

# IPS 7.X:使用ACS 5.X作為Radius伺服器配置示例的使用者登入身份驗證

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[使用IME配置IPS以從ACS伺服器進行身份驗證](#)

[將ACS配置為RADIUS伺服器](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本文提供如何使用RADIUS伺服器設定使用者登入驗證的Cisco入侵防禦系統(IPS)的相關資訊。ACS用作RADIUS伺服器。

## 必要條件

### 需求

本文檔假定Cisco Intrusion Prevention System(IPS)已完全正常運行且已配置為允許Cisco Intrusion Prevention System Manager Express(IME)或CLI更改配置。除了本地AAA身份驗證外，您現在還可以配置RADIUS伺服器以執行感測器使用者身份驗證。Cisco Intrusion Prevention System 7.0(4)E4及更高版本提供將IPS配置為對使用者帳戶使用AAA RADIUS身份驗證的功能，這有助於操作大型IPS部署。

**注意：**沒有在IPS上啟用記帳的選項。IPS 7.04中支援RADIUS身份驗證，但不支援TACACS或授權或記帳。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科入侵防禦系統版本7.0(4)E4及更高版本
- 入侵防禦系統管理員Express版本7.1(1)及更高版本
- 思科安全存取控制伺服器5.x

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

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

## 設定

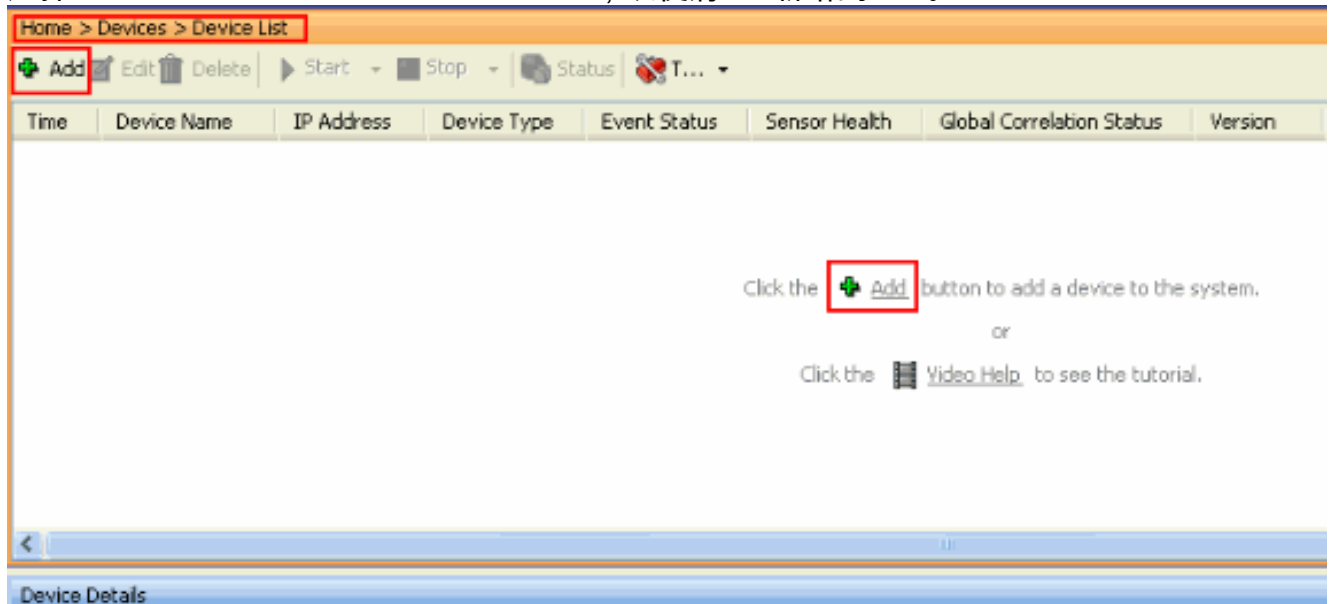
本節提供用於設定本文件中所述功能的資訊。

註：使用[Command Lookup Tool](#)（僅限註冊客戶）可獲取本節中使用的命令的詳細資訊。

### 使用IME配置IPS以從ACS伺服器進行身份驗證

完成以下步驟，以便將IPS新增到IME，然後配置IPS以從ACS伺服器進行身份驗證：

1. 選擇Home > Devices > Device List > Add，以便將IPS新增到IME。



2. 完成Add Device視窗中的欄位（如此處所示），以便提供有關IPS的詳細資訊。此處使用的感測器名稱為IPS。按一下「OK」（確定）。

**Add Device** [Close]

Sensor Name:

Sensor IP Address:

Web Server Port:

**Communication protocol**

Use encrypted connection (https)

Use non-encrypted connection (http)

**Authentication**

Configuration User Name:  ⓘ

Configuration Password:

Use the Same Account for Configuration and Event Subscription (This is not recommended):

Event Subscription User Name:  ⓘ

Event Subscription Password:

**Event Start Time (UTC)**

Most Recent Alerts

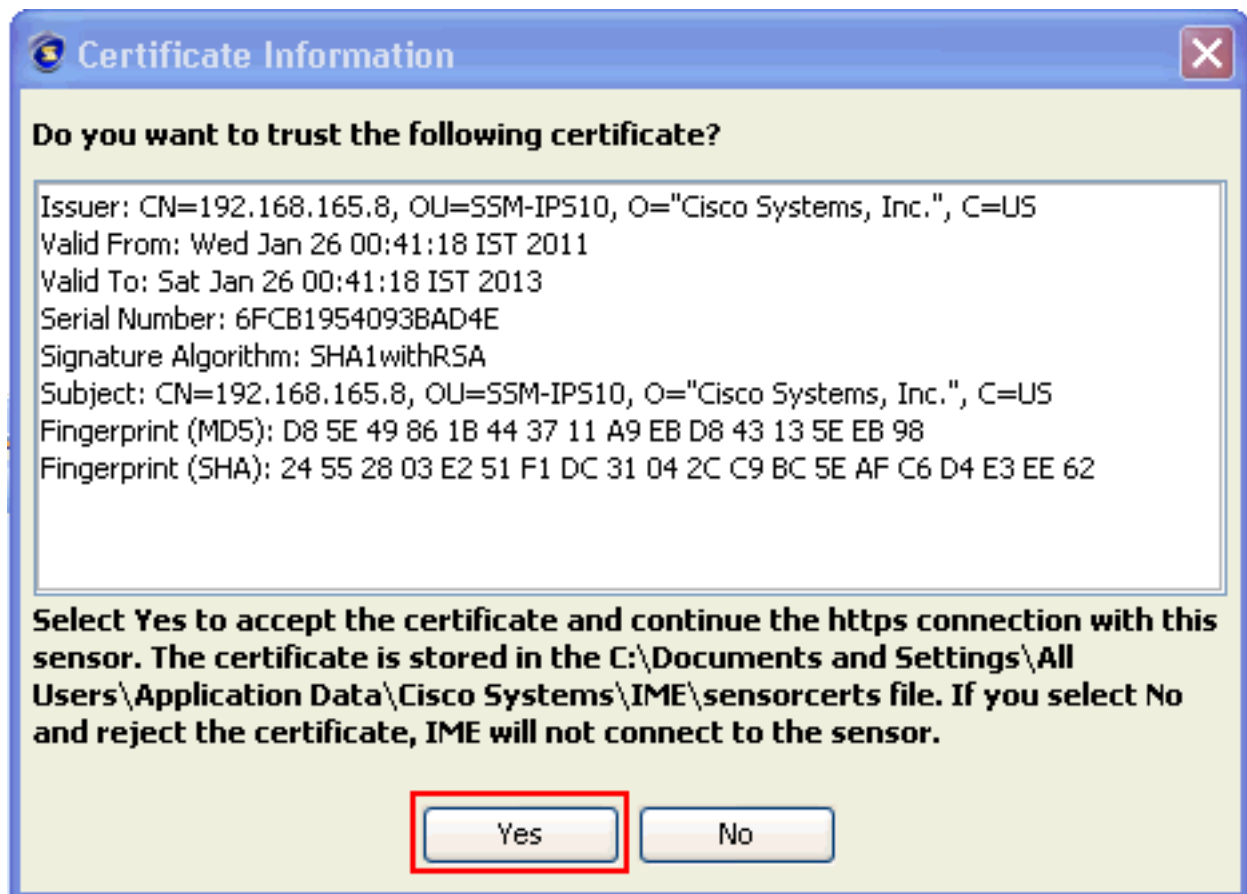
Start Date (YYYY:MM:DD):  :  :

Start Time (HH:MM:SS):  :  :

