# 基於SSID的ISE策略配置示例

## 目錄



## 簡介

本文檔介紹如何在思科身份服務引擎(ISE)中配置授權策略以區分不同的服務集識別符號(SSID)。 組織在其無線網路中擁有多個SSID以用於各種目的的情況非常普遍。最常見的用途之一是為員工提供一個公司SSID，為組織訪客提供一個訪客SSID。

本指南假設：

1. 無線LAN控制器(WLC)已設定並且適用於所涉及的所有SSID。
2. 身份驗證工作在ISE涉及的所有SSID上。

**此系列中的其他檔案**

- 使用交換機和身份服務引擎進行中央Web身份驗證的配置示例
- WLC 和 ISE 的中央 Web 驗證的組態範例
- RADIUS/802.1x身份驗證的ISE訪客帳戶配置示例
- 使用iPEP ISE和ASA的VPN內聯狀態

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 無線LAN控制器版本7.3.101.0

- 身分識別服務引擎版本1.1.2.145

早期版本也同時具有這兩個功能。

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。

# 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(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

## 組態

本檔案會使用以下設定：

- 方法1:Airespace-Wlan-Id
- 方法2:Called-Station-ID

一次只能使用一種配置方法。如果同時實施這兩種配置，則ISE處理的量會增加並影響規則的可讀性。本文檔介紹了每種配置方法的優缺點。

### 方法1:Airespace-Wlan-Id

在WLC上建立的每個無線區域網路(WLAN)都有一個WLAN ID。WLAN ID顯示在WLAN Summary頁面上。


當客戶端連線到SSID時，ISE的RADIUS請求包含Airespace-WLAN-ID屬性。此簡單屬性用於在ISE中進行策略決策。此屬性的一個缺點是，如果分佈在多個控制器上的SSID上的WLAN ID不匹配。如果這描述了您的部署，請繼續執行方法2。

在這種情況下，Airespace-Wlan-Id用作條件。它可以作為一個簡單的條件（單獨使用）或複合條件（與另一個屬性結合）使用，以獲得期望的結果。本文檔介紹了這兩種使用案例。使用上述兩個SSID，可以建立這兩個規則。

