

如何推出多因素驗證

Salesforce, Spring '23



此文件的英文版本優先於翻譯版本。

© Copyright 2000—2023 Salesforce, Inc. 保留所有權利。Salesforce 為 Salesforce, Inc. 的商標。本文件中所提及的所有其他商標為其各自擁有者的資產。

目錄

如何推出多因素驗證	1
現在正是啟用多因素驗證的時機	2
準備階段：評估及計畫多因素驗證推出	7
首展階段：準備啟動多因素驗證	26
管理階段：維護及增強多因素驗證	36
多因素驗證詞彙	43
索引	45

如何推出多因素驗證

多因素驗證 (MFA) 這個最簡單有效的方式可協助您保護使用者的帳戶存取權。由於 MFA 是保護帳戶存取權的重要元件，因此 Salesforce 要求直接登入使用者介面的所有使用者都需要進行 MFA。MFA 需求於 2022 年 2 月 1 日生效。我們使用簡單創新的 MFA 解決方案，這個解決方案可在強大安全性和使用者便利性之間取得平衡，讓您得以輕鬆實現目標。

重要事項: 2023 年 Salesforce 將針對所有 Salesforce 組織自動啟用與強制執行 MFA。若要深入瞭解這些里程碑，請參閱[多因素驗證 \(MFA\) 強制執行藍圖](#)。若要瞭解如何自行滿足 MFA 需求，請參閱[MFA 常見問題](#)與本指南。有關 MFA 需求的契約詳細資料，請參閱[Salesforce 信任與合規性文件](#)。

身為管理員，您是您公司針對 Salesforce 所有事物之值得信賴的顧問，您將協助決定如何準備 MFA 以及向使用者推出。本指南會指引您完成建議的流程，包含關鍵步驟與最佳作法。

備註: 本指南的重點在於為透過使用者名稱和密碼直接登入 Salesforce 產品的使用者啟用 MFA。此內容不適用於為單一登入 (SSO) 身分提供者、API 登入，或為透過 Salesforce Experience Cloud 網站或電子商務網站與您互動的合作夥伴或客戶設定 MFA。

現在正是啟用多因素驗證的時機

隨著安全性威脅越來越常見，實作強式的度量來保護 Salesforce 資料和業務，以及最終保護您的客戶變得越來越重要。僅使用者名稱和密碼已不足以防止未經授權的帳戶存取。為了針對網路釣魚、認證填充和帳戶接管等常見攻擊新增一層保護，Salesforce 要求所有登入組織的使用者都必須使用多因素驗證 (MFA) 進行驗證。為了提供協助，我們具備您所需的資源和工具，讓您能夠順暢地計畫和執行對 Salesforce 使用者的首展。

準備階段：評估及計畫多因素驗證推出

透過探索和計畫期間來開始多因素驗證 (MFA) 專案。瞭解為何我們需要 MFA 來增強登入安全性、您的驗證方法選擇為何，以及您的公司可以從使用 MFA 中獲得哪些好處。評估企業和使用者要求以及您的實作選項，並向關鍵專案關係人說明理由。計畫 MFA 專案，包含首展、變更管理和支援策略，如此您就可以清楚瞭解成功啟動的路徑。

首展階段：準備啟動多因素驗證

隨著專案計畫準備就緒並與專案關係人保持一致，下一步就是展開工作，以向 Salesforce 使用者提供多因素驗證 (MFA)。現在是時候讓使用者準備好使用 MFA 登入，並制定實作和測試計畫。如此您就做好啟動 MFA 的準備。如果您正逐步向使用者群組推出 MFA，請在此階段重複一些活動，直到每個人都使用 MFA 為止。

管理階段：維護及增強多因素驗證

恭喜，您已為 Salesforce 使用者啟用多因素驗證 (MFA)！但請勿只「設定好就遺忘」。請透過持續關注每個人體驗 MFA 的方式來確保專案順利進行。在此階段中，請估量 MFA 推出的成效，並以每天持續進行的作業來支援使用者。這也是尋找方法來最佳化 MFA 實作及整體安全狀況的好時機。

另請參照：

[支援多因素驗證的產品](#)

