適用於每個WLAN的ACS 5.2和WLC驗證組態範例

目錄

簡介

本文提供根據服務組識別碼(SSID)限制每個使用者存取無線LAN(WLAN)的組態範例。

必要條件

需求

思科建議您瞭解以下主題：

- 如何設定無線LAN控制器(WLC)和輕量型存取點(LAP)以達成基本操作
- 如何設定思科安全存取控制伺服器(ACS)
- 輕量型存取點通訊協定(LWAPP)和無線安全方法

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5500系列WLC（執行韌體版本7.4.110）
- 思科1142系列LAP
- Cisco安全ACS伺服器版本5.2.0.26.11

設定

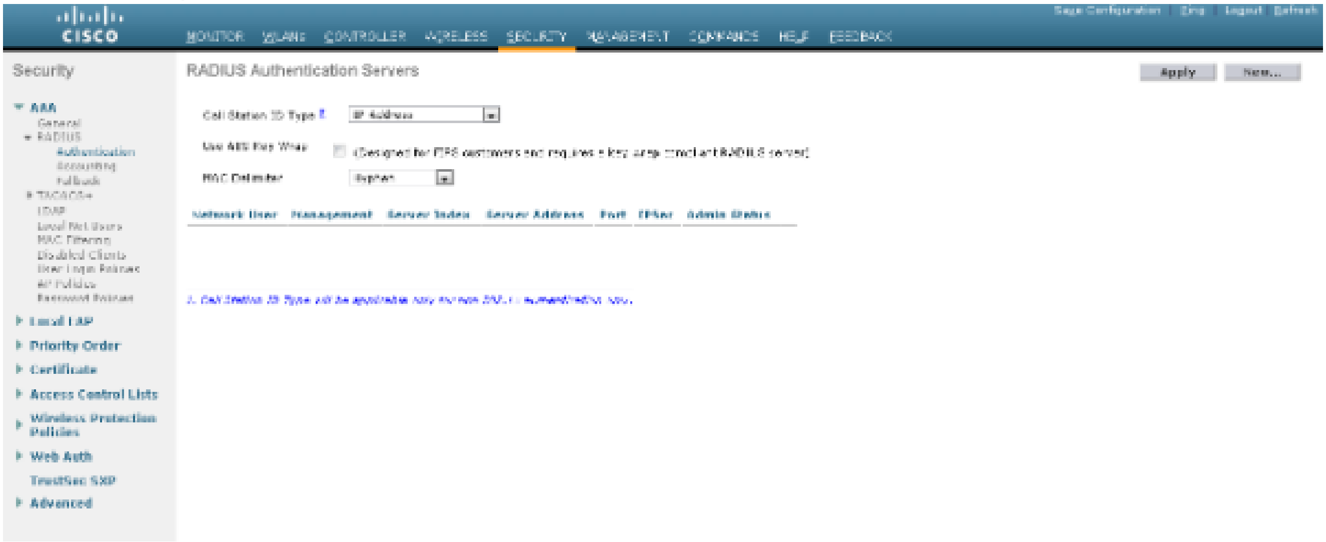
要為此設定配置裝置，您需要：

1. 為兩個WLAN和RADIUS伺服器配置WLC。
2. 配置Cisco Secure ACS。
3. 配置無線客戶端並驗證配置。

設定WLC

完成以下步驟，以便為此設定設定WLC:

1. 設定WLC以將使用者認證轉送到外部RADIUS伺服器。外部RADIUS伺服器（此案例為思科安全ACS）然後驗證使用者認證並提供對無線使用者端的存取許可權。請完成以下步驟： 從控制器GUI中選擇**Security > RADIUS Authentication**，以顯示「RADIUS Authentication Servers」頁面。

   RADIUS Authentication Servers

   Call Station ID Type 1: IP Address

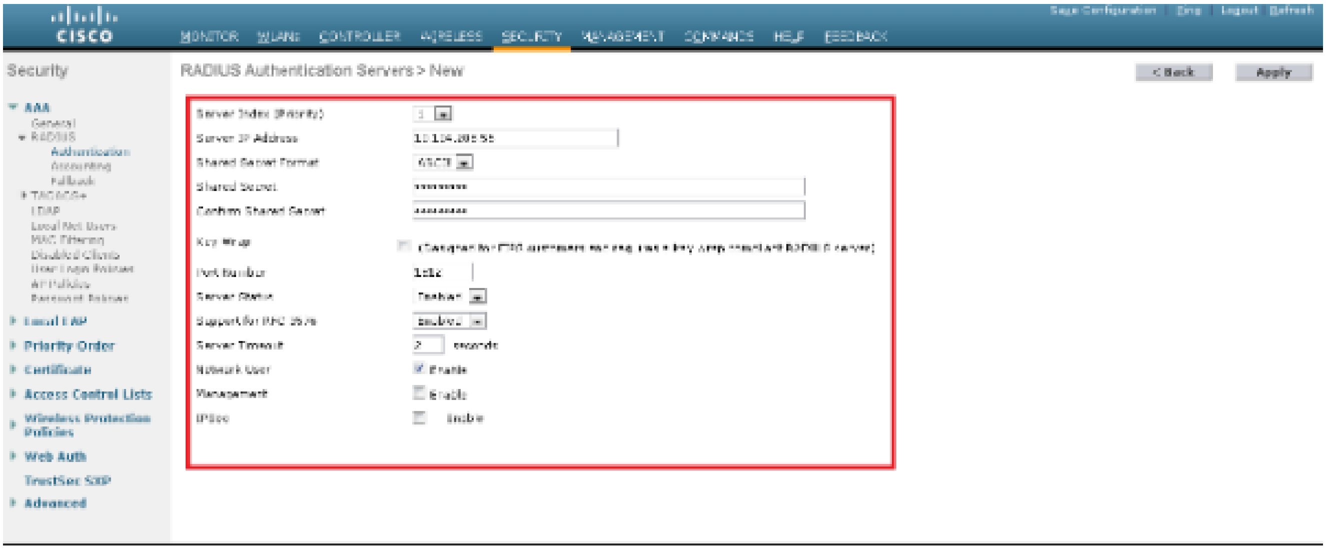
   Use AES Key Wrap ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

   MAC Delimiter: Hyphen

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status

   1. Call Station ID Type will be applicable only for non 802.1x authentication only.

   按一下「**New**」以定義RADIUS伺服器引數。 這些引數包括RADIUS伺服器IP地址、共用金鑰、埠號和伺服器狀態。Network User和Management覈取方塊確定基於RADIUS的身份驗證是否適用於管理和網路使用者。此示例使用Cisco Secure ACS作為IP地址為10.104.208.56的RADIUS伺服器。

   RADIUS Authentication Servers > New

   Server Index (Priority): 1

   Server IP Address: 10.104.208.56

   Shared Secret Format: ASCII

   Shared Secret: ********

   Confirm Shared Secret: ********

   Key Wrap ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

   Port Number: 1812

   Server Status: Enabled

   Support for RFC 3576: Enabled

   Server Timeout: 2 seconds

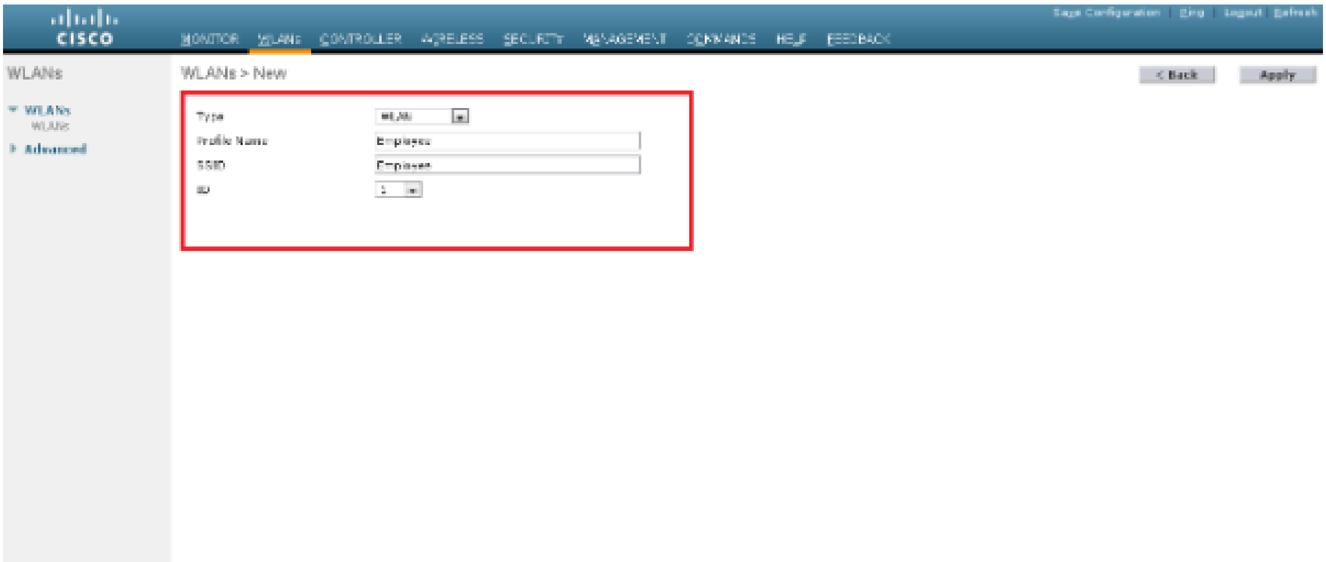
   Network User ☑ Enable

   Management ☐ Enable

   IPSec ☐ Enable

   按一下「**Apply**」。

2. 完成這些步驟，為使用SSID **Employee**的員工配置一個WLAN，為使用SSID Contractor的承包商配置另**一個WLAN**。 在控制器GUI上按一下「**WLANs**」以建立WLAN。出現WLANs視窗。此視窗列出控制器上設定的WLAN。按一下**New**以設定新的WLAN。此範例建立名為Employee的WLAN，且WLAN ID為1。按一下**Apply**。



