在使用ISE的WLC上使用FlexConnect AP配置CWA

目錄

簡介

本文說明如何使用身分識別服務引擎(ISE)在本地交換模式下在無線LAN控制器(WLC)上使用FlexConnect存取點(AP)設定中央Web驗證。

重要註意：目前此方案不支援FlexAP上的本地身份驗證。

此系列中的其他檔案

- 使用交換機和身份服務引擎進行中央Web身份驗證的配置示例
- WLC 和 ISE 的中央 Web 驗證的組態範例

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎(ISE)版本1.2.1
- 無線LAN控制器軟體版本 — 7.4.100.0

設定

在無線LAN控制器(WLC)上設定中央Web驗證的方法有多種。第一種方法是本地Web驗證，其中WLC將HTTP流量重新導向至內部或外部伺服器，以提示使用者進行驗證。然後WLC取得憑證（如果是外部伺服器，則透過HTTP GET要求傳回）並進行RADIUS驗證。在訪客使用者的情況下，需要外部伺服器(如身份服務引擎(ISE)或NAC訪客伺服器(NGS))，因為門戶提供裝置註冊和自助調配等功能。此過程包括以下步驟：

1. 使用者關聯到Web身份驗證SSID。
2. 使用者開啟其瀏覽器。
3. 輸入URL後，WLC會立即重新導向到訪客輸入網站（例如ISE或NGS）。
4. 使用者在門戶上進行身份驗證。
5. 訪客輸入網站會使用輸入的憑證重新導向回WLC。
6. WLC透過RADIUS驗證訪客使用者的身分。
7. WLC重新導向回原始URL。

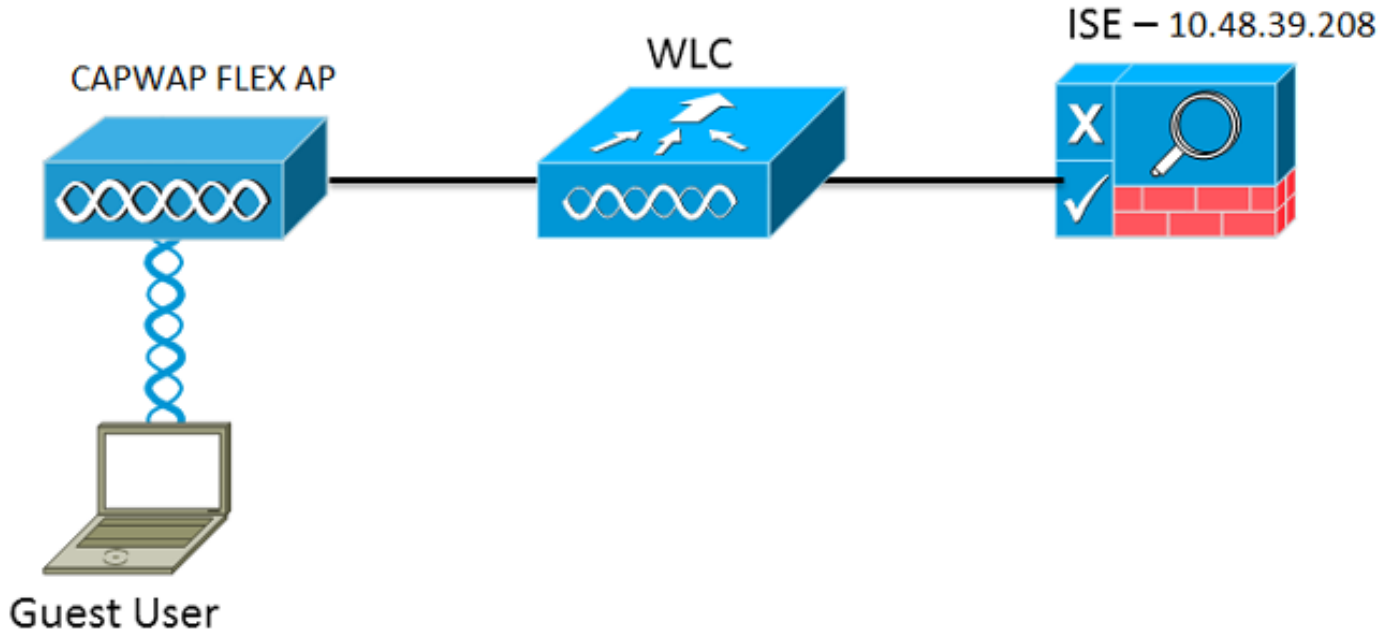
此過程包括許多重新導向。新方法是使用中央Web驗證，這與ISE（1.1版之後）和WLC（7.2版之後）配合使用。此過程包括以下步驟：

1. 使用者關聯到Web身份驗證SSID。
2. 使用者開啟其瀏覽器。
3. WLC重新導向至訪客輸入網站。
4. 使用者在門戶上進行身份驗證。
5. ISE會傳送RADIUS授權變更（CoA - UDP連線埠1700）以告知控制器使用者為有效且最終會推送RADIUS屬性，例如存取控制清單(ACL)。
6. 系統將提示使用者重試原始URL。

