

為ISE管理配置證書或基於智慧卡的身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[將ISE加入Active Directory](#)

[選擇目錄組](#)

[為管理訪問啟用Active Directory基於密碼的身份驗證](#)

[將外部身份組對映到管理員組](#)

[匯入受信任的證書](#)

[配置證書身份驗證配置檔案](#)

[啟用基於客戶端證書的身份驗證](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹如何為身份服務引擎(ISE)管理訪問配置基於客戶端證書的身份驗證。在本示例中，ISE管理員根據使用者證書進行身份驗證，以獲得對思科身份服務引擎(ISE)管理GUI的管理員訪問許可權。

必要條件

需求

思科建議瞭解以下主題：

- 用於密碼和證書身份驗證的ISE配置。
- Microsoft Active Directory(AD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

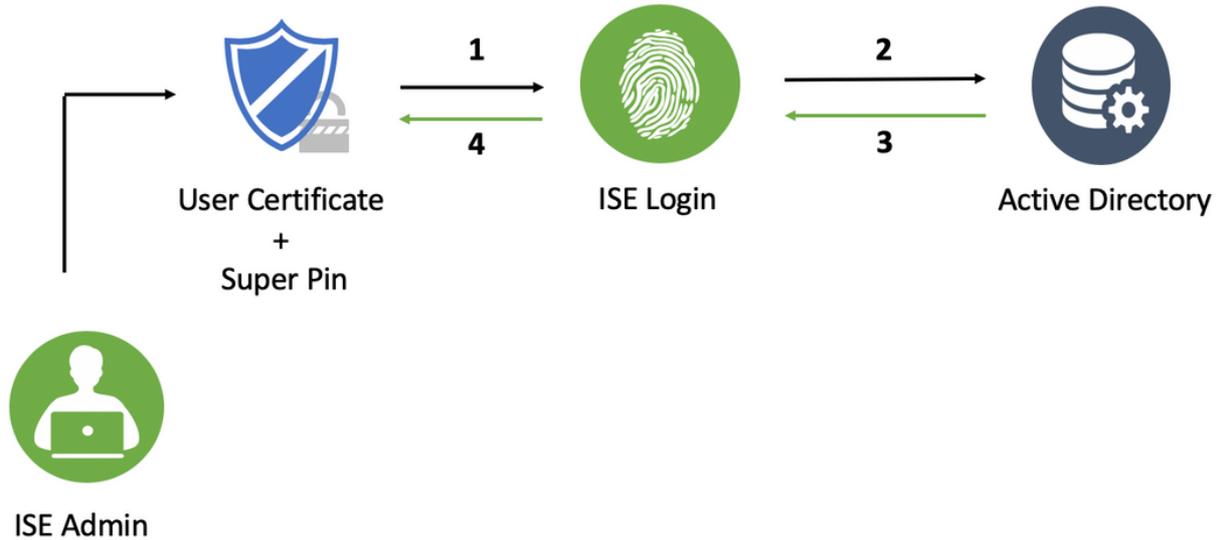
- 思科身分識別服務引擎(ISE)版本2.6
- Windows Active Directory(AD)Server 2008版本2
- 憑證

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。如果網路處於活動狀態，請確保瞭解任何配置的潛在影響。

設定

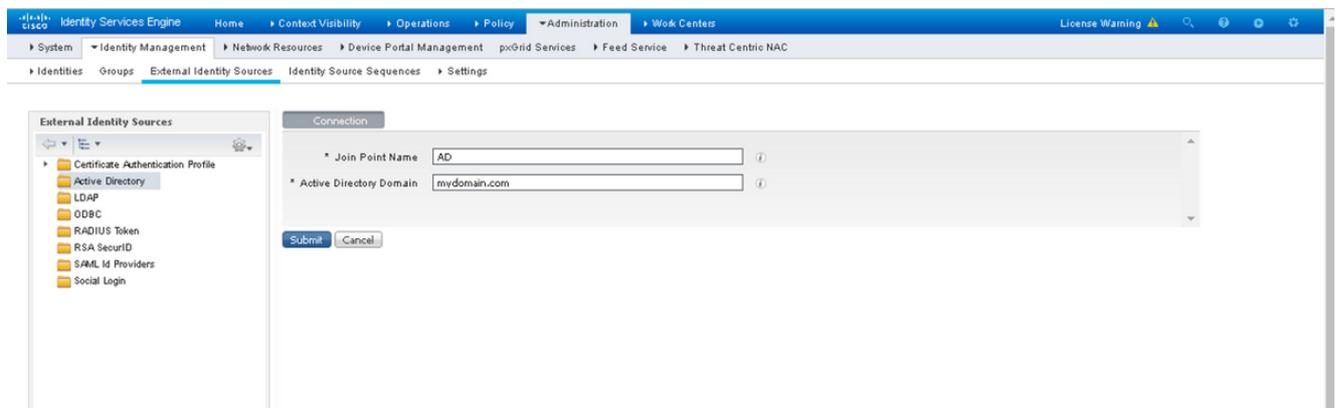
使用此部分將客戶端證書或智慧卡配置為外部身份，以便管理訪問思科ISE管理GUI。

