在ISE上配置證書續訂

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[設定](#)
[檢視 ISE 自我簽署憑證](#)
[判斷變更憑證的時機](#)
[產生憑證簽署要求](#)
[安裝憑證](#)
[設定警示系統](#)
[驗證](#)
[驗證警示系統](#)
[驗證憑證變更](#)
[驗證憑證](#)
[疑難排解](#)
[結論](#)

簡介

本文件說明更新 Cisco Identity Services Engine (ISE) 憑證的最佳作法和主動式程序。 它還檢查如何設定警報和通知，從而警告管理員即將發生的事件（如證書過期）。

> **附註**：不應將本文作為證書的診斷指南。

必要條件

需求

思科建議您瞭解以下主題：

- X509 憑證
- 使用憑證設定 Cisco ISE

採用元件

"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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。」

- Cisco ISE 版本 3.0.0.458
- 設備或 VMware

背景資訊

身為 ISE 系統管理員，您終究會面臨 ISE 憑證到期的事實。如果您的ISE伺服器具有過期的證書，則可能會出現嚴重問題，除非您將過期的證書替換為一個新的有效證書。

> **附註**：如果用於可擴展身份驗證協定(EAP)的證書過期，所有身份驗證都會失敗，因為客戶端不再信任ISE證書。如果ISE管理員證書過期，風險更大：管理員將無法再登入到ISE，並且分散式部署可以停止運行和複製。

ISE管理員必須在舊證書過期之前在ISE上安裝新的有效證書。此主動方法可防止或有效減少停機時間，以及避免對一般使用者造成影響。新安裝證書的時間期開始後，您可以在新證書上啟用EAP/管理員或任何其他角色。

您可以設定 ISE，使其產生警示並通知系統管理員在舊憑證到期之前安裝新的憑證。

> **附註**：本文檔使用ISE管理員證書作為自簽名證書來演示證書續訂的影響，但不推薦在生產系統中使用此方法。最好為EAP角色和Admin角色都使用CA證書。

設定

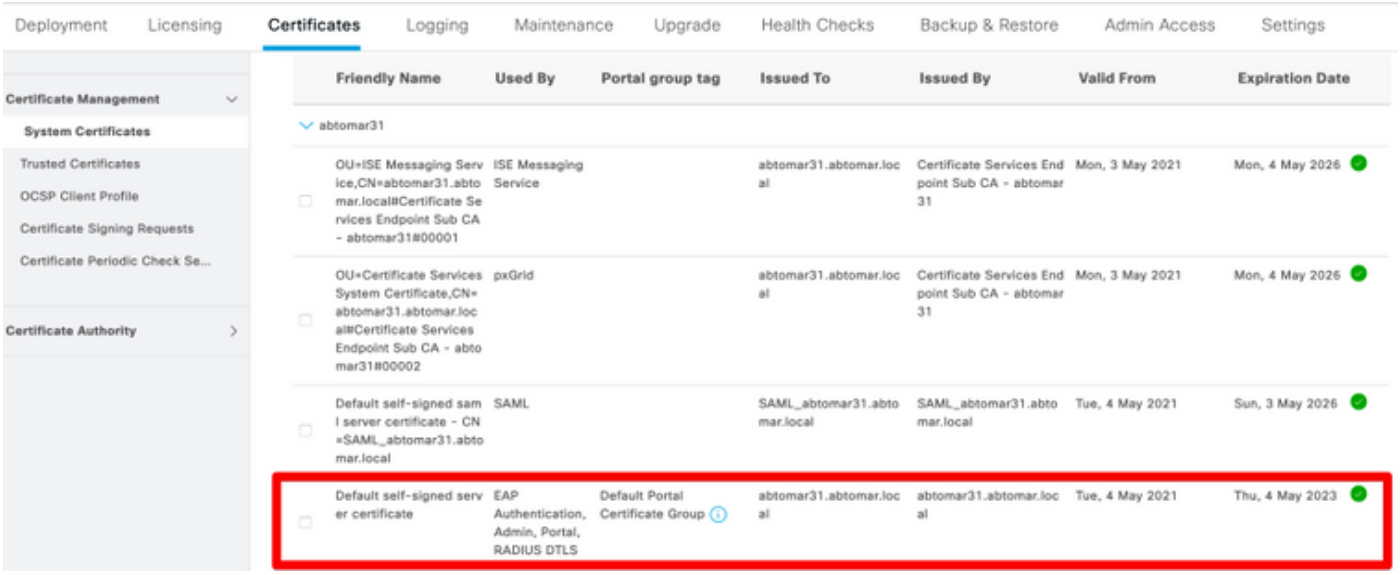
檢視 ISE 自我簽署憑證

安裝 ISE 後，此平台會產生自我簽署憑證。此自我簽署憑證可用來進行系統管理存取和分散式部署 (HTTPS) 的內部溝通，以及用來進行使用者驗證 (EAP)。 在實際運作的系統中，請使用 CA 憑證而非自我簽署憑證。

> **提示：**請參閱 Cisco Identity Services Engine 硬體安裝指南 3.0 版中的「Cisco ISE 中的憑證管理」一節，以取得其他相關資訊。

ISE 憑證的格式必須為隱私增強郵件 (PEM) 或辨別編碼規則 (DER)。

若要檢視初始的自我簽署憑證，請在 ISE GUI 中導覽至**「系統管理」>「系統」>「憑證」>「系統憑證」**，如下圖所示。



如果您透過憑證簽署要求 (CSR) 在 ISE 上安裝伺服器憑證，並變更系統管理員或 EAP 通訊協定的憑證，則自我簽署伺服器憑證仍會存在，但處於「未使用」狀態。