本節介紹在WLC和ISE上配置中央Web身份驗證的必要步驟。

網路圖表

此配置使用以下網路設定：

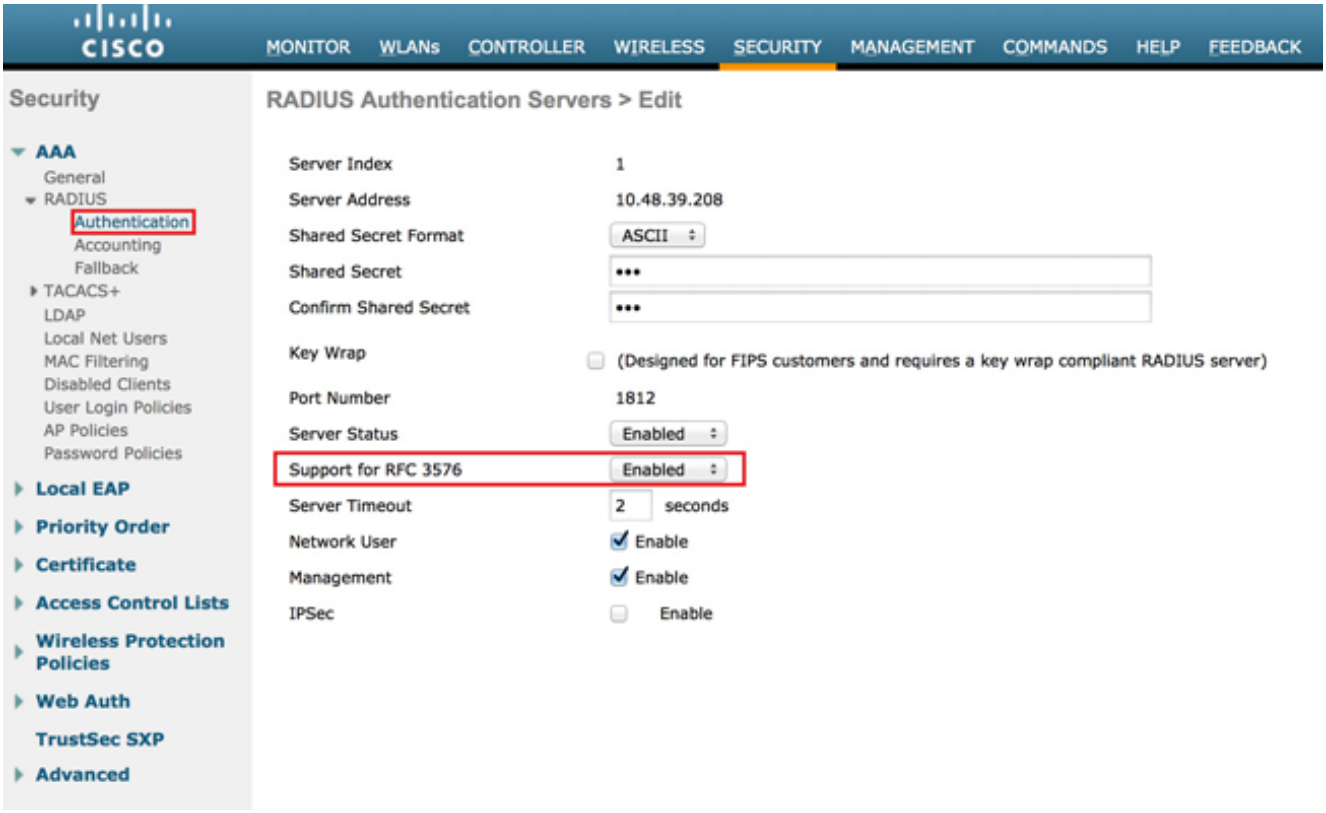


WLC組態

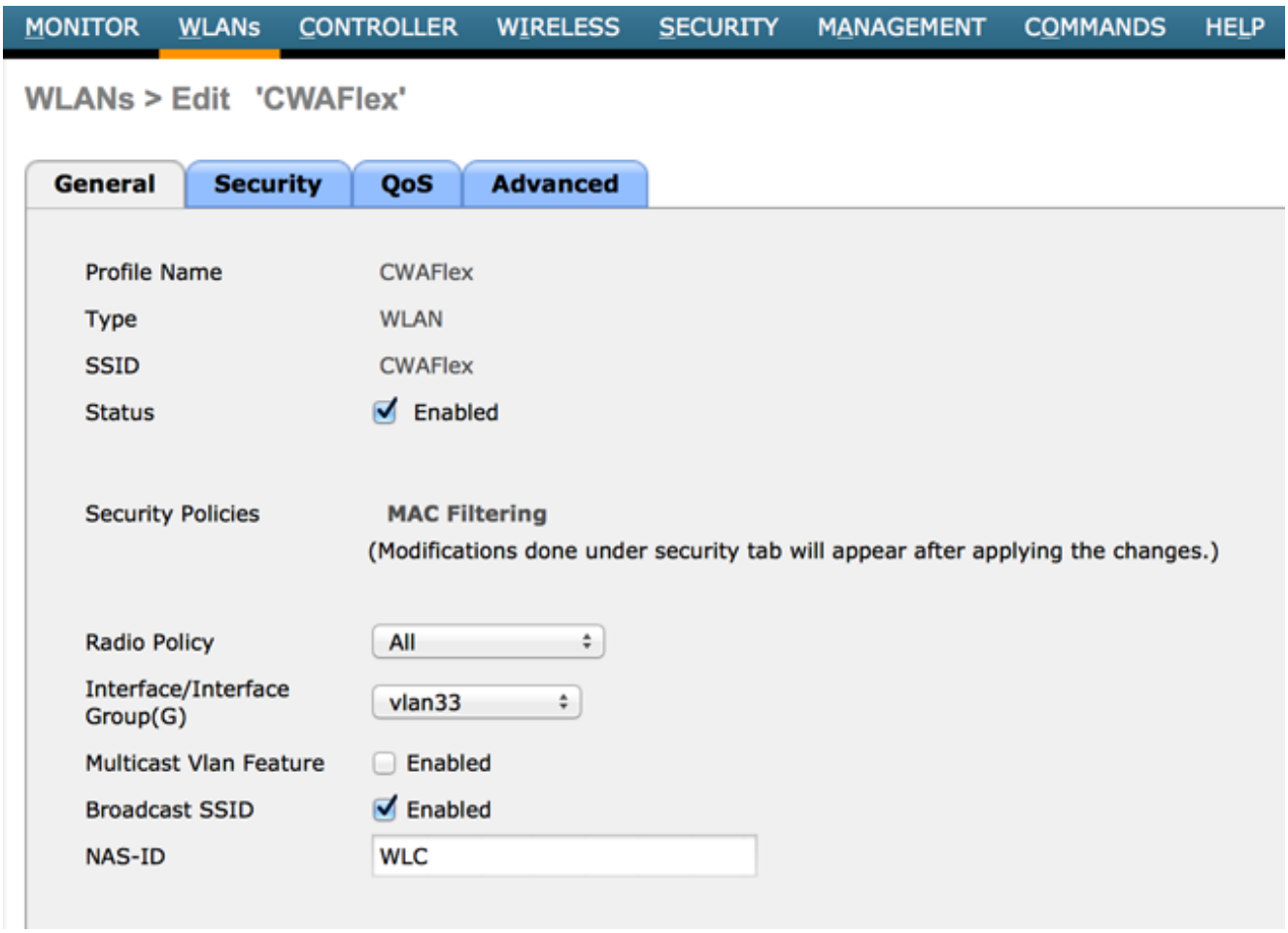
WLC的組態相當簡單。使用「技巧」（與交換機上的相同）從ISE獲取動態身份驗證URL。（由於它使用CoA，因此需要建立會話，因為會話ID是URL的一部分。）SSID配置為使用MAC過濾，而ISE配置為返回訪問接受消息，即使MAC地址未找到，也如此ISE會為所有使用者傳送重定向URL。

此外，必須啟用RADIUS網路認可控制(NAC)和AAA覆寫。RADIUS NAC允許ISE傳送CoA要求，表示使用者現已通過驗證且能夠存取網路。它還用於安全評估中，其中ISE根據安全評估結果更改使用者配置檔案。

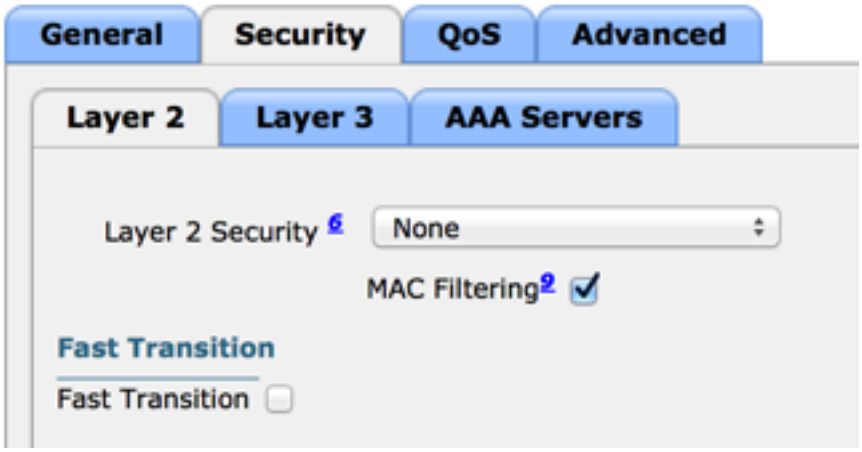
1. 確保RADIUS伺服器已啟用RFC3576(CoA)（這是預設值）。



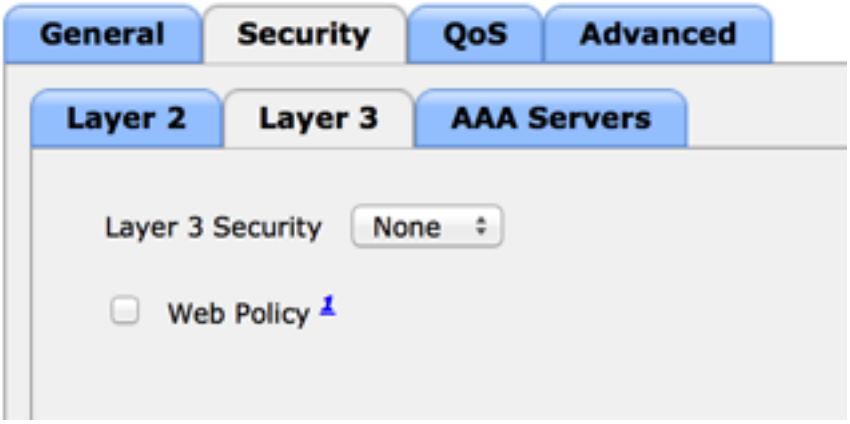
2. 建立一個新的 WLAN。此範例建立名為*CWAFlex*的新WLAN，並將其分配給vlan33。（請注意，由於存取點處於本機交換模式，因此不會有太大影響。）



