使用融合接入配置外部Web身份驗證(5760/3650/3850)

目錄

簡介

本檔案定義了如何使用融合存取控制器設定外部Web驗證。在此示例中，訪客門戶頁面和憑證身份驗證都位於身份服務引擎(ISE)上。

必要條件

需求

思科建議您瞭解以下主題：

1.思科融合接入控制器。

2. Web驗證

3.思科ISE

採用元件

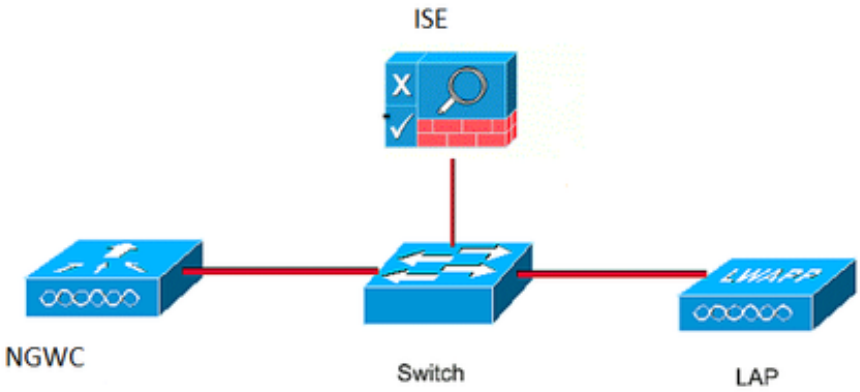
本文中的資訊係根據以下軟體和硬體版本：

1. Cisco 5760控制器（下圖中的NGWC），03.06.05E

2. ISE 2.2

設定

網路圖表



CLI組態

控制器上的RADIUS配置

第1步：定義外部RADIUS伺服器

```
radius server ISE.161
address ipv4 10.48.39.161 auth-port 1812 acct-port 1813
timeout 10
retransmit 5
key Cisco123
```

第2步：。定義AAA radius組並指定要使用的radius伺服器

```
aaa group server radius ISE-Group
server name ISE.161
deadtime 10
```

步驟3.定義指向radius組的方法清單並將其對映到WLAN下。

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

引數對映配置

步驟4.使用外部和內部webauth所需的虛擬ip地址配置全域性引數對映。註銷按鈕使用虛擬IP。配置不可路由的虛擬IP始終是一種很好的做法。

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 1.1.1.1
```

第5步：配置命名引數對映。它將像一種webauth方法一樣工作。這將會在WLAN配置下呼叫。

```
parameter-map type webauth web
type webauth
redirect for-login https://10.48.39.161:8443/portal/PortalSetup.action?portal=0c712cd0-6d90-
11e5-978e-005056bf2f0a
redirect portal ipv4 10.48.39.161
```

預先驗證ACL。這也會在WLAN下稱為。

第6步：配置Preauth_ACL，允許在身份驗證結束之前訪問ISE、DHCP和DNS

```
ip access-list extended Preauth_ACL
permit ip any host 10.48.39.161
permit ip host 10.48.39.161 any
permit udp any eq bootps any
permit udp any any eq bootpc
permit udp any eq bootpc any
permit udp any eq domain any
permit udp any any eq domain
```

WLAN配置

第7步：設定WLAN

```
wlan ext-webauth 7 ext-webauth
client vlan vlan232
ip access-group web Preauth_ACL
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauth
security web-auth parameter-map web
session-timeout 1800
no shutdown
```

第8步：開啟http伺服器。

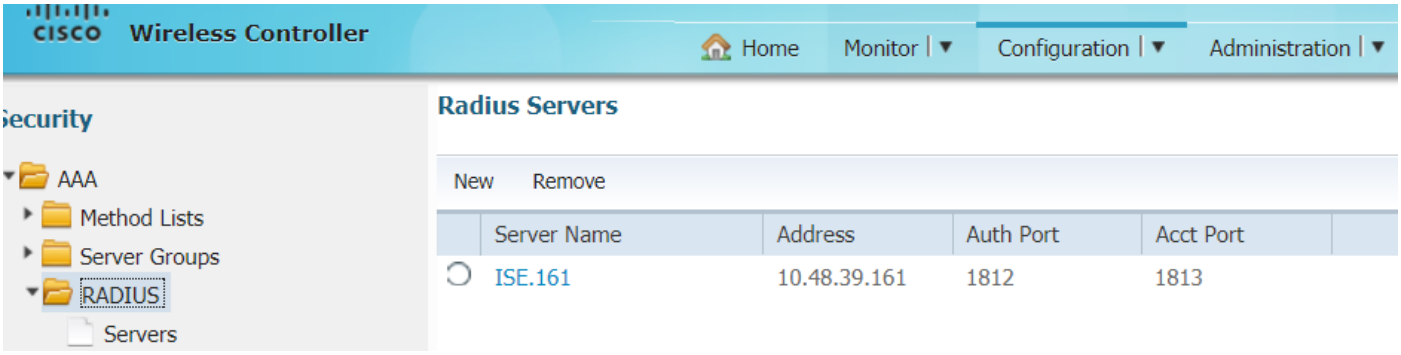
```
ip http server

