ISE版本1.3自註冊訪客門戶配置示例

目錄

簡介

思科身份服務引擎(ISE)版本1.3具有稱為自註冊訪客門戶的新型訪客門戶，允許訪客使用者在獲得網路資源訪問許可權時自行註冊。此門戶允許您配置和自定義多個功能。本文說明如何設定和疑難排解此功能。

必要條件

需求

思科建議您瞭解ISE配置和以下主題的基本知識：

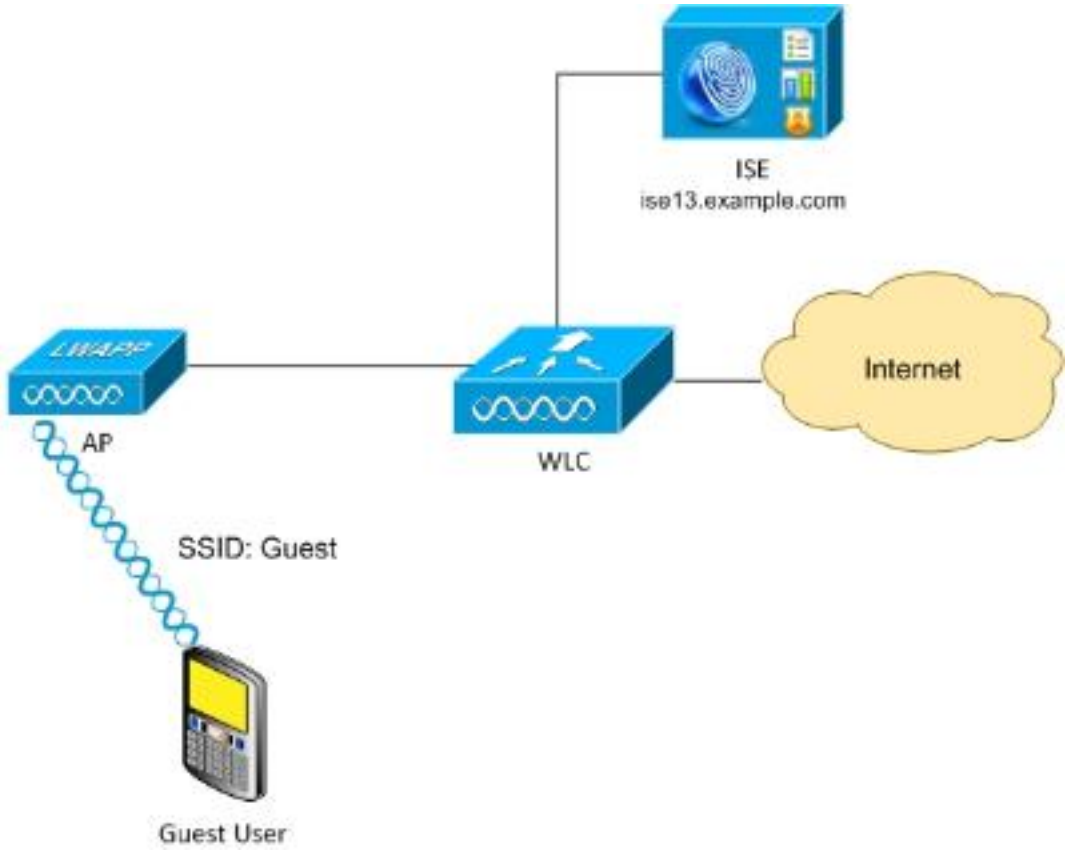
- ISE部署和訪客流量
- 無線區域網路控制器(WLC)的組態

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3.1版及更高版本

拓撲和流



此案例為訪客使用者執行自助註冊時提供了多個可用選項。

以下是一般流程：

步驟1.訪客使用者與服務組識別碼(SSID)建立關聯：訪客.這是一個開放式網路，使用ISE進行MAC過濾以進行身份驗證。此身份驗證匹配ISE上的第二個授權規則，並且授權配置檔案重定向到訪客自行註冊門戶。ISE返回包含兩個cisco-av-pair的RADIUS Access-Accept:

- url-redirect-acl(應重定向哪些流量，以及在WLC本機上定義的訪問控制清單(ACL)名稱)
- url-redirect（將流量重定向到ISE的位置）

步驟2.將訪客使用者重定向到ISE。使用者按一下「沒有帳戶」而不是提供憑證以便登入。 系統會將使用者重新導向至可建立該帳戶的頁面。可以啟用可選的秘密註冊代碼，以便將自行註冊許可權限製為知道該秘密值的人員。建立帳戶後，將為使用者提供憑證（使用者名稱和密碼）並使用這些憑證登入。

步驟3. ISE將RADIUS授權變更(CoA)重新驗證傳送到WLC。當使用者傳送具有Authorize-Only屬性的RADIUS存取要求時，WLC會重新驗證使用者。ISE通過WLC本地定義的Access-Accept和Airespace ACL進行響應，僅提供對Internet的訪問（訪客使用者的最終訪問取決於授權策略）。

請注意，對於可擴展身份驗證協定(EAP)會話，ISE必須傳送CoA Terminate以觸發重新身份驗證，因為EAP會話位於請求方和ISE之間。但是對於MAB（MAC過濾），CoA Reauthenticate就足夠了；無需取消關聯/取消驗證無線客戶端。

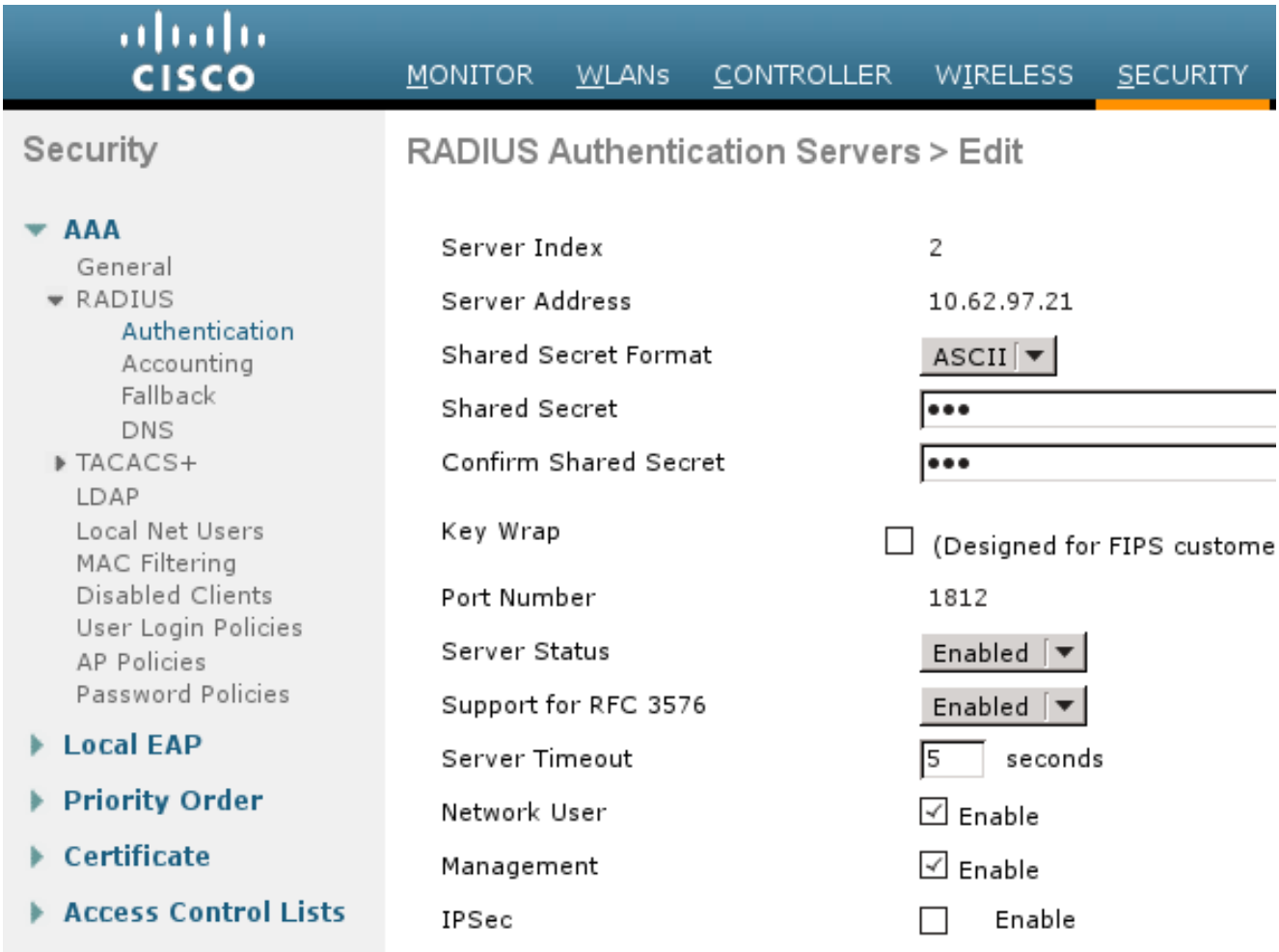
步驟4.訪客使用者具有所需的網路存取許可權。

可以啟用（稍後討論）多種其他功能，如狀態和自帶裝置(BYOD)。

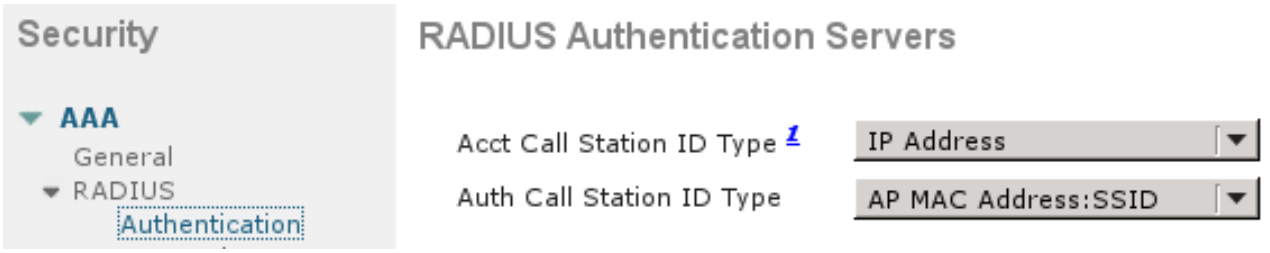
設定

WLC

1. 新增用於身份驗證和記帳的新RADIUS伺服器。導覽至**Security > AAA > Radius > Authentication**以啟用RADIUS CoA(RFC 3576)。