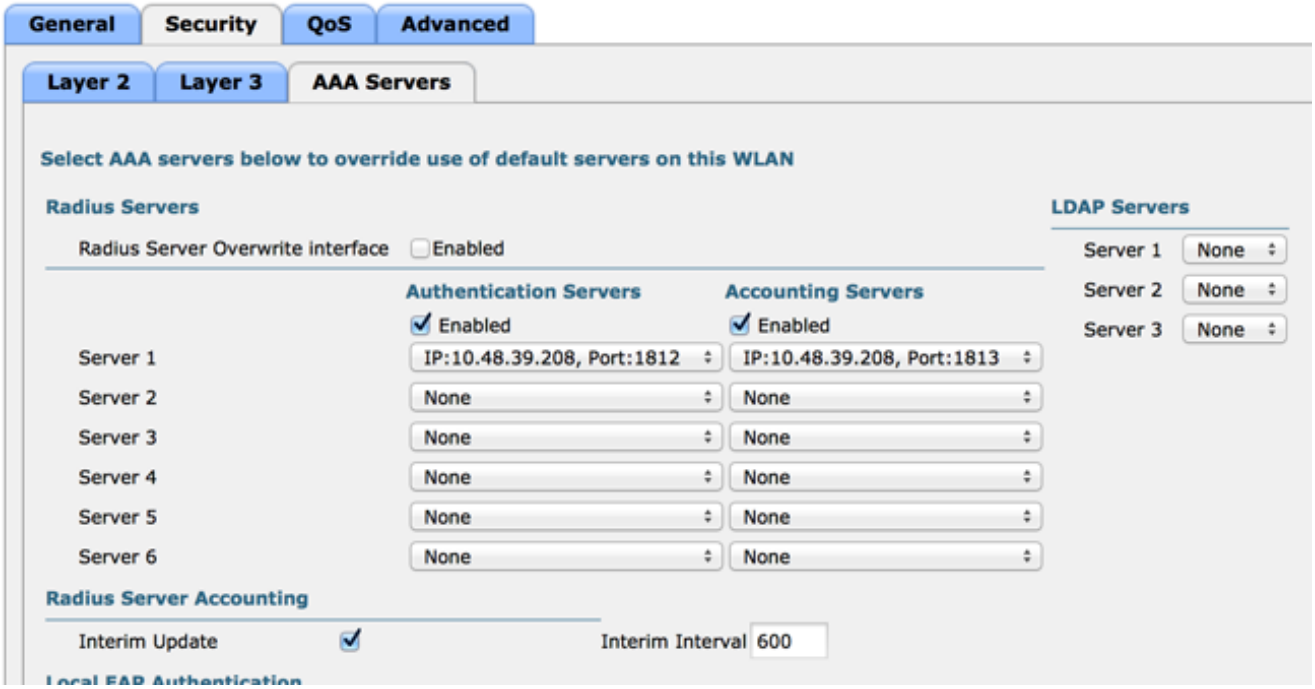
3. 在Security頁籤上，啟用MAC Filtering as Layer 2 Security。



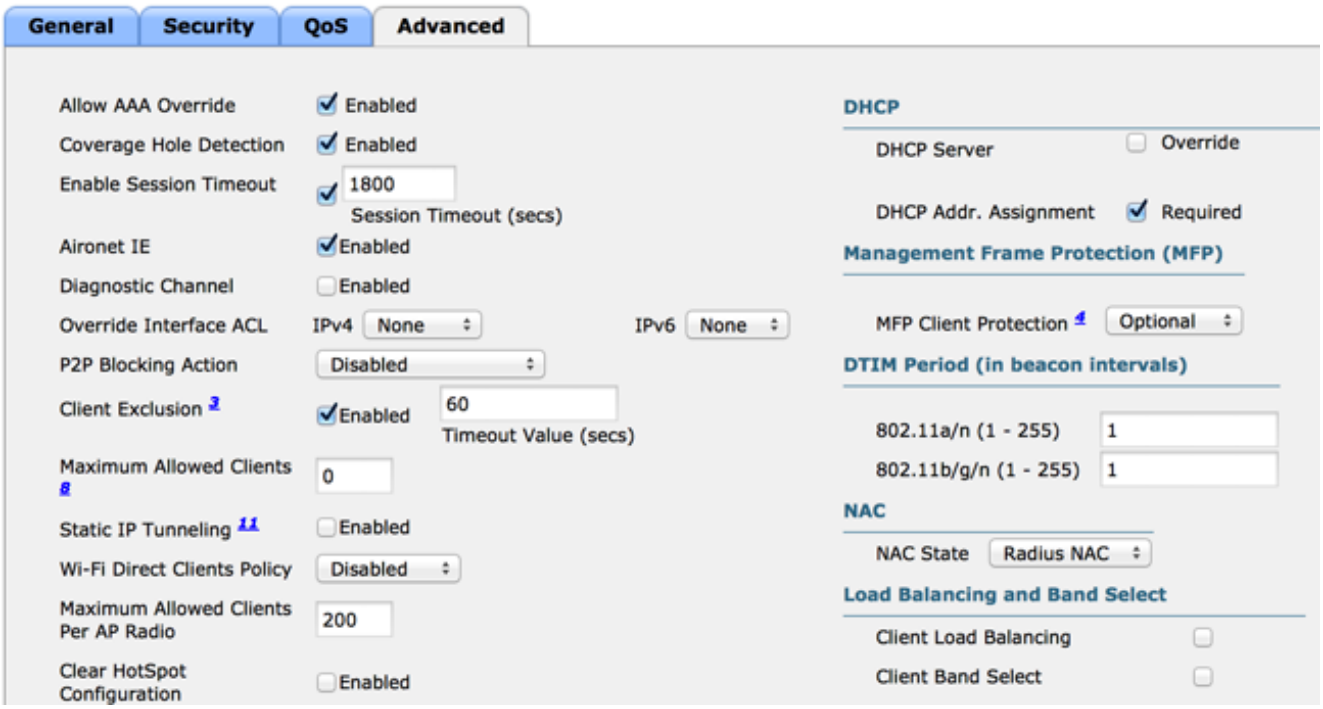
4. 在第3層頁籤上，確保已禁用安全性。（如果在第3層啟用Web驗證，則啟用本地Web驗證，而不是中央Web驗證。）



