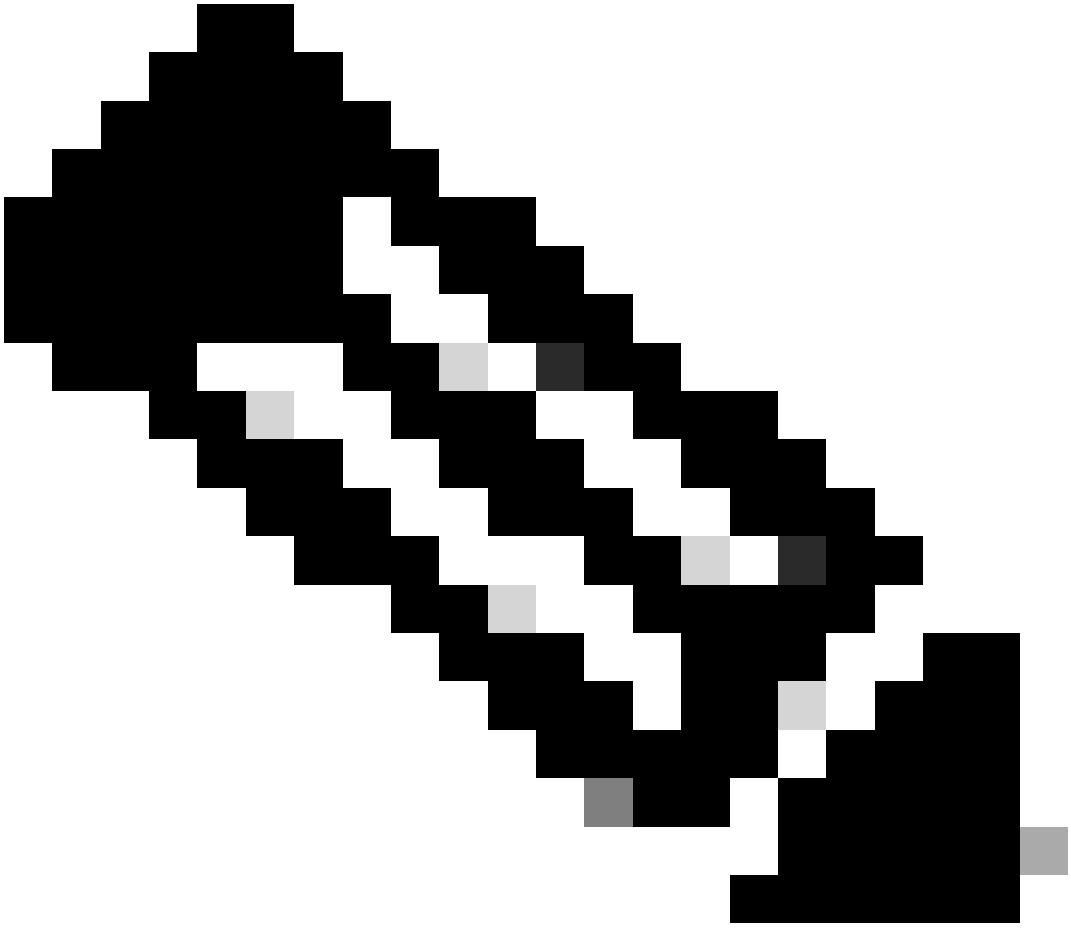


附註：您需要為站點配置無線LAN控制器，以使SSID顯示在無線SSID下

選擇SSID池，或者關聯Security Group Tag，然後按一下Deploy。僅當分配了池時，接入點才會廣播SSID。



在AireOS和Catalyst 9800控制器上，在網路設定中的任何SSID配置更改後重新調配無線LAN控制器。



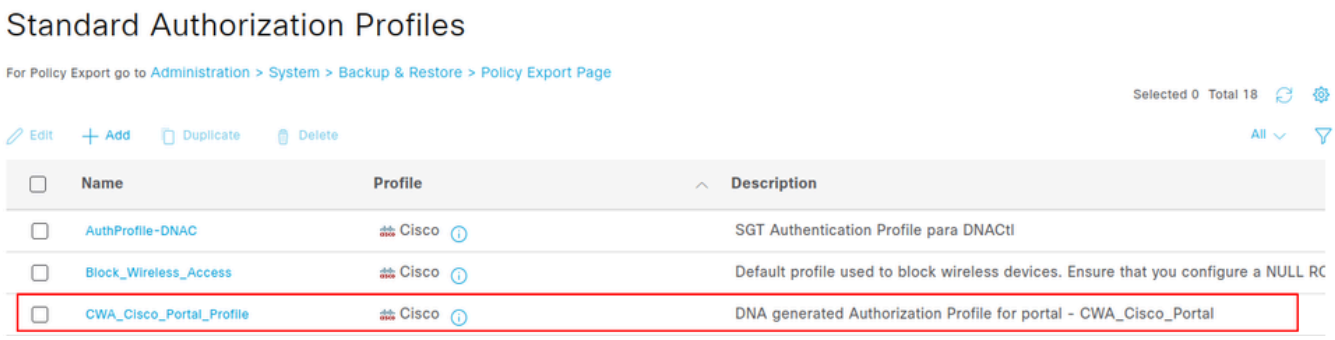
附註：如果沒有為SSID分配池，則預計AP不會廣播它。只有在分配了池之後才會廣播SSID。一旦分配池，就無需重新布建控制器。

