配置ISE訪客臨時和永久訪問

目錄

簡介

本文檔介紹身份服務引擎(ISE)訪客訪問配置的不同方法。根據授權規則中的不同條件：

- 可以提供對網路的永久訪問（無需進行後續身份驗證）
- 可以提供對網路的臨時訪問（需要在會話過期後進行訪客身份驗證）

此外，還會結合對臨時存取案例的影響，提供作業階段移除的特定無線LAN控制器(WLC)行為。

必要條件

需求

思科建議您瞭解以下主題：

- ISE部署和訪客流量
- 無線區域網路控制器(WLC)的組態

採用元件

本文中的資訊係根據以下軟體和硬體版本：

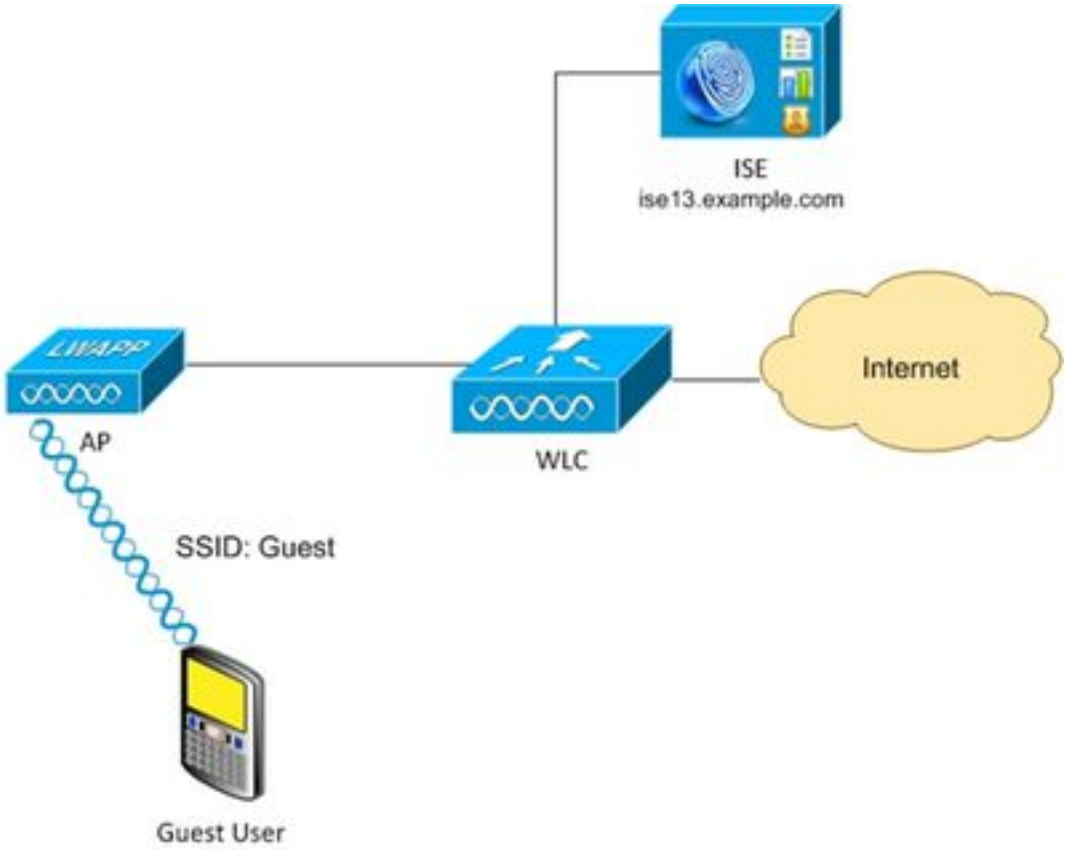
- Microsoft Windows 7
- Cisco WLC版本7.6及更高版本

- ISE軟體1.3版及更高版本

設定

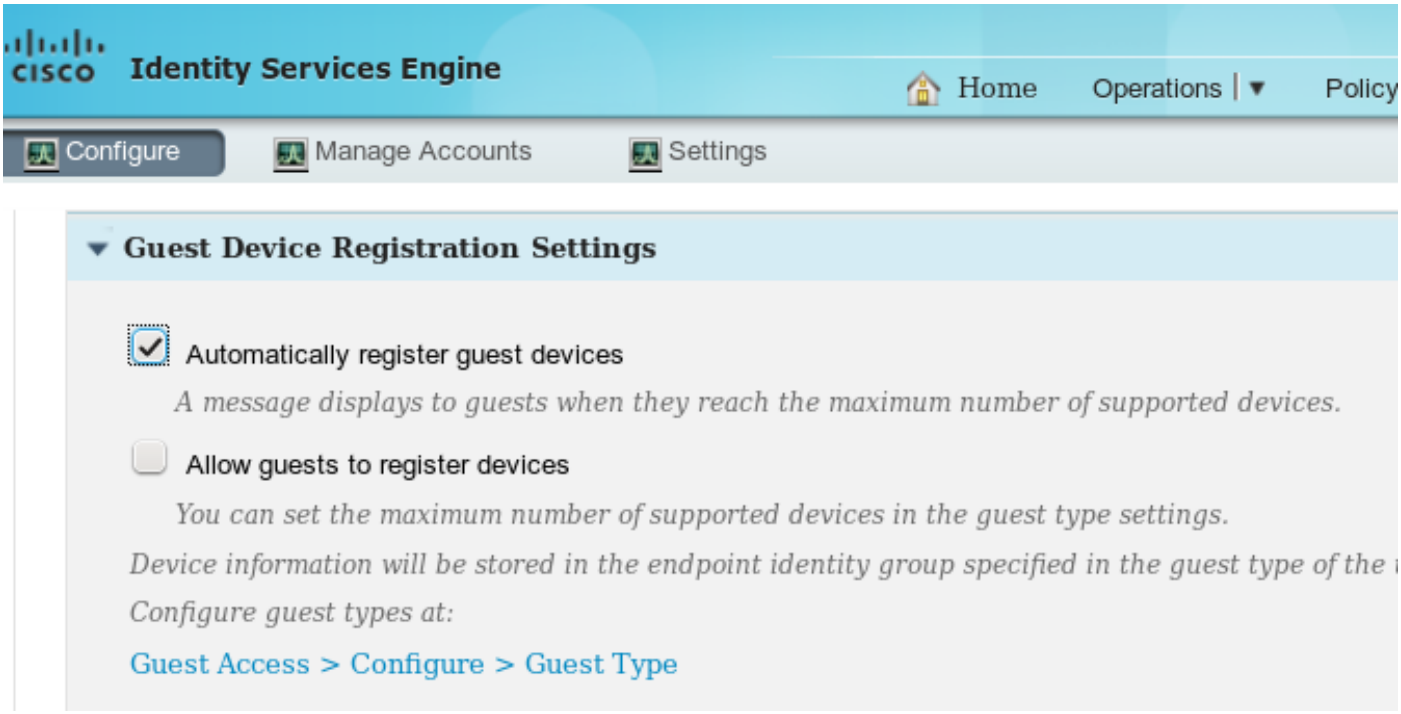
有關基本訪客訪問配置，請通過配置示例檢查參考。本文重點介紹授權規則配置以及授權條件之間的差異。