5. 在AAA Servers頁籤上，選擇ISE伺服器作為WLAN的radius伺服器。或者，您可以選擇它進行記帳，以便獲得有關ISE的更多詳細資訊。

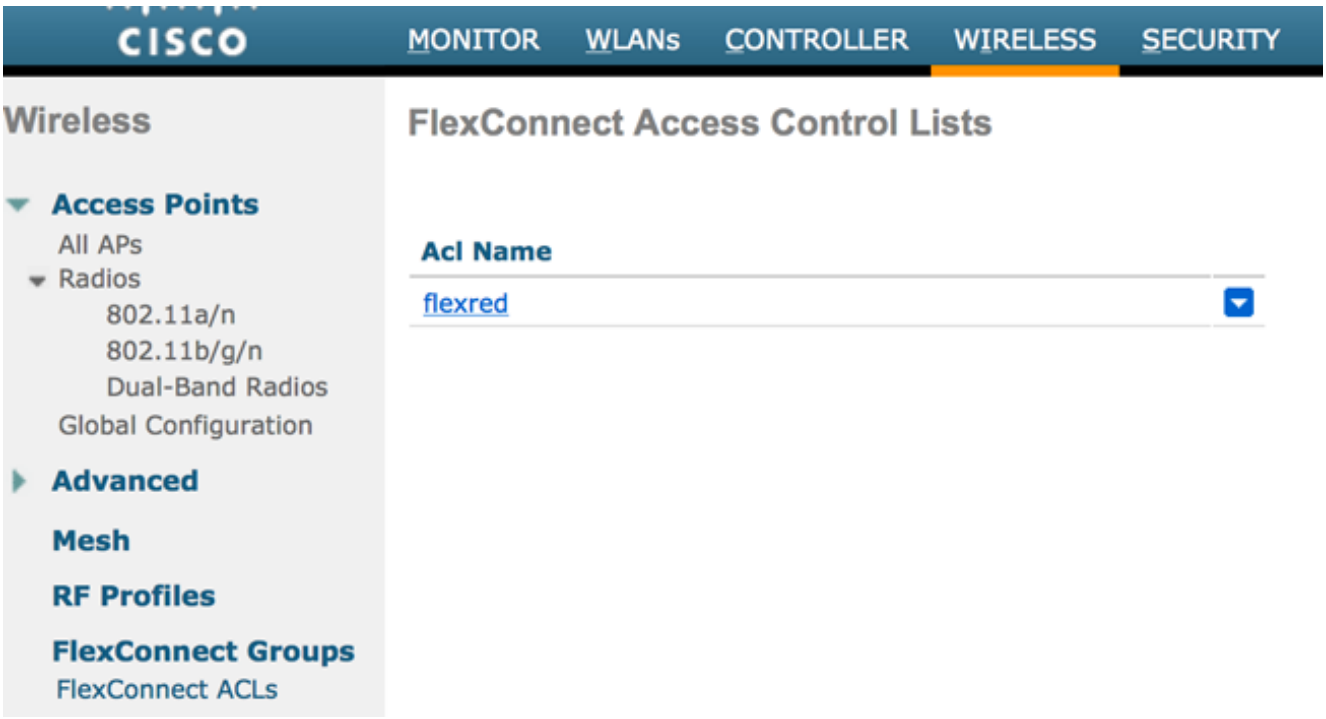


6. 在Advanced頁籤上，確保選中Allow AAA Override並為NAC狀態選擇Radius NAC。

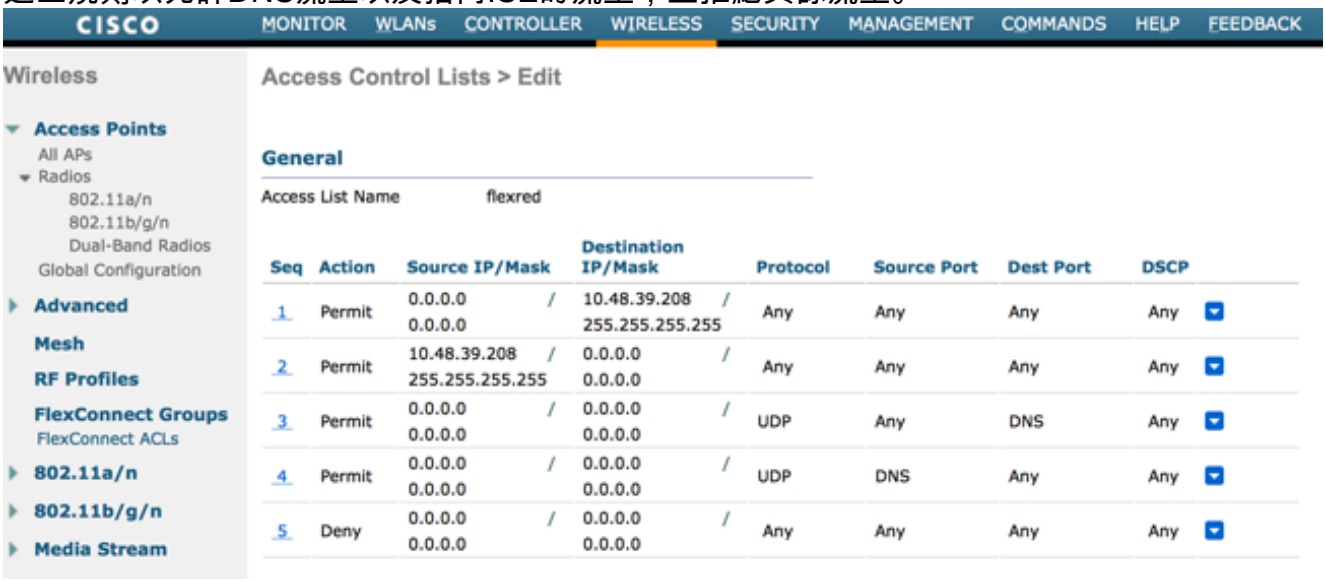


7. 建立重新導向ACL。

此ACL在ISE的Access-Accept消息中引用，並定義哪些流量應重定向（由ACL拒絕）以及哪些流量不應重定向（由ACL允許）。基本上，需要允許DNS和來自ISE的流量。 **註**:FlexConnect AP的問題是您必須建立獨立於普通ACL的FlexConnect ACL。此問題已記錄在Cisco錯誤CSCue68065中，並在7.5版中修正。在WLC 7.5及更新版本中，僅需使用FlexACL，不需要標準型ACL。WLC預期ISE返回的重定向ACL是普通ACL。但是，要確保它正常工作，您需要應用與FlexConnect ACL相同的ACL。
以下範例顯示如何建立名為flexred的*FlexConnect* ACL:

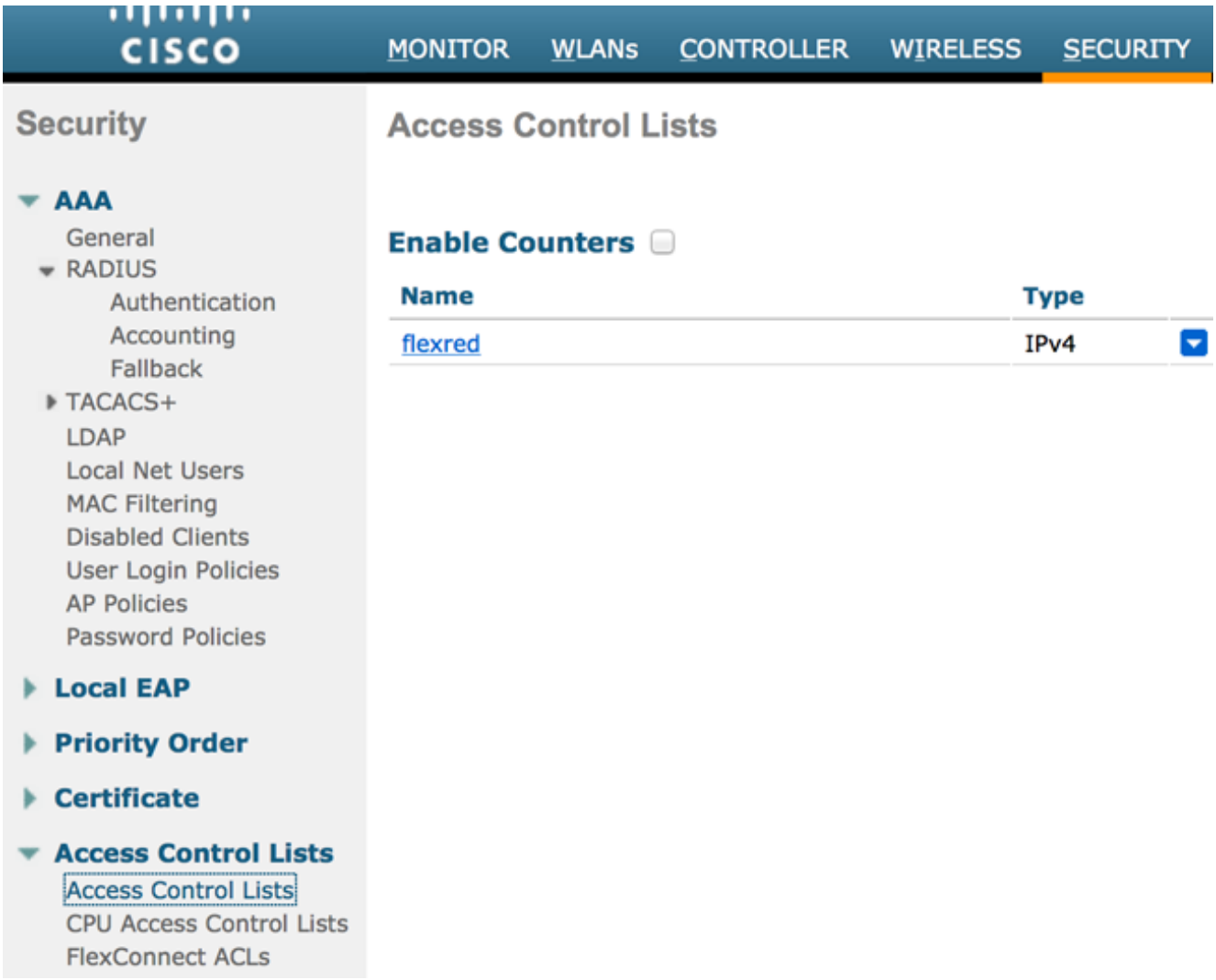


建立規則以允許DNS流量以及指向ISE的流量，並拒絕其餘流量。



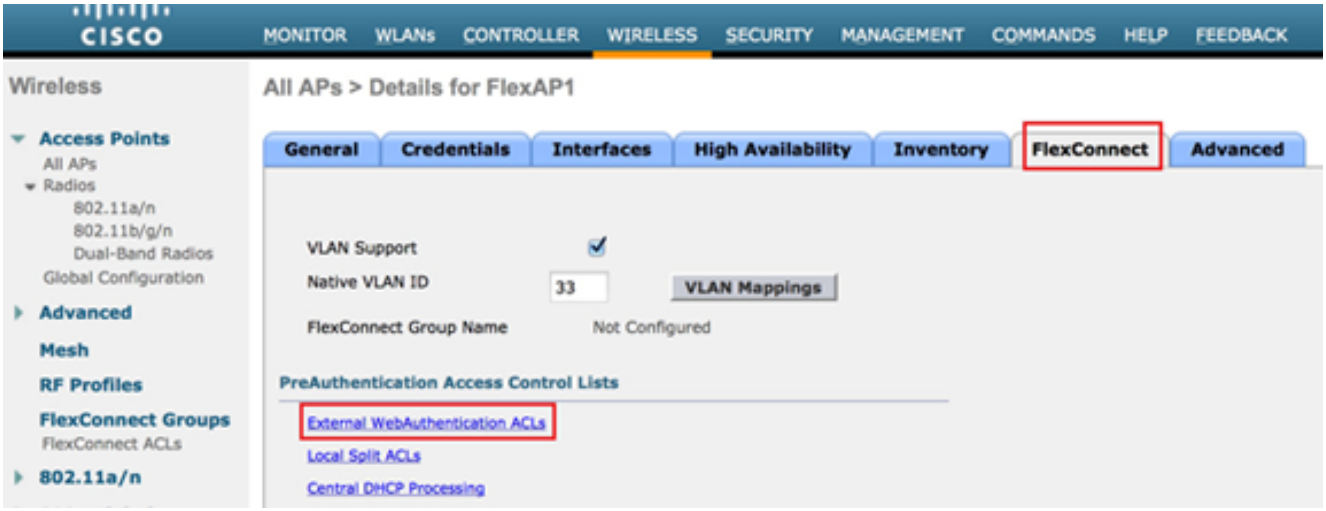
如果您希望獲得最高安全性，則只能允許埠8443指向ISE。（如果進行姿態，必須新增典型終端安全評估埠，例如8905、8906、8909、8910。）

(僅限於7.5版之前的代碼，因為CSCue68065)選擇**Security > Access Control Lists**可建立同名同一ACL。

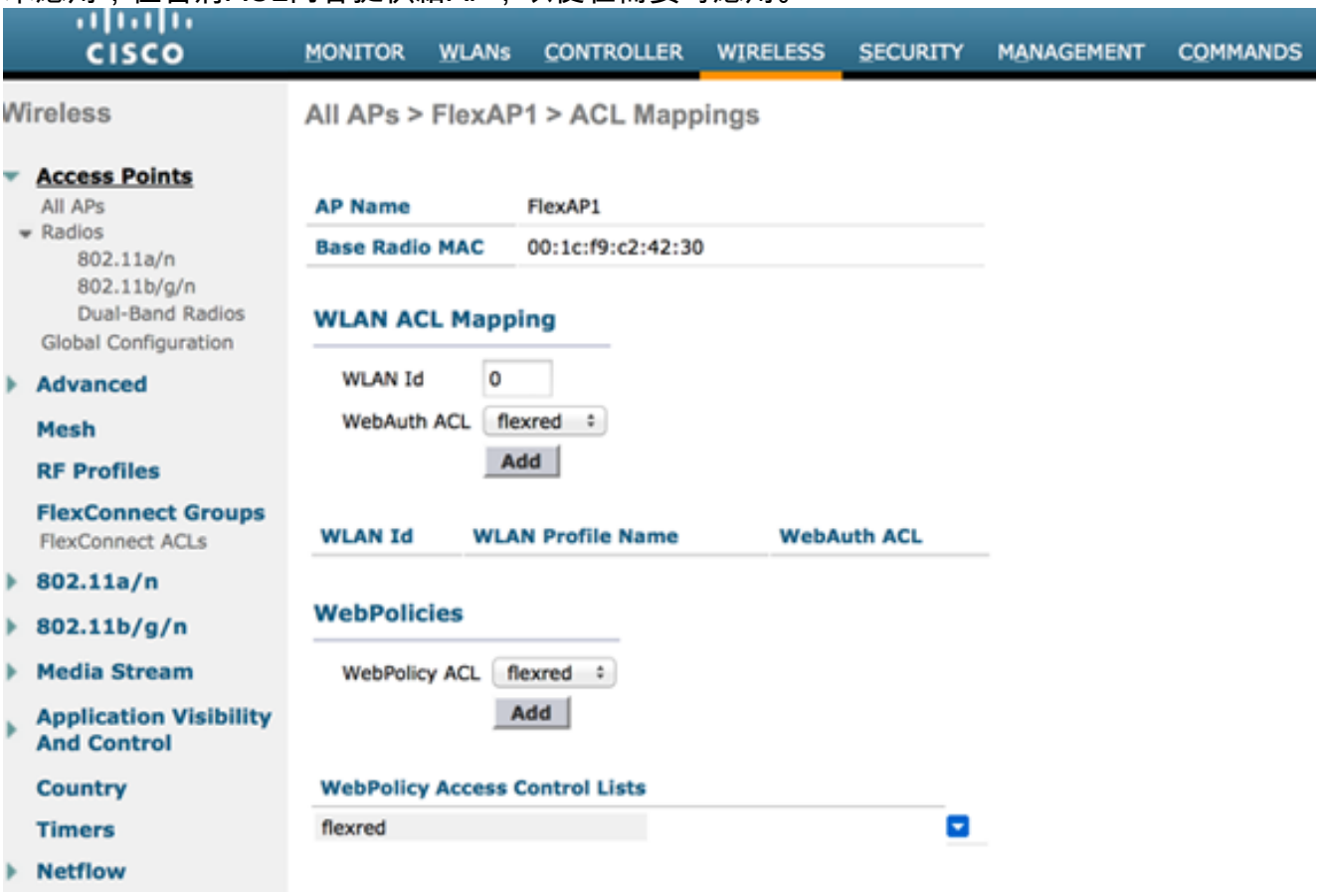


準備特定FlexConnect AP。請注意，對於大型部署，通常使用FlexConnect組，出於可擴充性原因，不會逐個AP執行這些專案。

按一下「**Wireless**」，然後選擇特定的存取點。按一下**FlexConnect**頁籤，然後按一下**External Webauthentication ACLs**。(在版本7.4之前，此選項名為*Web policies*。)