> **注意**：如果變更系統管理員通訊協定，則必須重新啟動 ISE 服務，而且會產生幾分鐘的停機時間。變更 EAP 通訊協定不會觸發 ISE 服務重新啟動，也不會發生停機情況。

判斷變更憑證的時機

假設安裝的憑證即將到期。應該等到憑證到期再來更新，還是在到期之前先變更憑證比較好？必須在到期之前更改證書，以便有時間計畫證書交換並管理交換導致的任何停機時間。

何時必須更改證書？請取得開始日期早於舊憑證到期日期的新憑證。這兩個日期之間的時間間隔即為變更期間。

> **注意**：如果您啟用「系統管理員」，將導致 ISE 伺服器的服務重新啟動，並會出現幾分鐘的停機時間。

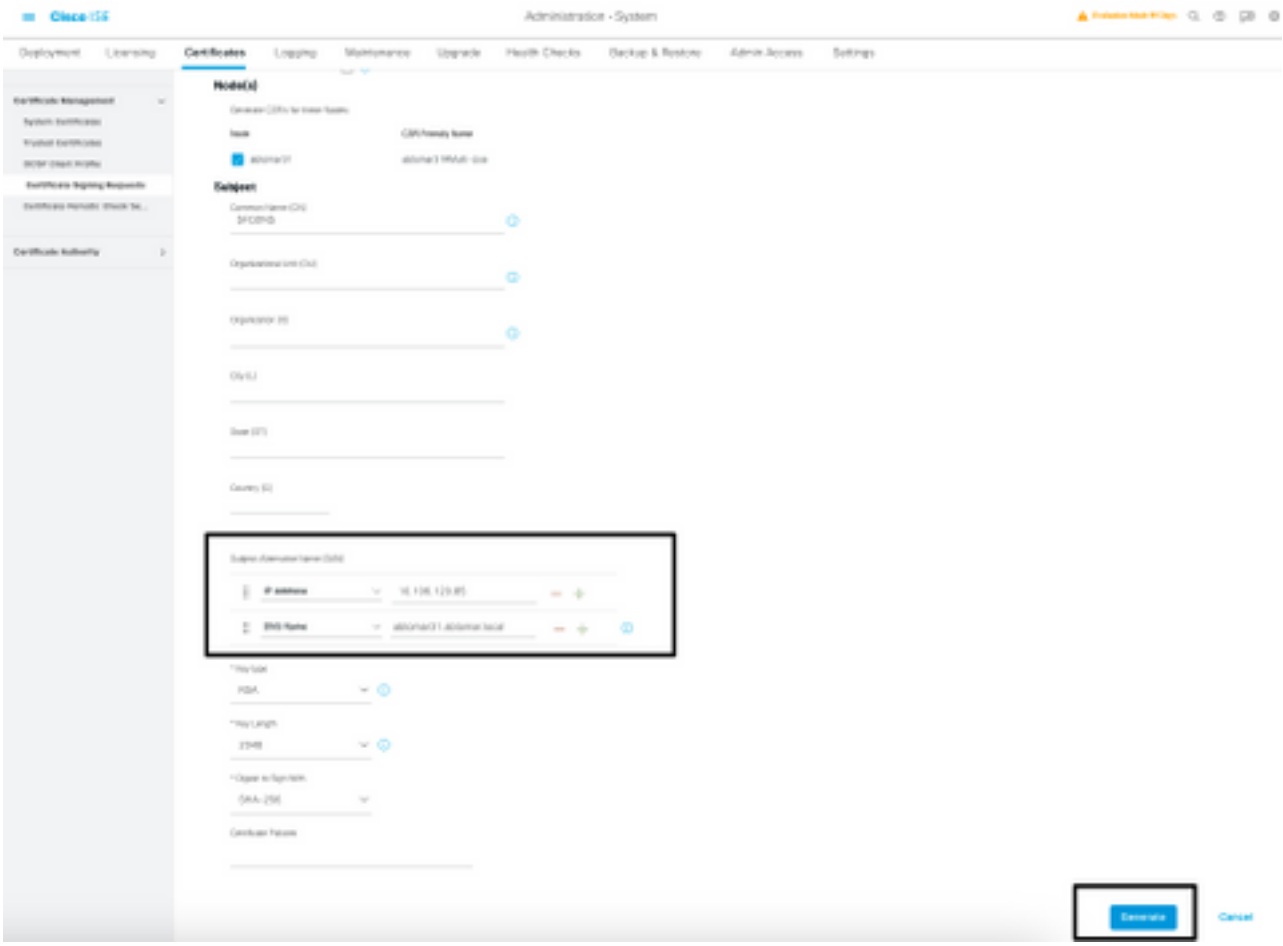
此圖描述即將到期之憑證的相關資訊：

產生憑證簽署要求

此程序說明如何透過 CSR 更新憑證：

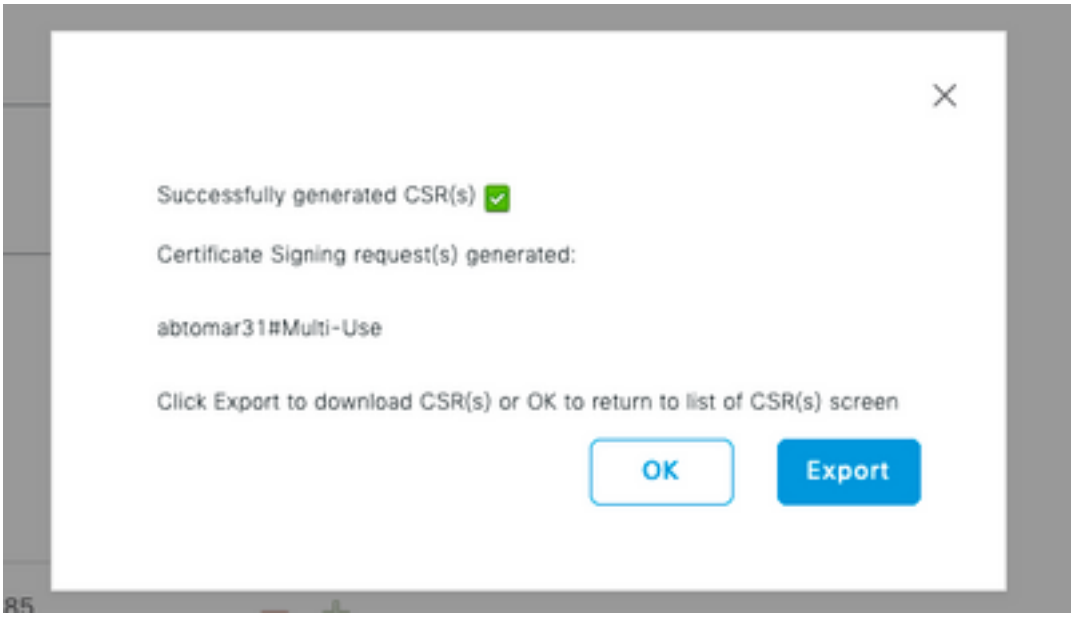
1. 在 ISE 主控台中，導覽至**「系統管理」**>**「系統」**>**「憑證」**>**「憑證簽署要求」**，然後按一下**「產生憑證簽署要求」**：

2. 您必須在**「憑證主體」**文字欄位中輸入的最少資訊為 CN=*ISEfqdn*，其中 *ISEfqdn* 是 ISE 的完整網域名稱 (FQDN)。使用逗號在「憑證主體」中新增其他欄位，例如：O（組織）、OU（組織單位）或 C（國家/地區）：

