使用ISE 2.0和Aruba WLC配置訪客流

目錄

簡介

本檔案介紹使用Aruba無線LAN控制器(WLC)設定訪客入口的步驟。 從身份服務引擎(ISE)版本2.0引入了對第三方網路接入裝置(NAD)的支援。ISE目前支援與Aruba Wireless for Guest、Posture和Bring Your Own Device(BYOD)流整合。

> **附註**：思科不負責其他供應商的裝置的配置或支援。

必要條件

需求

思科建議您瞭解以下主題：

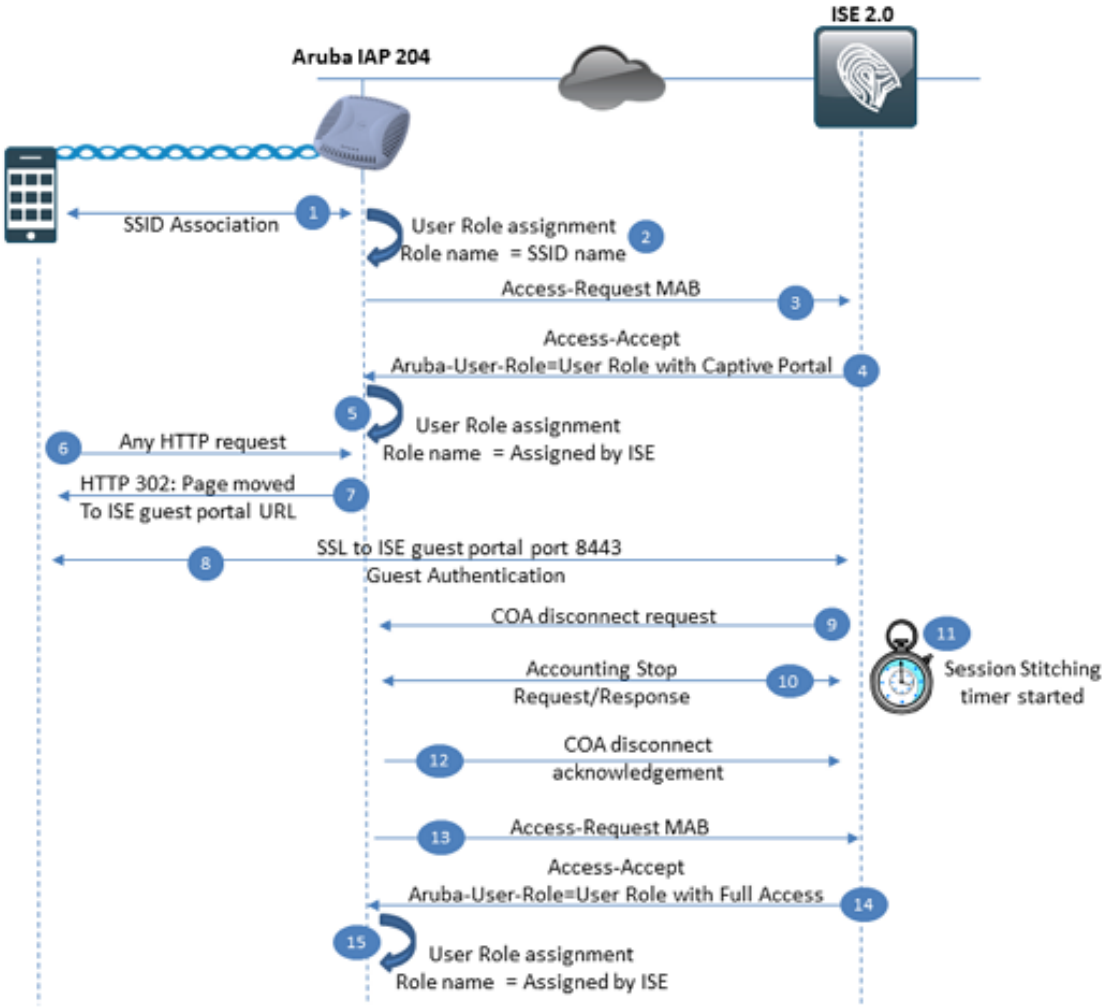
- Aruba IAP配置
- ISE上的訪客流

採用元件

- Aruba IAP 204軟體6.4.2.3
- 思科身分識別服務引擎2.0

背景資訊

訪客流量



步驟1.使用者與服務組識別碼(SSID)關聯。SSID可以配置為開放或預共用金鑰身份驗證。

步驟2. Aruba將使用者角色應用於此連線。第一個使用者角色始終是SSID本身。使用者角色包含不同的設定，例如VLAN、訪問控制限制、強制網路門戶設定等。在當前示例中，分配給SSID的預設使用者角色只有Permit-All語句。

步驟3. SSID配置為通過外部radius伺服器提供MAC過濾。Radius MAB(MAC Authentication Bypass)access-request傳送到ISE。

步驟4.在策略評估時，ISE為訪客選擇授權配置檔案。此授權配置檔案包含等於ACCESS_ACCEPT的訪問型別以及等於Aruba WLC（無線LAN控制器）本地配置的使用者角色名稱的Aruba-User-Role。 此使用者角色配置為強制網路門戶，流量重定向至ISE。

Aruba使用者角色

Aruba WLC使用的主要元件是使用者角色。User-Role定義在連線時適用於使用者的訪問限制。訪

問限制可包括：強制網路門戶重定向、訪問控制清單、VLAN（虛擬區域網）、頻寬限制等。Aruba WLC上存在的每個SSID都有預設的使用者角色，其中使用者角色等於SSID名稱，連線到特定SSID的所有使用者最初都從預設角色獲得限制。Radius伺服器可以覆蓋使用者角色，在這種情況下，訪問接受應包含Aruba供應商特定屬性Aruba-User-Role。WLC使用此屬性的值查詢本地使用者角色。

步驟5.使用屬性Aruba-User-Role的WLC在本地檢查已配置的使用者角色並應用所需的角色。

步驟6.使用者在瀏覽器中啟動HTTP請求。

步驟7.由於已為強制網路門戶配置了使用者角色，Aruba WLC會攔截請求。作為對此請求的響應，WLC返回隨ISE訪客門戶作為新位置移動的HTTP代碼302頁面。

步驟8.使用者在埠8443上建立與ISE的SSL連線，並在訪客門戶中提供使用者名稱/密碼。

步驟9. ISE將COA斷開請求消息傳送到Aruba WLC。

步驟10.在COA斷開連線消息**後**,WLC將丟棄與使用者的連線，並通知ISE應使用Radius Accounting-Request(Stop)消息終止連線。ISE必須確認已使用記帳收到此消息。

步驟11.ISE啟動會話縫合計時器。此計時器用於將COA之前和之後的會話繫結在一起。在此期間，ISE會記住所有會話引數，如使用者名稱等。必須在此計時器到期之前進行第二次身份驗證嘗試，以便為客戶端選擇正確的授權策略。如果計時器過期，則新的Access-Request將解釋為完全新的會話，並且會再次應用具有Guest Redirect的授權策略。

