



啟用多因素驗證 (MFA) 帳戶 ONTAP 9

NetApp
February 12, 2026

目錄

啟用多因素驗證（MFA）帳戶.....	1
瞭解 ONTAP 多因素驗證.....	1
使用 SSH 和 TOTP 啟用 ONTAP 多因素驗證.....	2
使用 SSH 公開金鑰和使用者密碼來啟用 MFA.....	3
使用 TOTP 啟用 MFA.....	3
使用 TOTP 設定 MFA 的本機 ONTAP 使用者帳戶.....	5
重設 ONTAP 使用者帳戶的 TOTP 秘密金鑰.....	6
如果金鑰遭到入侵、請重設 TOTP.....	6
如果金鑰遺失、請重設 TOTP.....	6
停用 ONTAP 使用者帳戶的 TOTP 秘密金鑰.....	7

啟用多因素驗證（MFA）帳戶

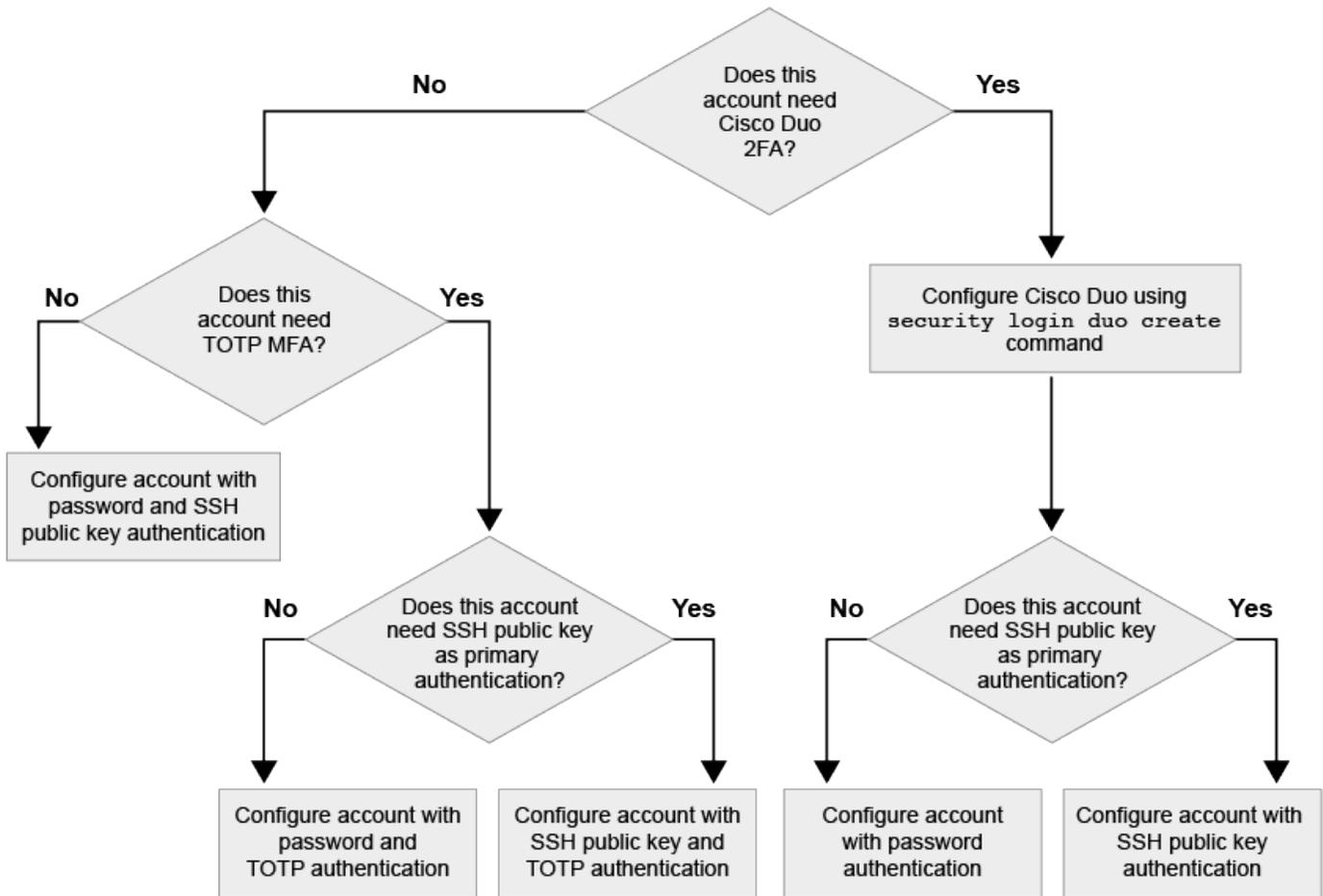
瞭解 ONTAP 多因素驗證

多因素驗證（MFA）可讓您要求使用者提供兩種驗證方法來登入管理或資料儲存 VM、以增強安全性。

視您的 ONTAP 版本而定、您可以結合使用 SSH 公開金鑰、使用者密碼和時間型一次性密碼（TOTP）進行多因素驗證。當您啟用和設定 Cisco Duo（ONTAP 9.14.1 及更新版本）時、它會作為額外的驗證方法、以補充所有使用者的現有方法。

