憑證
SANtricity software

NetApp
March 12, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/e-series-santricity/um-certificates/overview-certificates-um.html on March 12, 2026. Always check docs.netapp.com for the latest.

目錄

憑證 1
憑證總覽 1
什麼是憑證？ 1
如何設定憑證？ 1
概念 1
憑證在 SANtricity Unified Manager 中的工作方式 1
了解 SANtricity Unified Manager 中的憑證術語 2
管理系統使用CA簽署的憑證 3
步驟1：完成CSR檔案 4
步驟2：提交CSR檔案 4
步驟3：匯入管理憑證 5
重設管理憑證 5
使用陣列憑證 6
在 SANtricity Unified Manager 中匯入陣列憑證 6
在 SANtricity Unified Manager 中刪除受信任的憑證 6
解決不受信任的憑證 7
管理憑證 8
檢視憑證 8
在 SANtricity Unified Manager 中匯出憑證 8

憑證

憑證總覽

「憑證管理」可讓您建立憑證簽署要求（CSR）、匯入憑證、以及管理現有的憑證。

什麼是憑證？

_Certificates_是數位檔案、可識別網站和伺服器等線上實體、以便在網際網路上進行安全通訊。憑證有兩種類型：_簽署的憑證_由憑證授權單位（CA）驗證、_自我簽署的憑證_則由實體擁有者（而非第三方）驗證。

深入瞭解：

- "憑證的運作方式"
- "憑證術語"

如何設定憑證？

從「憑證管理」中、您可以設定裝載Unified Manager的管理站台憑證、也可以匯入陣列中控制器的憑證。

深入瞭解：

- "管理系統使用CA簽署的憑證"
- "匯入陣列的憑證"

概念

憑證在 **SANtricity Unified Manager** 中的工作方式

憑證是數位檔案、可識別網站和伺服器等線上實體、以便在網際網路上進行安全通訊。

簽署的憑證

憑證可確保Web通訊只能在指定的伺服器與用戶端之間以加密形式私下傳輸且不會變更。使用Unified Manager、您可以管理主機管理系統上瀏覽器的憑證、以及探索到的儲存陣列中的控制器。

憑證可以由信任的授權單位簽署、也可以自行簽署。「簽署」只是指有人驗證擁有者的身分、並判斷其裝置是否值得信任。儲存陣列會在每個控制器上隨附自動產生的自我簽署憑證。您可以繼續使用自我簽署的憑證、或是取得CA簽署的憑證、以便在控制器與主機系統之間建立更安全的連線。

> 雖然CA簽署的憑證可提供更好的安全保護（例如預防攔截式攻擊）、但如果您的網路規模較大、也需要支付昂貴的費用。相較之下、自我簽署的憑證較不安全、但完全免費。因此、自我簽署的憑證最常用於內部測試環境、而非正式作業環境。

已簽署的憑證會由信任的協力廠商組織之憑證授權單位（CA）驗證。簽署的憑證包括實體擁有者（通常是伺服器或網站）、憑證發行日期和到期日期、實體的有效網域、以及由字母和數字組成的數位簽章等詳細資料。

當您開啟瀏覽器並輸入網址時、系統會在背景執行憑證檢查程序、以判斷您是否要連線至內含有效CA簽署憑證的網站。一般而言、以簽署憑證保護的站台會在位址中包含掛鎖圖示和https指定名稱。如果您嘗試連線至不含CA簽署憑證的網站、瀏覽器會顯示網站不安全的警告。

CA會在應用程式處理期間採取步驟來驗證您的身分。他們可能會傳送電子郵件給您的註冊企業、驗證您的公司地址、並執行HTTP或DNS驗證。應用程式程序完成後、CA會傳送數位檔案給您、以便載入主機管理系統。通常、這些檔案包括信任鏈、如下所示：