現在正是啟用多因素驗證的時機

隨著安全性威脅越來越常見，實作強式的度量來保護 Salesforce 資料和業務，以及最終保護您的客戶變得越來越重要。僅使用者名稱和密碼已不足以防止未經授權的帳戶存取。為了針對網路釣魚、認證填充和帳戶接管等常見攻擊新增一層保護，Salesforce 要求所有登入組織的使用者都必須使用多因素驗證 (MFA) 進行驗證。為了提供協助，我們具備您所需的資源和工具，讓您能夠順暢地計畫和執行對 Salesforce 使用者的首展。



備註: 如果您很熟悉雙因素驗證 (2FA) 的概念，則多因素驗證本質上是一樣的。2FA 是其中一種 MFA。

推出和支援 MFA 的架構

根據我們的經驗，以及已為 Salesforce 實作多因素驗證 (MFA) 之客戶的體驗，我們定義了您可以在自己的旅程上遵循的路徑。此路徑是一種架構，內含最佳作法、考慮事項以及推出 MFA 和確保使用者正確採用的實際建議。使用適用於您公司和 Salesforce 產品的步驟。

歡迎使用多因素驗證助理

尋找在向 Salesforce 使用者推出多因素驗證 (MFA) 時的協助嗎？歡迎使用多因素驗證助理，此中心將提供所有建議的活動、工具和資源來幫助您成功完成專案。

使用 MFA 首展套件取得可自訂的範本

為了協助您迅速開始多因素驗證 (MFA) 專案，我們提供包含變更管理指南和可自訂範本的首展套件。使用此套件以計畫 MFA 實作，並讓使用者做好準備。

另請參照：

[瞭解多因素驗證](#)

推出和支援 MFA 的架構

根據我們的經驗，以及已為 Salesforce 實作多因素驗證 (MFA) 之客戶的體驗，我們定義了您可以在自己的旅程上遵循的路徑。此路徑是一種架構，內含最佳作法、考慮事項以及推出 MFA 和確保使用者正確採用的實際建議。使用適用於您公司和 Salesforce 產品的步驟。

為了更方便管理以及更快速轉換，我們建議您分三個階段完成作業。這些階段細分為數個階段，每個階段都有一組推薦的活動。

準備就緒

- 瞭解為何 Salesforce 需要 MFA 來獲得增強登入安全性、可啟用 MFA 的選項為何，以及您的公司可以獲得哪些益處。
- 評估企業和使用者要求，並使這些要求與 Salesforce 產品的 MFA 選項保持一致，以開始定義您的實作策略。
- 計畫 MFA 實作，包含首展、變更管理和支援策略，以便您做好投入使用的準備。

首展

- 讓使用者做好 MFA 首展的準備，方法是實踐您的變更管理策略。
- 實作 MFA，方法是開始實作和測試計畫，包含建立 MFA 支援流程和小組。
- 在您預定的上線日期向使用者啟動 MFA。

管理

- 透過使用者回饋意見和度量來測量 MFA 首展的成效。
- 支援使用者進行持續的每日操作。
- 最佳化 MFA 實作和整體的安全性狀況。

根據組織的大小，您可以使用「變更管理」小組，或將專案經理指派給此首展。或者，您可能是負責從開始到結束組織與執行專案的人。無論如何分工，請使用這份指引來在整個過程中為您提供協助。

歡迎使用多因素驗證助理

尋找在向 Salesforce 使用者推出多因素驗證 (MFA) 時的協助嗎？歡迎使用多因素驗證助理，此中心將提供所有建議的活動、工具和資源來幫助您成功完成專案。