會計也有類似的配置。建議在Called Station ID屬性中配置WLC以傳送SSID，這允許ISE根據SSID配置靈活的規則：

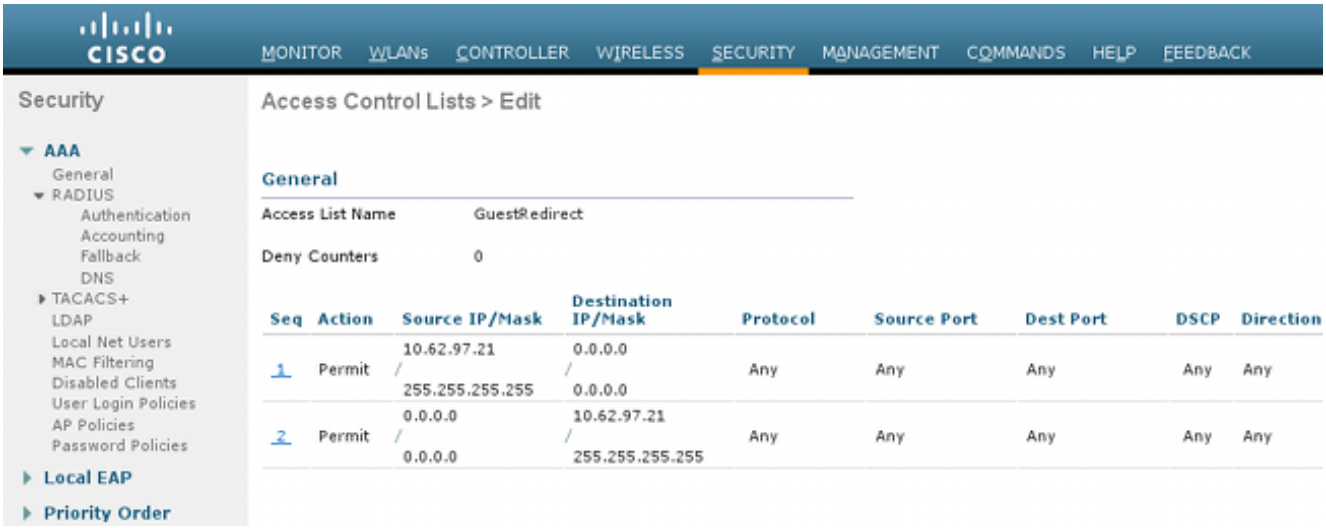


2. 在WLANs頁籤下，建立無線LAN(WLAN)訪客，並配置正確的介面。使用MAC過濾將Layer2 security設定為**None**。在安全/身份驗證、授權和記帳(AAA)伺服器中，選擇身份驗證和記帳的ISE IP地址。在Advanced索引標籤上，啟用**AAA Override**，並將網路認可控制(NAC)狀態設定為RADIUS NAC（CoA支援）。

3. 導覽至**Security > Access Control Lists > Access Control Lists**，然後建立兩個存取清單：

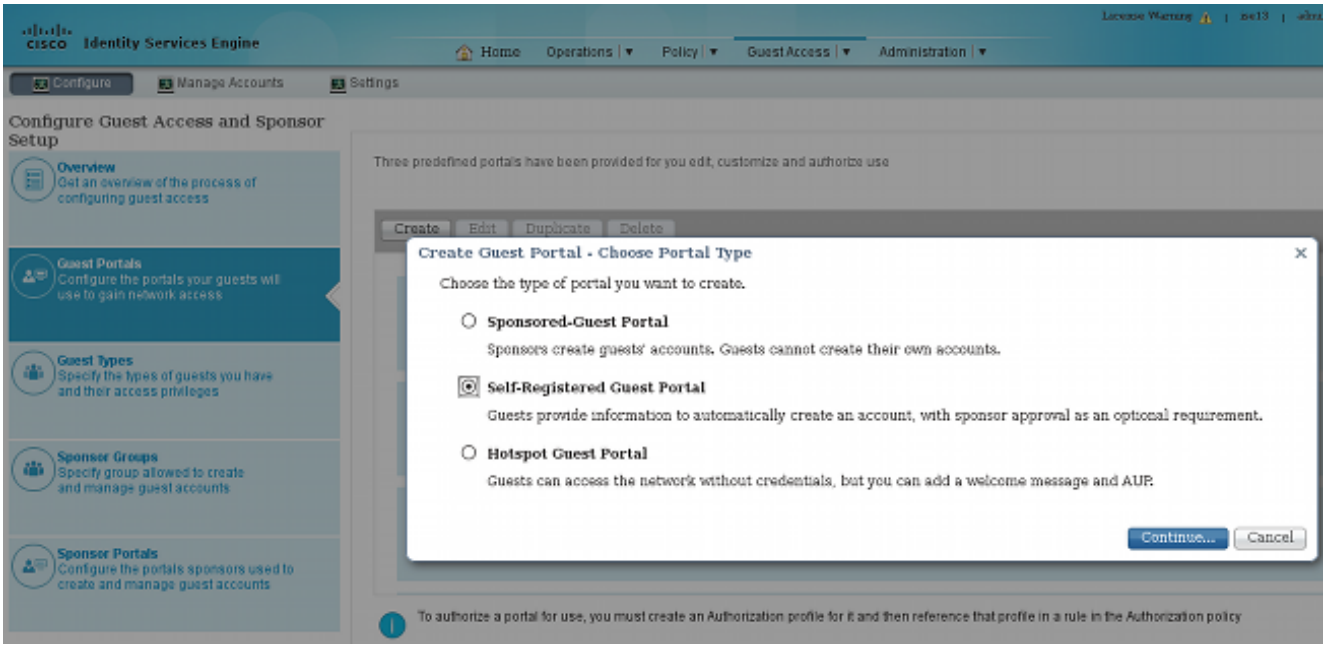
   GuestRedirect，允許不應重定向的流量並重定向所有其他流量Internet，公司網路被拒絕，所有其他網路都允許

   以下是GuestRedirect ACL的範例（需要從重新導向中排除ISE來往流量）：



ISE

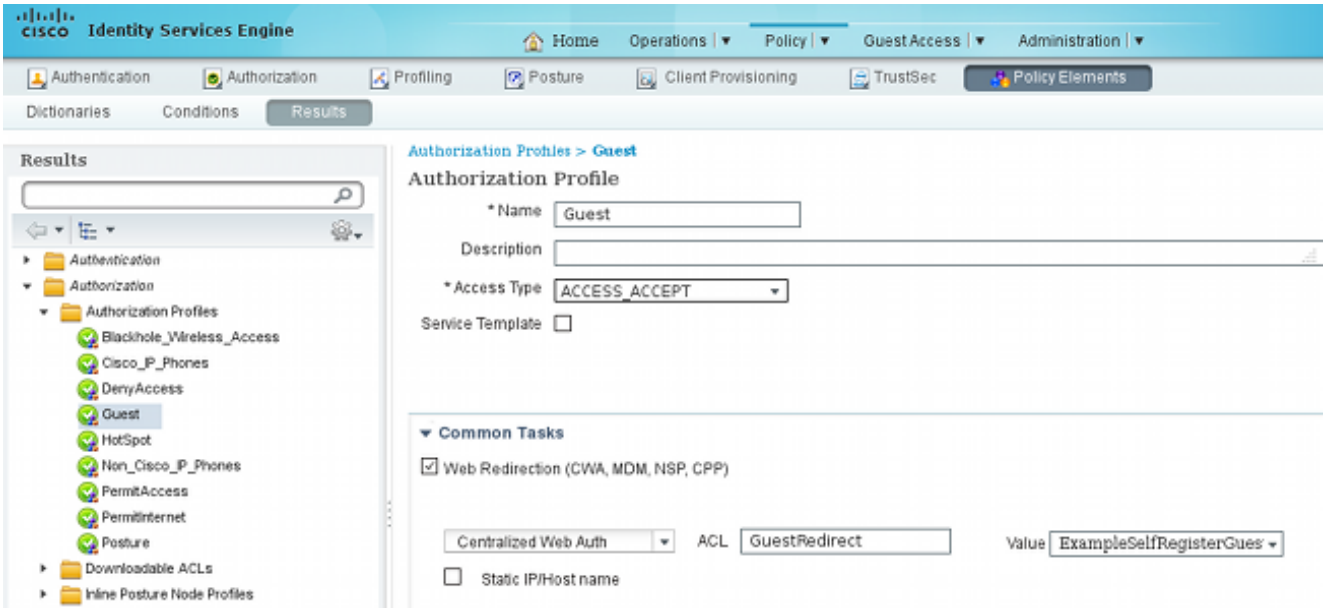
1. 導航到**Guest Access > Configure > Guest Portals**，然後建立新的門戶型別Self Registered Guest Portal:



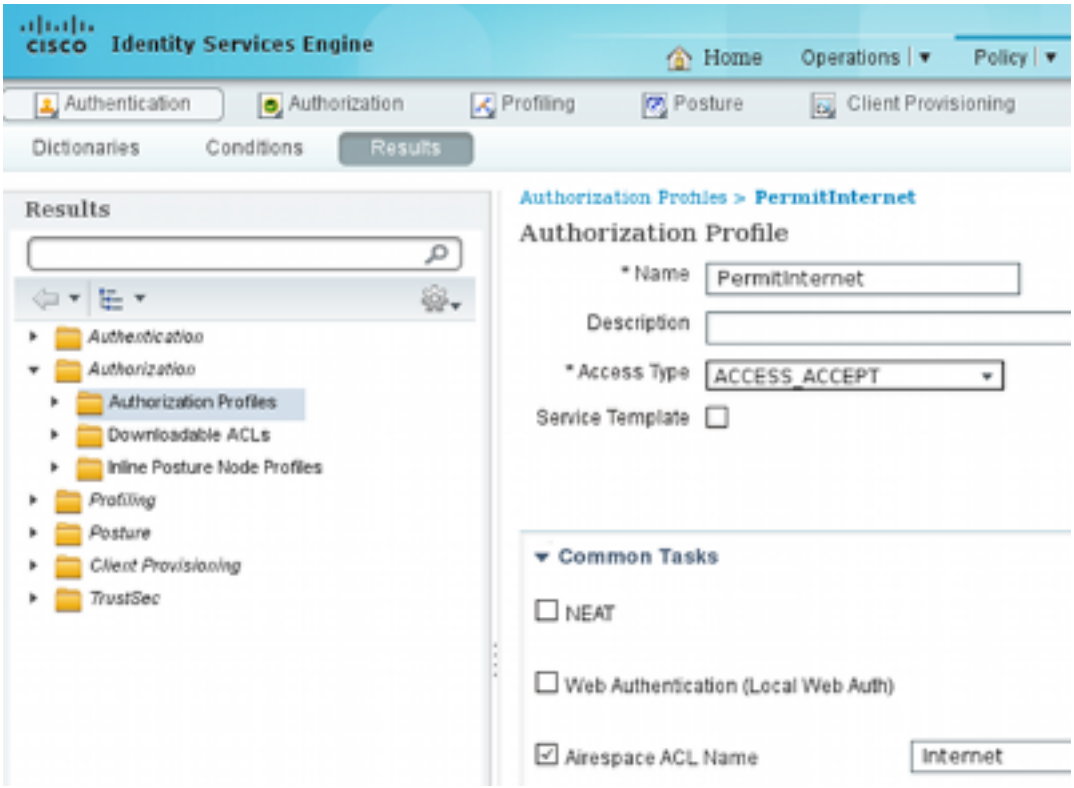
2. 選擇將在授權配置檔案中引用的門戶名稱。將所有其他設定設定為預設值。在Portal Page Customization下，可以自定義顯示的所有頁面。