網路圖表

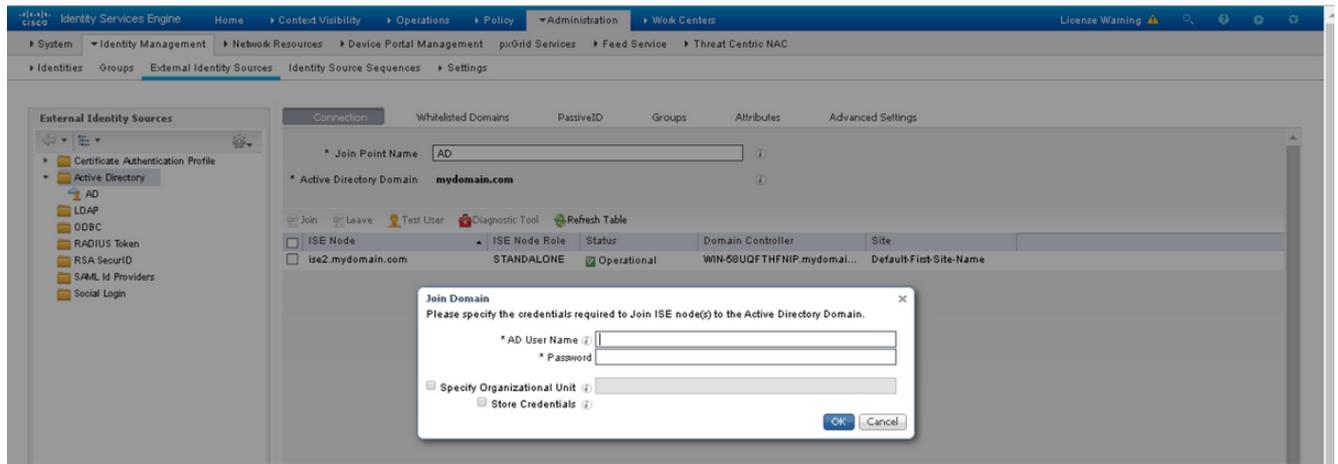


將ISE加入Active Directory

1. 選擇Administration > 身份管理>外部身份源> Active Directory。
2. 在思科ISE中建立具有加入點名稱和AD域的Active Directory例項。
3. 按一下「Submit」。