您也可從 Lightning Experience 中的「設定」存取多因素驗證助理。

版本

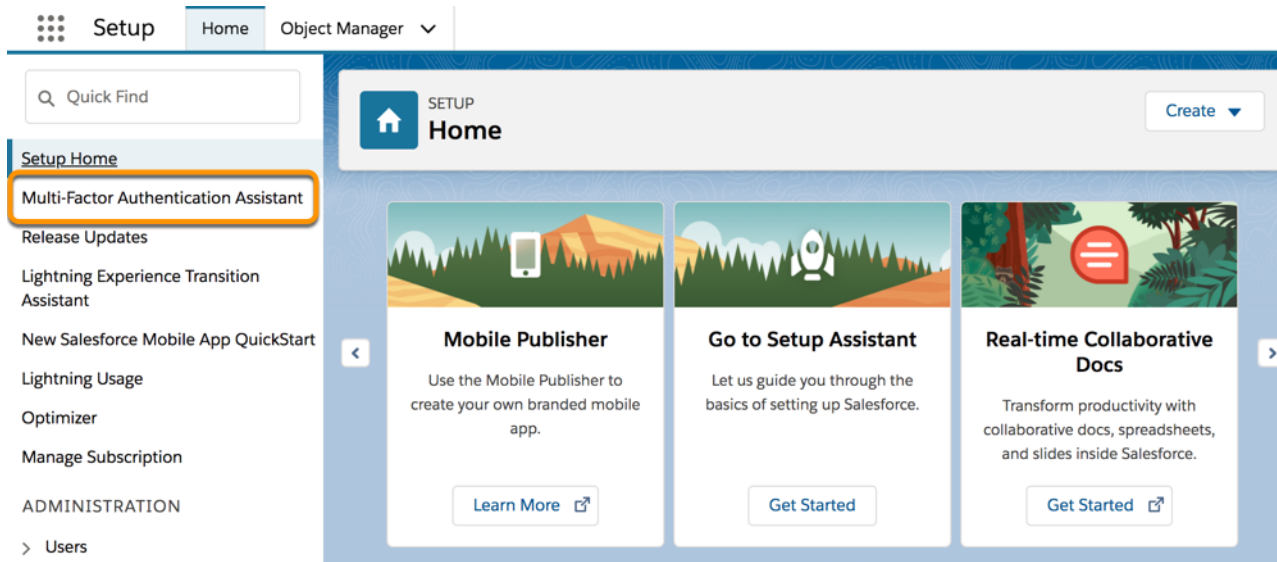
提供版本：僅限 Lightning Experience

提供版本：**Essentials**、**Group**、**Professional**、**Enterprise**、**Performance**、**Unlimited** 及 **Developer Edition**