3. 配置授權配置檔案：

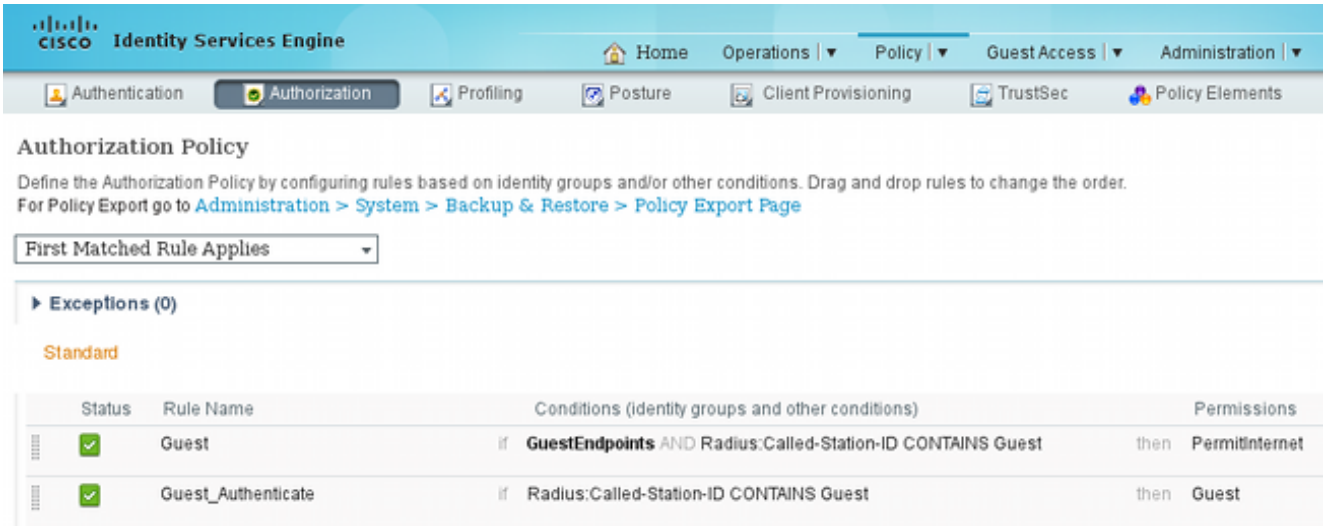
訪客（重新導向至訪客入口名稱和ACL GuestRedirect）



PermitInternet（Airespace ACL與Internet相同）



4. 若要驗證授權規則，請導航到**Policy > Authorization**。在ISE版本1.3中，預設情況下失敗的MAC身份驗證繞行(MAB)訪問（找不到MAC地址）身份驗證會繼續（未拒絕）。 這對於訪客門戶非常有用，因為不需要更改預設身份驗證規則中的任何內容。



與訪客SSID關聯的新使用者尚未屬於任何身份組。這就是它們與第二個規則匹配的原因，後者使用訪客授權配置檔案將它們重定向到正確的訪客門戶。

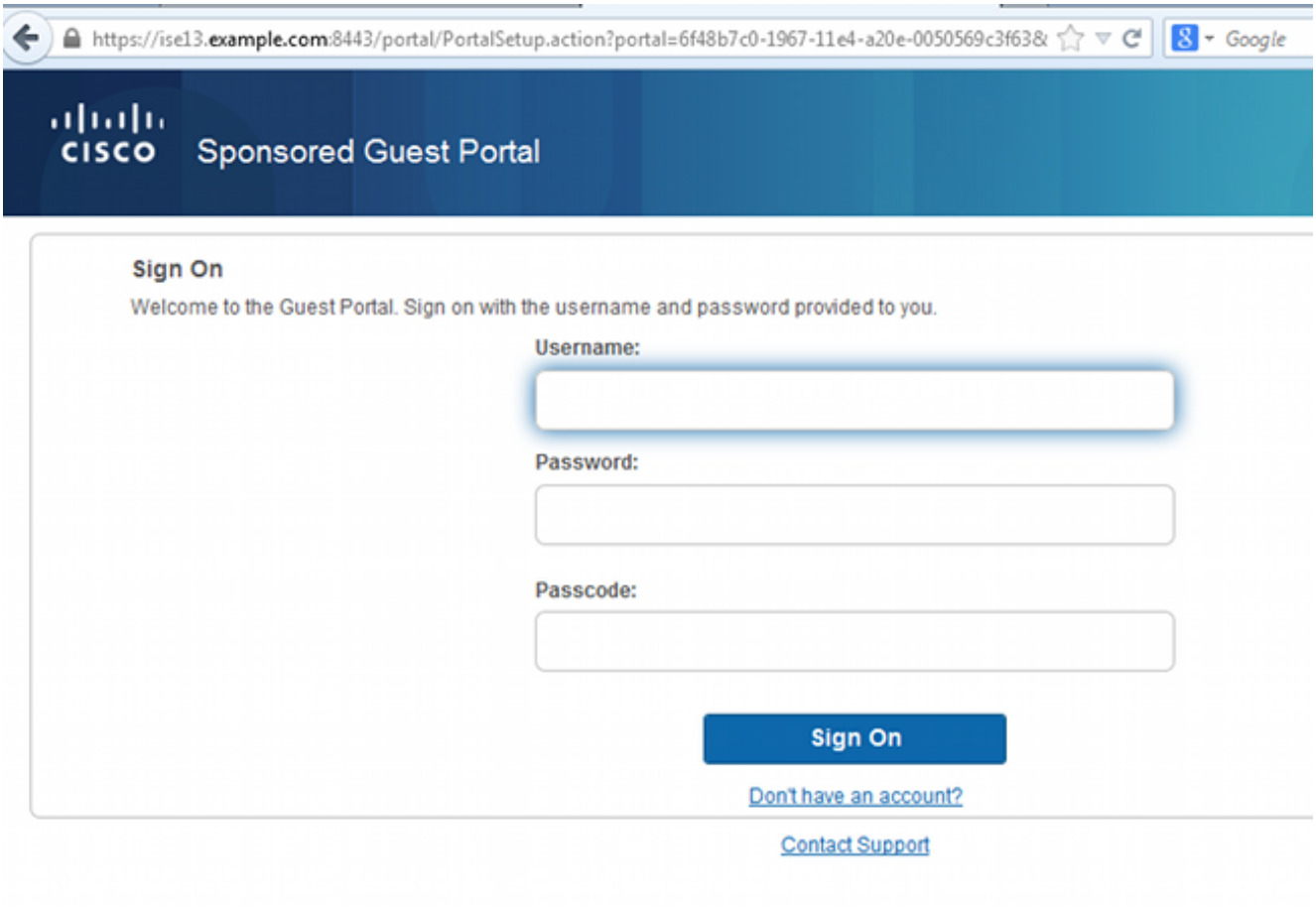
使用者建立帳戶並成功登入後，ISE會傳送RADIUS CoA，而WLC會執行重新驗證。這一次，第一個規則與授權配置檔案PermitInternet匹配，並返回應用於WLC的ACL名稱。