步驟12. Aruba **WLC**使用COA斷開連線確認確認確認先前收到的COA斷開連線請求。

步驟13. Aruba WLC傳送新的MAB Radius存取要求。

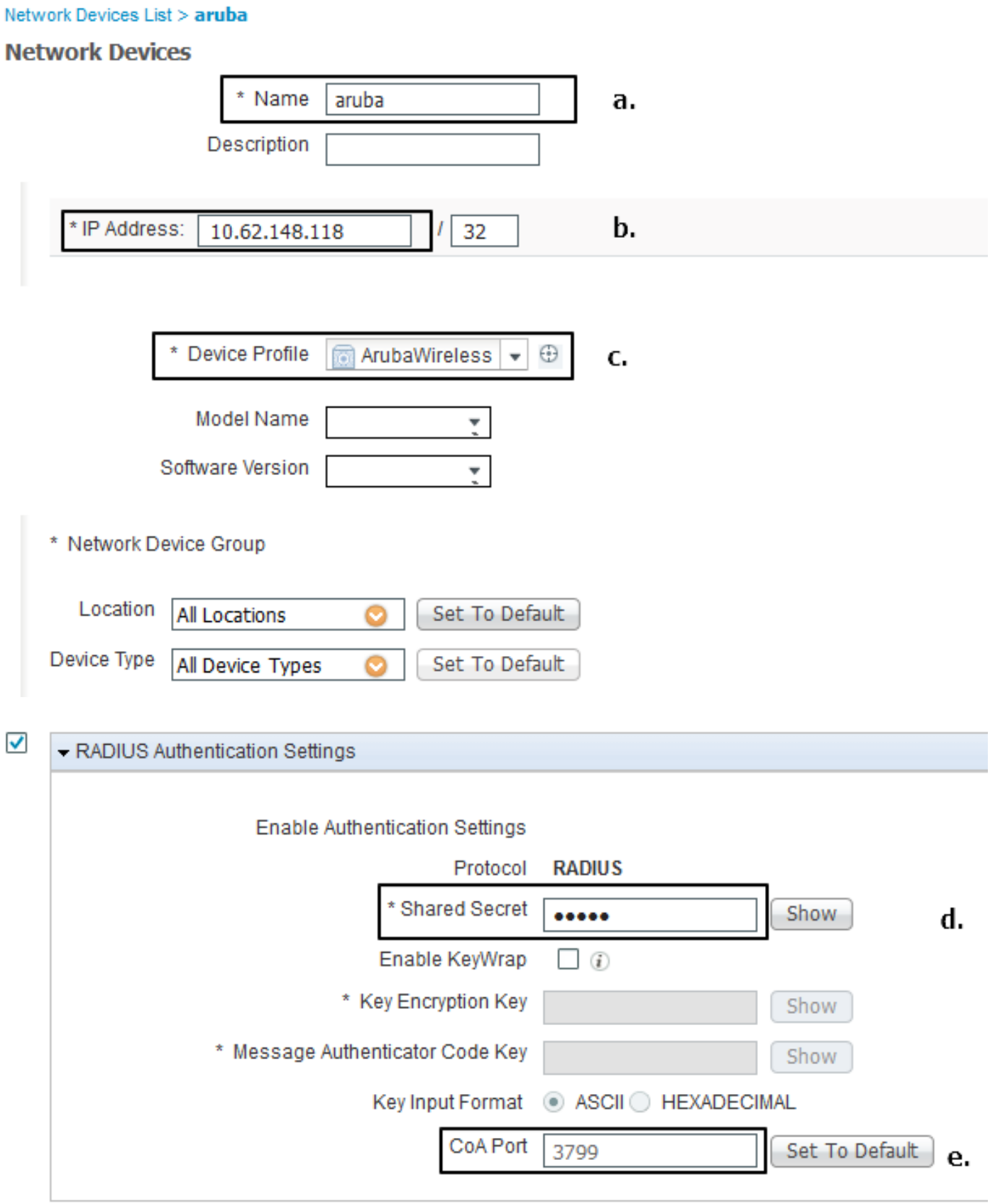
步驟14.在策略評估時，ISE在身份驗證後為訪客選擇授權配置檔案。此授權配置檔案包含等於ACCESS_ACCEPT的訪問型別以及等於Aruba WLC本地配置的使用者角色名稱的Aruba-User-Role。此使用者角色配置為允許所有流量。

步驟15.使用Aruba-User-Role屬性的WLC檢查本地配置的使用者角色並應用所需的角色。

設定

步驟1.將Aruba WLC新增為ISE中的NAD。

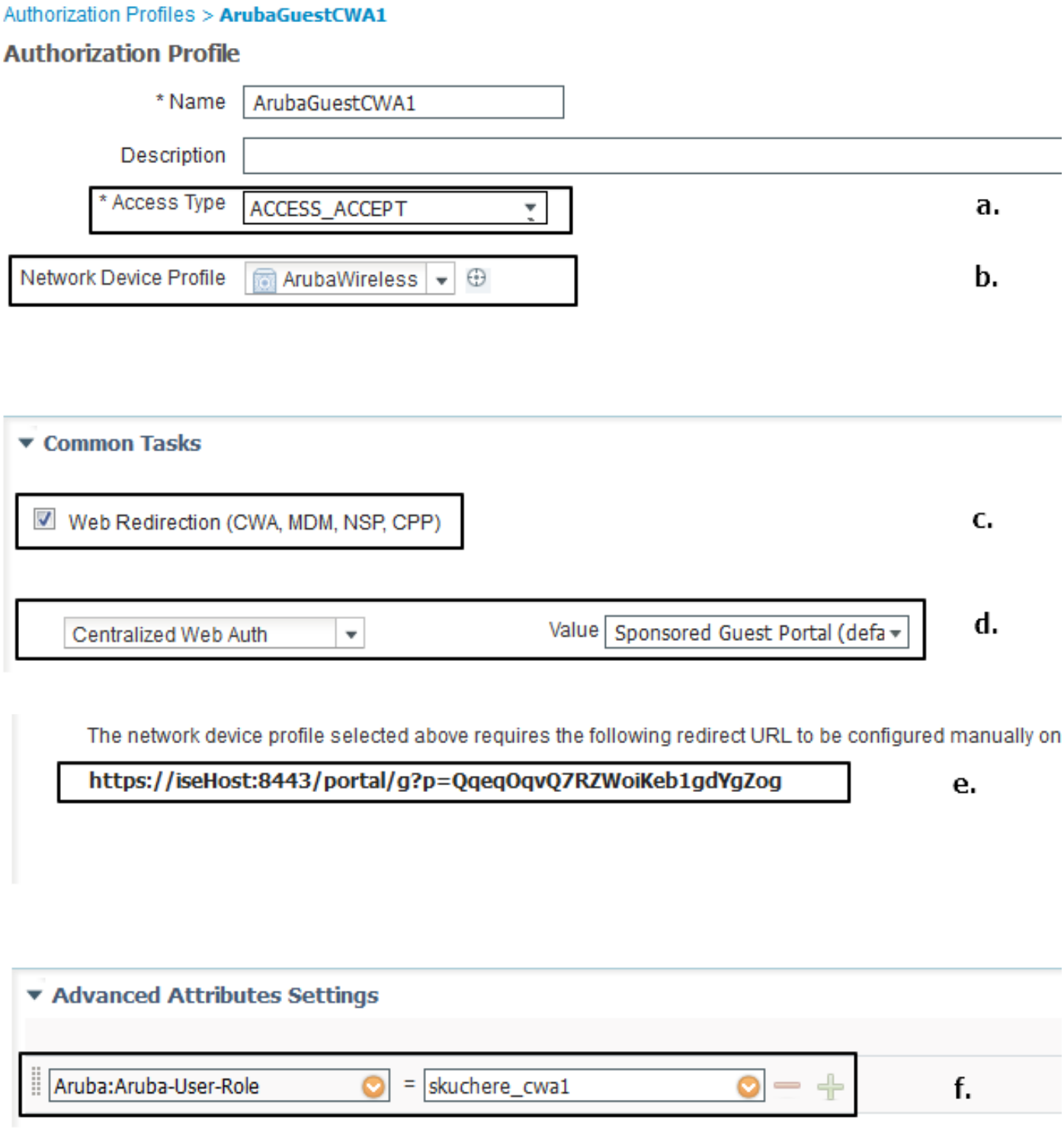
導覽至**Administration > Network Resources > Network Devices**，然後按一下**Add**