WLANs > New

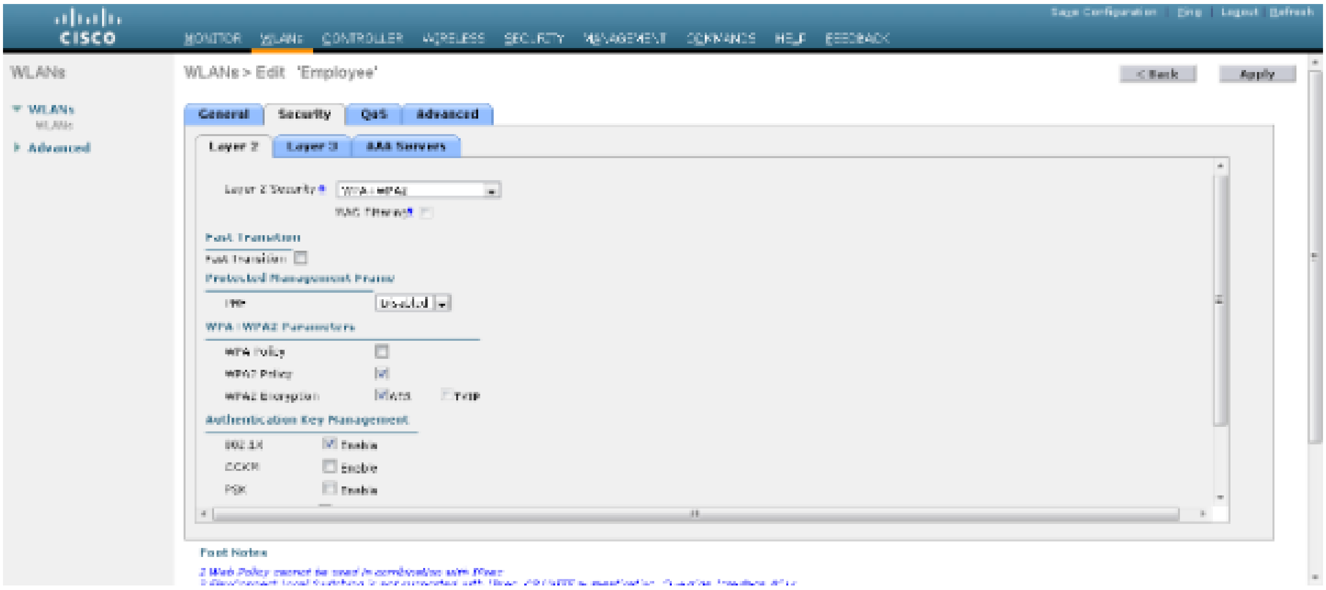
Type: WLAN

Profile Name: Employee

SSID: Employee

ID: 1

選擇**WLAN > Edit**視窗並定義特定於WLAN的引數： 在Layer 2 Security頁籤中選擇**802.1x**。預設情況下，第2層安全選項為802.1x。這將為WLAN啟用802.1 x/可擴展身份驗證協定(EAP)身份驗證。



WLANs > Edit 'Employee'

Layer 2 Security: WPA+WPA2

PMF: Disabled

WPA Policy ☐

WPA2 Policy ☑

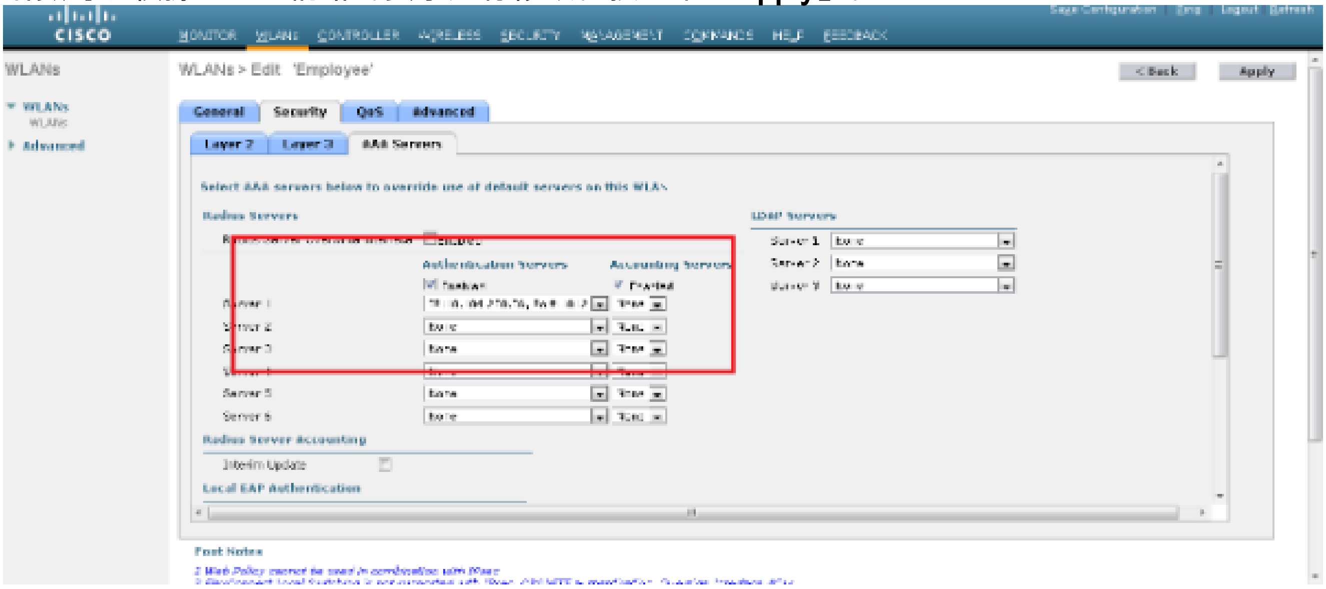
WPA2 Encryption ☑AES ☐TKIP

802.1X ☑ Enable

CCKM ☐ Enable

PSK ☐ Enable

在AAA servers頁籤中，從RADIUS Servers下的下拉選單中選擇適當的RADIUS伺服器。其它引數可以根據WLAN網路的要求進行修改。按一下「**Apply**」。



WLANs > Edit 'Employee'

Select AAA servers below to override use of default servers on this WLAN

Authentication Servers ☑ Enabled

Accounting Servers ☑ Enabled

Server 2: None

Server 3: None

Server 4: None

Server 5: None

Server 6: None

Interim Update ☐

同樣地，若要為承建商建立WLAN，請重複步驟b至d。

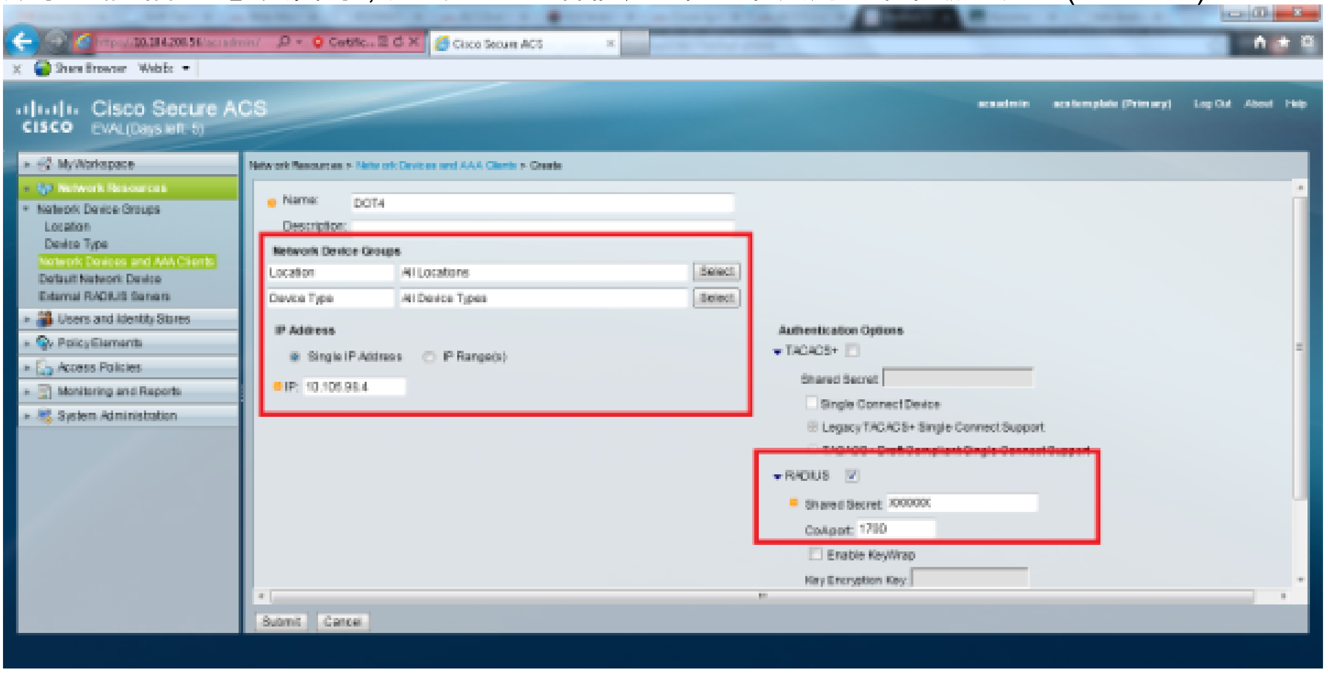
配置Cisco Secure ACS

在Cisco Secure ACS伺服器上，您需要：

1. 將WLC配置為AAA客戶端。
2. 為基於SSID的身份驗證建立使用者資料庫（憑據）。
3. 啟用EAP身份驗證。

在Cisco Secure ACS上完成以下步驟：

1. 若要將控制器定義為ACS伺服器上的AAA使用者端，請從ACS GUI中選擇**Network Resources > Network Devices and AAA Clients**。在Network Devices and AAA Clients下，**單擊Create。**
2. 顯示「網路組態」頁面時，定義WLC的名稱、IP位址和共用金鑰和驗證方法(RADIUS)。