網路圖表

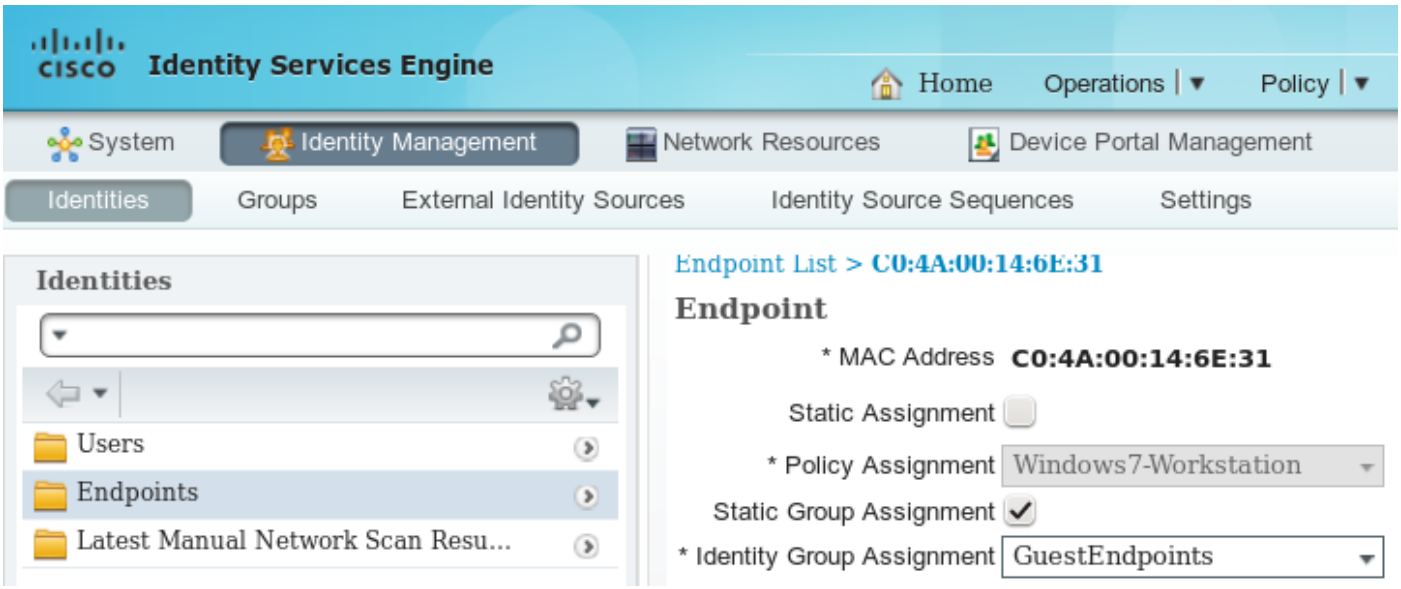


永久訪問

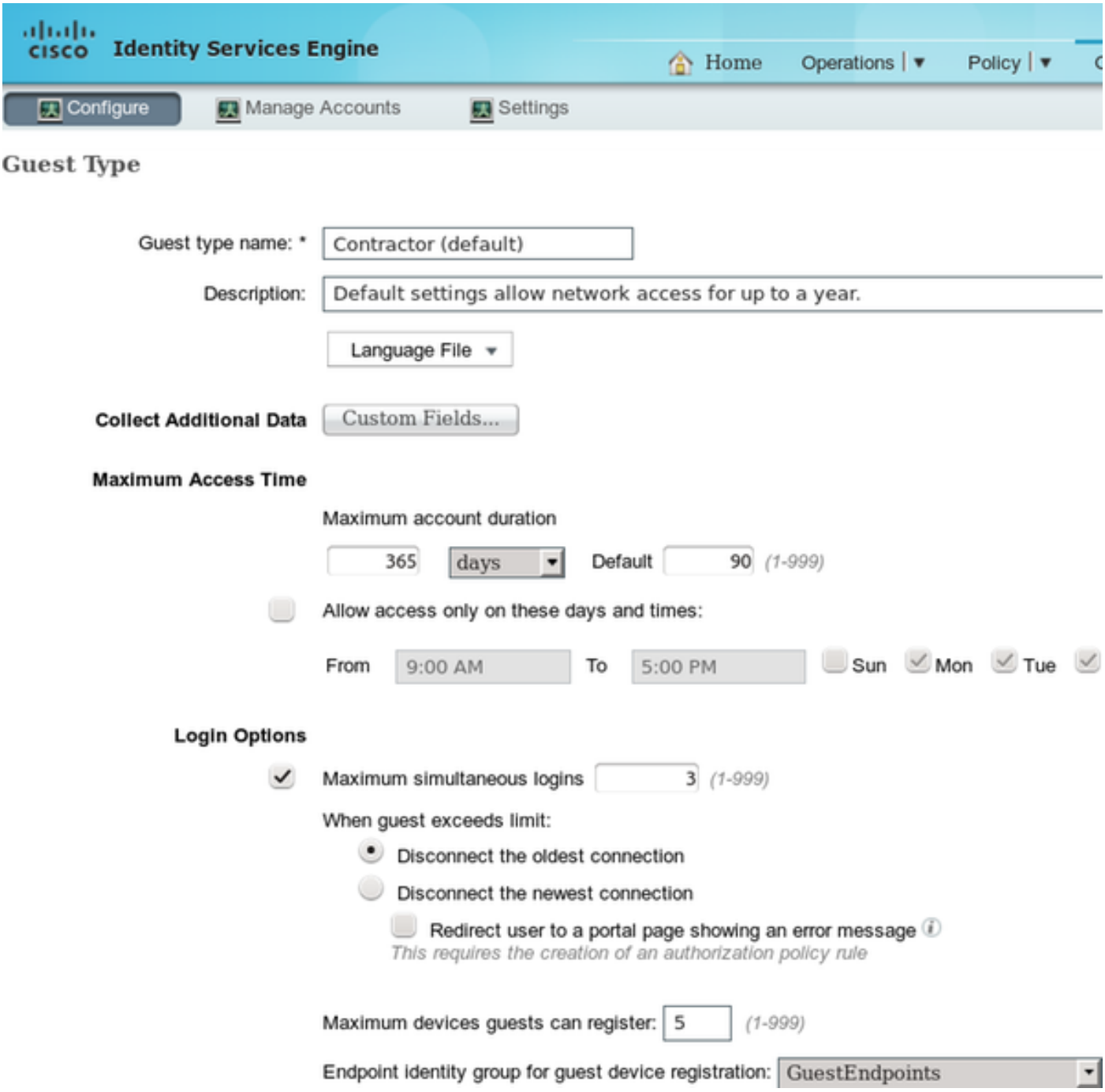
在啟用了裝置註冊的訪客門戶上成功身份