

使用LAP配置ACS 5.2進行基於埠的身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[假設](#)

[配置步驟](#)

[配置LAP](#)

[配置交換機](#)

[設定RADIUS伺服器](#)

[配置網路資源](#)

[配置使用者](#)

[定義策略元素](#)

[應用訪問策略](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文說明如何將輕量型存取點(LAP)設定為802.1x要求者，以便對RADIUS伺服器(例如存取控制伺服器(ACS)5.2)進行驗證。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 瞭解無線LAN控制器(WLC)和LAP的基本知識。
- 具有AAA伺服器的功能知識。
- 全面瞭解無線網路和無線安全問題。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5508 WLC (執行韌體版本7.0.220.0)
- Cisco 3502系列LAP
- 執行5.2版的Cisco Secure ACS
- Cisco 3560系列交換器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

背景資訊

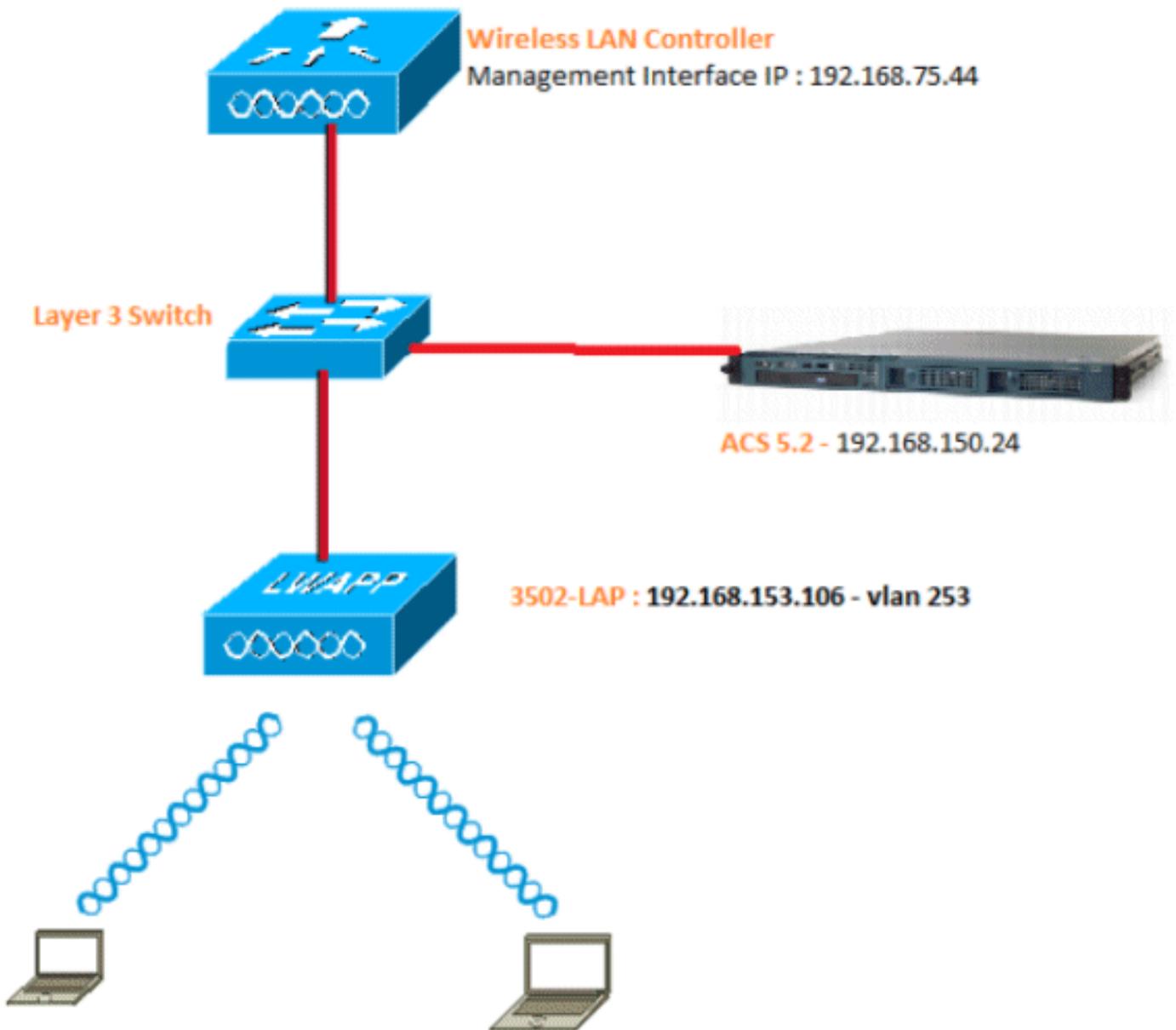
LAP在工廠安裝了X.509證書 (由私鑰簽名)，這些證書在製造時燒錄到裝置中。LAP使用此憑證以在加入過程中與WLC進行驗證。此方法描述了驗證LAP的另一種方式。藉助WLC軟體，您可以在Cisco Aironet接入點(AP)和Cisco交換機之間配置802.1x身份驗證。在此例項中，AP充當802.1x請求方，並由交換機針對使用EAP-FAST和匿名PAC調配的RADIUS伺服器(ACS)進行身份驗證。一旦設定為802.1x驗證，交換器就不會允許802.1x流量以外的任何流量通過連線埠，直到連線到連線埠的裝置成功驗證為止。AP可以在加入WLC之前或加入WLC之後進行驗證，在這種情況下，您可以在LAP加入WLC之後在交換器上設定802.1x。

設定

本節提供用於設定本文件中所述功能的資訊。

網路圖表

此文件使用以下網路設定：



以下是此圖中所用元件的配置詳細資訊：

- ACS(RADIUS)伺服器的IP地址是192.168.150.24。
- WLC的管理和AP管理器介面地址為192.168.75.44。
- DHCP伺服器地址為192.168.150.25。
- LAP位於VLAN 253中。
- VLAN 253:192.168.153.x/24。網關：192.168.153.10
- VLAN 75:192.168.75.x/24。網關：192.168.75.1

假設

- 所有第3層VLAN都配置了交換機。

- 為DHCP伺服器分配一個DHCP作用域。
- 網路中所有裝置之間都存在第3層連線。
- LAP已連線到WLC。
- 每個VLAN都有一個/24掩碼。
- ACS 5.2已安裝自簽名證書。

配置步驟

此配置分為三類：

1. [配置LAP。](#)
2. [設定交換器。](#)
3. [設定RADIUS伺服器。](#)

配置LAP

假設：

LAP已使用選項43、DNS或靜態配置的WLC管理介面IP註冊到WLC。

請完成以下步驟：

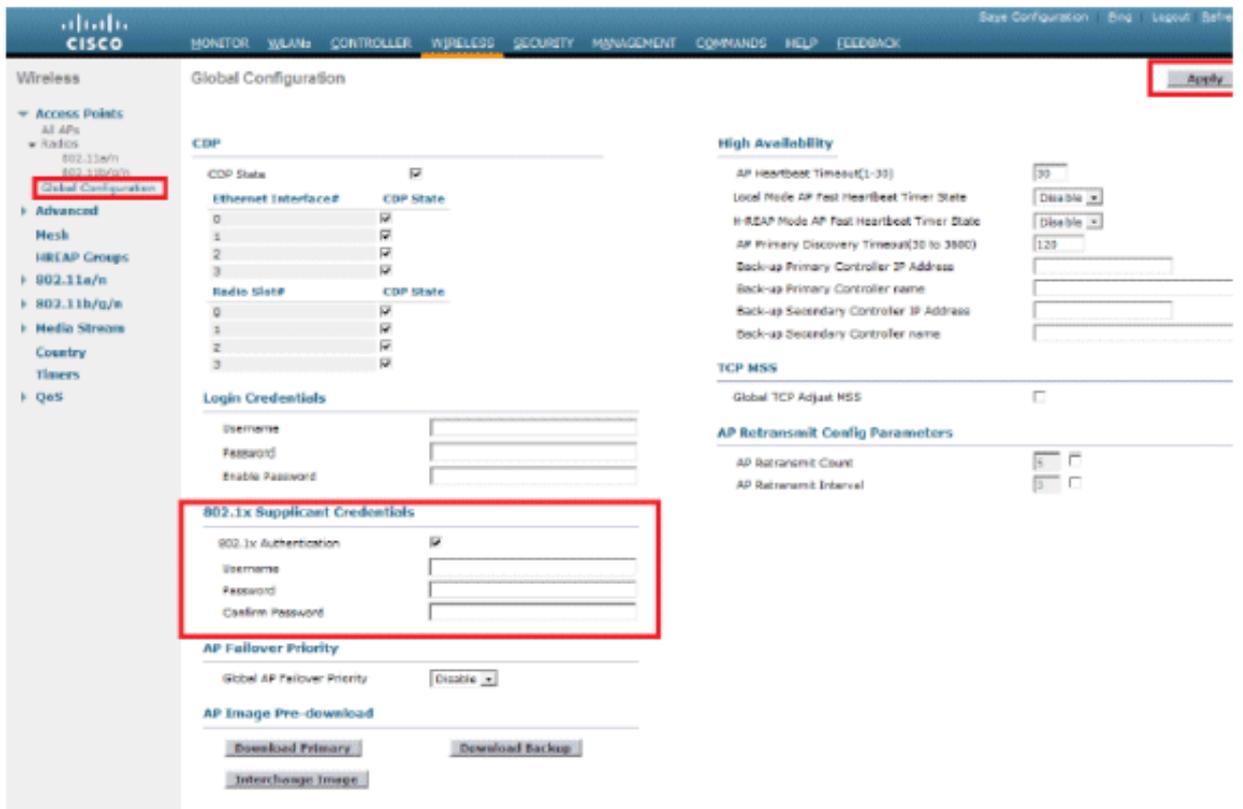
1. 前往Wireless > Access Points > All APs以驗證WLC上的LAP註冊。

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode
3162c	AIR-CT5502E-A-K9	cc:ef:40:7a:33:19	1 d, 02 h 32 m 42 s	Enabled	REG	13	Local