5. 從**管理>網路資源>網路裝置**新增WLC作為網路接入裝置。

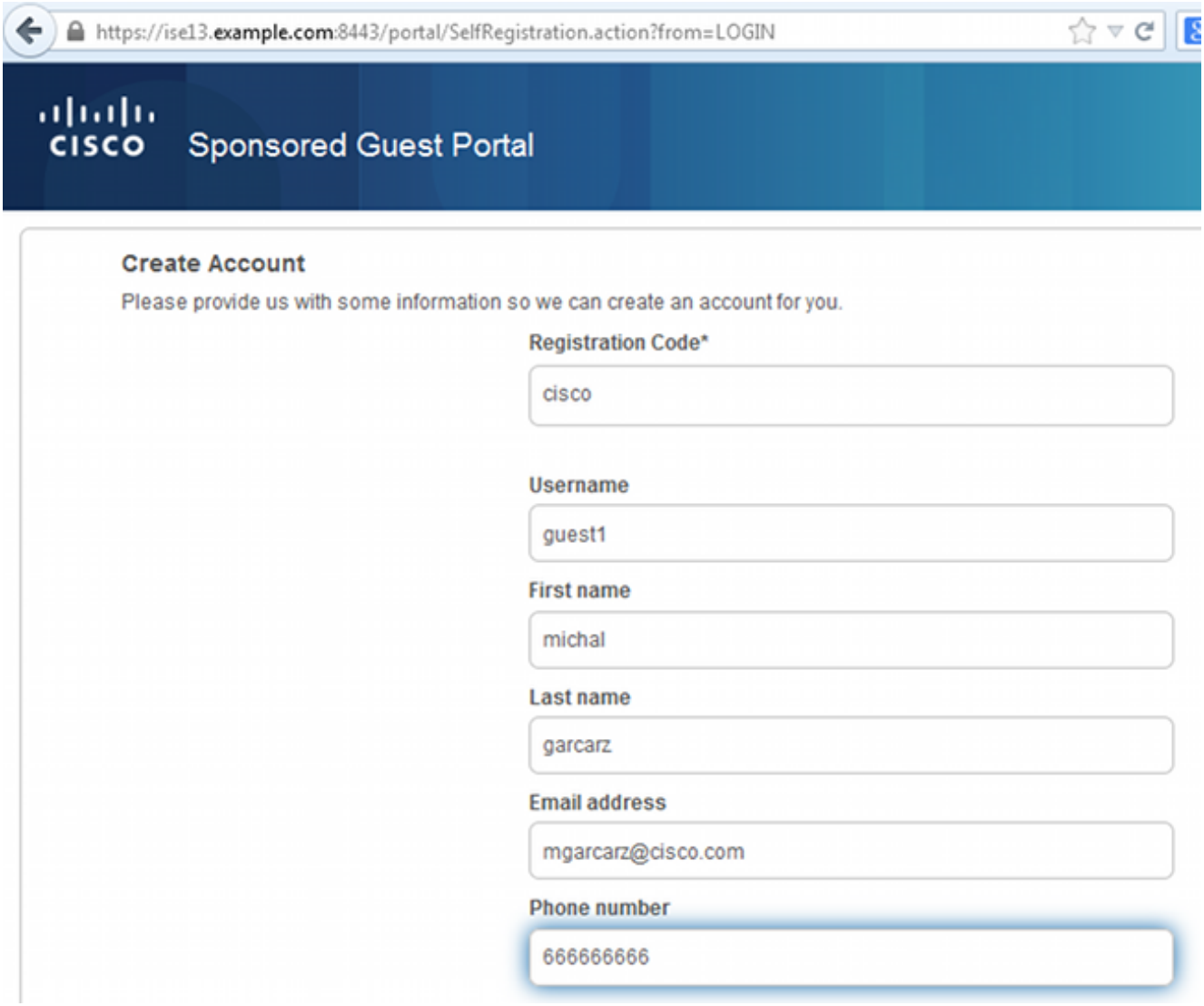
驗證

使用本節內容，確認您的組態是否正常運作。

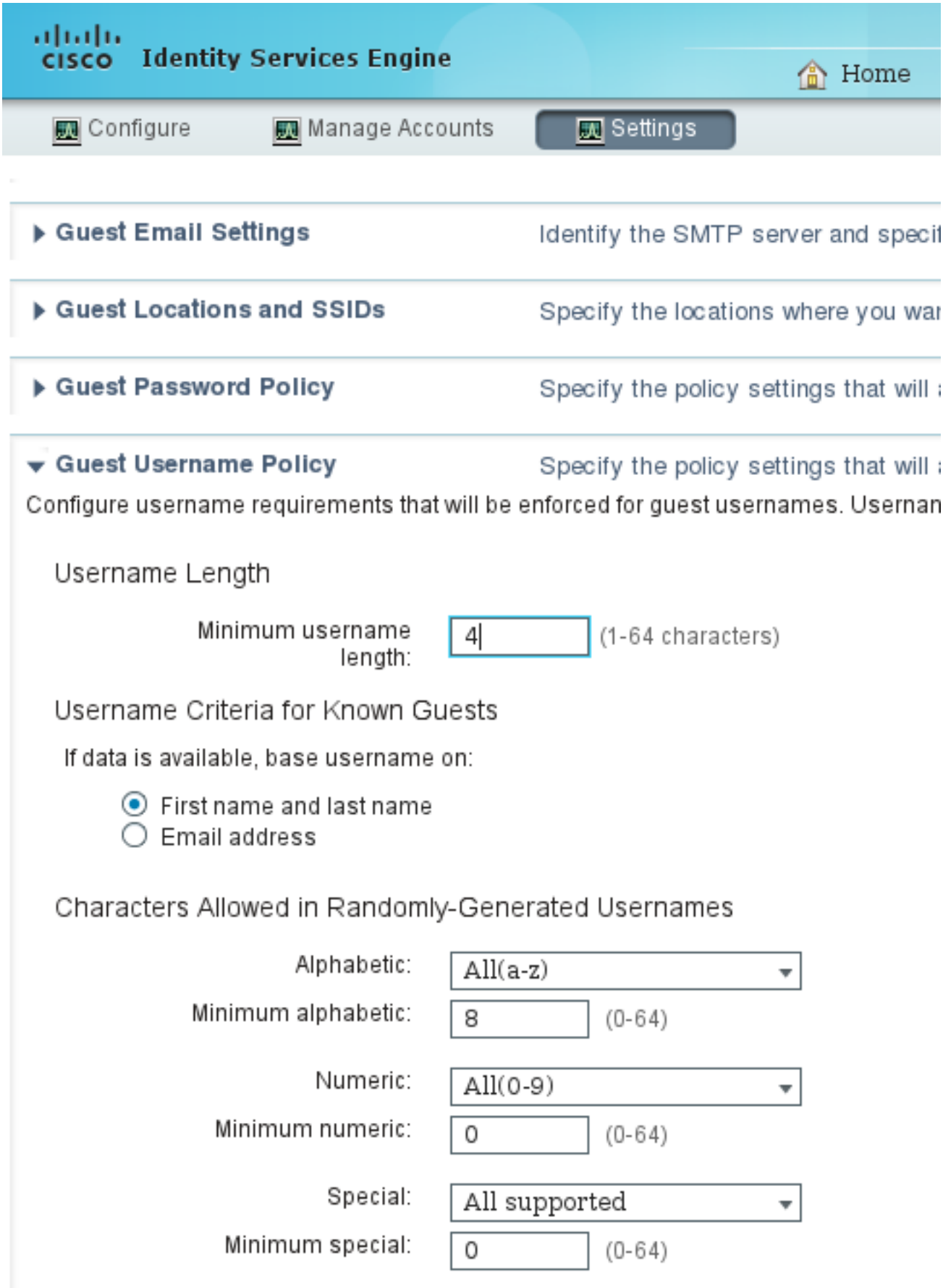
1. 與訪客SSID關聯並輸入URL後，系統會將您重新導向至登入頁面：



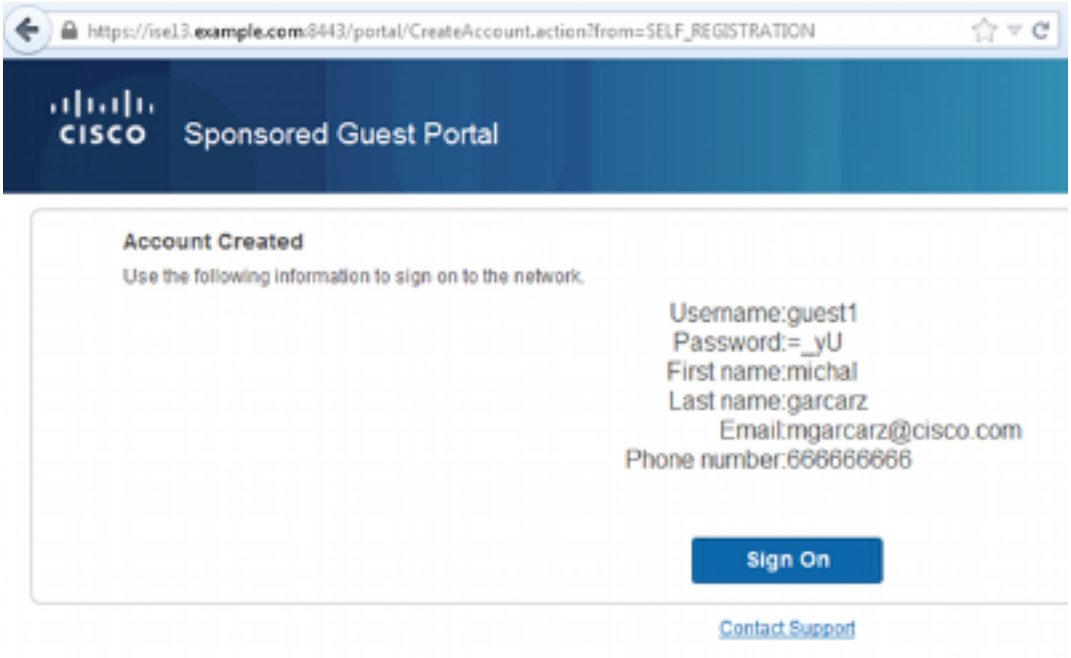
2. 由於您沒有任何憑據，您必須選擇**Don't have an account?**選項。將顯示允許建立帳戶的新頁面。如果在「訪客門戶」配置下啟用了「註冊代碼」選項，則需要該金鑰值（這可以確保僅允許具有正確許可權的人員自行註冊）。



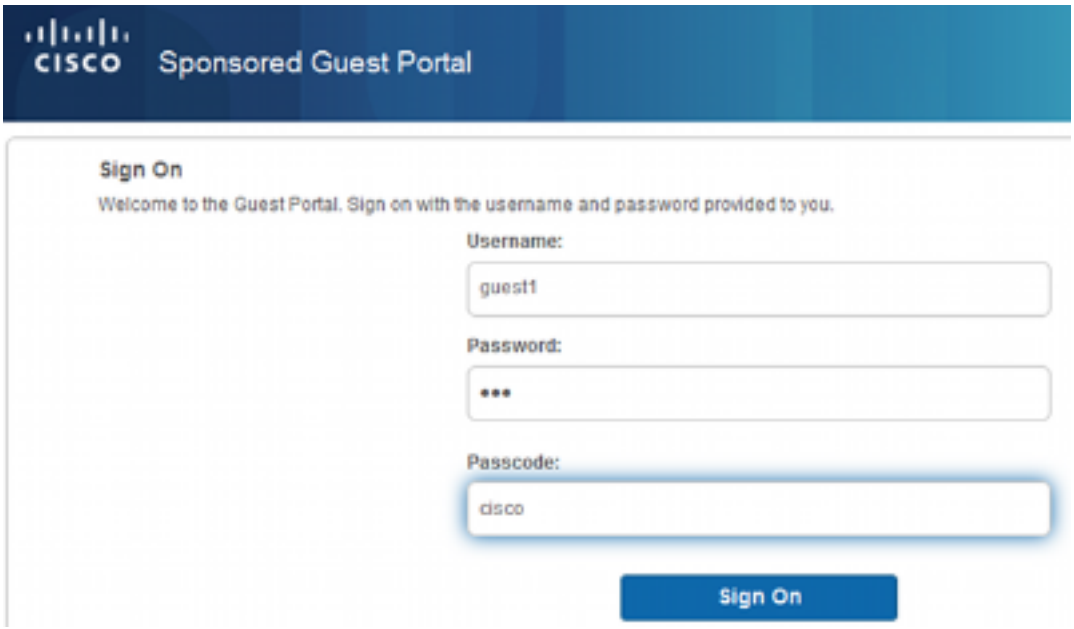
3. 如果密碼或使用者策略有任何問題，請導航到**Guest Access > Settings > Guest Password Policy**或**Guest Access > Settings > Guest Username Policy**以更改設定。以下是範例：



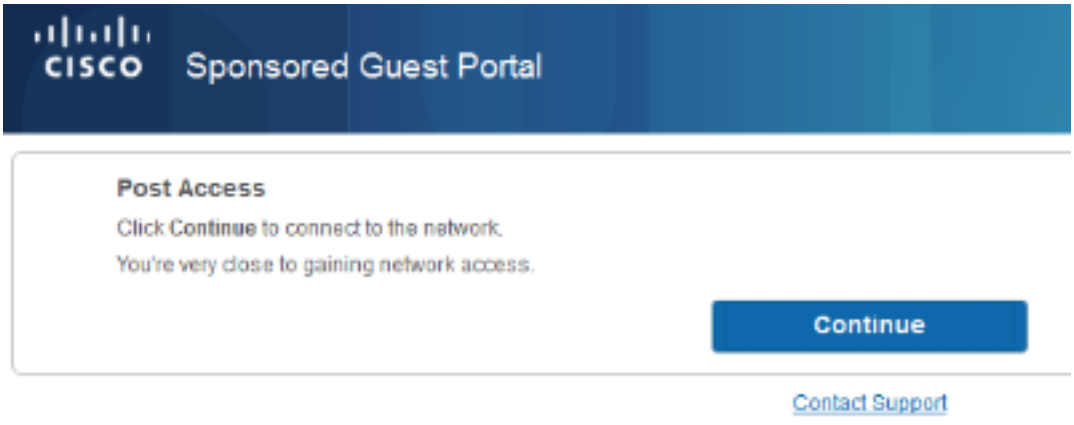
4. 成功建立帳戶後，系統將顯示憑證（根據訪客密碼策略生成的密碼）：



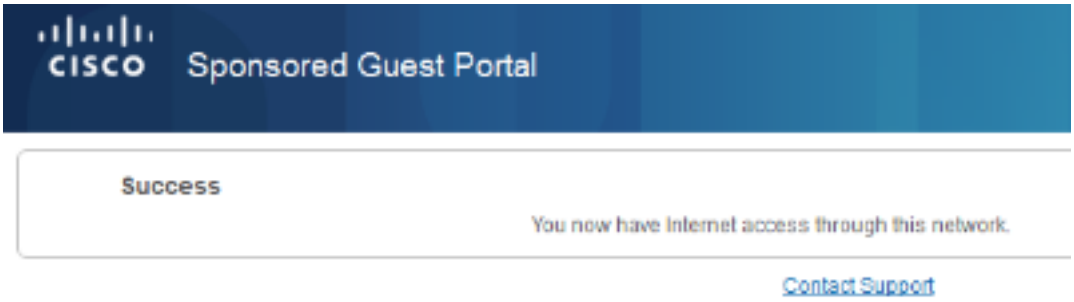
5. 按一下Sign On並提供憑證(如果在訪客輸入網站下設定，可能需要額外的存取密碼；這是另一種安全機制，僅允許知道密碼的人登入)。