檢視布建至Cisco ISE的組態

本節檢查Catalyst Center調配到Cisco ISE的配置。

授權配置檔案

Catalyst Center在Cisco ISE上調配的部分配置是Authorization Profile。此配置檔案根據客戶端的引數定義分配給客戶端的結果，可包括特定設定，例如VLAN分配、ACL或URL重定向。
要在ISE中檢視授權配置檔案，請導航到Policy > Policy Elements > Results。如果門戶名稱為CWA_Cisco_Portal，則配置檔名稱為CWA_Cisco_Portal_Profile。說明欄位顯示文本：DNA為門戶生成授權配置檔案 — CWA_Cisco_Portal。



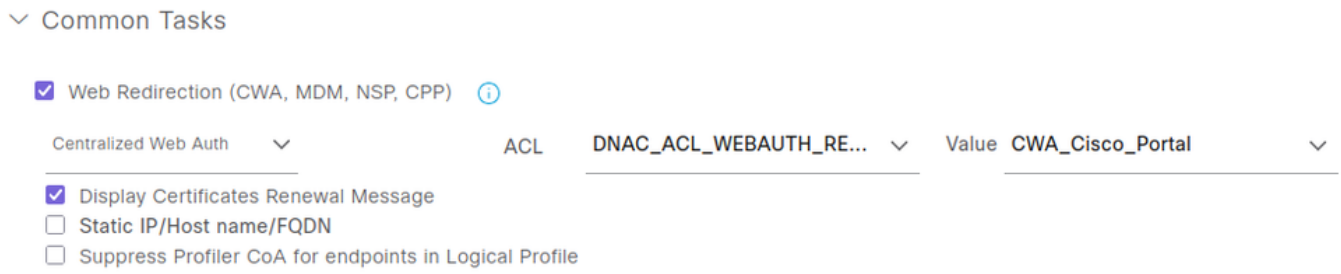
要檢視通過此授權配置檔案傳送到無線LAN控制器的屬性，請按一下授權配置檔名稱，並參閱常見任務部分。
此授權設定檔提供重新導向ACL和重新導向URL。

Web重定向屬性包括兩個引數：

1. ACL名稱：設定為Cisco DNA_ACL_WEBAUTH_REDIRECT。
2. 值：是指強制網路門戶的名稱，在本例中為CWA_Cisco_Portal。

Display Certificates Renewal Message選項使門戶可用於續訂終端當前使用的證書。

Display Certificates Renewal下提供了另一個選項Static IP/Host Name/FQDN。此功能允許傳遞門戶的IP地址而不是FQDN，當強制網路門戶因無法訪問DNS伺服器而無法載入時，此功能非常有用。

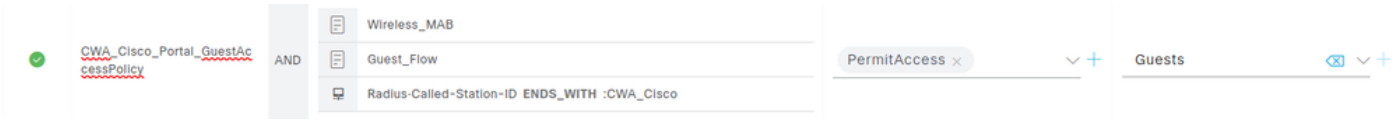


策略集

導航到Policy > Policy Sets > Default > Authorization Policy，以檢視為名為CWA_Cisco_Portal的門戶建立的兩個策略集。這些策略集包括：

- CWA_Cisco_Portal_GuestAccessPolicy
- CWA_Cisco_Portal_RedirectPolicy

當客戶端已通過自行註冊或通過熱點門戶完成Web身份驗證過程時，將應用CWA_Cisco_Portal_GuestAccessPolicy。

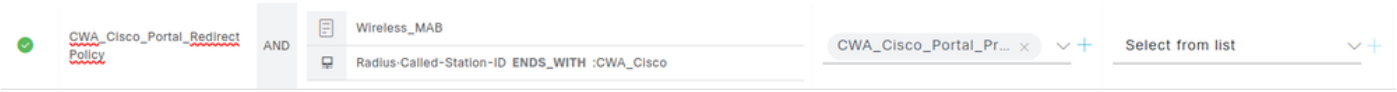


此策略集符合三個條件：

- Wireless_MAB：在Cisco ISE收到來自無線LAN控制器的MAC身份驗證繞行(MAB)身份驗證請求時使用。
- Guest_Flow:是指根據GuestEndpoints身份組檢查終端的MAC地址的ISE。如果此組中沒有終端MAC地址，則不應用策略。
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco:Called-Station-ID是ISE中的RADIUS屬性，以ASCII格式儲存網橋或接入點MAC地址並附加正在訪問的SSID，用分號(:)分隔。 在本示例中，CWA_Cisco表示SSID名稱。

在列配置檔案下可以看到名稱PermitAccess，這是不能編輯的保留授權配置檔案，它授予對網路的完全訪問許可權，您也可以在Security Groups列下分配SGT，在本例中為Guests。

使用PermitAccess配置檔案。這是保留的授權配置檔案，無法編輯此配置檔案並授予對網路的完全訪問許可權。還可以在Security Groups列下分配SGT;在這種情況下，SGT設定為Guests。
下一個要審查的策略是CWA_Cisco_Portal_RedirectPolicy。