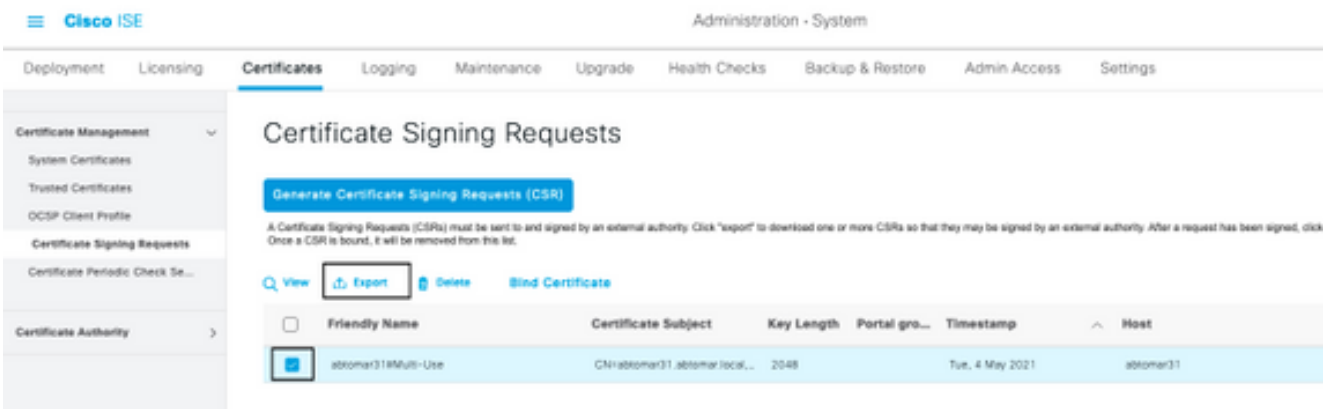


3. **「主體別名 (SAN)」**文字欄位行必須重複輸入 ISE FQDN。如果您想要使用別名或萬用字元憑證，可以新增第二個 SAN 欄位。

4. 按一下**「產生」**，快顯視窗會指出是否已正確完成 CSR 欄位：



5. 若要匯出 CSR，請在左側面板中按一下**「憑證簽署要求」**，選取您的 CSR，然後按一下**「匯出」**：

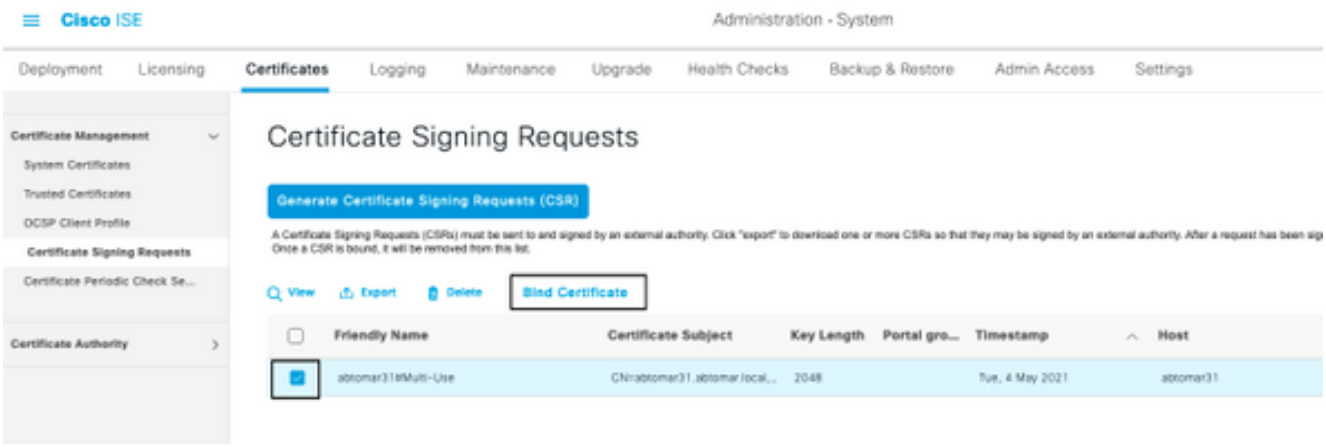


6. CSR儲存在您的電腦上。請將其提交至您的 CA 以供簽署。

安裝憑證

從 CA 收到最終憑證後，您必須將憑證新增至 ISE：

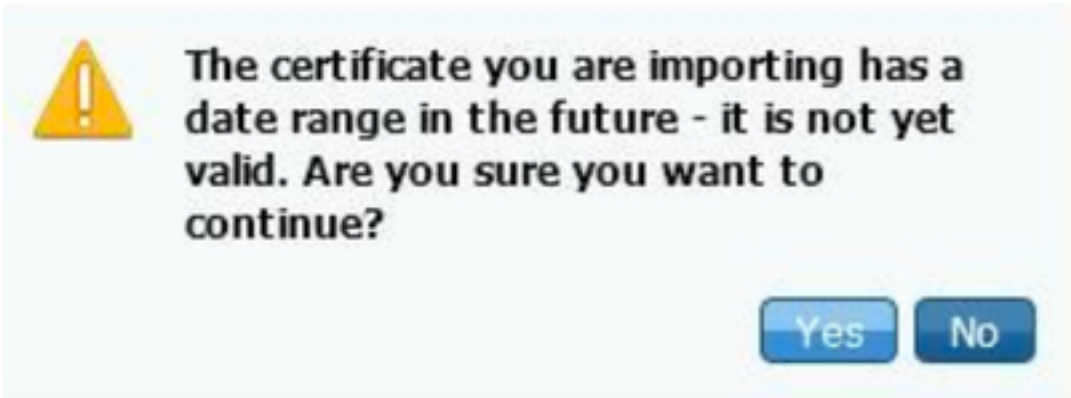
1. 在 ISE 主控台中，導覽至**「系統管理」>「系統」>「憑證」>「憑證簽署要求」**，然後勾選 CRS 的核取方塊，並按一下**「繫結憑證」**：



2. 在**「易記名稱」**文字欄位中輸入簡單且清楚的憑證說明， 然後點擊「提交」。

   附註：請勿在此時啟用 EAP 或系統管理員通訊協定。
3. 在「系統憑證」下，您具有非使用中的新憑證，如下所示：

4. 因為新憑證是在舊憑證到期之前安裝，因此您會看到報告未來日期範圍的錯誤：



5. 按一下「**Yes**」以繼續。此憑證已經安裝但未使用，如綠框所示。

附註：如果您在分散式部署中使用自我簽署憑證，則必須將主要的自我簽署憑證安裝在次要 ISE 伺服器的受信任憑證存放區。 同樣地，次要的自我簽署憑證也必須安裝到主要 ISE 伺服器的受信任憑證存放區。這可讓 ISE 伺服器彼此相互驗證。 否則，部署可能會中斷。如果您從第三方 CA 更新憑證，請驗證根憑證鏈結是否已變更，並據此更新 ISE 中的受信任憑證存放區。在這兩種情況下，確保ISE節點、終端控制系統和請求方能夠驗證根證書鏈。