- 根-階層頂端是根憑證、其中包含用於簽署其他憑證的私密金鑰。根可識別特定的CA組織。如果您的所有網路裝置都使用相同的CA、則只需要一個根憑證。
- 中級：從根目錄下分出的是中繼憑證。CA會發出一或多個中繼憑證、做為受保護根憑證與伺服器憑證之間的中間人。
- 伺服器：在鏈結底部是伺服器憑證、可識別您的特定實體、例如網站或其他裝置。儲存陣列中的每個控制器都需要個別的伺服器憑證。

自我簽署的憑證

儲存陣列中的每個控制器都包含預先安裝的自我簽署憑證。自我簽署的憑證與CA簽署的憑證類似、只是由實體擁有者（而非第三方）驗證。如同CA簽署的憑證、自我簽署的憑證也包含自己的私密金鑰、同時確保資料經過加密、並透過伺服器與用戶端之間的HTTPS連線傳送。

自我簽署的憑證並非瀏覽器的「信任」。每次您嘗試連線至僅包含自我簽署憑證的網站時、瀏覽器都會顯示警告訊息。您必須按一下警告訊息中的連結、以便繼續前往網站；如此一來、您基本上就會接受自我簽署的憑證。

Unified Manager認證

Unified Manager介面會與主機系統上的Web Services Proxy一起安裝。當您開啟瀏覽器並嘗試連線至Unified Manager時、瀏覽器會檢查數位憑證、以驗證主機是否為信任來源。如果瀏覽器找不到伺服器的CA簽署憑證、則會開啟警告訊息。您可以從這裡繼續前往網站、接受該工作階段的自我簽署憑證。或者、您也可以從CA取得已簽署的數位憑證、因此您不會再看到警告訊息。

控制器的憑證

在Unified Manager工作階段期間、當您嘗試存取沒有CA簽署憑證的控制器時、可能會看到其他安全訊息。在此情況下、您可以永久信任自我簽署的憑證、或是匯入控制器的CA簽署憑證、讓Web服務Proxy伺服器能夠驗證這些控制器傳入的用戶端要求。

了解 **SANtricity Unified Manager** 中的憑證術語

下列條款適用於憑證管理。

期限	說明
CA	憑證授權單位（CA）是信任的實體、可發行稱為數位憑證的電子文件、以確保網際網路安全。這些憑證可識別網站擁有者、以便在用戶端與伺服器之間進行安全連線。
CSR	憑證簽署要求（CSR）是一則訊息、會從申請者傳送至憑證授權單位（CA）。CSR會驗證CA核發憑證所需的資訊。

期限	說明
憑證	憑證可識別站台的擁有者、以確保安全性、防止攻擊者模擬站台。憑證包含網站擁有者的相關資訊、以及認證（簽署）此資訊的信任實體身分。
憑證鏈結	將安全層新增至憑證的檔案階層。一般而言、此鏈包括階層頂端的一個根憑證、一個或多個中繼憑證、以及識別實體的伺服器憑證。
中介憑證	一個或多個中繼憑證會從憑證鏈結的根目錄下分支。CA會發出一或多個中繼憑證、做為受保護根憑證與伺服器憑證之間的中間人。
Keystore	Keystore是主機管理系統上的儲存庫、內含私密金鑰及其對應的公開金鑰和憑證。這些金鑰和憑證可識別您自己的實體、例如控制器。
根憑證	根憑證位於憑證鏈結階層的頂端、其中包含用於簽署其他憑證的私密金鑰。根可識別特定的CA組織。如果您的所有網路裝置都使用相同的CA、則只需要一個根憑證。
簽署的憑證	由憑證授權單位（CA）驗證的憑證。此資料檔案包含私密金鑰、可確保資料以加密形式透過HTTPS連線在伺服器與用戶端之間傳送。此外、已簽署的憑證還包含實體擁有者（通常是伺服器或網站）的詳細資料、以及由字母和數字組成的數位簽章。簽署的憑證使用信任鏈、因此最常用於正式作業環境。也稱為「CA簽署的憑證」或「管理憑證」。
自我簽署的憑證	自行簽署的憑證由實體擁有者驗證。此資料檔案包含私密金鑰、可確保資料以加密形式透過HTTPS連線在伺服器與用戶端之間傳送。其中也包含由字母和數字組成的數位簽名。自我簽署的憑證不會使用與CA簽署憑證相同的信任鏈結、因此最常用於測試環境。也稱為「預先安裝」憑證。
伺服器憑證	伺服器憑證位於憑證鏈結的底部。它會識別您的特定實體、例如網站或其他裝置。儲存系統中的每個控制器都需要個別的伺服器憑證。
信任存放區	信任存放區是一個儲存庫、其中包含來自信任的第三方（例如CA）的憑證。