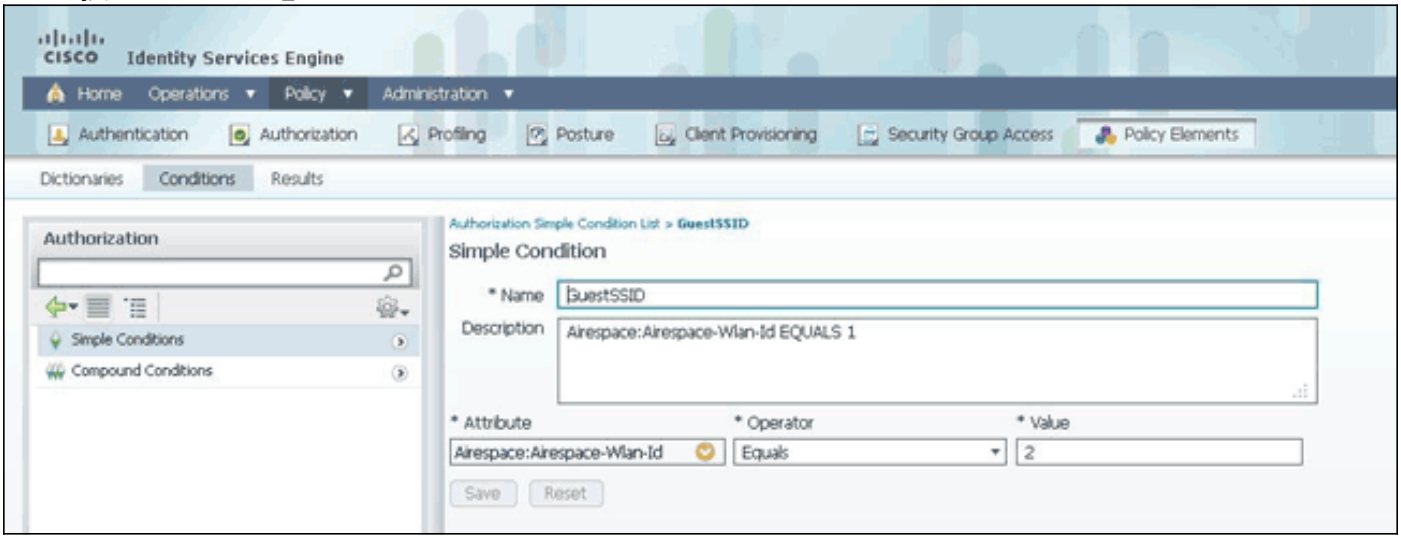
A)訪客使用者必須登入到訪客SSID。

B)企業使用者必須位於Active Directory(AD)組「Domain Users」（域使用者）中，並且必須登入到企業SSID。

### 規則A

規則A只有一個要求，因此您可以構建簡單條件（基於上述值）：

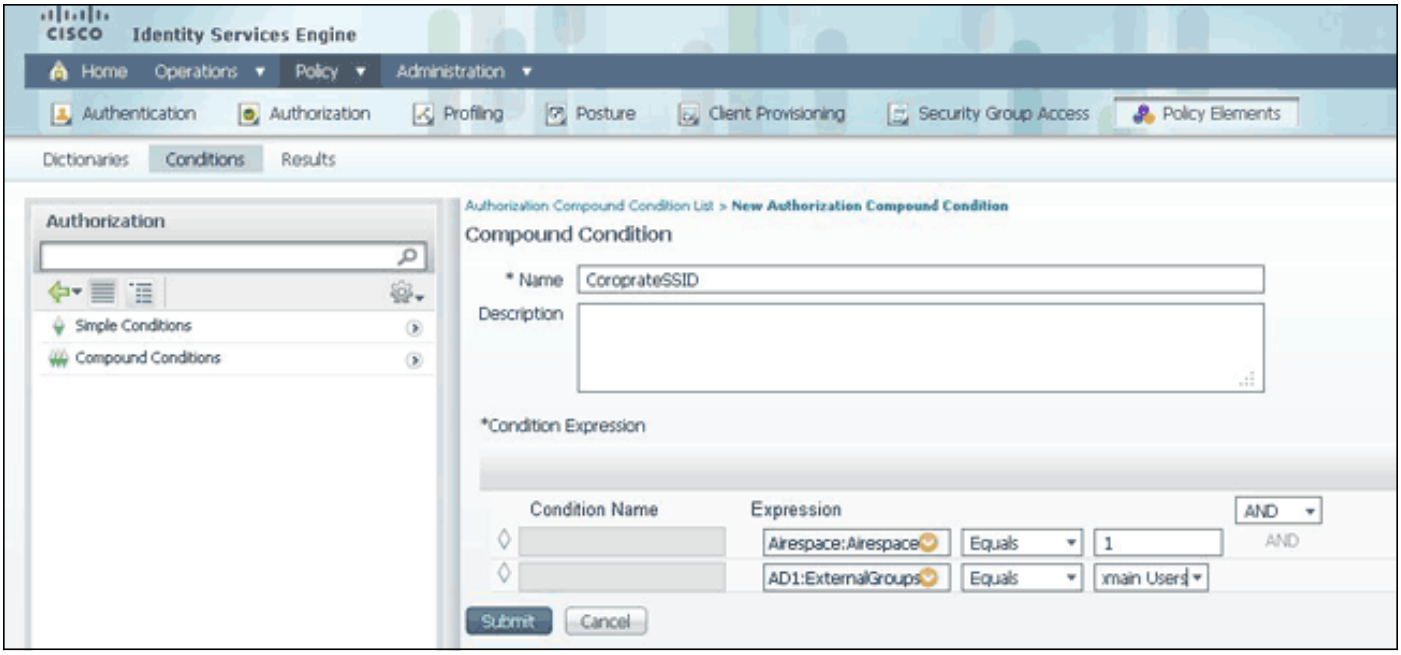
1. 在ISE中，轉至**Policy > Policy Elements > Conditions > Authorization > Simple Conditions**並建立新條件。
2. 在「名稱」欄位中，輸入條件名稱
3. 在「說明」欄位中輸入說明（可選）。
4. 在「屬性」下拉選單中，選擇**「Airespace > Airespace-Wlan-Id—[1]」**。
5. 從Operator下拉選單中選擇**Equals。**
6. 在「值」下拉式清單中選擇**2。**
7. 按一下**「Save」。**