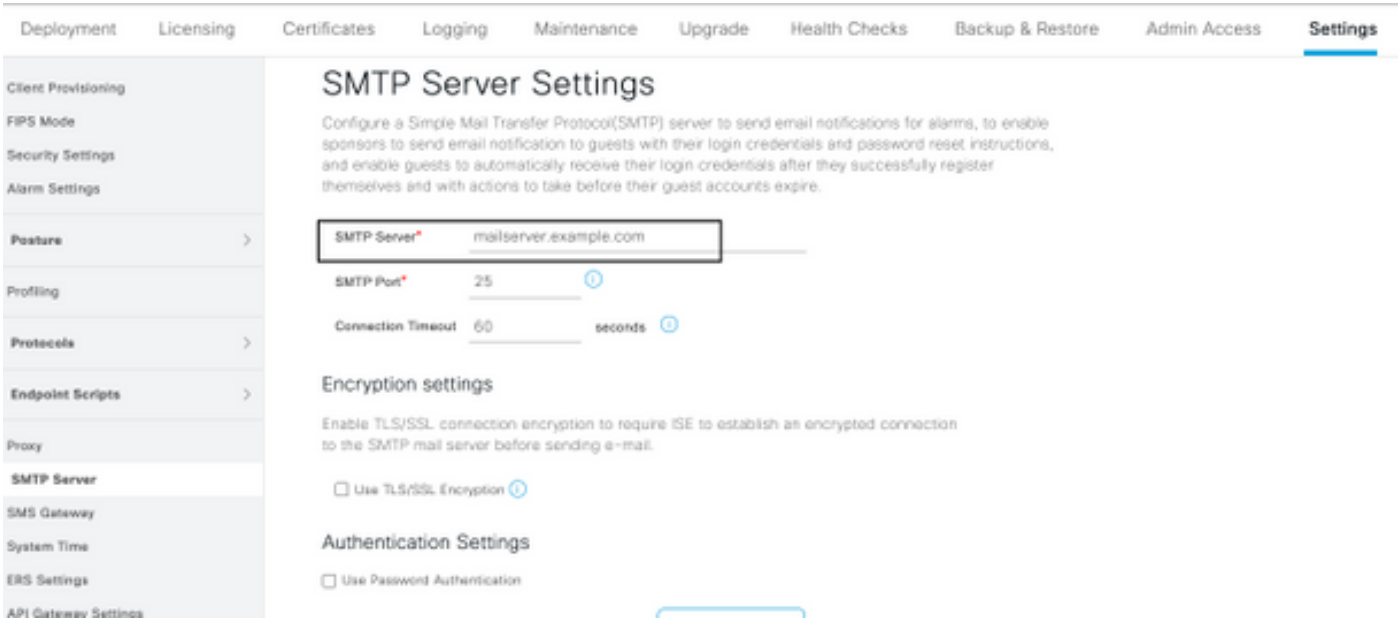
設定警示系統

Cisco ISE 會在距離本機憑證到期日期不到 90 天時通知您。此提前通知可協助您避免憑證到期、規劃憑證變更，以及防止或有效減少停機時間。

通知會以各種方式出現：

- 彩色到期狀態圖示會出現在「本機憑證」頁面上。
- 到期訊息會出現在 Cisco ISE 系統診斷報告中。
- 系統會在 90 天和 60 天時產生到期警示，並在到期之前的最後 30 天每日產生警示。

設定 ISE 以取得到期警示的電子郵件通知。在 ISE 主控台中，導覽至**「系統管理」>「系統」>「設定」>「SMTP 伺服器」**，找出簡易郵件傳輸通訊協定 (SMTP) 伺服器，然後定義另一個伺服器設定，以便傳送警示的電子郵件通知：

