

思科安全管理員3.0.1:生成用於安裝後伺服器的自簽名證書

目錄

- [簡介](#)
- [必要條件](#)
- [需求](#)
- [採用元件](#)
- [慣例](#)
- [建立自簽名證書](#)
- [相關資訊](#)

簡介

本文檔介紹如何為伺服器上的根受信任證書清單建立自簽名證書。

必要條件

需求

建立證書之前，請確保完成[安裝後伺服器任務](#)的[要立即完成的伺服器任務](#)部分中的步驟1、2和3。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

建立自簽名證書

[Server Tasks To Complete](#)的第4步介紹了如何在伺服器中設定自簽名證書。以下步驟指導您如何通過自簽名證書通過HTTPS訪問思科安全管理器伺服器。

1. 系統將顯示Security Alert對話方塊，提示您接受、拒絕或驗證自簽名證書。每次連線到伺服器時都會出現此對話方塊。
2. 按一下**Yes**以接受該特定作業階段的自簽憑證。為了避免每次通過HTTPS連線到思科安全管理器時出現此提示，請按一下**View Certificate**而不是Yes。
3. 此時會出現一個新視窗，顯示「Issued to」 = 「issued by」。這表示它是一個自簽名的證書

- 。
4. 按一下「**Install Certificate**」以安裝自簽名的憑證，當您連線到思科安全管理器時，系統不再提示安裝自簽名的憑證。

註：安裝自簽名證書後，安全警報對話方塊不再顯示提示。可以選擇將自簽名證書新增到根信任證書清單中。

相關資訊

- [思科資安管理者](#)
- [技術支援與文件 - Cisco Systems](#)