6. 成功後，可能會顯示可選的使用策略(AUP)（如果在訪客門戶下配置）。 也可能顯示Post Access頁面（也可在Guest Portal下配置）。



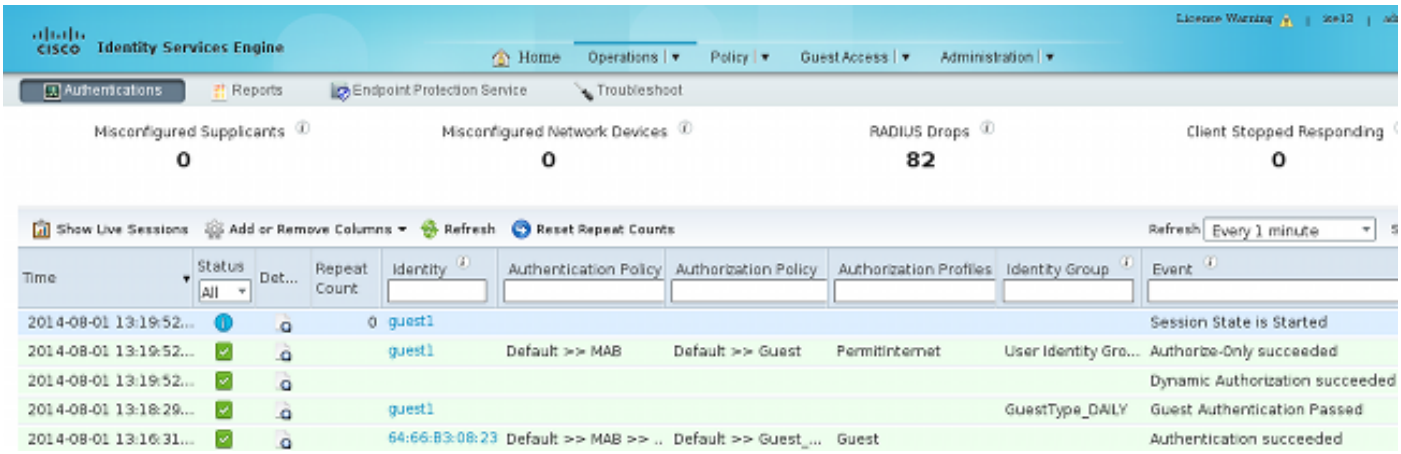
最後一頁確認已授予訪問許可權：



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

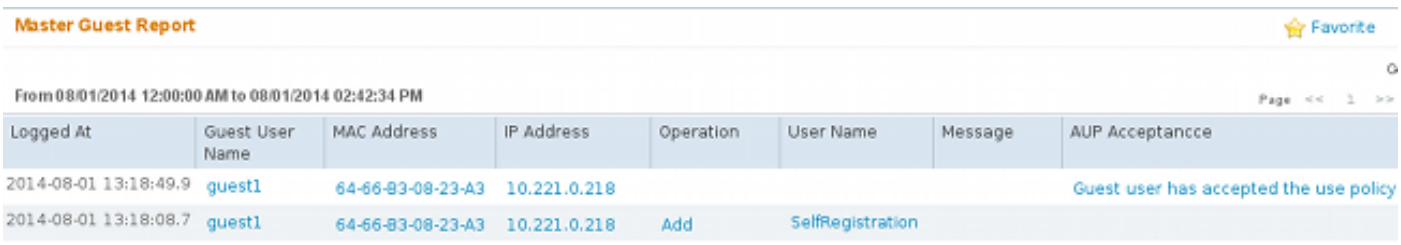
在此階段，ISE顯示以下日誌：



以下是流程：

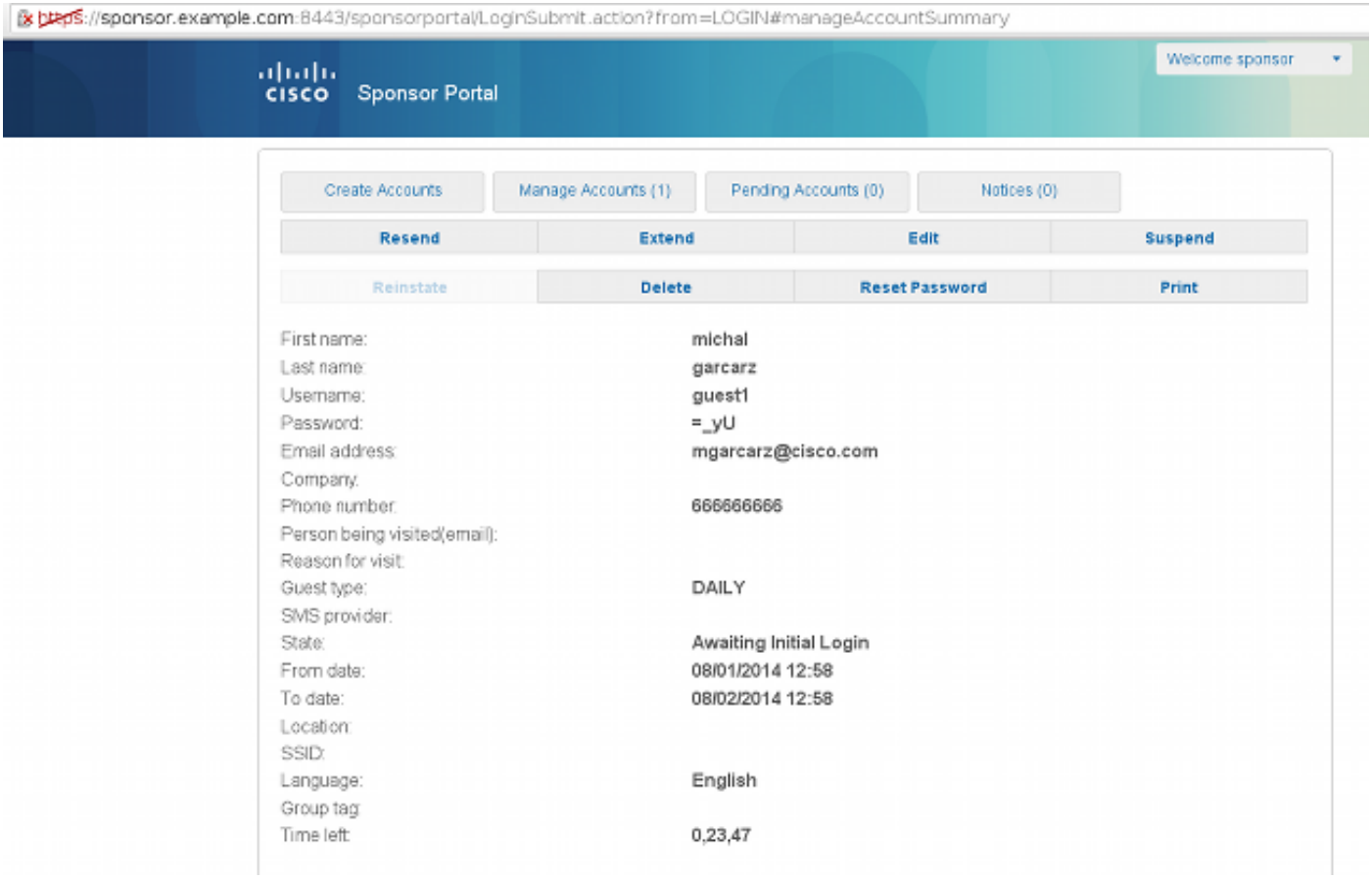
- 訪客使用者遇到第二個授權規則(Guest_Authenticate)，並被重定向到訪客（「驗證成功」）。
- 訪客被重新導向以進行自我註冊。成功登入（使用新建立的帳戶）後，ISE會傳送CoA重新驗證，並由WLC確認（「動態授權成功」）。
- WLC使用Authorize-Only屬性執行重新身份驗證，並返回ACL名稱(「Authorize-Only succeeded」)。 為訪客提供了正確的網路訪問。

報告(**Operations > Reports > ISE Reports > Guest Access Reports > Master Guest Report**)還確認：



保證人使用者（具有正確許可權）可以驗證訪客使用者的當前狀態。

此示例確認已建立帳戶，但使用者從未登入（「等待初始登入」）：



可選配置

對於此流程中的每個階段，可以配置不同的選項。所有這一切都是根據訪客門戶在**Guest Access > Configure > Guest Portals > PortalName > Edit > Portal Behavior and flow settings**下配置的。更重要的設定包括：

自助註冊設定

- 訪客型別 — 描述帳戶活動時間、密碼到期選項、登入時間和選項（這是ISE版本1.2的時間配置檔案和訪客角色的混合）
- 註冊碼 — 如果啟用，則僅允許知道密碼的使用者進行自我註冊（必須在建立帳戶時提供密碼）
- AUP — 在自行註冊期間接受使用策略
- 發起人批准/啟用訪客帳戶的要求

登入訪客設定

- 訪問代碼 — 如果啟用，則只允許知道密碼的訪客使用者登入
- AUP — 在自行註冊期間接受使用策略
- 密碼更改選項

裝置註冊設定

- 預設情況下，裝置會自動註冊

訪客裝置合規性設定

- 允許流量中的狀態

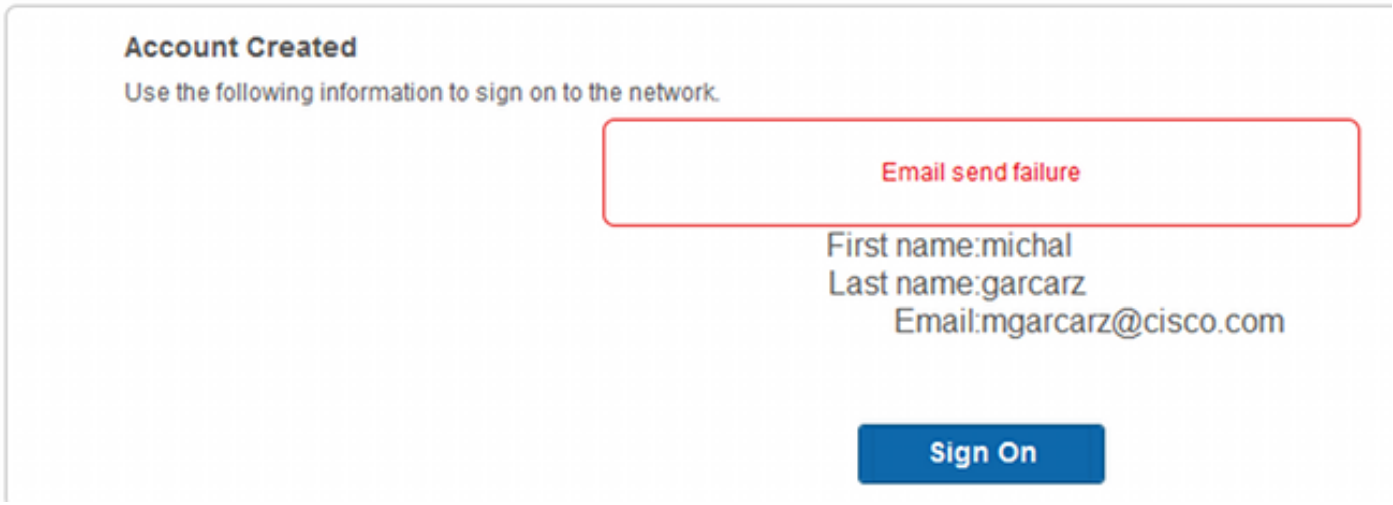
BYOD設定

- 允許將門戶用作訪客的企業使用者註冊其個人裝置

發起人批准的帳戶

如果選擇**Require self-registered guests to be approved**選項，則訪客建立的帳戶必須由發起人批准。此功能可能使用電子郵件將通知傳送給發起人（用於訪客帳戶批准）：