驗證後，對於ISE版本1.3及更高版本。



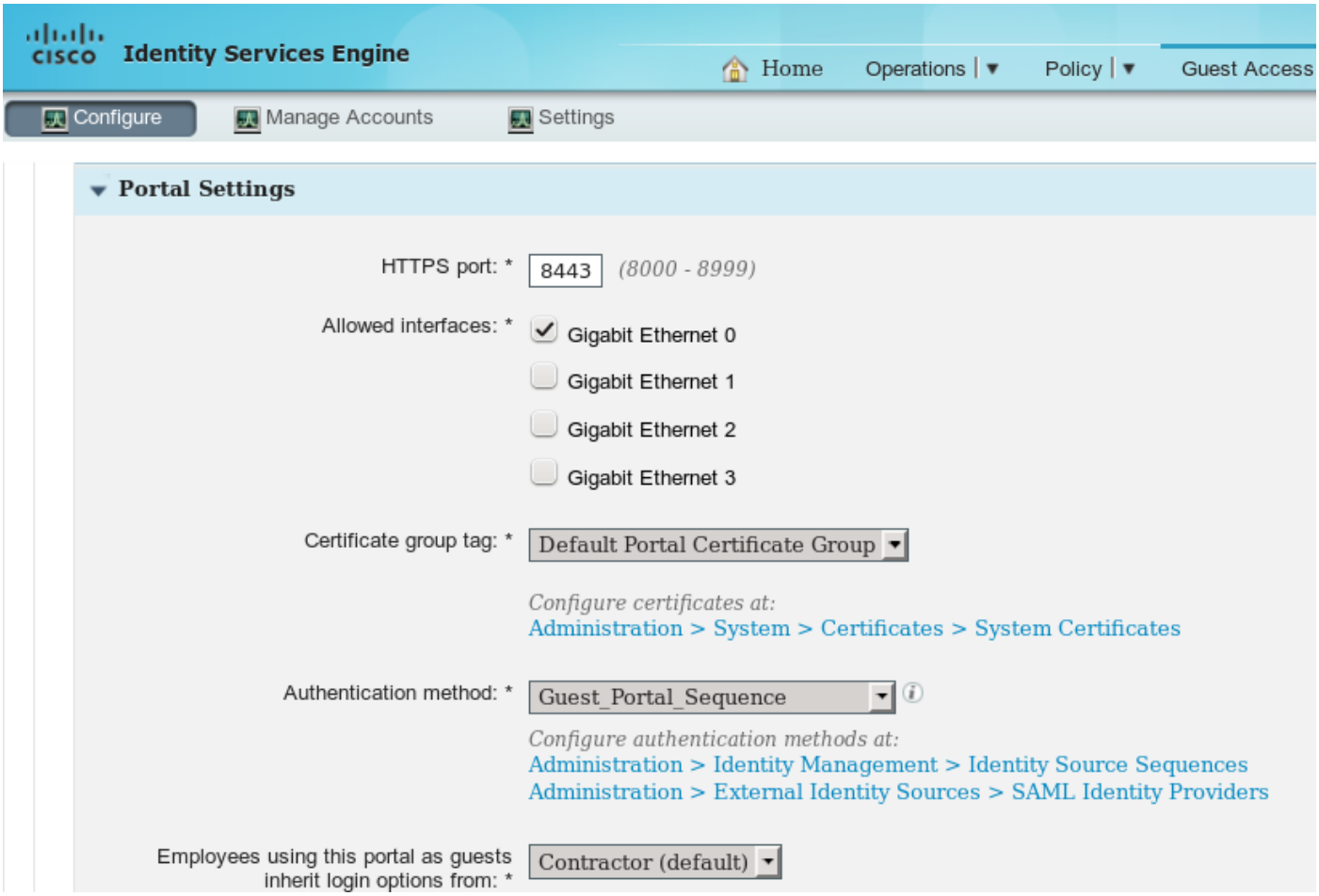
終端裝置（mac地址）在特定終端組（本示例中為GuestEndpoints）中靜態註冊。