Network Resources > Network Devices and AAA Clients > Create

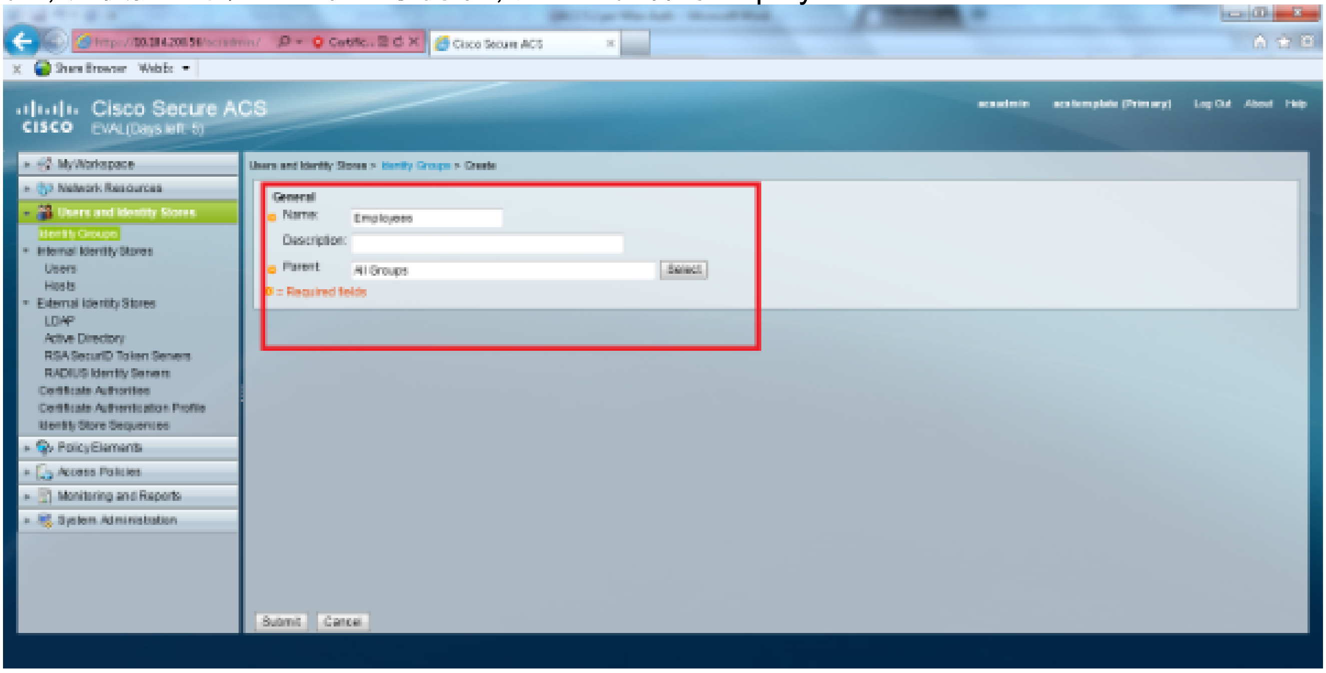
Name: DOT4
Description:

Network Device Groups
Location: All Locations [Select]
Device Type: All Device Types [Select]

IP Address
● Single IP Address ○ IP Range(s)
IP: 10.106.95.4

Authentication Options
TACACS+ □
Shared Secret:
□ Single Connect Device
Legacy TACACS+ Single Connect Support
TACACS+ Draft Compliant Single Connect Support
RADIUS ☑
Shared Secret: XXXXXX
CoA port: 1700
□ Enable KeyWrap
Key Encryption Key:

3. 從ACS GUI中選擇**Users and Identity Stores > Identity Groups**。為員工和承包商建立相應的組，然後按一下**建立**。在此示例中，建立的組名為Employees。

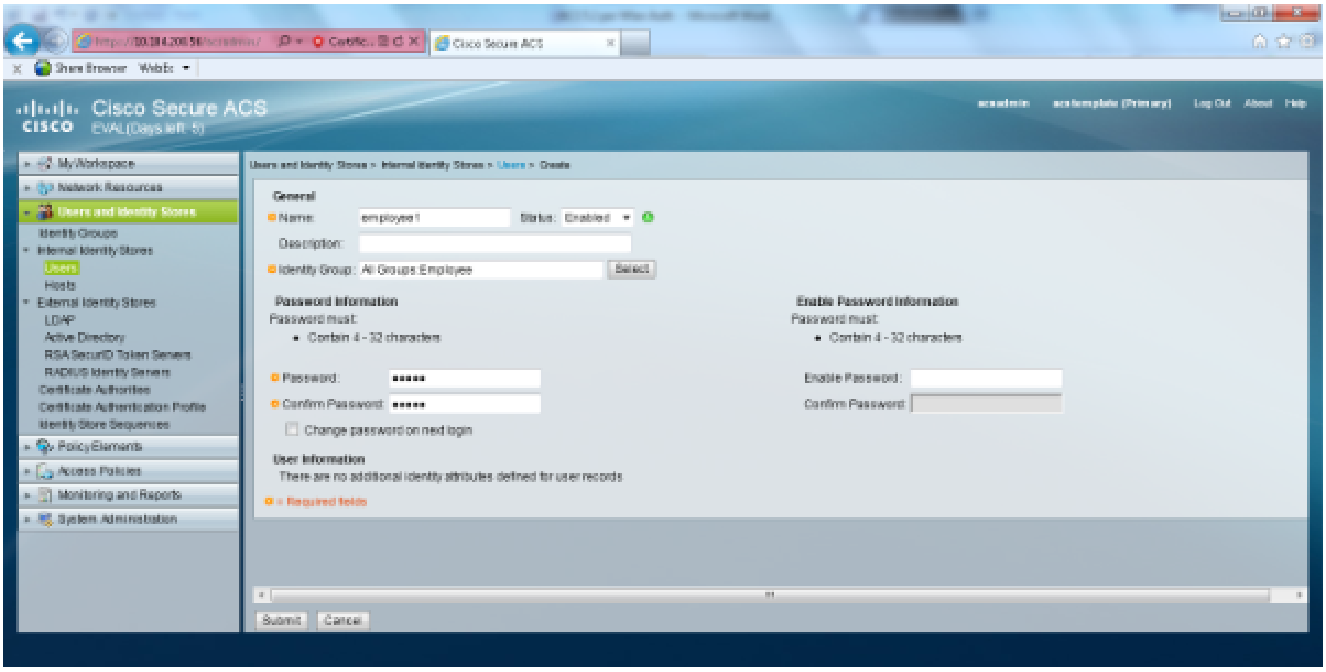


Users and Identity Stores > Identity Groups > Create

General
Name: Employees
Description:
Parent: All Groups [Select]
= Required fields

4. 選擇**Users and Identity Stores > Internal Identity Stores**。按一下「**Create**」，然後輸入使用者名稱。將它們放在正確的組中，定義其密碼，然後按一下**提交**。在此示例中，建立了

Employee組中名為employee1的使用者。同樣，在組contractors下建立一個名為contractor1的使用者。



Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: employee1 Status: Enabled

Description:

Identity Group: All Groups:Employee [Select]

Password Information
Password must:
- Contain 4 - 32 characters

Password: ●●●●●

Confirm Password: ●●●●●

□ Change password on next login

Enable Password Information
Password must:
- Contain 4 - 32 characters

Enable Password:

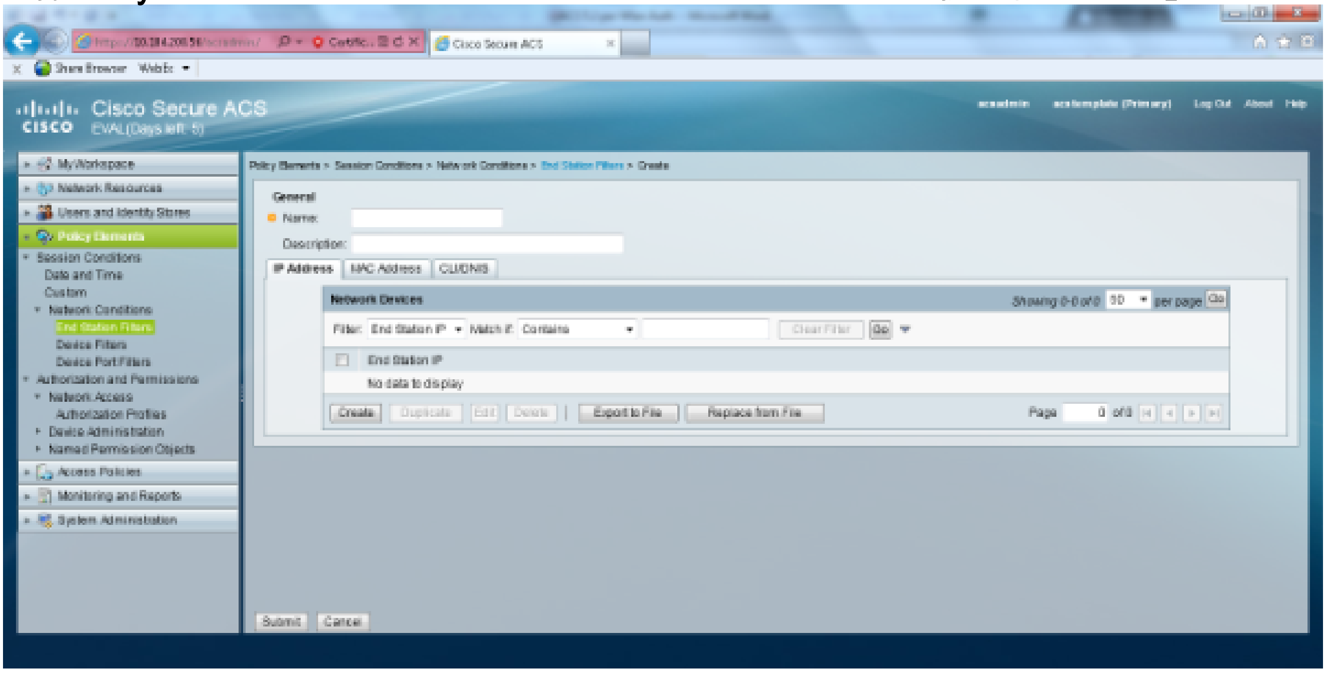
Confirm Password:

User Information
There are no additional identity attributes defined for user records

= Required fields

Submit Cancel

5. 選擇**Policy Elements > Network Conditions > End Station Filters**。按一下「**Create**」。



Policy Elements > Session Conditions > Network Conditions > End Station Filters > Create

General

Name:

Description:

IP Address | MAC Address | CLI/DNIS

Network Devices Showing 0-0 of 0 50 per page Go

Filter: End Station IP Match if: Contains Clear Filter Go

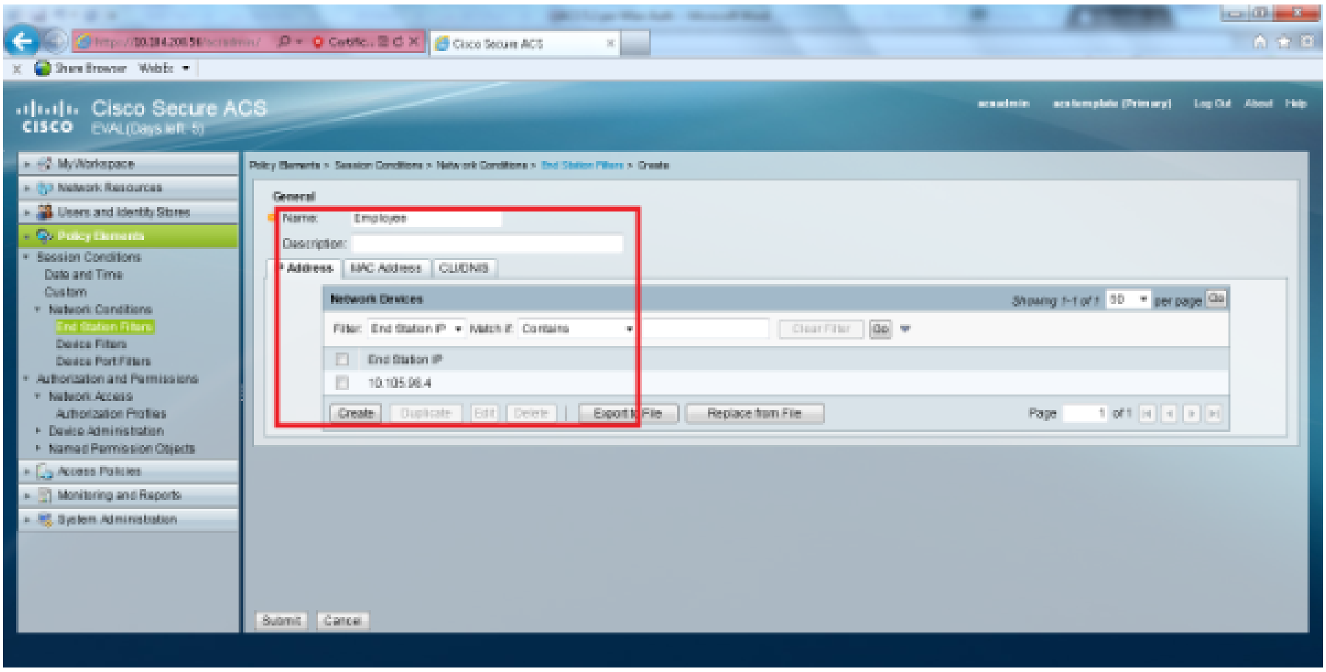
□ End Station IP

No data to display

Create Duplicate Edit Delete Export to File Replace from File Page 0 of 0

Submit Cancel

輸入一個有意義的名稱，然後在**IP address**頁籤下輸入WLC的IP地址。在本示例中，名稱是Employee和Contractor。



Policy Elements > Session Conditions > Network Conditions > End Station Filters > Create

General

Name: Employee

Description:

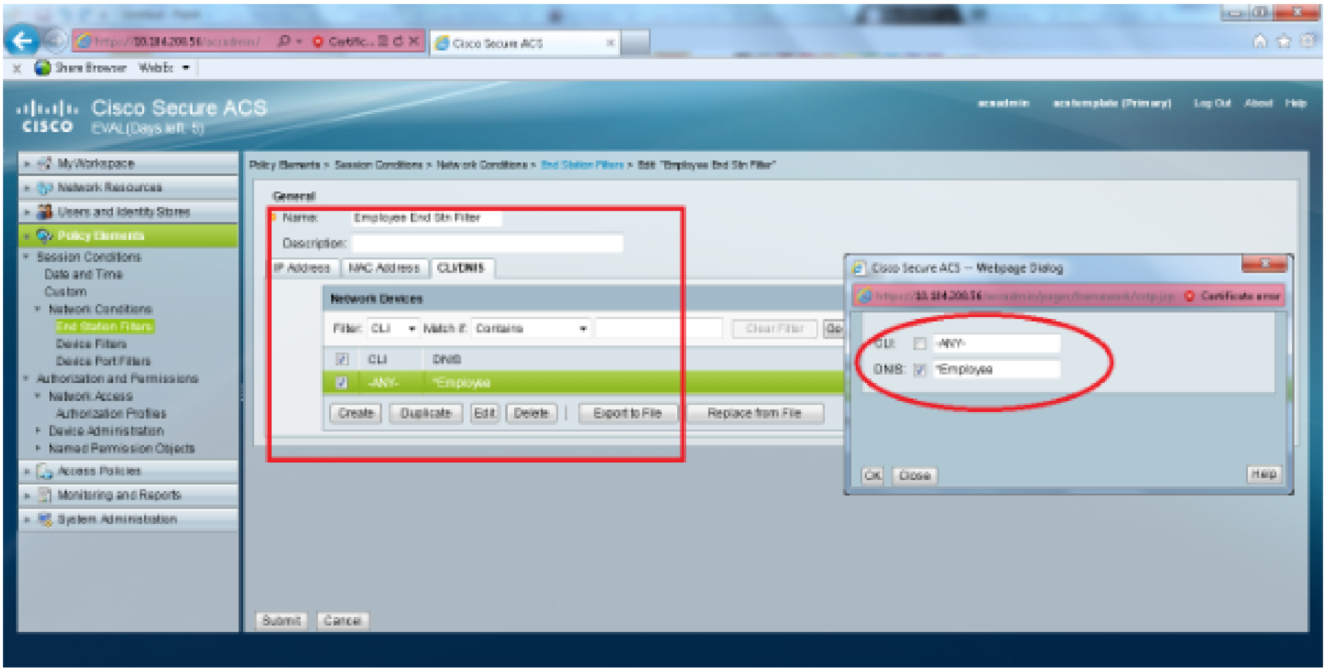
IP Address | MAC Address | CLI/DNIS

Network Devices — Showing 1-1 of 1, 50 per page

Filter: End Station IP, Match if: Contains

☐	End Station IP
☐	10.105.98.4

在CLI/DNIS頁籤下，將CLI保留為 — ANY-，並將DNIS輸入為*<SSID>。在此示例中，DNIS欄位輸入為*Employee，因為此終端站過濾器用於限制僅對員工WLAN的訪問。DNIS屬性定義允許使用者訪問的SSID。WLC將DNIS屬性中的SSID傳送到RADIUS伺服器。對承包商終端站過濾器重複相同步驟。



Policy Elements > Session Conditions > Network Conditions > End Station Filters > Edit: "Employee End Stn Filter"

General

Name: Employee End Stn Filter

Description:

IP Address | MAC Address | CLI/DNIS

Network Devices

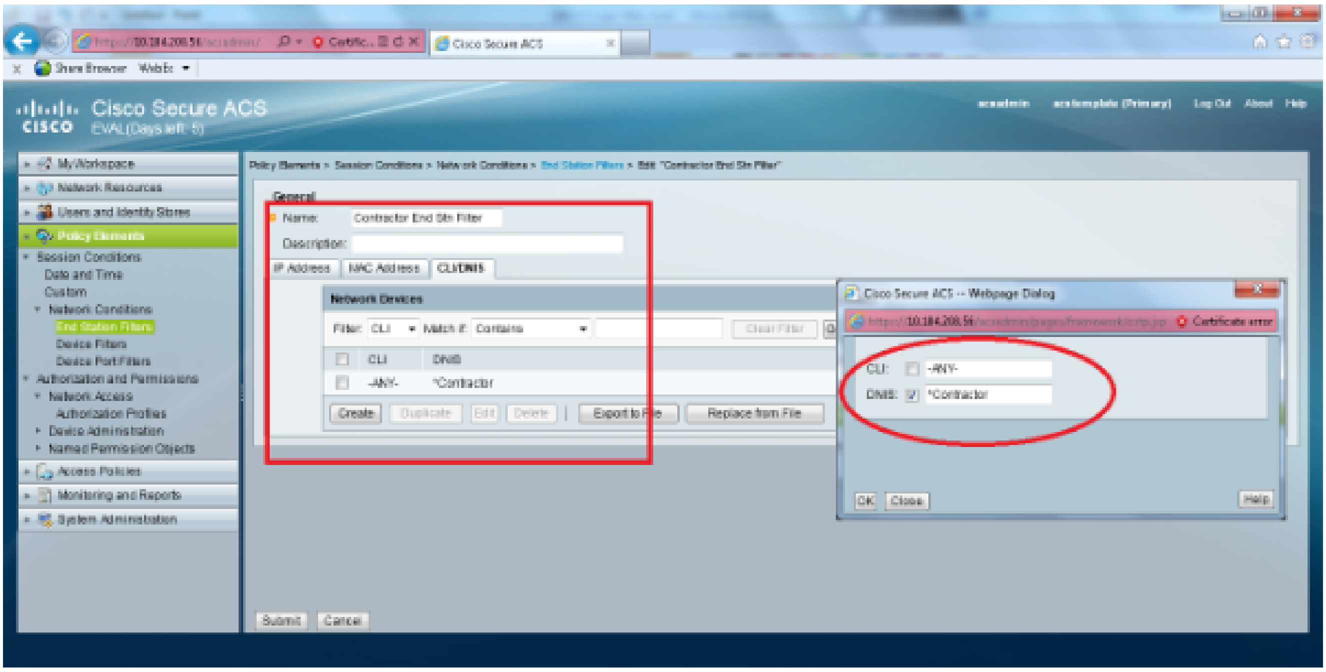
Filter: CLI, Match if: Contains

☑	CLI	DNIS
☑	-ANY-	*Employee

Cisco Secure ACS -- Webpage Dialog

CLI: ☐ -ANY-

DNIS: ☑ *Employee



Policy Elements > Session Conditions > Network Conditions > End Station Filters > Edit "Contractor End Stn Filter"

General

Name: Contractor End Stn Filter

Description:

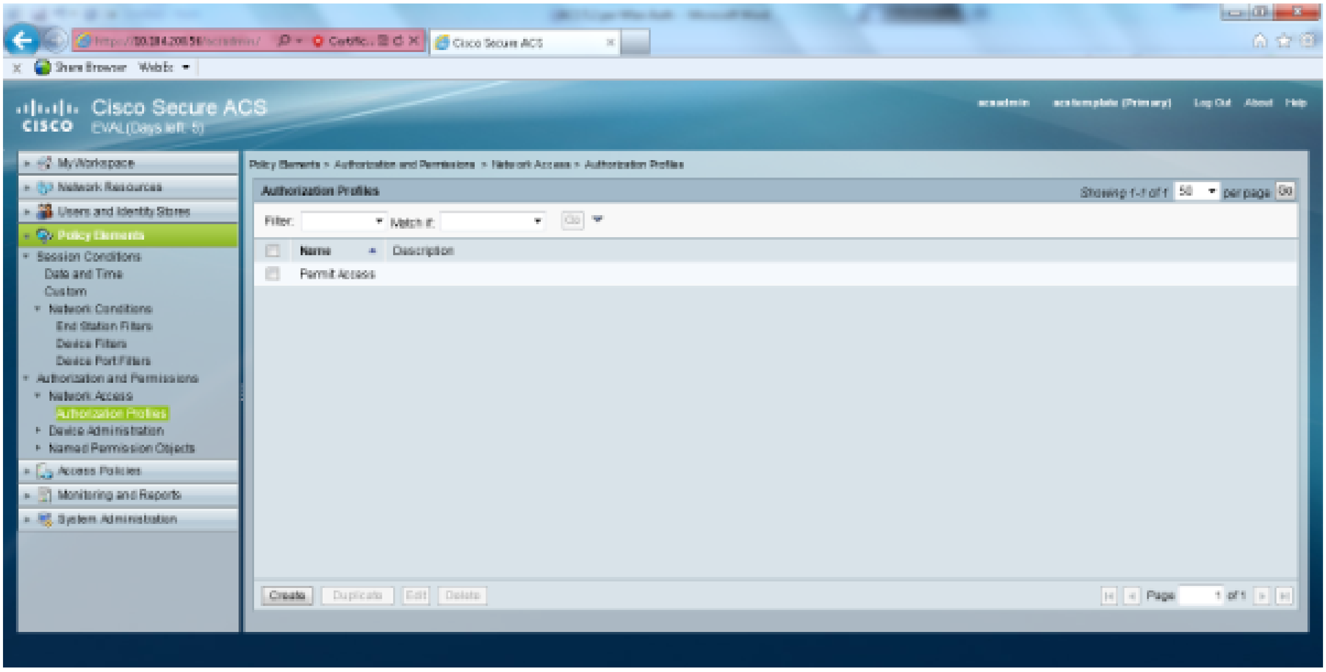
□	CLI	DNIS
□	-ANY-	*Contractor

Cisco Secure ACS -- Webpage Dialog

CLI: □ -ANY-

DNIS: ☑ *Contractor

6. 選擇**Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**。Permit Access應該有一個預設配置檔案。

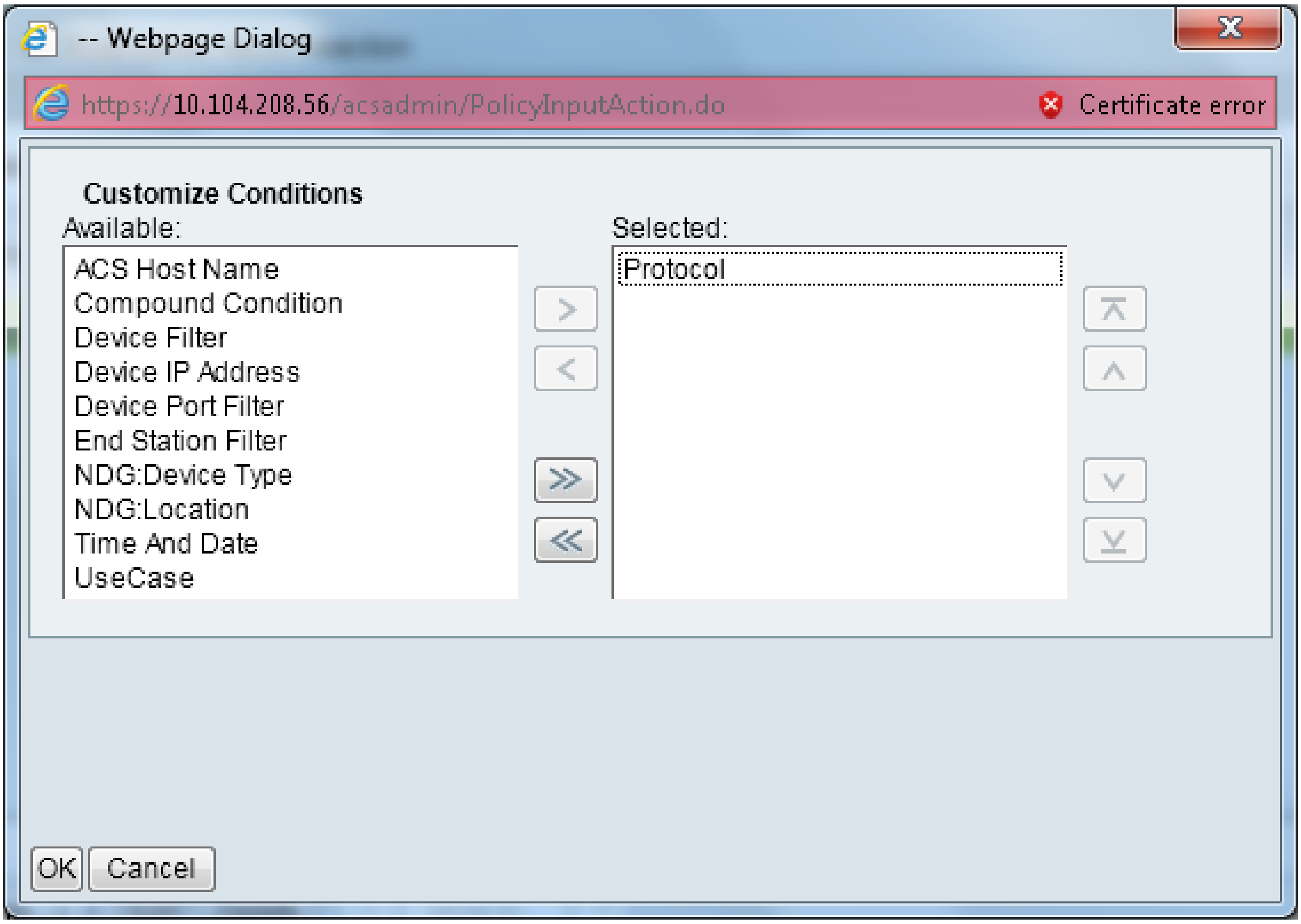


Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles

Authorization Profiles

□	Name	Description
□	Permit Access	

7. 選擇**Access Policies > Access Services > Service Selection Rules**。按一下「**Customize**」。新增任何適當的條件。此範例使用Protocol as Radius作為匹配條件。按一下「**Create**」。命名規則。選擇**Protocol**，然後選擇**Radius。**在**Results**下，選擇適當的訪問服務。在本例中，保留為**Default Network Access**。



