管理 SAML 驗證設定

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/concept_manage_saml_authentication_settings_um.html on November 13, 2026. Always check docs.netapp.com for the latest.

目錄

管理 SAML 驗證設定 . . . 1
在 Active IQ Unified Manager 中啟用 SAML 驗證 . . . 1
在 Active IQ Unified Manager 中使用身分供應商 . . . 1
支援的加密標準 . . . 1
已驗證的身分供應商 . . . 1
ADFS 組態要求 . . . 1
其他組態要求 . . . 2
在 Active IQ Unified Manager 中啟用 SAML 驗證 . . . 2
在 Active IQ Unified Manager 中變更 SAML 驗證身分供應商 . . . 3
在 Active IQ Unified Manager 安全性憑證變更後更新 SAML 驗證設定 . . . 4
在 Active IQ Unified Manager 中停用 SAML 驗證 . . . 5
從 Active IQ Unified Manager 維護主控台停用 SAML 驗證 . . . 5
在 Active IQ Unified Manager 中使用 SAML 驗證頁面 . . . 6

管理 SAML 驗證設定

在 Active IQ Unified Manager 中啟用 SAML 驗證

設定遠端驗證設定後，您可以啟用安全性聲明標記語言 (SAML) 驗證，以便遠端使用者在存取 Unified Manager Web UI 之前，透過安全的身分供應商 (IdP) 進行驗證。

請注意，啟用 SAML 驗證後，只有遠端使用者才能存取 Unified Manager 圖形化使用者介面。本機使用者和維護使用者將無法存取 UI。此組態不會影響存取維護主控台的使用者。

在 Active IQ Unified Manager 中使用身分供應商

設定 Unified Manager 使用身分供應商（IdP）為所有遠端使用者執行 SAML 驗證時，您需要感知一些必要的組態設定，以便成功連線到 Unified Manager。

您必須將 Unified Manager URI 和中繼資料輸入到 IdP 伺服器中。您可以從 Unified Manager SAML 驗證頁面複本此資訊。Unified Manager 在安全性聲明標記語言 (SAML) 標準中被視為服務供應商 (SP)。

支援的加密標準

- 進階加密標準（AES）：AES-128 和 AES-256
- 安全雜湊演算法（SHA）：SHA-1 和 SHA-256

已驗證的身分供應商

- Shibboleth
- Active Directory Federation Services (ADFS)

ADFS 組態要求

- 您必須依照下列順序定義三個宣告規則，這些規則是 Unified Manager 解析此信賴憑證者信任項目的 ADFS 安全性聲明標記語言 (SAML) 回應時所需的。

宣告規則	價值
SAM-account-name	名稱 ID
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
權杖群組 — 非限定名稱	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- 您必須將身分驗證方法設定為 “Forms Authentication”，否則使用者在登出 Unified Manager 時可能會收到錯誤。請依照以下步驟操作：
  a. 開啟 ADFS 管理控制台。
  b. 點選左側樹狀檢視中的「驗證策略」資料夾。
  c. 在右側的「動作」下，按一下「編輯全域主要驗證原則」。

d. 將 Intranet 身分驗證方法設定為 “表單驗證”，而不是預設的 “Windows 驗證”。

- 在某些情況下，當 Unified Manager 安全性憑證由 CA 簽署時，透過身分提供者 (IdP) 登入會被拒絕。有兩種方法可以解決此問題：
  - 請依照連結中的說明，停用 ADFS 伺服器上與鏈結 CA 憑證關聯之信賴方的撤銷檢查：

    "停用依賴方信任的撤銷檢查"

  - 讓 CA 伺服器位於 ADFS 伺服器內，以便對 Unified Manager 伺服器憑證要求進行簽署。

其他組態要求

- Unified Manager 的時鐘偏差設定為 5 分鐘，因此 IdP 伺服器和 Unified Manager 伺服器之間的時間差不能超過 5 分鐘，否則驗證會失敗。

在 **Active IQ Unified Manager** 中啟用 **SAML** 驗證

您可以啟用安全性聲明標記語言 (SAML) 驗證，以便遠端使用者在存取 Unified Manager Web UI 之前，先透過安全的身分供應商 (IdP) 進行驗證。

開始之前

- 您必須已設定遠端驗證並驗證其已成功。
- 您必須至少建立一個具有應用程式管理員角色的遠端使用者或遠端群組。
- 身分供應商（IdP）必須受 Unified Manager 支援，並且必須進行設定。
- 您必須擁有 IdP URL 和中繼資料。
- 您必須能夠存取 IdP 伺服器。

在 Unified Manager 中啟用 SAML 驗證後，使用者必須先使用 Unified Manager 伺服器主機資訊設定身分提供者（IdP），才能存取圖形化使用者介面。因此，您必須準備好在開始組態程序之前完成連線的兩個部分。IdP 可以在設定 Unified Manager 之前或之後進行設定。

