管理安全性證書

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/active-iq-unified-manager-918/config/task_view_https_security_certificate_ocf.html on November 13, 2026. Always check docs.netapp.com for the latest.

目錄

管理安全性證書 . . . 1
在 Active IQ Unified Manager 中檢視 HTTPS 安全性憑證 . . . 1
在 Active IQ Unified Manager 中下載 HTTPS 憑證簽署要求 . . . 1
在 Active IQ Unified Manager 中安裝由 CA 簽署的 HTTPS 憑證 . . . 1
憑證鏈範例 . . . 2
了解 Active IQ Unified Manager Unified Manager 中如何使用外部工具產生 HTTPS 憑證 . . . 2
用於載入包含 EC 金鑰對的憑證的格式 . . . 3
用於載入包含 RSA 金鑰對的憑證的格式 . . . 3
上傳外部產生的憑證時的檢查 . . . 4
憑證管理頁面描述 . . . 5
了解 Active IQ Unified Manager 中的 HTTPS 憑證頁面 . . . 5
在 Active IQ Unified Manager 中重新產生 HTTPS 憑證對話方塊 . . . 5

管理安全性證書

在 **Active IQ Unified Manager** 中檢視 **HTTPS** 安全性憑證

您可以將 HTTPS 憑證詳細資訊與瀏覽器中擷取的憑證進行比較，以確保瀏覽器與 Unified Manager 的加密連線沒有被攔截。

開始之前

您必須擁有操作員、應用程式管理員或儲存管理員角色。

檢視憑證可讓您驗證重新產生的憑證內容，或檢視可從中存取 Unified Manager 的主題備用名稱（SAN）。

步驟

1. 在左側導覽窗格中，按一下 一般 > **HTTPS** 憑證。

   HTTPS 憑證顯示在頁面頂部

如果您需要檢視比 HTTPS 憑證頁面上所顯示更詳細的安全性憑證資訊，您可以在瀏覽器中檢視連線憑證。

在 **Active IQ Unified Manager** 中下載 **HTTPS** 憑證簽署要求

您可以下載目前 HTTPS 安全性憑證的認證簽署要求，以便將該檔案提供給憑證授權單位（CA）進行簽署。由 CA 簽署的憑證有助於防止中間人攻擊，並提供比自簽名憑證更好的安全性保護。

開始之前

您必須擁有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下 一般 > **HTTPS** 憑證。
2. 按一下 下載 **HTTPS** 憑證簽章請求。
3. 儲存 `<hostname>.csr`檔案。

您可以將檔案提供給憑證授權單位進行簽署，然後安裝已簽署的憑證。

在 **Active IQ Unified Manager** 中安裝由 **CA** 簽署的 **HTTPS** 憑證

在憑證授權單位（CA）簽署並傳回憑證後，您可以上傳並安裝安全性憑證。您上傳並安裝的檔案必須是現有自簽憑證的簽署版本。CA 簽署的憑證有助於防止中間人攻擊，並提供比自簽憑證更好的安全性保護。

*什麼。開始之前

您必須完成以下操作：

- 已下載憑證簽署要求檔案，並由憑證授權單位簽署
- 已將憑證鏈儲存為 PEM 格式
- 包含憑證鏈中的所有憑證，從 Unified Manager 伺服器憑證到根目錄簽署憑證，包括任何存在的中繼憑證

您必須擁有應用程式管理員角色。

如果已建立 CSR 的憑證有效期超過 397 天，則 CA 在簽署並傳回憑證之前，會將憑證有效期縮短至 397 天

步驟

1. 在左側導覽窗格中，按一下 一般 > **HTTPS** 憑證。
2. 按一下 安裝 **HTTPS** 憑證。
3. 在顯示的對話方塊中，按一下 選擇檔案..... 以找到要上傳的檔案。
4. 選擇檔案，然後按一下 安裝 來安裝檔案。

   如需相關資訊，請參閱 "安裝使用外部工具產生的 HTTPS 憑證"。

憑證鏈範例

以下範例顯示憑證鏈檔案的可能格式：

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

了解 **Active IQ Unified Manager Unified Manager** 中如何使用外部工具產生 **HTTPS** 憑證

您可以安裝自我簽署或 CA 簽署的憑證，這些憑證是使用 OpenSSL、BoringSSL、LetsEncrypt 等外部工具所產生。

您應該將私鑰與憑證鏈一起載入，因為這些憑證是外部產生的公私鑰對。允許使用的金鑰對演算法為 “RSA” 和 “EC”。安裝 **HTTPS** 憑證 選項位於「一般」區段下的「HTTPS 憑證」頁面中。您上傳的檔案應採用下列輸入格式。

1. 屬於 Active IQ Unified Manager 主機的伺服器的私鑰
2. 與私鑰匹配的伺服器憑證
3. 用於簽署上述憑證的 CA 憑證（反向排列直至根目錄 CA）