該組是從使用者的Guest Type派生的，如下圖所示。



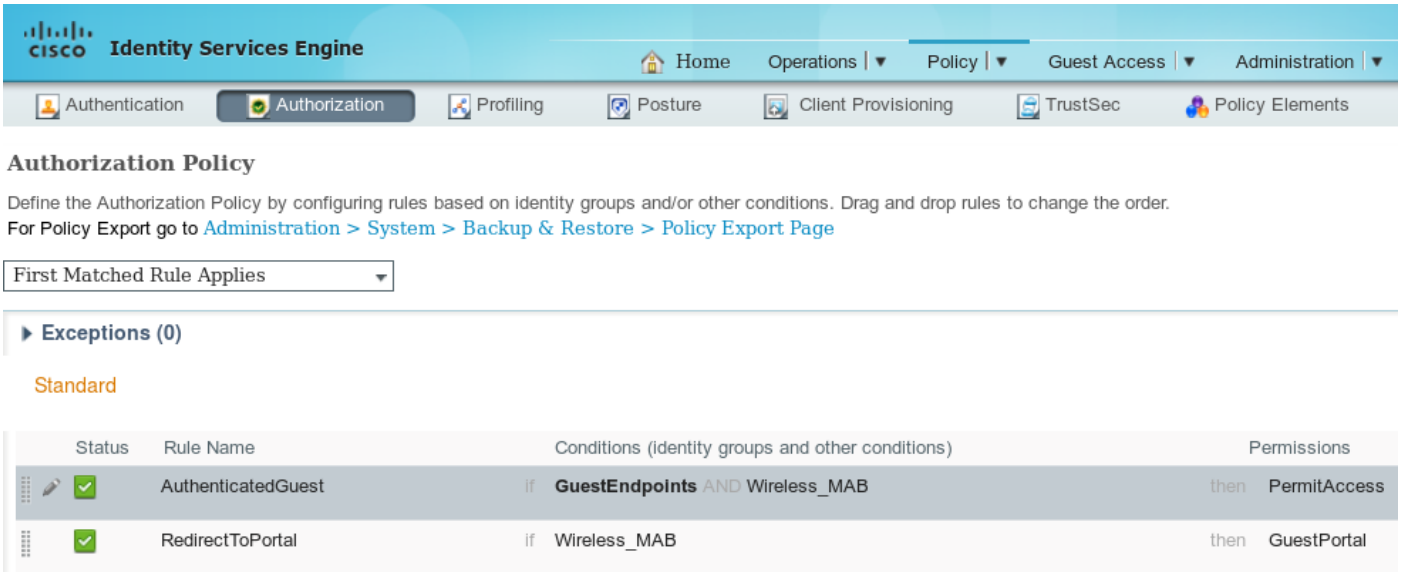
如果是企業使用者（身份儲存不是訪客），則該設定是從門戶設定派生的。



因此，與訪客關聯的MAC地址始終屬於該特定身份組。不能自動更改（例如Profiler服務）。

附註：若要應用Profiler結果，可使用EndPointPolicy授權條件。

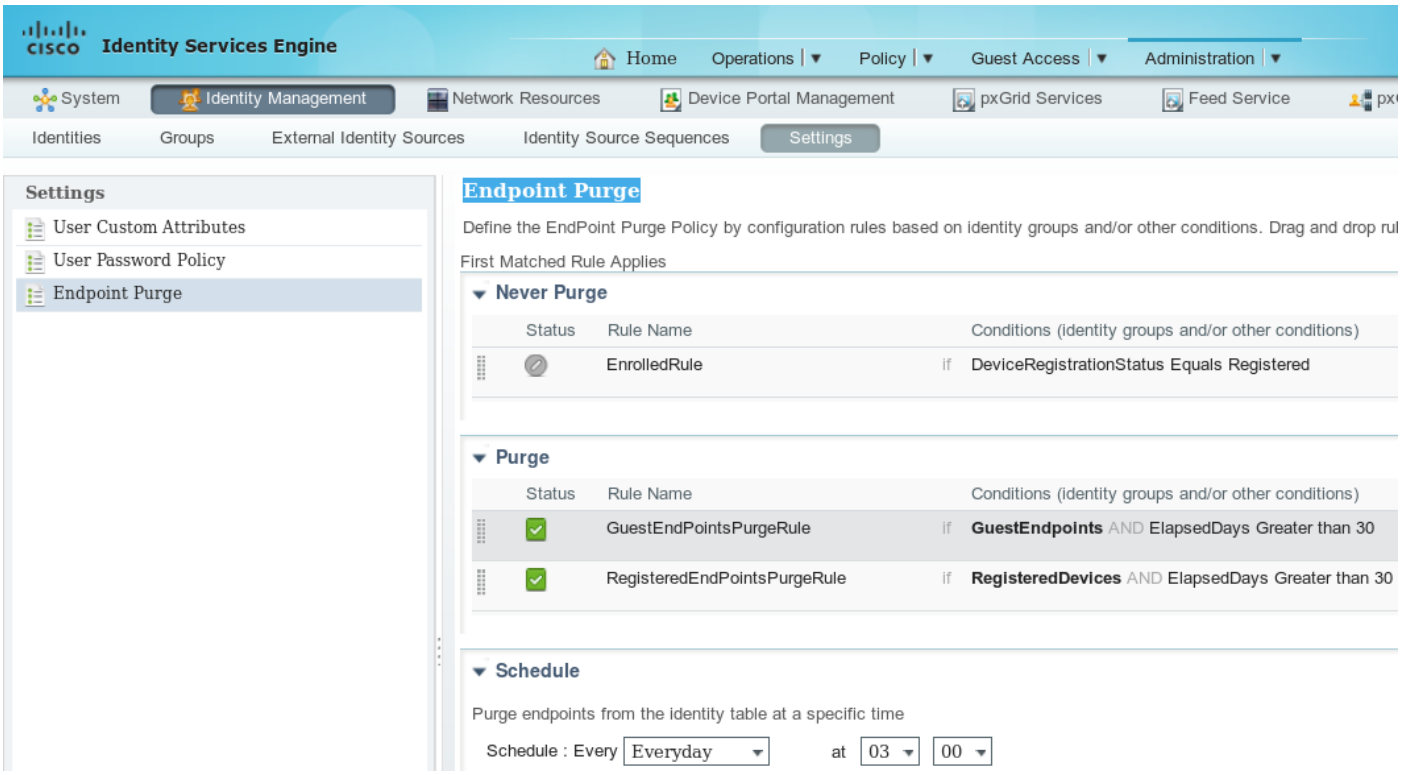
如果知道裝置始終屬於特定終端身份組，則可能基於該身份組構建授權規則，如下圖所示。