2. 您可以通過兩種方式為所有LAP配置802.1x憑據（即使用者名稱/密碼）：

- 全域性

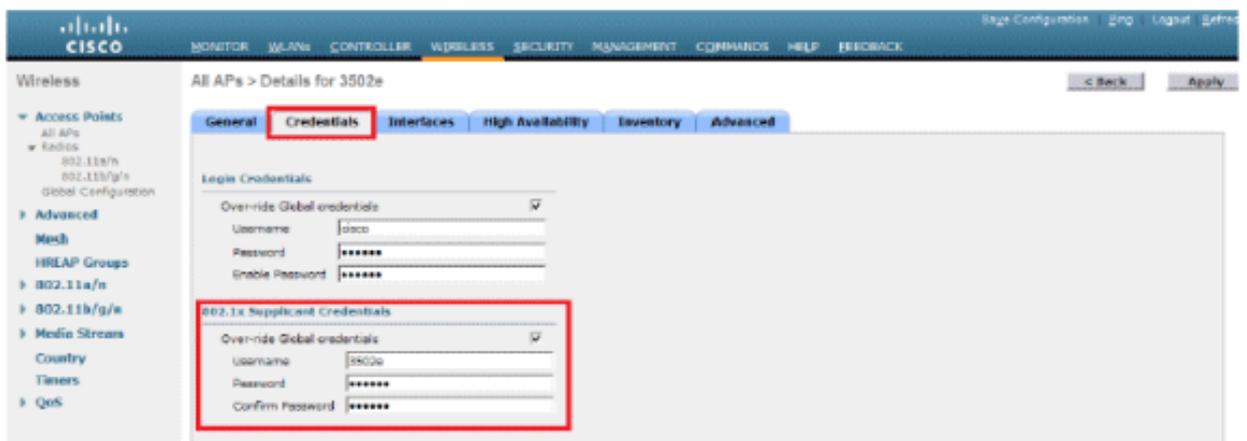
對於已加入的LAP，您可以全域性設定憑據，以便每個加入WLC的LAP都將繼承這些憑據。



- 單獨

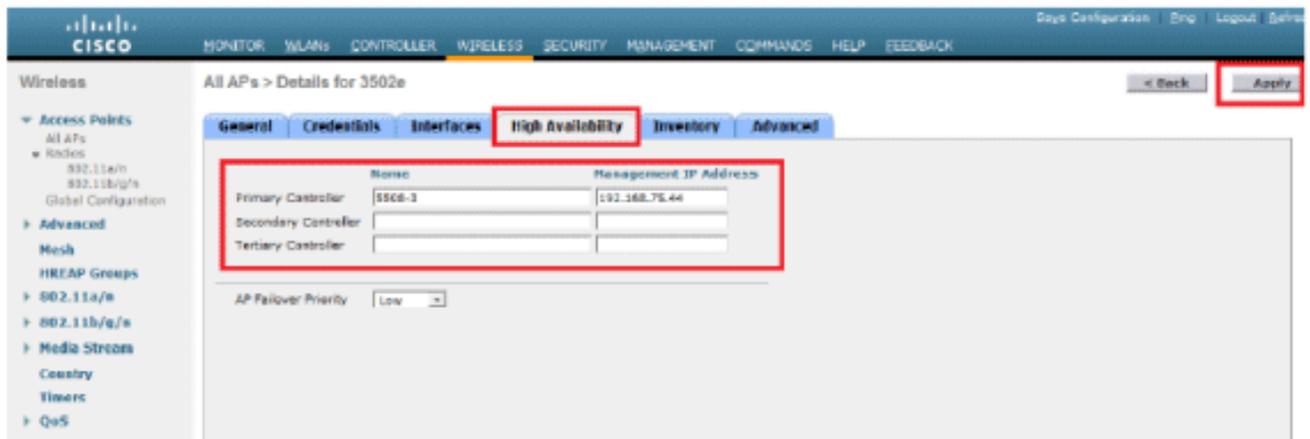
為每個AP配置802.1x配置檔案。在我們的示例中，我們將為每個AP配置憑據。

- 轉到無線 > 所有AP，然後選擇相關的AP。
- 在802.1x Supplicant Credentials欄位中新增使用者名稱和密碼。



注意：登入憑據用於通過Telnet、SSH或控制檯連線到AP。

- 配置「高可用性」部分，然後按一下應用。



注意：儲存後，這些憑證將保留在WLC中，且AP將重新啟動。只有當LAP加入新WLC時，憑證才會更改。LAP採用在新WLC上配置的使用者名稱和密碼。

如果AP尚未加入WLC，您必須通過控制檯連線到LAP才能設定憑據。在啟用模式下發出此CLI命令：

```
LAP#lwapp ap dot1x username <username> password <password>
```

或

```
LAP#capwap ap dot1x username <username> password <password>
```

注意：此命令僅適用於運行恢復映像的AP。

LAP的預設使用者名稱和密碼分別為cisco和Cisco。

配置交換機

交換器充當LAP的驗證器，並針對RADIUS伺服器驗證LAP。如果交換器沒有相容的軟體，請升級交換器。在交換器CLI中，核發以下命令，以便在交換器連線埠上啟用802.1x驗證：

```
<#root>
```

```
switch#
```

```
configure terminal
```

```
switch(config)#
```

```
dot1x system-auth-control
```

```
switch(config)#
```

```
aaa new-model
```

```
!--- Enables 802.1x on the Switch.
```

```
switch(config)#
```

```
aaa authentication dot1x default group radius
```

```
switch(config)#
```

```
radius server host 192.168.150.24 key cisco
```

!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x information

```
switch(config)#
```

```
ip radius source-interface vlan 253
```

!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.

```
switch(config)interface gigabitEthernet 0/11
```

```
switch(config-if)switchport mode access
```

```
switch(config-if)switchport access vlan 253
```

```
switch(config-if)mls qos trust dscp
```

```
switch(config-if)spanning-tree portfast
```

!--- gig0/11 is the port number on which the AP is connected.

```
switch(config-if)dot1x pae authenticator
```

!--- Configures dot1x authentication.

```
switch(config-if)dot1x port-control auto
```

!--- With this command, the switch initiates the 802.1x authentication.

註：如果您在同一交換機上有其他AP，並且您不希望它們使用802.1x，則可以保持未為802.1x配置該埠，或者發出以下命令：

```
<#root>
```

```
switch(config-if)authentication port-control force-authorized
```

設定RADIUS伺服器

LAP使用EAP-FAST進行身份驗證。如果您未使用Cisco ACS 5.2，請確保您使用的RADIUS伺服器支援此EAP方法。

RADIUS伺服器設定分為四個步驟：

1. [配置網路資源。](#)
2. [配置使用者。](#)
3. [定義策略元素。](#)
4. [應用訪問策略。](#)

ACS 5.x是基於策略的ACS。換句話說，ACS 5.x使用基於規則的策略模型，而不是4.x版本中使用的基於組的模型。

ACS 5.x基於規則的策略模型提供比舊的基於組的方法更強大、更靈活的訪問控制。

在較舊的基於組的模型中，組定義策略是因為它包含三種型別的資訊並將它們連線在一起：

- 身份信息 — 此資訊可以基於AD或LDAP組中的成員身份或內部ACS使用者的靜態分配。
- 其他限制或條件 — 時間限制、裝置限制等。
- 許可權- VLAN或Cisco IOS®許可權級別。