管理系統使用**CA**簽署的憑證

您可以取得及匯入 CA 簽署的憑證，以安全存取託管 SANtricity Unified Manager 的管理系統。

開始之前

您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。

關於這項工作

使用CA簽署的憑證是三個步驟的程序。

步驟1：完成CSR檔案

您必須先產生憑證簽署要求（CSR）檔案、以識別您的組織和安裝Web服務Proxy和Unified Manager的主機系統。

或者、您也可以使用諸如OpenSSL的工具來產生CSR檔案、然後跳至 步驟2：提交CSR檔案。

步驟

1. 選擇*憑證管理*。
2. 從「管理」索引標籤中、選取*完整的csr*。
3. 輸入下列資訊、然後按一下*下一步*：
   - 組織：貴公司或組織的完整法定名稱。包括尾碼、例如Inc.或Corp.
   - 組織單位（選用）：您組織處理憑證的部門。
   - 城市/地區：您的主機系統或企業所在的城市。
   - 州/地區（選用）：主機系統或企業所在的州或地區。
   - 國家**ISO**代碼：您所在國家/地區的兩位數ISO（國際標準化組織）代碼、例如US。
4. 輸入下列有關安裝Web服務Proxy的主機系統資訊：
   - 一般名稱：安裝Web服務Proxy之主機系統的IP位址或DNS名稱。請確定此位址正確無誤、而且必須完全符合您輸入的內容、才能在瀏覽器中存取Unified Manager。請勿包含http：//或https：//。DNS名稱不能以萬用字元開頭。
   - 備用**IP**位址-如果一般名稱是IP位址、您可以選擇輸入主機系統的任何其他IP位址或別名。對於多個項目、請使用以逗號分隔的格式。
   - 備用**DNS**名稱-如果通用名稱是DNS名稱、請輸入主機系統的任何其他DNS名稱。對於多個項目、請使用以逗號分隔的格式。如果沒有替代DNS名稱、但您在第一個欄位中輸入DNS名稱、請在此處複製該名稱。DNS名稱不能以萬用字元開頭。
5. 確認主機資訊正確無誤。如果不是、當您嘗試匯入CA時、從CA傳回的憑證將會失敗。
6. 單擊*完成*。
7. 前往 步驟2：提交CSR檔案。

步驟2：提交CSR檔案

建立憑證簽署要求（CSR）檔案之後、您會將其傳送至憑證授權單位（CA）、以接收裝載Unified Manager和Web Services Proxy之系統的簽署管理憑證。

E系列系統要求簽署的憑證使用PEm格式（Base64 Ascii編碼）、其中包含下列檔案類型：.pem、.crt、.cer或.key。

步驟

1. 找到下載的CSR檔案。

   下載的資料夾位置取決於您的瀏覽器。

2. 將CSR檔案提交給CA（例如、Verisign或Digiting）、並以PEV格式要求簽署的憑證。

*將CSR檔案提交給CA後、請勿重新產生其他CSR檔案。*每當您產生CSR時、系統會建立私密與公開金鑰配對。公開金鑰是CSR的一部分、而私密金鑰則保留在系統的Keystore中。當您收到簽署的憑證並匯入時、系統會確保私密金鑰和公開金鑰都是原始配對。如果金鑰不符、簽署的憑證將無法運作、您必須向CA要求新的憑證。