使用者未通過身份驗證後，授權將匹配通用規則RedirectToPortal。重定向到訪客門戶並進行身份驗證後，終端被置於特定終端身份組中。這是第一個更具體的情況。該端點的所有後續認證均滿足第一授權規則，並且向使用者提供完全的網路訪問，而無需在訪客門戶上重新進行認證。

訪客帳戶的終端清除

這種情況可能會永遠持續下去。但在ISE 1.3中引入了清除端點功能。使用預設配置。



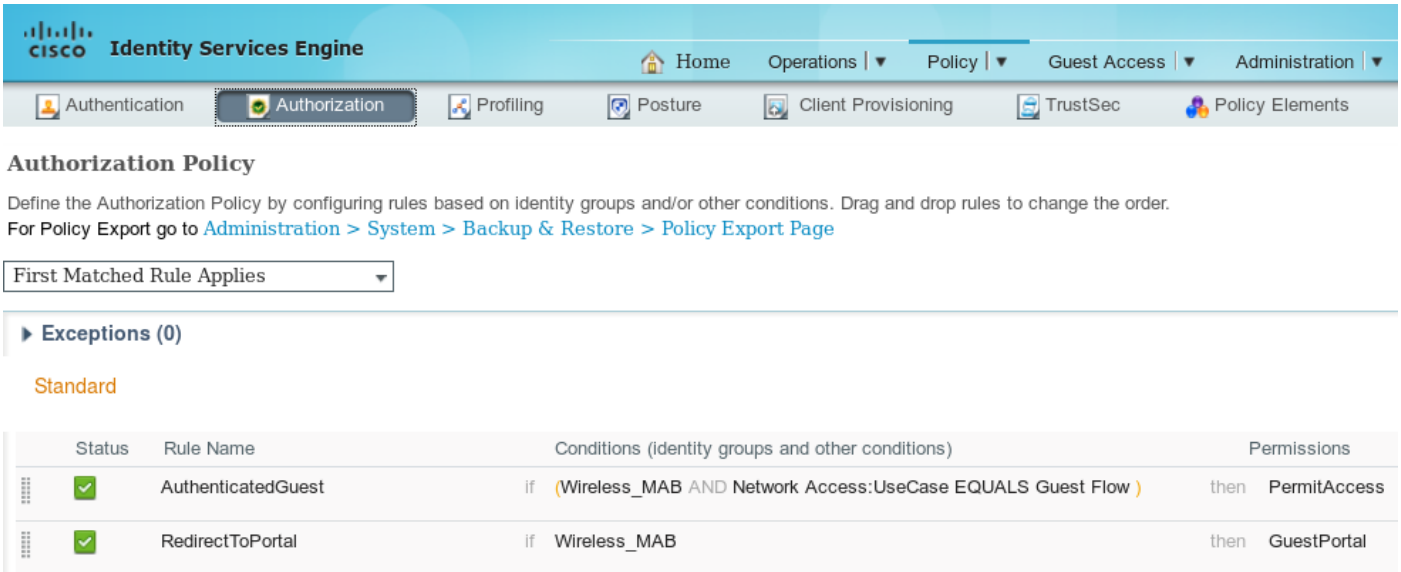
用於訪客身份驗證的所有終端將在30天後刪除（從終端建立）。 因此，通常在30天後，嘗試訪問網路的訪客使用者會命中RedirectToPortal授權規則，然後重定向以進行身份驗證。

附註：終端清除功能獨立於訪客帳戶清除策略和訪客帳戶過期。

附註：在ISE 1.2中，只有在達到內部探查器隊列限制時，才能自動刪除端點。然後刪除最近最少使用的終結點。

臨時訪問

訪客訪問的另一種方法是使用訪客流條件。



該條件檢查ISE上的活動會話及其屬性。如果該會話具有指示先前訪客使用者已成功通過身份驗證的屬性，則匹配條件。ISE收到來自網路接入裝置(NAD)的Radius記帳停止消息後，會話被終止並隨後刪除。在此階段，不再滿足Network Access:UseCase = Guest Flow的條件。結果，該端點的所有後續驗證都命中通用規則重定向到訪客驗證。

> **附註**：使用者通過HotSpot門戶進行身份驗證時不支援訪客流。對於這些情況，UseCase屬性設定為Host Lookup而不是Guest Flow。

WLC結束通話行為

客戶端與無線網路斷開連線後（例如，在Windows中使用disconnect按鈕），它會傳送取消身份驗證幀。但是，WLC會省略這一點，可以使用「debug client xxxx」確認這一點 — WLC在客戶端從WLAN斷開連線時不會顯示調試。因此，在Windows客戶端上：