**Exclude alerts of the following severity level(s)**

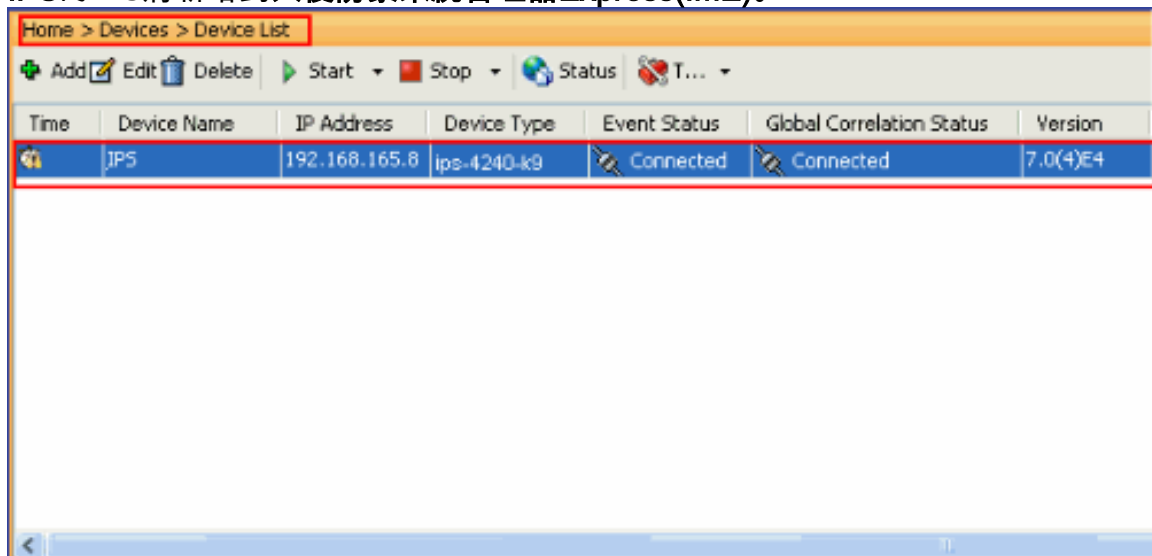
Informational  Low  Medium  High

3. 按一下「Yes」以接受憑證並繼續https連線到感應器。您必須接受該證書，才能連線並訪問感測器。



名為

IPS的IPS將新增到入侵防禦系統管理器Express(IME)。



4. 選擇 Configuration > IPS > Sensor Setup > Authentication，然後完成以下步驟：按一下「RADIUS Server」單選按鈕，以選擇「RADIUS Server」作為驗證裝置。提供RADIUS Authentication引數，如下所示。選擇Local和RADIUS作為控制檯身份驗證，以便在RADIUS伺服器不可用時使用本地身份驗證。按一下「Apply」。

Configuration > IPS > Sensor Setup > Authentication

User Authentication:  Local  Radius Server

**Local Authentication**  
Specify the users that have access to the sensor. The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed.

Username	Role	Status
disco	Administrator	Active
service	Service	Active

Add Edit Delete

**Radius Authentication**

Network Access ID:  Default User Role:

Allow Local Authentication if all Radius Servers are Unresponsive

**Primary Radius Server**

Server IP Address:   
 Authentication Port:   
 Timeout (seconds):   
 Shared Secret:

**Secondary Radius Server (optional)**

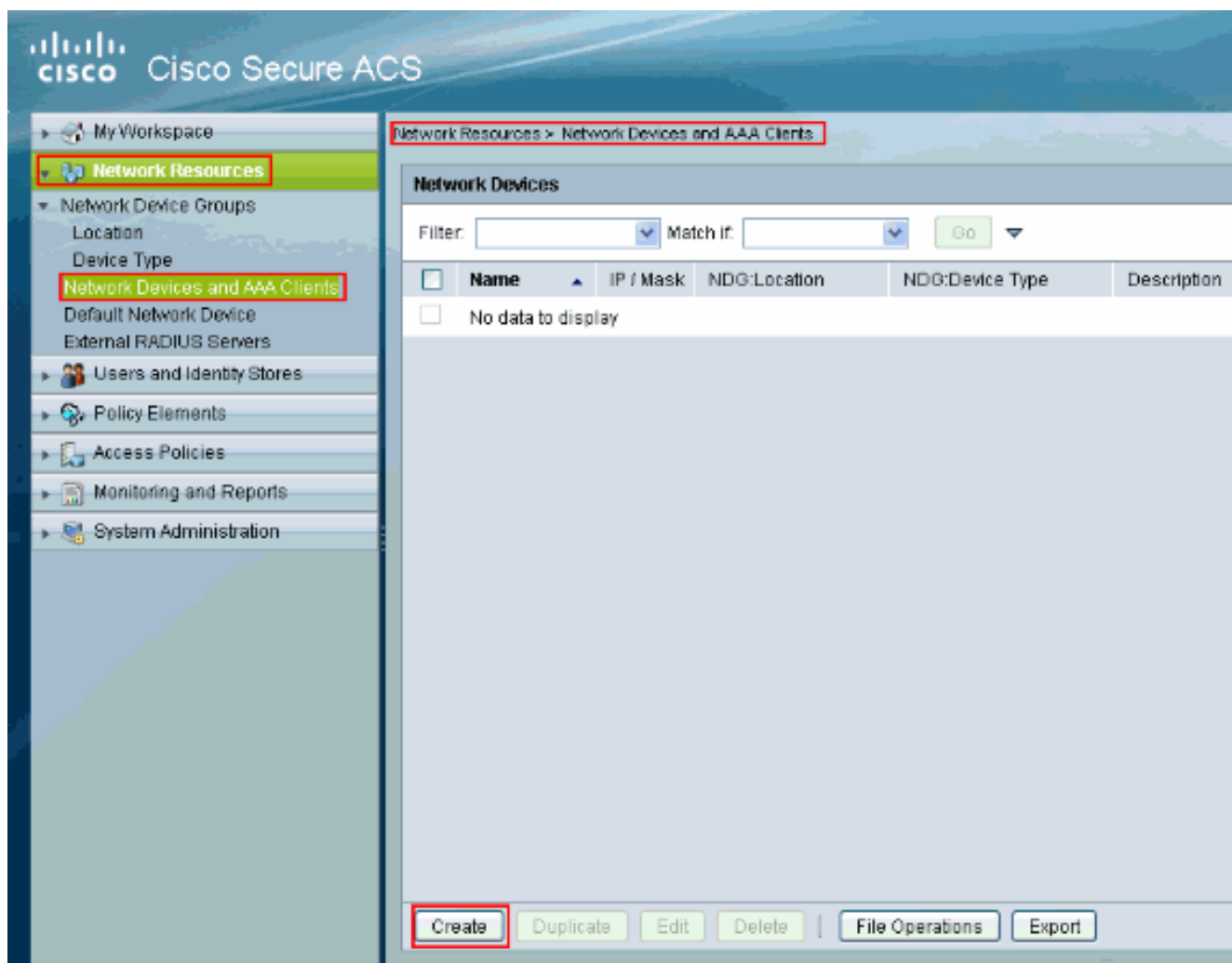
**Console Authentication**  
Console Authentication:

Apply Reset

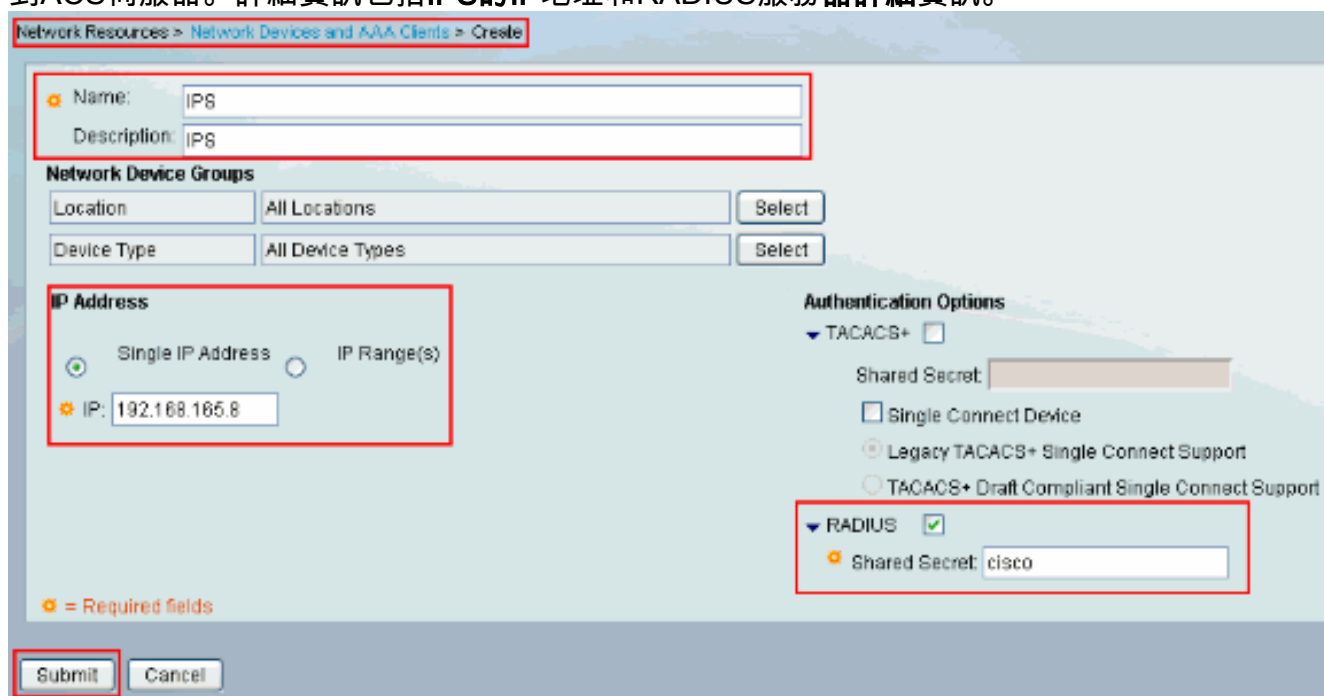
## 將ACS配置為RADIUS伺服器

完成以下步驟，將ACS配置為RADIUS伺服器：

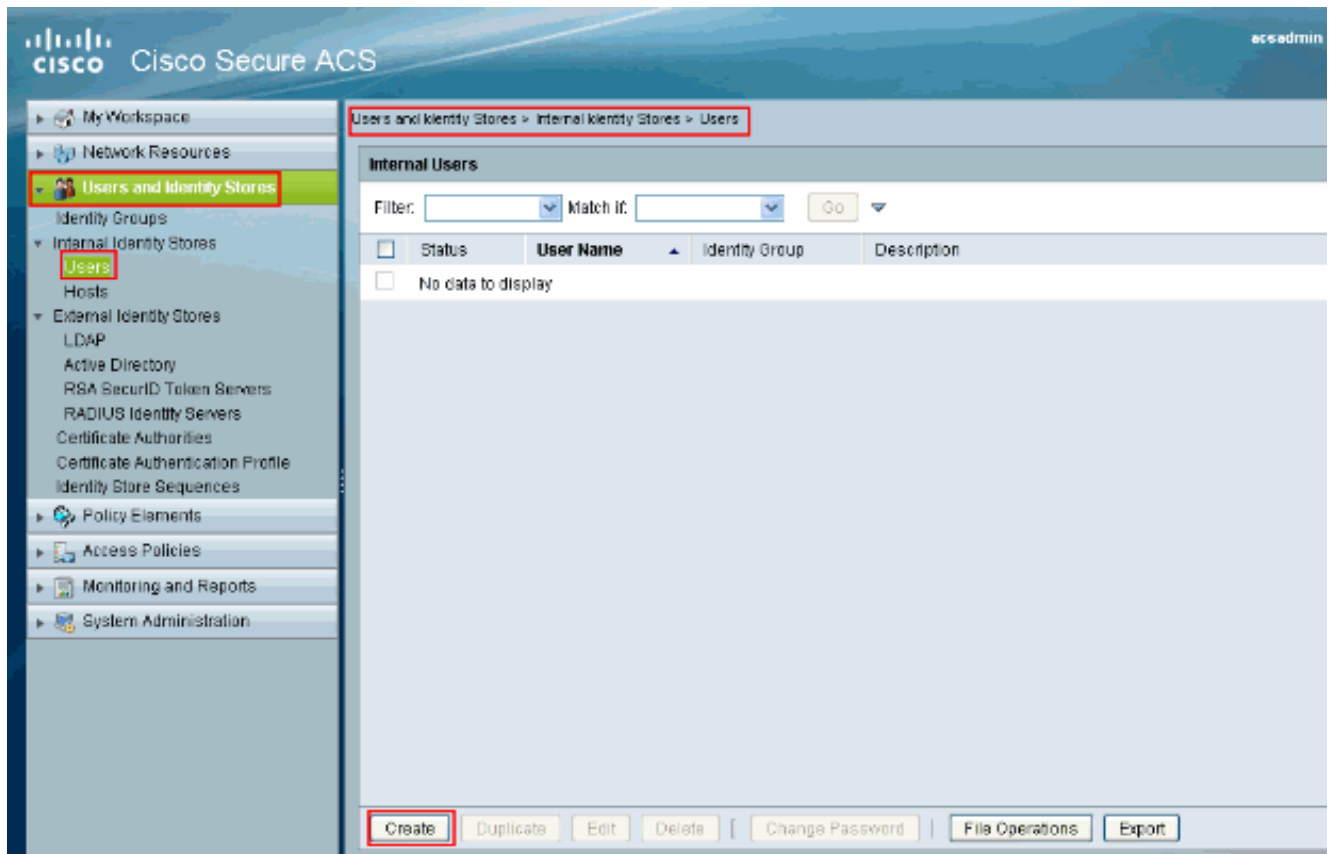
1. 選擇 **Network Resources > Network Devices and AAA Clients**，然後按一下 **Create** 以將IPS新增到ACS伺服器。



