



啟用多重身份驗證 Element Software

NetApp
November 12, 2025

目錄

啟用多重身份驗證	1
設定多重身份驗證	1
查找更多信息	1
多因素身份驗證的補充訊息	1
查找更多信息	2

啟用多重身份驗證

設定多重身份驗證

多因素身份驗證 (MFA) 使用第三方身分提供者 (IdP) 透過安全性斷言標記語言 (SAML) 來管理使用者會話。MFA 允許管理員根據需要配置其他身份驗證因素，例如密碼和短信，以及密碼和電子郵件。

您可以使用 Element API 的以下基本步驟來設定叢集以使用多因素身份驗證。

每個 API 方法的詳細資訊可以在以下位置找到：["元素 API 參考"](#)。

1. 透過呼叫以下 API 方法並以 JSON 格式傳遞 IdP 元數據，為叢集建立新的第三方身分提供者 (IdP) 配置：
`CreateIdpConfiguration`

從第三方身分提供者 (IdP) 擷取純文字格式的身分提供者元資料。需要驗證此元數據，以確保其 JSON 格式正確。有許多 JSON 格式化應用程式可供使用，例如：<https://freeformatter.com/json-escape.html>。

2. 透過 `spMetadataUrl` 檢索叢集元數據，並透過呼叫以下 API 方法將其複製到第三方身分提供者：
`ListIdpConfigurations`

`spMetadataUrl` 是一個 URL，用於從叢集中檢索身分提供者 (IdP) 的元數據，以便建立信任關係。

3. 在第三方身分提供者 (IdP) 上設定 SAML 斷言，使其包含「NameID」屬性，以便唯一識別使用者進行稽核日誌記錄，並使單點登出功能正常運作。
4. 透過呼叫下列 API 方法，建立一個或多個由第三方身分提供者 (IdP) 進行驗證的叢集管理員使用者帳戶：
`AddIdpClusterAdmin`



為了達到預期效果，IdP 叢集管理員的使用者名稱應與 SAML 屬性名稱/值對應相匹配，如下例所示：

- `email=bob@company.com` — 其中 IdP 配置為在 SAML 屬性中發布電子郵件地址。
- `group=cluster-administrator` - 其中 IdP 配置為釋放一個群組屬性，所有使用者都應該有權存取該群組屬性。請注意，出於安全考慮，SAML 屬性名稱/值對區分大小寫。

5. 透過呼叫以下 API 方法為叢集啟用 MFA：`EnableIdpAuthentication`

查找更多信息

- ["SolidFire和 Element 軟體文檔"](#)
- ["NetApp Element vCenter Server 插件"](#)

多因素身份驗證的補充訊息

關於多因素身份驗證，您應該注意以下注意事項。

- 若要刷新不再有效的身分提供者 (IdP) 證書，您需要使用非身分提供者管理員使用者呼叫下列 API 方法：

UpdateIdpConfiguration

- MFA 與長度小於 2048 位元的憑證不相容。預設情況下，叢集上會建立一個 2048 位元 SSL 憑證。呼叫 API 方法時，應避免設定較小的憑證：SetSSLCertificate



如果叢集在升級前使用的憑證小於 2048 位，則升級至 Element 12.0 或更高版本後，必須將叢集憑證更新為 2048 位元或更高版本的憑證。

- IdP 管理員使用者不能直接用於進行 API 呼叫（例如，透過 SDK 或 Postman），也不能用於其他整合（例如，OpenStack Cinder 或 vCenter 外掛程式）。如果需要建立具有這些權限的用戶，請新增 LDAP 叢集管理員用戶或本機叢集管理員用戶。

查找更多信息

- ["使用 Element API 管理存儲"](#)
- ["SolidFire和 Element 軟體文檔"](#)
- ["NetApp Element vCenter Server 插件"](#)

版權資訊

Copyright © 2025 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。