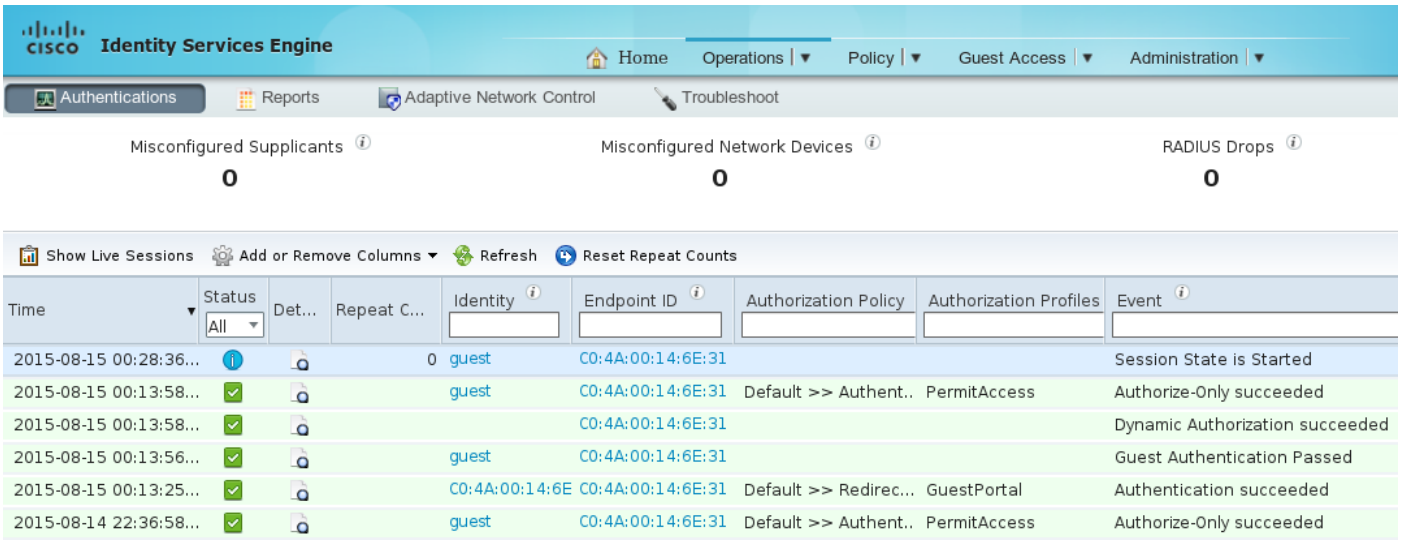
- ip address is removed from the interface
- 介面處於狀態：媒體已斷開連線

但是在WLC上，狀態沒有變更（使用者端仍處於RUN狀態）。

這是WLC的規劃設計，在以下情況下會刪除會話：

- 使用者空閒超時命中數
- session-timeout hits
- 如果使用L2加密，則當組金鑰輪替間隔命中時
- 其他情況會導致AP/WLC關閉客戶端（例如AP無線電重置、有人關閉WLAN等）

使用此行為和使用者從WLAN會話斷開後的臨時訪問配置不會從ISE中刪除，因為WLC從未清除它（並且從未傳送Radius記帳停止）。 如果未刪除會話，ISE仍會記住舊會話，並且滿足訪客流條件。斷開連線並重新連線後，使用者無需重新驗證即可獲得完整的網路訪問許可權。



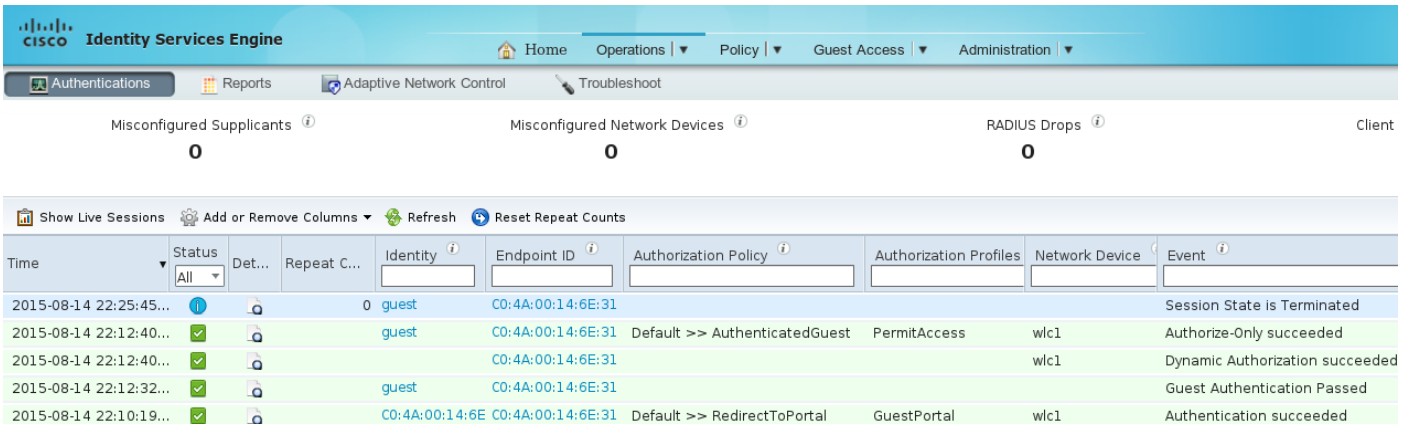
但是，如果使用者在斷開連線後連線到不同的WLAN，則WLC會決定清除舊作業階段。傳送Radius記賬停止，ISE刪除會話。如果使用者端嘗試連線到原始WLAN Guest Flow條件未獲滿足，系統會將使用者重新導向以進行驗證。

