ISE SAML證書

目錄

簡介

本檔案介紹思科身分識別服務引擎(ISE)中的安全宣告標籤語言(SAML)系統憑證。 它涵蓋SAML證書的目的、如何執行續訂，最後回答常見問題。它涵蓋從2.4版到3.0版的ISE，但是，它應該與其他ISE 2.x和3.x軟體版本相似或相同，除非另有說明。

必要條件

需求

思科建議您瞭解以下主題：

1. Cisco ISE
2. 用於描述不同型別ISE和身份驗證、授權和記帳(AAA)部署的術語
3. RADIUS協定和AAA基礎知識
4. SAML協定
5. SSL/TLS和x509證書
6. 公開金鑰基礎架構(PKI)基礎知識

採用元件

本檔案中的資訊是根據思科身分識別服務引擎(ISE)版本2.4 - 3.0

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或設定可能造成的影響。

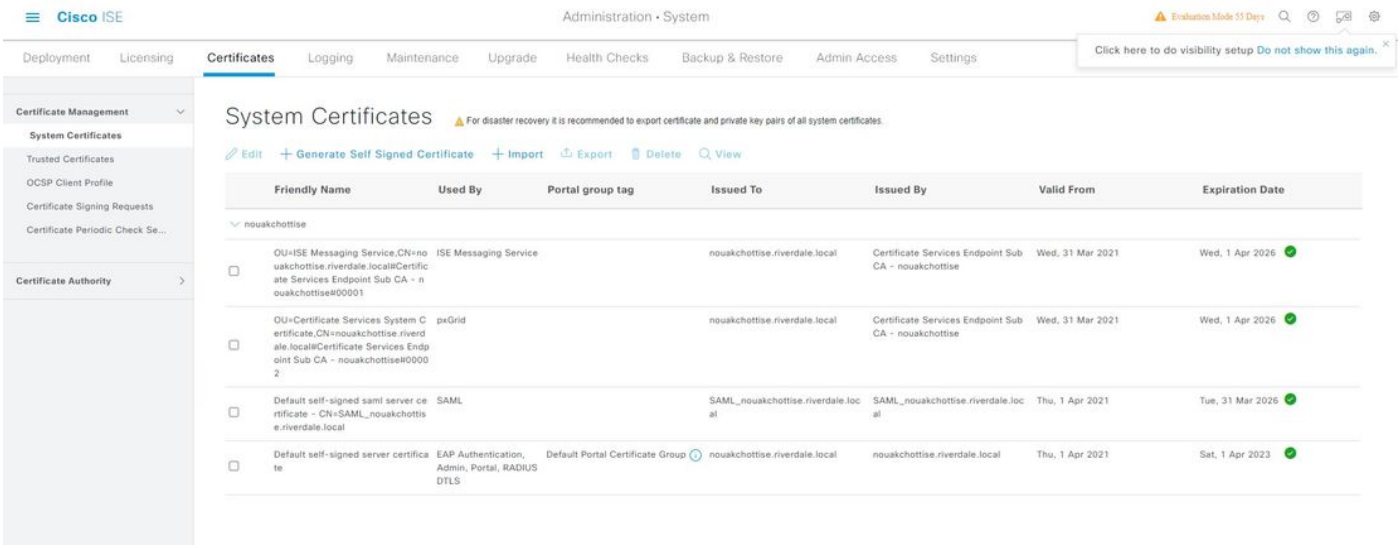
ISE中的SSL證書

安全套接字層(SSL)證書是標識個人、伺服器或任何其他數字實體，並將該實體與公鑰關聯的數字檔

案。自簽名證書由其建立者簽名。證書可以由外部證書頒發機構(CA)（通常是公司自己的CA伺服器或已知的CA供應商）自簽名或數位簽章。CA簽署的數位證書被視為行業標準，比自簽署證書更安全。

Cisco ISE依靠PKI來提供與終端和管理員、ISE與其他伺服器/服務之間以及多節點部署中的Cisco ISE節點之間的安全通訊。PKI依靠X.509數位證書來傳輸用於加密和解密消息的公鑰，以及驗證代表使用者和裝置的其他證書的真實性。通過思科ISE管理門戶，您可以管理這些X.509證書。

在ISE中，系統證書是標識思科ISE節點到其他應用（如終端、其他伺服器等）的伺服器證書。 每個思科ISE節點都有自己的系統證書與相應的私鑰一起儲存在節點上。每個系統證書都可以對映到「角色」，這些角色指示證書的用途，如下圖所示。