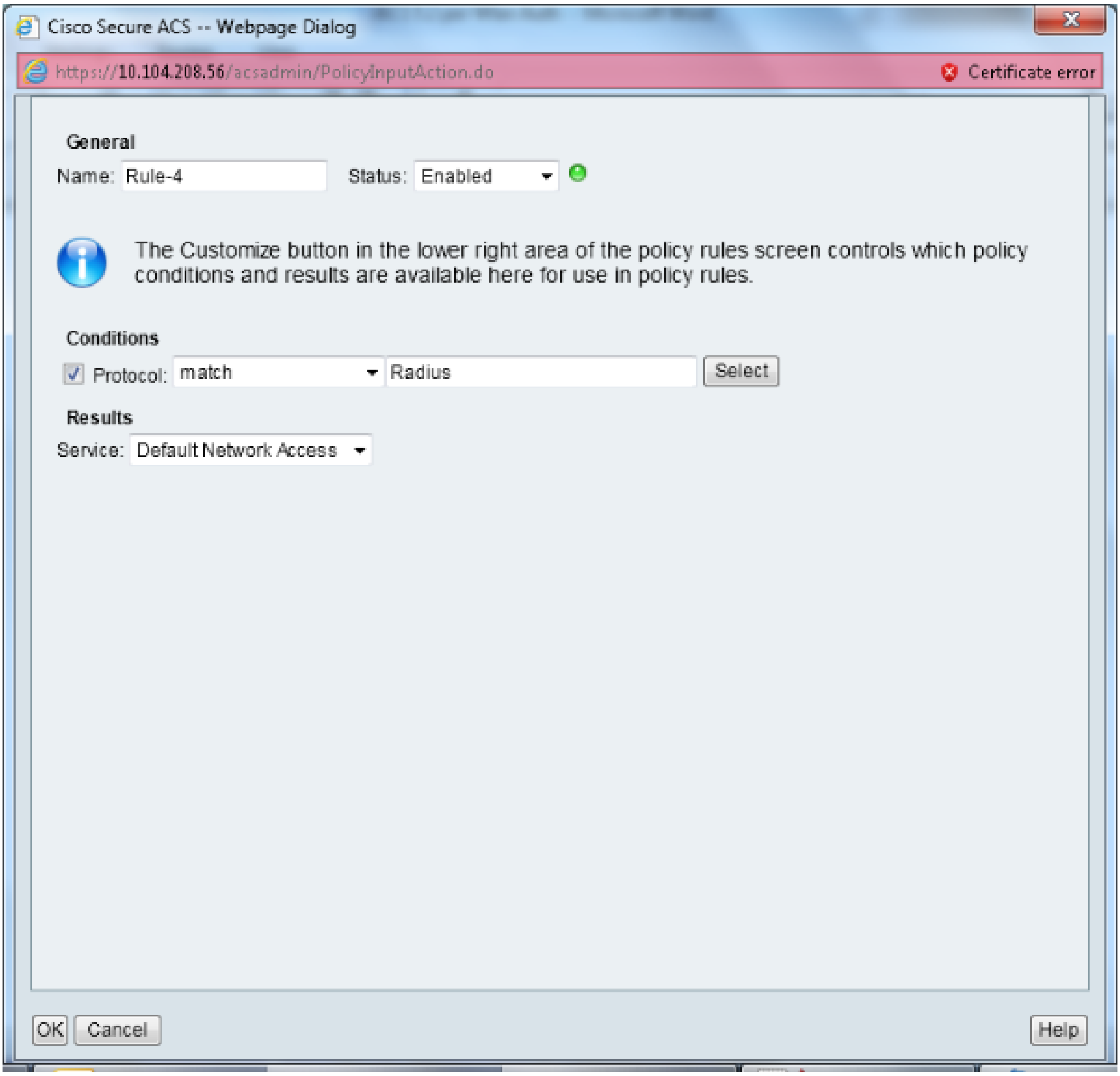
Customize Conditions

Available:

ACS Host Name
Compound Condition
Device Filter
Device IP Address
Device Port Filter
End Station Filter
NDG:Device Type
NDG:Location
Time And Date
UseCase

Selected:

Protocol



Cisco Secure ACS -- Webpage Dialog

https://10.104.208.56/acsadmin/PolicyInputAction.do Certificate error

General

Name: Rule-4

Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

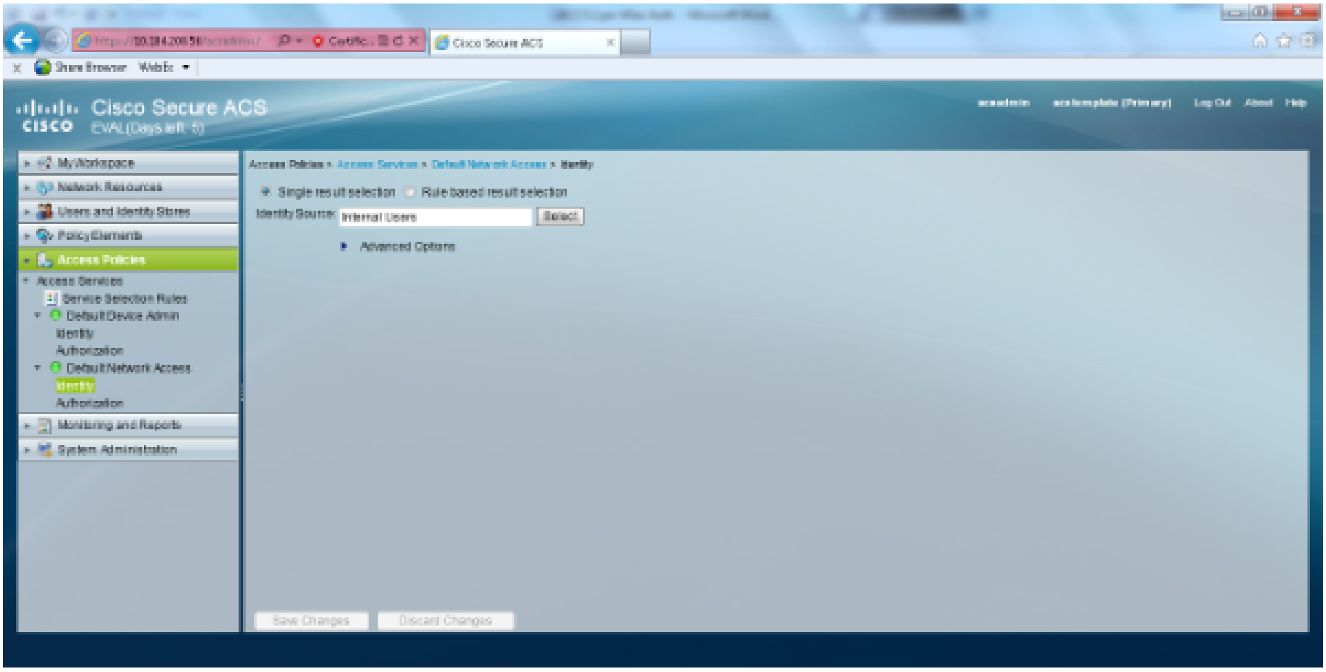
Conditions

☑ Protocol: match Radius

Results

Service: Default Network Access

8. 選擇**Access Policies > Access Services > Default Network Access > Identity**。選擇單個結果選擇和**身份源**作為內部使用者。



Cisco Secure ACS

EVAL(Days left: 5)