ip http secure-server (for secure web-auth, use 'no' to disable secure web)
```

GUI配置

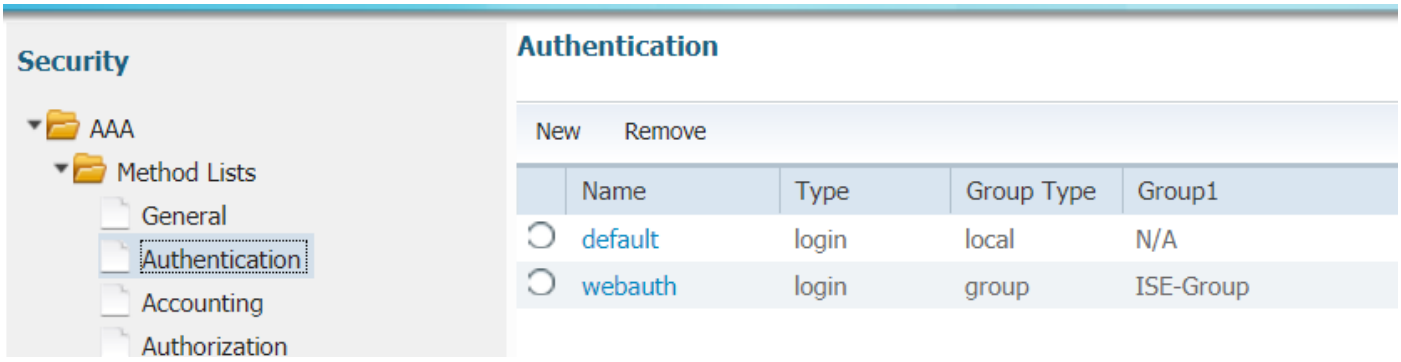
我們在此採取的步驟與上文相同。螢幕截圖只是供交叉參考。

第1步：定義外部radius伺服器



第2步：。定義AAA radius組並指定要使用的radius伺服器

步驟3.定義指向radius組的方法清單並將其對映到WLAN下。



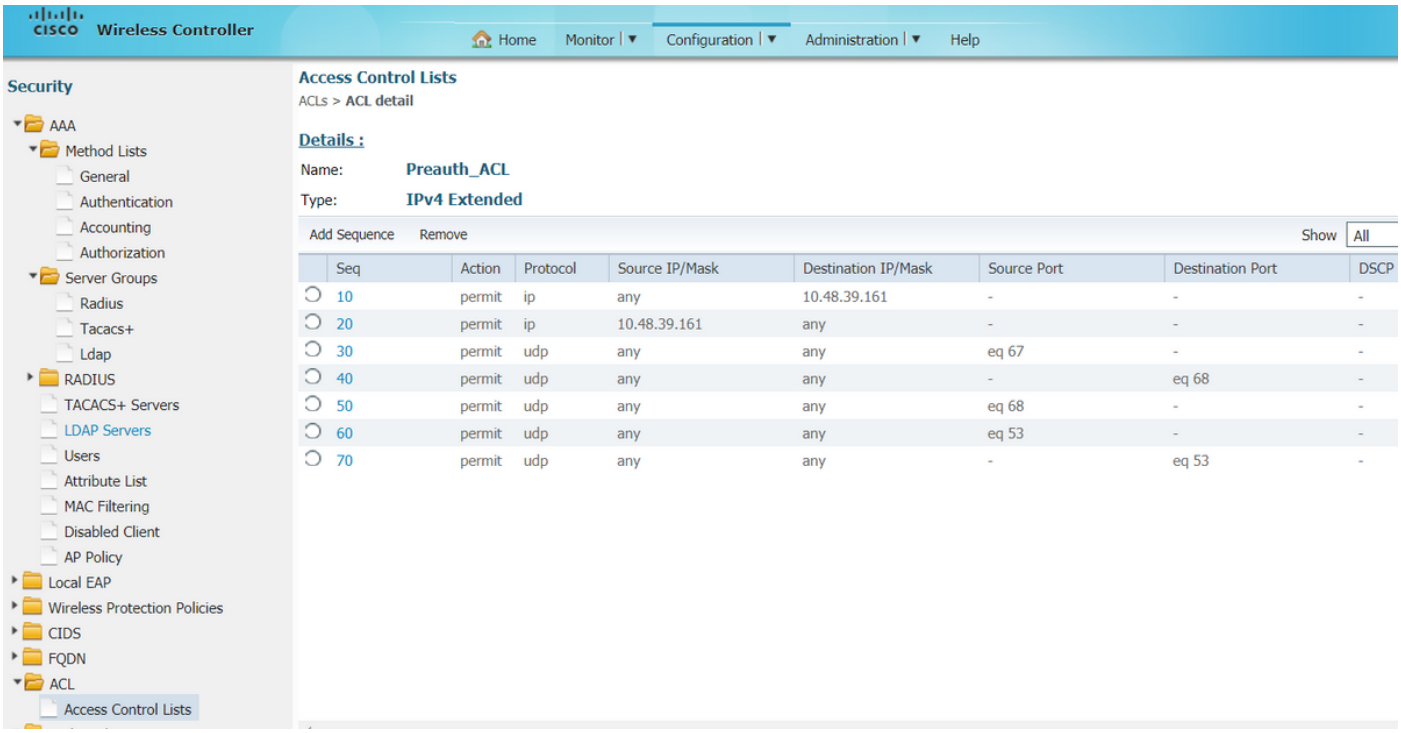
引數對映配置

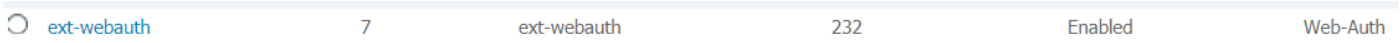
步驟4.使用外部和內部webauth所需的虛擬ip地址配置全域性引數對映。註銷按鈕使用虛擬IP。配置不可路由的虛擬IP始終是一種很好的做法。