1. 提供網路接入裝置(NAD)名稱。
2. 指定NAD IP地址。
3. 選擇網路裝置配置檔案。對於Aruba WLC，您可以使用內建配置檔案ArubaWireless。
4. 提供預共用金鑰。
5. 定義COA埠，裝置從當前示例使用UDP埠3799進行COA。

步驟2.配置授權配置檔案。

導航到**Policy > Policy Elements > Results > Authorization > Authorization Profile**，然後點選**Add**。首先，您必須為中央Web驗證(CWA)重新導向建立授權設定檔，如下圖所示。

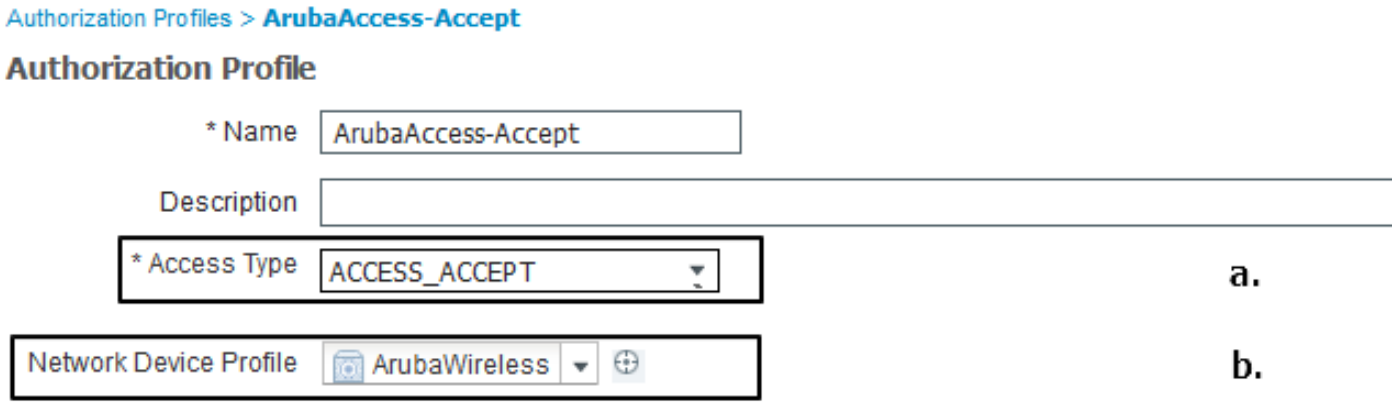


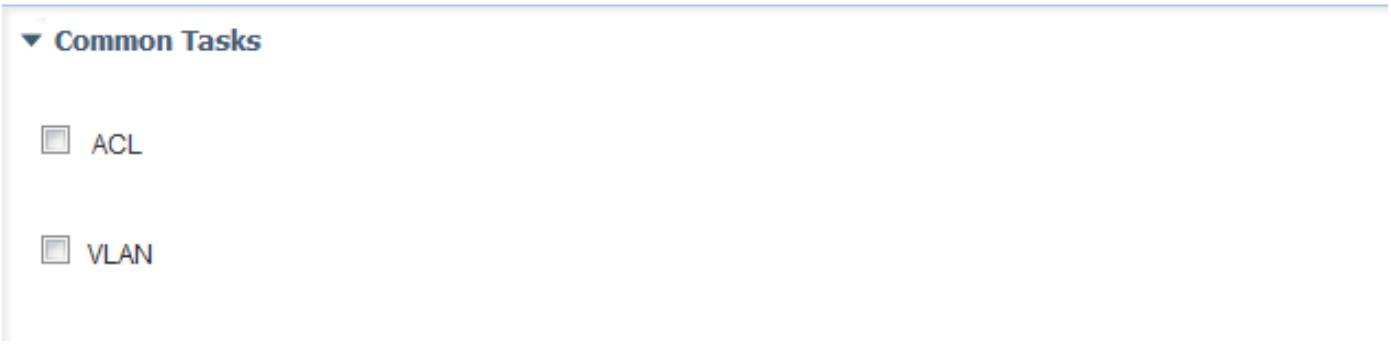
附註：預設情況下，所有授權配置檔案的網路裝置型別均與思科相同。如果將NAD本身配置為ArubaWireless，並且為其他裝置型別建立了授權配置檔案，則此配置檔案永遠無法與此裝置匹配。

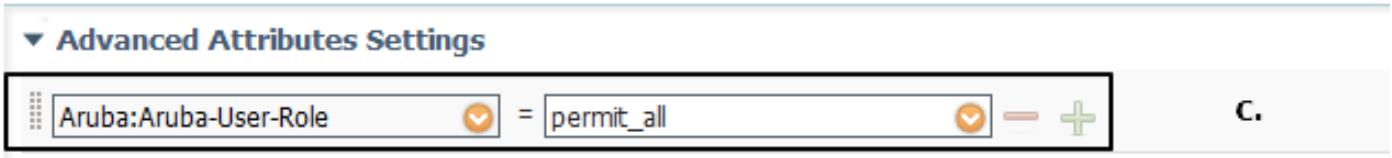
1. 將**Access-Type**定義為**Access-Accept**。
2. 在**Network Device Profile**中選擇**ArubaWireless**。
3. 在common task部分，啟用**Web Redirection**選項。
4. 作為重定向型別，請選擇**集中式Web身份驗證**，然後選擇要用於重定向的訪客門戶。
5. ISE提供的URL應在Aruba WLC上定義為外部強制網路門戶URL。

6. 在**高級屬性設定**部分中，定義Aruba使用者角色屬性值。

應建立第二個授權配置檔案，以便在門戶身份驗證之後為訪客使用者提供訪問許可權：







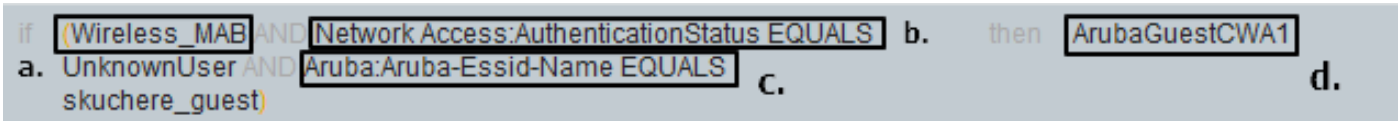
1. 將**Access-Type**定義為**Access-Accept**。
2. 在**Network Device Profile**中選擇**ArubaWireless**。
3. 在**高級屬性設定**部分中定義Aruba使用者角色屬性值。稍後，您將使用相同名稱在Aruba WLC上配置本地使用者角色。

步驟3.配置授權策略。

第一個授權策略負責使用者重定向到訪客門戶。在最簡單的情況下，可以使用內建複合條件

- Wireless_MAB(a.)和
- 網路訪問身份驗證狀態等於未知使用者(b.)和
- 阿魯巴 Aruba-Essid-Name 等於您的訪客SSID名稱(c.)。

對於此策略，請將授權配置檔案配置為重定向至訪客門戶，結果為(d.)