> **附註**：配置有管理幀保護(MFP)的WLC接受來自CCXv5 MFP客戶端的加密解除身份驗證幀。

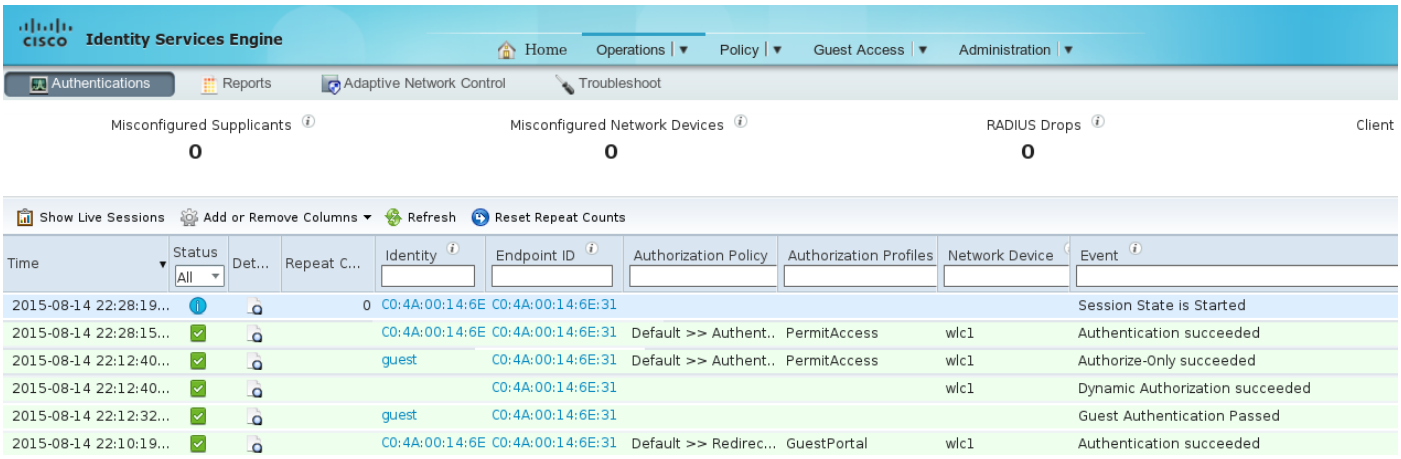
驗證

永久訪問

重定向到訪客門戶並成功進行身份驗證後，ISE傳送授權更改(CoA)以觸發重新身份驗證。因此，正在構建新的MAC身份驗證繞行(MAB)會話。此時間終結點屬於GuestEndpoints身份組並匹配提供完全訪問許可權的規則。

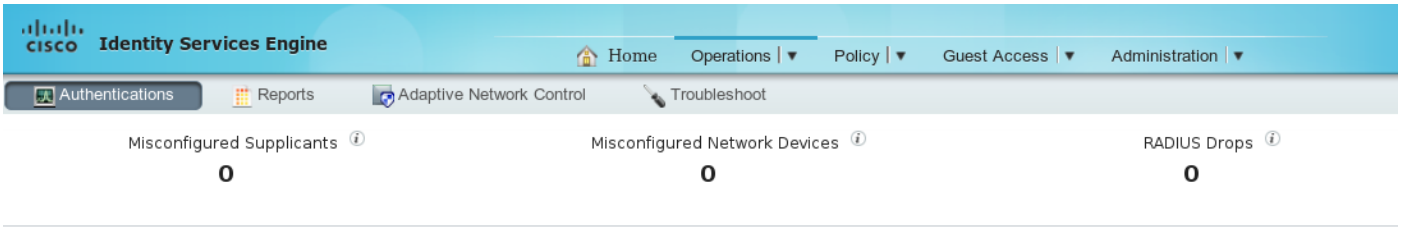


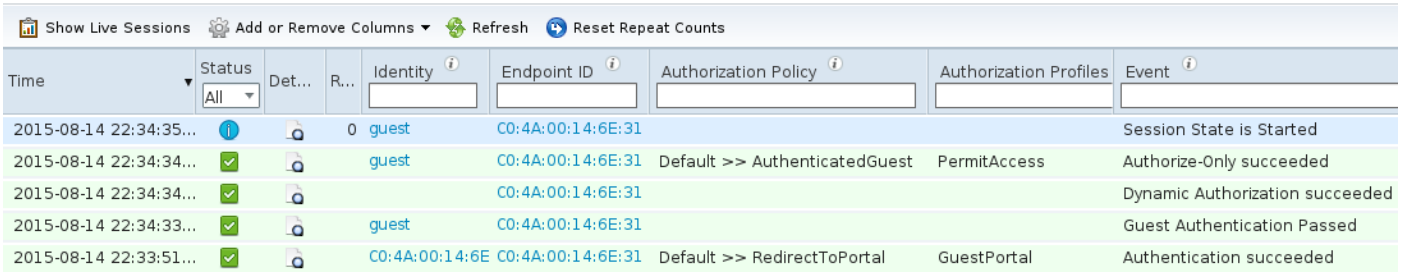
在此階段，無線使用者可以斷開連線，連線到不同的WLAN，然後重新連線。所有後續身份驗證都使用基於MAC地址的身份，但由於終端屬於特定身份組，而命中了第一個規則。提供完全網路訪問而無需來賓身份驗證。