3. 當CA傳回簽署的憑證時、請前往 [步驟3：匯入管理憑證]。

步驟3：匯入管理憑證

從憑證授權單位（CA）收到簽署的憑證後、請將憑證匯入安裝Web服務Proxy和Unified Manager介面的主機系統。

開始之前

- 您已從CA收到簽署的憑證。這些檔案包括根憑證、一或多個中繼憑證和伺服器憑證。
- 如果CA提供鏈結的憑證檔案（例如.p7b檔案）、您必須將鏈結的檔案解壓縮至個別檔案：根憑證、一或多個中繼憑證及伺服器憑證。您可以使用Windows「certmgr」公用程式來解壓縮檔案（按一下滑鼠右鍵、然後選取功能表：All Tasks（所有工作）[Export（匯出）]）。建議使用Base 64編碼。匯出完成後、會針對鏈中的每個憑證檔案顯示一個CER.檔案。
- 您已將憑證檔案複製到執行Web服務Proxy的主機系統。

步驟

1. 選擇*憑證管理*。
2. 從「管理」索引標籤中、選取*匯入*。

   隨即開啟一個對話方塊、用於匯入憑證檔案。

3. 按一下*瀏覽*以先選取根和中繼憑證檔案、然後選取伺服器憑證。如果您是從外部工具產生CSR、也必須匯入與CSR一起建立的私密金鑰檔案。

   檔案名稱會顯示在對話方塊中。

4. 按一下*匯入*。

結果

檔案會上傳並驗證。憑證資訊會顯示在「憑證管理」頁面上。

重設管理憑證

您可以將管理憑證還原為原始的原廠自我簽署狀態。

開始之前

您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。

關於這項工作

此工作會從安裝Web服務Proxy和Unified Manager的主機系統刪除目前的管理憑證。重設憑證後、主機系統會恢復使用自我簽署的憑證。

步驟

1. 選取 * 設定 > 憑證 * 。
2. 選擇 **Array Management** 選項卡，然後選擇 **Reset** 。

   隨即開啟「確認重設管理憑證」對話方塊。

3. 在欄位中輸入「重設」、然後按一下「重設」。

   瀏覽器重新整理之後、瀏覽器可能會封鎖對目的地站台的存取、並回報該站台使用HTTP嚴格傳輸安全性。當您切換回自我簽署的憑證時、就會出現這種情況。若要清除封鎖目的地存取的條件、您必須從瀏覽器清除瀏覽資料。

結果

系統會從伺服器恢復使用自我簽署的憑證。因此、系統會提示使用者手動接受其工作階段的自我簽署憑證。

使用陣列憑證

在 **SANtricity Unified Manager** 中匯入陣列憑證

如有必要、您可以匯入儲存陣列的憑證、以便使用裝載SANtricity 了VMware Unified Manager的系統進行驗證。憑證可以由憑證授權單位（CA）簽署、也可以自行簽署。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- 如果您要匯入信任的憑證、則必須使用System Manager匯入儲存陣列控制器的憑證。