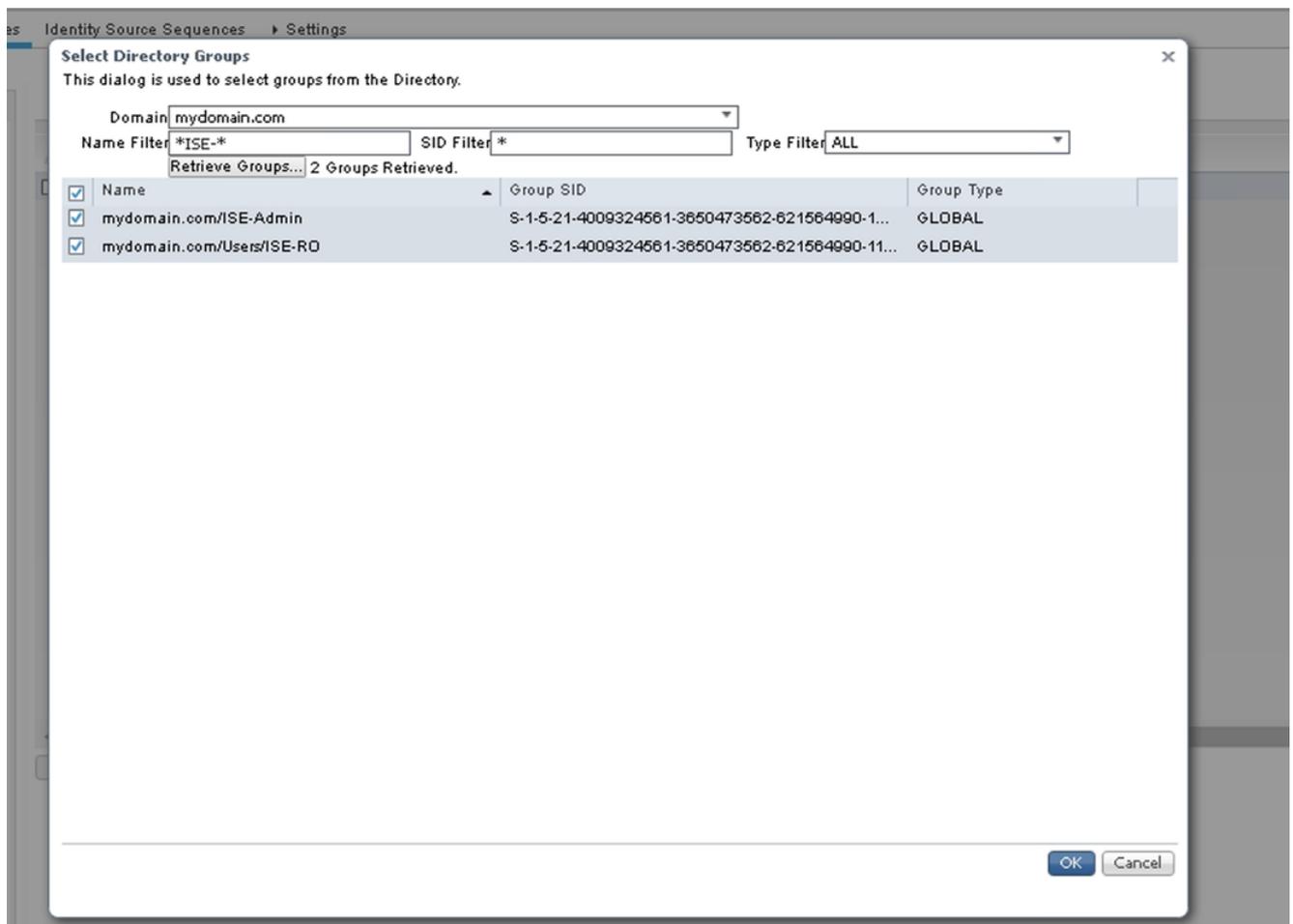
4. 在提示中使用適當的使用者名稱和密碼加入所有節點。



5. 按一下「Save」。

選擇目錄組

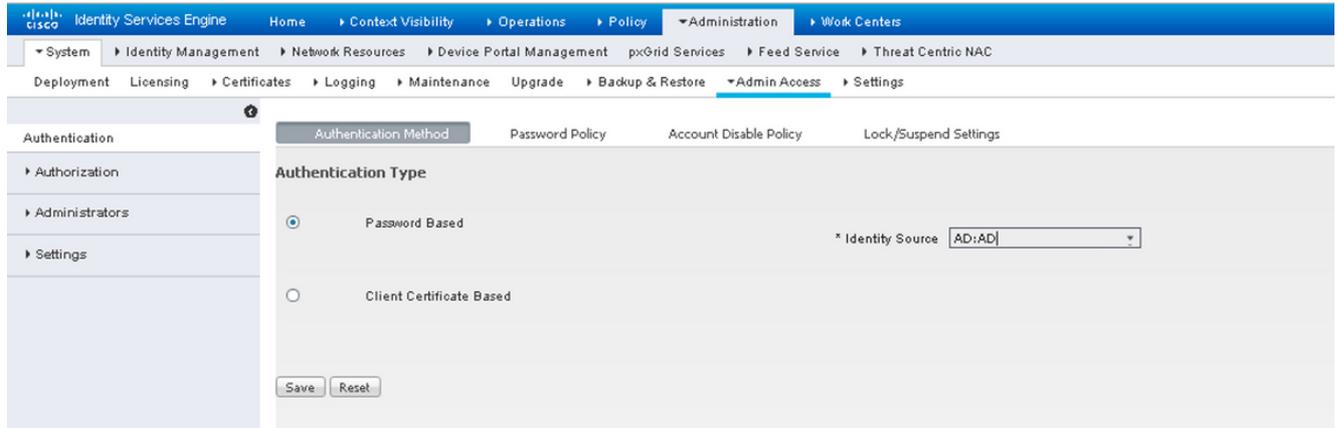
1. 建立外部管理員組並將其對映到Active Directory組。
2. 選擇**管理>身份管理>外部身份源>Active Directory>組>從目錄選擇組**。
3. 至少檢索管理員所屬的一個AD組。



4. 按一下「Save」。

為管理訪問啟用Active Directory基於密碼的身份驗證

1. 啟用Active Directory例項作為之前加入ISE的基於密碼的身份驗證方法。
2. 選擇Administration > System > Admin access > Authentication，如下圖所示。