使用者權限

若要使用多因素驗證助理：

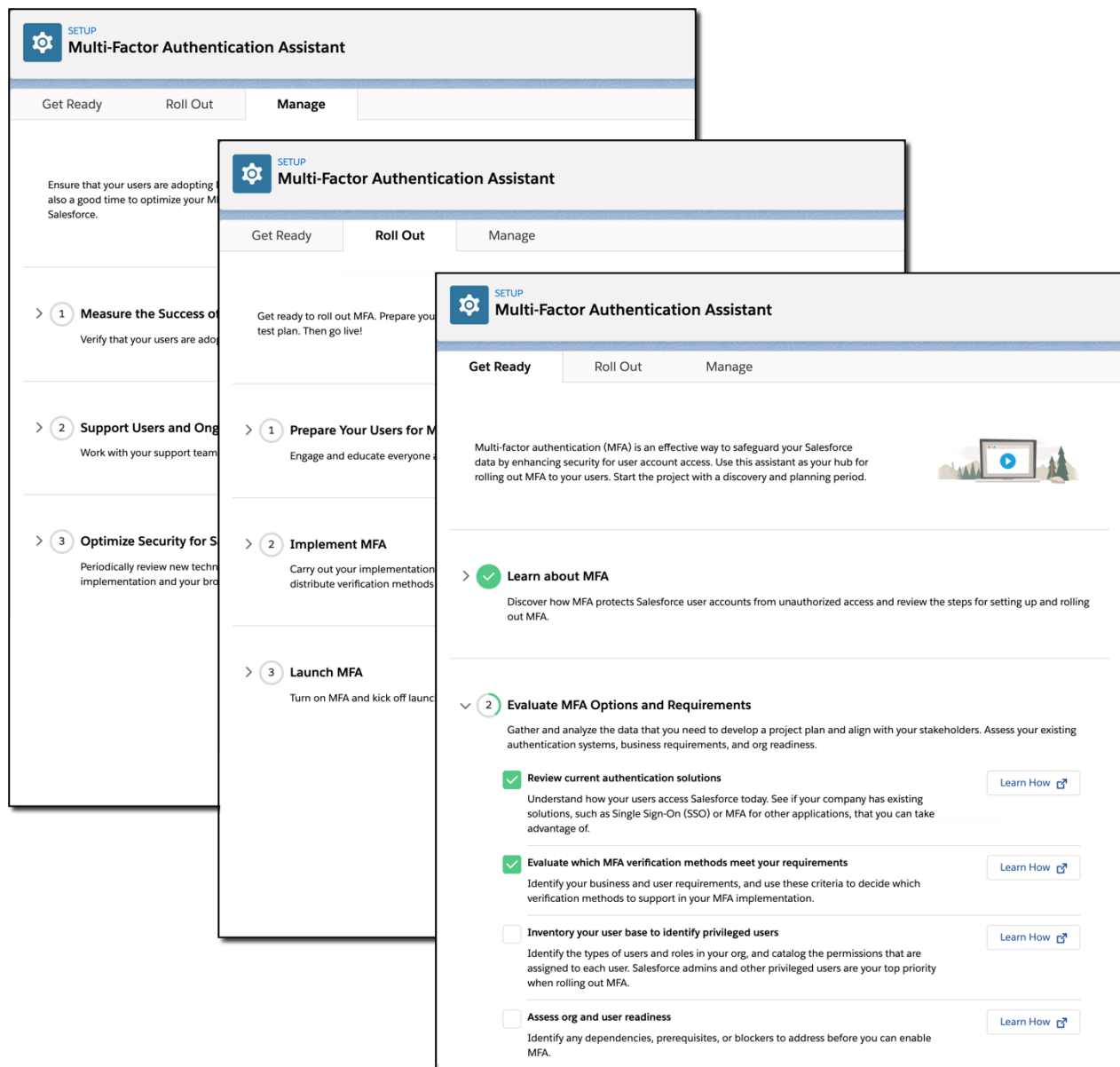
- 檢視設定和組態和自訂應用程式



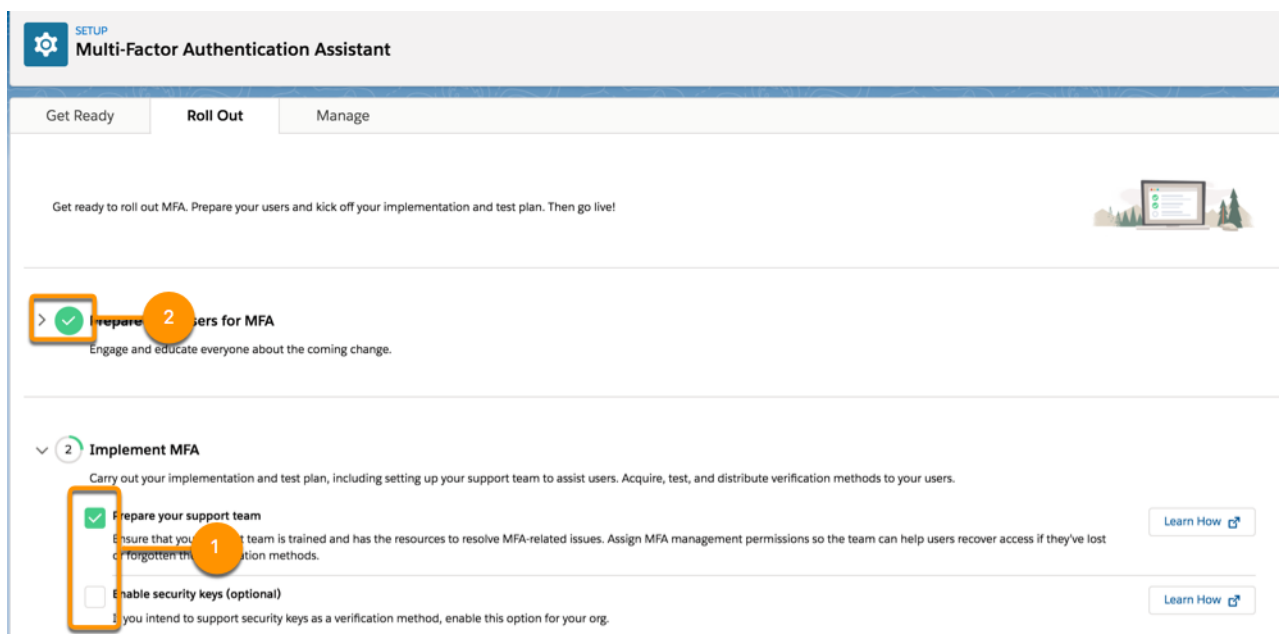
多因素驗證助理可引導您完成通往 MFA 的每個路徑和環節。

- 準備階段：透過探索和計畫期間來開始多因素驗證 (MFA) 專案。
- 首展階段：透過變更管理活動，讓使用者做好使用 MFA 的準備、完成實作和測試計畫，然後上線。
- 管理階段：測量 MFA 首展的成效，支援須每日持續操作的使用者，並最佳化 MFA 實作和整體安全性狀況。