第二個授權策略應在通過門戶進行身份驗證後為訪客使用者提供訪問許可權。此策略可依賴會話資料（使用者身份組/用例訪客流等）。 在此情況中，使用者應在會話縫合計時器過期之前重新連線：

if	GuestType_Contractor (default) AND (Wireless_MAB AND Aruba:Aruba-Essid-Name EQUALS skuchere_guest)	then	ArubaAccess-Accept

要保護自己免受會話拼接計時器過期的影響，可以依靠終端資料而不是會話資料。預設情況下，ISE 2.0上的發起訪客門戶配置為自動註冊訪客裝置（訪客裝置自動放置在Guest_Endpoints終端身份組中）。 此組可用作條件：

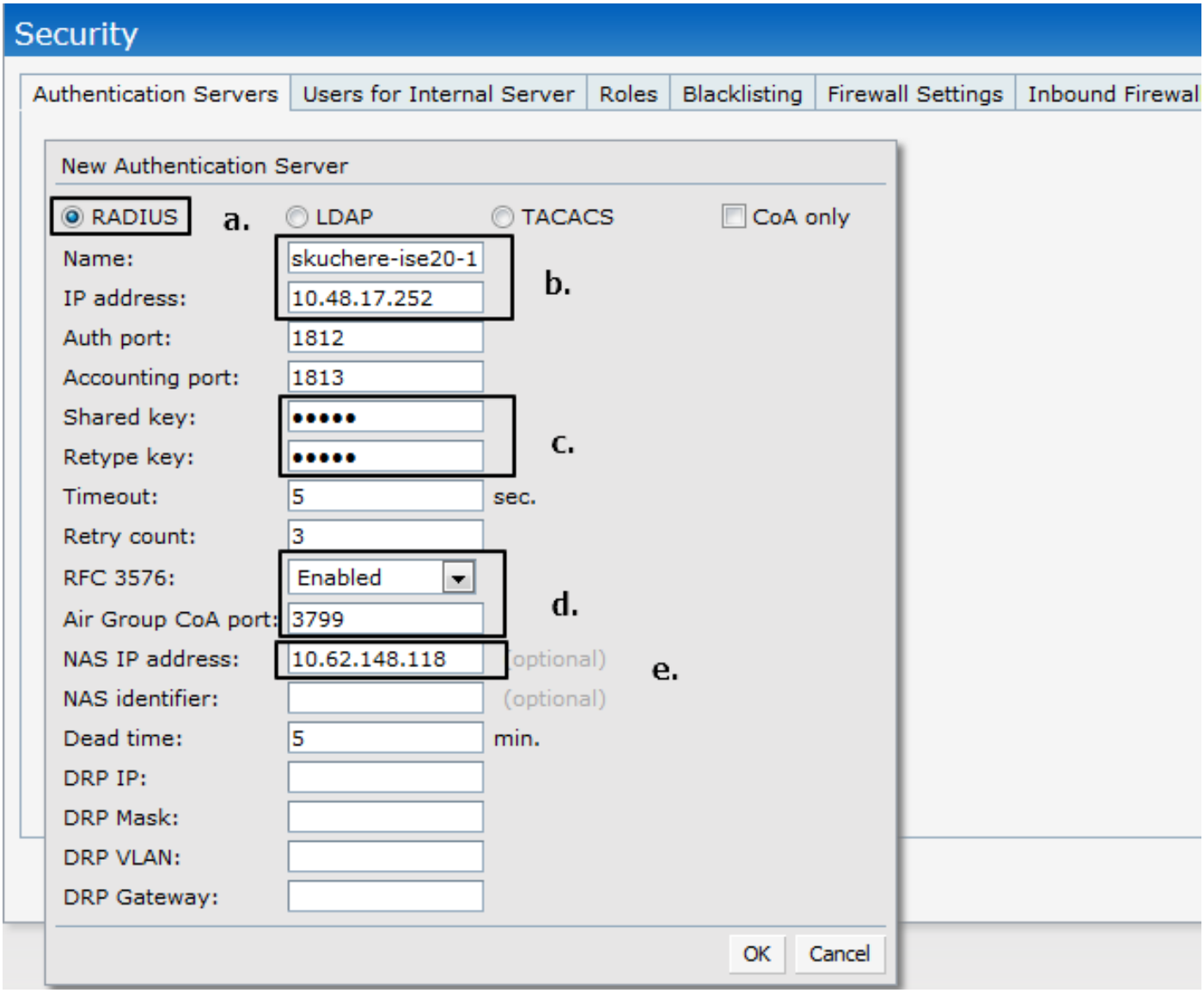
if	GuestEndpoints AND (Wireless_MAB AND Aruba:Aruba-Essid-Name EQUALS skuchere_guest)	then	ArubaAccess-Accept

按正確順序執行授權策略：

if	**GuestEndpoints** AND (Wireless_MAB AND Aruba:Aruba-Essid-Name EQUALS skuchere_guest)	then	ArubaAccess-Accept
if	(Wireless_MAB AND Network Access:AuthenticationStatus EQUALS UnknownUser AND Aruba:Aruba-Essid-Name EQUALS skuchere_guest)	then	ArubaGuestCWA1

步驟4.在Aruba上配置Radius伺服器。

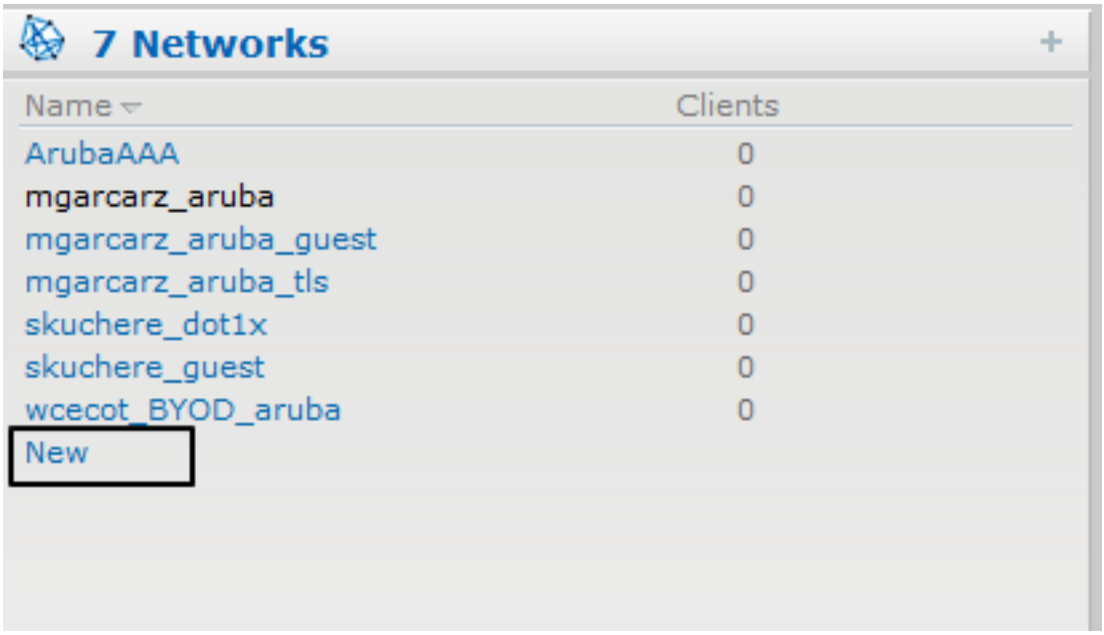
導覽至**Security > Authentication Servers**，然後按一下**New:**