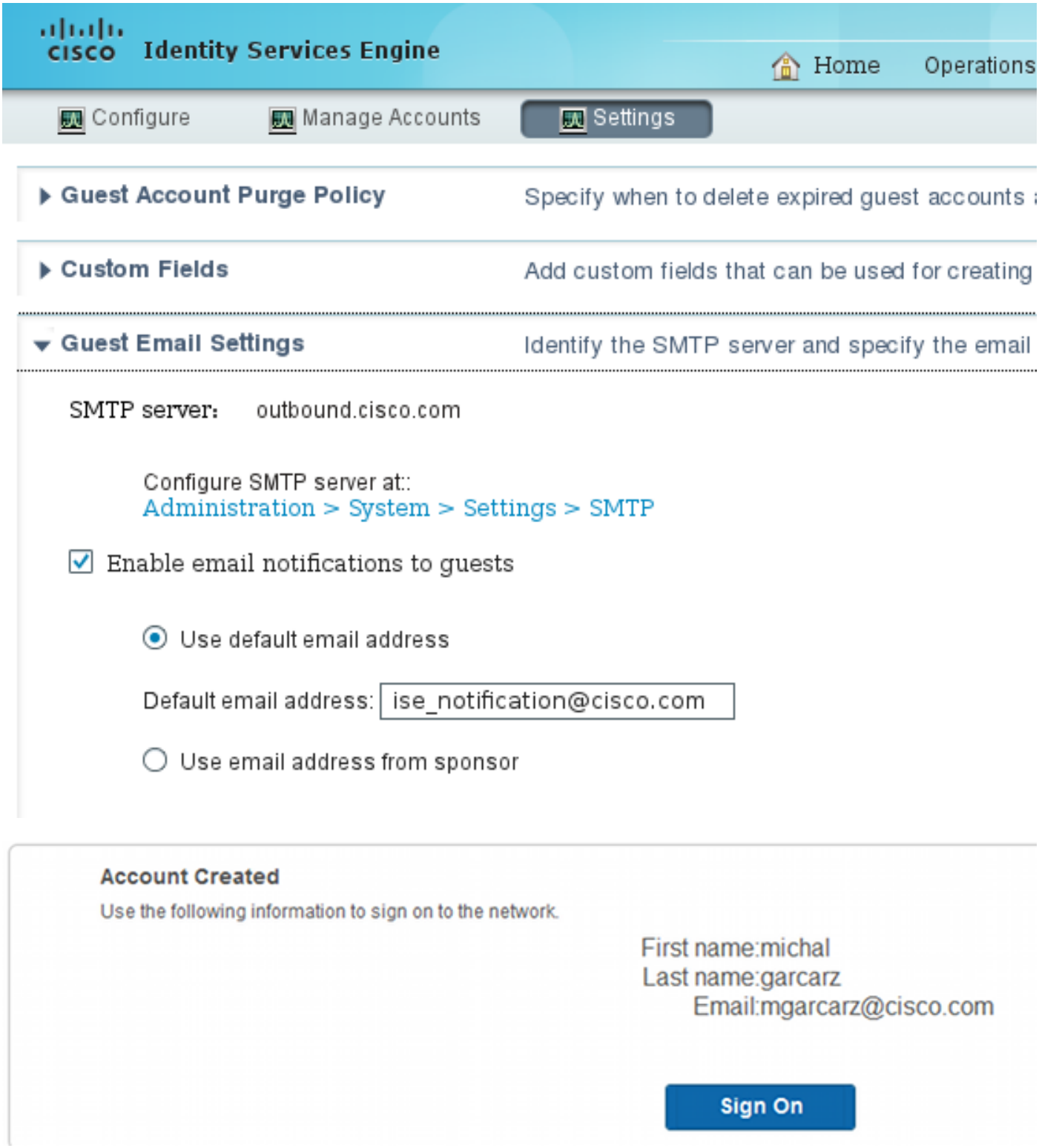
如果未配置簡單郵件傳輸協定(SMTP)伺服器或預設郵件通知，則不會建立帳戶：



來自guest.log的日誌確認用於通知的全域性發件人地址丟失：

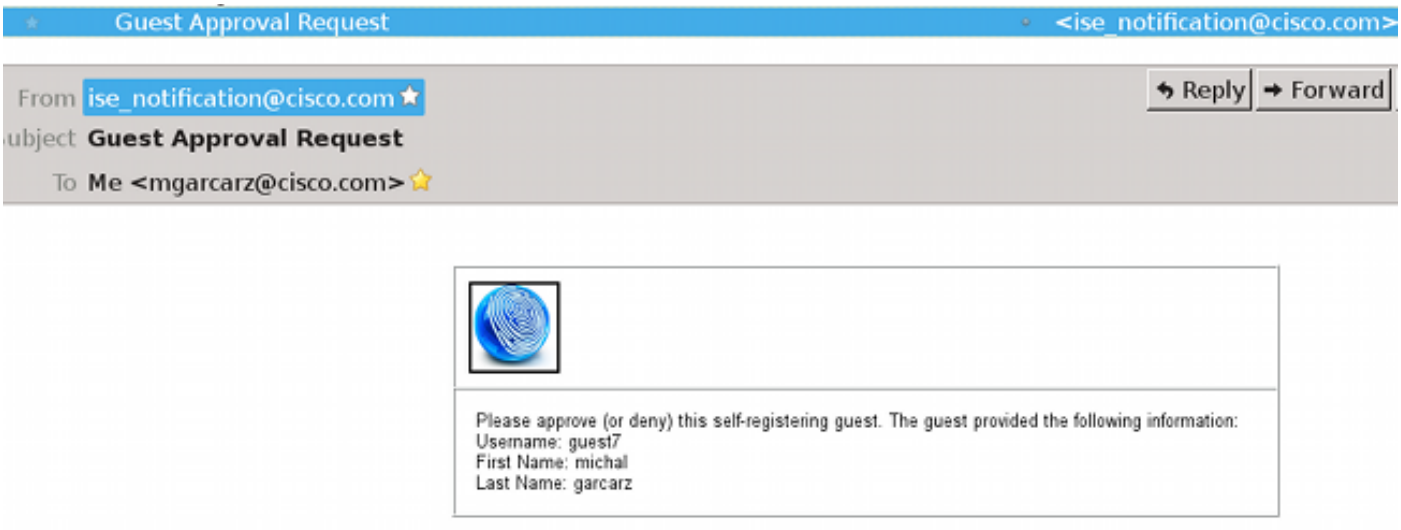
```
2014-08-01 22:35:24,271 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.SelfRegStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
Catch GuestAccessSystemException on sending email for approval: sendApproval
Notification: From address is null.  A global default From address can be
configured in global settings for SMTP server.
```

當您擁有正確的電子郵件配置時，帳戶將建立：

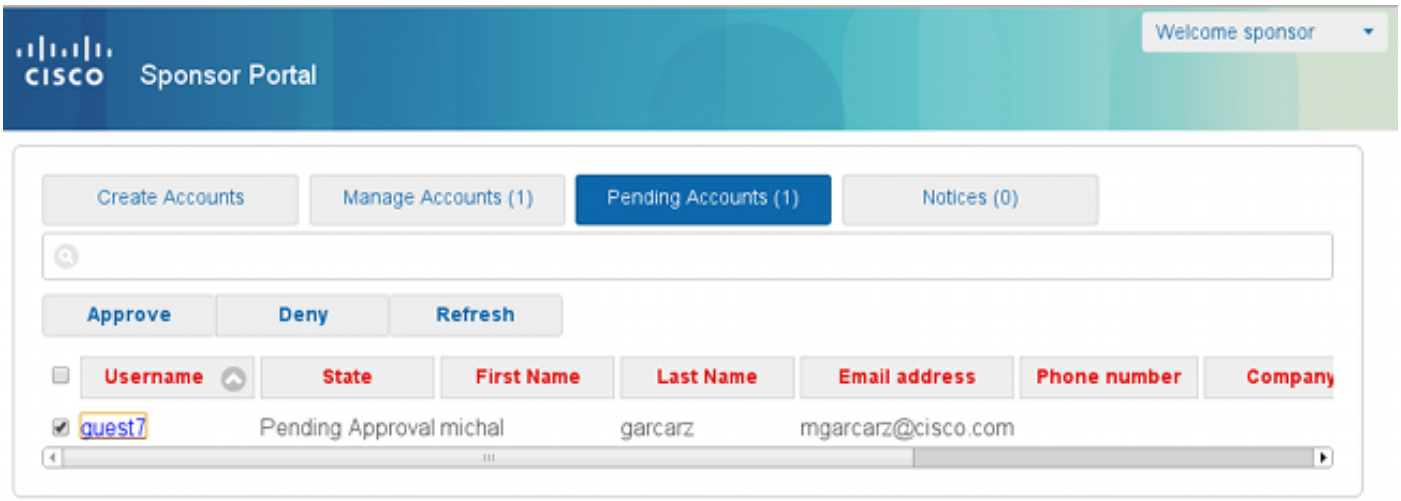


啟用**要求自助註冊訪客獲得批准**選項後，使用者名稱和密碼欄位將自動從**Include this information on the Self-Registration Success page**部分刪除。這就是在需要發起人批准時，訪客使用者的憑據預設情況下不會顯示在顯示帳戶已建立資訊的網頁上的原因。相反，它們必須通過簡訊服務(SMS)或電子郵件傳送。此選項必須在**Send credential notification upon approval using**部分(標籤電子郵件/SMS)中啟用。

向發起人傳送通知電子郵件：



發起人登入發起人門戶並批准帳戶：



從此時起，允許訪客使用者登入（使用電子郵件或SMS接收的憑證）。

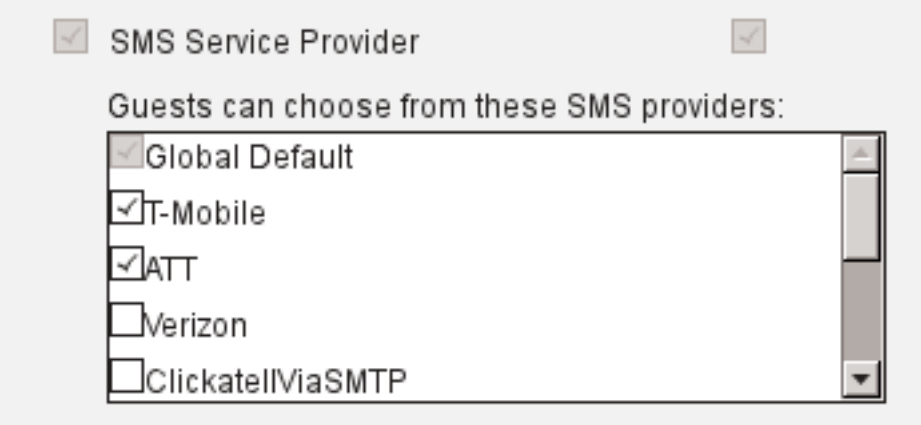
總之，此流程中使用了三個電子郵件地址：

- 通知「發件人」地址。這是靜態定義的，或者取自發起人帳戶，並用作兩者的起始地址：向發起人傳送通知（供審批），並向訪客傳送憑據詳細資訊。此配置在**Guest Access > Configure > Settings > Guest Email Settings**下配置。
- 通知「收件人」地址。用於通知發起人已收到要審批的帳戶。這在Guest Portal中的**Guest Access > Configure > Guest Portals > Portal Name > Require self-registered guests to be approved > Email approval request to**下配置。
- 訪客「收件人」地址。這是由訪客使用者在註冊期間提供的。如果選中**Send credential notification upon approval using Email**，則會將包含憑據詳細資訊（使用者名稱和密碼）的電子郵件傳送給訪客。