啟用 SAML 驗證後，只有遠端使用者才能存取 Unified Manager 圖形化使用者介面。本機使用者和維護使用者將無法存取 UI。此組態不會影響存取維護主控台、Unified Manager 命令或 ZAPI 的使用者。

完成此頁面上的 SAML 組態後，Unified Manager 將自動重新啟動。

步驟

1. 在左側導覽窗格中，按一下 一般 > **SAML** 驗證。
2. 選取 啟用 **SAML** 驗證 核取方塊。

   顯示設定 IdP 連線所需的欄位。

3. 輸入將 Unified Manager 伺服器連接至 IdP 伺服器所需的 IdP URI 與 IdP 中繼資料。

   如果可以從 Unified Manager 伺服器直接存取 IdP 伺服器，您可以在輸入 IdP URI 後按一下 取得 **IdP** 中繼資料 按鈕，自動填入 IdP 中繼資料欄位。

4. 複製 Unified Manager 主機中繼資料 URI，或將主機中繼資料儲存到 XML 文字檔案。

   現在您可以使用此資訊設定 IdP 伺服器。

5. 按一下 **Save** 。

   系統會顯示訊息方塊，確認您要完成組態並重新啟動 Unified Manager。

6. 按一下 確認並登出 ， Unified Manager 將重新啟動。

下次獲得授權的遠端使用者嘗試存取 Unified Manager 圖形介面時，他們將在 IdP 登入頁面而不是 Unified Manager 登入頁面輸入他們的憑證。

如果尚未完成，請存取您的 IdP 並輸入 Unified Manager 伺服器 URI 和中繼資料以完成組態。

> 當使用 ADFS 作為身分供應商時，Unified Manager GUI 不會遵循 ADFS 逾時設定，而是會持續運作，直到達到 Unified Manager 工作階段逾時為止。您可以按一下 一般 > 功能設定 > 閒置逾時來變更 GUI 工作階段逾時。

在 **Active IQ Unified Manager** 中變更 **SAML** 驗證身分供應商

您可以變更 Unified Manager 用來驗證遠端使用者的身份供應商（IdP）。

開始之前

- 您必須擁有 IdP URL 和中繼資料。
- 您必須能夠存取 IdP。

新的 IdP 可以在設定 Unified Manager 之前或之後進行設定。

步驟

1. 在左側導覽窗格中，按一下 一般 > **SAML** 驗證。
2. 輸入新的 IdP URI 和將 Unified Manager 伺服器連接到 IdP 所需的 IdP 中繼資料。

   如果可以從 Unified Manager 伺服器直接存取 IdP，您可以在輸入 IdP URL 後按一下 取得 **IdP** 中繼資料 按鈕，自動填入 IdP 中繼資料欄位。

3. 複製 Unified Manager 中繼資料 URI，或將中繼資料儲存到 XML 文字檔案。
4. 按一下 儲存組態。

   螢幕上會顯示訊息方塊，確認您要變更組態。

5. 按一下 **OK** 。

存取新的 IdP 並輸入 Unified Manager 伺服器 URI 和中繼資料以完成組態。

下次獲得授權的遠端使用者嘗試存取 Unified Manager 圖形介面時，他們將在新的 IdP 登入頁面而不是舊的 IdP 登入頁面中輸入其憑證。

在 **Active IQ Unified Manager** 安全性憑證變更後更新 **SAML** 驗證設定

對 Unified Manager 伺服器上安裝的 HTTPS 安全性憑證的任何變更都需要更新 SAML 驗證組態設定。如果您重新命名主機系統、為主機系統指派新的 IP 位址或手動變更系統的安全性憑證，則憑證會更新。

更改安全性憑證並重新啟動 Unified Manager 伺服器後，SAML 驗證將無法運作，使用者將無法存取 Unified Manager 圖形介面。您必須在 IdP 伺服器和 Unified Manager 伺服器上更新 SAML 驗證設定，才能重新啟用使用者介面存取。

步驟

1. 登入維護主控台。
2. 在*主選單*中，輸入*停用 SAML 驗證*選項的編號。

   螢幕上會顯示一則訊息，確認您是否要停用 SAML 驗證並重新啟動 Unified Manager。
3. 使用更新的 FQDN 或 IP 位址啟動 Unified Manager 使用者介面，在瀏覽器中接受更新後的伺服器憑證，並使用維護使用者憑證登入。
4. 在 設定/驗證 頁面中，選擇 **SAML** 驗證 標籤並設定 IdP 連線。
5. 複製 Unified Manager 主機中繼資料 URI，或將主機中繼資料儲存到 XML 文字檔案。
6. 按一下 **Save** 。

   系統會顯示訊息方塊，確認您要完成組態並重新啟動 Unified Manager。
7. 按一下 確認並登出 ， Unified Manager 將重新啟動。
8. 存取您的 IdP 伺服器，並輸入 Unified Manager 伺服器 URI 和中繼資料，以完成設定。