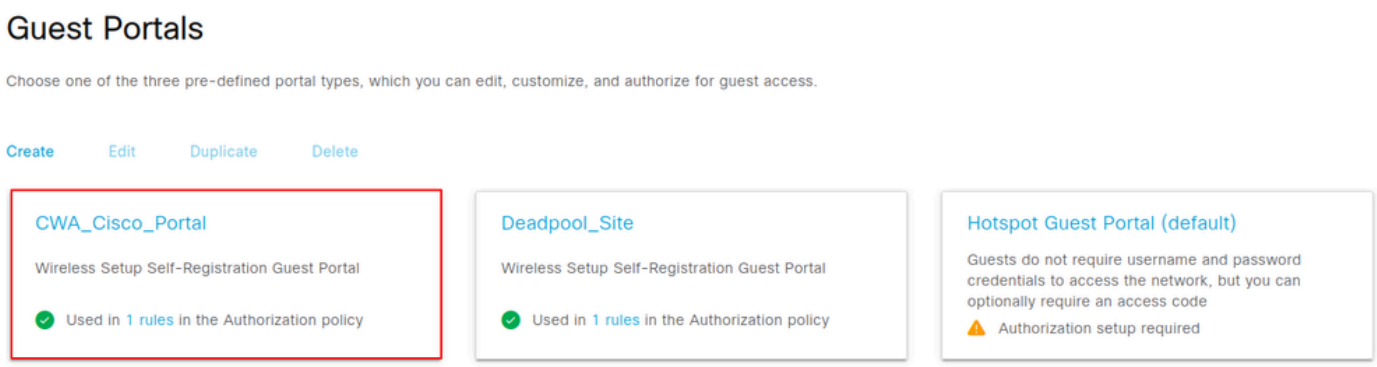
此策略集符合以下兩個條件：

- Wireless_MAB：在Cisco ISE收到來自無線LAN控制器的MAB身份驗證請求時使用。
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco:Called-Station-ID是ISE中的RADIUS屬性，以ASCII格式儲存網橋或接入點MAC地址並附加正在訪問的SSID，用分號(:)分隔。 在本示例中，:CWA_Cisco表示SSID名稱。

這些策略的順序至關重要。如果CWA_Cisco_Portal_RedirectPolicy首先出現在清單中，則它只匹配MAB身份驗證和SSID名稱，使用RADIUS屬性Called-Station-ID ENDS_WITH :CWA_Training。在此配置中，即使終端已通過門戶進行身份驗證，它仍將無限期地與此策略匹配。因此，永遠不會通過PermitAccess配置檔案授予完全訪問許可權，並且客戶端仍然停滯在身份驗證和重定向到門戶的連續循環中。

訪客門戶配置

導航到工作中心(Work Centers)>訪客訪問(Guest Access)>門戶和元件(Portals & Components)以檢視門戶。
此處建立的訪客門戶使用與Catalyst Center CWA_Cisco_Portal中相同的名稱。如果要檢視其他詳細資訊，請選擇門戶名稱。

