ACS 5.2版和WLC的每WLAN身份验证配置示例

目录

简介

本文档提供一个配置示例，根据服务集标识符(SSID)限制每个用户对无线LAN(WLAN)的访问。

先决条件

要求

Cisco 建议您了解以下主题：

- 如何针对基本运行来配置无线 LAN 控制器 (WLC) 和轻量接入点 (LAP)
- 如何配置思科安全访问控制服务器(ACS)
- 轻量接入点协议 (LWAPP) 和无线安全方法

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本7.4.110的Cisco 5500系列WLC
- Cisco 1142 系列 LAP
- 思科安全ACS服务器版本5.2.0.26.11

配置

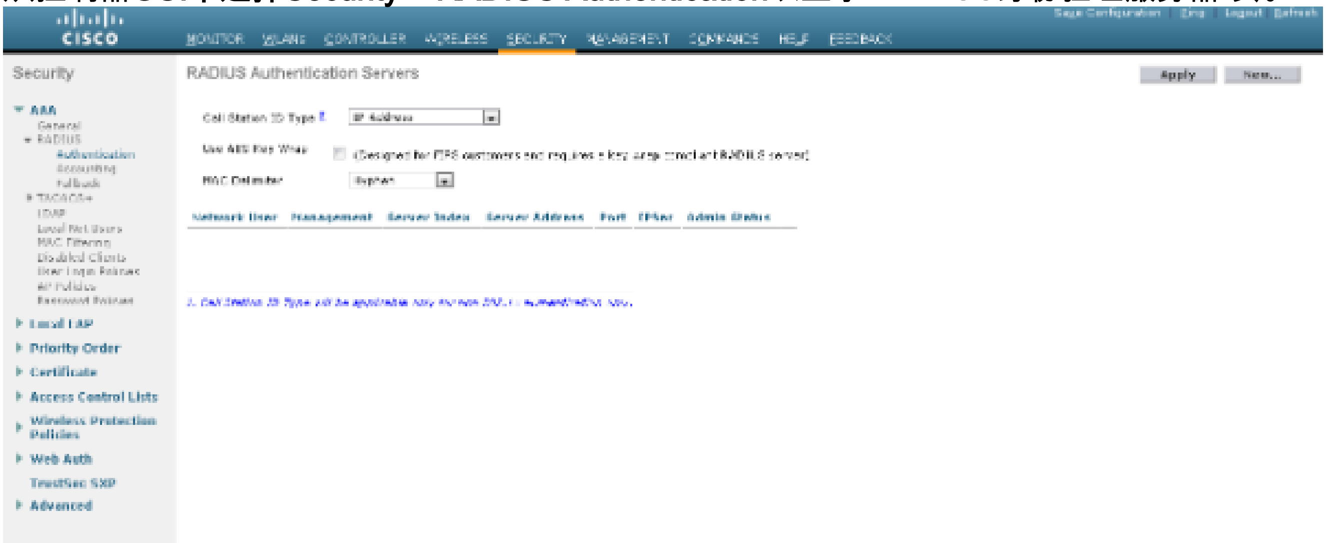
为了针对此设置配置设备，您需要：

1. 需要为 WLC 配置两个 WLAN 和 RADIUS 服务器。
2. 配置 Cisco Secure ACS。
3. 配置无线客户端并检验配置。

配置 WLC

要配置 WLC 使用该设置，请完成以下步骤：

1. 配置WLC以将用户凭证转发到外部RADIUS服务器。外部 RADIUS 服务器（在这种情况下是 Cisco Secure ACS）然后验证用户凭证并提供对无线客户端的访问权限。请完成以下步骤：从控制器**GUI中选择Security > RADIUS Authentication**以显示“RADIUS身份验证服务器”页。



RADIUS Authentication Servers

Call Station ID Type 1: IP Address

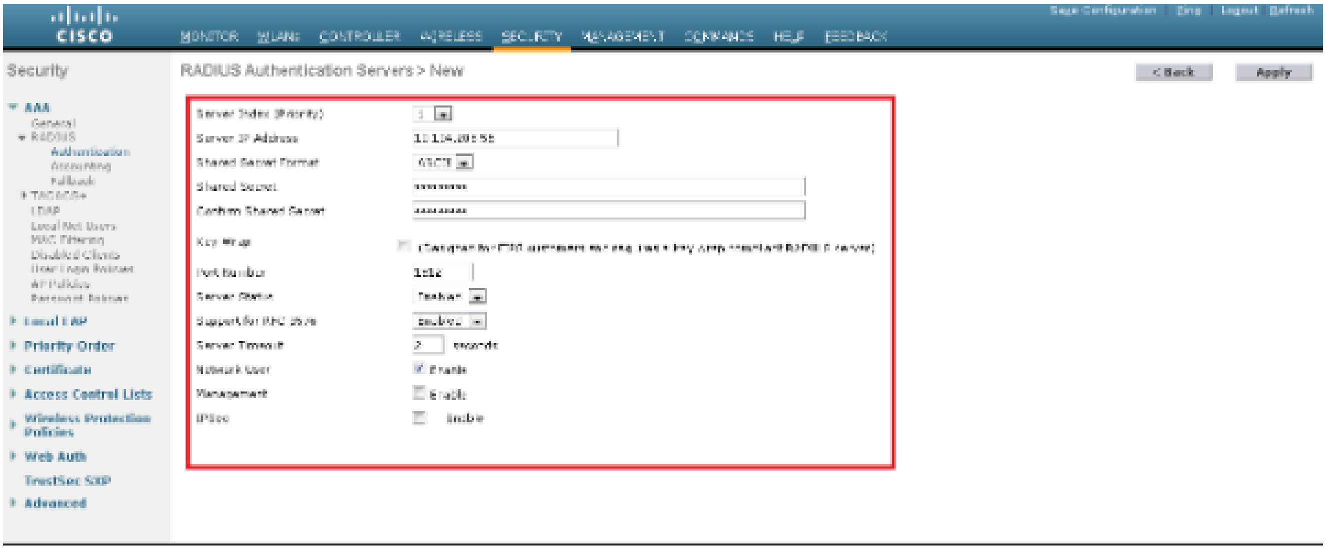
Use AES Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

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.

单击 New 以定义 RADIUS 服务器参数。 这些参数包括 RADIUS 服务器的 IP 地址、共享密钥、端口号和服务器状态。网络用户和管理复选框确定基于RADIUS的身份验证是否适用于管理和网络用户。此示例使用Cisco Secure ACS作为IP地址为10.104.208.56的 RADIUS服务器。