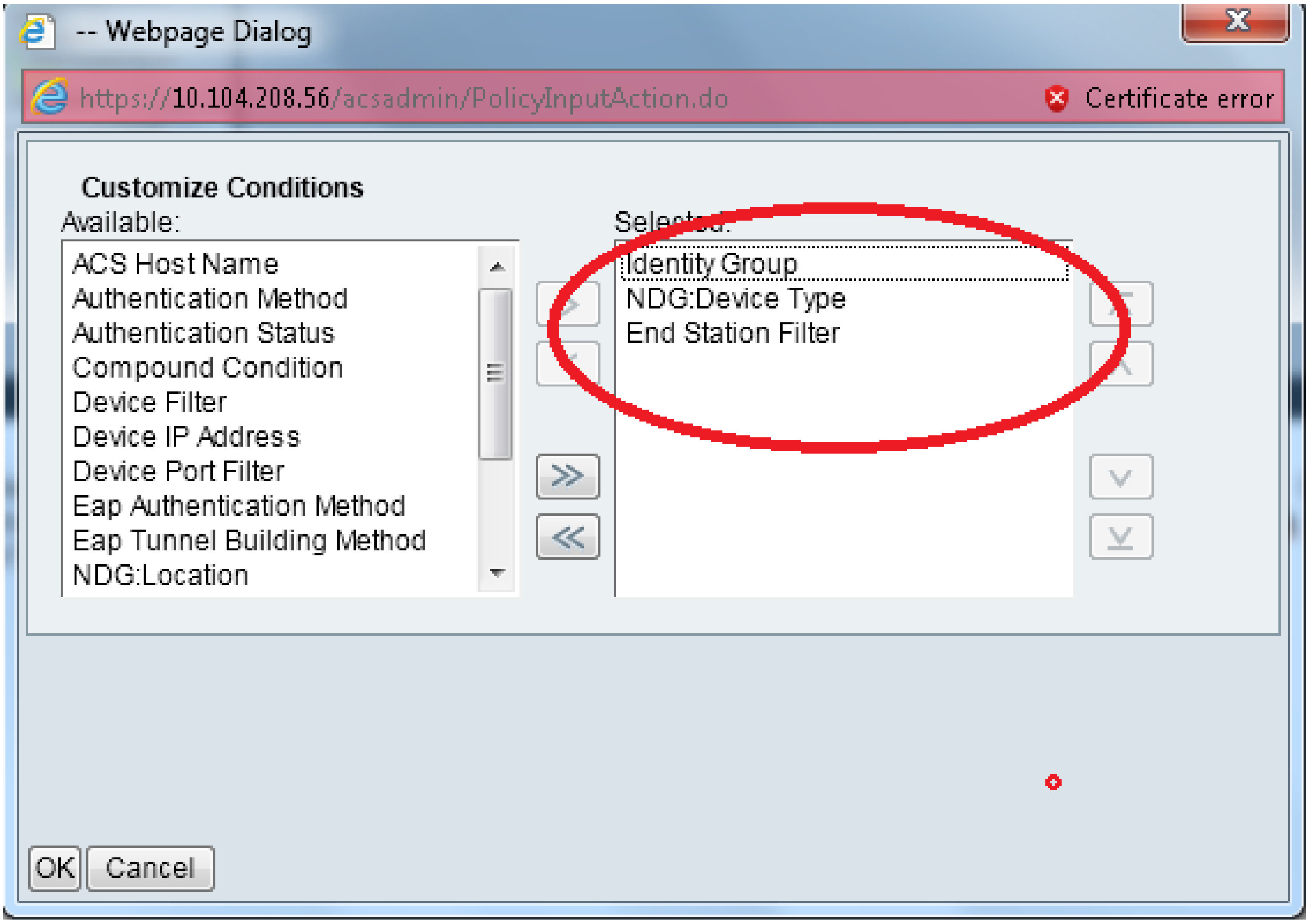
acsadmin acstemplate (Primary)

Access Policies > Access Services > Default Network Access > Identity

● Single result selection ○ Rule based result selection

Identity Source: Internal Users

選擇**Access Policies > Access Services > Default Network Access > Authorization**。單擊**Customize**並新增自定義條件。此示例按順序使用身份組、NDG：裝置型別和終端站過濾器。



-- Webpage Dialog

https://10.104.208.56/acsadmin/PolicyInputAction.do

Certificate error

Customize Conditions

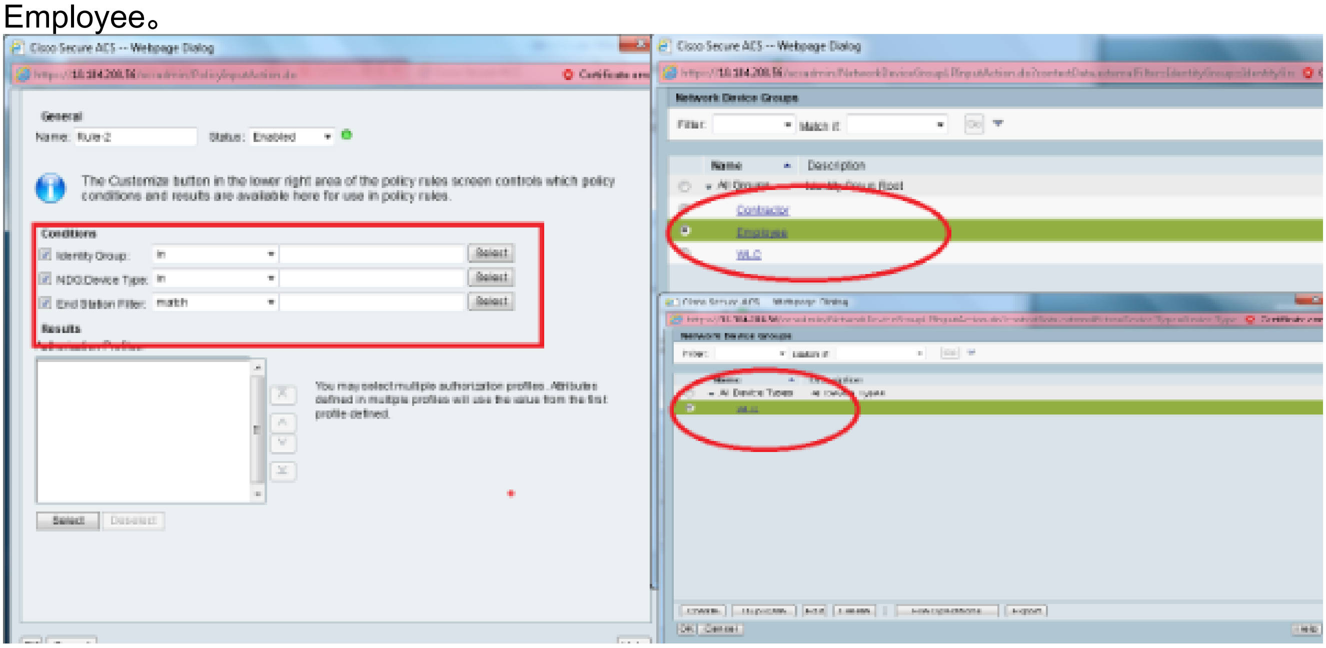
Available:

- ACS Host Name
- Authentication Method
- Authentication Status
- Compound Condition
- Device Filter
- Device IP Address
- Device Port Filter
- Eap Authentication Method
- Eap Tunnel Building Method
- NDG:Location

Selected:

- Identity Group
- NDG:Device Type
- End Station Filter

按一下「**Create**」。命名規則並在「所有組」下選擇適當的身份組。在本示例中，它是Employee。



Cisco Secure ACS -- Webpage Dialog

General

Name: Rule-2 Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

- ☑ Identity Group: in
- ☑ NDG:Device Type: in
- ☑ End Station Filter: match

Results

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

Cisco Secure ACS -- Webpage Dialog

Network Device Groups

Filter: Match if:

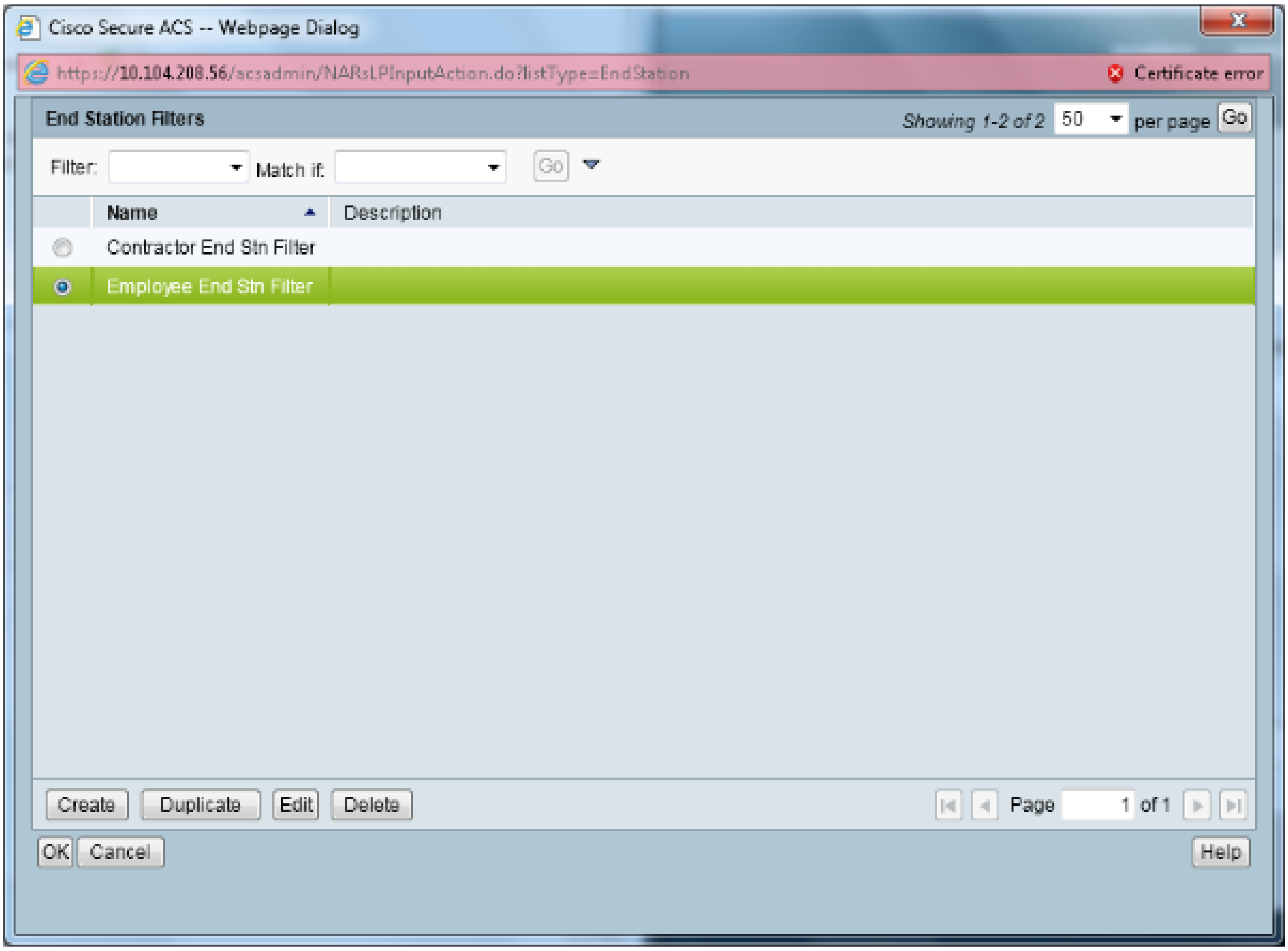
	Name	Description
○	All Groups	Identity Group Root
○	Contractor	
●	Employee	
○	WLC	