通過簡訊傳遞憑證

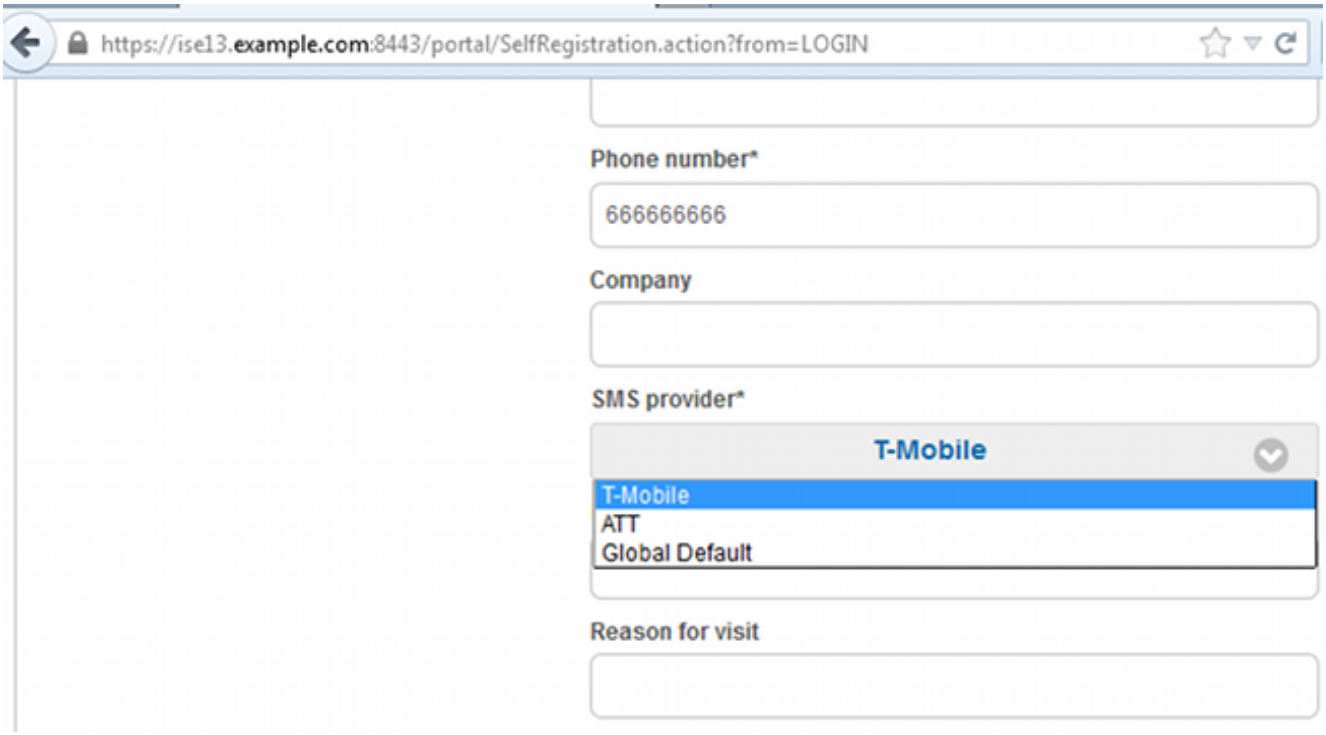
訪客憑證也可以通過SMS傳送。應配置以下選項：

1. 選擇SMS服務提供程式：

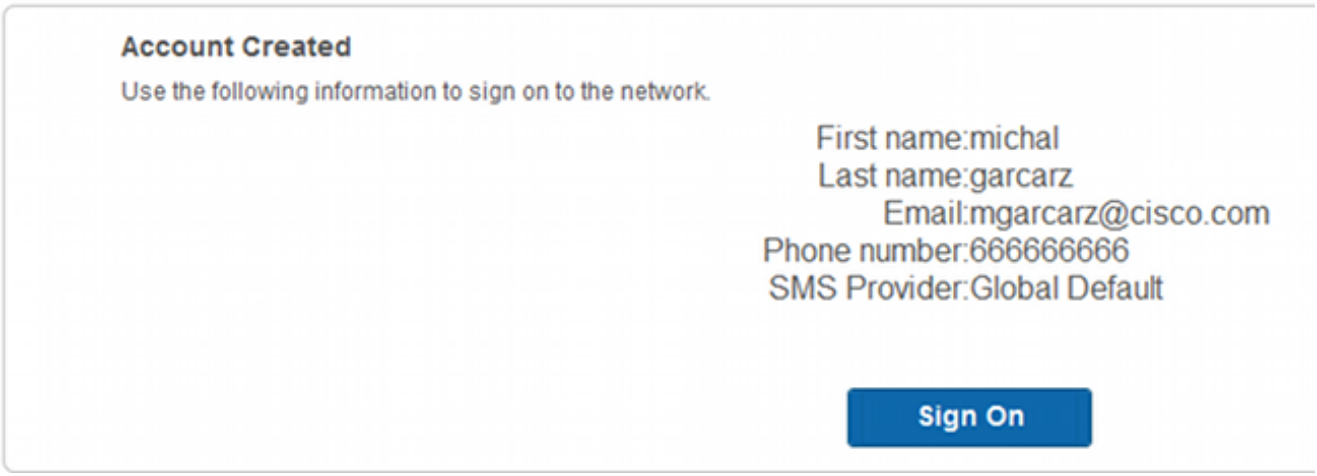


2. 使用以下命令選中**Send credential notification upon approval:SMS**覈取方塊。

3. 然後，訪客使用者在建立帳戶時需要選擇可用的提供商：



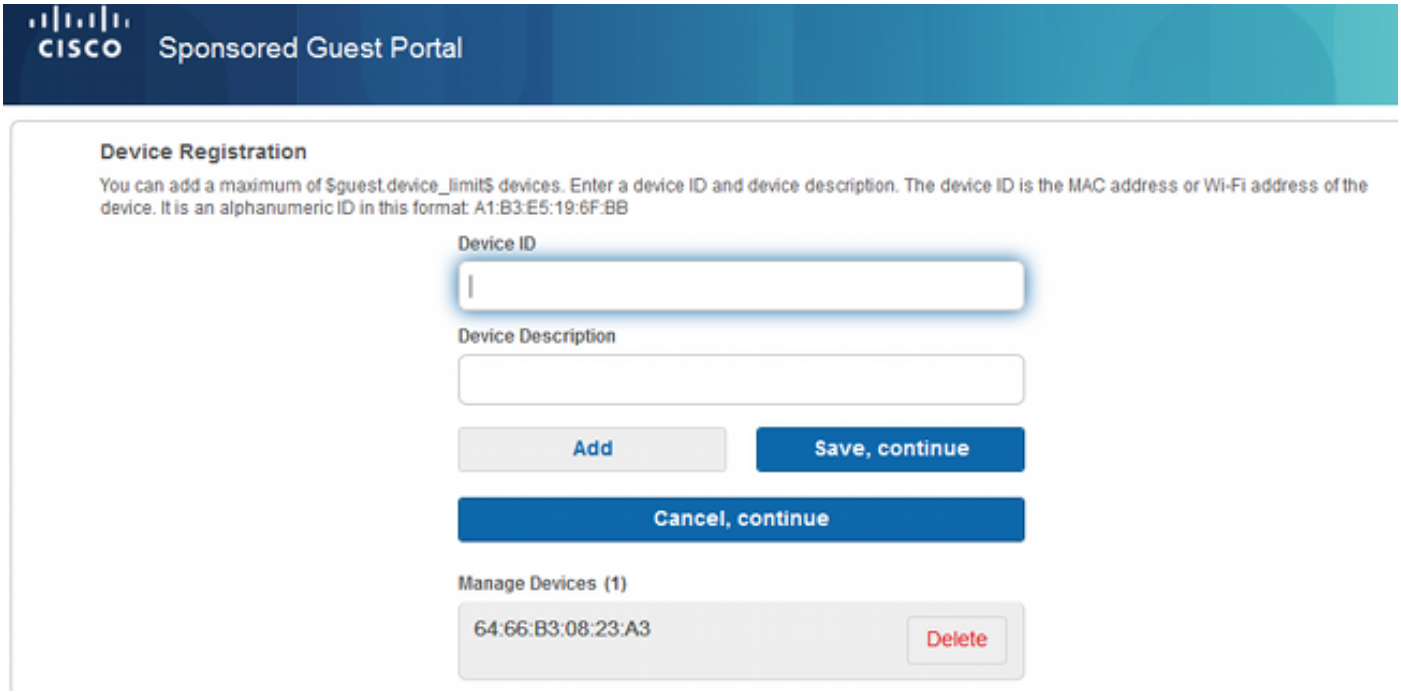
4. 隨所選提供商和電話號碼傳送SMS:



5. 您可以在**管理>系統>設定> SMS網關**下配置SMS提供程式。

裝置註冊

如果在訪客使用者登入並接受AUP後選擇了**Allow guests to register devices**選項，則可以註冊裝置：

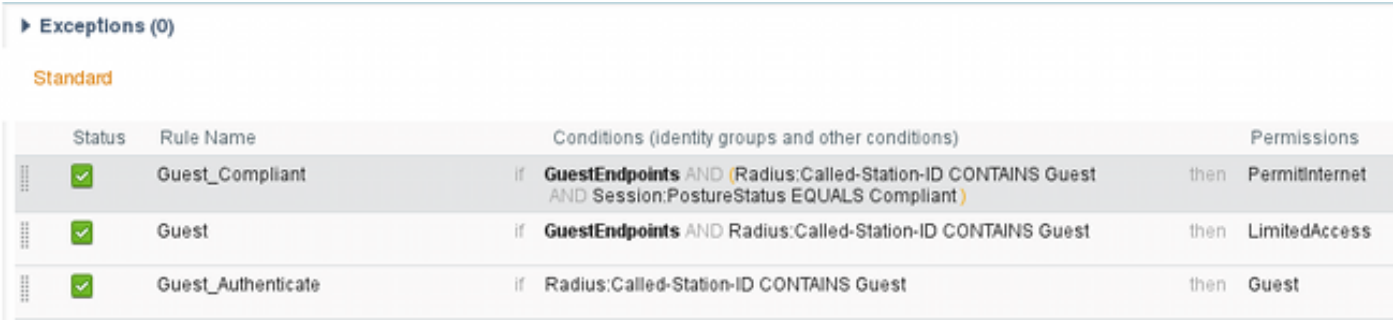


請注意，裝置已自動新增（它位於「管理裝置」清單中）。 這是因為選擇了**Automatically register guest devices**。

狀態

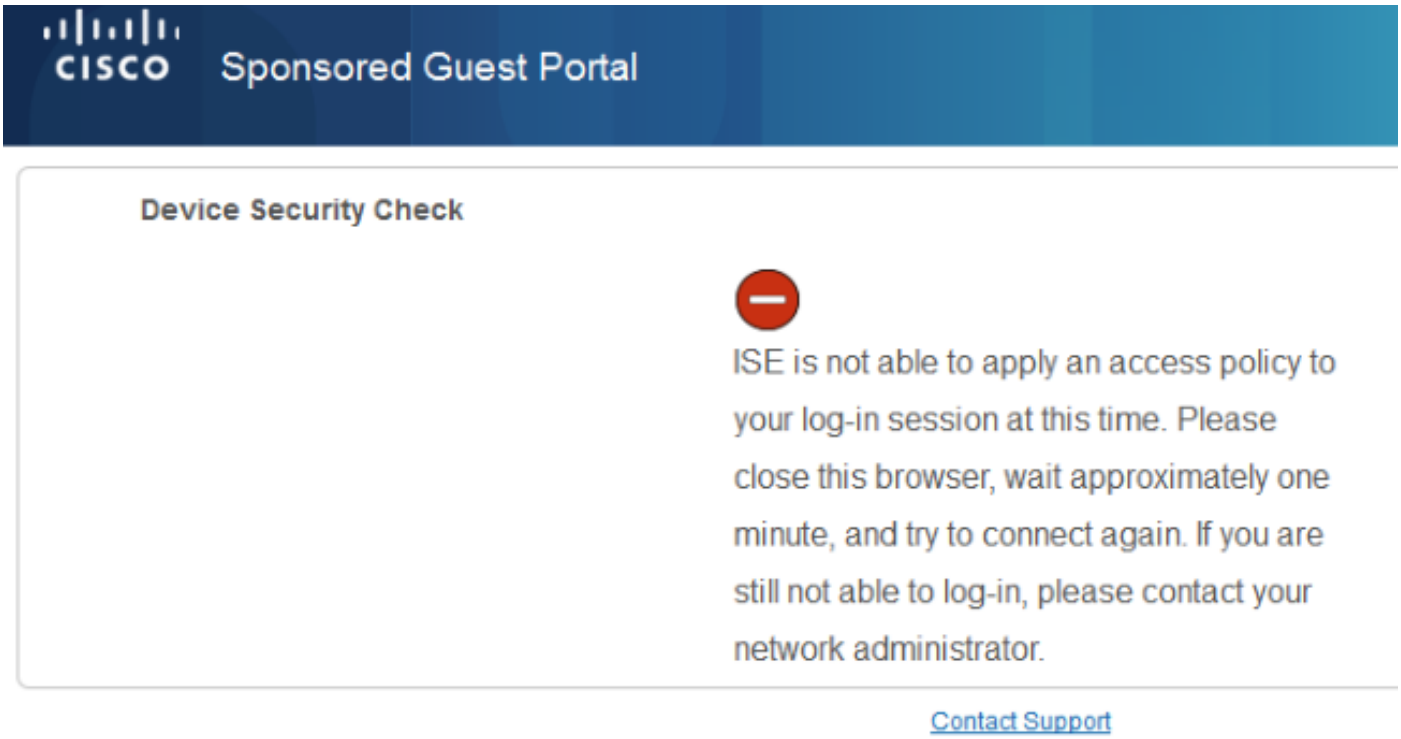
如果選擇了**Require guest device compliance**選項，則訪客使用者登入並接受AUP（以及可選地執行裝置註冊）後，會使用執行狀態（NAC/Web代理）的代理進行調配。ISE處理客戶端調配規則，以決定應調配哪個代理。然後，在站點上運行的代理執行安全評估（根據安全評估規則）並將結果傳送到ISE，ISE會根據需要傳送CoA重新身份驗證以更改授權狀態。