### Rule B

規則B有兩個要求，因此您可以構建複合條件（基於上述值）：

1. 在ISE中，轉至**Policy > Policy Elements > Conditions > Authorization > Compound Conditions**並建立新條件。
2. 在「名稱」欄位中，輸入條件名稱。
3. 在「說明」欄位中輸入說明（可選）。
4. 選擇**建立新條件（高級選項）**。
5. 在「屬性」下拉選單中，選擇**「Airespace > Airespace-Wlan-Id—[1]」**。
6. 從Operator下拉選單中選擇**Equals。**
7. 在「值」下拉式清單中選擇**1。**
8. 按一下右側的齒輪，然後選擇**「新增屬性/值」**。
9. 從Attribute下拉選單中，選擇**AD1 > External Groups。**
10. 從Operator下拉選單中選擇**Equals。**
11. 從值下拉選單中，選擇所需的組。在此示例中，它設定為Domain Users。
12. 按一下**「Save」。**




**注意：在**本文檔中，我們使用在Policy > Policy Elements > Results > Authorization > Authorization Profiles下配置的簡單授權配置檔案。它們被設定為「允許訪問」，但可以進行調整以滿足部署的需要。

現在有了這些條件，我們可以將它們應用到授權策略。轉至**Policy > Authorization**。確定將規則插入到清單中的位置或編輯現有規則。

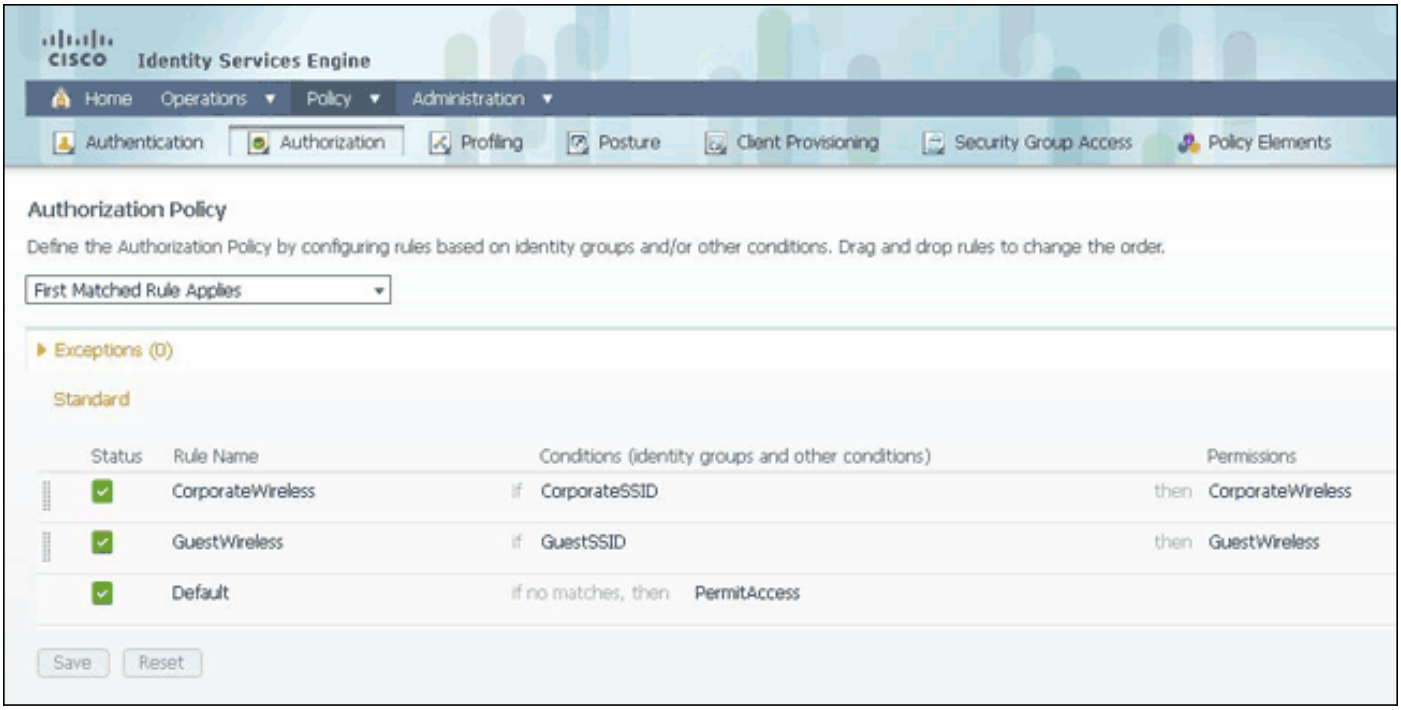
**訪客規則**

1. 點選現有規則右側的向下箭頭，然後選擇**插入新規則**。
2. 輸入訪客規則的名稱，並將身份組欄位設定為Any。
3. 在「條件」(Conditions)下，按一下加號並按一下**「從庫中選擇現有條件」(Select Existing Condition from Library)**。
4. 在Condition Name下，選擇**Simple Condition > GuestSSID**。
5. 在「許可權」下，為您的訪客使用者選擇適當的授權配置檔案。
6. 按一下**「完成」**。

**公司規則**

1. 點選現有規則右側的向下箭頭，然後選擇**插入新規則**。
2. 輸入公司規則的名稱，並將身份組欄位設定為Any。
3. 在「條件」(Conditions)下，按一下加號並按一下**「從庫中選擇現有條件」(Select Existing Condition from Library)**。