ACS 5.x策略模型基於以下形式的規則：

如果condition為result

例如，我們使用為基於組的模型描述的資訊：

如果為identity-condition、restriction-condition、則為authorization-profile。

因此，這使我們能夠靈活地限制允許使用者訪問網路的條件，以及在滿足特定條件時允許何種授權級別。

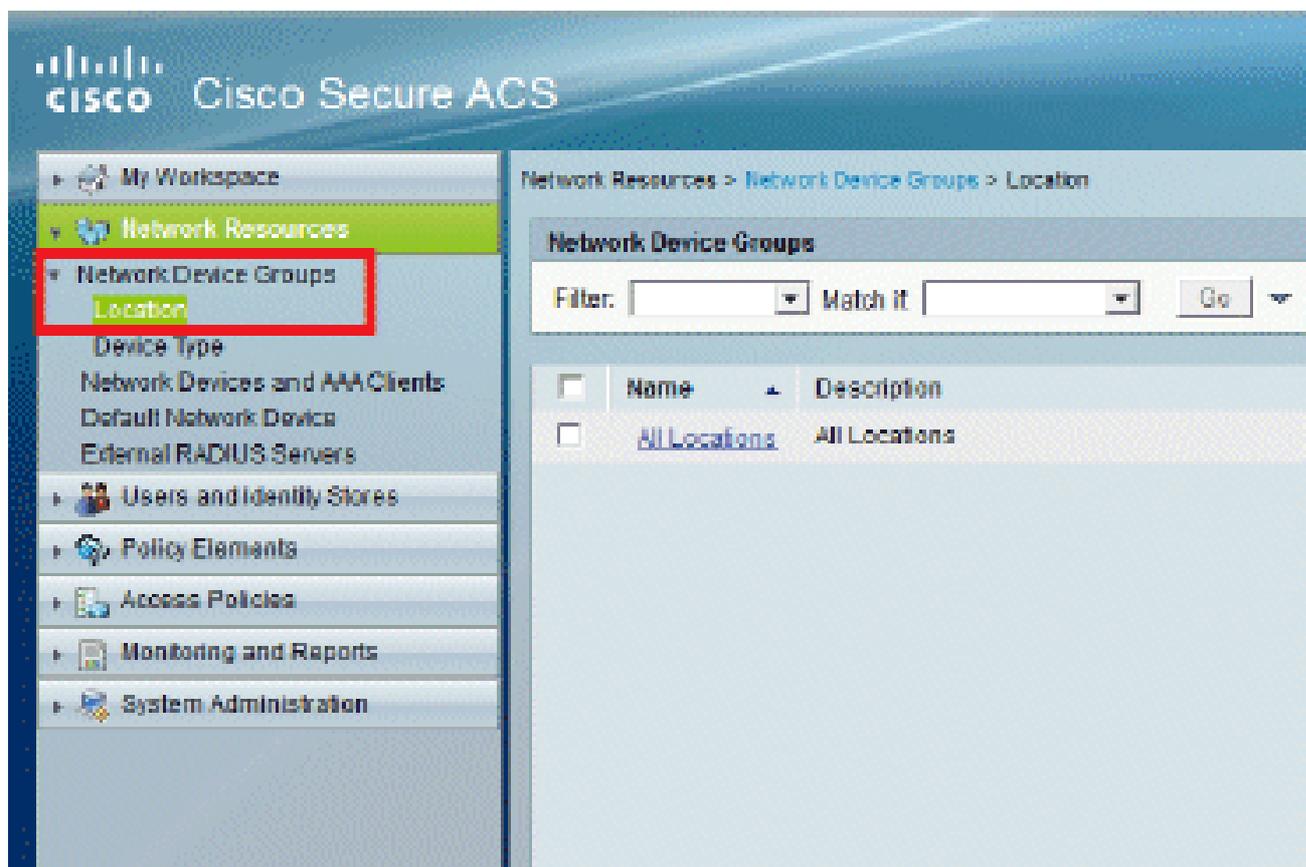
配置網路資源

在本節中，我們將為RADIUS伺服器上的交換機配置AAA客戶端。

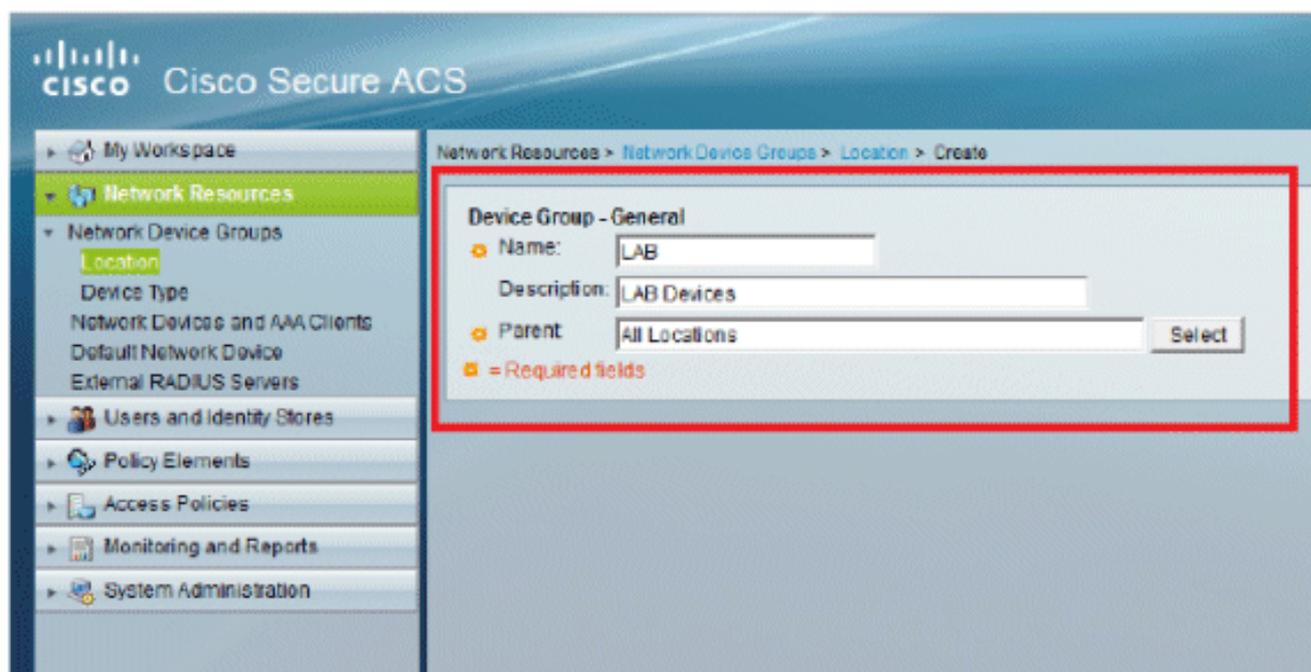
以下程式介紹如何將交換器作為AAA使用者端新增到RADIUS伺服器上，以便交換器可以將LAP的使用者憑證傳遞到RADIUS伺服器。

請完成以下步驟：

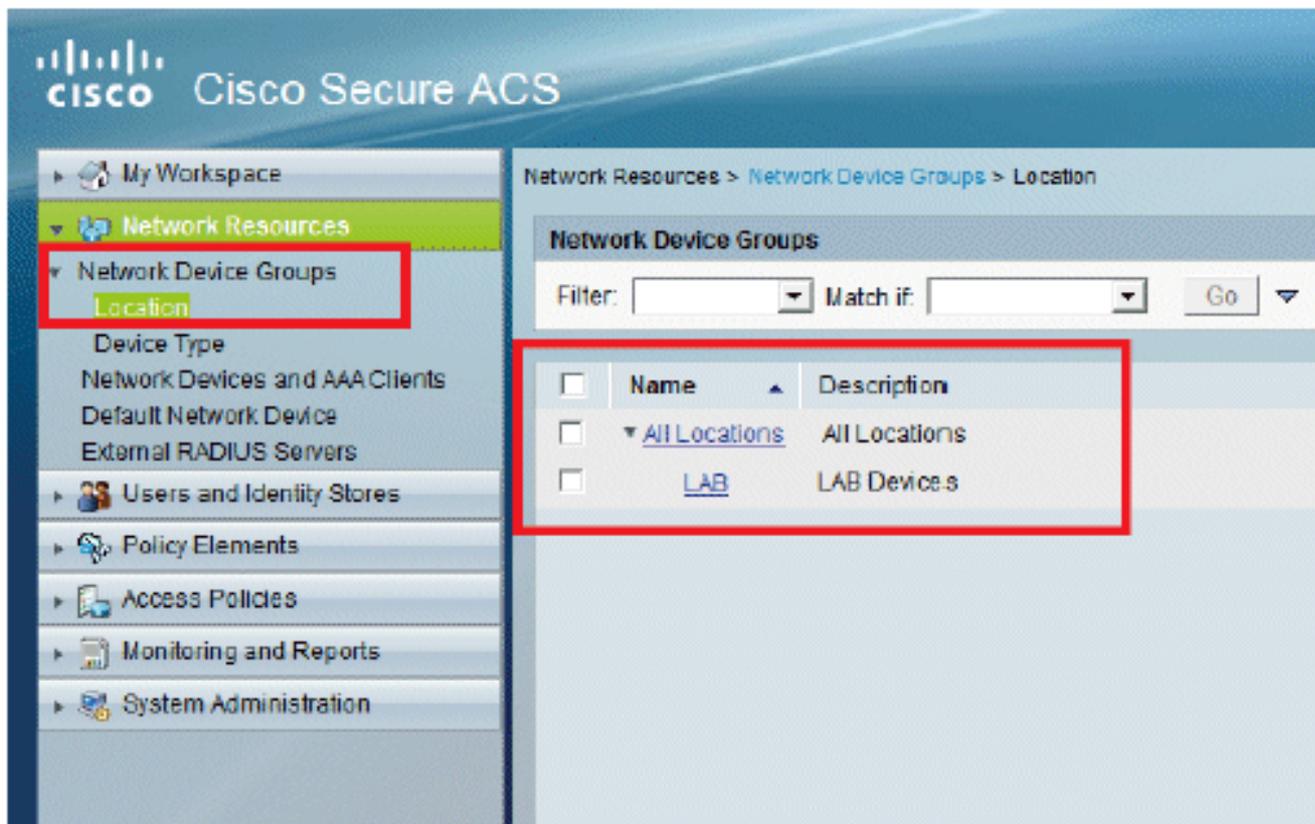
1. 在ACS GUI中，按一下Network Resources。
2. 按一下Network Device Groups。
3. 轉至Location > Create (位於底部)。