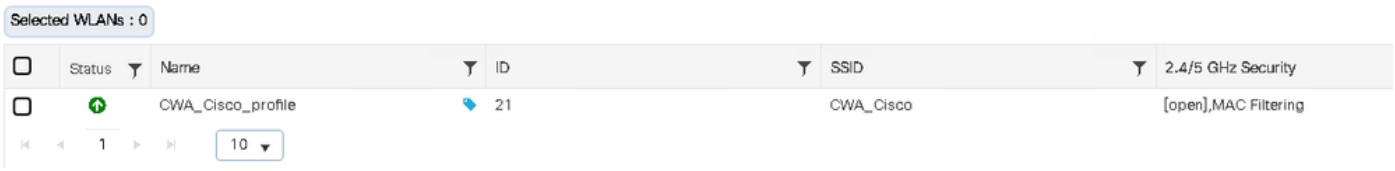


檢討布建至WLC的組態

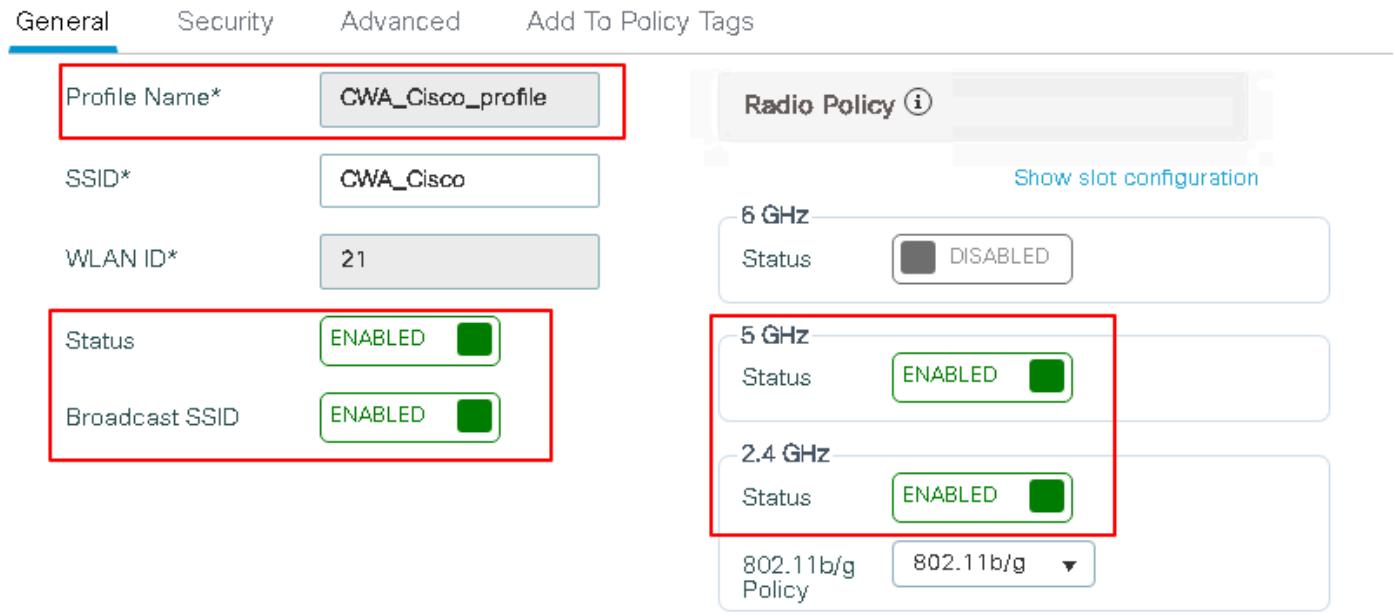
本節檢查Catalyst Center布建到無線LAN控制器的組態。

SSID配置

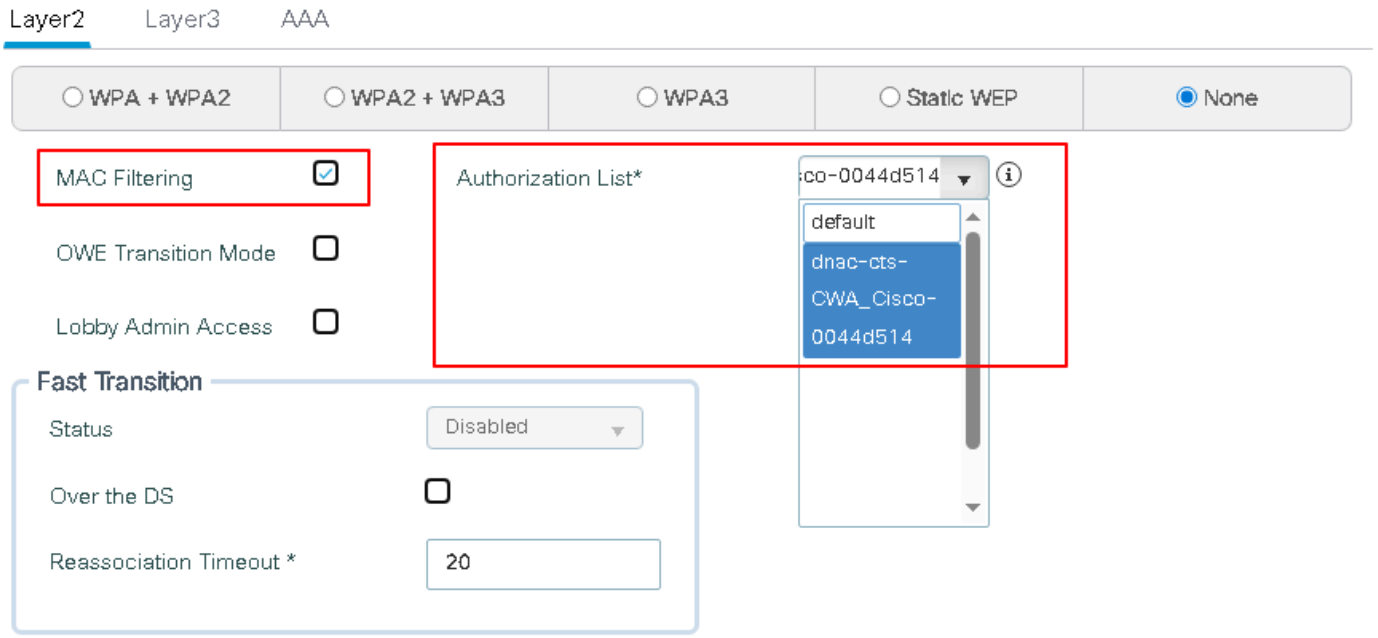
在WLC GUI中，導覽至Configuration > Tags & Profiles > WLANs以檢視SSID組態。



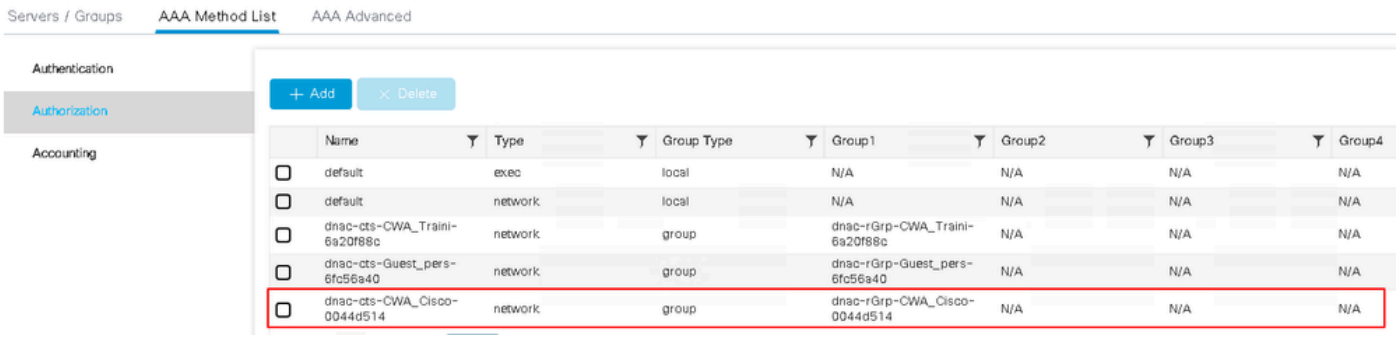
SSID CWA_Cisco在WLC上的名稱為CWA_Cisco_profile，ID為21，且使用MAC過濾的Open安全型別。按兩下SSID以檢視其配置。