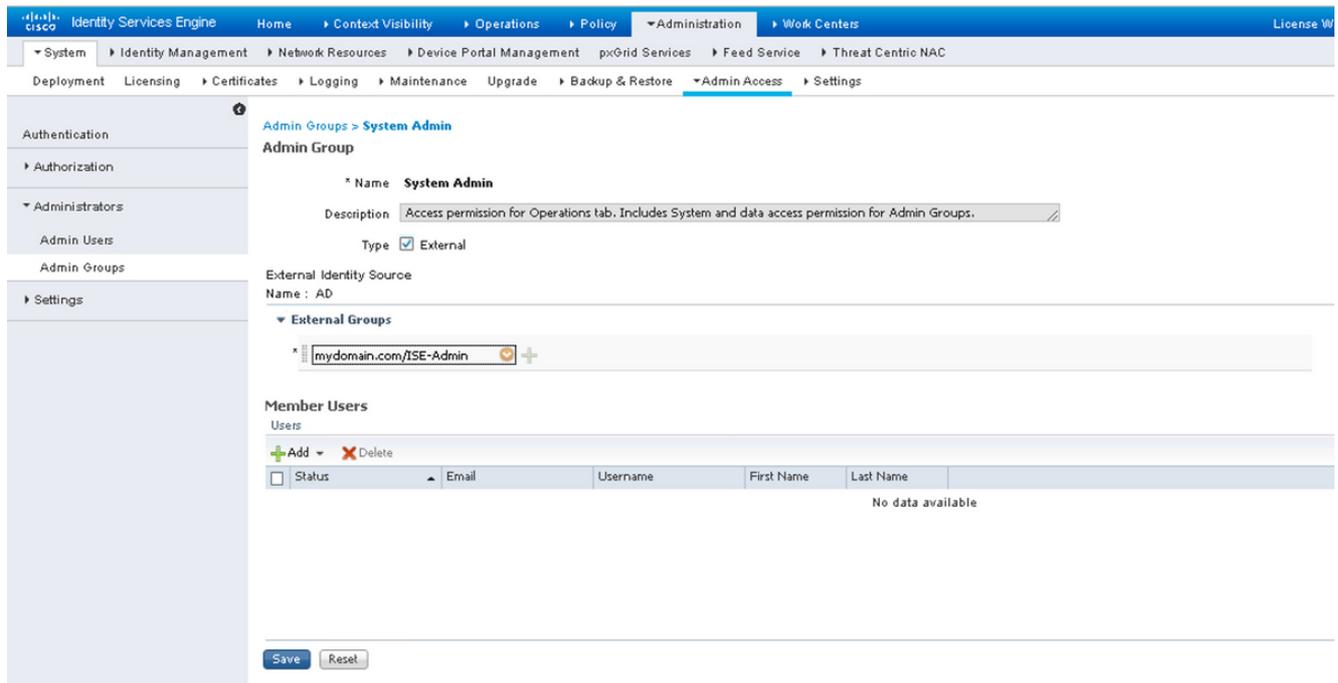
3. 按一下「Save」。

附註：啟用基於證書的身份驗證需要基於密碼的身份驗證配置。成功設定基於憑證的驗證後，應還原此組態。

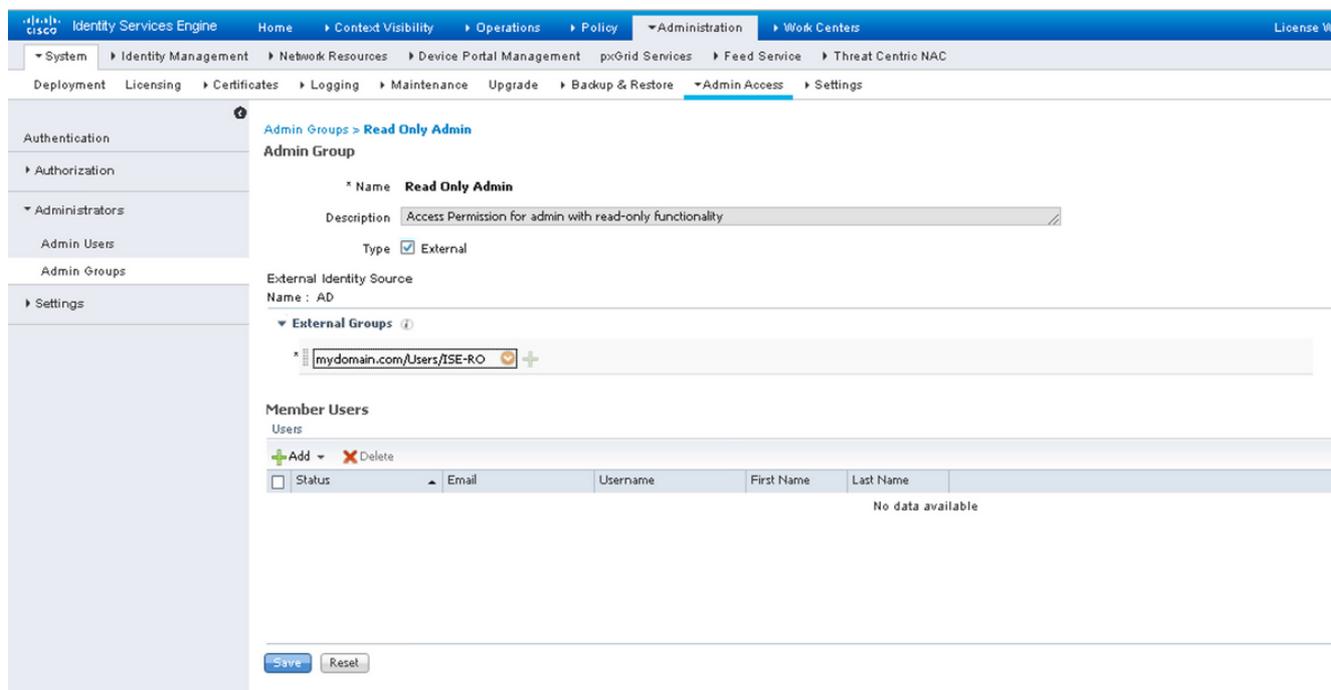
將外部身份組對映到管理員組

在本示例中，外部AD組對映到預設的Admin組。

1. 選擇Administration > System > Admin Access > Administrators > Admin Groups > Super admin。
2. 選中Type as External，然後在External groups下選擇AD組。



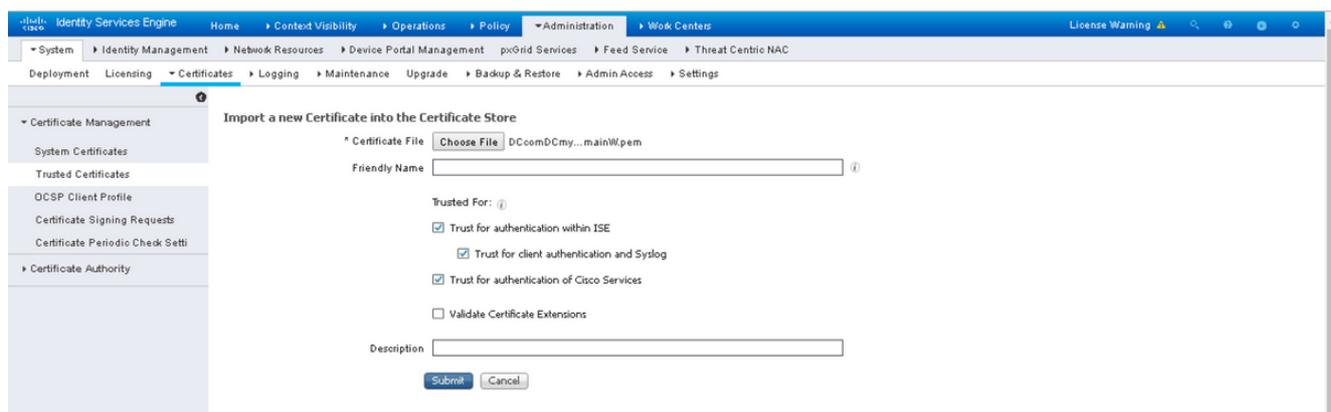
- 按一下「Save」。
- 選擇 Administration > System > Admin Access > Administrators > Admin Groups > Read Only Admin。
- 選中 Type as External，然後在 External groups 下選擇 AD 組，如下圖所示。