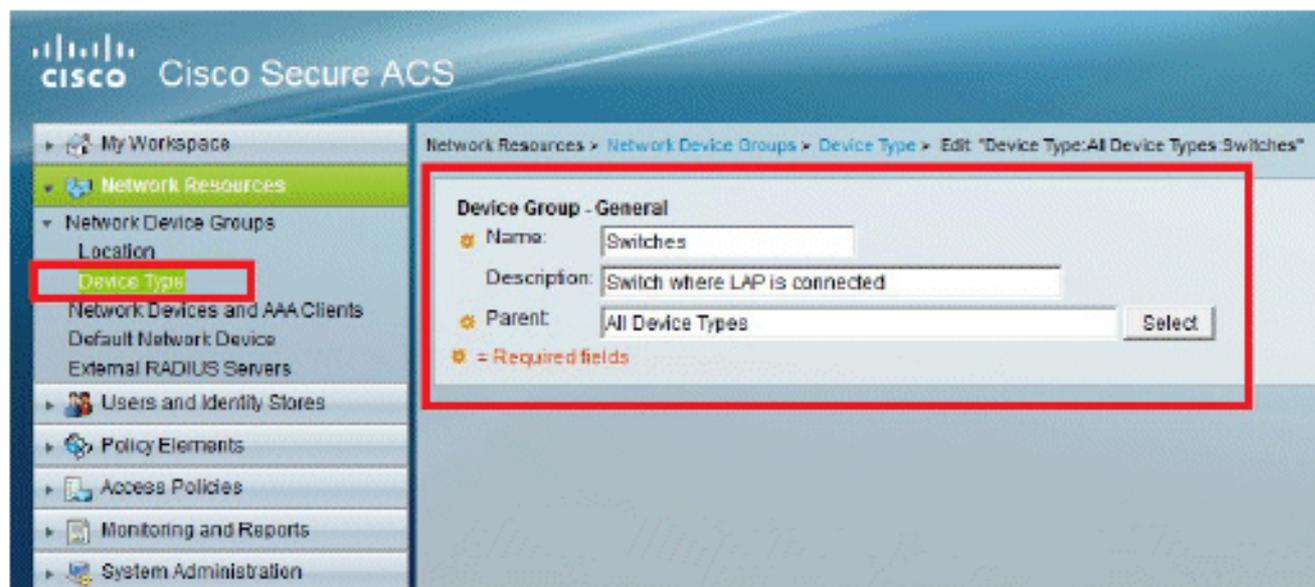
4. 新增必填欄位，然後按一下Submit。



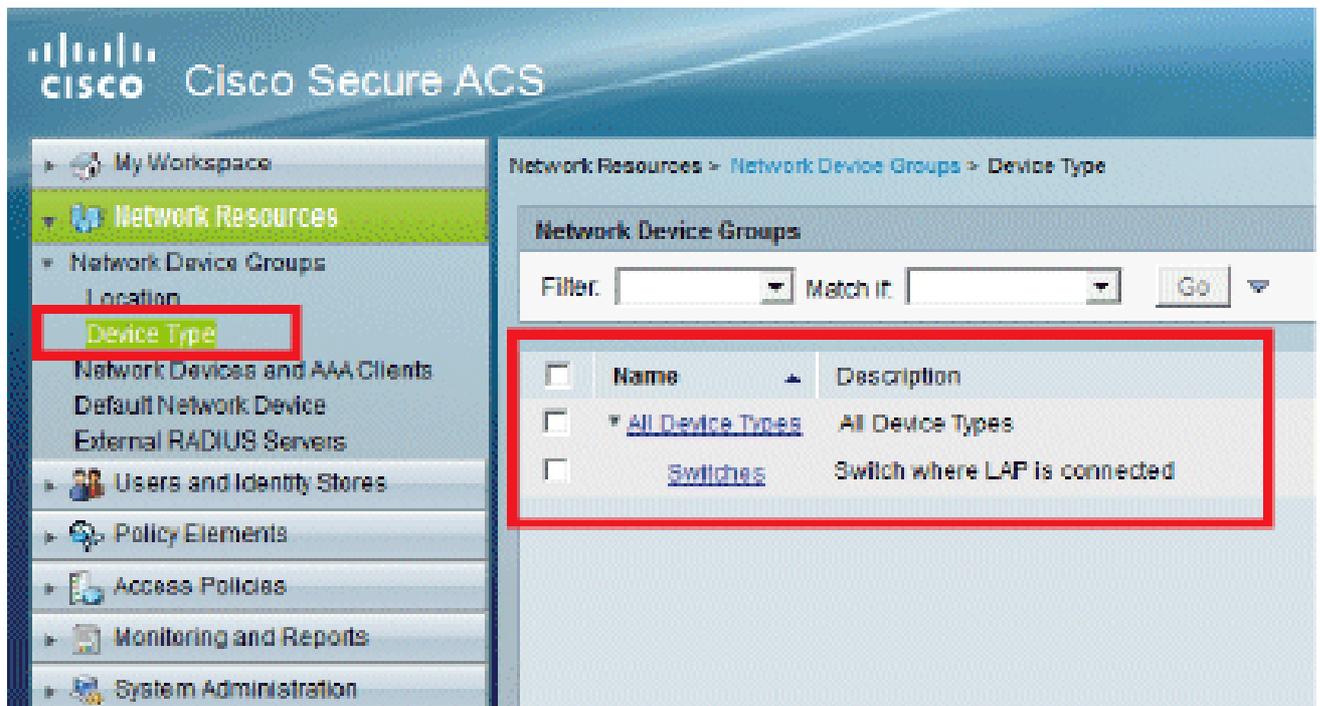
5. 視窗將刷新：



6. 按一下Device Type > Create。

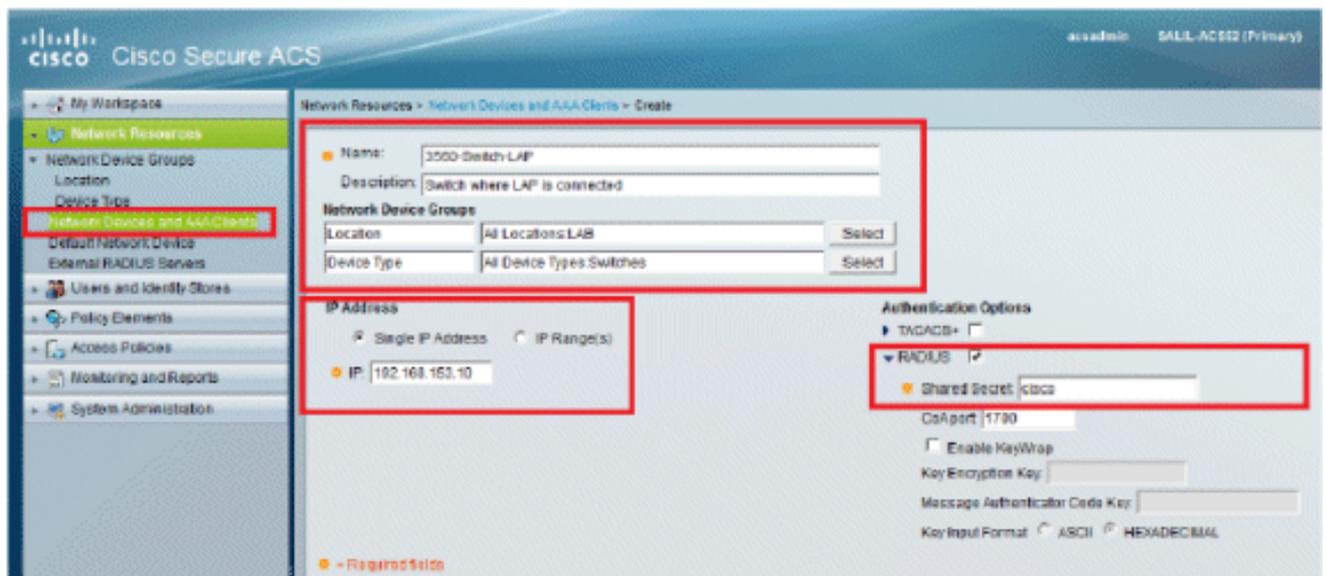


7. 按一下「Submit」。完成後，視窗將刷新：

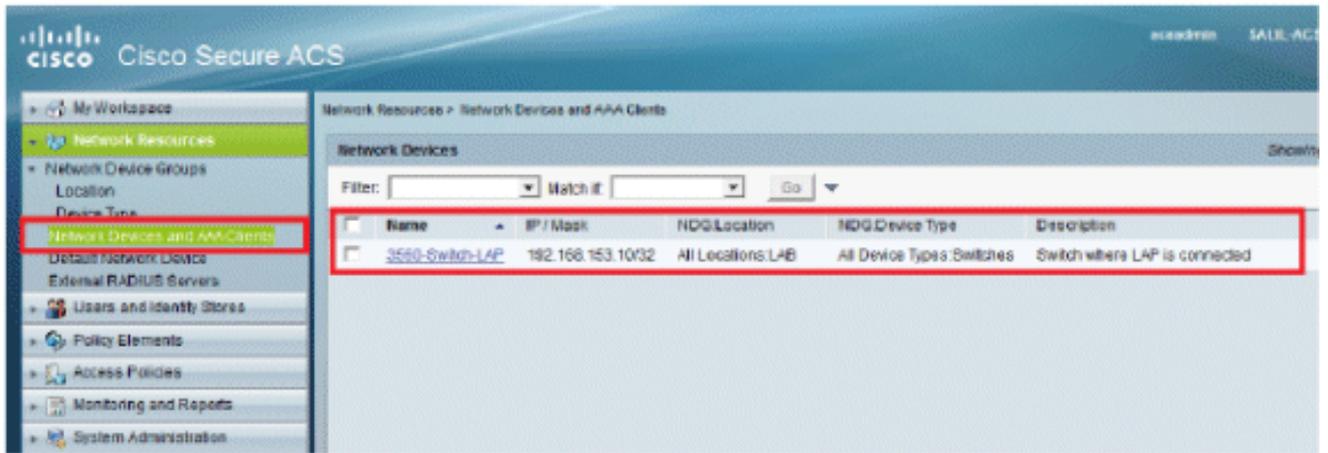


8. 前往 Network Resources > Network Devices and AAA Clients。

9. 按一下「Create」，然後填寫詳細資訊，如下所示：



10. 按一下「Submit」。視窗將刷新：

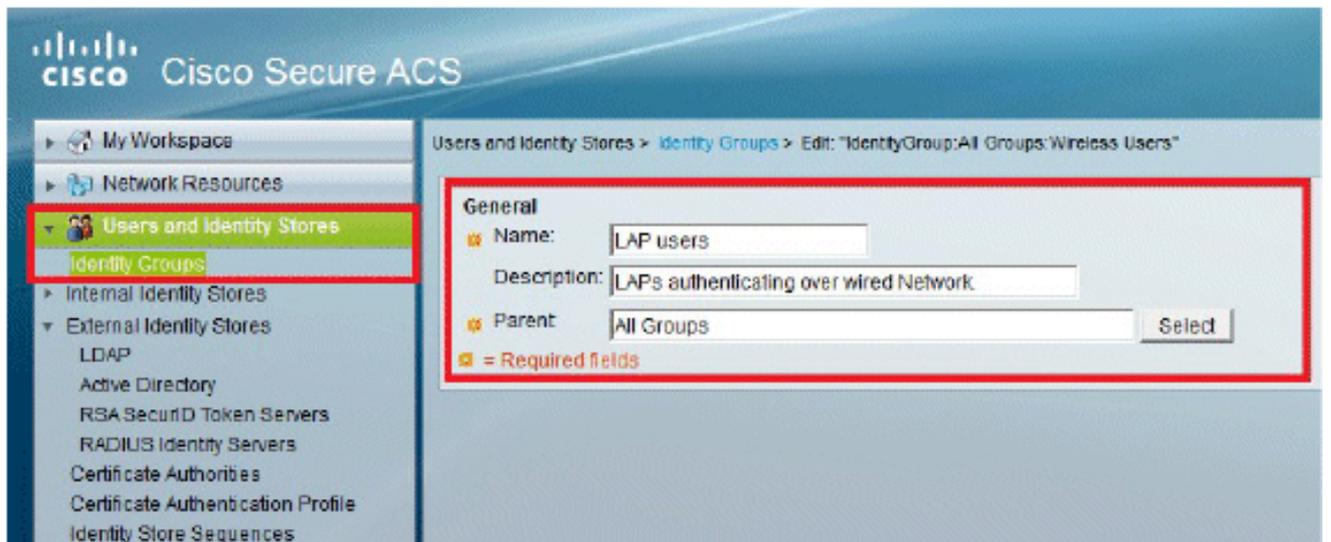


配置使用者

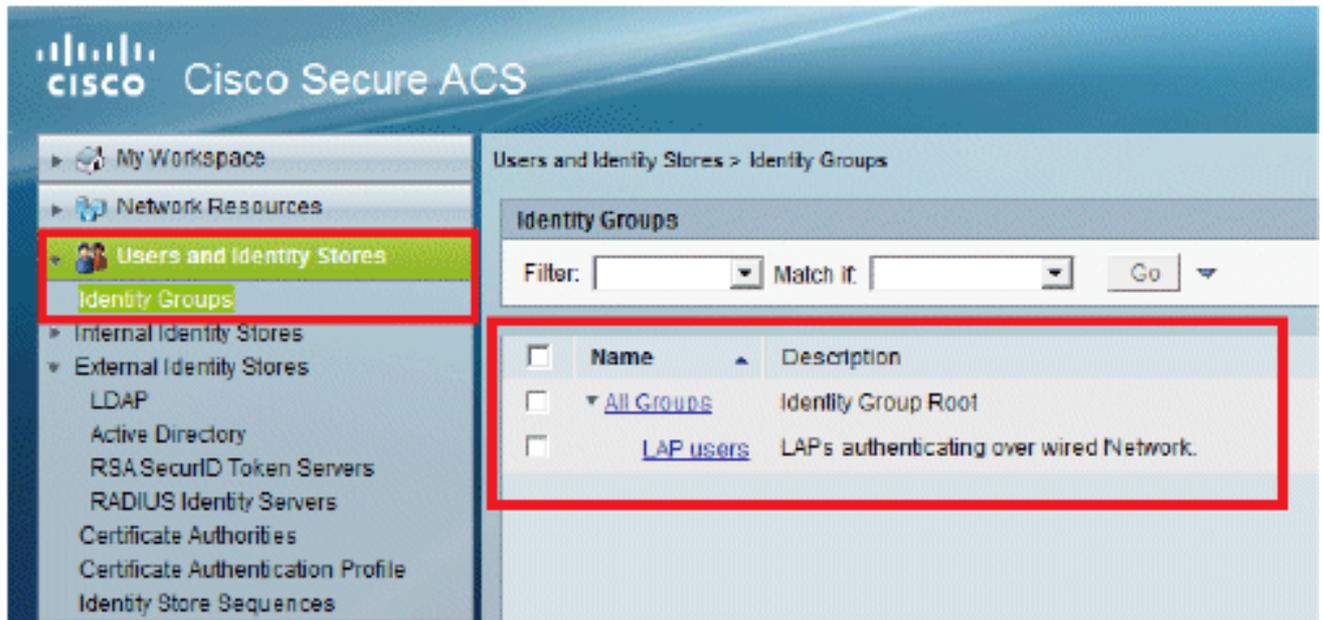
在本節中，您將看到如何在以前配置的ACS上建立使用者。您將將該使用者分配到名為「LAP使用者」的組。