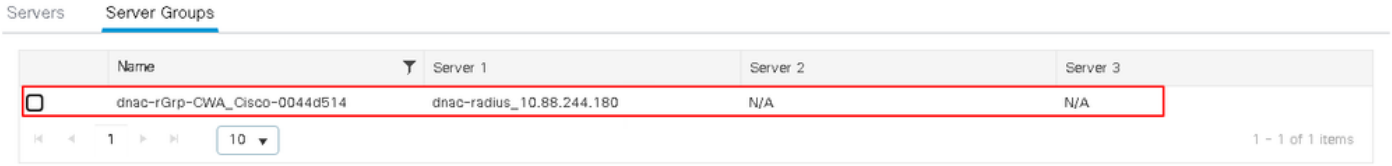
SSID為UP，在5 GHz和2.4 GHz通道上廣播，並且連線到策略配置檔案CWA_CIsco_Profile。按一下Security頁籤以檢視設定。



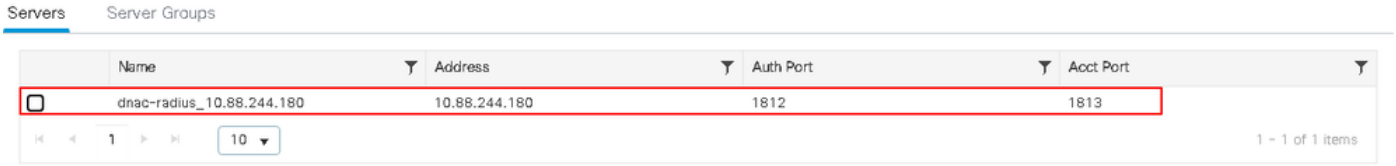
金鑰設定包括第2層安全方法（MAC過濾）和AAA授權清單(Cisco DNA-cts-CWA_Cisco-0044d514)。 要檢視其配置，請導航至Configuration > Security > AAA > AAA Method List > Authorization。



方法清單指向Group1列中的RADIUS組Cisco DNA-rGrp-CWA_Cisco-0044d514。要檢視其配置，請導航到Configuration > Security > AAA > Server/Groups > Server Groups。



伺服器組Cisco DNA-rGrp-CWA_Cisco-0044d514指向Server 1列中的Cisco DNA-radius_10.88.244.180。在Servers頁籤中檢視其配置。



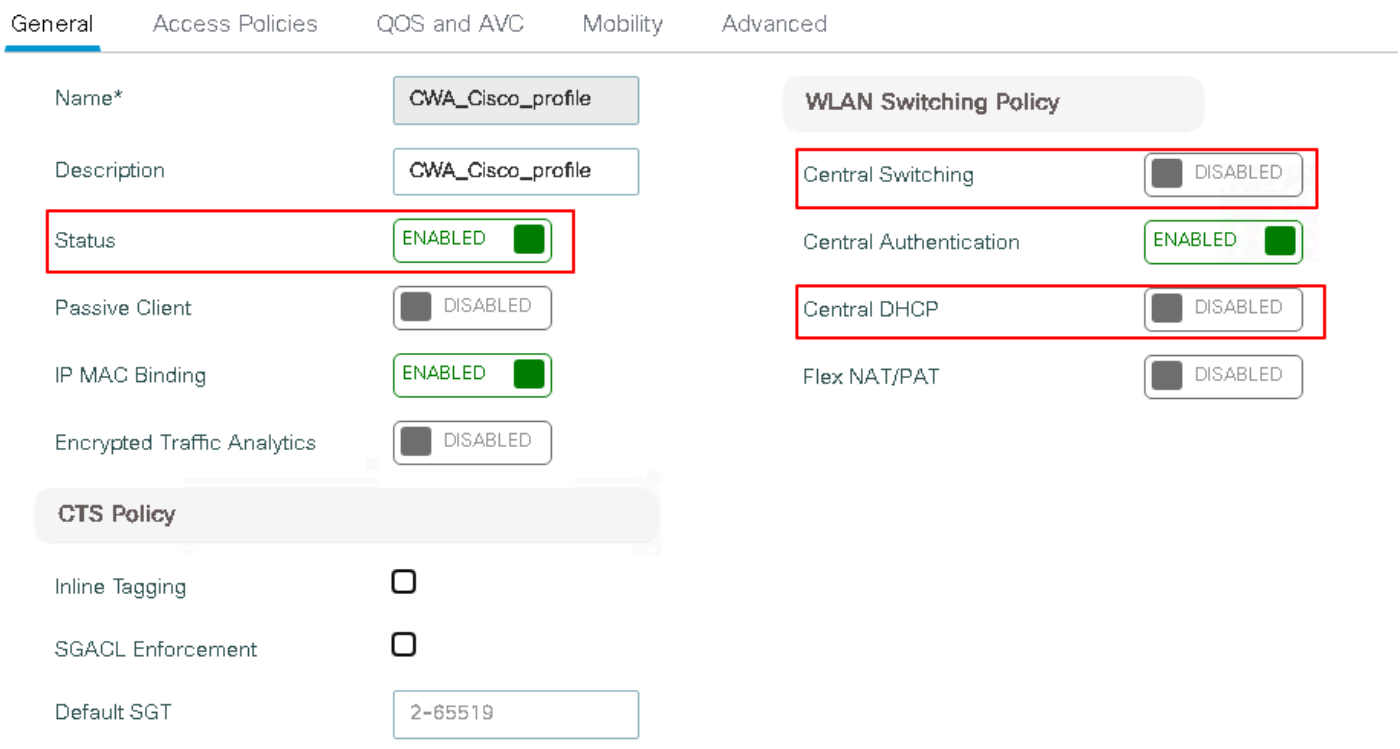
伺服器Cisco DNA-radius_10.88.244.180的IP地址為10.88.244.180，按一下其名稱檢視其配置