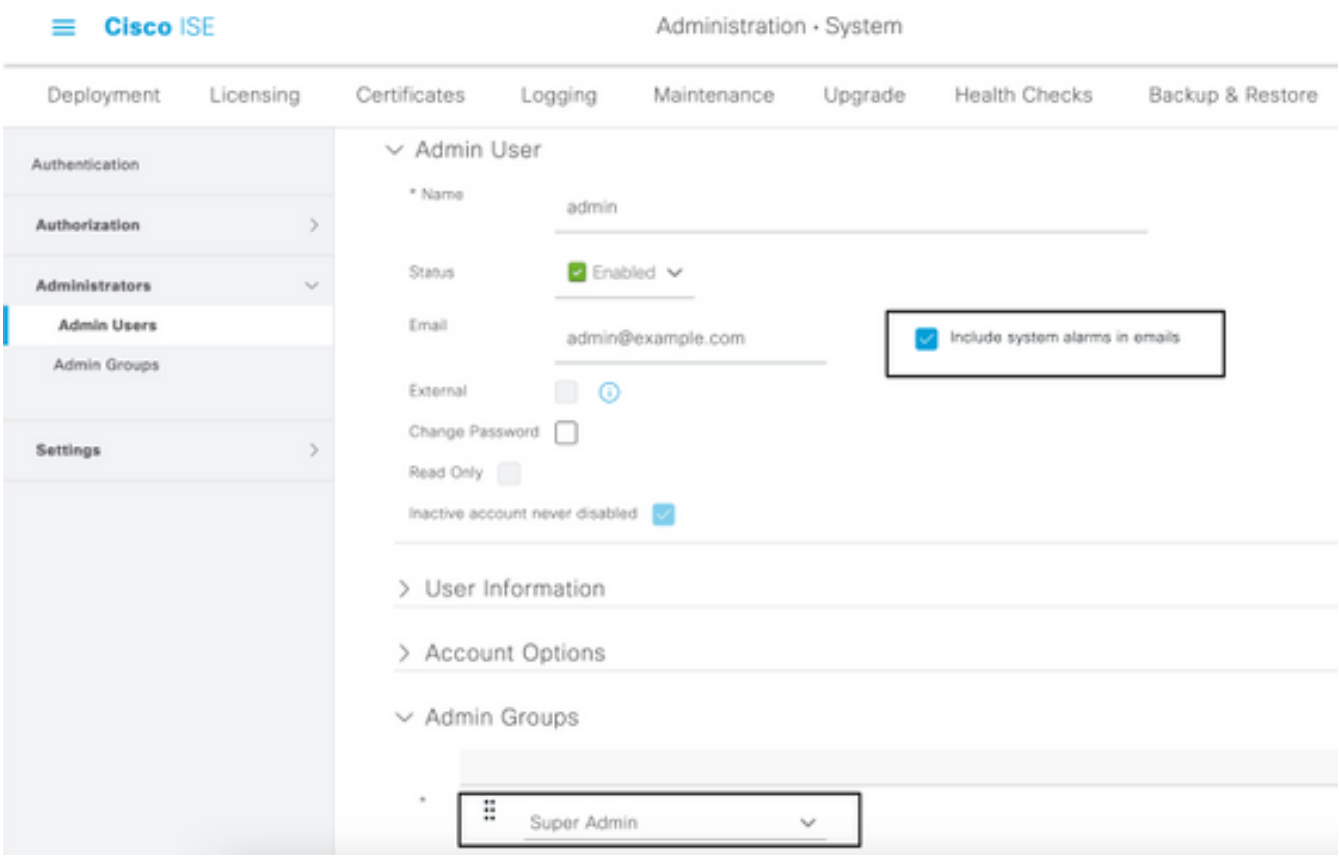


您可以透過兩種方式設定通知：

- 使用系統管理員存取權以通知系統管理員：

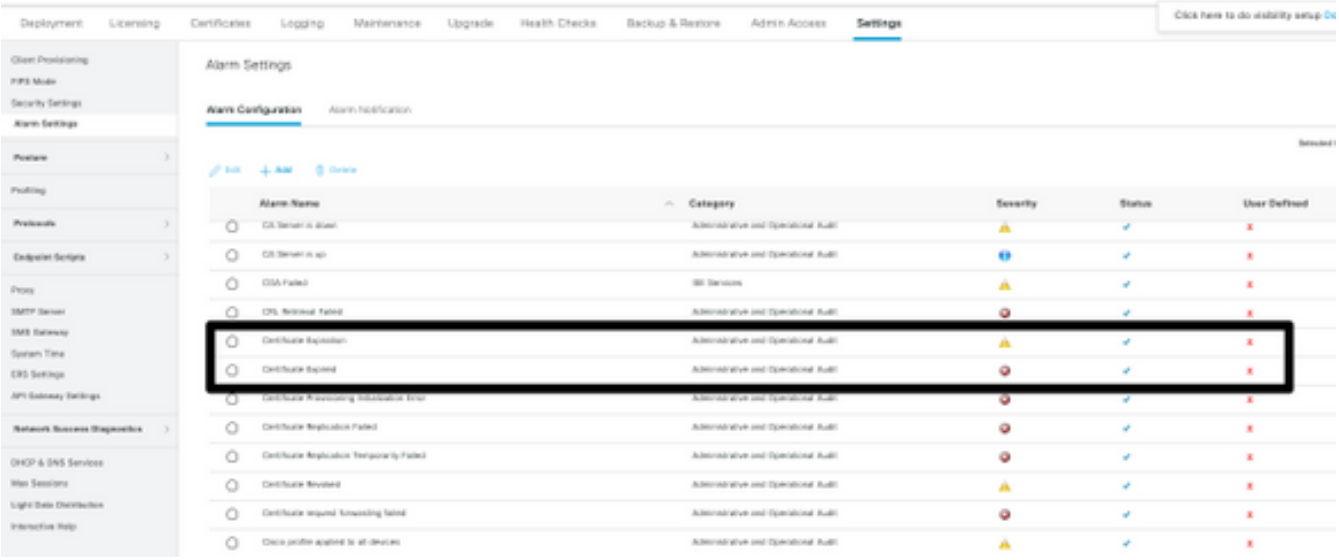
  導覽至**「系統管理」>「系統」>**「系統管理員存取權」>「系統管理員」>「系統管理員使用者」。

  為需要收到警示通知的系統管理員使用者勾選**「在電子郵件中包含系統警示」**核取方塊。警示通知寄件者的電子郵件地址已硬式編碼為 ise@*hostname*。