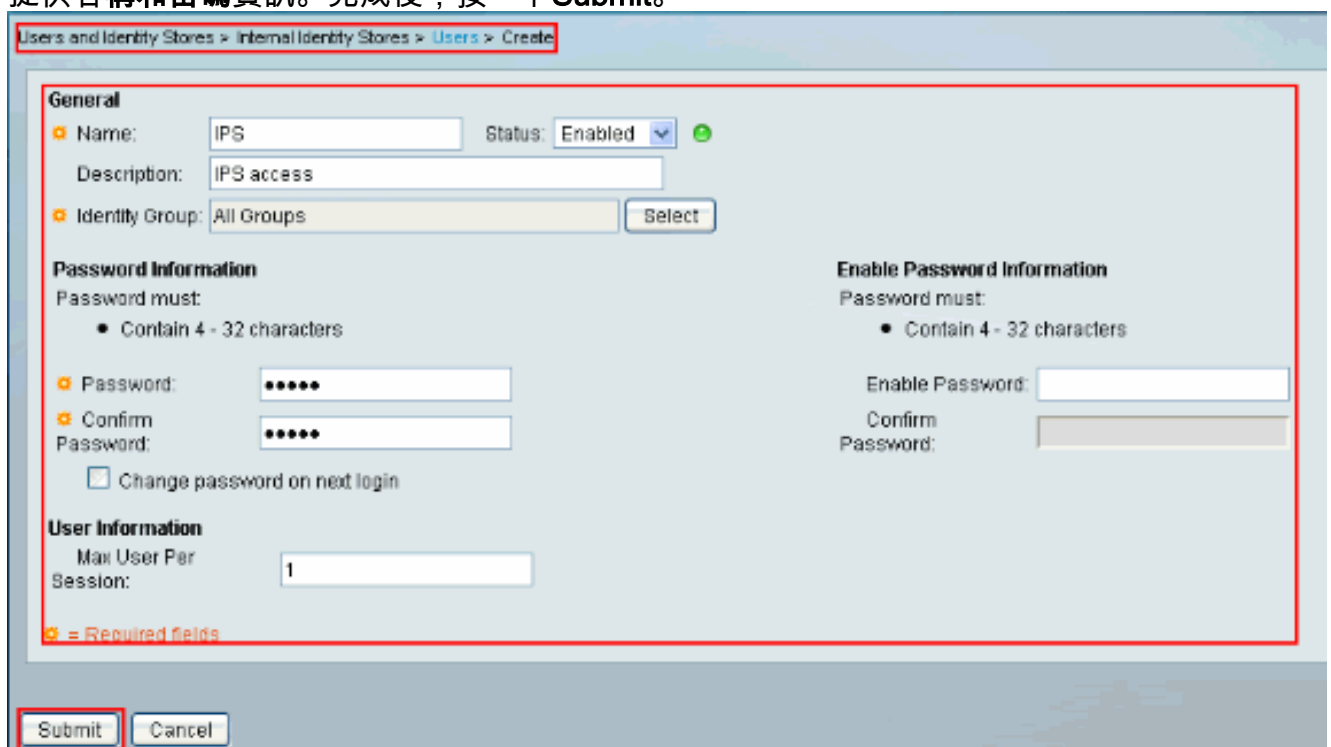
2. 提供客戶端所需的資訊（IPS是此處的客戶端），然後按一下**Submit**。這樣，IPS就可以新增到ACS伺服器。詳細資訊包括IPS的IP地址和RADIUS服務器詳細資訊。



3. 選擇Users and Identity stores > Internal Identity Stores > Users，然後按一下Create以建立新使用者。