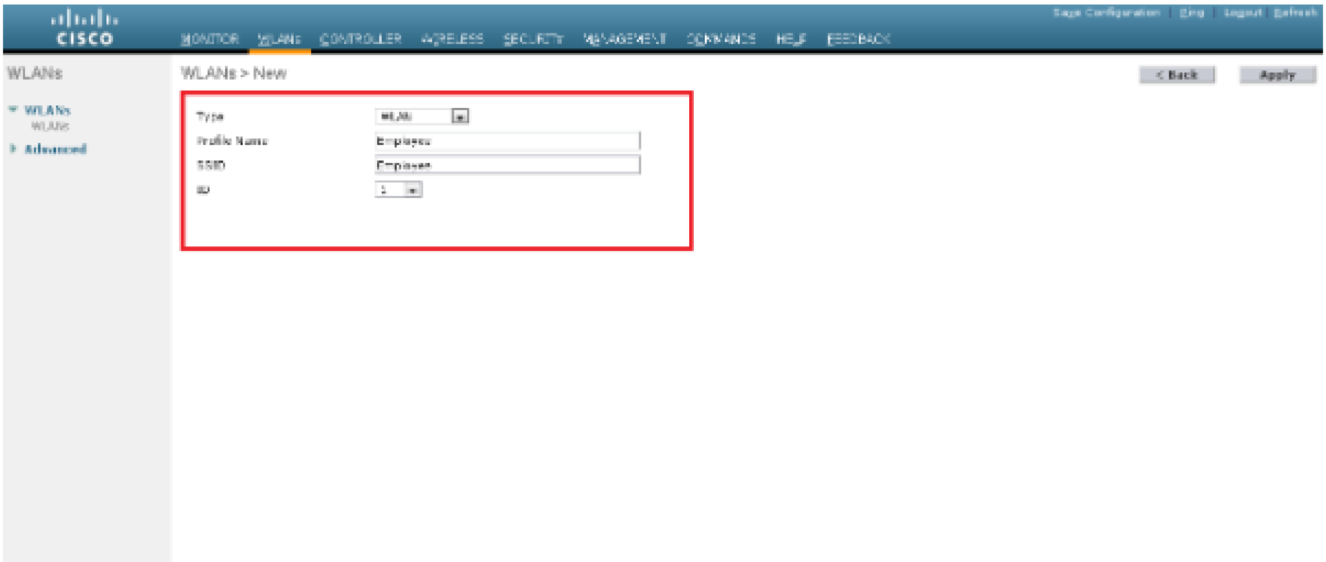


RADIUS Authentication Servers > New

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

单击 **Apply**。

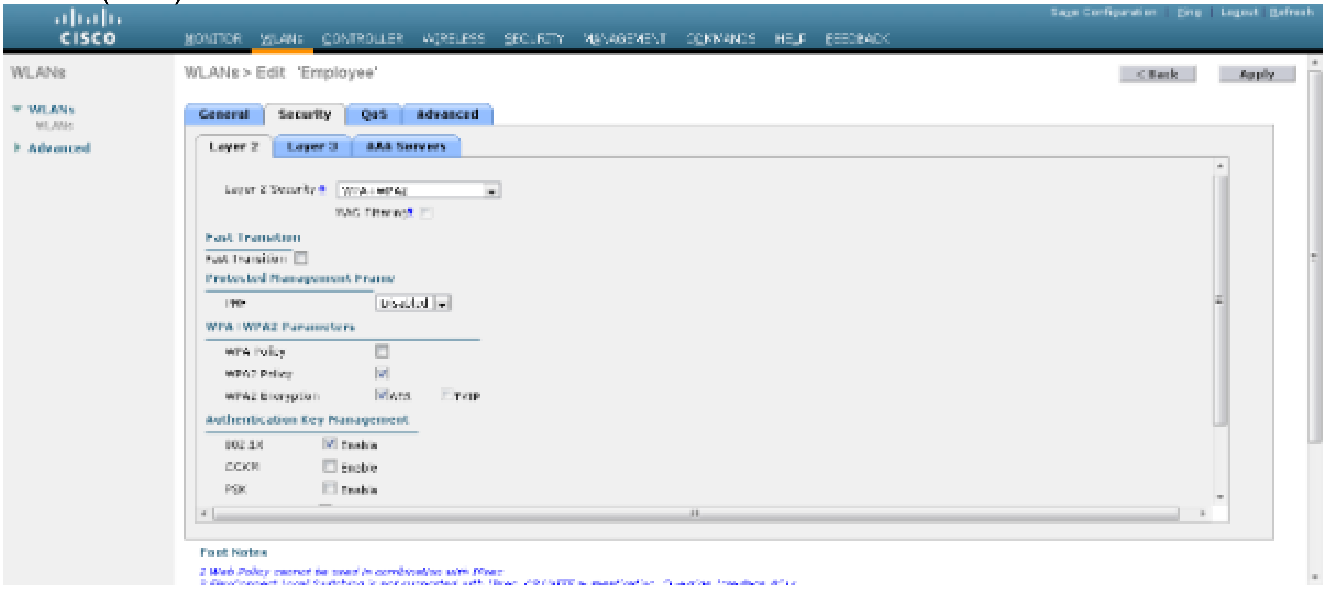
2. 完成以下步骤，为具有SSID Employee的员工配置一个WLAN，为具有SSID Contractor的承包商配置**一个**WLAN，为另一个WLAN配置**SSID Contractor**。 要创建 WLAN，请从控制器 GUI 中单击 **WLANs。**随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。要配置新的 WLAN，请单击 **New。**此示例创建名为Employee的WLAN，WLAN ID为1。单击“应**用”**。



WLANs > New

Type: WLAN
Profile Name: Employee
SSID: Employee
ID: 1

选择“WLAN**”>“编辑**”窗口并定义特定于WLAN的参数： 从Layer 2 Security选项卡中，选**择802.1x**。默认情况下，Layer 2 Security 选项为 802.1x。这为WLAN启用802.1 x/可扩展身份验证协议(EAP)身份验证。



WLANs > Edit 'Employee'

Layer 2 Security: WPA+WPA2
MAC Filtering ☐

Fast Transition
Fast Transition ☐

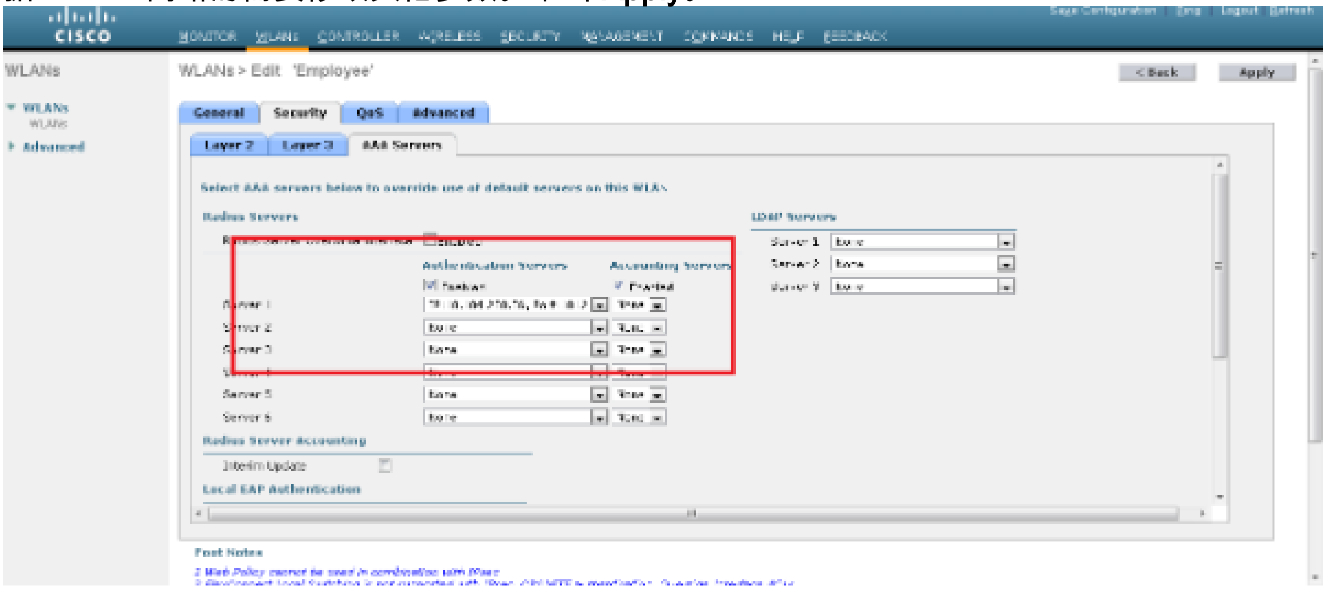
Protected Management Frame
PMF: Disabled

WPA+WPA2 Parameters
WPA Policy ☐
WPA2 Policy ☑
WPA2 Encryption ☑AES ☐TKIP

Authentication Key Management
802.1X ☑ Enable
CCKM ☐ Enable
PSK ☐ Enable

Foot Notes

从AAA服务器选项卡，从RADIUS服务器下的下拉列表中选择适当的RADIUS服务器。可以根据 WLAN 网络的需要修改其他参数。单击 **Apply**。



WLANs > Edit 'Employee'

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

Radius Servers

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	[illegible]	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