- 按一下「Save」。

匯入受信任的證書

- 匯入簽署客戶端證書的證書頒發機構(CA)證書。
- 選擇 Administrator > System > Certificates > Trusted Certificate > Import。
- 按一下「瀏覽」並選擇CA證書。
- 勾選「Trust for client authentication and Syslog」覈取方塊，如下圖所示。



5. 按一下**Submit** (提交)。

配置證書身份驗證配置檔案

1. 要為基於客戶端證書的身份驗證建立證書身份驗證配置檔案，請選擇**Administration > 身份管理 > 外部身份源 > 證書身份驗證配置檔案 > 新增**。
2. 新增配置檔名稱。
3. 在證書屬性中選擇包含管理員使用者名稱的相應屬性。
4. 如果使用者的AD記錄包含使用者的證書，並且希望將從瀏覽器收到的證書與AD中的證書進行比較，請選中**Always perform binary comparison**覈取方塊，並選擇之前指定的Active Directory例項名稱。

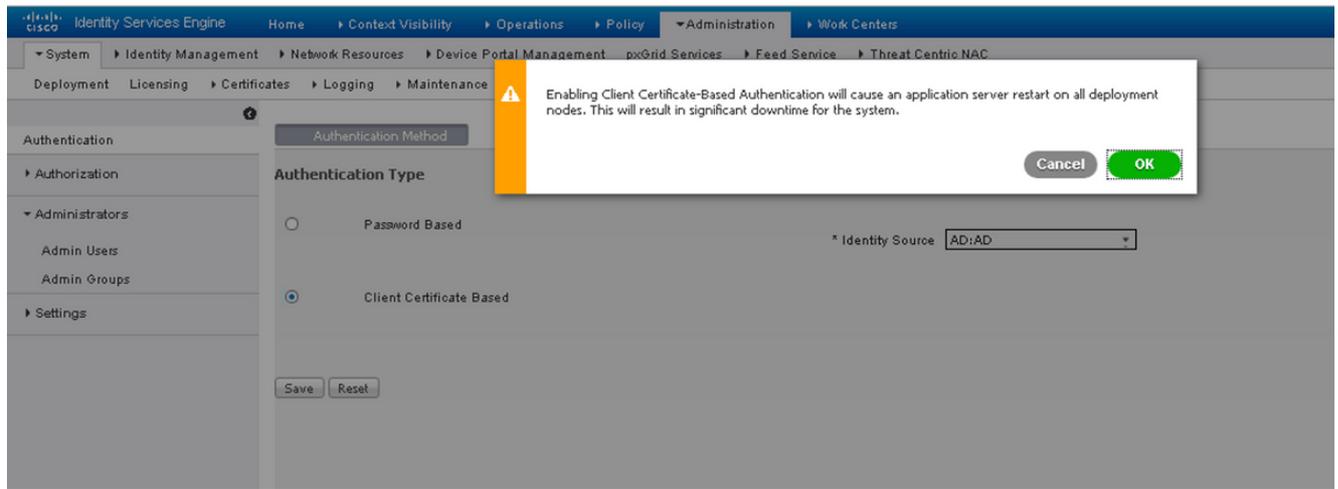
The screenshot shows the Cisco ISE configuration page for a new Certificate Authentication Profile. The breadcrumb navigation is: Administration > Work Centers > Identity Management > External Identity Sources > Certificate Authentication Profiles List > New Certificate Authentication Profile. The left sidebar shows a tree view of External Identity Sources, with 'Active Directory' expanded to show 'AD' selected. The main form fields are: Name: CAC_Login_Profile; Description: (empty text area); Identity Store: AD; Use Identity From: Certificate Attribute (selected), with a dropdown menu showing 'Subject Alternative Name - Other Name'; Match Client Certificate Against Certificate In Identity Store: Always perform binary comparison (selected). There are 'Submit' and 'Cancel' buttons at the bottom.