身分供應商	設定步驟
ADFS	a. 在 ADFS 管理 GUI 中刪除現有的信賴方信任項目。 b. 使用更新後 Unified Manager 伺服器的 `saml_sp_metadata.xml`新增依賴方信任項目。 c. 定義 Unified Manager 解析此信賴方信任項目的 ADFS SAML 回應所需的三個宣告規則。 d. 重新啟動 ADFS Windows 服務。
Shibboleth	a. 將 Unified Manager 伺服器的新 FQDN 更新至 `attribute-filter.xml` 和 `relying-party.xml` 檔案中。 b. 重新啟動 Apache Tomcat Web 伺服器，並等待 8005 連接埠上線。

9. 登入 Unified Manager 並驗證 SAML 驗證是否透過您的身分提供者（IdP）如預期運作。

在 **Active IQ Unified Manager** 中停用 **SAML** 驗證

如果您想要在遠端使用者登入 Unified Manager Web UI 之前，停止透過安全的身分供應商（IdP）對其進行驗證，您可以停用 SAML 驗證。停用 SAML 驗證後，已設定的目錄服務供應商（例如 Active Directory 或 LDAP）將執行登入驗證。

停用 SAML 驗證後，除了已設定的遠端使用者外，本機使用者和維護使用者也將能夠存取圖形化使用者介面。

如果您無法存取圖形化使用者介面，也可以使用 Unified Manager 維護主控台停用 SAML 驗證。

停用 SAML 驗證後，Unified Manager 將自動重新啟動。

步驟

1. 在左側導覽窗格中，按一下 一般 > **SAML** 驗證。
2. 取消勾選 啟用 **SAML** 驗證 核取方塊。
3. 按一下 **Save** 。

   系統會顯示訊息方塊，確認您要完成組態並重新啟動 Unified Manager。
4. 按一下 確認並登出 ， Unified Manager 將重新啟動。

下次遠端使用者嘗試存取 Unified Manager 圖形介面時，他們將在 Unified Manager 登入頁面而非 IdP 登入頁面輸入其憑證。

存取您的 IdP 並刪除 Unified Manager 伺服器 URI 和中繼資料。

從 **Active IQ Unified Manager** 維護主控台停用 **SAML** 驗證

當無法存取 Unified Manager 介面（GUI）時，您可能需要從維護控制台停用 SAML 驗證。這種情況可能發生在組態錯誤或身分提供者（IdP）無法存取時。

開始之前

您必須以維護使用者的身分存取維護控制台。

停用 SAML 驗證後，已設定的目錄服務供應商（例如 Active Directory 或 LDAP）將執行登入驗證。除了已設定的遠端使用者外，本機使用者和維護使用者也將能夠存取圖形化使用者介面。

您也可以在使用者介面中的「設定/驗證」頁面停用 SAML 驗證。

停用 SAML 驗證後，Unified Manager 將自動重新啟動。

步驟

1. 登入維護主控台。
2. 在*主選單*中，輸入*停用 SAML 驗證*選項的編號。

   螢幕上會顯示一則訊息，確認您是否要停用 SAML 驗證並重新啟動 Unified Manager。

3. 輸入 **y**，然後按 Enter 鍵，Unified Manager 將重新啟動。

下次遠端使用者嘗試存取 Unified Manager 圖形介面時，他們將在 Unified Manager 登入頁面而非 IdP 登入頁面輸入其憑證。

如有需要，存取您的 IdP 並刪除 Unified Manager 伺服器 URL 和中繼資料。

在 **Active IQ Unified Manager** 中使用 **SAML** 驗證頁面

您可以使用 SAML 驗證頁面設定 Unified Manager，以便在遠端使用者登入 Unified Manager Web UI 之前，透過安全的身分供應商 (IdP) 使用 SAML 對其進行驗證。

- 您必須擁有應用程式管理員角色才能建立或修改 SAML 組態。
- 您必須設定遠端驗證。
- 您必須至少設定一個遠端使用者或遠端群組。

設定遠端驗證和遠端使用者後，您可以選取「啟用 SAML 驗證」核取方塊，以啟用透過安全的身分供應商進行驗證。

- **IdP URI**

  從 Unified Manager 伺服器存取 IdP 的 URI。範例 URI 如下所示。

  ADFS 範例 URI：

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Shibboleth 範例 URI：

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **IdP** 中繼資料

  XML 格式的 IdP 中繼資料。

  如果可以從 Unified Manager 伺服器存取 IdP URL，則可以按一下 取得 **IdP** 中繼資料 按鈕來填入此欄位。

- 主機系統（**FQDN**）

  安裝期間所定義的 Unified Manager 主機系統的完整網域名稱（FQDN）。如有必要，您可以變更此值。

- 主機 **URI**

  從身分識別提供者（IdP）存取 Unified Manager 主機系統的 URI。

- 主機中繼資料

  XML 格式的主機系統中繼資料。

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。