LDAP Servers
Server 1: None
Server 2: None
Server 3: None

Radius Server Accounting
Interim Update ☐

Local EAP Authentication

Foot Notes

同样，要为承包商创建WLAN，请重复步骤b到d。

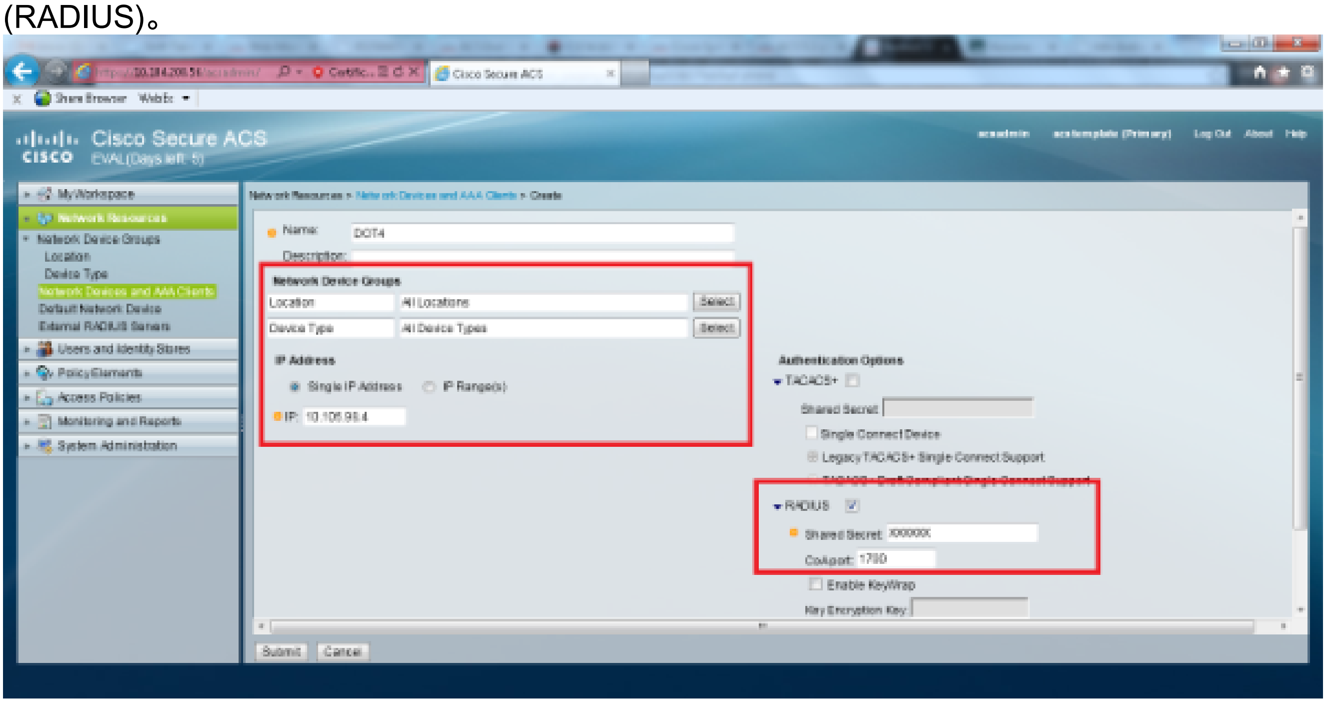
配置 Cisco Secure ACS

在 Cisco Secure ACS 服务器上，您需要：

1. 配置 WLC 作为 AAA 客户端。
2. 为基于SSID的身份验证创建用户数据库（凭证）。
3. 启用 EAP 认证。

在 Cisco Secure ACS 上完成以下步骤：

1. 要将控制器定义为ACS服务器上的AAA客户端，请从ACS GUI中选择**Network Resources > Network Devices and AAA Clients**。在Network Devices and AAA Clients下，单击**Create**。
2. 当Network Configuration页面显示时，定义WLC的名称、IP地址和共享密钥和身份验证方法(RADIUS)。



Network Resources > Network Devices and AAA Clients > Create

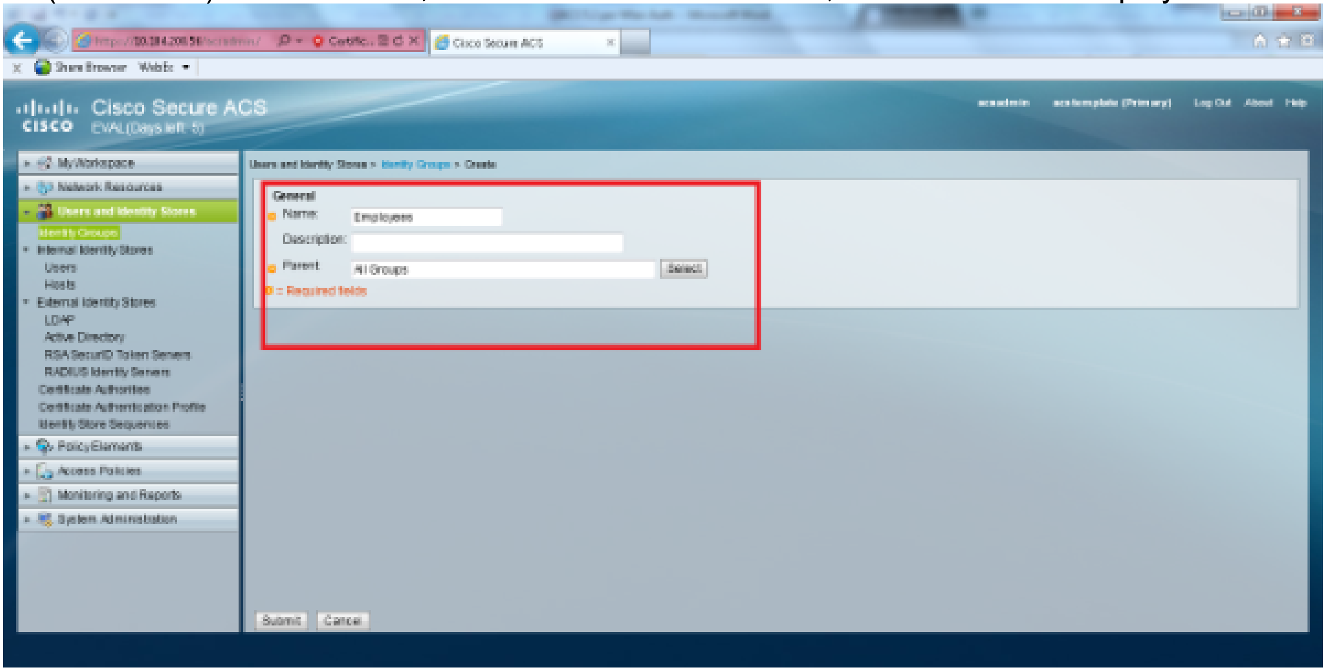
Name: DOT4
Description:

Network Device Groups
Location: All Locations
Device Type: All Device Types

IP Address
● Single IP Address ○ IP Range(s)
IP: 10.105.95.4

Authentication Options
TACACS+ □
Shared Secret:
□ Single Connect Device
RADIUS ☑
Shared Secret: xxxxxxx
CoA port: 1700
□ Enable KeyWrap
Key Encryption Key:

3. 从ACS **GUI中选择Users and Identity Stores > Identity Groups。**为“员工”(Employee)和“承包商”(Contractor)创建各自的组，然后单**击“创建**”。在本例中，创建的组命名为Employees。

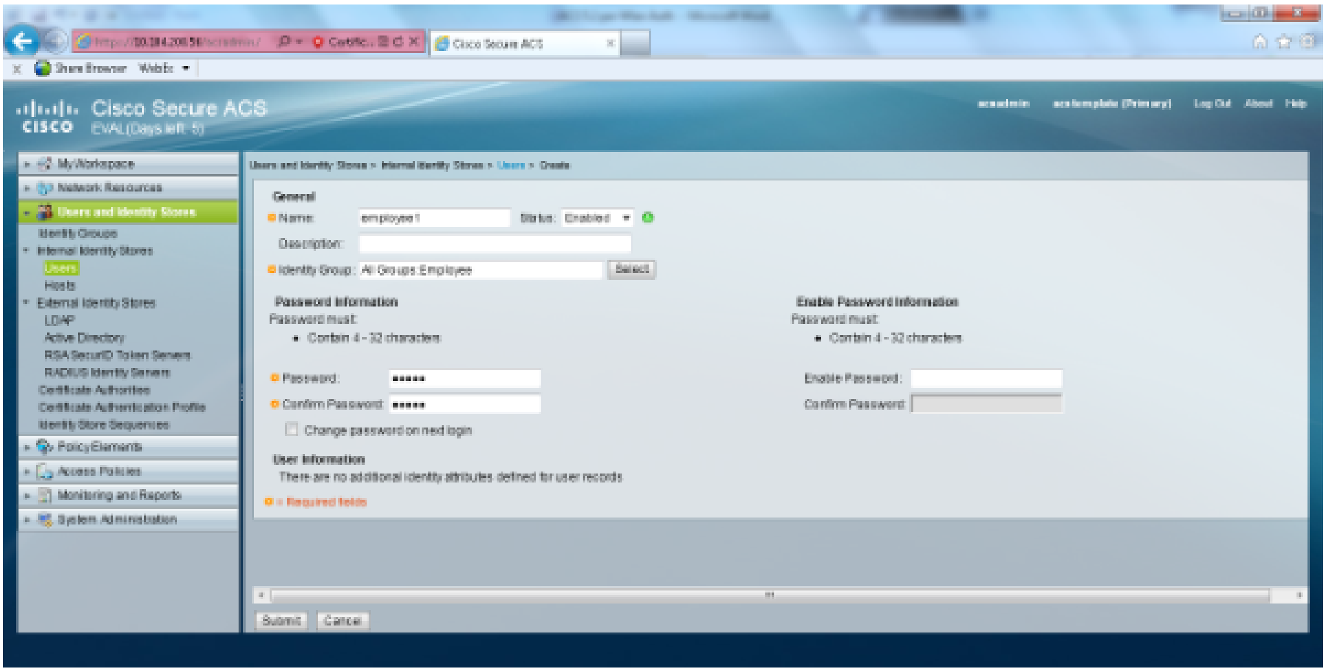


Users and Identity Stores > Identity Groups > Create

General
Name: Employees
Description:
Parent: All Groups
= Required fields

4. 选择**用户和身份库>内部身份库**。单击**Create**并输入用户名。将其放在正确的组中，定义其密

码，然后单击**提交**。在本示例中，创建了组Employee中名为employee1的用户。同样，在组承包商下创建名为contractor1的用户。



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

General

Name: employee1 Status: Enabled

Description:

Identity Group: All Groups:Employee

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:

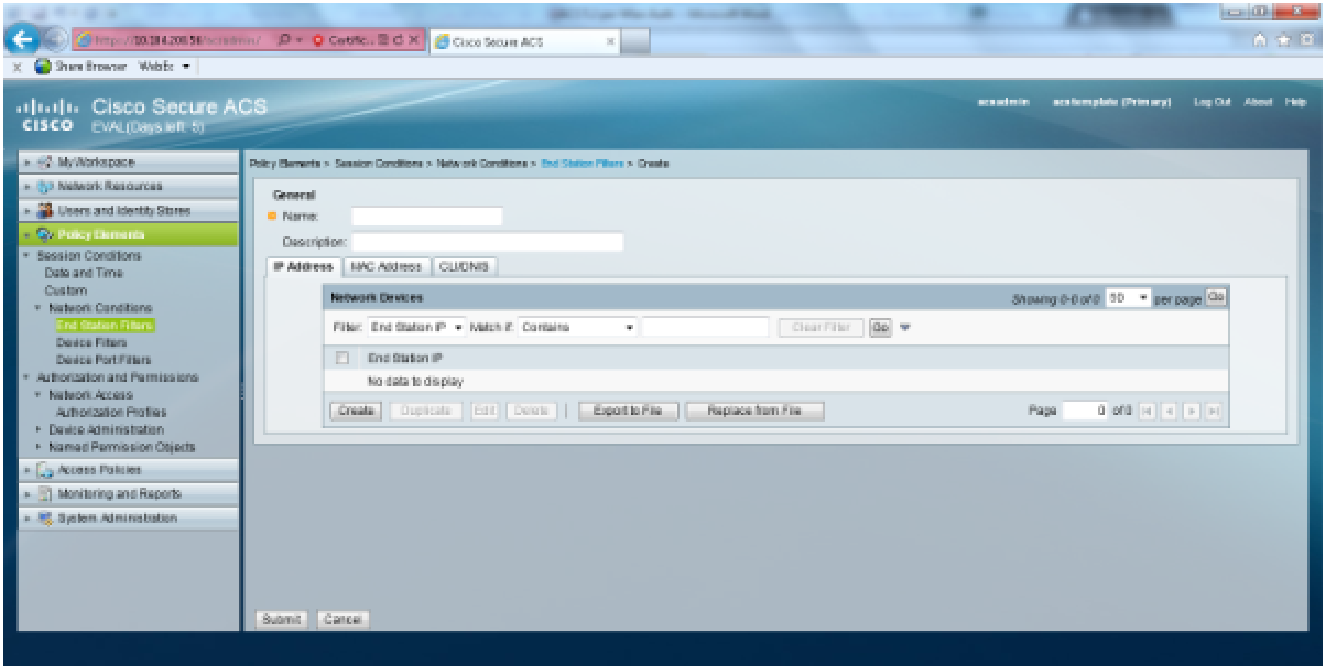
Confirm Password:

User Information

There are no additional identity attributes defined for user records

= Required fields

5. 选择**策略元素>网络条件>终端站过滤器**。Click **Create**.



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

General

Name:

Description:

Network Devices Showing 0-0 of 0 50 per page

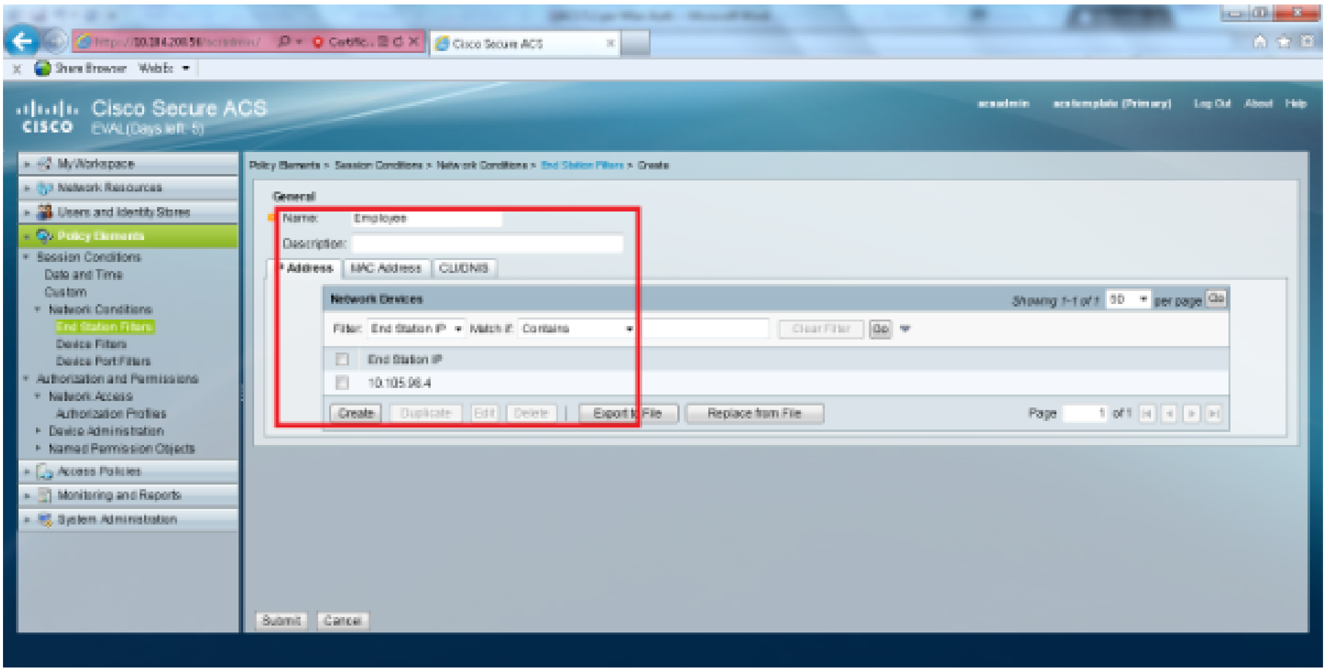
Filter: End Station IP Match if: Contains

□ End Station IP

No data to display

Page 0 of 0

输入有意义的名称，在“IP地址”选项卡下输入WLC的IP地址。在本例中，名称为Employee和Contractor。


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

General

Name: Employee

Description:

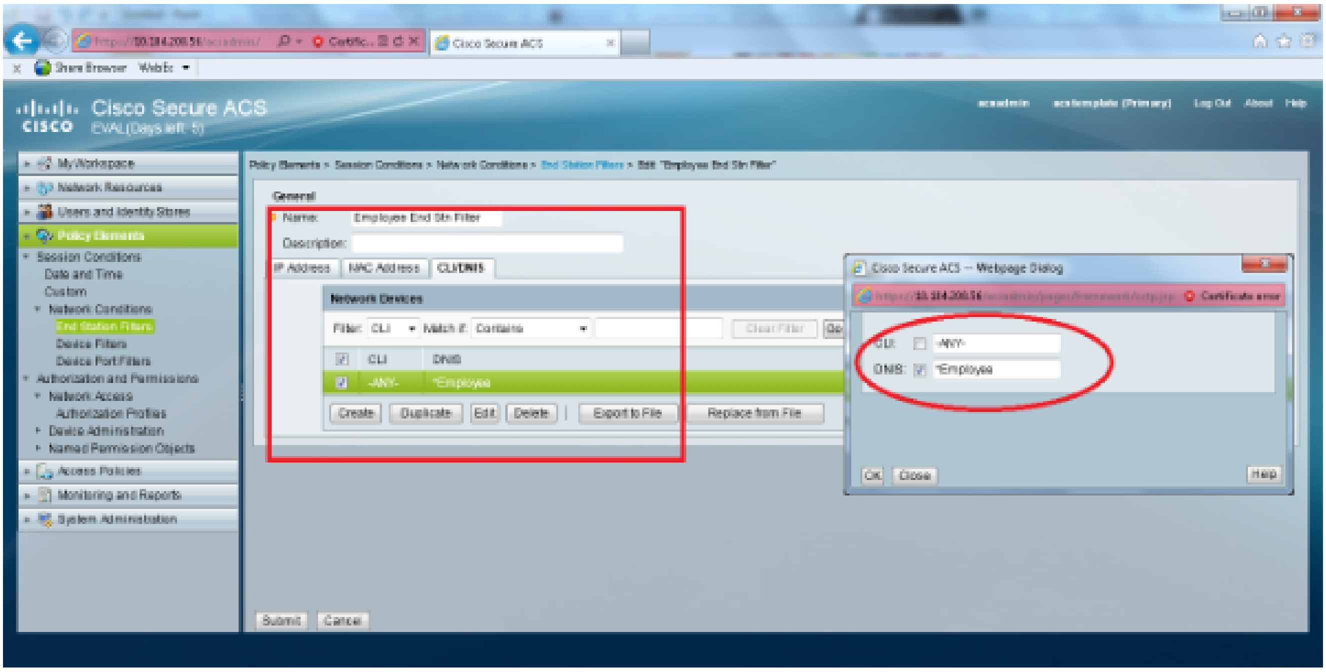
IP Address | MAC Address | CLI/DNIS

Network Devices

Filter: End Station IP Match if: Contains

☐	End Station IP
☐	10.105.98.4

在CLI/DNIS选项卡下，将CLI保留为 — ANY-，并输入DNIS作为*<SSID>。在本示例中，DNIS字段输入为*Employee，因为此终端站过滤器仅用于限制对员工WLAN的访问。DNIS属性定义了允许用户访问的 SSID。WLC 将 DNIS 属性中的 SSID 发送到 RADIUS 服务器。对承包商终端站过滤器重复相同步骤。