4. 在Condition Name下，選擇**Compound Condition > CorporateSSID**。
5. 在「許可權」下，為您的公司使用者選擇適當的授權配置檔案。
6. 按一下**「完成」**。

**注意：**在按一下「策略清單」底部的「儲存」之前，不會將此螢幕中所做的更改應用於您的部署。




### 方法2:Called-Station-ID

可以將WLC配置為在RADIUS Called-Station-ID屬性中傳送SSID名稱，這反過來又可以作為ISE的一個條件。此屬性的優勢在於，無論WLC上的WLAN ID設定為何，都可使用該屬性。預設情況下，WLC不會在Called-Station-ID屬性中傳送SSID。要在WLC上啟用此功能，請轉到**Security > AAA > RADIUS > Authentication**，並將Call Station ID Type設定為AP MAC Address:SSID。這會將Called-Station-ID的格式設定*為<使用者正在連線的AP的MAC>:<SSID Name>*。


您可以從WLAN摘要頁面看到要傳送的SSID名稱。


由於Called-Station-Id屬性還包含AP的MAC地址，因此使用正規表示式(REGEX)來匹配ISE策略中的SSID名稱。條件配置中的運算子「Matches」可以從值欄位讀取REGEX。

### REGEX示例

**'Starts with'** — 例如，使用REGEX值**^(Acme)。*** — 此條件配置為CERTIFICATE:Organization MATCHES 'Acme'（任何與以"Acme"開頭的條件匹配）。

**'Ends with'** — 例如，使用REGEX值。***(mktg)$** — 此條件配置為CERTIFICATE:Organization MATCHES 'mktg'（任何條件以"mktg"結尾的匹配項）。

**'Contains' — 例**如，使用。***(1234)的REGEX值。*** — 此條件配置為CERTIFICATE:Organization MATCHES '1234'(與包含「1234」的條件（例如Eng1234、1234Dev和Corp1234Mktg）的任何匹配。

**'not start with'** — 例如，使用REGEX值**^(?!LDAP)。*** — 此條件配置為CERTIFICATE:Organization MATCHES 'LDAP'(與不以「LDAP」開頭的條件（如usLDAP或CorpLDAPmktg）的任何匹配。