請完成以下步驟：

1. 轉至使用者和身份庫 > 身份組 > 建立。

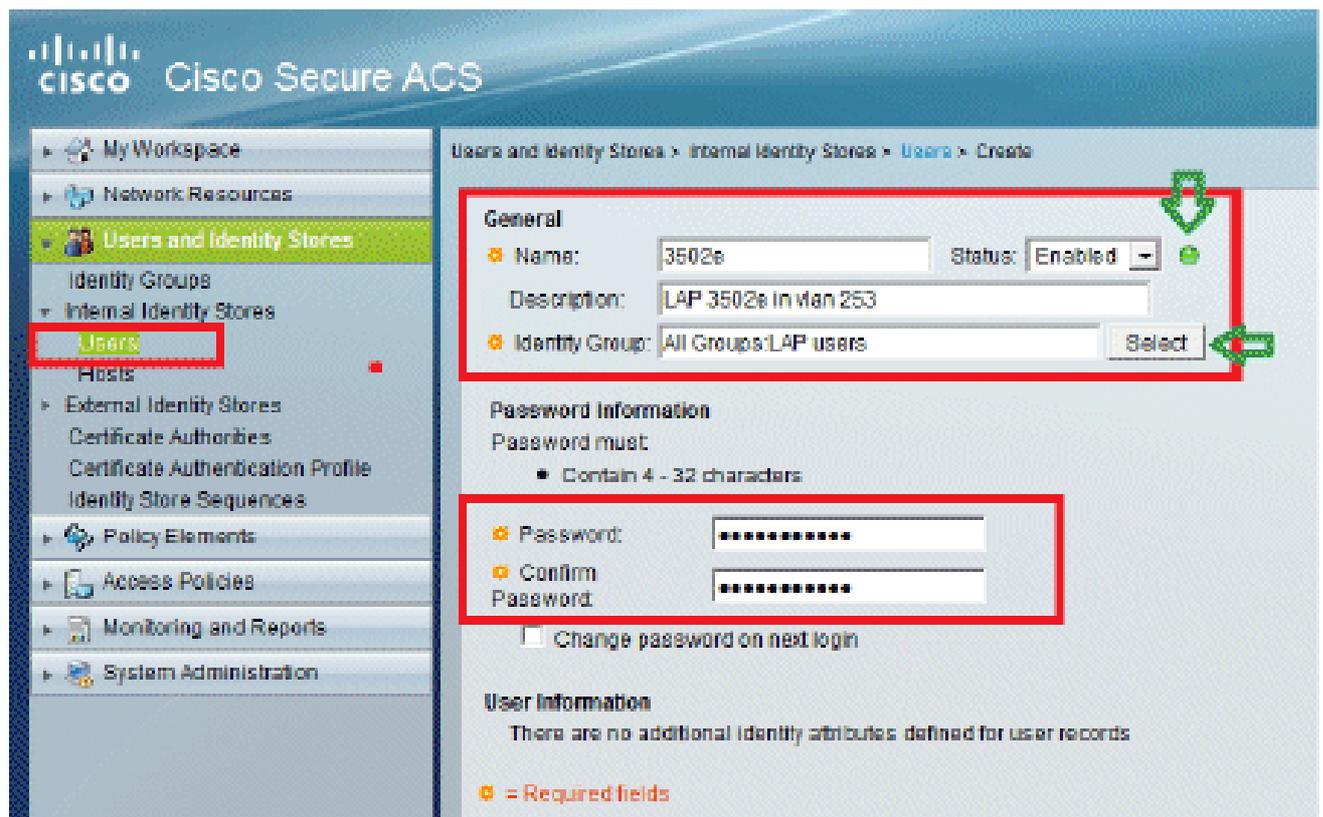


2. 點選提交(Submit)。

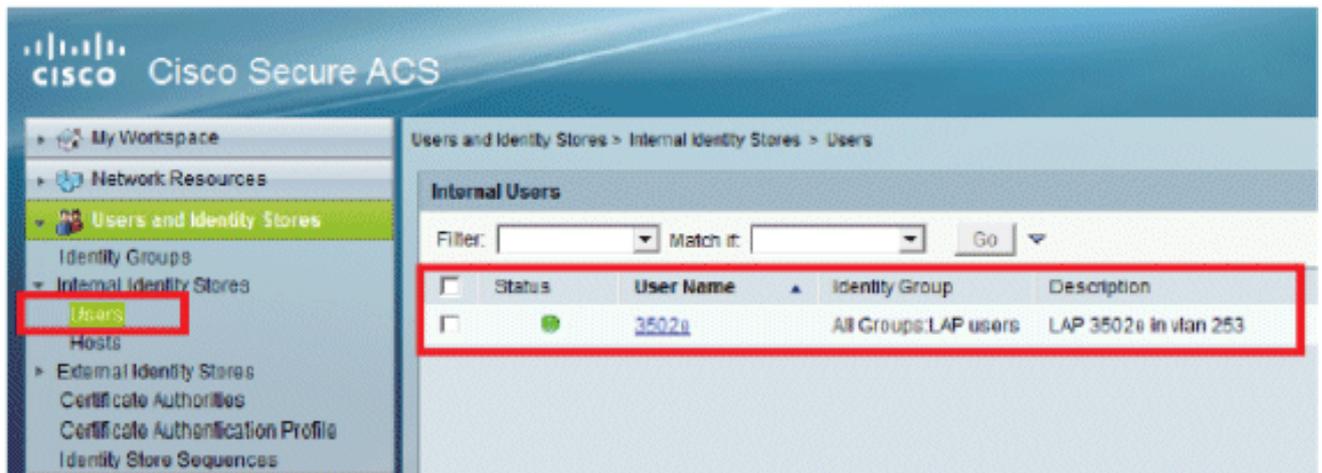


3. 建立3502e，並將其分配給組「LAP使用者」。

4. 轉至Users and Identity Stores > Identity Groups > Users > Create。

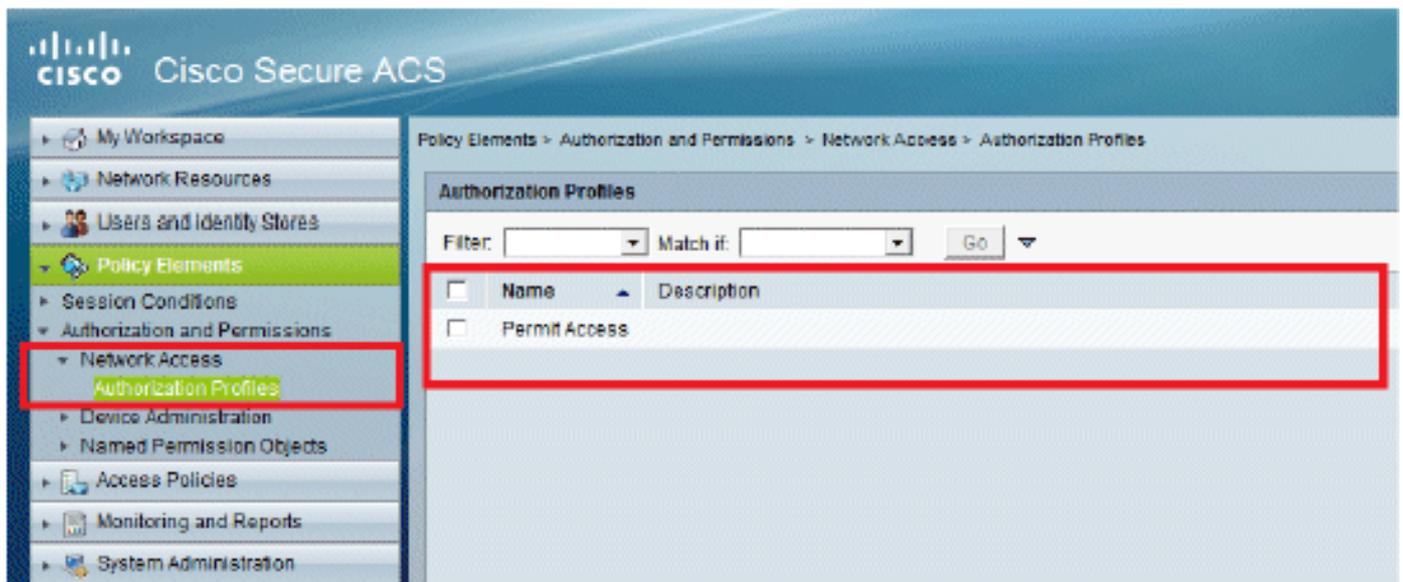


5. 您將看到更新的資訊：



定義策略元素

驗證Permit Access是否已設定。

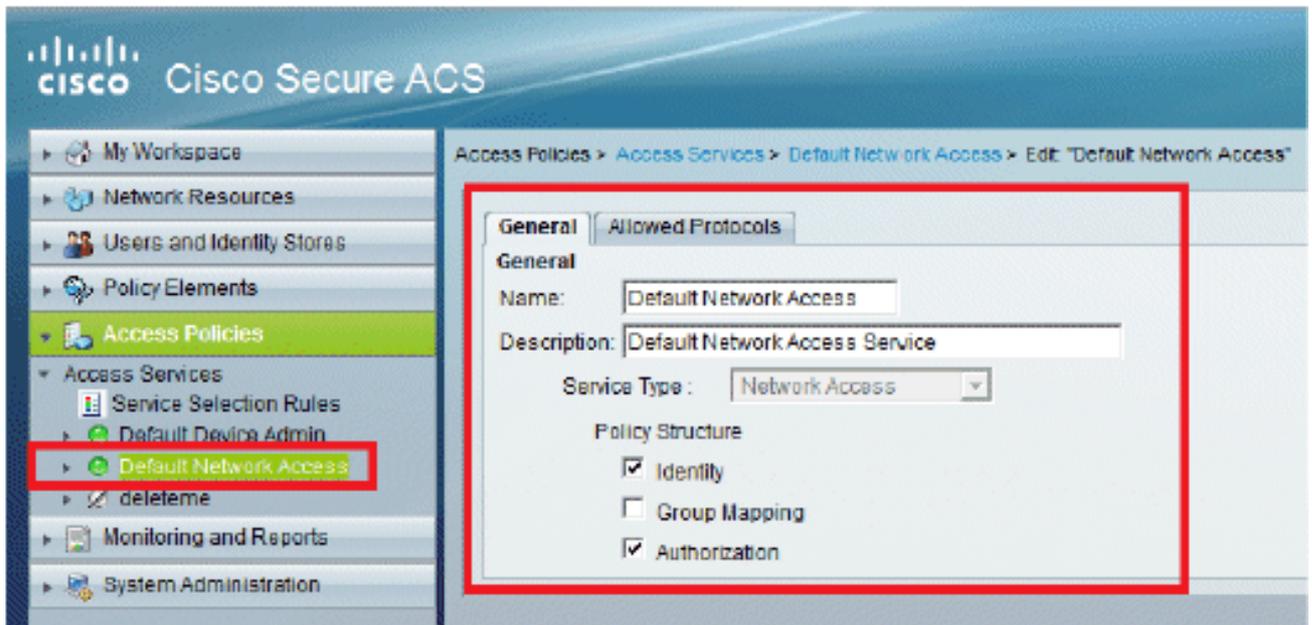


應用訪問策略

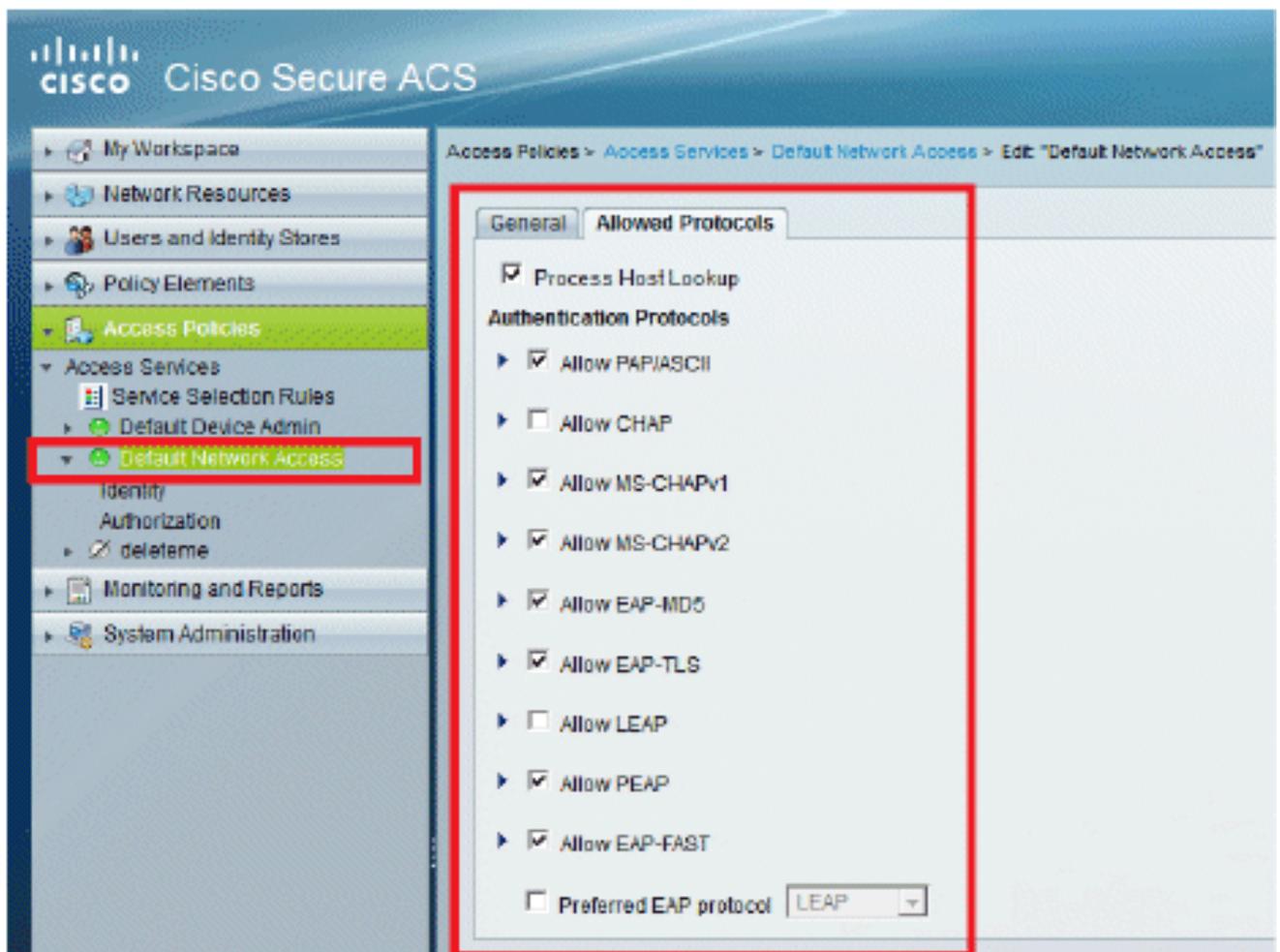
在本部分中，您將選擇EAP-FAST作為LAP的身份驗證方法，以便進行身份驗證。然後，您將基於上述步驟建立規則。