在每個階段中，您都會獲得逐步指示和資源的支援。活動分為一系列階段，讓一切井然有序，幫助您追蹤進度。若要查看階段中的建議活動，請按一下 ➤ 圖示。



此助理可讓您檢查已完成的步驟，協助您追蹤已完成的工作及尚未完成的工作 (1)。此助理會顯示您在階段中何時完成所有步驟 (2)。



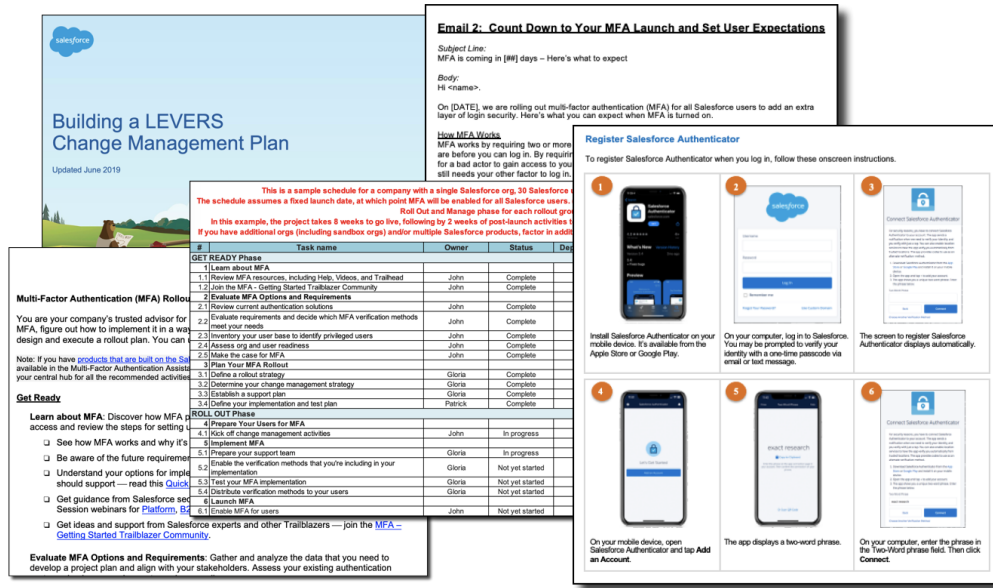
多因素驗證助理是專為協助您有效率地快速完成流程而設計。但是您可以按照組織需求，以任何順序來處理活動。您也可以略過任何不相關的步驟，或是不將值新增至專案。如果您採取反覆的方法來推出MFA，您可以在啟用所有使用者前重複執行活動。

另請參照：

[推出和支援 MFA 的架構](#)

使用 MFA 首展套件取得可自訂的範本

為了協助您迅速開始多因素驗證 (MFA) 專案，我們提供包含變更管理指南和可自訂範本的首展套件。使用此套件以計畫 MFA 實作，並讓使用者做好準備。



內含功能：

- 簡報組，可協助說明 MFA 的個案，並與利害關係人及領導者達成共識。
- 使用者庫存範本和指南，用於稽核指派給使用者的權限，並識別應先取得 MFA 的使用者。
- 開發變更管理策略加上支援範本的指南。
- 範例電子郵件批次行銷活動，用於增加對近期發表會的認知與宣傳 MFA 的價值。
- 使用者訓練組，用來訓練您的使用者瞭解 MFA 的用途、運作方式，以及如何使用支援的驗證方法註冊和登入。
- 上線指南，顯示使用者使用 Salesforce 產品支援的每個 MFA 驗證方法進行註冊及登入的步驟。

此套件也包含可用於首展計畫的資源，包括追蹤檢查清單、專案排程範本和簡單的測試計畫範本。

MFA 首展套件是壓縮檔，您可以在[此下載](#)。

準備階段：評估及計畫多因素驗證推出

透過探索和計畫期間來開始多因素驗證 (MFA) 專案。瞭解為何我們需要 MFA 來增強登入安全性、您的驗證方法選擇為何，以及您的公司可以從使用 MFA 中獲得哪些好處。評估企業和使用者要求以及您的實作選項，並向關鍵專案關係人說明理由。計畫 MFA 專案，包含首展、變更管理和支援策略，如此您就可以清楚瞭解成功啟動的路徑。