Called-Station-ID以SSID名稱結尾，因此本示例中使用的REGEX為**.*(:<SSID NAME>)$**。進行組態時，請記住這一點。

使用上述兩個SSID，您可以建立符合以下要求的兩個規則：

A)訪客使用者必須登入到訪客SSID。

B)企業使用者必須位於AD組「Domain Users」中，並且必須登入到企業SSID。

**規則A**

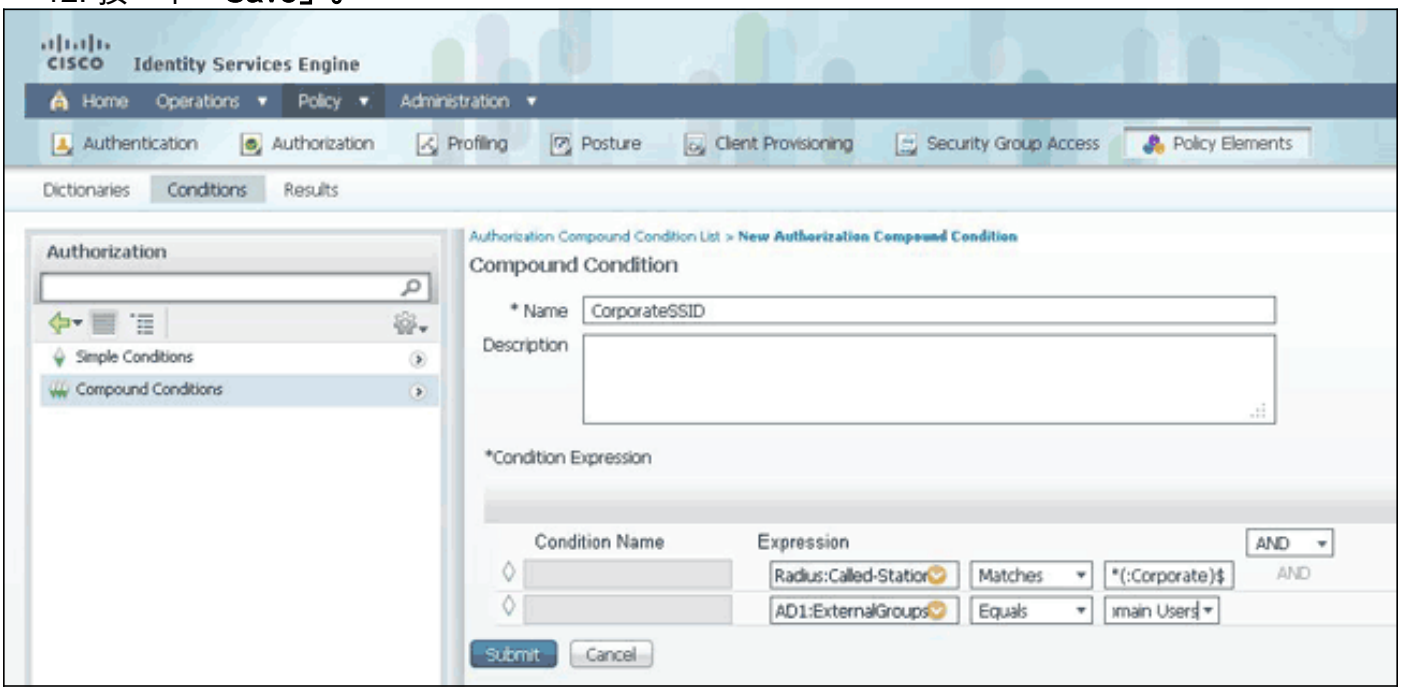
規則A只有一個要求，因此您可以構建簡單條件（基於上述值）：

1. 在ISE中，轉至**Policy > Policy Elements > Conditions > Authorization > Simple Conditions**並建立新條件。
2. 在「名稱」欄位中，輸入條件名稱。
3. 在「說明」欄位中輸入說明（可選）。
4. 在「屬性」下拉選單中，選擇**Radius -> Called-Station-ID -[30]**。
5. 從Operator下拉選單中，選擇**Matches**。
6. 從Value下拉選單中選擇**.*(:Guest)$**。區分大小寫。
7. 按一下「**Save**」。


**Rule B**

規則B有兩個要求，因此您可以構建複合條件（基於上述值）：

1. 在ISE中，轉至**Policy > Policy Elements > Conditions > Authorization > Compound Conditions**並建立新條件。
2. 在「名稱」欄位中，輸入條件名稱。
3. 在「說明」欄位中輸入說明（可選）。
4. 選擇**建立新條件（高級選項）**。
5. 在「屬性」下拉選單中，選擇**Radius -> Called-Station-Id -[30]**。
6. 從Operator下拉選單中，選擇**Matches。**
7. 從「值」下拉選單中，選擇**.*(:Corporate)$**。區分大小寫。
8. 按一下右側的齒輪，然後選擇**「新增屬性/值」**。
9. 從Attribute下拉選單中，選擇**AD1 > External Groups**。
10. 從Operator下拉選單中選擇**Equals。**
11. 從值下拉選單中，選擇所需的組。在此示例中，它設定為Domain Users。
12. 按一下**「Save」。**