用於載入包含 **EC** 金鑰對的憑證的格式

允許的曲線為「`prime256v1`」和「`secp384r1`」。包含外部產生 EC 對的憑證範例：

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

用於載入包含 **RSA** 金鑰對的憑證的格式

屬於主機憑證的 RSA 金鑰對允許的金鑰長度為 2048、3072 和 4096。具有外部產生之 **RSA** 金鑰對 的憑證：

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
```

```
-----END CERTIFICATE-----
```

憑證上傳後，您應該重新啟動 Active IQ Unified Manager 執行個體，以使變更生效。

上傳外部產生的憑證時的檢查

系統在上傳使用外部工具產生的憑證時會進行檢查。如果任何一項檢查失敗，則憑證將被拒絕。此外，系統也會對產品內部從 CSR 產生的憑證以及使用外部工具產生的憑證進行驗證。

- 輸入中的私鑰會根據輸入中的主機憑證進行驗證。
- 主機憑證中的通用名稱（CN）會與主機的 FQDN 進行比對。
- 主機憑證的通用名稱（CN）不應為空，也不應設定為 localhost。
- 憑證的有效期限起始日期不應在未來，有效期限終止日期也不應在過去。
- 如果存在中繼 CA 或 CA，憑證的有效起始日期不應在未來，且有效到期日期不應在過去。

輸入的私鑰不應加密。如果存在任何加密的私鑰，系統將拒絕該私鑰。

範例 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

範例 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

範例 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

如果憑證安裝失敗，請參閱知識庫（KB）文章：https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager 無法安裝外部產生的憑證"^]

憑證管理頁面描述

了解 **Active IQ Unified Manager** 中的 **HTTPS** 憑證頁面

HTTPS 憑證頁面可讓您檢視目前安全性憑證、下載憑證簽署要求、產生新的自簽名 HTTPS 憑證或安裝新的 HTTPS 憑證。

如果您尚未產生新的自簽署 HTTPS 憑證，則此頁面上顯示的憑證是安裝期間所產生的憑證。

命令按鈕

命令按鈕可用於執行以下操作：

- 下載 **HTTPS** 憑證簽署請求

  下載目前已安裝的 HTTPS 憑證的認證請求。瀏覽器會提示您儲存 <hostname>.csr 檔案，以便您可以將該檔案提供給憑證授權單位進行簽署。

- 安裝 **HTTPS** 憑證

  允許您在憑證授權單位簽署並返回安全性憑證後上傳並安裝該憑證。新憑證將在您重新啟動管理伺服器後生效。

- 重新產生 **HTTPS** 憑證

  允許您產生新的自簽名 HTTPS 憑證，以取代目前的安全性憑證。重新啟動 Unified Manager 後，新憑證將生效。

在 **Active IQ Unified Manager** 中重新產生 **HTTPS** 憑證對話方塊

「重新產生 HTTPS 憑證」對話方塊可讓您自訂安全性資訊，然後使用該資訊產生新的 HTTPS 憑證。

此頁面顯示目前的憑證資訊。

"\`使用目前憑證屬性重新產生\`" 和 "\`更新目前憑證屬性\`" 選項可讓您使用目前資訊重新產生憑證，或使用新資訊產生憑證。

- 通用名稱

  必填。您希望安全的完整網域名稱（FQDN）。

  在 Unified Manager 高可用度組態中，使用虛擬 IP 位址。

- 電子郵件

  選用。用於聯絡貴組織的電子郵件地址；通常是憑證系統管理員或 IT 部門的電子郵件地址。

- 公司

  選填。通常為貴公司的法定名稱。

- 部門

  選用。貴公司的部門名稱。

- 城市

  選用。貴公司所在的城市。

- 狀態

  選用。貴公司所在的州或省份位置，請勿縮寫。

- 國家

  選用。貴公司所在的國家。這通常是該國家的兩個字母 ISO 代碼。

- 別名

  必填。除了現有的 localhost 或其他網路位址之外，可用來存取此伺服器的其他非主要網域名稱。請以逗號分隔每個替代名稱。

  如果您想要從憑證的「備用名稱」欄位移除本機識別資訊，請選取 “排除本機識別資訊（例如 localhost）” 核取方塊。選取此核取方塊後，「備用名稱」欄位將僅使用您在此欄位中輸入的內容。如果留空，則產生的憑證將完全不包含「備用名稱」欄位。

- 金鑰長度（金鑰演算法：**RSA**）

  金鑰演算法設定為 RSA。您可以從下列金鑰長度中選擇：2048 位元、3072 位元或 4096 位元。預設金鑰長度設定為 2048 位元。

- 有效期限

  預設有效期為 397 天。如果您是從舊版本升級而來，則可能會發現先前的憑證有效期未變更。

如需詳細資訊，請參閱 "產生 HTTPS 憑證"。

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。