可從 ... 開始使用。	第一種驗證方法	第二種驗證方法
ONTAP 9.14.1.	SSH公開金鑰	TOTP
	使用者密碼	TOTP
	SSH公開金鑰	Cisco Duo™
	使用者密碼	Cisco Duo™
ONTAP 9.13.1.12.9.11.9.11.	SSH公開金鑰	TOTP
	使用者密碼	TOTP
ONTAP 9.3	SSH公開金鑰	使用者密碼

如果已設定 MFA、叢集管理員必須先啟用本機使用者帳戶、則該帳戶必須由本機使用者設定。



使用 SSH 和 TOTP 啟用 ONTAP 多因素驗證

多因素驗證（MFA）可讓您要求使用者提供兩種驗證方法來登入管理或資料 SVM、以增強安全性。

關於這項工作

- 您必須是叢集管理員才能執行此工作。
- 如果您不確定要指派給登入帳戶的存取控制角色，可以使用 `security login modify` 命令稍後再新增該角色。

如"[指令參考資料ONTAP](#)"需詳細 `security login modify` 資訊，請參閱。

"[修改指派給系統管理員的角色](#)"

- 如果您使用公開金鑰進行驗證、則必須先將公開金鑰與帳戶建立關聯、帳戶才能存取 SVM。

"[將公開金鑰與使用者帳戶建立關聯](#)"

您可以在啟用帳戶存取之前或之後執行此工作。

- 從S廳9.12.1開始ONTAP、您可以使用FIDO2（Fast Identity Online）或個人身分驗證（PIV）驗證標準、將Yobikey硬體驗證裝置用於SSH用戶端MFA。

使用 SSH 公開金鑰和使用者密碼來啟用 MFA

從 ONTAP 9.3 開始、叢集管理員可以設定本機使用者帳戶、使用 SSH 公開金鑰和使用者密碼登入 MFA。

1. 使用 SSH 公開金鑰和使用者密碼、在本機使用者帳戶上啟用 MFA：

```
security login create -vserver <svm_name> -user-or-group-name  
<user_name> -application ssh -authentication-method <password|publickey>  
-role admin -second-authentication-method <password|publickey>
```

下列命令需要 SVM 系統管理員帳戶 admin2 使用預先定義的 admin 登入 SVM 的角色engData1 使用 SSH 公開金鑰和使用者密碼：

```
cluster-1::> security login create -vserver engData1 -user-or-group-name  
admin2 -application ssh -authentication-method publickey -role admin  
-second-authentication-method password  
  
Please enter a password for user 'admin2':  
Please enter it again:  
Warning: To use public-key authentication, you must create a public key  
for user "admin2".
```

如"[指令參考資料ONTAP](#)"需詳細 `security login create` 資訊，請參閱。

使用 TOTP 啟用 MFA

從 ONTAP 9.13.1 開始、您可以要求本機使用者同時使用 SSH 公開金鑰或使用者密碼和時間型一次性密碼（TOTP）登入管理或資料 SVM、以增強安全性。啟用 MFA 與 TOTP 的帳戶後、本機使用者必須登入 "[完成組態設定](#)"。

TOTP 是一種電腦演算法、使用目前時間來產生一次性密碼。如果使用 TOTP、它永遠是 SSH 公開金鑰或使用者密碼之後的第二種驗證形式。

開始之前

您必須是儲存管理員才能執行這些工作。

步驟

您可以將 MFA 設為使用者密碼或 SSH 公開金鑰做為第一種驗證方法、並將 TOTP 設為第二種驗證方法。

使用使用者密碼和 TOTP 啟用 MFA

1. 使用使用者密碼和 TOTP 啟用多因素驗證的使用者帳戶。

- 適用於新使用者帳戶 *

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

- 適用於現有使用者帳戶 *

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

2. 確認 MFA 已啟用 TOTP :

```
security login show
```

使用 SSH 公開金鑰和 TOTP 啟用 MFA

1. 使用 SSH 公開金鑰和 TOTP 啟用多因素驗證的使用者帳戶。

- 適用於新使用者帳戶 *

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role>  
-comment <comment>
```

- 適用於現有使用者帳戶 *

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

+ 如"[指令參考資料ONTAP](#)"需詳細 `security login modify` 資訊，請參閱。

2. 確認 MFA 已啟用 TOTP :