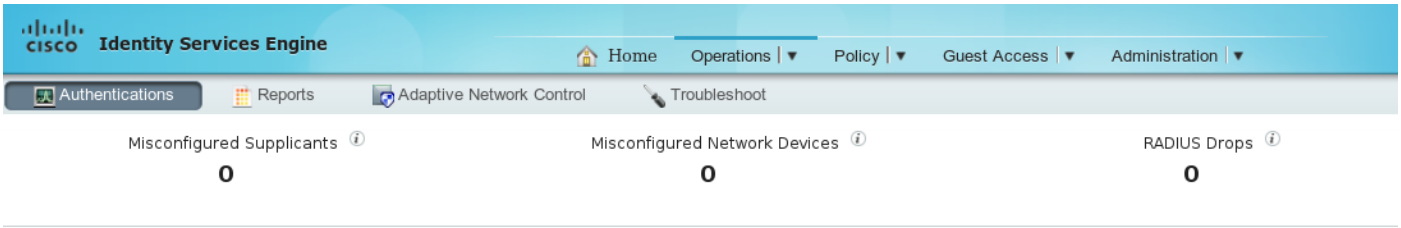
臨時訪問

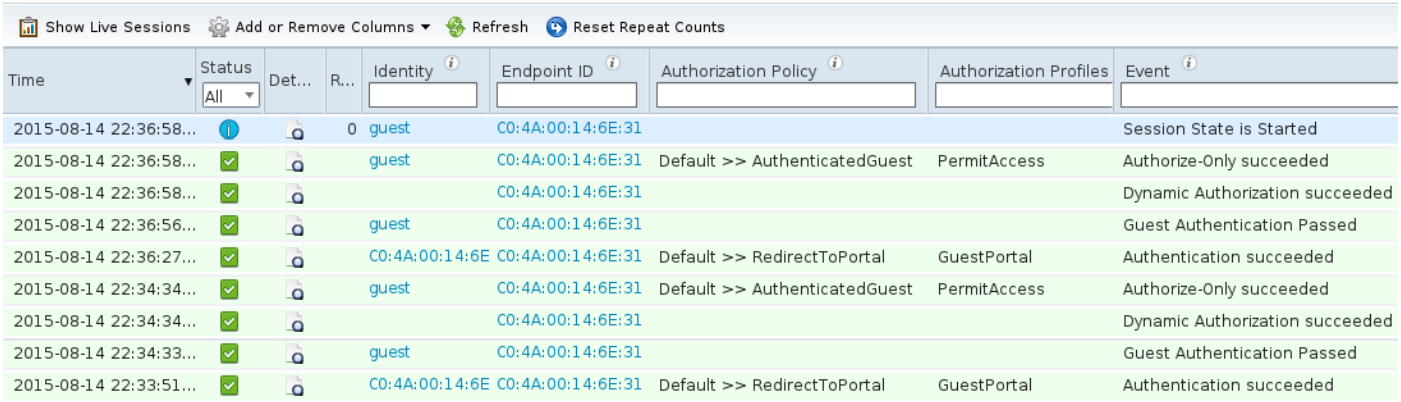
對於第二個方案（條件基於訪客流），開始處相同。



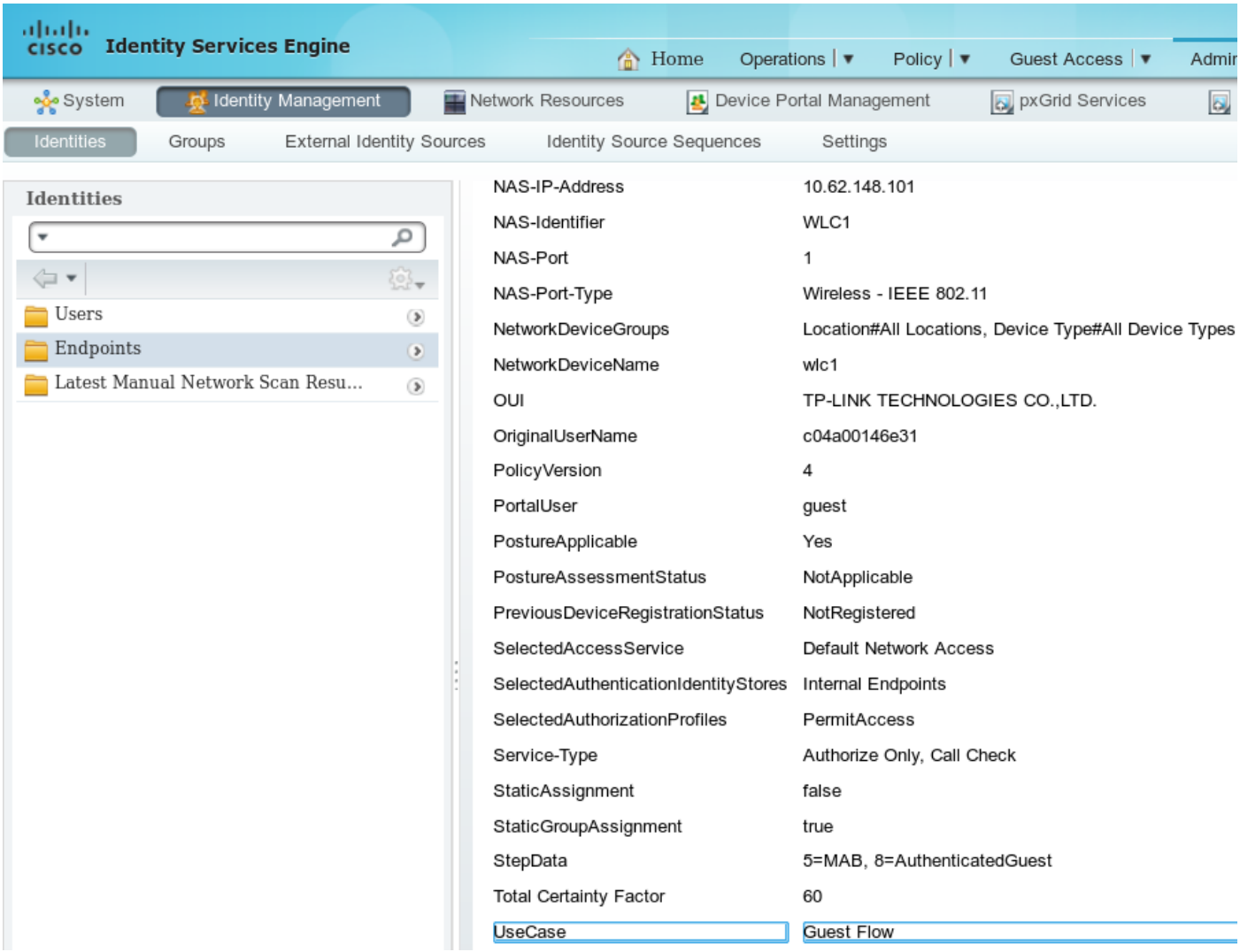


但在刪除所有後續身份驗證的會話後，訪客會點選通用規則，然後再次重定向以進行訪客身份驗證。





如果會話存在正確的屬性，則滿足訪客流條件。可以通過檢視端點屬性來驗證。指示成功的訪客身份驗證的結果。




```
PortalUser guest
StepData 5=MAB, 8=AuthenticatedGuest
UseCase Guest Flow
```

錯誤

CSCuu41157 ISE ENH CoA terminate send on guest account removal or expiry。

（在訪客帳戶刪除或到期後終止訪客會話的增強請求）

參考資料

- 思科ISE 1.3管理員指南
- 思科ISE 1.4管理員指南
- ISE版本1.3熱點配置示例
- ISE版本1.3自註冊訪客門戶配置示例
- WLC 和 ISE 的中央 Web 驗證的組態範例
- 使用ISE的WLC上使用FlexConnect AP進行中央Web身份驗證的配置示例
- 技術支援與文件 - Cisco Systems