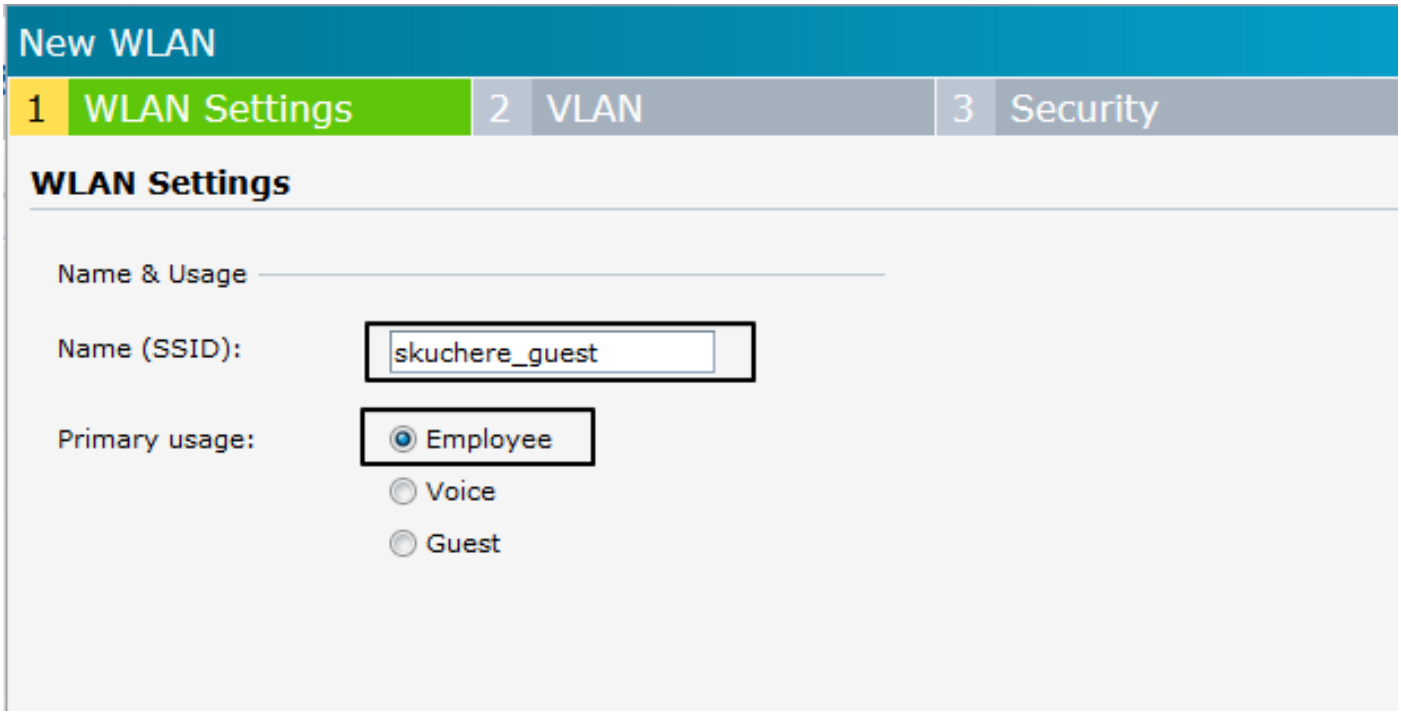
1. 選擇RADIUS作為AAA協定。
2. 定義AAA伺服器名稱和IP地址。
3. 指定預共用金鑰。
4. 啟用RFC 3576支援並定義COA埠。
5. 指定Aruba WLC管理介面IP作為NAS IP地址。

步驟5.在Aruba上建立訪客SSID。

在儀表板頁面中，選擇網路清單末尾的**New**。應啟動SSID建立嚮導。遵循嚮導步驟。

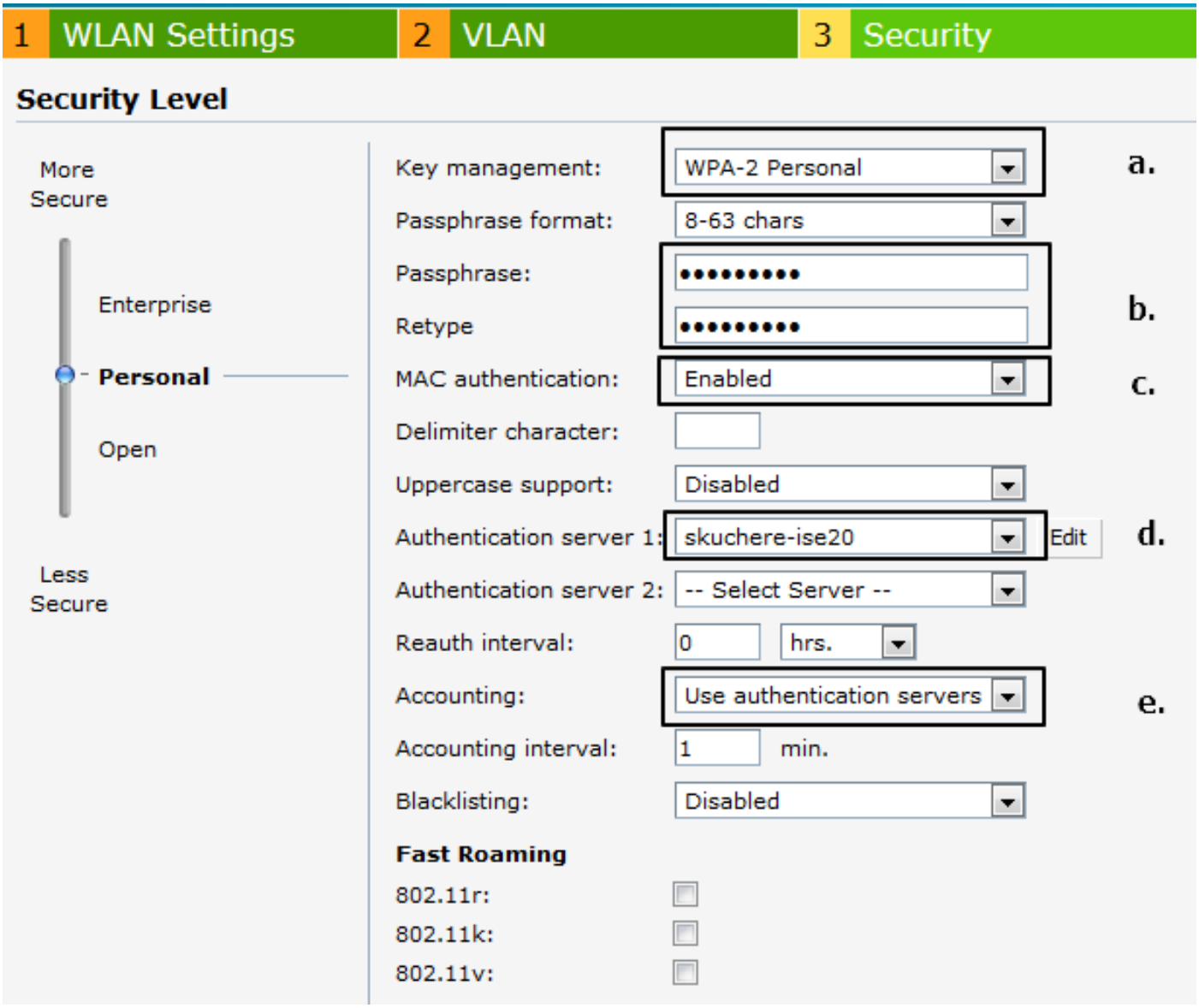


步驟1.定義SSID名稱並選擇SSID型別。此處使用了SSID型別Employee。此SSID型別的預設角色為permit all和no Captive Portal Enforcement。此外，您還可以選擇型別Guest。在這種情況下，您應該在SSID配置期間定義強制網路門戶設定。