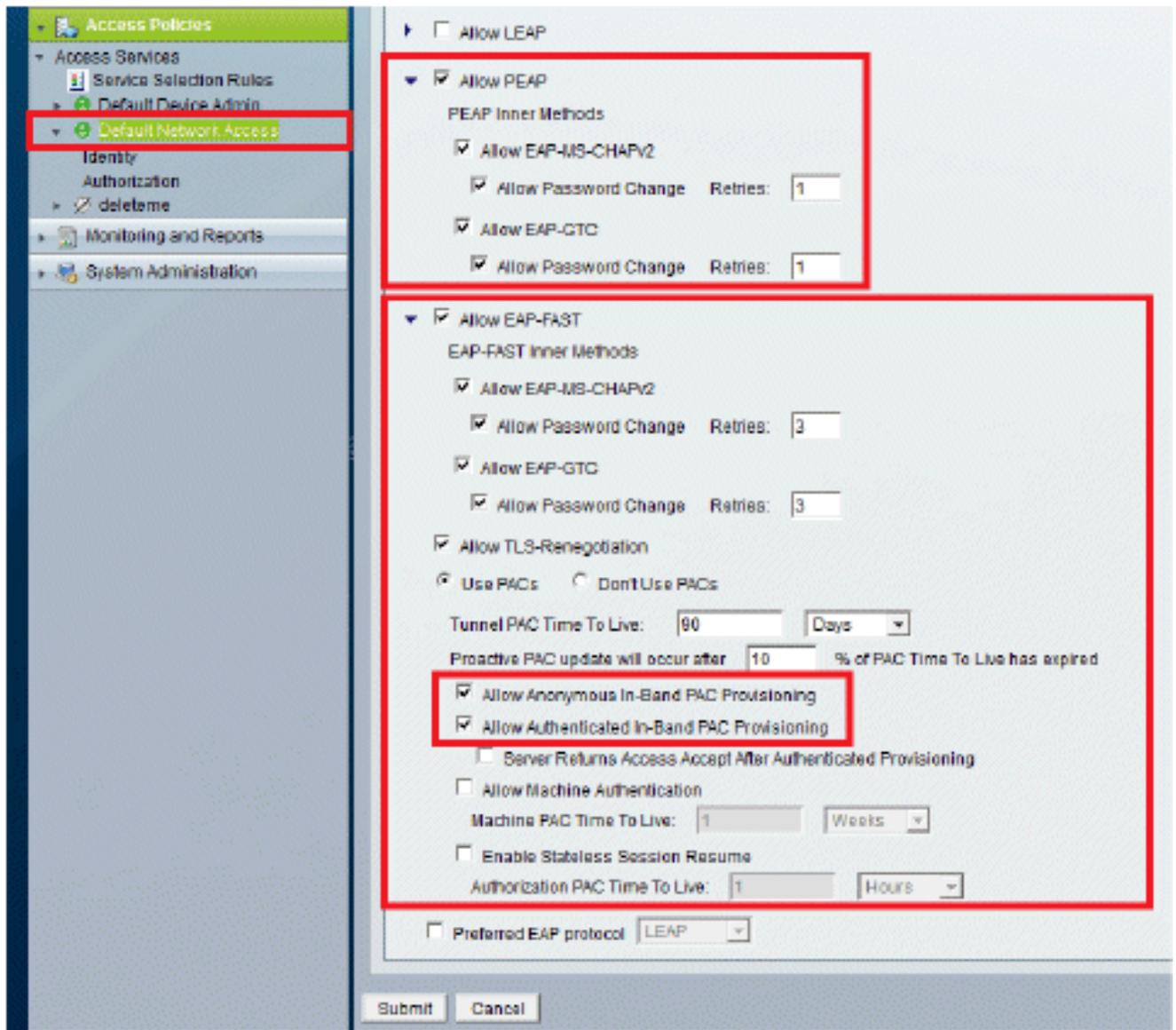
請完成以下步驟：

1. 前往Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"。



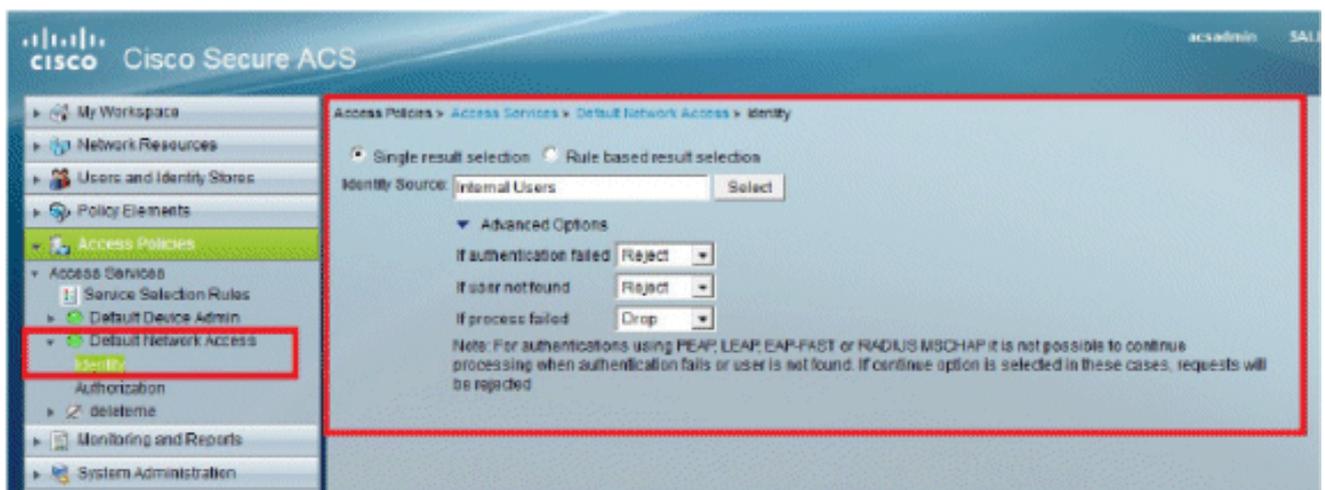
2. 確保您已啟用EAP-FAST和匿名帶內PAC調配。





3. 按一下「Submit」。

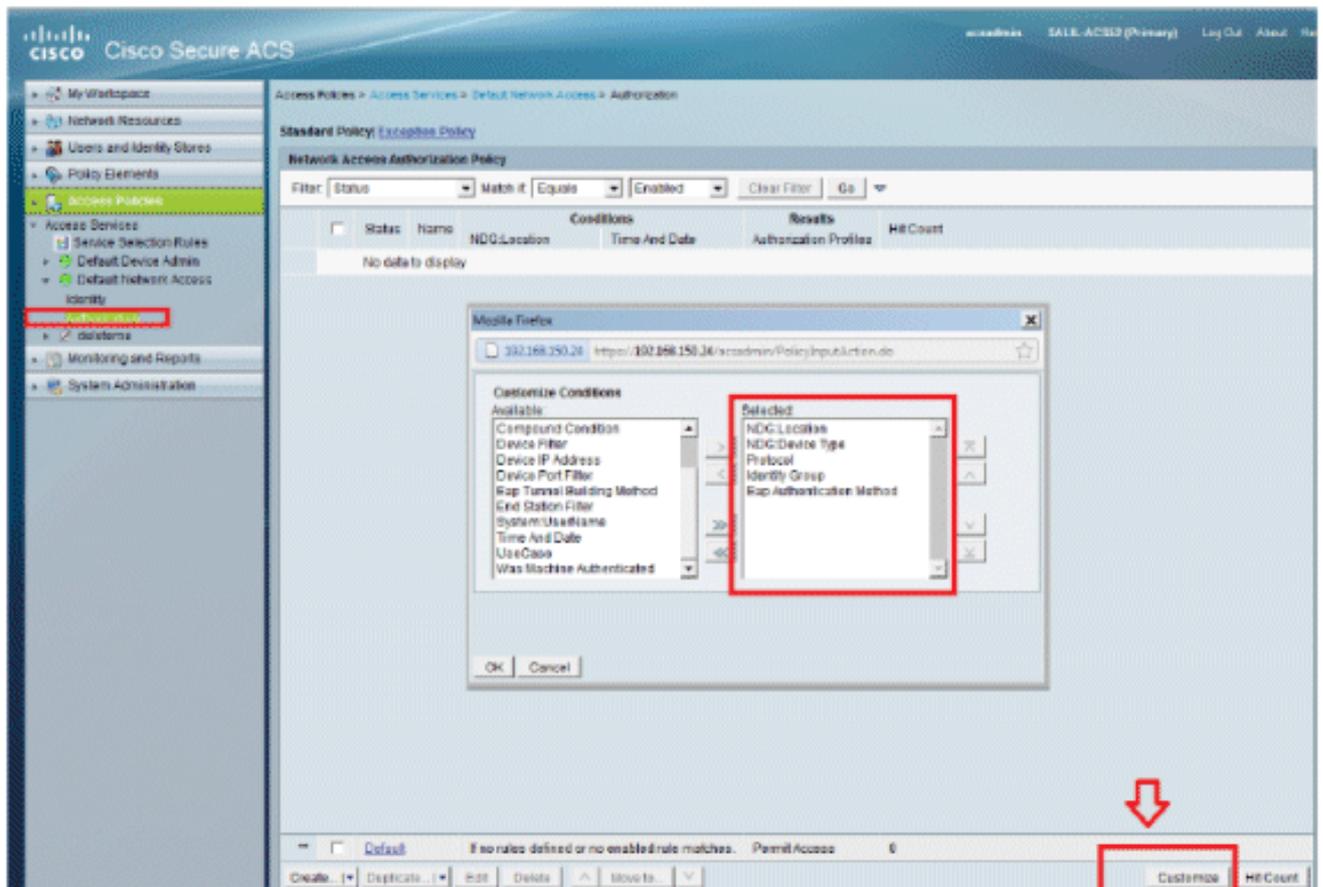
4. 驗證您選擇的身份組。在本示例中，使用Internal Users (在ACS上建立) 並儲存更改。