第5步：配置命名引數對映。它將像一種webauth方法一樣工作。這將會在WLAN配置下呼叫。

預先驗證ACL。這也會在WLAN下稱為。

第6步：配置Preauth_ACL，允許在身份驗證結束之前訪問ISE、DHCP和DNS



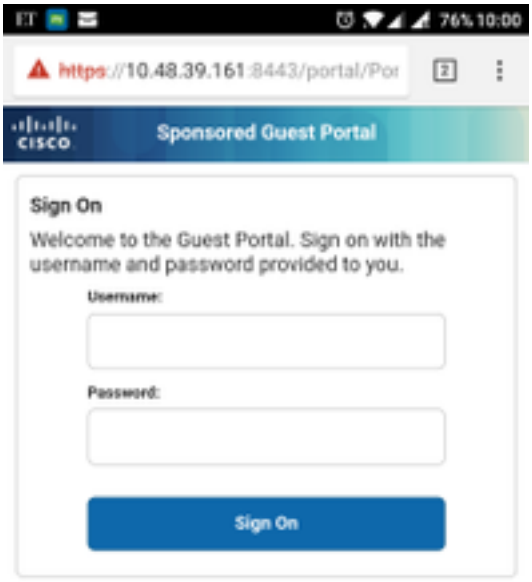


WLAN配置

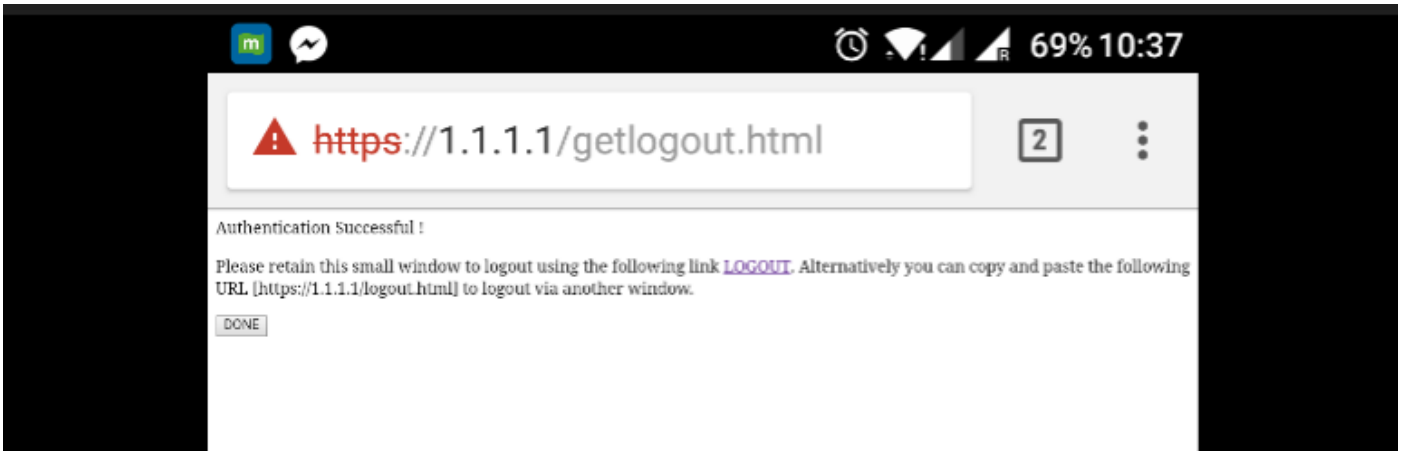
第7步：設定WLAN

驗證

連線使用者端，並確保如果您開啟瀏覽器，使用者端將重新導向到您的登入入口頁面。以下螢幕截圖說明ISE訪客門戶頁面。



提交正確的憑證後，將顯示成功頁面：



ISE伺服器將報告兩個身份驗證：一次在訪客頁面上（底部僅包含使用者名稱），另一次在WLC透過radius驗證提供相同使用者名稱/密碼後進行驗證（只有此驗證才能使使用者端進入成功階段）。如果沒有執行radius驗證（將mac位址和WLC詳細資料作為NAS），則需驗證radius組態。