瞭解多因素驗證

多因素驗證 (MFA) 透過要求使用者輸入二個或以上的證據或因素來證明他們的身分，進而增強登入流程的安全性。其中一個因素就是使用者知道的資訊，像是使用者名稱和密碼組合。其他因素像是使用者擁有的驗證方法，例如驗證器應用程式、實體安全性金鑰，或內建驗證器。透過將使用者存取權與多個不同類型的因素連結在一起，執行動作的惡意使用者就難以進入您的 Salesforce 環境。即使使用者的密碼遭入侵，攻擊者能猜到或是模擬使用者實際擁有之因素的可能性也很小。

[多因素驗證的評估選項和要求](#)

啟用多因素驗證 (MFA) 的步驟很簡單直接。在深入瞭解前，請用一些時間來瞭解現有的驗證系統，並識別 MFA 解決方案的要求。如果您從評估期間開始，您可以收集配合主管要求所需的資料，並開發專案計畫。

[計畫多因素驗證首展](#)

在完成評估期間以瞭解您對多因素驗證 (MFA) 的選項和要求後，您就可以擬定自己的專案計畫。

瞭解多因素驗證

多因素驗證 (MFA) 透過要求使用者輸入二個或以上的證據或因素來證明他們的身分，進而增強登入流程的安全性。其中一個因素就是使用者知道的資訊，像是使用者名稱和密碼組合。其他因素像是使用者擁有的驗證方法，例如驗證器應用程式、實體安全性金鑰，或內建驗證器。透過將使用者存取權與多個不同類型的因素連結在一起，執行動作的惡意使用者就難以進入您的 Salesforce 環境。即使使用者的密碼遭入侵，攻擊者能猜到或是模擬使用者實際擁有之因素的可能性也很小。

MFA 的運作方式

MFA 將額外的驗證步驟新增至 Salesforce 登入流程。

1. 使用者會像平常一樣輸入使用者名稱和密碼。
2. 接著使用者會收到提示，要求其提供強大驗證方法。

查看[多因素驗證的驗證方法](#)，以瞭解您的 Salesforce 產品支援哪些種類的方法。您可以視需要部署許多種類的方法來滿足您的企業和使用者要求。

每名使用者必須花幾分鐘的時間來註冊至少一個驗證方法，如此才能讓此方法跟使用者的 Salesforce 帳戶相連接。使用者也可以隨時註冊方法。如果使用者在 MFA 啟用前尚未準備好方法，則系統會自動發出提示來要求使用者在他們下一次登入時進行註冊。畫面上的提示會引導使用者執行流程。



小祕訣：鼓勵使用者註冊多個驗證方法來降低被鎖定在 Salesforce 之外的風險。如果使用者忘記或遺失其中一個方法，他們就有其他可依靠的選項。

另請參照：

[支援多因素驗證的產品](#)

[現在正是啟用多因素驗證的時機](#)

[適用於管理員的多因素驗證快速指南](#)

[多因素驗證常見問題](#)

[Trailblazer Community 群組：MFA - 入門](#)

支援多因素驗證的產品

這些 Salesforce 產品包含多因素驗證 (MFA) 支援：

- 在 Salesforce Platform 上建立的所有產品，包括：
 - Sales Cloud
 - Service Cloud

- Analytics Cloud
- B2B Commerce Cloud
- Experience Cloud
- 產業產品 (Consumer Goods Cloud、Education Cloud、Financial Services Cloud、Government Cloud、Health Cloud、Manufacturing Cloud、Nonprofit Cloud、Philanthropy Cloud)
- Marketing Cloud—Audience Studio (先前的 DMP)
- Marketing Cloud—Pardot
- 平台
- Salesforce Essentials
- Salesforce Field Service
- 合作夥伴解決方案
- B2C Commerce Cloud
- Heroku
- Marketing Cloud 參與 (由電子郵件、傳訊和旅程支援)
- Marketing Cloud Intelligence (由 Datorama 提供技術支援)
- Marketing Cloud Social
- MuleSoft Anypoint 平台
- Quip 產品
- Tableau Online