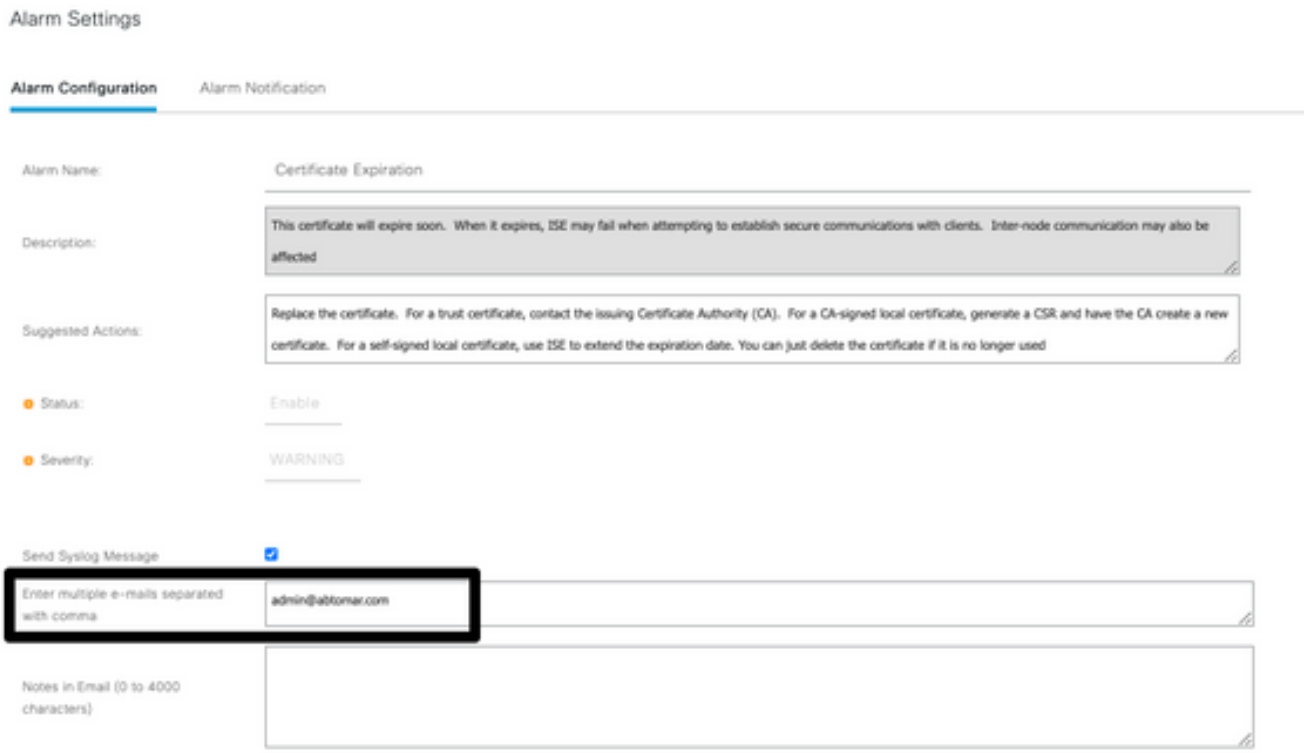


- 設定 ISE 警示設定以通知使用者：

  導覽至**「系統管理」>「系統」>「設定」>「警示設定」>「警示組態」**，如下圖所示。



附註：如果您想要避免某個類別的警示，請停用該類別的狀態。選取「憑證到期」，接著按一下**「警示通知」**，輸入要通知的使用者電子郵件地址，然後儲存變更。更改可能需要15分鐘才能生效。