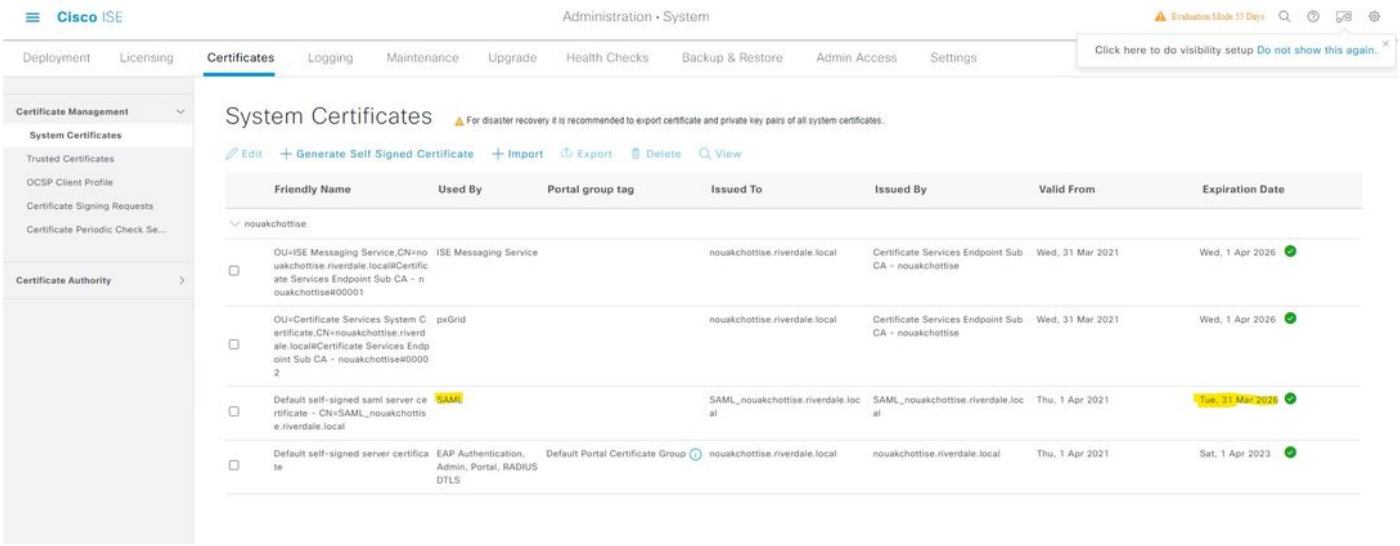


ISE 3.0系統證書

本文檔的範圍僅適用於SAML證書。有關ISE中的其他證書以及有關ISE中的SSL證書的更多資訊，請參閱本文文檔：ISE中的TLS/SSL證書 — 思科

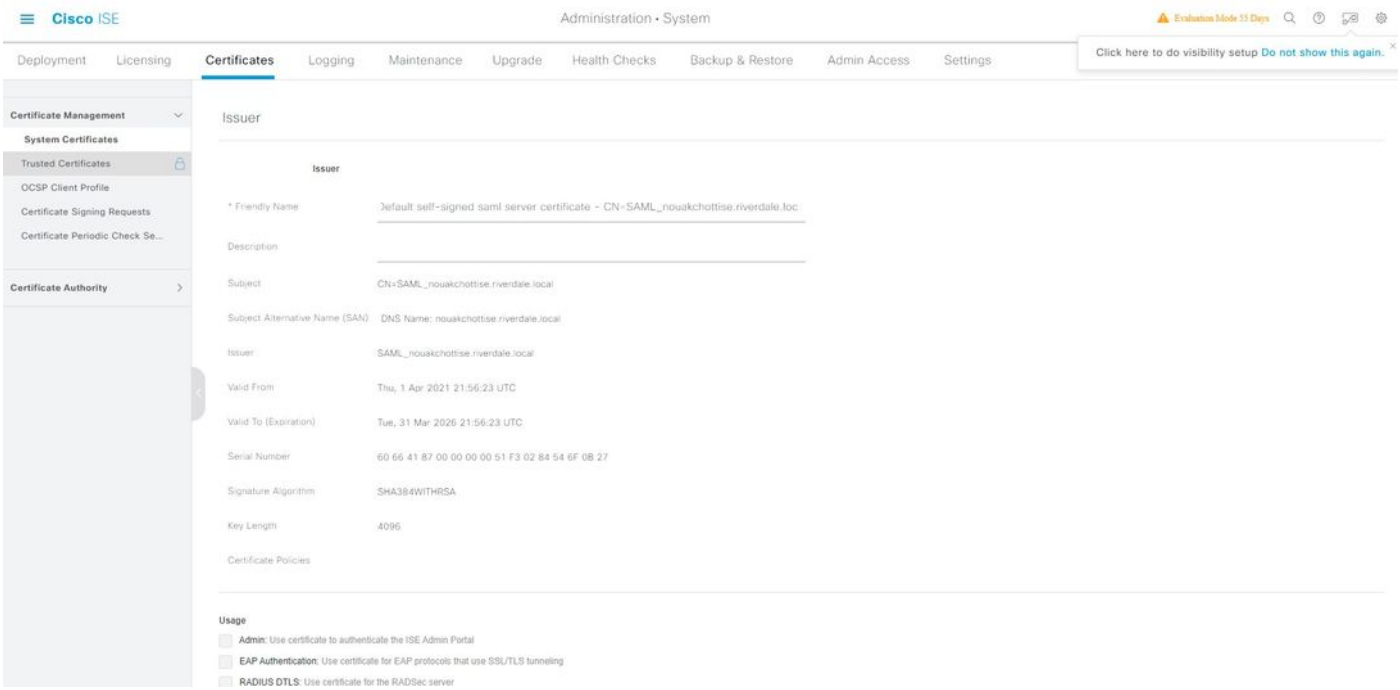
ISE中的SAML證書

ISE中的SAML證書通過查詢使用欄位下具有SAML條目的系統證書來確定。此證書將用於與SAML身份提供程式(IdP)通訊，如驗證正在從正確的IdP接收SAML響應，以及確保與IdP的通訊安全。請注意，指定用於SAML使用的證書不能用於任何其他服務，如管理、EAP身份驗證等。



ISE首次安裝自簽名的SAML伺服器證書具有以下屬性：

金鑰大小：2048
有效性：一年
金鑰用法：數位簽章（簽名）
擴展金鑰用法：TLS Web伺服器身份驗證(1.3.6.1.5.5.7.3.1)



> **附註**：建議不要將包含2.5.29.37.0值的證書用於「擴展金鑰用法」屬性中的「任何目的」對象識別符號。如果在「擴展金鑰用法」屬性中使用的「任意用途」對象識別符號包含值2.5.29.37.0的證書，則該證書將被視為無效，並顯示以下錯誤消息："source=local ; type=fatal ; message="unsupported certificate"。