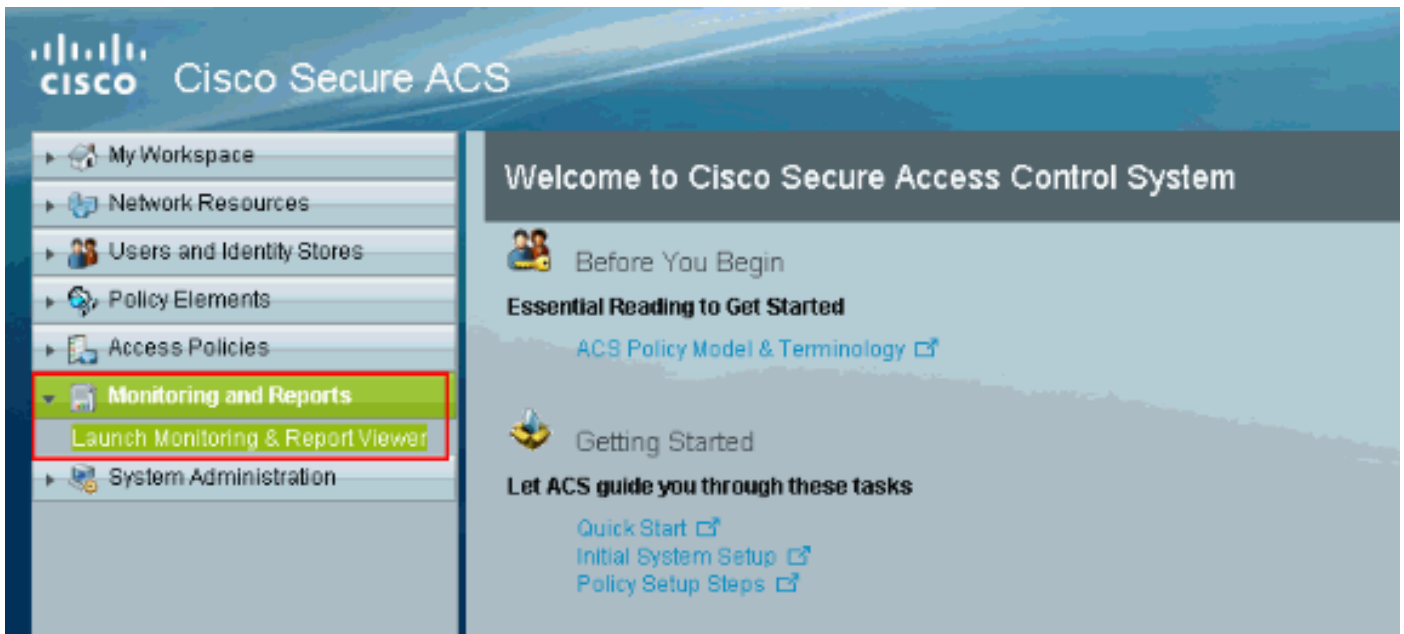
4. 提供名稱和密碼資訊。完成後，按一下Submit。



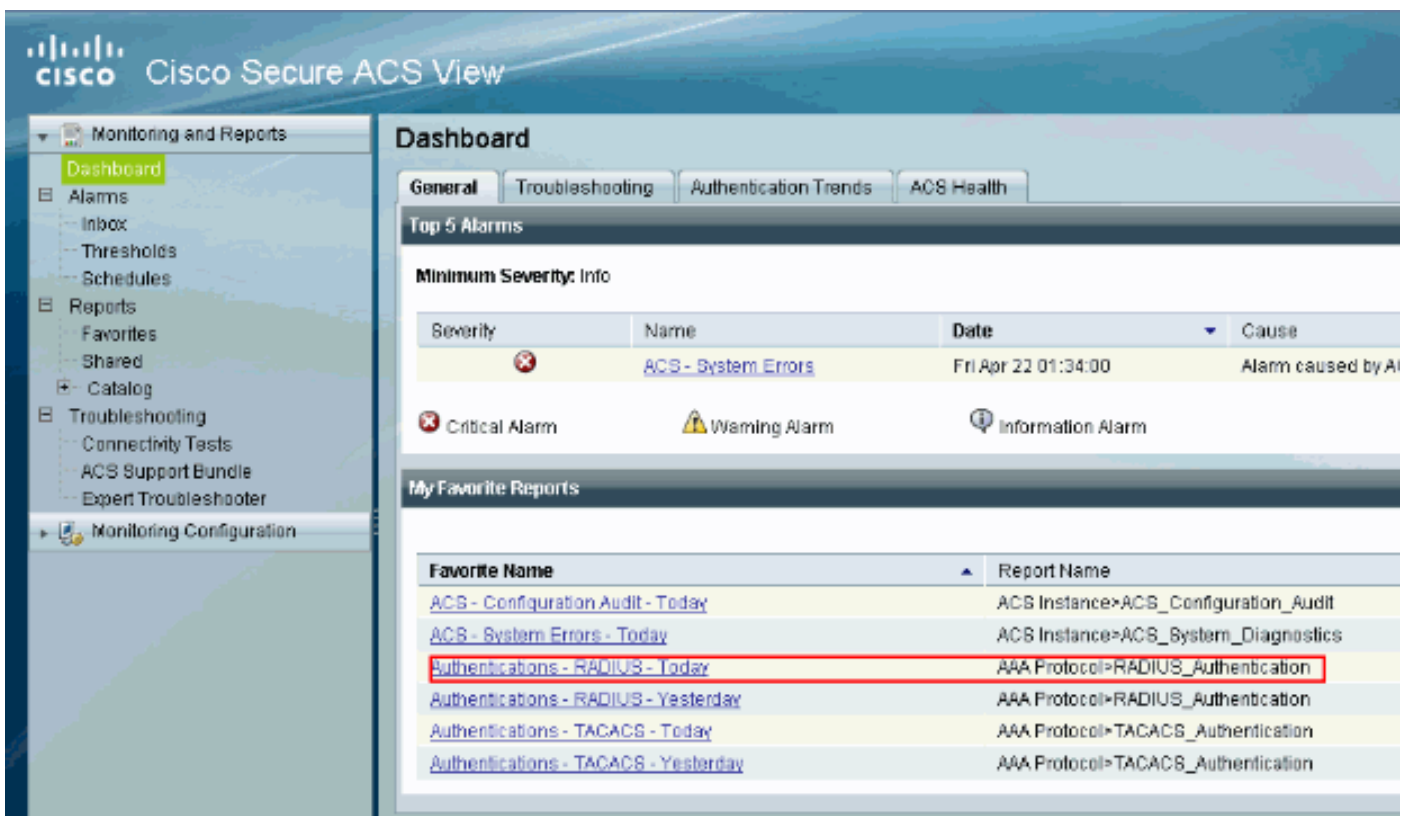
## 驗證

使用本節內容，確認您的組態是否正常運作。

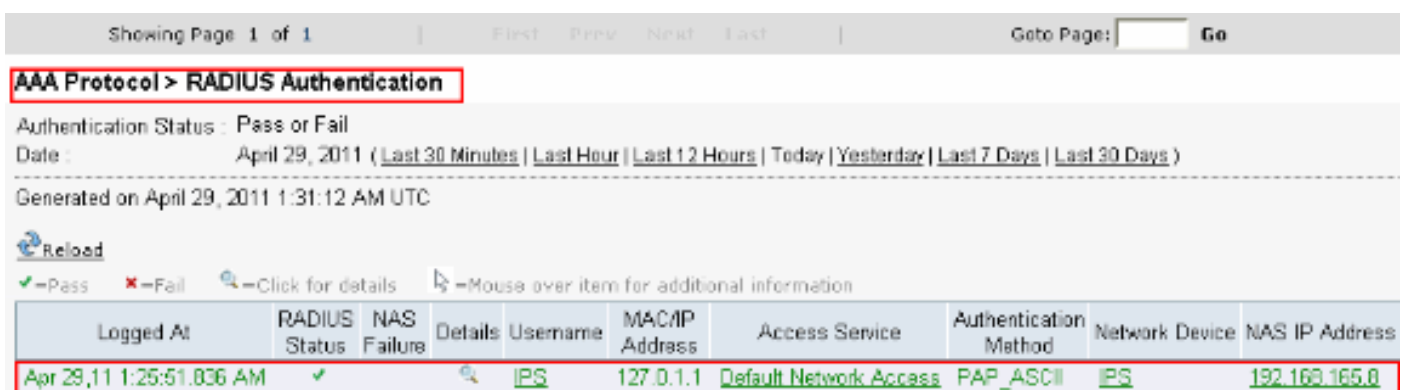
嘗試用新建立的使用者登入IPS。使用者通過身份驗證後，檢查ACS上的報告。



按一下「Authentications-RADIUS-Today」以檢視當前報告。



此圖顯示，連線到IPS的使用者由ACS伺服器進行身份驗證。





[輸出直譯器工具](#)(僅供[已註冊](#)客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析

。

## [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](#)

- [Cisco IPS 4200系列感應器支援頁面](#)
- [Cisco IPS 4200系列感測器命令參考](#)
- [Cisco IPS管理員Express版本](#)
- [IPsec協商/IKE通訊協定支援頁面](#)
- [思科安全存取控制伺服器 \( Windows專用 \)](#)
- [要求建議 \(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)