關鍵配置是授權變更(CoA)，它提供一種機制，用於在強制網路門戶上對身份驗證、授權和記帳(AAA)會話進行身份驗證後修改其屬性。如果沒有此功能，則終端即使完成在門戶上的註冊，仍會處於web-auth pending狀態。

無線策略配置檔案配置

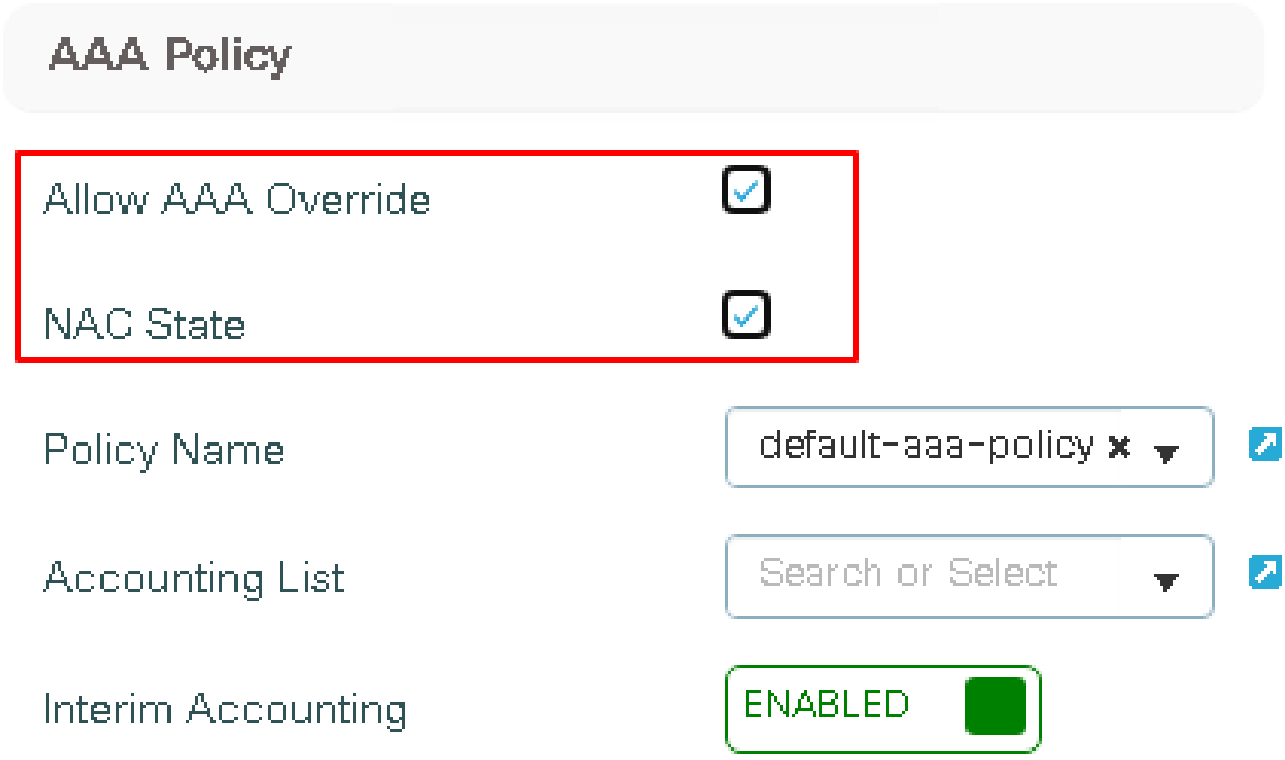
在策略配置檔案中，可以為客戶端分配設定，例如VLAN、ACL、QoS、移動錨點和計時器。要檢視策略配置檔案的配置，請導航到配置>標籤和配置檔案>策略。

按一下policy name以檢視其配置。



策略狀態為啟用，與任何交換矩陣SSID一樣，中心交換和中心DHCP被禁用。按一下高級頁籤，然

後導航到AAA策略部分以檢視其他配置詳細資訊。



可啟用AAA覆寫和網路存取控制(NAC)。AAA覆寫允許控制器接受RADIUS伺服器傳回的屬性（例如ACL或URL），並將這些屬性套用到使用者端。NAC在使用者端在入口上註冊後啟用授權變更(CoA)。
也可透過WLC上的CLI檢視此組態。
要驗證策略配置檔案，SSID已連線以運行命令：

<#root>

WLC#show fabric wlan summary

```
Number of Fabric wlan : 1

WLAN  Profile Name       SSID       Status
------------------------------------------------------------------------------
21
```