步驟2. VLAN和IP地址分配。此處，設定保留為預設值，如圖所示。

步驟3.安全設定。對於訪客SSID，您可以選擇開啟或個人。個人需要預共用金鑰。

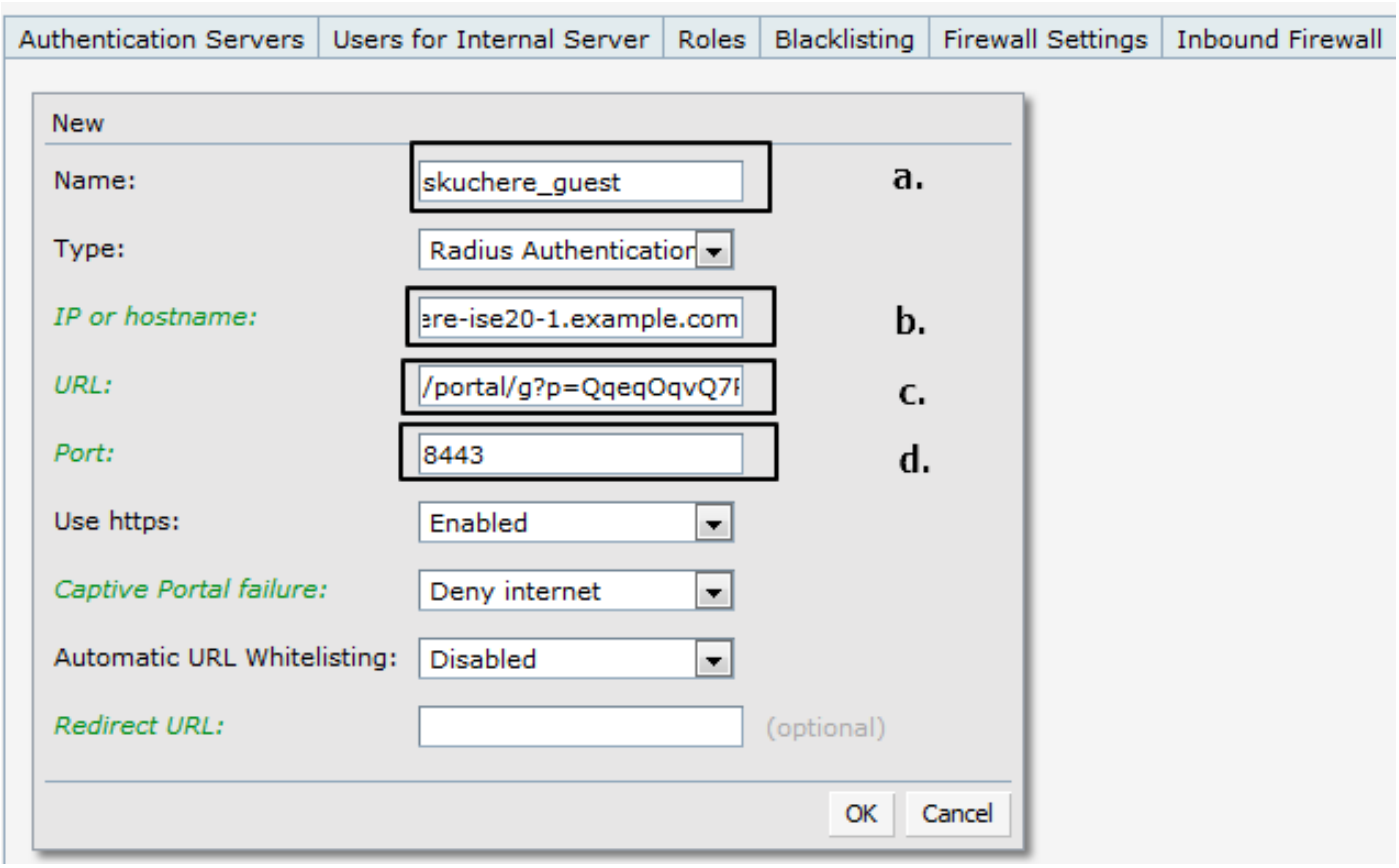


1. 選擇金鑰管理機制。
2. 定義預共用金鑰。
3. 要使用MAB MAC過濾對ISE驗證使用者身份，需要啟用。
4. 在身份驗證伺服器清單中，選擇您的AAA伺服器。
5. 要對以前定義的AAA伺服器啟用記帳，請在下拉選單中選擇Use Authentication server。

附註：會計對於第三方NAD至關重要。如果策略服務節點(PSN)沒有從NAD接收使用者的記帳停止，會話可能會停滯在「已啟動」狀態。

步驟6.配置強制網路門戶。

導覽至**Security > External Captive Portals**，然後建立新門戶，如下圖所示：



步驟1.指定強制網路門戶名稱。

步驟2.定義ISE FQDN或IP地址。如果使用IP地址，請確保在訪客門戶證書的Subject Alternative Name(SAN)欄位中定義的此IP。

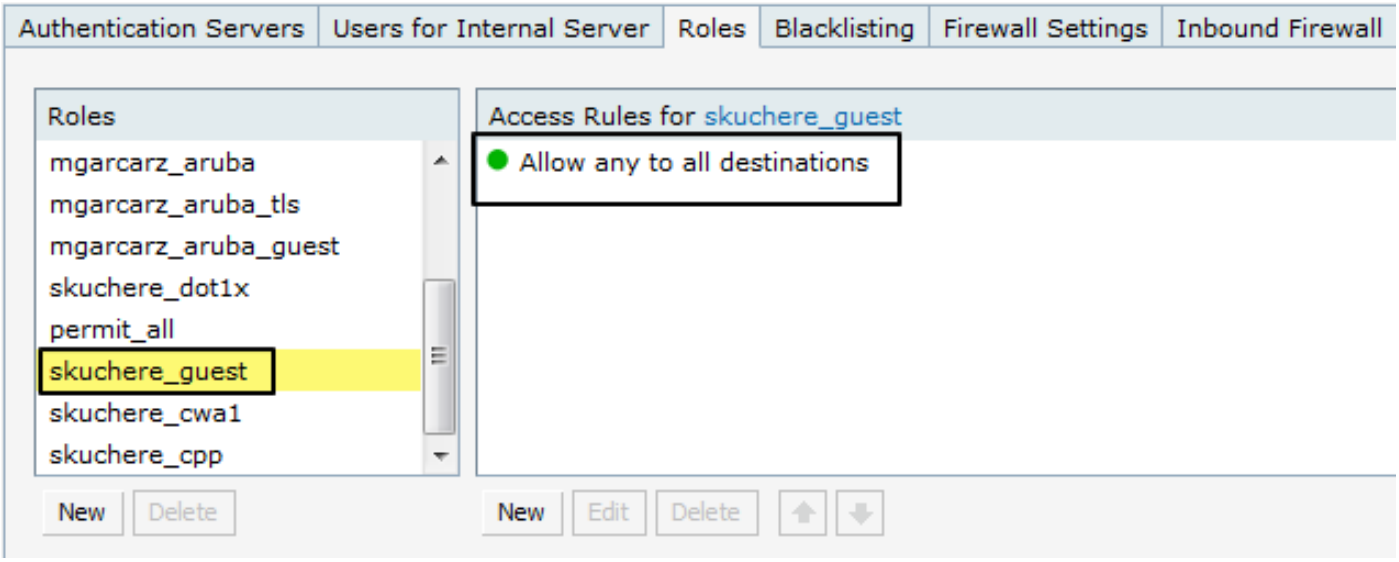
附註：您可以使用任何PSN伺服器，但應始終將使用者重定向到發生MAB的伺服器。通常，您必須定義已在SSID上配置的Radius伺服器的FQDN。