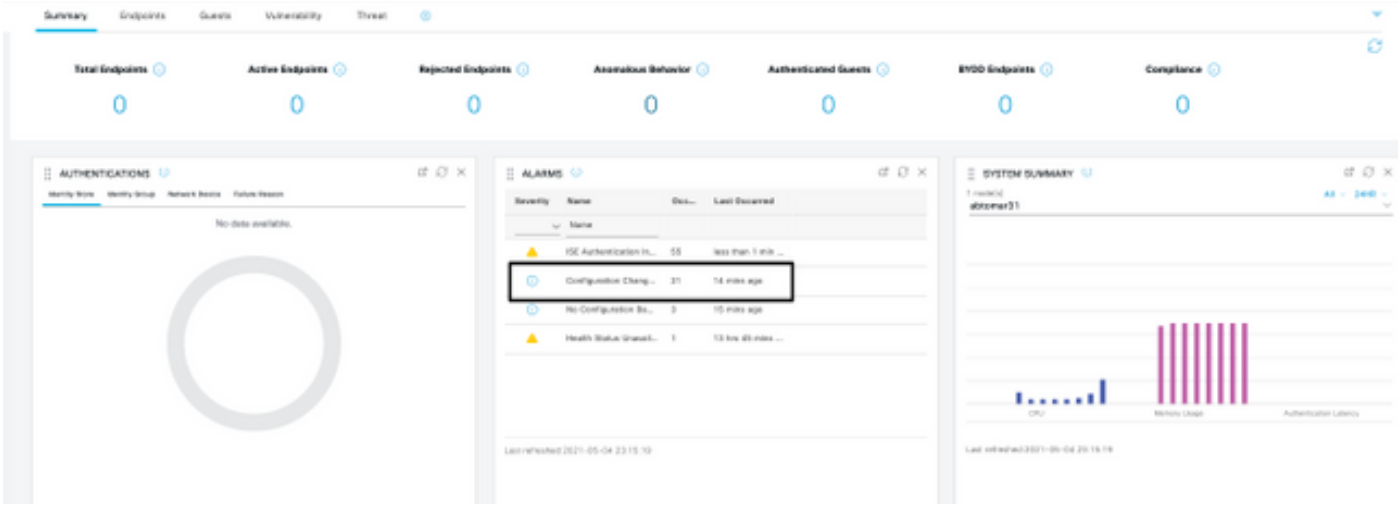


驗證

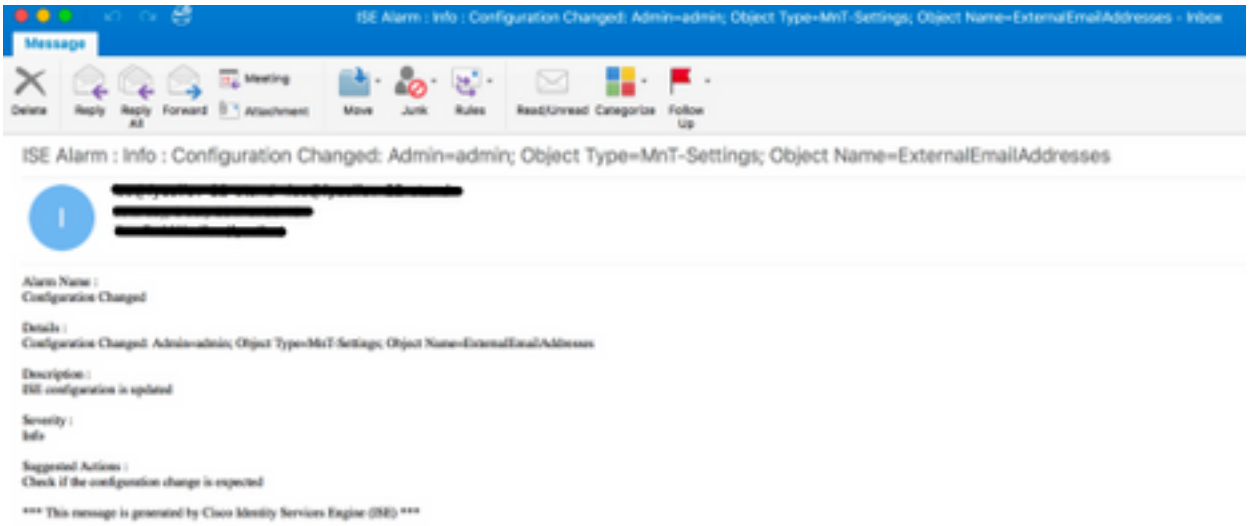
使用本節內容，確認您的組態是否正常運作。

驗證警示系統

驗證警示系統是否可以正常運作。在此範例中，組態變更會產生嚴重性等級為「資訊」的警示。（「訊息」警示的嚴重性最低，而憑證到期則會產生更高的「警告」嚴重性等級。）



這是 ISE 傳送之電子郵件警示的範例：

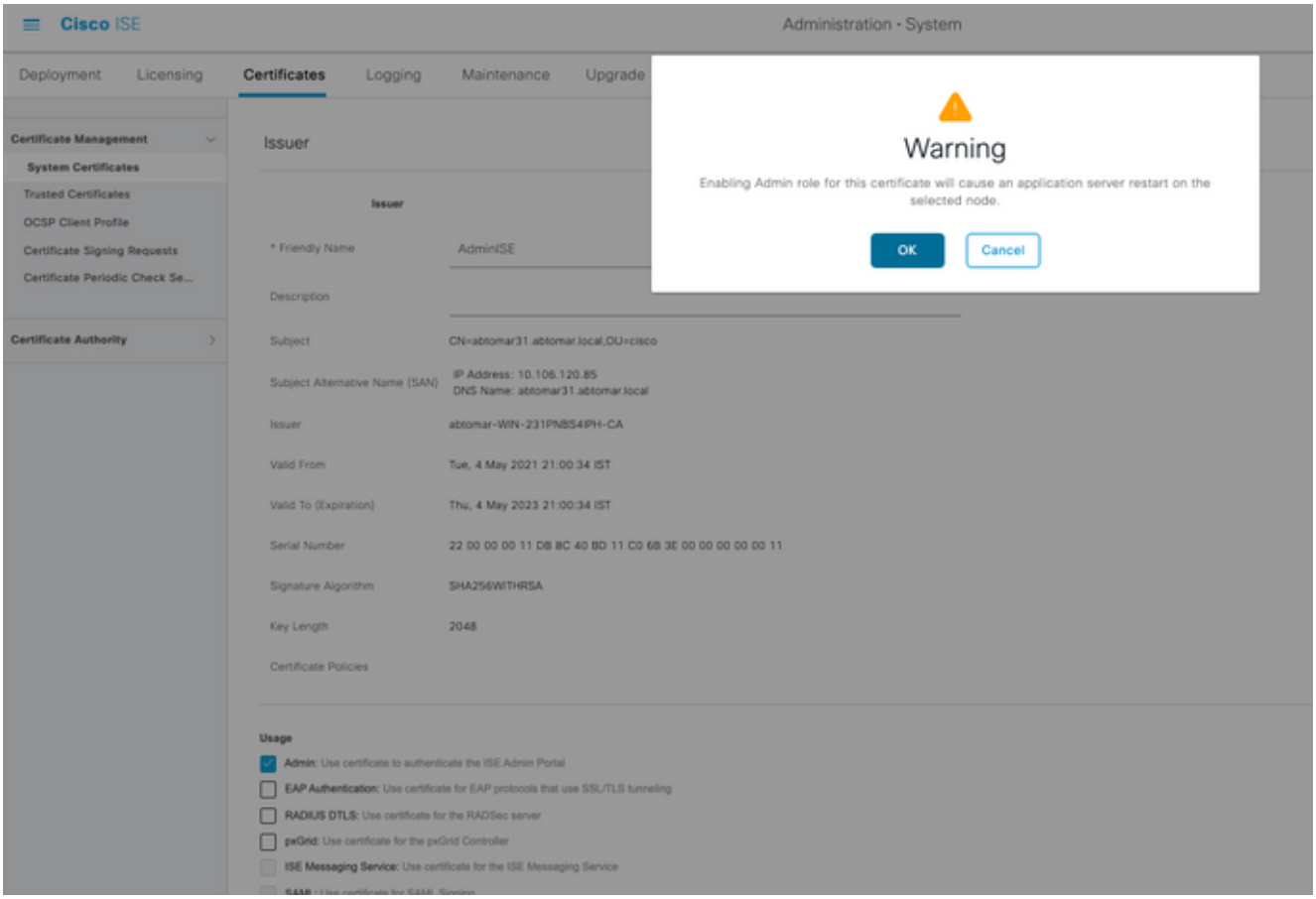


驗證憑證變更

以下過程介紹了如何驗證證書是否正確安裝，以及如何更改EAP和/或Admin角色：

1. 在 ISE 主控台上，導覽至**「系統管理」>「憑證」>「系統憑證」**，然後選取新的憑證以檢視詳細資料。

   注意：如果啟用「系統管理員使用情況」，ISE 服務將會重新啟動，進而導致伺服器停機時間。



2. 若要驗證 ISE 伺服器的憑證狀態，請在 CLI 中輸入此命令：

```
CLI:> show application status ise
```

3. 當所有服務均處於作用中狀態時，請嘗試以系統管理員身分登入。

4. 對於分散式部署方案，請導航到**管理>系統>部署。**驗證節點是否具有綠色圖示。將游標置於圖示上，驗證圖例是否顯示「已連線」。