CWA_Cisco_profile

```
  CWA_Cisco  UP
```

要檢視策略配置檔案CWA_Cisco_profile的配置，請運行命令：

<#root>

WLC#show running-config | section policy CWA_Cisco_profile

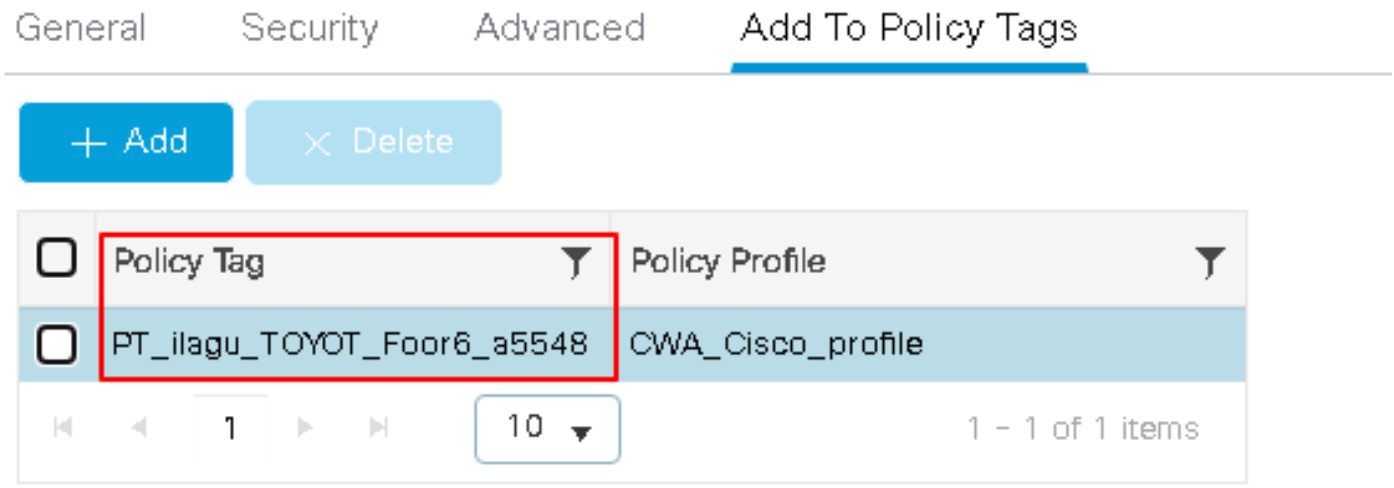
```
wireless profile policy CWA_Cisco_profile
```

aaa-override

```
no central dhcp


no central switching


description CWA_Cisco_profile
dhcp-tlv-caching
exclusionlist timeout 180
fabric CWA_Cisco_profile
http-tlv-caching

nac


service-policy input platinum-up
service-policy output platinum
no shutdown
```

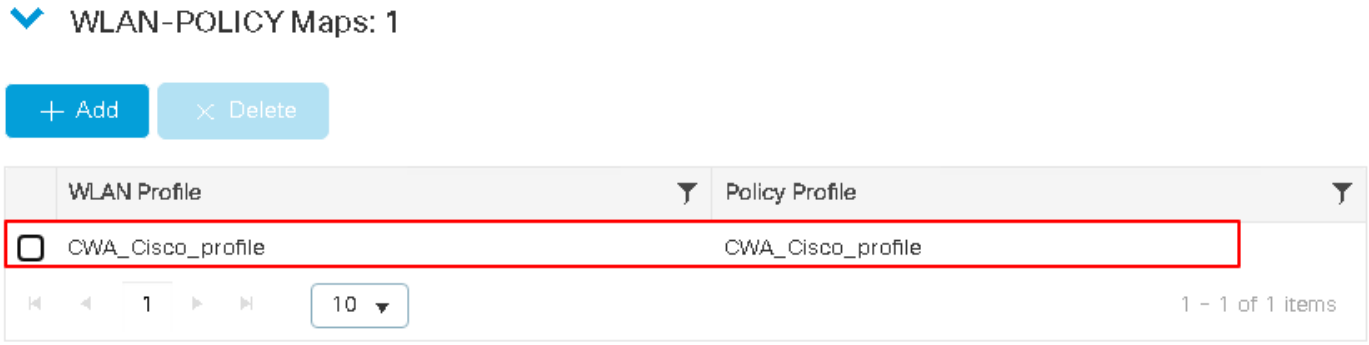
原則標籤組態

策略標籤是將WLAN與策略配置檔案連結的方式，導航到Configuration > Tags & Profiles > WLANs，按一下WLAN name，然後導航到Add to Policy Tags以識別分配給SSID的策略標籤。



對於SSID CWA_Cisco_profile，策略標籤PT_ilagu_TOYOT_Foor6_a5548用於驗證此配置，導航到Configuration > Tags & Profiles > Tags > Policy。

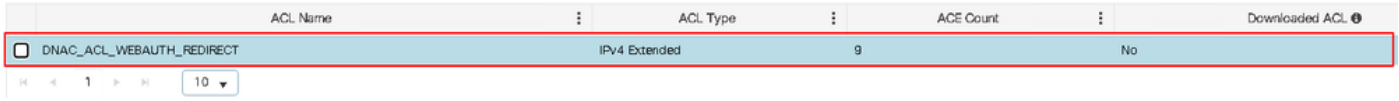
按一下name可檢視其詳細資訊。策略標籤PT_ilagu_TOYOT_Foor6_a5548將與WLC上的名稱CWA_Cisco_profile關聯的WLAN CWA_Cisco連結到策略配置檔案CWA_Cisco_profile（請參閱WLANs頁面以獲得參考）。