步驟3.提供從ISE授權配置檔案進行重定向。你應該把部件放在埠號之後，

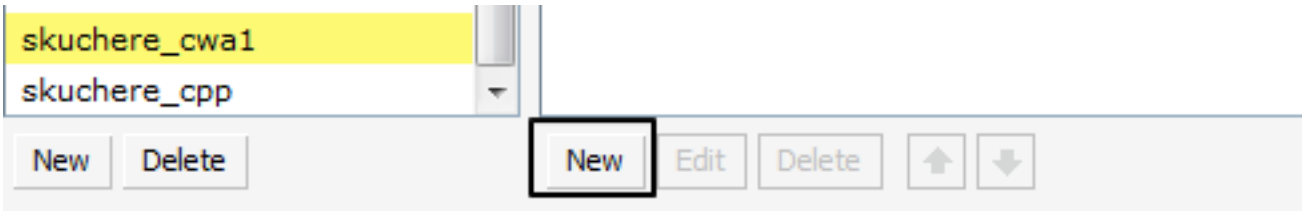
步驟4.定義ISE訪客門戶埠。

步驟7.配置使用者角色。

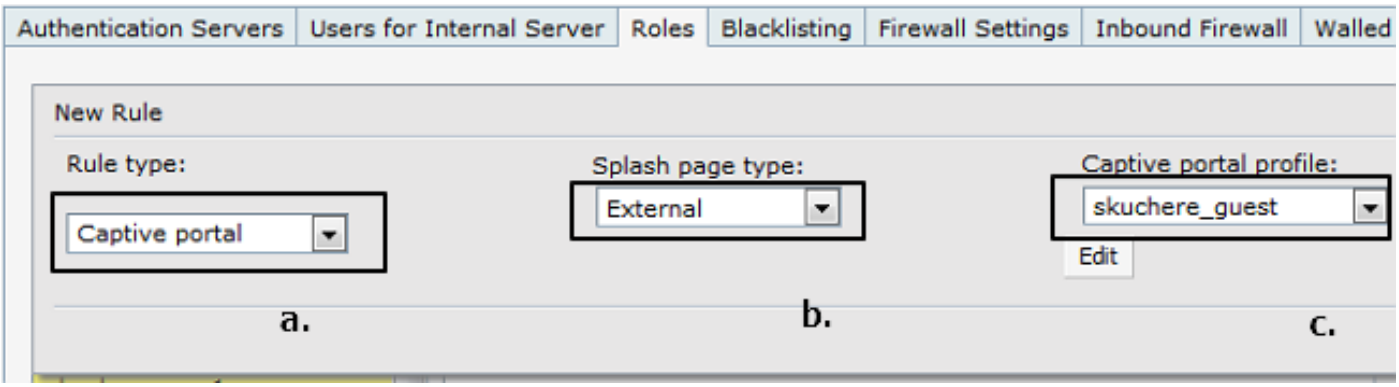
導航到**安全>角色。**確保建立SSID後，清單中存在具有相同名稱的新角色，且訪問規則允許任意訪問所有目標。此外，建立兩個角色：一個用於CWA重新導向，另一個用於在訪客門戶上進行身份驗證後允許訪問。這些角色的名稱應與ISE授權配置檔案中定義的Aruba使用者角色相同。



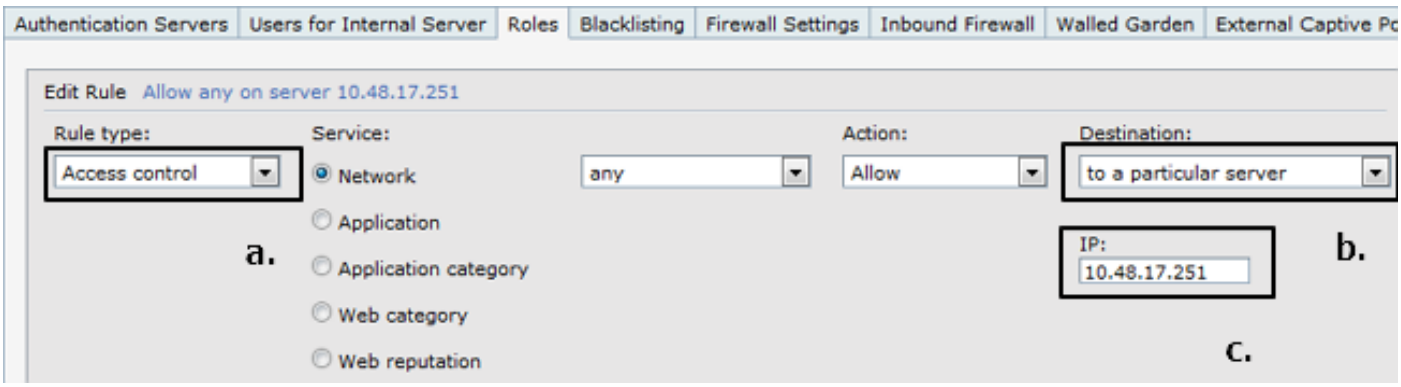
如圖所示，為重新導向建立新使用者角色並新增安全限制。



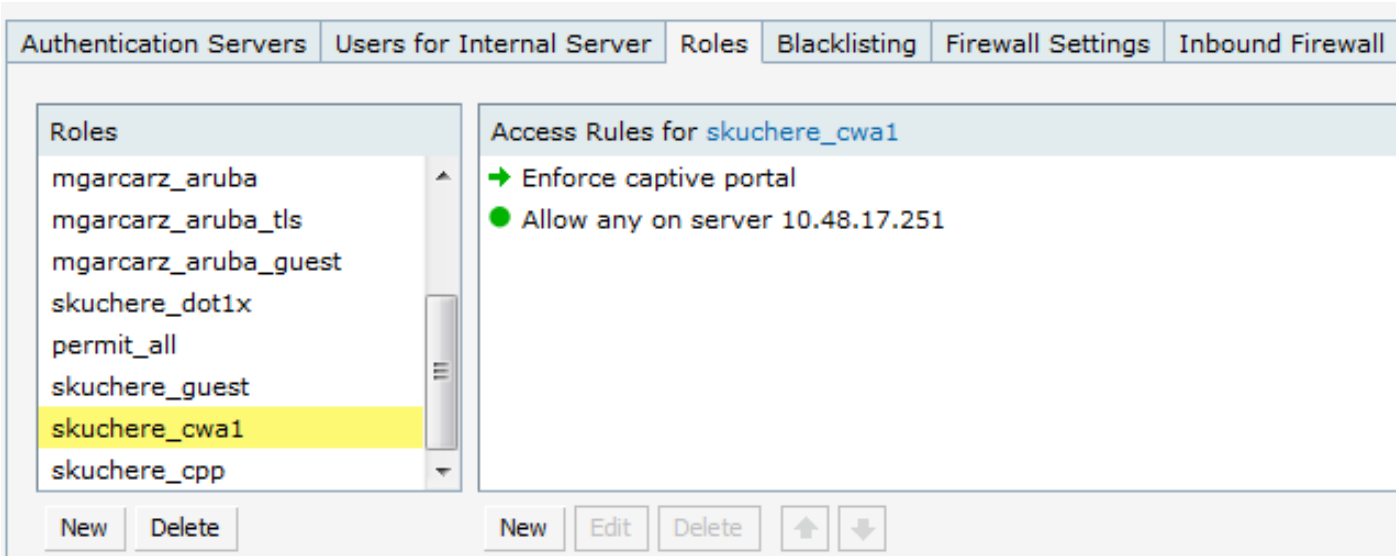
對於第一個限制，您需要定義：



對於第二個限制，您需要定義：

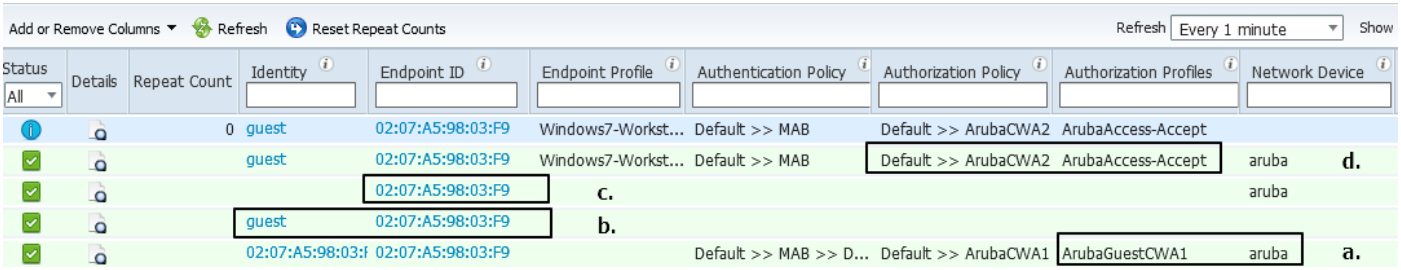


如圖所示，可以刪除預設規則Allow any to all destinations。這是角色配置的摘要結果。



驗證

ISE **Operations > Radius Livelog中的訪客流示例。**



1. 第一個MAB，因此是具有CWA重定向和使用者角色的授權配置檔案，在Aruba端配置強制網路門戶。
2. 訪客身份驗證。
3. 授權變更成功(CoA)。
4. 第二個MAB，從而生成一個授權配置檔案，該配置檔案具有permit access和User-Role，允許在Aruba端的所有規則。