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

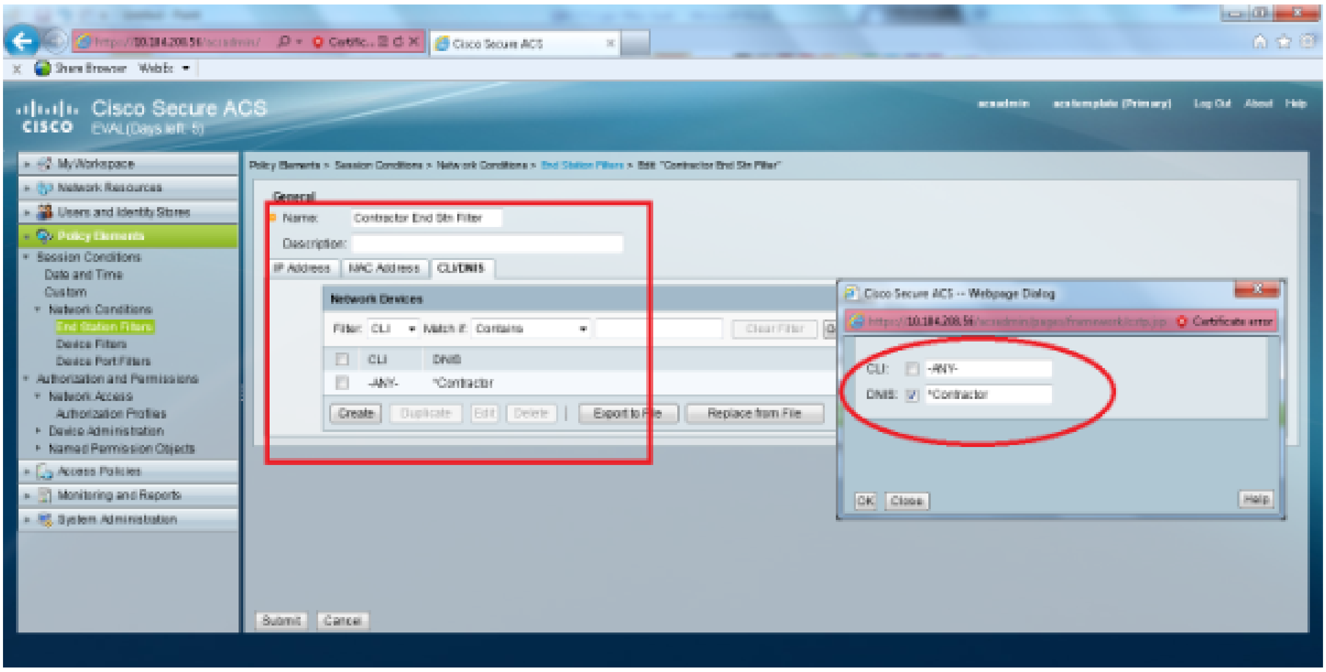
Filter: CLI Match if: Contains

☑	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:

IP Address | MAC Address | CLI/DNIS

Network Devices

Filter: CLI Match if: Contains

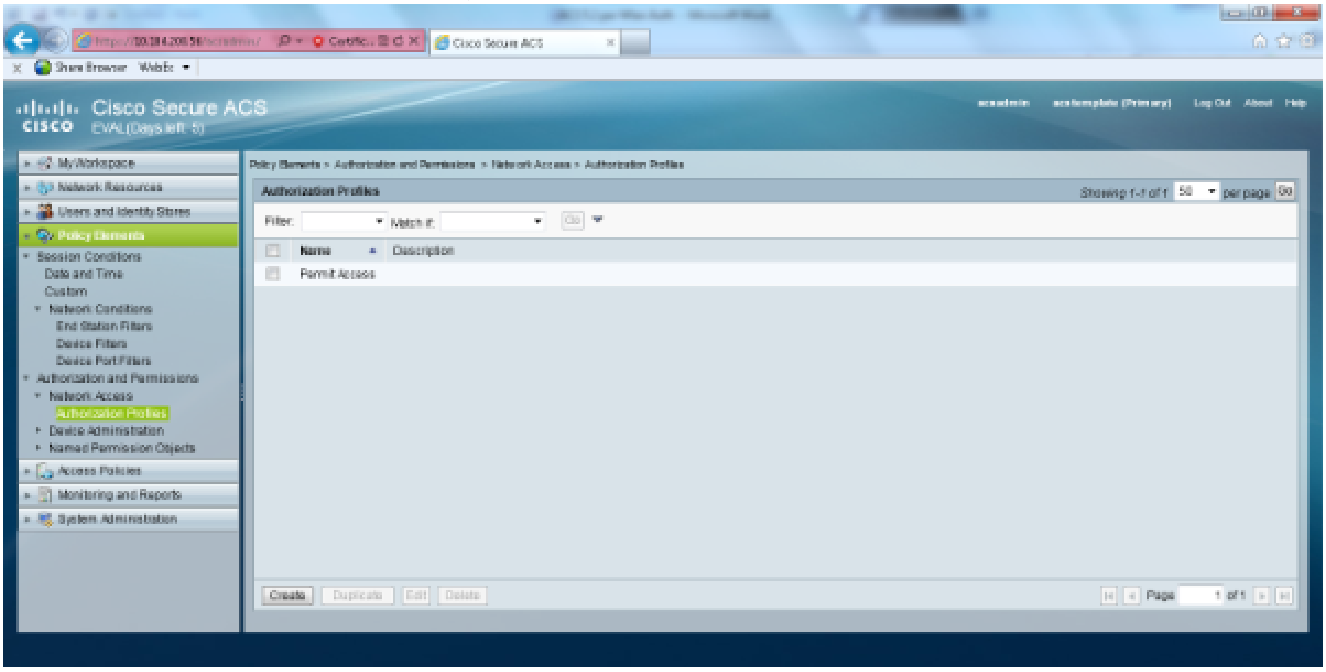
	CLI	DNIS
□	-ANY-	*Contractor

Cisco Secure ACS -- Webpage Dialog

CLI: □ -ANY-

DNIS: ☑ *Contractor

6. 选择**策略元素>授权和权限>网络访问>授权配置文件**。应该有允许访问的默认配置文件。

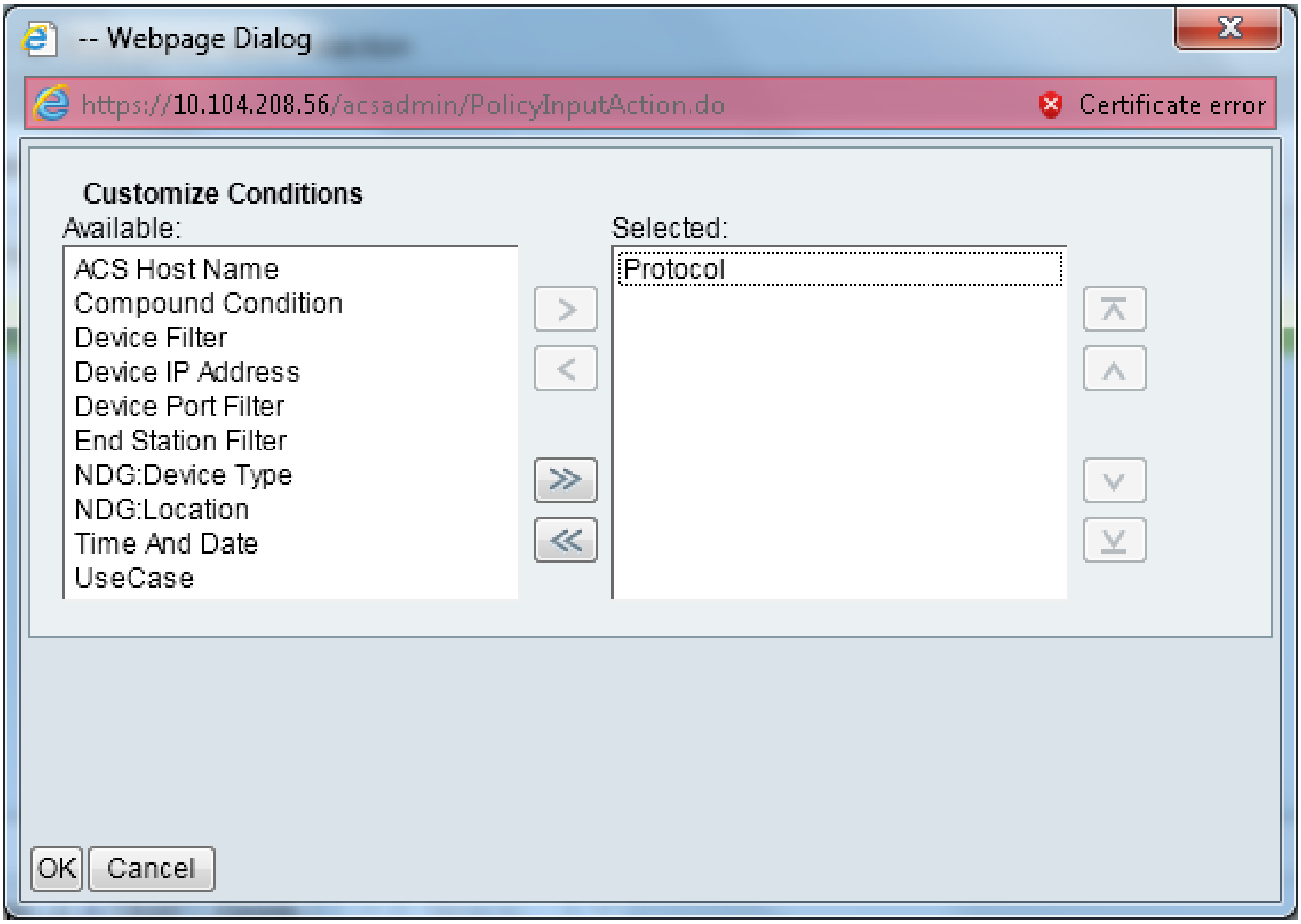


Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles

Authorization Profiles

	Name	Description
□	Permit Access	

7. 选择**访问策略>访问服务>服务选择规则**。单击“**Customize**(自**定义)”。** 添加任何合适的条件。本示例使用协议作为Radius作为匹配条件。Click **Create.**命名规则。选择**协议**并选择**Radius。**在**结果**下，选择适当的访问服务。在本例中，它保留为“默认网**络访问”。**