5. 按一下**Submit** (提交)。

附註：相同的證書身份驗證配置檔案也可用於基於身份의終端身份驗證。

啟用基於客戶端證書的身份驗證

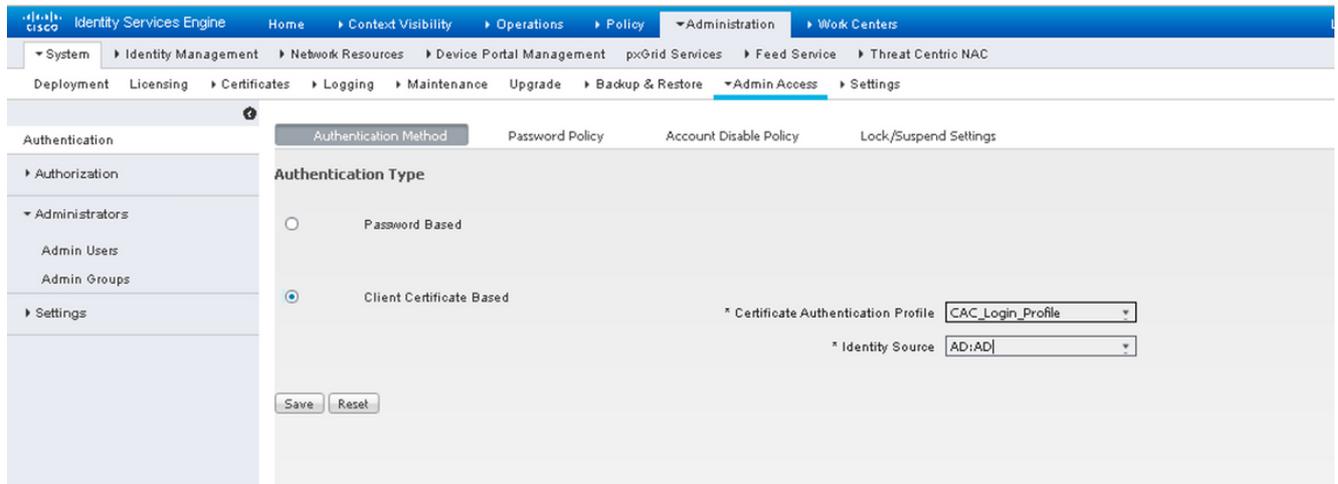
1. 選擇 **Administration > System > Admin Access > Authentication > Authentication Method Client Certificate Based**。



2. 按一下「OK」（確定）。

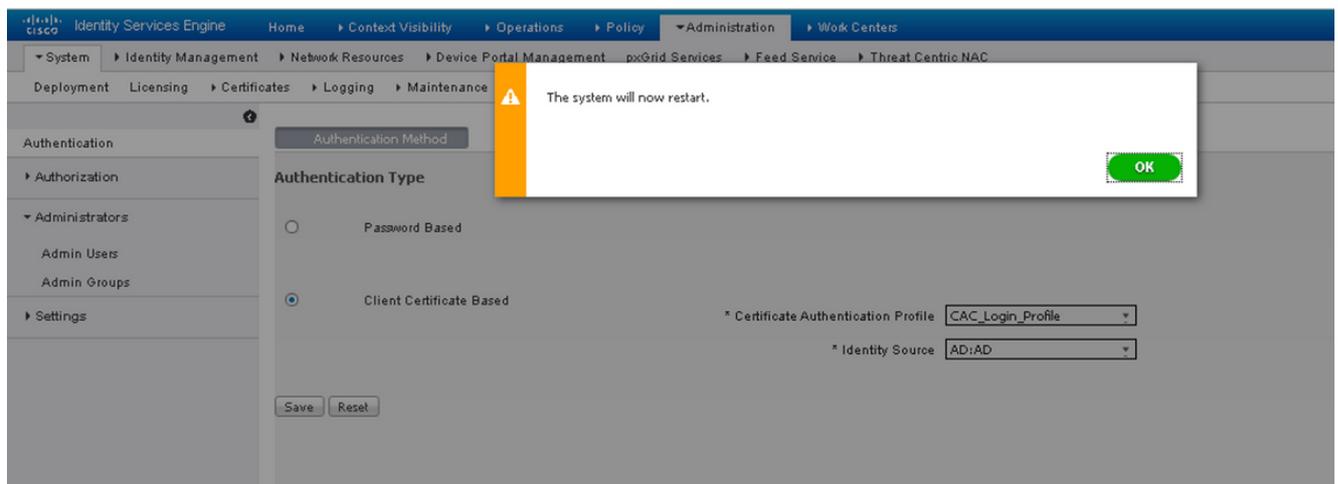
3. 選擇之前配置的Certificate Authentication Profile。