Cisco Secure ACS -- Webpage Dialog

Network Device Groups

	Name	Description
○	All Device Types	All Device Types
●	WLC	

按一下「**Employee End Stn Filter**」單選按鈕，或輸入在「Configure the WLC」一節的步驟1b中輸入的名稱。



Cisco Secure ACS -- Webpage Dialog

https://10.104.208.56/acsadmin/NARsLPInputAction.do?listType=EndStation

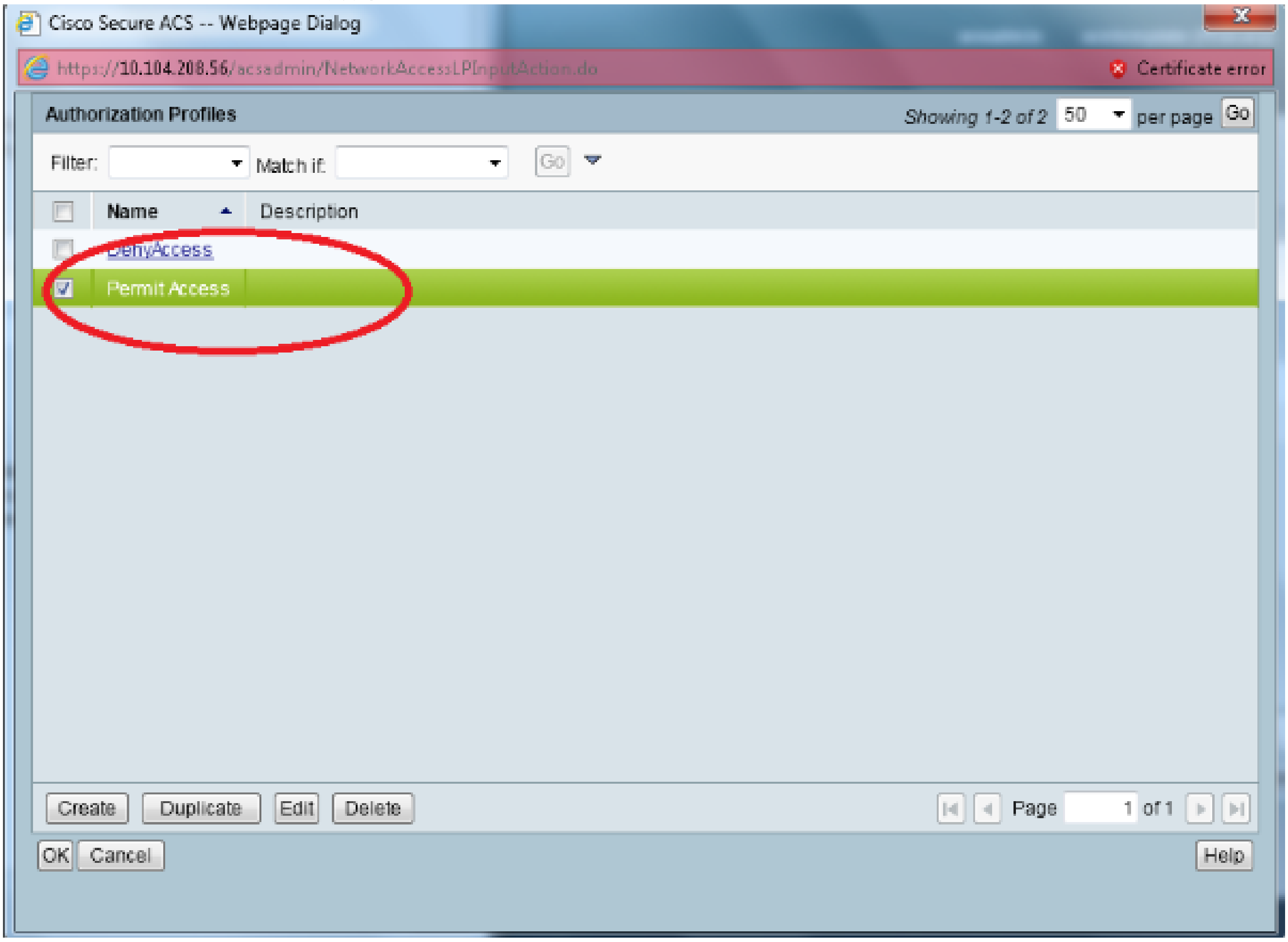
Certificate error

End Station Filters — Showing 1-2 of 2 | 50 per page | Go

Filter: | Match if: | Go

	Name	Description
○	Contractor End Stn Filter	
●	Employee End Stn Filter	

勾選「**Permit Access**」覈取方塊。



Cisco Secure ACS -- Webpage Dialog

https://10.104.208.56/acsadmin/NetworkAccessLPInputAction.do

Certificate error

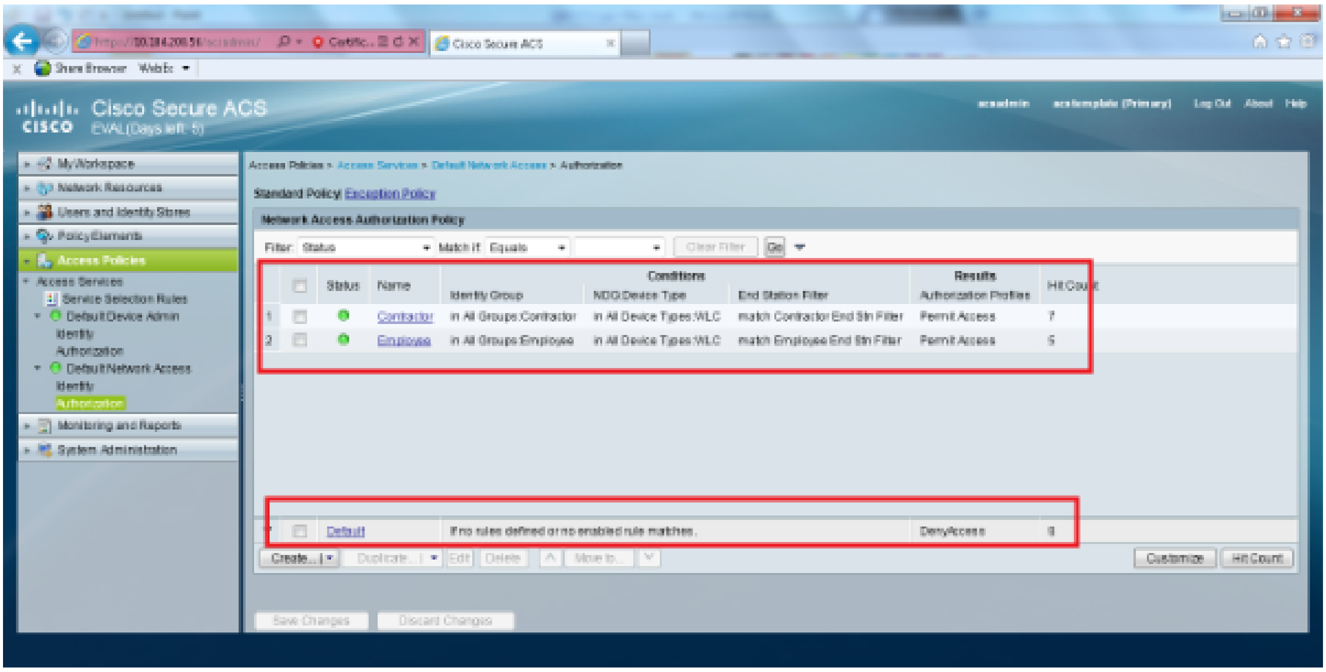
Authorization Profiles — Showing 1-2 of 2 | 50 per page | Go

Filter: | Match if: | Go

□	Name	Description
□	DenyAccess	
☑	Permit Access	

對「承包商規則」也重複上述相同步驟。確保預設操作為**Deny Access**。 完成步驟e後，規則

應如下所示
：



Access Policies > Access Services > Default Network Access > Authorization

Standard Policy Exception Policy

Network Access Authorization Policy

Filter: Status Match if: Equals

	☐	Status	Name	Conditions			Results	Hit Count
				Identity Group	NDG:Device Type	End Station Filter	Authorization Profiles	
1	☐	●	Contractor	in All Groups:Contractor	in All Device Types:WLC	match Contractor End Stn Filter	Permit Access	7
2	☐	●	Employee	in All Groups:Employee	in All Device Types:WLC	match Employee End Stn Filter	Permit Access	5
	☐		Default	If no rules defined or no enabled rule matches.			DenyAccess	0

配置到此結束。在本節之後，需要使用SSID和安全引數相應地配置客戶端以進行連線。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。