**注意：在**本文檔中，我們使用在Policy > Policy Elements > Results > Authorization > Authorization Profiles下配置的簡單授權配置檔案。它們被設定為「允許訪問」，但可以進行調整以滿足部署的需要。

現在條件已配置，請將其應用於授權策略。轉至**Policy > Authorization**。將規則插入到清單中適當的位置或編輯現有規則。

**訪客規則**

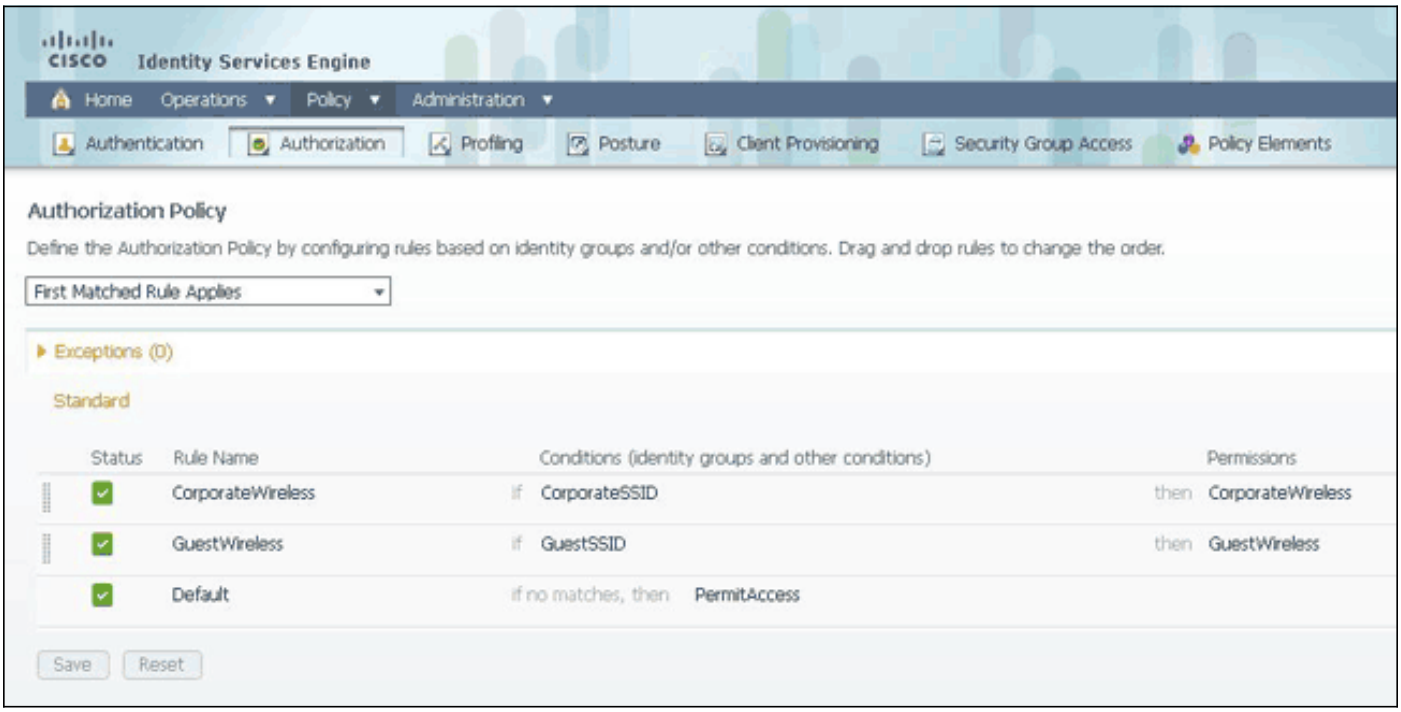
1. 按一下現有規則右側的向下箭頭，然後選擇**插入新規則**。
2. 輸入訪客規則的名稱，並將身份組欄位設定為Any。
3. 在「條件」(Conditions)下，按一下加號並按一下**「從庫中選擇現有條件」(Select Existing Condition from Library)**。
4. 在Condition Name下，選擇**Simple Condition > GuestSSID**
5. 在「許可權」下，為您的訪客使用者選擇適當的授權配置檔案。
6. 按一下「**完成**」。