4. 選擇Active Directory例項名稱。



5. 按一下「Save」。

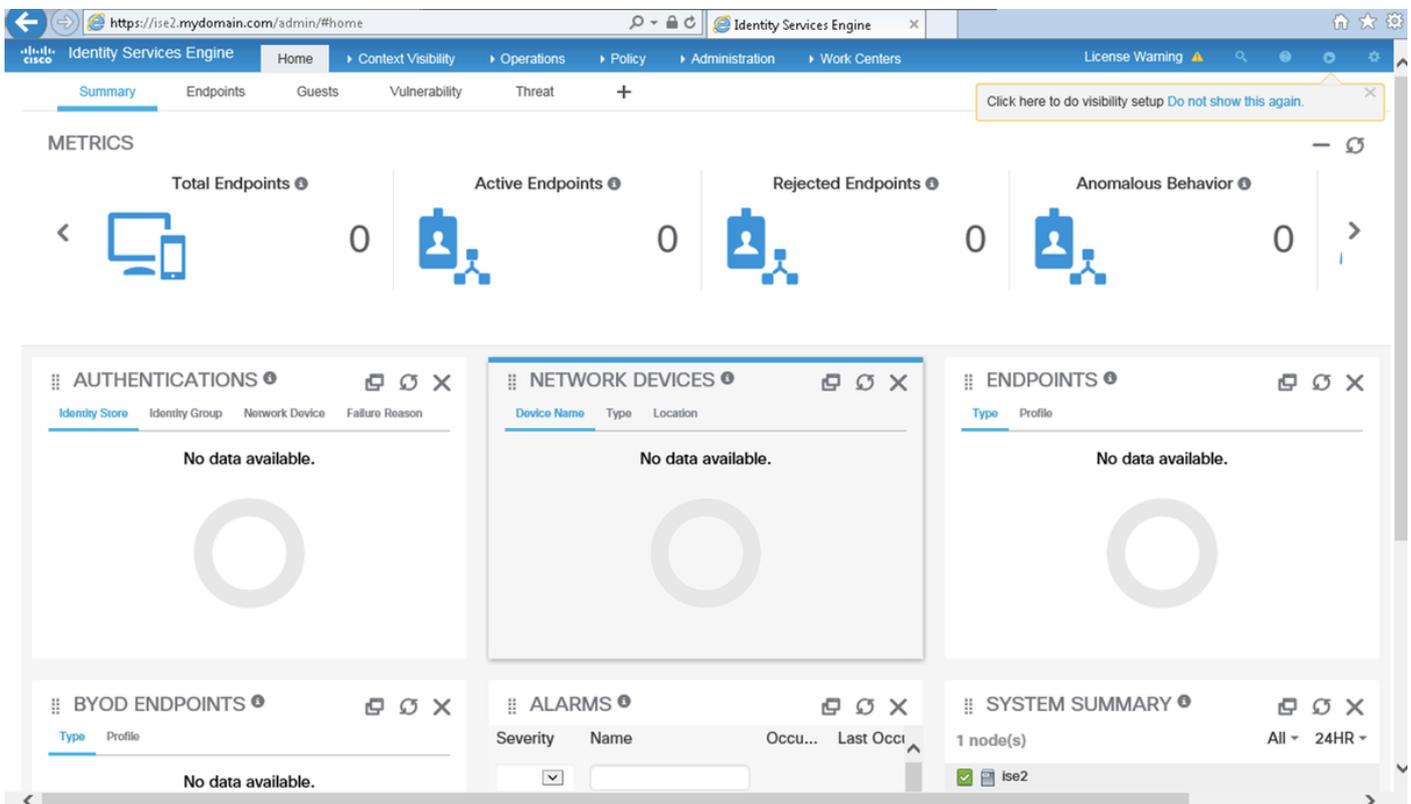
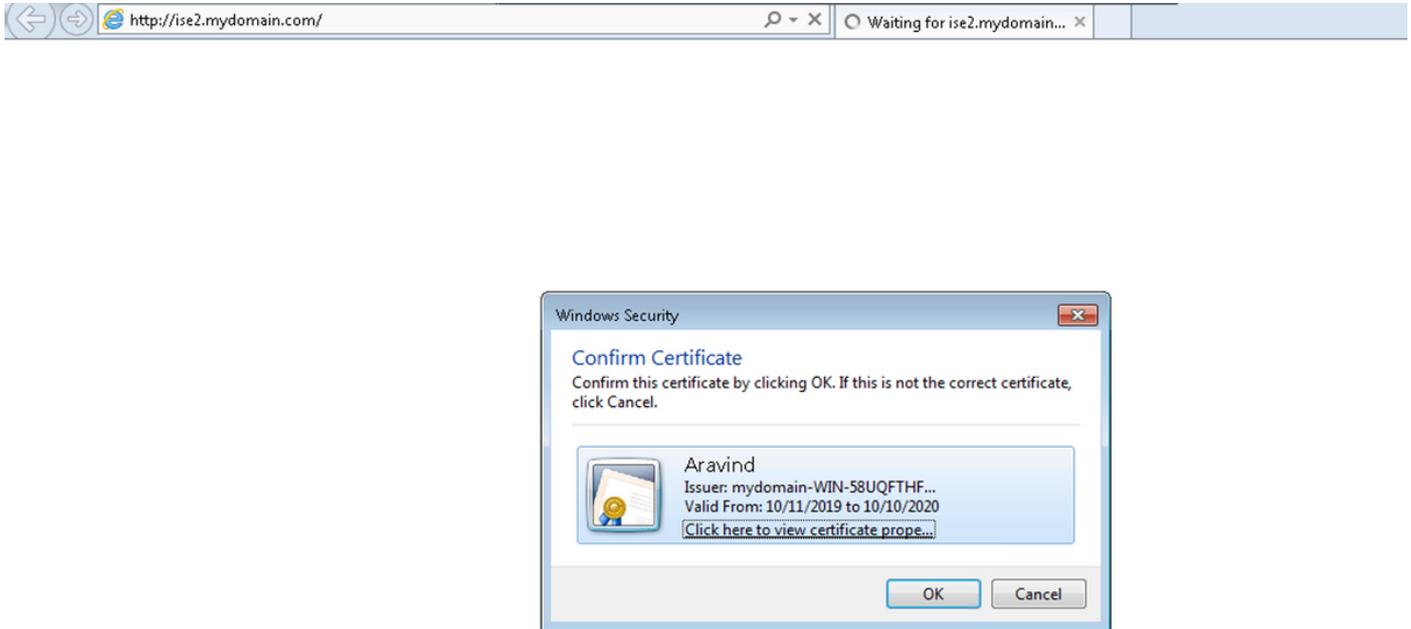
6. 部署中的所有節點上的ISE服務重新啟動。