ISE管理員需要在到期之前續訂此自簽名SAML證書，即使SAML功能未主動使用。

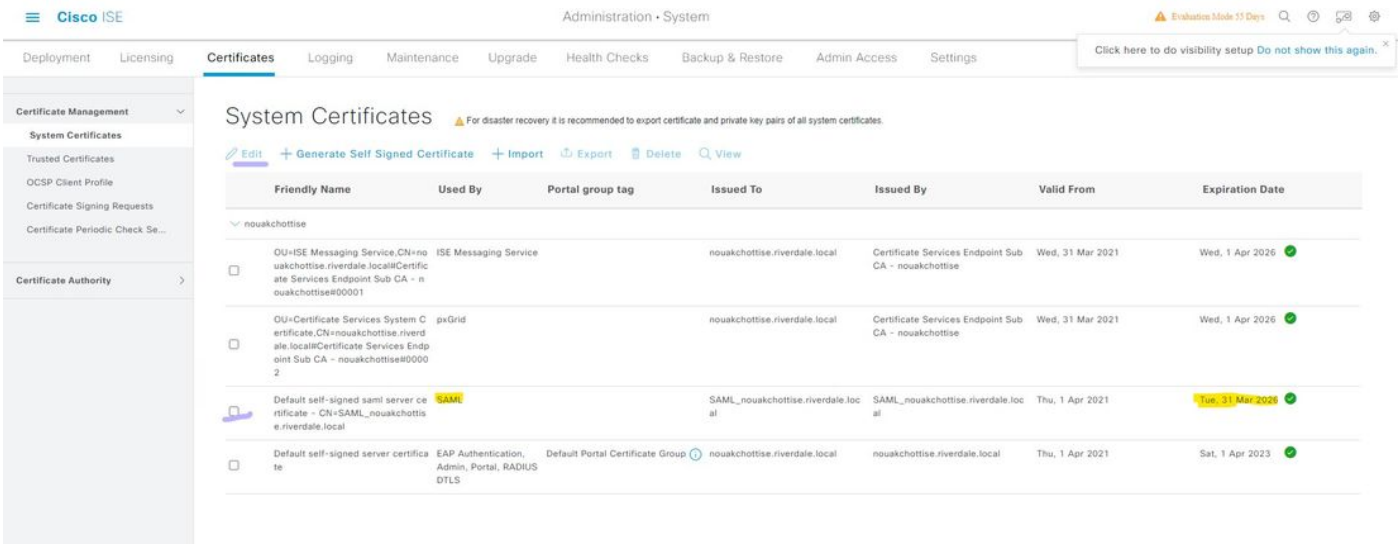
在ISE中續訂自簽名SAML證書

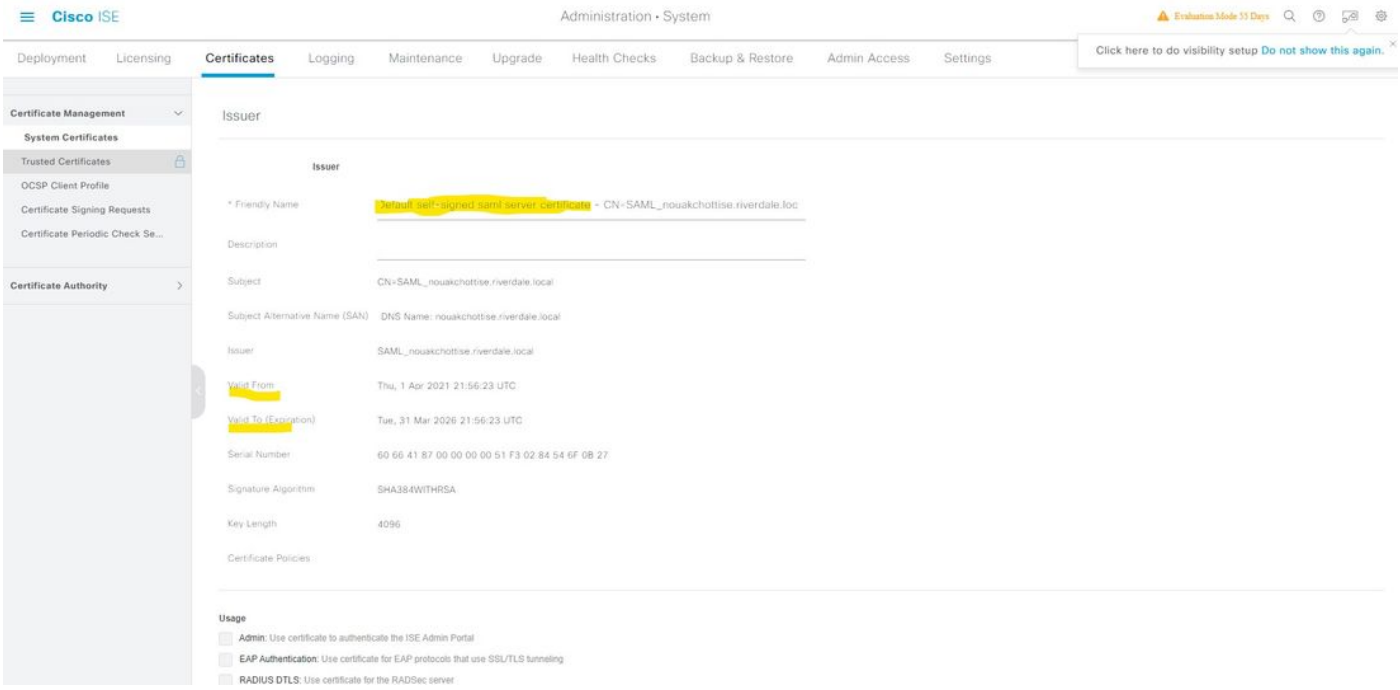
使用者面臨的一個常見問題是，他們的SAML證書最終將過期，ISE會使用以下消息提醒他們：