```
security login show
```

如"[指令參考資料ONTAP](#)"需詳細 `security login show` 資訊，請參閱。

完成後

- 如果您尚未將公開金鑰與系統管理員帳戶建立關聯、則必須先建立公開金鑰、帳戶才能存取SVM。

["將公開金鑰與使用者帳戶建立關聯"](#)

- 本機使用者必須登入才能使用 TOTP 完成 MFA 組態。

["使用 TOTP 設定 MFA 的本機使用者帳戶"](#)

相關資訊

- ["支援多因素驗證ONTAP 功能 \(TR-4647\) "](#)
- ["指令參考資料ONTAP"](#)

使用 TOTP 設定 MFA 的本機 ONTAP 使用者帳戶

從 ONTAP 9.13.1 開始，使用者帳戶可以使用時間型一次性密碼（TOTP）來設定多因素驗證（MFA）。

開始之前

- 儲存管理員必須 ["使用 TOTP 啟用 MFA"](#) 作為使用者帳戶的第二種驗證方法。
- 您的主要使用者帳戶驗證方法應為使用者密碼或公開 SSH 金鑰。
- 您必須將 TOTP 應用程式設定為與智慧型手機搭配使用、並建立 TOTP 秘密金鑰。

支援 Microsoft Authenticator、Google Authenticator、Authy 及任何其他 TOTP 相容驗證器。

步驟

1. 使用目前的驗證方法登入您的使用者帳戶。

您目前的驗證方法應該是使用者密碼或 SSH 公開金鑰。

2. 在您的帳戶上建立 TOTP 組態：

```
security login totp create -vserver "<svm_name>" -username  
"<account_username >"
```

3. 確認您的帳戶已啟用 TOTP 組態：

```
security login totp show -vserver "<svm_name>" -username
"<account_username>"
```

相關資訊

- ["安全登入 totp 創建"](#)
- ["安全登入 totp 顯示"](#)

重設 ONTAP 使用者帳戶的 TOTP 秘密金鑰

為了保護您的帳戶安全、如果 TOTP 秘密金鑰遭到洩漏或遺失、您應該停用該金鑰並建立新的金鑰。

如果金鑰遭到入侵、請重設 TOTP

如果您的 TOTP 秘密金鑰已洩漏、但您仍有權存取、您可以移除洩漏的金鑰並建立新的金鑰。

1. 使用您的使用者密碼或 SSH 公開金鑰、以及您遭入侵的 TOTP 秘密金鑰、登入您的使用者帳戶。
2. 移除遭入侵的 TOTP 秘密金鑰：

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. 建立新的 TOTP 秘密金鑰：

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. 確認您的帳戶已啟用 TOTP 組態：

```
security login totp show -vserver <svm_name> -username
<account_username>
```

如果金鑰遺失、請重設 TOTP

如果 TOTP 秘密金鑰遺失、請聯絡您的儲存管理員 ["停用金鑰"](#)。停用金鑰後、您可以使用第一種驗證方法登入並設定新的 TOTP。

開始之前

TOTP 秘密金鑰必須由儲存管理員停用。如果您沒有儲存管理員帳戶、請聯絡您的儲存管理員以停用金鑰。

步驟

1. 儲存管理員停用 TOTP 密碼後、請使用主要驗證方法登入您的本機帳戶。
2. 建立新的 TOTP 秘密金鑰：

```
security login totp create -vserver <svm_name> -username  
<account_username >
```

3. 確認您的帳戶已啟用 TOTP 組態：

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

相關資訊

- ["安全登入 totp 創建"](#)
- ["安全登入 totp 刪除"](#)
- ["安全登入 totp 顯示"](#)

停用 ONTAP 使用者帳戶的 TOTP 秘密金鑰

如果本機使用者的時間型一次性密碼（TOTP）秘密金鑰遺失、則儲存管理員必須先停用遺失的金鑰、使用者才能建立新的 TOTP 秘密金鑰。

關於這項工作

此工作只能從叢集管理員帳戶執行。

步驟

1. 停用 TOTP 秘密金鑰：

```
security login totp modify -vserver <svm_name> -username  
<account_username> -enabled false
```

如"[指令參考資料ONTAP](#)"需詳細 `security login totp modify` 資訊，請參閱。

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。