-- Webpage Dialog

https://10.104.208.56/acsadmin/PolicyInputAction.do

Certificate error

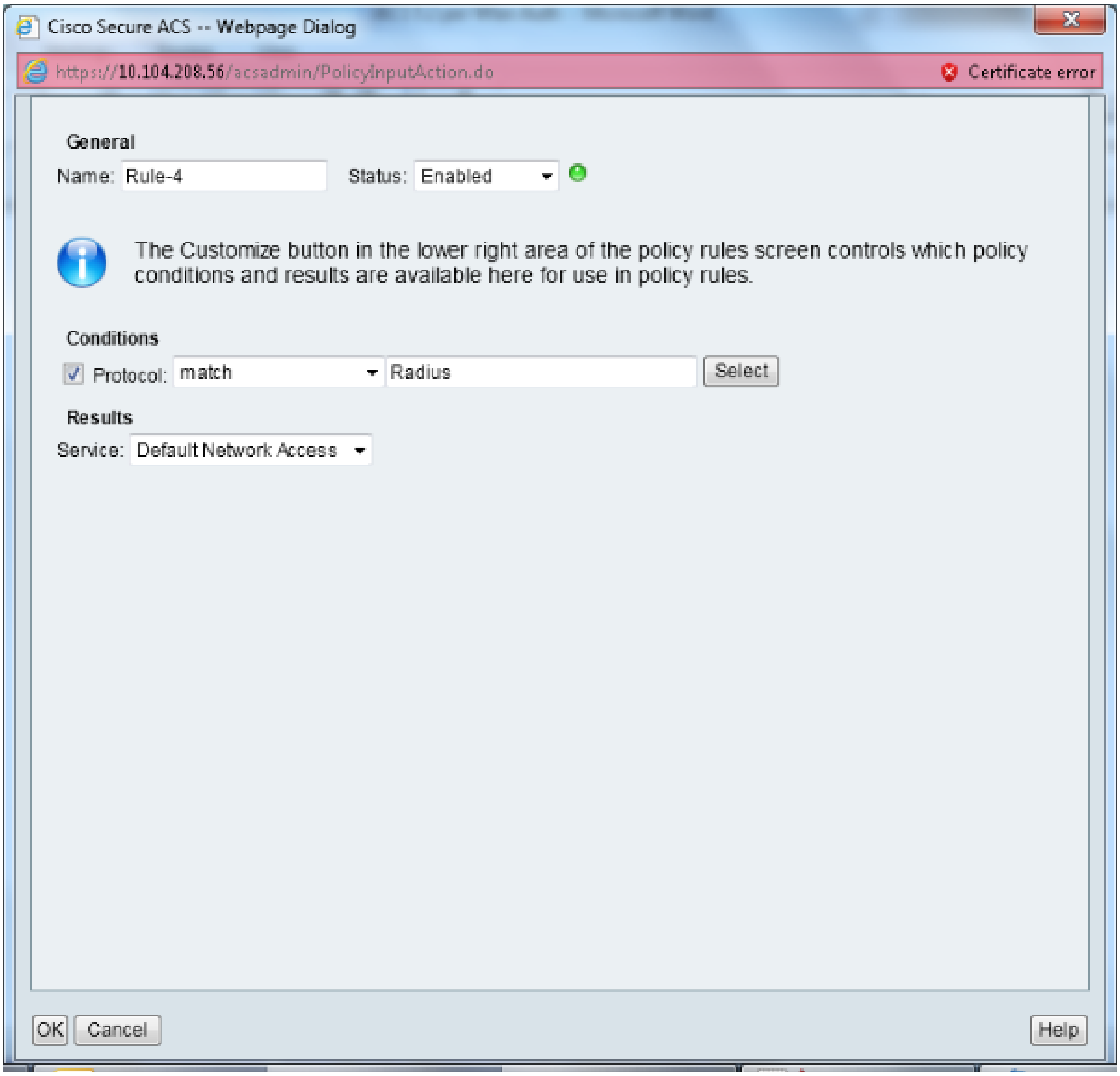
Customize Conditions

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
OK
Cancel
Help

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.

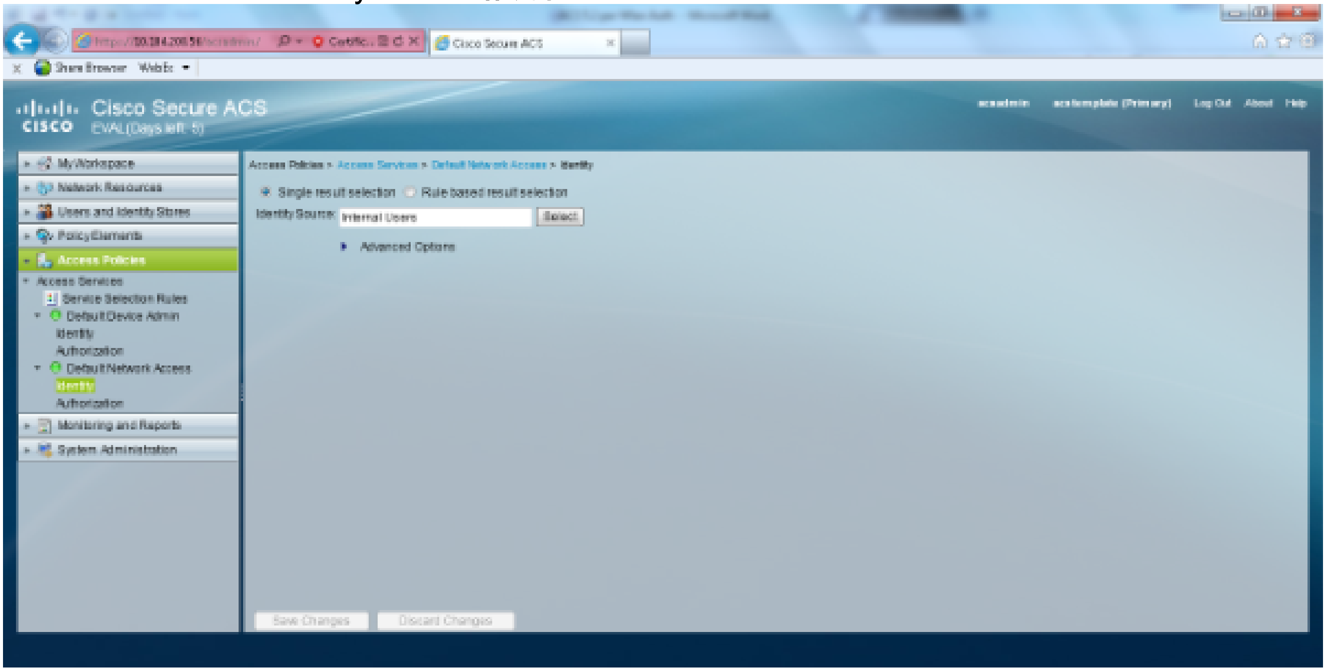
Conditions

☑ Protocol: match Radius Select

Results

Service: Default Network Access

8. 选择**Access Policies > Access Services > Default Network Access > Identity**。选择Single Result Selection和Identity Source**作为内**部用户。