將ACL(在本示例中命名為*flexred*)新增到Web策略區域。這會將ACL預先推送到存取點。它尚未應用，但會將ACL內容提供給AP，以便在需要時應用。



WLC配置現在已完成。

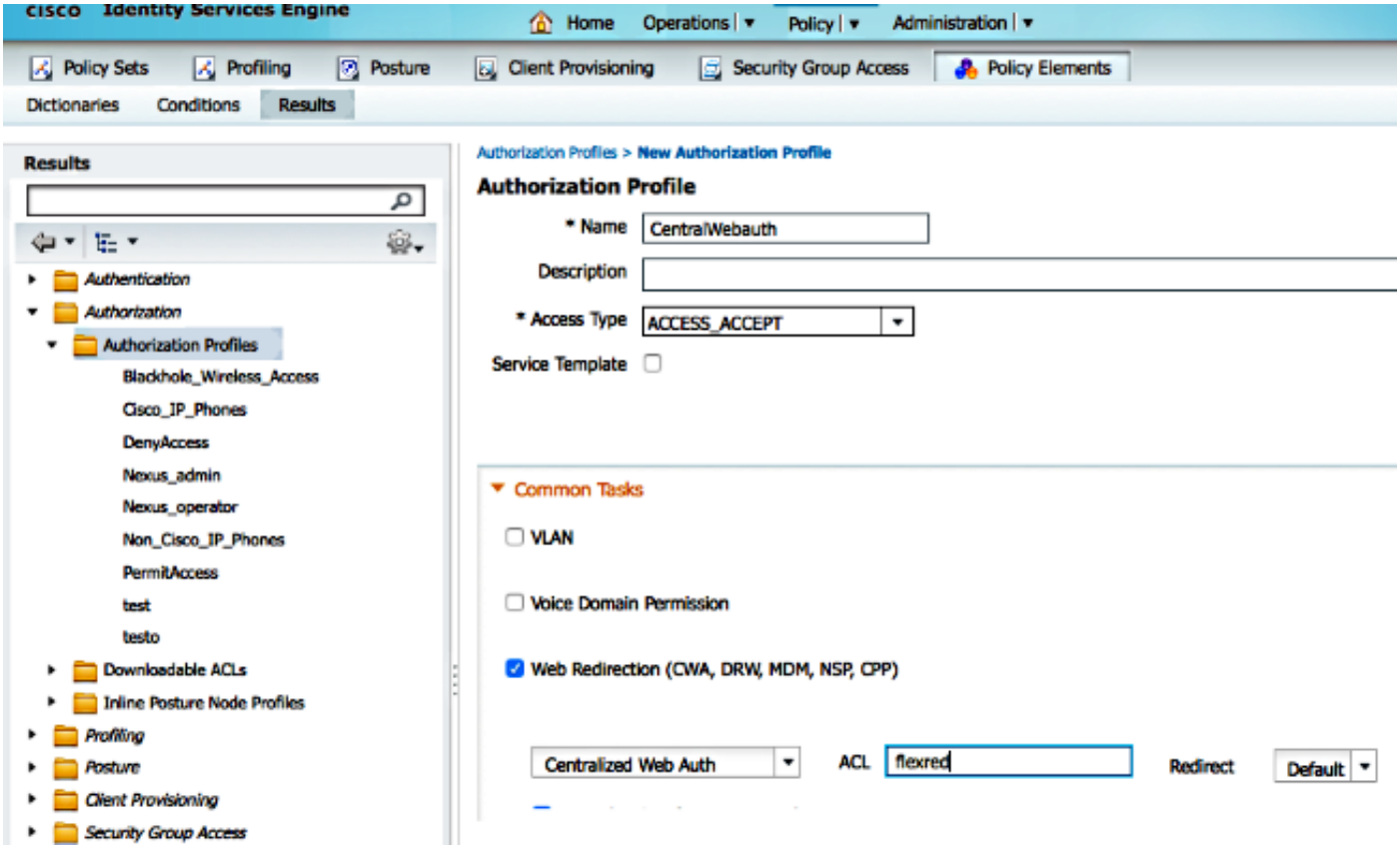
ISE 組態

建立授權配置檔案

完成以下步驟以建立授權配置檔案：

1. 按一下**Policy**，然後按一下**Policy Elements**。
2. 按一下「**Results**」。
3. 展開**Authorization**，然後按一下**Authorization profile**。
4. 按一下**Add**按鈕，為中央webauth建立一個新的授權設定檔。
5. 在「**Name**」欄位中，輸入設定檔的名稱。此範例使用*CentralWebauth*。
6. 從Access Type下拉選單中選擇**ACCESS_ACCEPT**。
7. 勾選「**Web Authentication**」覈取方塊，然後從下拉選單中選擇**集中式Web Auth**。
8. 在ACL欄位中，輸入WLC上用於定義將重新導向的流量的ACL名稱。此示例使用*flexred*。
9. 從Redirect下拉選單中選擇**Default**。

Redirect屬性定義ISE看到預設Web門戶還是ISE管理員建立的自定義Web門戶。例如，此範例中的*flexred* ACL會觸發從使用者端到任何位置的HTTP流量重新導向。

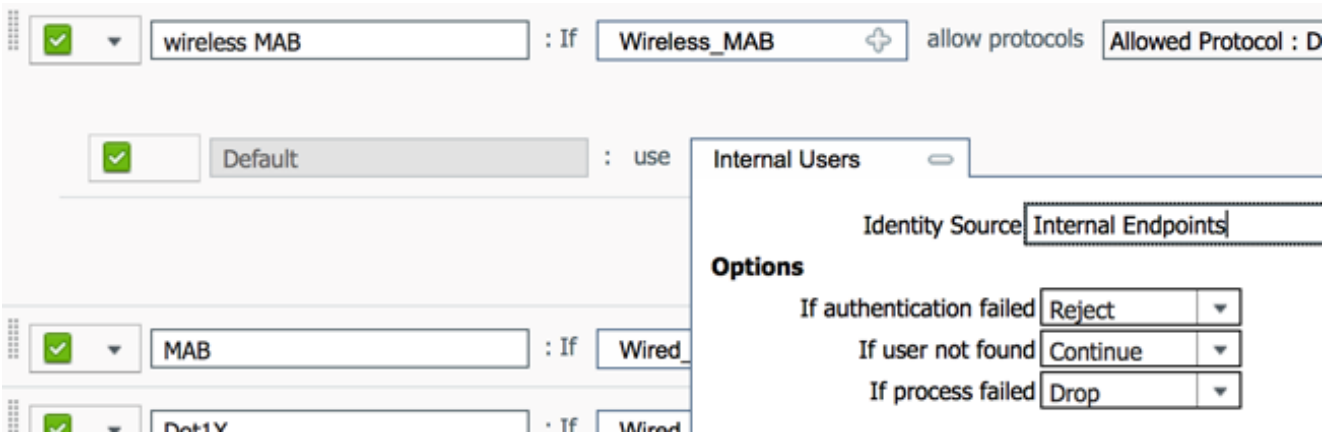


建立身份驗證規則

完成以下步驟，即可使用驗證設定檔建立驗證規則：

1. 在Policy（策略）選單下，按一下**Authentication**。 此圖顯示如何配置身份驗證策略規則的示例。在此示例中，配置了一個規則，當檢測到MAC過濾時將觸發該規則。

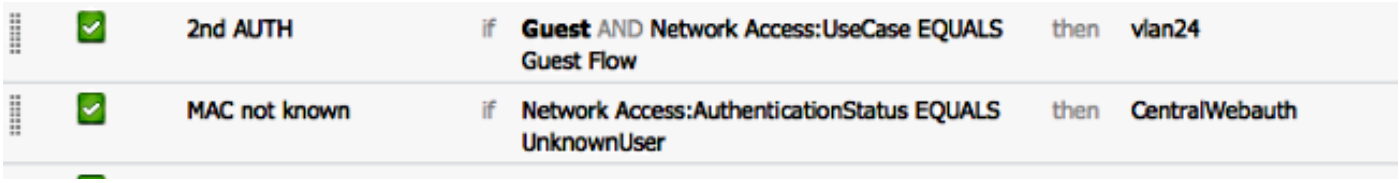
2. 輸入身份驗證規則的名稱。本示例使用*Wireless mab*。
3. 在If條件欄位**中**選擇加號(+)圖示。
4. 選擇**複合條件**，然後選擇**Wireless_MAB**。
5. 選擇「Default network access（預設網路訪問）」作為允許的協定。
6. 按一下位於**和...旁邊的箭頭**，以進一步擴展規則。
7. 按一下Identity Source欄位中的**+**圖示，然後選擇**Internal endpoints**。
8. 從If user not found下拉選單中選擇**Continue**。