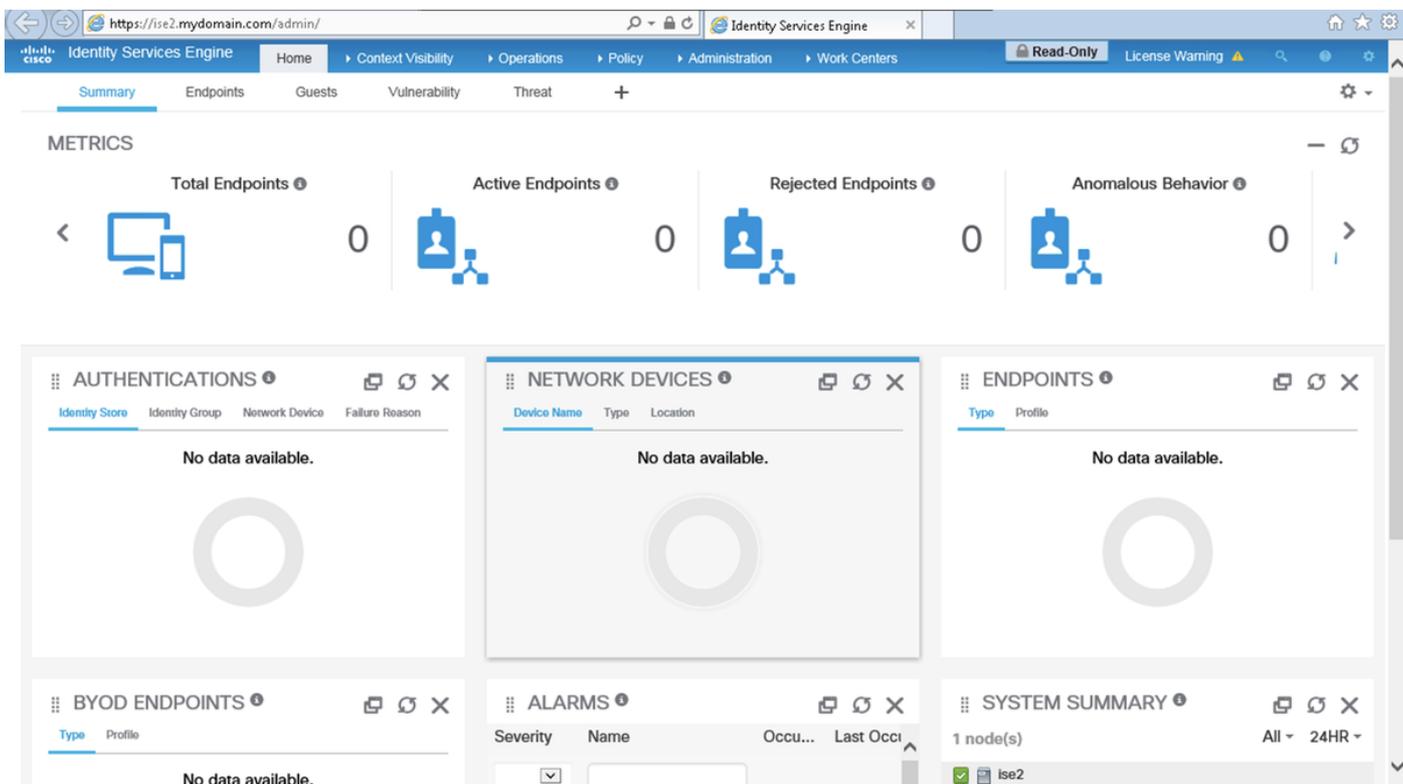
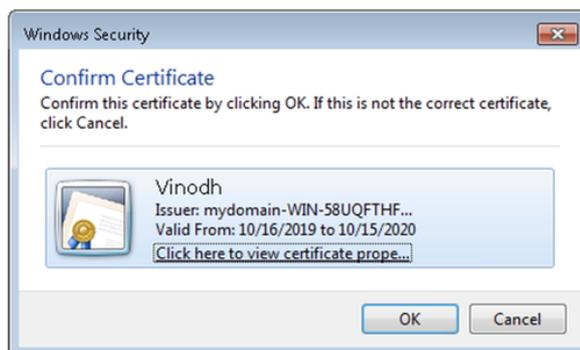
驗證

在應用伺服器服務狀態更改為正在運行後驗證對ISE GUI的訪問。

超級管理員用戶：驗證是否提示使用者選擇證書以登入到ISE GUI，如果證書屬於超級管理員外部身份組的使用者部分，則授予超級管理員許可權。



只讀管理員用戶：驗證是否提示使用者選擇證書以登入ISE GUI，如果證書屬於只讀管理員外部身份組的使用者部分，則授予只讀管理員許可權。



附註：如果使用通用訪問卡(CAC)，則智慧卡在使用者輸入其有效的超級個人識別碼後向ISE提供使用者證書。

疑難排解

1. 使用 `application start ise safe` 命令以安全模式啟動Cisco ISE，該模式允許臨時禁用對管理員門戶的訪問控制，並使用 `application stop ise` 命令，然後使用 `application start ise` 命令更正配置並重新啟動ISE的服務。
2. 如果管理員無意中阻止所有使用者訪問Cisco ISE管理員門戶，安全選項提供恢復方法。如果

管理員在Administration > Admin Access > Settings > Access頁面中配置了一個不正確的IP Access清單，則會發生此事件。**safe**選項還可繞過基於證書的身份驗證，並還原為預設使用者名稱和密碼身份驗證，以便登入到思科ISE管理員門戶。