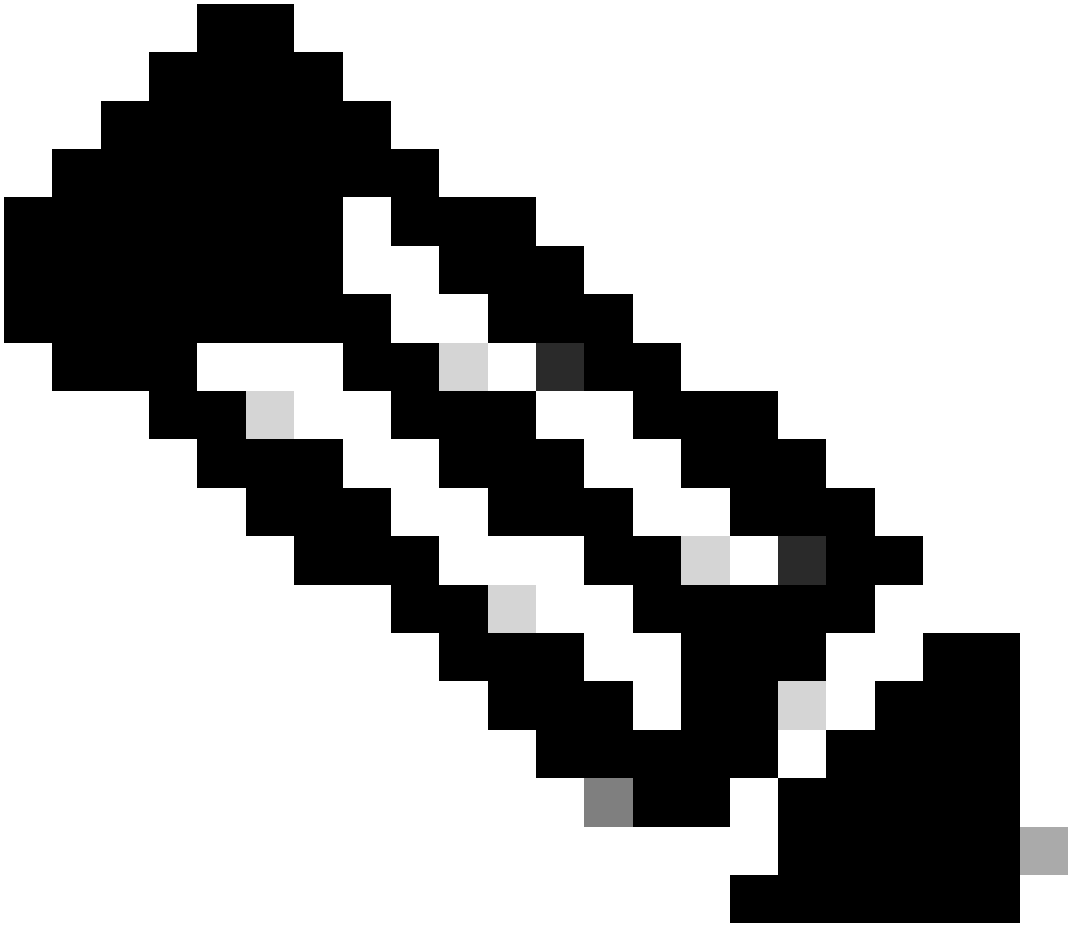
WLAN名稱CWA_Cisco_profile引用WLAN CWA_Cisco。

重新導向 ACL 組態

在CWA中，重新導向存取控制清單定義將哪些流量重新導向到WLC以進行進一步處理，以及哪些流量會繞過重新導向
在建立SSID並從清單調配WLC後，此配置會被推送到WLC。若要檢視，請導覽至Configuration > Security > ACL,Catalyst Center用於重新導向ACL的ACL名稱為Cisco DNA_ACL_WEBAUTH_REDIRECT。



按一下name可檢視其配置。這些值是從Catalyst Center上站點的網路設定的網路設定中派生出來的。



附註：這些值是從在Catalyst Center中配置的站點的網路設定中獲取的，而DHCP/DNS值來源於WLAN中配置的池。ISE PSN IP地址在SSID工作流程中的AAA配置中引用。

若要檢視WLC CLI上的重新導向ACL，請執行以下命令：

<#root>

```
WLC#show ip access-lists Cisco DNA_ACL_WEBAUTH_REDIRECT


Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 deny udp host 8.8.8.8 eq bootps any eq bootpc
2 deny udp any eq bootpc host 8.8.8.8 eq bootps
3 deny udp host 1.1.1.1 eq bootps any eq bootpc
4 deny udp any eq bootpc host 1.1.1.1 eq bootps
5 deny udp host 9.9.9.9 eq bootps any eq bootpc
6 deny udp any eq bootpc host 9.9.9.9 eq bootps
7 deny ip host 10.88.244.180 any
8 deny ip any host 10.88.244.180
9 permit tcp any range 0 65535 any eq www
```

重新導向ACL可以套用到Flex設定檔，以便將其傳送至存取點。運行此命令以確認此配置

<#root>

```
WLC#show running-config | section flex


wireless profile flex default-flex-profile

 acl-policy Cisco DNA_ACL_WEBAUTH_REDIRECT



central-webauth



urlfilter list Cisco DNA_ACL_WEBAUTH_REDIRECT
```

在存取點上重新導向ACL

在接入點上，允許值和拒絕值顛倒：permit表示轉發流量，deny表示重定向。要在AP上檢查重定向ACL的配置，請運行以下命令：

<#root>

```
AP#sh ip access-lists


Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 permit udp 8.8.8.8 0.0.0.0 dhcp_server any eq 68
2 permit udp any dhcp_client 8.8.8.8 0.0.0.0 eq 67
3 permit udp 1.1.1.1 0.0.0.0 dhcp_server any eq 68
4 permit udp any dhcp_client 1.1.1.1 0.0.0.0 eq 67
5 permit udp 9.9.9.9 0.0.0.0 dhcp_server any eq 68
6 permit udp any dhcp_client 9.9.9.9 0.0.0.0 eq 67
7 permit ip 10.88.244.180 0.0.0.0 any
8 permit ip any 10.88.244.180 0.0.0.0
9 deny tcp any range 0 65535 any eq 80
```

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）。