步驟

1. 選擇*憑證管理*。
2. 選取*信任的*索引標籤。

   此頁面顯示針對儲存陣列所報告的所有憑證。

3. 選取功能表：匯入[憑證]以匯入CA憑證、或選取功能表：匯入[自我簽署的儲存陣列憑證]以匯入自我簽署的憑證。

   若要限制檢視、您可以使用*顯示…*篩選的憑證欄位、或按一下其中一個欄位標題來排序憑證列。

4. 在對話方塊中、選取憑證、然後按一下*匯入*。

   憑證已上傳並驗證。

在 **SANtricity Unified Manager** 中刪除受信任的憑證

您可以刪除一或多個不再需要的憑證、例如過期的憑證。

開始之前

請先匯入新的憑證、再刪除舊的憑證。

請注意、刪除根或中繼憑證可能會影響多個儲存陣列、因為這些陣列可以共用相同的憑證檔案。

步驟

1. 選擇*憑證管理*。
2. 選取*信任的*索引標籤。
3. 在表格中選取一或多個憑證、然後按一下*刪除*。

   *刪除*功能不適用於預先安裝的憑證。

   「確認刪除信任的憑證」對話方塊隨即開啟。

4. 確認刪除、然後按一下*刪除*。

   該憑證會從表格中移除。

解決不受信任的憑證

當儲存陣列嘗試建立安全連線至SANtricity NetApp Unified Manager、但連線無法確認安全性時、就會發生不受信任的憑證。

從「憑證」頁面、您可以從儲存陣列匯入自我簽署的憑證、或匯入由信任的第三方所核發的憑證授權單位（CA）憑證、藉此解決不受信任的憑證。

開始之前

- 您必須以包含「安全性管理」權限的使用者設定檔登入。
- 如果您打算匯入CA簽署的憑證：
  - 您已為儲存陣列中的每個控制器產生憑證簽署要求（.CSR檔案）、並將其傳送至CA。
  - CA傳回信任的憑證檔案。
  - 您可以在本機系統上使用憑證檔案。

關於這項工作

如果符合下列任一項條件、您可能需要安裝其他信任的CA憑證：

- 您最近新增了儲存陣列。
- 一個或兩個憑證都已過期。
- 一個或兩個憑證均已撤銷。
- 一或兩個憑證都遺失根或中繼憑證。

步驟

1. 選擇*憑證管理*。
2. 選取*信任的*索引標籤。

   此頁面顯示針對儲存陣列所報告的所有憑證。

3. 選取功能表：匯入[憑證]以匯入CA憑證、或選取功能表：匯入[自我簽署的儲存陣列憑證]以匯入自我簽署的憑證。

   若要限制檢視、您可以使用*顯示…*篩選的憑證欄位、或按一下其中一個欄位標題來排序憑證列。

4. 在對話方塊中選取憑證、然後按一下*匯入*。

   憑證已上傳並驗證。

管理憑證

檢視憑證

您可以檢視憑證的摘要資訊、包括使用憑證的組織、發行憑證的授權單位、有效期間及指紋（唯一識別碼）。

開始之前

您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。

步驟

1. 選擇*憑證管理*。
2. 選取下列其中一個索引標籤：
   - 管理：顯示託管Web服務Proxy之系統的憑證。管理憑證可由憑證授權單位（CA）自行簽署或核准。可安全存取Unified Manager。
   - * Trusted （受信任的）-顯示Unified Manager可存取的憑證、以供儲存陣列和其他遠端伺服器（例如LDAP伺服器）使用。這些憑證可以從憑證授權單位（CA）核發、也可以自行簽署。
3. 若要查看有關憑證的詳細資訊、請選取其列、選取列尾端的省略符號、然後按一下*檢視*或*匯出*。

在 **SANtricity Unified Manager** 中匯出憑證

您可以匯出憑證以檢視其完整詳細資料。

開始之前

若要開啟匯出的檔案、您必須擁有憑證檢視器應用程式。

步驟

1. 選擇*憑證管理*。
2. 選取下列其中一個索引標籤：
   - 管理：顯示託管Web服務Proxy之系統的憑證。管理憑證可由憑證授權單位（CA）自行簽署或核准。可安全存取Unified Manager。
   - * Trusted （受信任的）-顯示Unified Manager可存取的憑證、以供儲存陣列和其他遠端伺服器（例如LDAP伺服器）使用。這些憑證可以從憑證授權單位（CA）核發、也可以自行簽署。
3. 從頁面選取憑證、然後按一下列結尾的省略符號。
4. 按一下「匯出」、然後儲存憑證檔案。

5. 在憑證檢視器應用程式中開啟檔案。

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。