多因素驗證的驗證方法

當為您的 Salesforce 產品啟用 MFA 時，登入流程會要求使用者除了使用者名稱和密碼外，還要提供驗證方法。Salesforce MFA 僅允許使用強式驗證方法，也就是能高度保證使用者身分的方法。Salesforce 產品支援數種強大驗證方法類型，包括 Salesforce Authenticator 行動應用程式和協力廠商驗證者應用程式。某些產品也支援使用實體安全性金鑰和內建驗證器。針對您的 MFA 實作，選擇最適合您業務和使用者需求的選項。

重要事項：為了滿足於 2022 年 2 月 1 日生效的 MFA 需求，使用者可以使用 Salesforce 產品支援的任何強式驗證方法登入。

Salesforce MFA 不允許使用透過電子郵件、SMS 簡訊或電話傳送的安全性問題或一次性密碼，因為這些方法本身具有漏洞。電子郵件認證可能會遭到盜用，而手機號碼可能會遭到 SIM 交換攻擊或被駭的行動裝置帳戶所攔截。

如果您有使用者透過單一登入 (SSO) 存取 Salesforce 產品，則 SSO 提供者的 MFA 服務可能會支援此處未討論的方法。有關滿足 MFA 要求的驗證方法指南，請參閱 [MFA 常見問題](#)。

讓我們來看看 Salesforce 產品所支援每種驗證方法的好處和考量事項。

Salesforce Authenticator	協力廠商驗證者應用程式	安全性金鑰*	內建驗證器*
聰明又簡單的行動應用程式，可讓使用者輕鬆連結至 Salesforce 帳戶。	應用程式會根據 OATH TOTP 演算法 (在 RFC 6238 中指定) 產生唯一的暫存驗證碼。	使用公用金鑰加密的實體裝置。	使用指紋、虹膜或臉部識別掃描，或使用 PIN 或密碼來驗證身分。

Salesforce Authenticator	協力廠商驗證者應用程式	安全性金鑰 [*]	內建驗證器 [*]
尺寸規格： iOS 和 Android 版的行動應用程式	尺寸規格： 適用於多個作業系統的應用程式	尺寸規格： 支援 WebAuthn 和 U2F 標準的 USB、Lightning 和 NFC 裝置	尺寸規格： 可透過裝置內建驗證器服務使用 (Windows Hello™、Touch ID®、Face ID® 等)
使用者體驗： - 向使用者的電話發出推送通知[*]來快速存取。 - 請參閱即時詳細資料來確認要求有效性。 - 使用點擊來拒絕詐欺要求。 - 從信任的位置自動化驗證 - 如果無法連線，則產生 TOTP 代碼。	使用者體驗： - 多種可供選擇的應用程式。 - 不需要連線。	使用者體驗： - 使用方式快速又簡單。 - 識別和拒絕詐欺要求。 - 不需要連線。 - 不需任何電池。	使用者體驗： - 使用方式快速又簡單。 - 無須應用程式。 - 使用者帳戶唯一的強大公用金鑰加密。
考量事項： 需要行動裝置。	考量事項： - 需要行動裝置。 - 請輸入當手動輸入代碼時可能發生的錯誤。 - 如果行動裝置時鐘未與 Salesforce 同步，則可能出現無效代碼。	考量事項： - 需要瀏覽器支援 (限 U2F)。 - 使用者可以將金鑰放在無人看管的位置或隨時插著電源。 - 購買、儲備裝置並將其散佈給使用者的營運費用。	考量事項： - 裝置、OS 和瀏覽器必須支援 FIDO2 WebAuthn 標準。 - 必須啟用並設定內建驗證器服務。 - 綁定至單一裝置。 - 支援生物識別所需的掃描器。
成本：免費	成本：免費與付費的選項	成本：大約 \$20 起	成本：若有需要，生物識別周邊設備最低 \$25 美元起
深入瞭解	深入瞭解	深入瞭解	深入瞭解

^{*} 注意：

❑ Salesforce Platform 上建立的產品不支援使用 NFC 規格的金鑰。

❑ Chromium 版的 Edge 瀏覽器不支援與 WebAuth 相容的安全性金鑰。

❑ 下列版本目前支援內建驗證器：[所有在 Salesforce Platform 上建立的產品](#)、Heroku、Marketing Cloud、Atrorama、MuleSoft Anypoint Platform 及 Tableau Online。

協力廠商驗證器應用程式

Salesforce 多因素驗證 (MFA) 支援使用產生時間型一次性密碼 (TOTP) 代碼的協力廠商驗證器應用程式。有多種可用的應用程式，包括免費版本。一些熱門選項包括：Google Authenticator™、Google Authenticator™ 和 Authy™。