**公司規則**

1. 按一下現有規則右側的向下箭頭，然後選擇**插入新規則**。

2. 輸入公司規則的名稱，並將身份組欄位設定為Any。
3. 在「條件」(Conditions)下，按一下加號並按一下**「從庫中選擇現有條件」(Select Existing Condition from Library)**。
4. 在Condition Name下，選擇**Compound Condition > CorporateSSID**。
5. 在「許可權」下，為您的公司使用者選擇適當的授權配置檔案。
6. 按一下**「完成」**。
7. 按一下Policy清單底部的**Save**。

**注意**：在按一下「策略清單」底部的「儲存」之前，不會將此螢幕中所做的更改應用於您的部署。



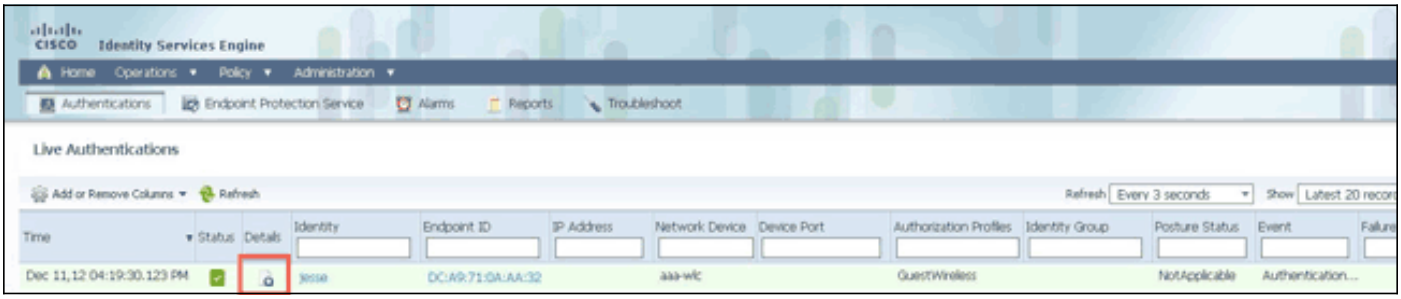

## 驗證

目前沒有適用於此組態的驗證程序。

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

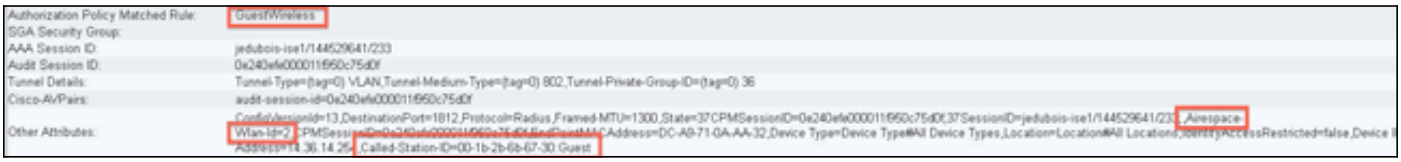
要瞭解是否正確建立了策略並確保ISE接收到正確的屬性，請檢視詳細的身份驗證報告，瞭解使用者身份驗證通過或失敗。選擇**Operations > Authentications**，然後按一下**Details**圖示進行身份驗證。




首先檢查身份驗證摘要。這顯示了身份驗證的基本資訊，其中包括提供給使用者的授權配置檔案。

| Authentication Summary | |
|---|---|
| Logged At: | December 11,2012 4:19:30.123 PM |
| RADIUS Status: | Authentication succeeded |
| NAS Failure: | |
| Username: | jesse |
| MAC/IP Address: | DC:A9:71:0A:AA:32 |
| Network Device: | aaa-wlc : 14.36.14.254 : |
| Allowed Protocol: | Default Network Access |
| Identity Store: | AD1 |
| Authorization Profiles: | GuestWireless |
| SGA Security Group: | |
| Authentication Protocol : | PEAP(EAP-MSCHAPv2) |

如果策略不正確，身份驗證詳細資訊將顯示從WLC傳送的Airespace-Wlan-Id和什麼被叫站Id。相應地調整規則。授權策略匹配規則確認身份驗證是否與預期規則匹配。




這些規則通常配置錯誤。要顯示配置問題，請將規則與身份驗證詳細資訊中顯示的內容進行匹配。如果您在「Other Attributes」欄位中看不到屬性，請確認WLC已正確設定。

## 相關資訊

- 技術支援與文件 - Cisco Systems