在Aruba端，可以使用**show clients**命令確保使用者已連線，IP地址已分配，而且身份驗證的結果是分配了正確的使用者角色：

```
04:bd:88:c3:88:14# show clients

Client List
-----------
Name              IP Address    MAC Address        OS     Network        Access Point       Channel  Type  Role
----              ----------    -----------        --     -------        ------------       -------  ----  ----
02-07-A5-98-03-F9  10.62.148.77  02:07:a5:98:03:f9  Win 7  skuchere_guest  04:bd:88:c3:88:14  11       GN    skuchere_cwa1
Number of Clients   :1
Info timestamp      :92552
```

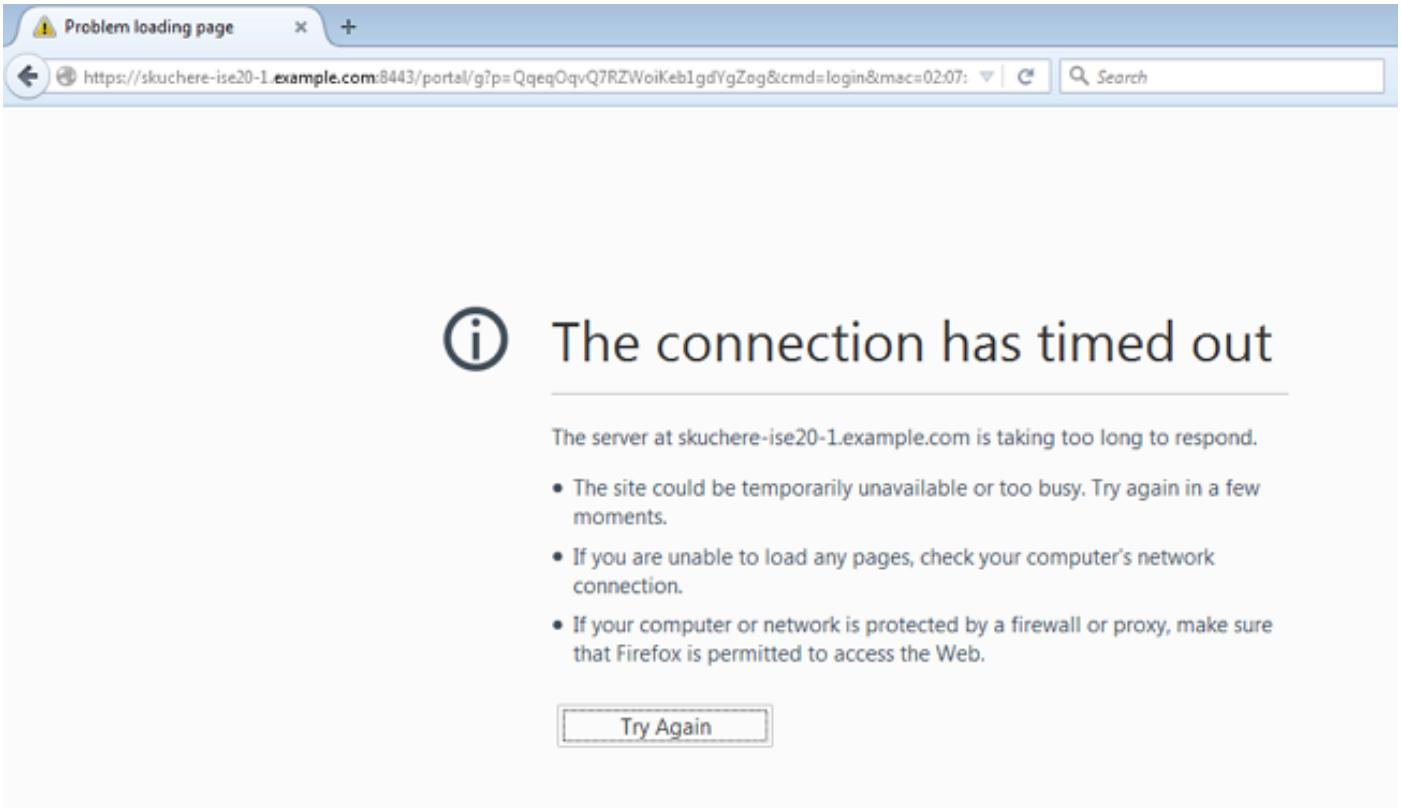
疑難排解

失敗的COA

在ISE設定中，確保Aruba NAD在ISE端配置了正確的網路裝置型別，並且COA埠在NAD設定中定義正確。在Aruba端，確保在身份驗證伺服器設定中啟用RFC 3576，並正確定義COA埠。從網路角度檢查ISE和Aruba WLC之間是否允許UDP埠3799。

重定向問題

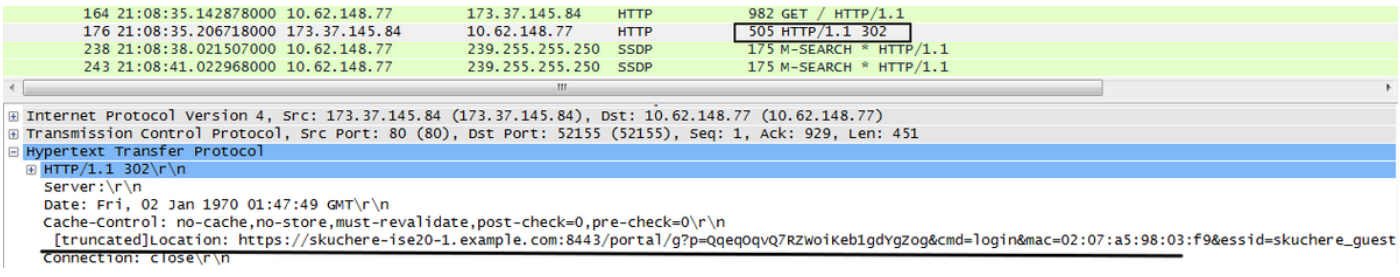
使用者在瀏覽器中看到ISE URL，但不會顯示ISE頁面，如下圖所示：



在使用者端，確保ISE FQDN可以成功解析為正確的IP。在Aruba端，檢查強制網路門戶設定中是否正確定義了ISE URL，以及使用者角色訪問限制中允許的指向ISE的流量。還要檢查SSID上的Radius伺服器和Captive portal設定中的ISE PSN是否為同一裝置。從網路角度檢查是否允許TCP埠8443從使用者段到ISE。

使用者瀏覽器中沒有重定向URL

在使用者端，確保每個HTTP請求的結果是Aruba WLC返回使用ISE URL移動的HTTP代碼302頁面。



會話拼接計時器已過期

此問題的典型症狀是使用者第二次被重定向到訪客門戶。在這種情況下，在ISE Radius Livelog中，您應該會看到，在COA之後，再次選擇具有CWA的第二個身份驗證授權配置檔案。在Aruba端，使用**show clients**命令的幫助檢查實際使用者角色。

作為此問題的解決方法，在成功進行訪客身份驗證後，您可以在ISE上使用基於終端的授權策略進行連線。