5. 檢查一般使用者驗證是否成功。為此，請導航至**操作> RADIUS >即時日誌。** 您可以找到特定的身份驗證嘗試，並驗證這些嘗試是否已成功進行身份驗證。

驗證憑證

如果想要從外部檢查憑證，可您以使用內嵌的 Microsoft Windows 工具或 OpenSSL 工具組。

OpenSSL 是安全通訊端層 (SSL) 通訊協定的開放原始碼實作。如果憑證使用您自己的私人 CA，則您必須將 CA 根憑證置於本機電腦上並使用 OpenSSL 選項 *-CApath*。如果您有中繼 CA，也必須將其置於相同的目錄中。

若要取得有關憑證的一般資訊並驗證憑證，請使用：

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

使用OpenSSL工具包轉換憑證也可能很實用：

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

疑難排解

目前尚無適用於此組態的具體診斷資訊。

結論

由於您可以在 ISE 處於作用中狀態前於 ISE 上安裝新的憑證，因此思科建議您在舊憑證到期之前安裝新的憑證。在舊憑證到期日期與新憑證開始日期之間的重疊期間，您將有時間更新憑證並規劃憑證的安裝作業，而且幾乎沒有停機時間。新憑證進入有效日期範圍後，請啟用 EAP 和/或系統管理員。請記住，如果您啟用「系統管理員使用情況」，服務將會重新啟動。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。