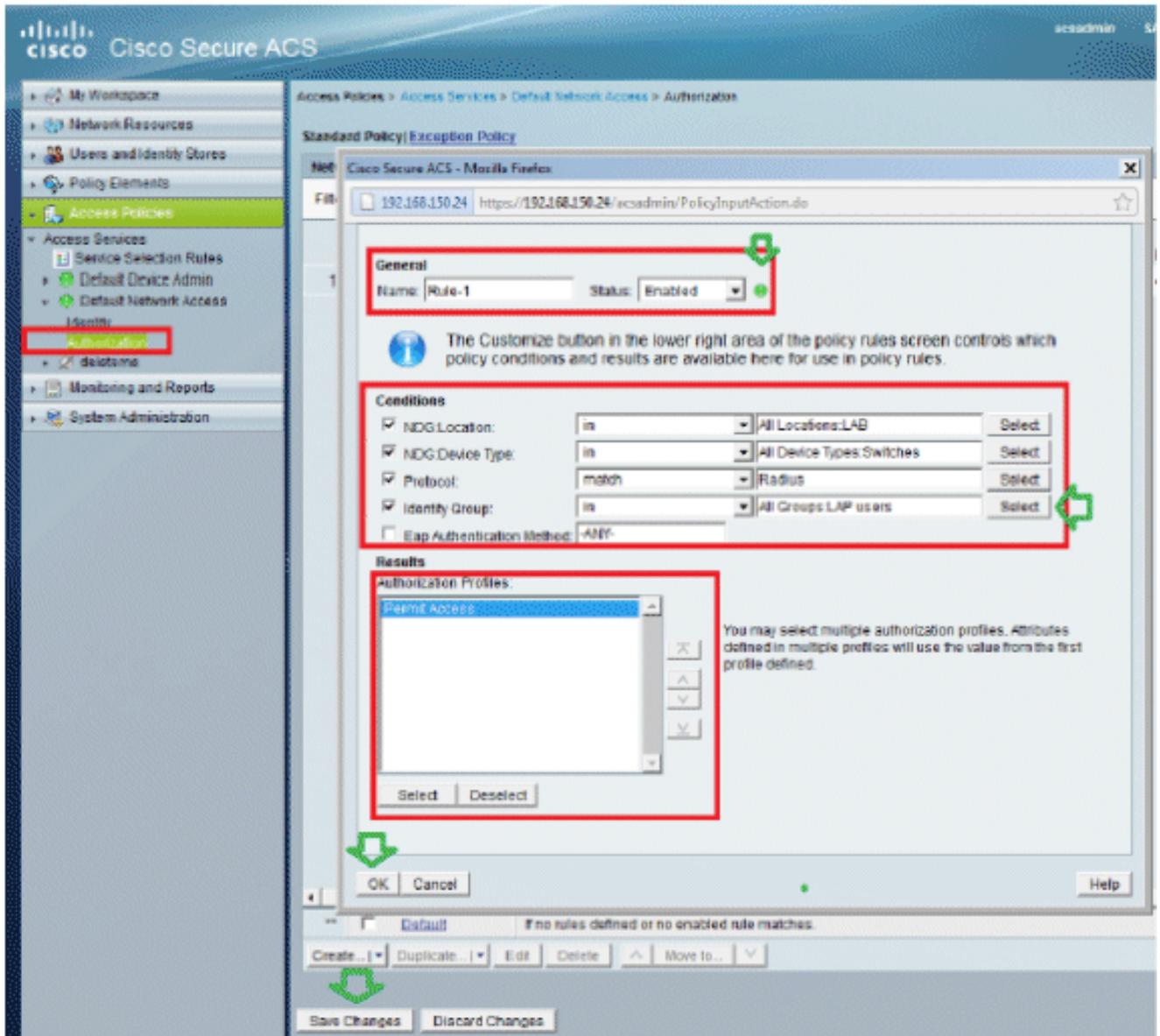
5. 若要驗證授權設定檔，請前往Access Policies > Access Services > Default Network Access >

Authorization。

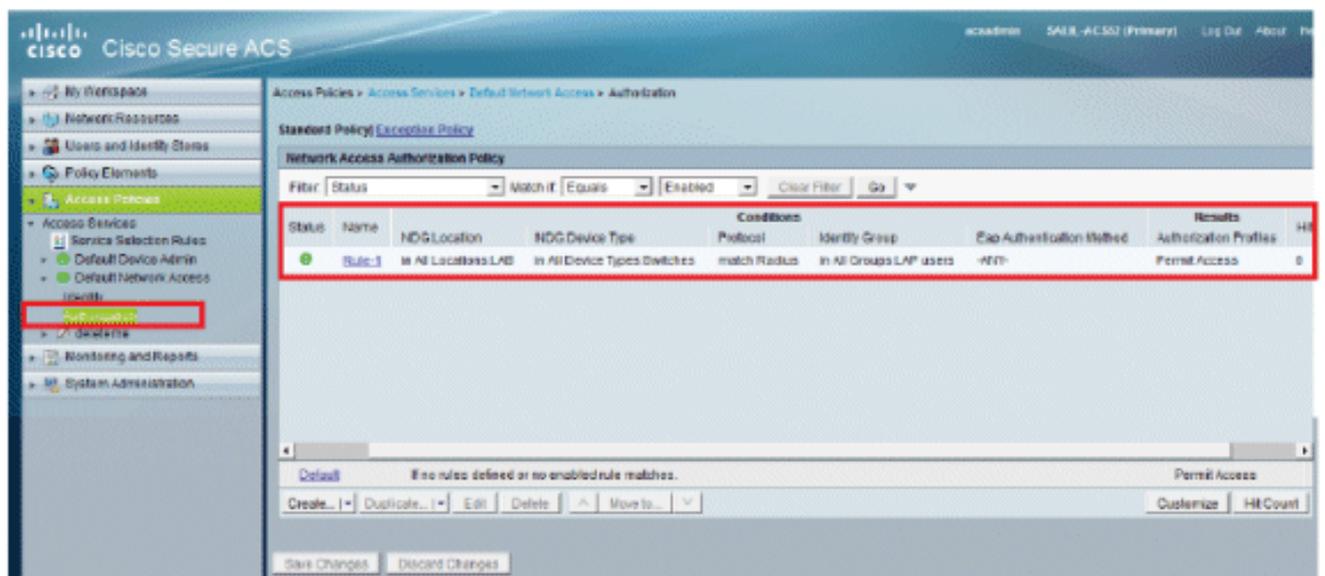
您可以自定義在什麼條件下允許使用者訪問網路，以及經過身份驗證後將通過的授權配置檔案（屬性）。此粒度僅在ACS 5.x中可用。在本示例中，Location、Device Type、Protocol、Identity Group和EAP Authentication Method均處於選中狀態。