此選項允許通過webauth對裝置進行身份驗證（即使裝置的MAC地址未知）。Dot1x使用者端仍可以使用其憑證進行驗證，因此不應關注此組態。

建立授權規則

現在，在授權策略中有幾個規則需要配置。連線PC後，會進行mac過濾；假設MAC地址未知，因此會返回webauth和ACL。此*MAC未知*規則如下圖所示，並在本節中配置。



完成以下步驟以建立授權規則：

1. 建立新規則並輸入名稱。此示例使用*未知的MAC*。
2. 按一下條件欄位**中的**加號(+)圖示，並選擇建立新條件。
3. 展開**expression**下拉選單。
4. 選擇**Network access**，然後展開它。
5. 按一下**AuthenticationStatus**，然後選擇**Equals**運算子。

6. 在右側欄位中選擇**UnknownUser**。
7. 在General Authorization頁面上，選擇Authorization Profile(Authorization Profile)(位於單詞右側)。即使使用者（或MAC）未知，此步驟也允許ISE繼續。現在，登入頁面將顯示未知使用者。但是，一旦他們輸入其憑證，他們就會再次在ISE上顯示身份驗證請求；因此，必須為另一規則配置一個條件，如果該使用者是訪客使用者，則此條件必須滿足。在本示例中，如果使用*UseridentityGroup equals Guest*，則假定所有來賓均屬於此組。
8. 按一下位於MAC未知規則末尾的*操作按*鈕，然後選擇在上方插入新規則。**注意：**此新規則位於MAC未知規則之前，這一*點非常*重要。
9. 在名稱欄位中輸入**2nd AUTH**。
10. 選擇身份組作為條件。此示例選擇**Guest**。

11. 在條件欄位中，按一下加號**(+)**圖示，然後選擇建立新條件。

12. 選擇**Network Access**，然後按一下**UseCase**。

13. 選擇**Equals**作為運算子。

14. 選擇**GuestFlow**作為正確的運算元。這意味著您將捕獲剛剛登入該網頁的使用者，並在授權更改（規則的訪客流部分）後再次登入，並且僅當這些使用者屬於訪客身份組時。

15. 在授權頁面上，點選加號(+)圖示(位於*then*旁邊)，為您的規則選擇結果。

    在本範例中，已指派一個預先設定的設定檔(vlan34)；本檔案沒有顯示此組態。

    您可以選擇**Permit Access**選項或建立自定義配置檔案，以返回您喜歡的VLAN或屬性。

重要註意：在ISE版本1.3中，根據Web身份驗證的型別，「訪客流」使用案例可能不再出現。然後，授權規則必須包含訪客使用者組作為唯一可能的條件。

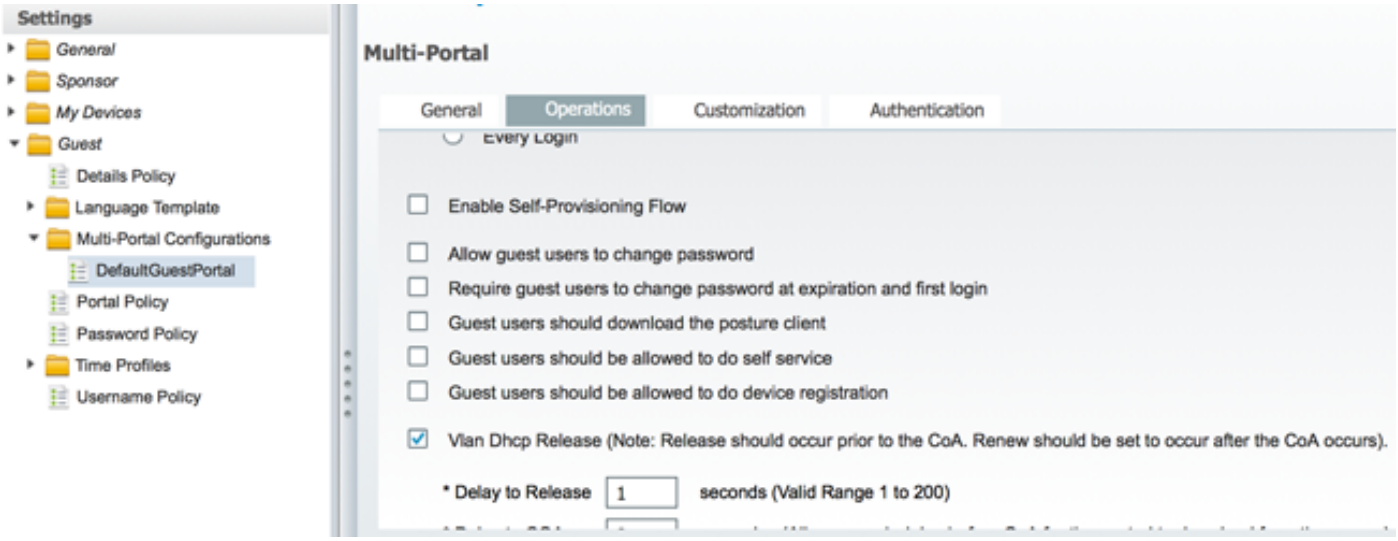
啟用IP續訂（可選）

如果分配VLAN，最後一步是客戶端PC更新其IP地址。此步驟由Windows客戶端的訪客門戶實現。如果您之前沒有為第2個AUTH*規則設*置VLAN，則可以跳過此步驟。

請注意，在FlexConnect存取點上，VLAN需要預先存在於AP上。因此，如果沒有，則您可以在AP本身或靈活組上建立VLAN-ACL對映，其中您不需要為要建立的新VLAN應用任何ACL。實際上會建立VLAN（不含ACL）。

如果您分配了VLAN，請完成以下步驟以啟用IP續訂：

1. 按一下**Administration**，然後按一下**Guest Management**。
2. 按一下「**Settings**」。
3. 展開**Guest**，然後展開**Multi-Portal Configuration**。
4. 按一下**DefaultGuestPortal**或您可能已建立的自定義門戶的名稱。
5. 按一下**Vlan DHCP Release**覈取方塊。**注意：**此選項僅適用於Windows客戶端。



流量

在此案例中，可能很難理解將哪些流量傳送到何處。以下是快速回顧：

- 客戶端通過無線方式傳送SSID的關聯請求。
- WLC使用ISE處理MAC過濾身份驗證（它接收重定向屬性）。
- 客戶端只在MAC過濾完成後收到關聯響應。
- 客戶端提交DHCP請求，即 **本地** 由接入點交換，以獲得遠端站點的IP地址。
- 在Central_webauth狀態下，重新導向ACL（因此通常是HTTP）上標籤為deny的流量會顯示 **集中** 交換.因此，進行重新導向的並非存取點，而是使用者連線埠WLC；例如，當使用者端要求建立任何網站時，AP會將此網站傳送至封裝在CAPWAP中的WLC，而WLC會偽裝該網站的IP位址，並將重新導向至ISE。
- 客戶端被重定向到ISE重定向URL。這是 **本地** 再次交換（因為它在flex重新導向ACL上命中permit）。
- 一旦進入RUN狀態，流量就會在本地進行交換。