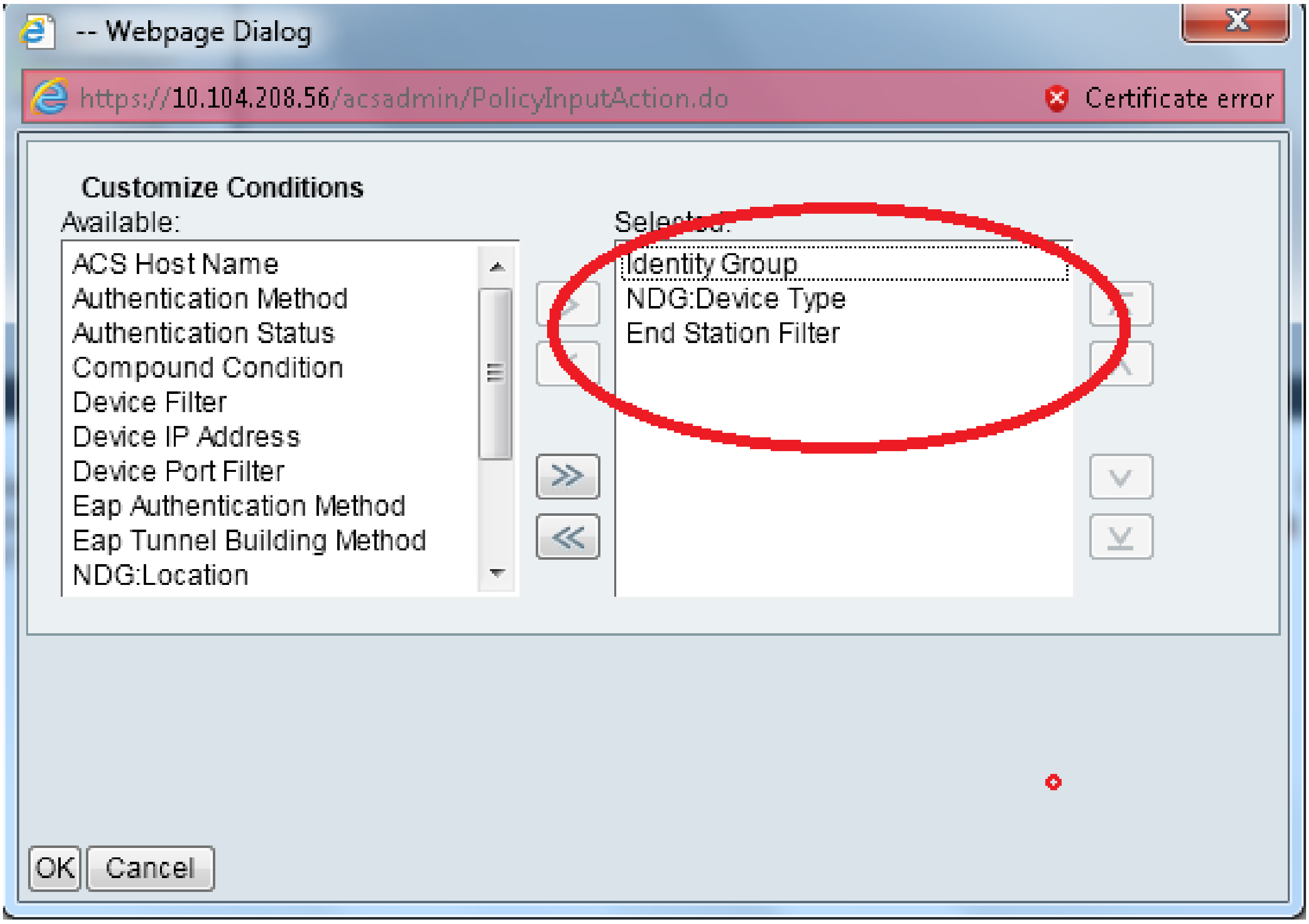
Access Policies > Access Services > Default Network Access > Identity

● Single result selection ○ Rule based result selection

Identity Source: Internal Users Select

Advanced Options

选择**访问策略>访问服务>默认网络访问>授权。单击自定义**并添加自定义条件。本示例按此顺序使用身份组、NDG：设备类型和终端站过滤器。



-- Webpage Dialog

https://10.104.208.56/acsadmin/PolicyInputAction.do

Certificate error

Customize Conditions

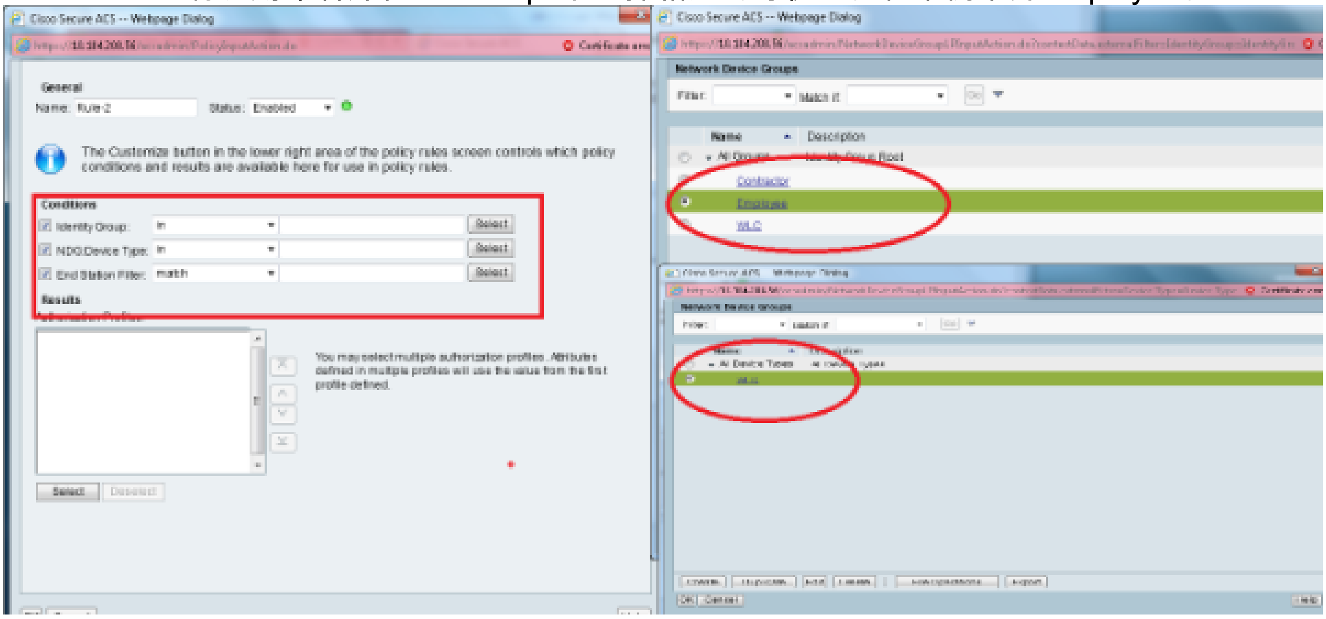
Available:

- 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

Click **Create**.将规则命名并在All Groups下选择相应的身份组。在本例中为Employee。



Cisco Secure ACS -- Webpage Dialog

https://10.104.208.56/acsadmin/PolicyInputAction.do

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

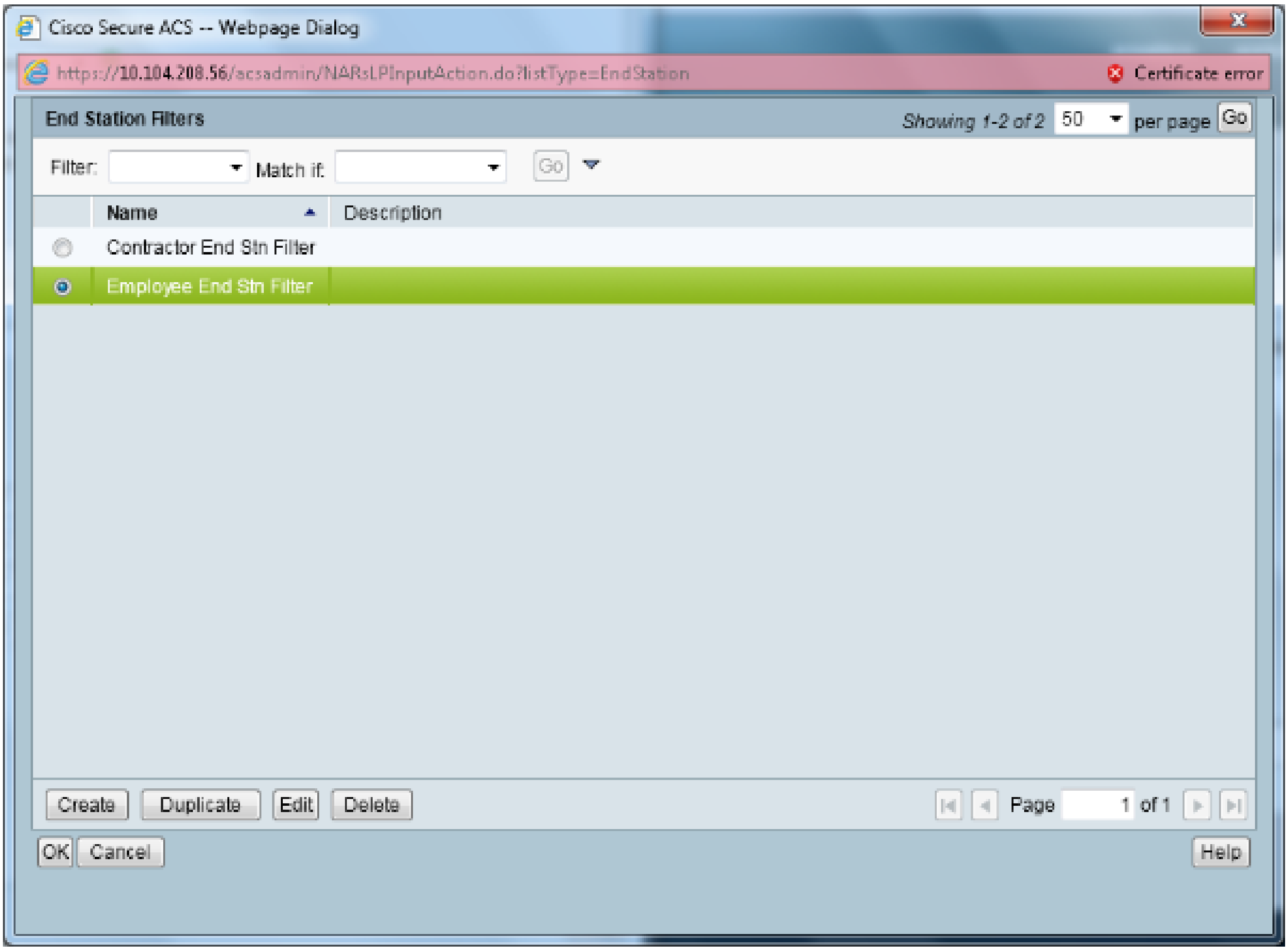
Filter: Match if:

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

Network Device Groups

	Name	Description
○	All Device Types	All Device Types
●	WLC	

单击**Employee End Stn Filter**单选按钮，或在“Configure the WLC”部分输入您在步骤1b中输入的名称。



Cisco Secure ACS -- Webpage Dialog

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

Certificate error

End Station Filters

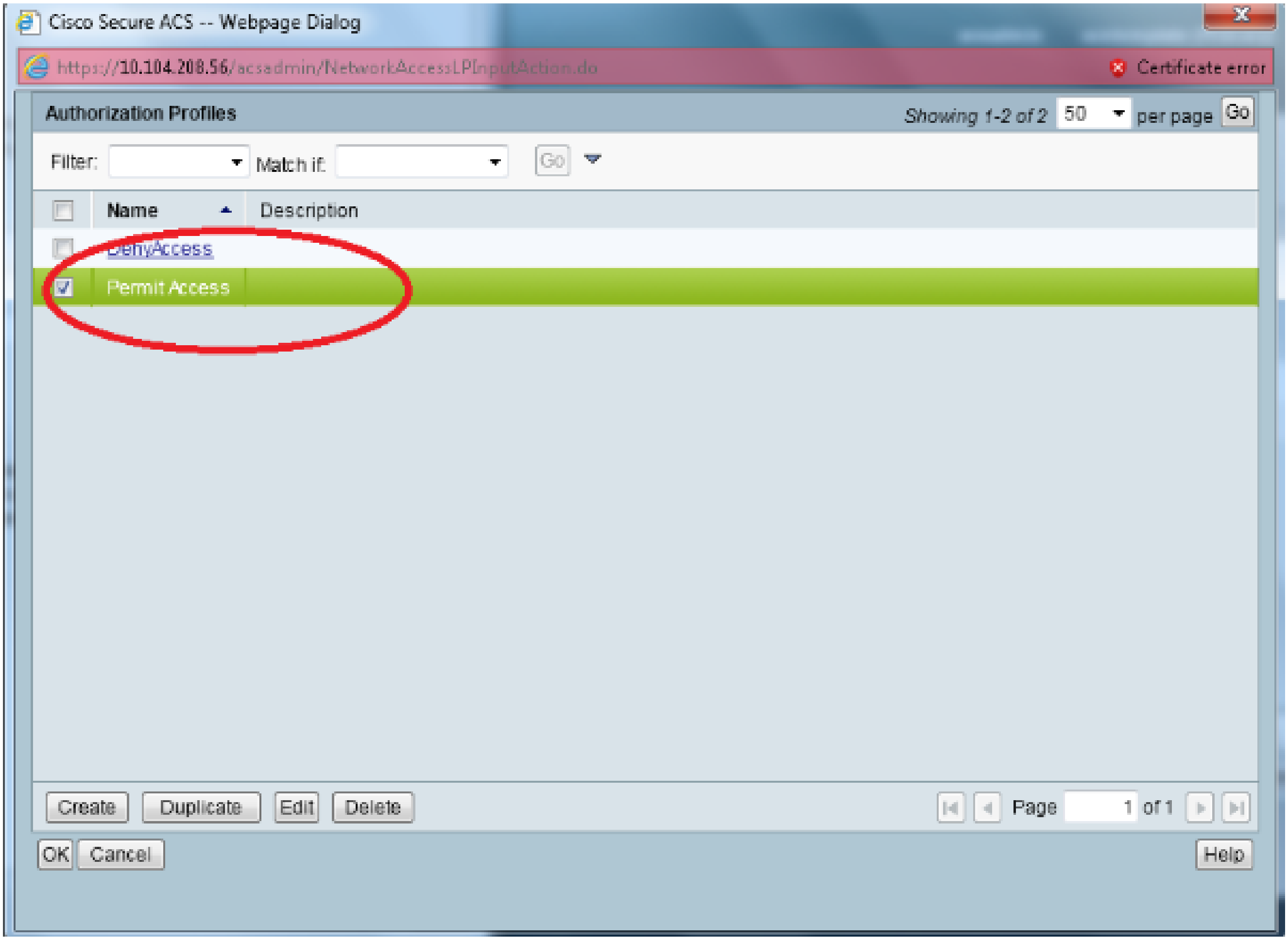
Showing 1-2 of 2 50 per page

Filter: Match if:

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

Page 1 of 1

选中允**许访问**复选框。



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

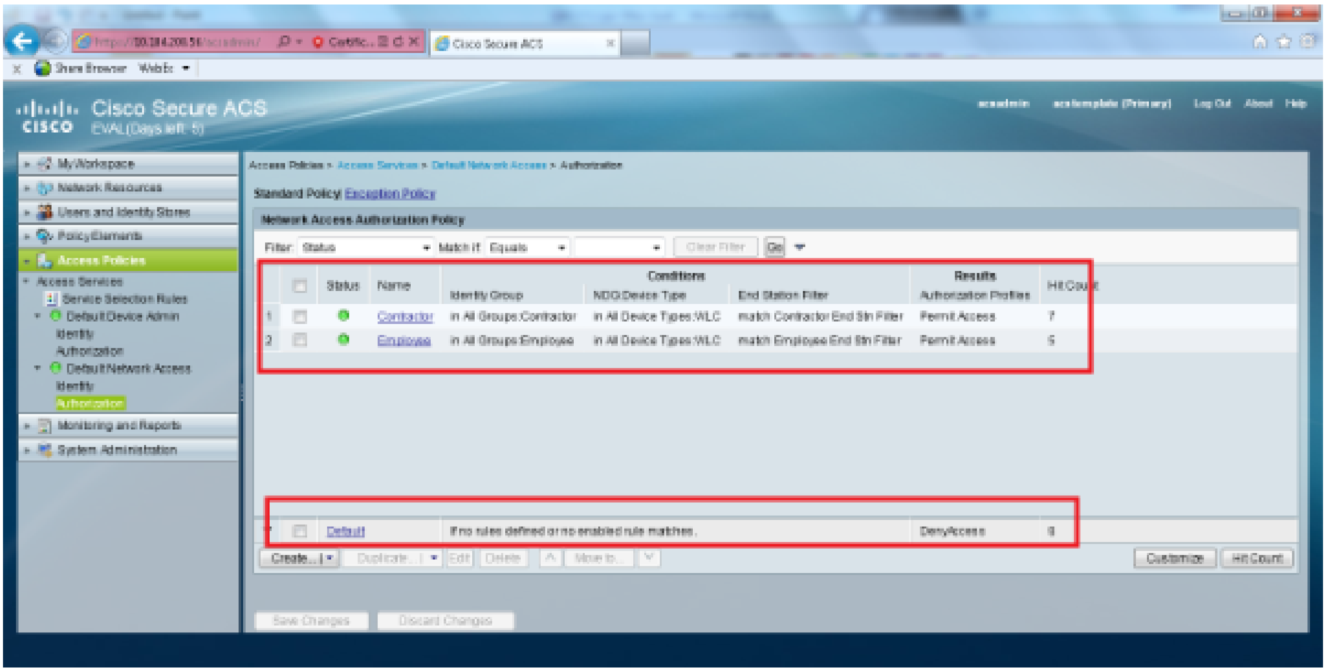
Filter: Match if:

□	Name	Description
□	DenyAccess	
☑	Permit Access	

Page 1 of 1

对“承包商规则”(Contractor Rules)也重复上述步骤。确保默认操作为拒**绝访问**。 完成步骤e后

，规则应如下所示
：



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

Create... | Duplicate... | Edit | Delete | Move to... | Customize | Hit Count
Save Changes | Discard Changes

配置到此结束。在本部分之后，需要为客户端相应地配置SSID和安全参数，以便连接。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。