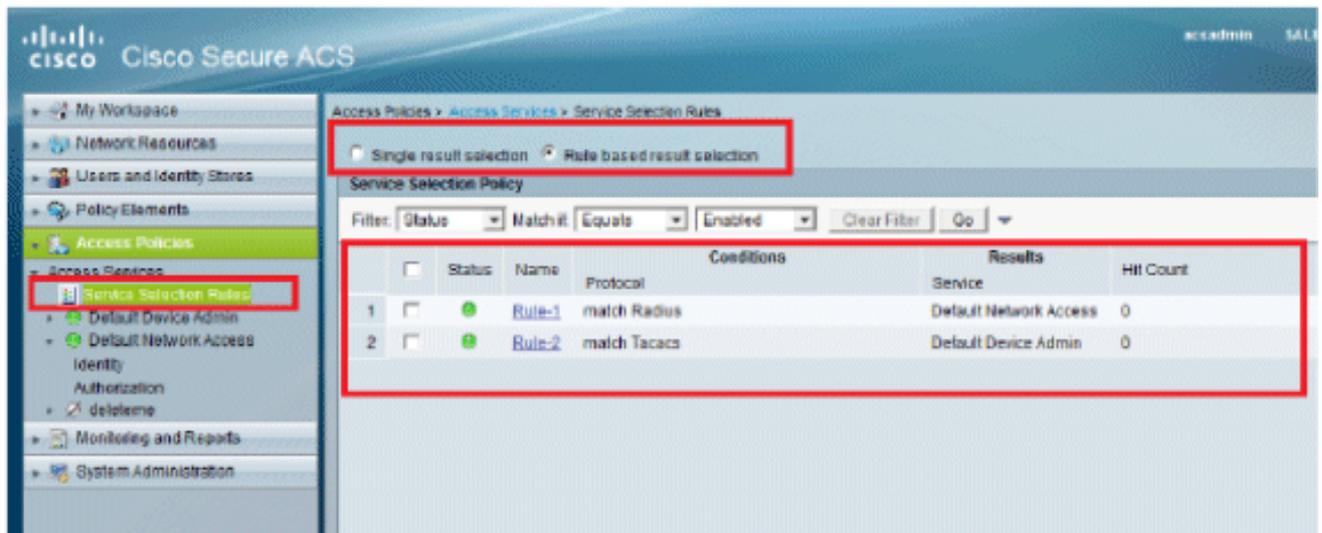
6. 按一下「OK」，然後「Save Changes」。
7. 下一步是建立規則。如果未定義規則，則允許LAP訪問而不帶任何條件。
8. 按一下Create > Rule-1。此規則適用於組「LAP使用者」中的使用者。



9. 按一下「Save Changes」。如果您希望拒絕不符合條件的使用者，請編輯預設規則以顯示「拒絕訪問」。



10. 最後一步是定義服務選擇規則。使用此頁可以配置簡單策略或基於規則的策略，以確定將哪種服務應用於傳入請求。舉例來說：



驗證

在交換器連線埠上啟用802.1x後，所有流量（除802.1x流量外）都會通過該連線埠遭到封鎖。已註冊到WLC的LAP將取消關聯。只有在802.1x驗證成功後，其他流量才允許通過。在交換器上啟用802.1x後，成功將LAP註冊到WLC表示LAP身份驗證成功。

AP控制檯：

```
<#root>
```

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 192.168.75.44:5247
```

!--- AP disconnects upon adding dot1x information in the gig0/11.

```
*Jan 29 09:10:30.104: %WIDS-5-DISABLED: IDS Signature is removed and disabled.
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to administratively down
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to administratively down
*Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset
```

```
Translating "CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25)
```

```
*Jan 29 09:10:36.203: status of voice_diag_test from WLC is false
```

```
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST] *Jan 29
```

!--- Authentication is successful and the AP gets an IP.

```
Translating "CISCO-CAPWAP-CONTROLLER.Wlab"...domain server (192.168.150.25)
*Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent
  peer_ip: 192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.000: %CAPWAP-5-CHANGED: CAPWAP changed state to
*Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS connection created
  successfully peer_ip: 192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.578: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44

*Jan 29 09:11:37.578: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN

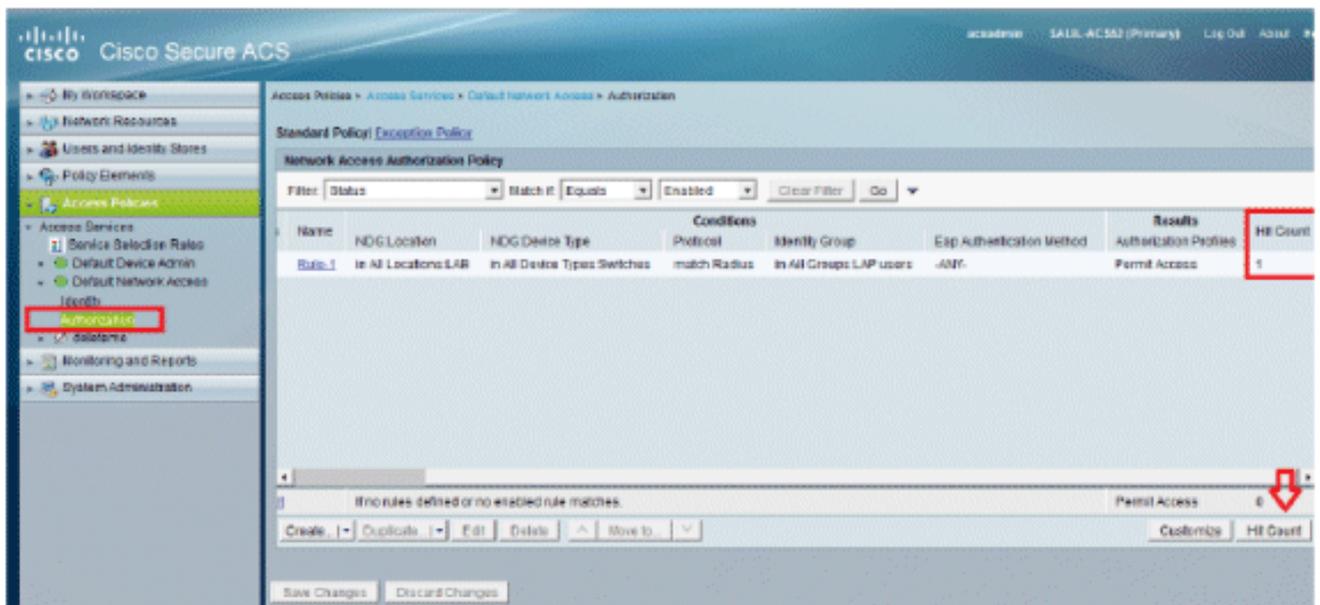
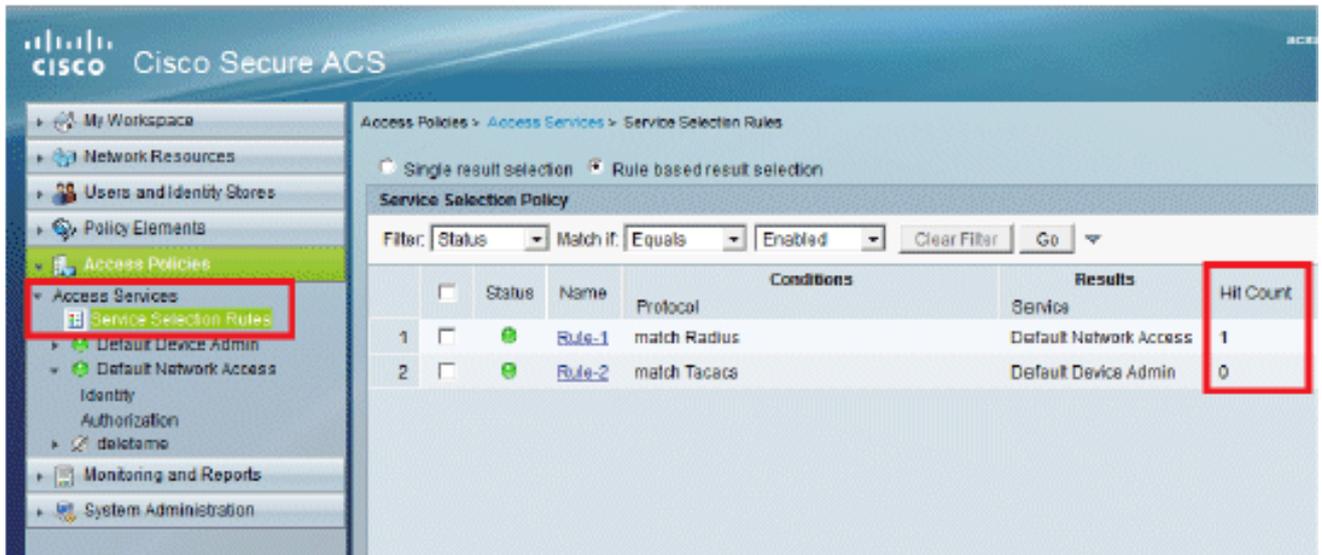
*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
  down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
  reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
  5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
  Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
  down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
  reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
  down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
  reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
  keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
  established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled
```

!--- AP joins the 5508-3 WLC.

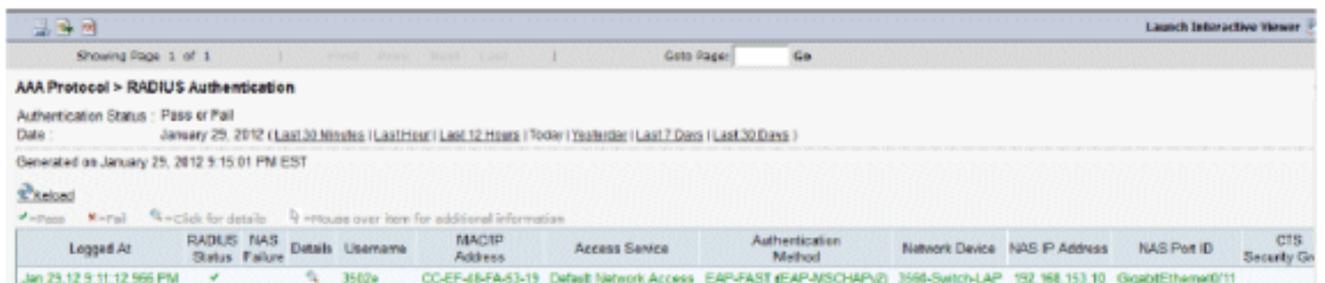
ACS日誌：

1. 檢視命中次數：

如果您在身份驗證的15分鐘內檢查日誌，請確保刷新命中計數。在同一頁面底部有一個Hit Count選項卡。



- 按一下「Monitoring and Reports」，系統會顯示一個新的彈出視窗。按一下「Authentications -RADIUS -Today」。您還可以按一下Details以驗證應用了哪個服務選擇規則。



疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [思科安全存取控制系統](#)
- [技術支援與文件 - Cisco Systems](#)

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）。