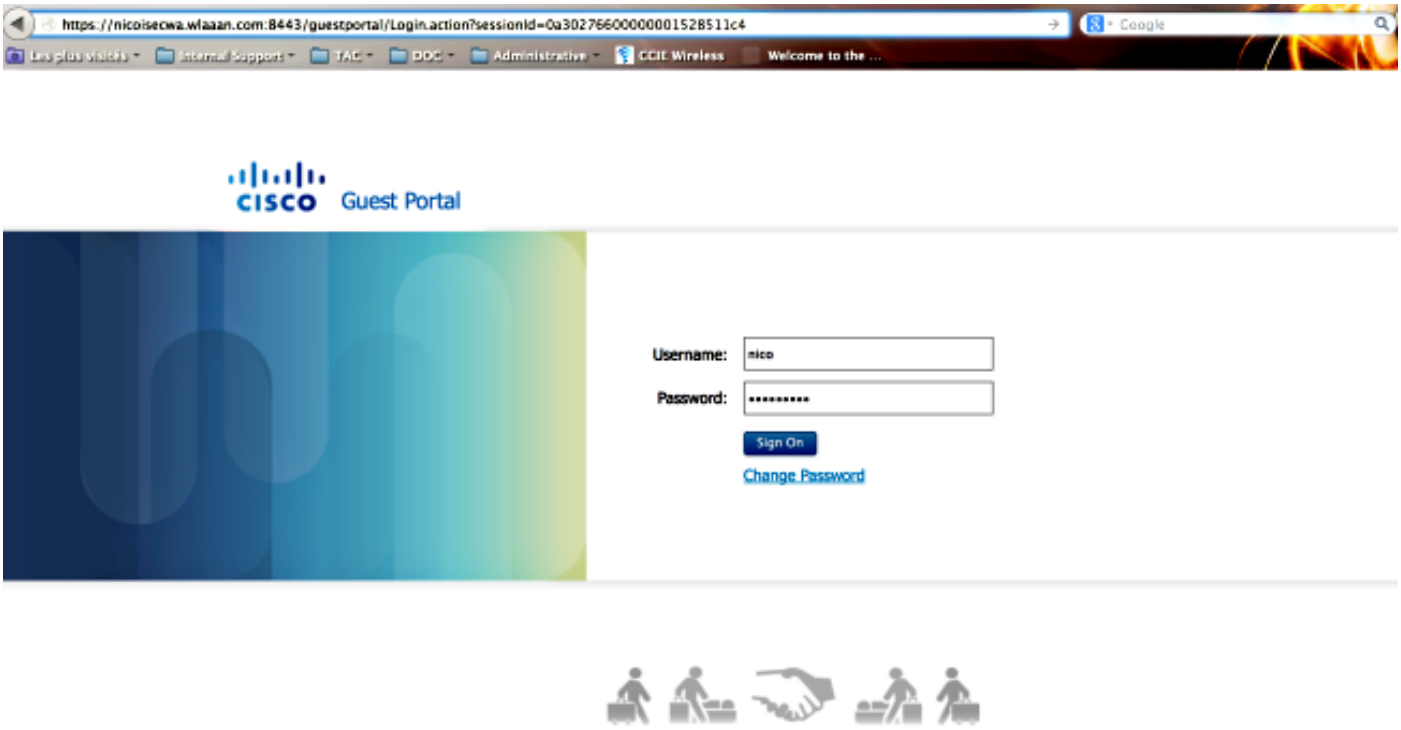
驗證

使用者與SSID關聯後，授權將顯示在ISE頁面中。

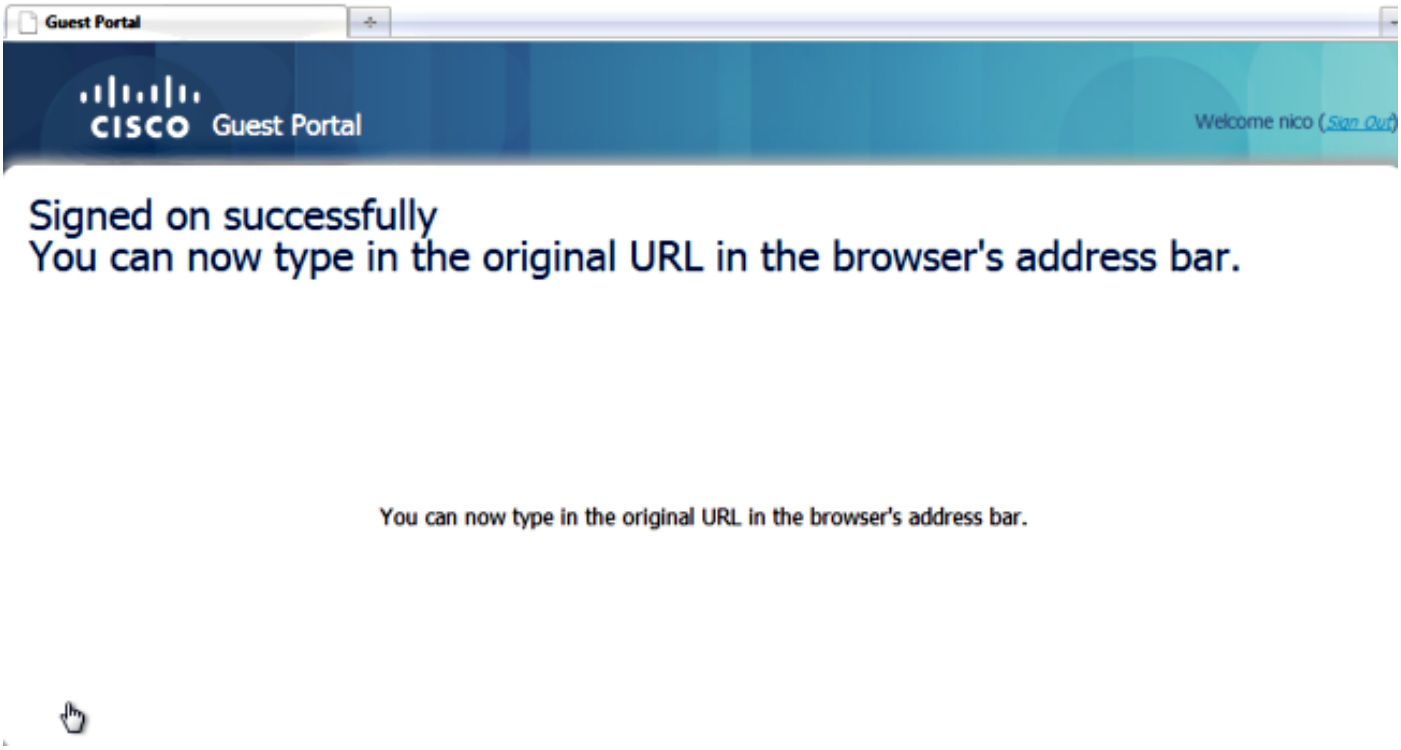
Apr 09,13 11:49:27.179 AM	✓		Nico	00:13:10:21:70:13	nicowlc	vlan34	Guest	NotApplicable	
Apr 09,13 11:49:27.174 AM	✓				nicowlc				Dynamic Author...
Apr 09,13 11:48:58.372 AM	✓		Nico	00:13:10:21:70:13			Guest		Guest Authentic..
Apr 09,13 11:47:19.475 AM	✓		00:13:10:21:70:13	00:13:10:21:70:13	nicowlc	CentralWebauth		Pending	Authentication ...

從下到上，您可以看到返回CWA屬性的MAC地址過濾身份驗證。接下來是使用使用者名稱的門戶登入。ISE然後向WLC傳送CoA，最後身份驗證是WLC端的第2層mac過濾身份驗證，但ISE會記住客戶端和使用者名稱並應用我們在此示例中配置的必要VLAN。

當在客戶端上開啟任何地址時，瀏覽器將重定向到ISE。確保域名系統(DNS)配置正確。



在使用者接受策略後授予網路訪問許可權。



在控制器上，策略管理器狀態和RADIUS NAC狀態從*POSTURE_REQD*更改為*RUN*。

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）。