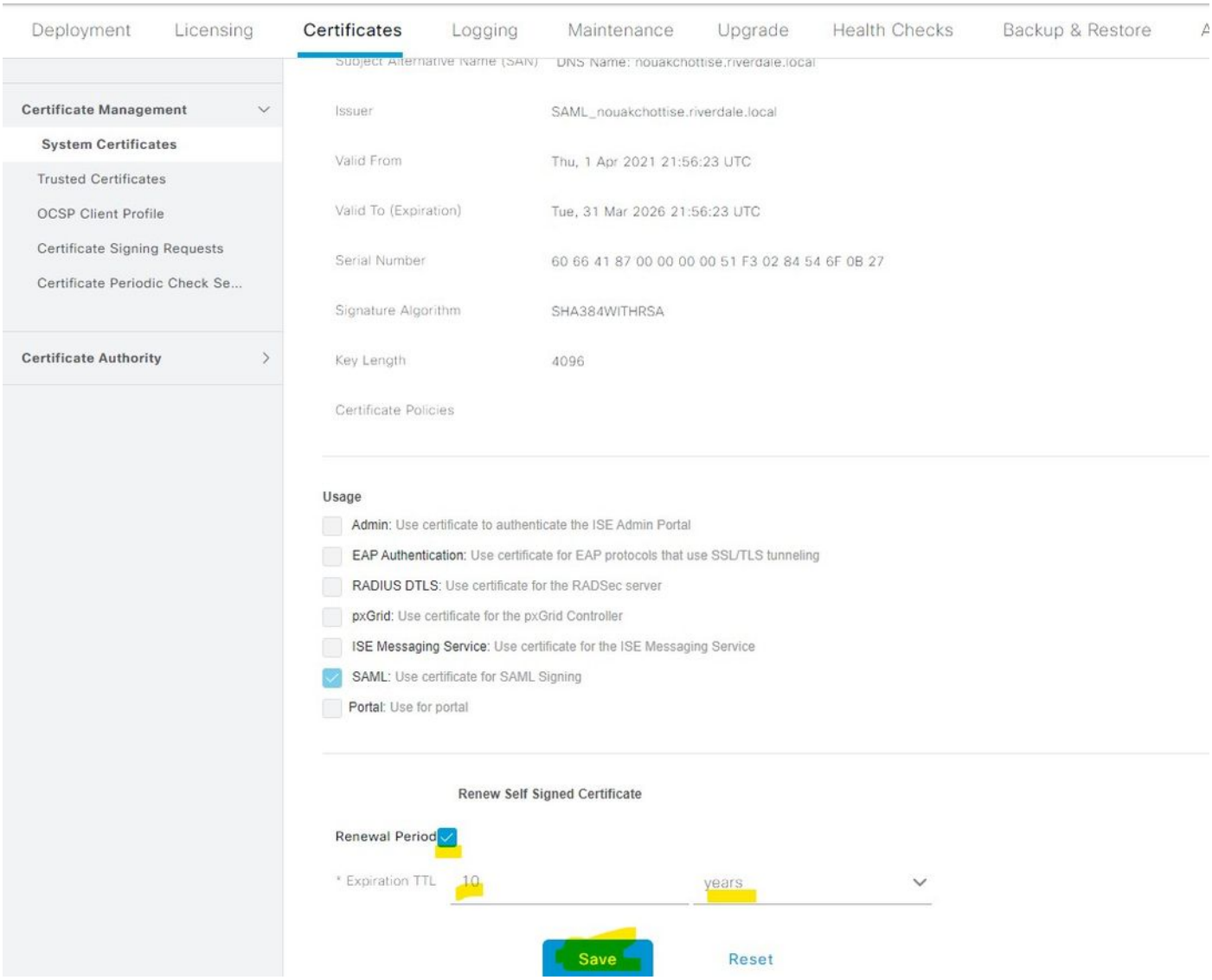
```
Alarm Name :
Certificate Expiration

Details :
Trust certificate 'Default self-signed server certificate' will expire in 60 days :
Server=Kolkata-ISE-001

Description :
This certificate will expire soon. When it expires, ISE may fail when attempting to establish
secure communications with clients. Inter-node communication may also be affected

Severity :
Warning

Suggested Actions :
```

Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use ISE to extend the expiration date. You can just delete the certificate if it is no longer used.

對於自簽名的伺服器證書，可以續訂證書，只需勾選續訂週期即可，還可以保留5-10年，如下圖所示。







事實上，ISE部署節點未使用的所有自簽名證書都可以續訂10年；這可確保不會收到您未使用的服務證書的任何過期通知。10年是ISE自簽名證書允許的最大壽命，通常應該足夠長。更新ISE上的任何系統證書不會觸發服務重新啟動，只要它不是指定為「管理」使用。

結論

對於未使用的任何過期ISE系統證書（自簽名和CA簽名），可以將其替換、刪除或續訂，建議在執行ISE升級之前不要在ISE上保留任何過期證書（系統或受信任）。

相關資訊

- **ISE 3.0管理證書：**[思科身份服務引擎管理員指南3.0版 — 基本設定[思科身份服務引擎] — 思科
- **ISE中的SSL證書：**[ISE中的TLS/SSL證書 — 思科
- [技術支援與文件 - Cisco Systems]