可能的授權規則可能如下所示：



第一個遇到Guest_Authenticate規則的新使用者重定向到自助註冊訪客門戶。使用者自行註冊並登入後，CoA會更改授權狀態，使用者將獲得執行狀態和補救的有限訪問許可權。只有在設定了NAC代理且工作站符合要求後，CoA才會再次更改授權狀態，以便提供對Internet的訪問。

安全狀態的典型問題包括缺少正確的客戶端調配規則：



如果您檢查guest.log檔案（ISE版本1.3中的新檔案），也可以確認這一點：

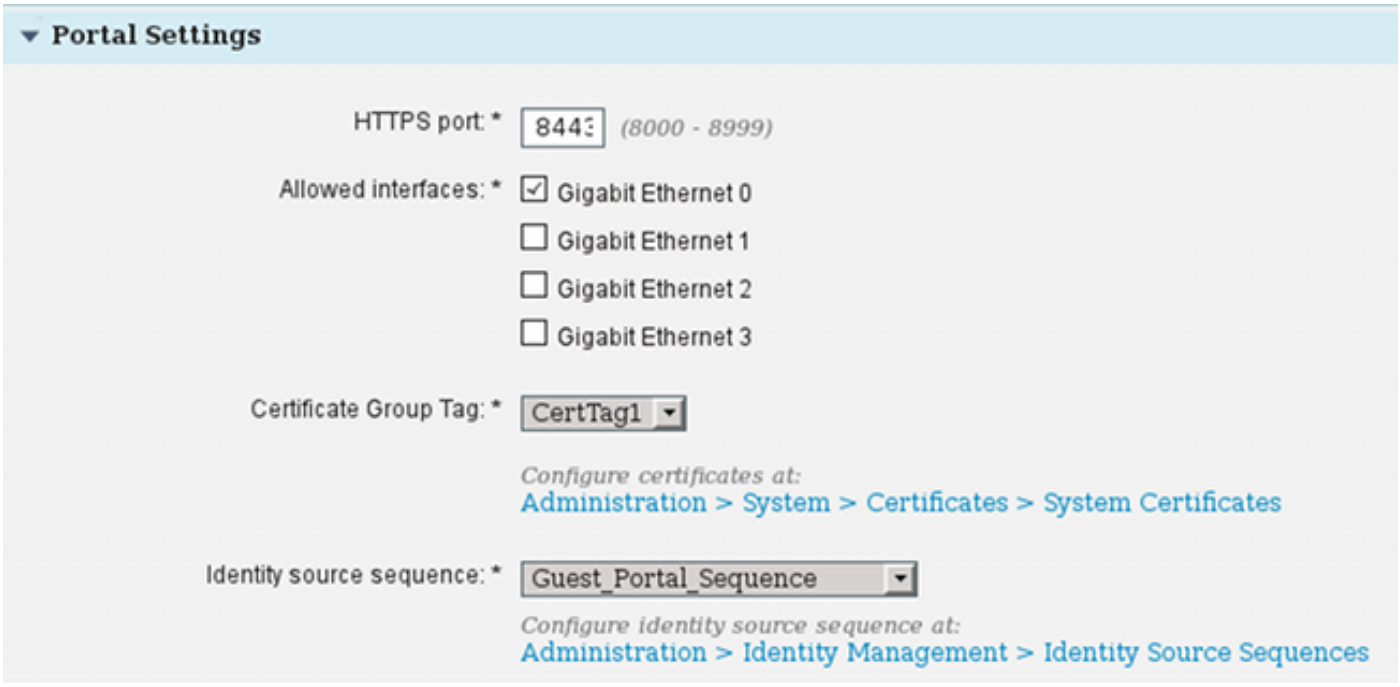
```
2014-08-01 21:35:08,435 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.ClientProvStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
CP Response is not successful, status=NO_POLICY
```

自帶裝置

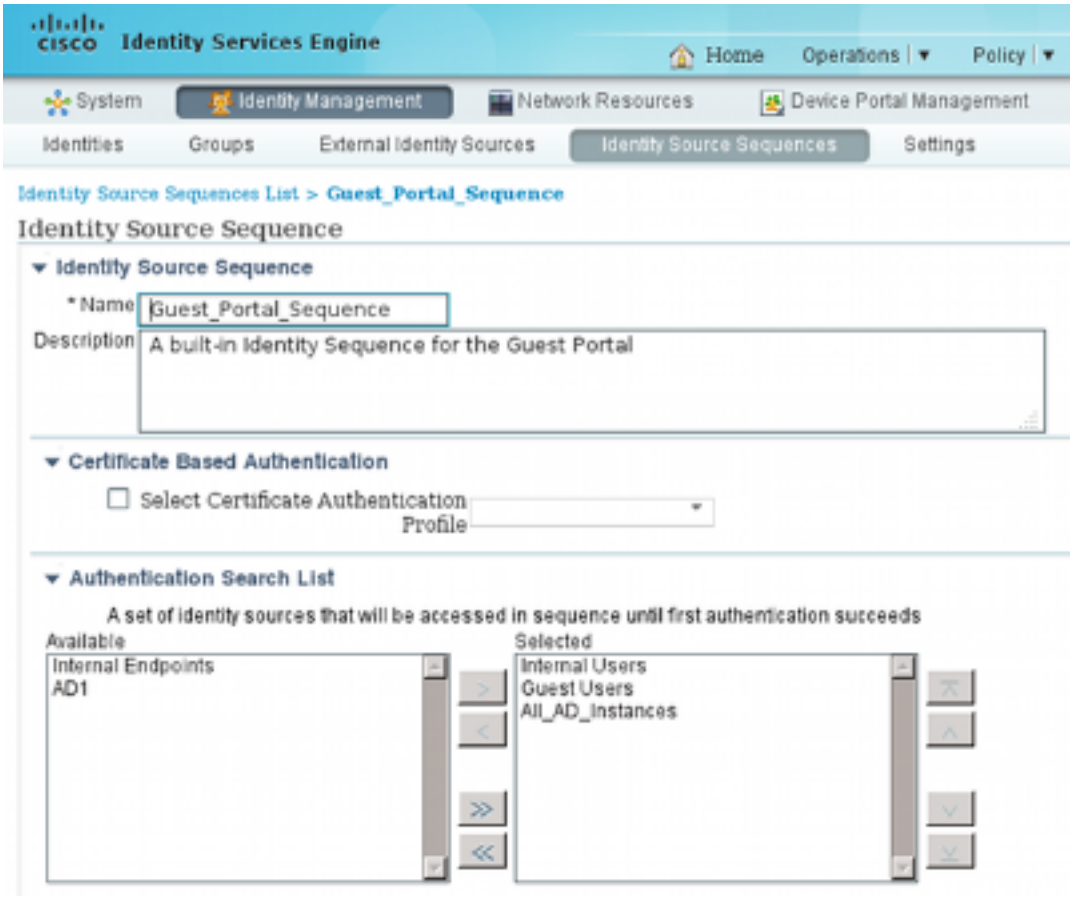
如果選中**Allow employees to use personal devices on the network**選項，則使用此門戶的公司使用者可以通過BYOD流程並註冊個人裝置。對於訪客使用者，該設定不會更改任何內容。

「員工使用門戶作為訪客」是什麼意思？

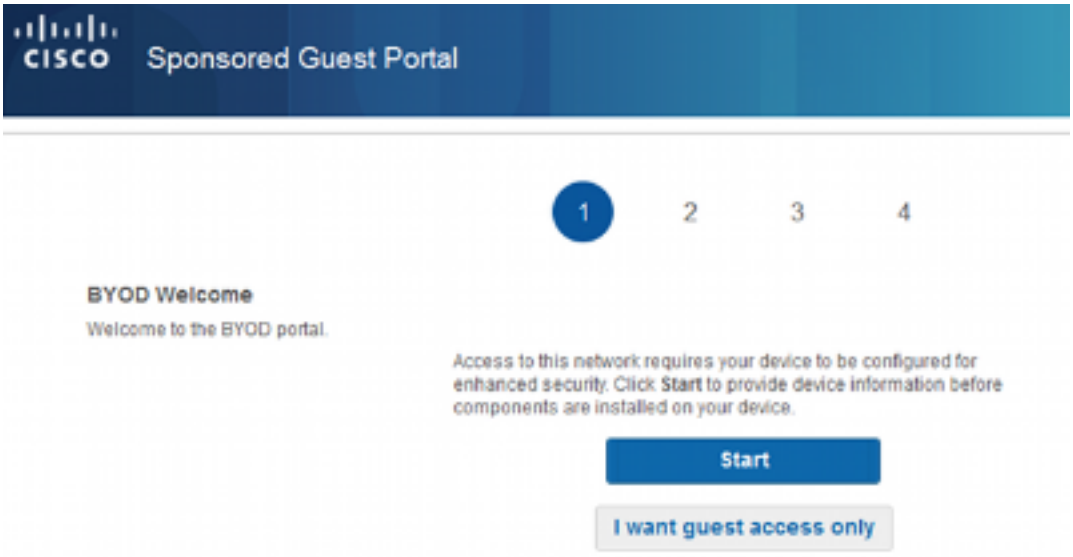
預設情況下，使用**Guest_Portal_Sequence** identity store配置訪客門戶：



這是首先嘗試內部使用者（在訪客使用者之前）的內部儲存序列：



在訪客門戶的此階段，使用者提供在內部使用者儲存中定義的憑證，並進行BYOD重定向：



這樣，企業使用者可以針對個人裝置執行BYOD。

如果提供了訪客使用者憑證而不是內部使用者憑證，則繼續正常流程（無BYOD）。

VLAN更改

此選項類似於ISE版本1.2中針對訪客門戶配置的VLAN更改。它允許您運行activeX或Java小程式，從而觸發DHCP釋放和續訂。當CoA觸發終端的VLAN更改時，需要執行此操作。使用MAB時，終端並不知道VLAN的變化。一種可能的解決方案是使用NAC代理更改VLAN（DHCP發佈/更新）。另一種方法是通過網頁上返回的小程式請求新的IP地址。可以配置發佈/CoA/續訂之間的延遲。流動裝置不支援此選項。

相關資訊

- 思科ISE上的終端安全評估服務配置指南
- 帶身份服務引擎的無線BYOD
- 適用於BYOD的ISE SCEP支援配置示例
- 思科ISE 1.3管理員指南
- 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