協力廠商驗證器應用程式的 Salesforce MFA 需求

- 協力廠商驗證器應用程式必須使用 OATH 時間型一次性密碼 (TOTP) 演算法 (RFC 6238)。
- 所有 Salesforce 產品都支援協力廠商 TOTP 驗證器應用程式。

 **備註:** 考量 TOTP 桌面應用程式或瀏覽器擴充功能？建議改用行動驗證器應用程式、實體安全性金鑰或內建驗證器。這是因為這幾種驗證方法與使用者的筆記型電腦或工作站分開存在。因此，如果惡意使用者嘗試存取使用者的電腦，使用者的第二個因素也不會遭到破解。然而，如果桌面應用程式或瀏覽器擴充功能是適用於您使用者的唯一選項，您可以使用以下幾種方法來滿足 MFA 需求。

當登入時協力廠商驗證器應用程式的運作方式

若要使用此類驗證方法登入，使用者會從 TOTP 驗證器應用程式取得代碼。接著會在 Salesforce 登入流程期間輸入該代碼。

 **小祕訣:** 如果使用者已安裝 TOTP 應用程式供個人或企業使用，則使用者可以為 Salesforce 登入設定相同的應用程式。

背景

TOTP 驗證器應用程式會根據密碼金鑰 (僅使用者和服務知道，例如 Salesforce) 和目前時間產生臨時代碼。代碼有效時間為 30 秒，然後會產生新的代碼。

即使使用者的手機沒有資料或網路連線，TOTP 驗證器應用程式仍能產生代碼。

安全性金鑰

安全性金鑰是小型實體裝置，適用於多因素驗證 (MFA)，因為不需要安裝任何程式或輸入密碼，因此容易使用。若使用者沒有行動裝置，或是如果您的使用者所在工作位置無法使用電話，則此類方法是絕佳選項。安全性金鑰需要支援的瀏覽器，作為金鑰與您 Salesforce 產品之間的中介。常見的安全性金鑰包含來自 Yubico™ 的 YubiKey™ 和來自 Google™ 的 Titan™ 安全性金鑰。

安全性金鑰的 Salesforce MFA 需求

支援安全性金鑰的 Salesforce 產品：	所有產品，Tableau Online 除外
支援的尺寸規格：	USB-A、USB-C、Lightning、NFC*
支援的安全性標準：	FIDO2 WebAuthn 和 FIDO U2F
WebAuthn 金鑰支援的瀏覽器：	Chrome、Edge Chromium、Firefox、Safari
U2F 金鑰支援的瀏覽器：	Chrome (41 版或更新版本)、Edge Chromium

安全性金鑰在登入時的運作方式

安全性金鑰可加快 MFA 登入速度。使用者只需：

1. 將金鑰連接至電腦。
2. 按下金鑰按鈕以驗證其身分。

背景

WebAuthn 和 U2F 標準使用強大公用金鑰加密來保護使用者免受中間人攻擊和惡意軟體的攻擊。若要深入瞭解安全性金鑰的背景，請參閱 [WebAuthn 指南](#) 或 [FIDO U2F 網站](#)。

考量事項

* 在 Salesforce Platform 上建立的產品不支援 NFC 裝置。

內建驗證器

使用內建驗證服務 (例如 Windows Hello™、Touch ID® 或 Face ID®)，可輕鬆地使用多因素驗證 (MFA) 驗證。使用者可以使用指紋、虹膜或臉部識別掃描 (或在某些情況下，使用使用者在裝置作業系統中設定的 PIN 或密碼) 快速驗證其身分。此類驗證方法可簡化 MFA 要求，因為它依賴內建機制，而不需要使用者擁有個別驗證器應用程式或實體安全性金鑰。

 **小祕訣:** 如果無法使用行動驗證器應用程式，則內建驗證器是相當好的選擇。例如，針對公司未提供行動裝置的使用者，請考慮此選項。而且在 PCI 標準環境或使用工作裝置沒有實體安全性金鑰連接埠的狀況下，使用內建驗證器可能更加合理。

內建驗證器的 Salesforce MFA 需求

 **重要事項:** 目前僅下列產品支援內建驗證器：[在 Salesforce Platform 上建立的所有產品](#)、Heroku、Marketing Cloud Intelligence (由 Datorama 提供技術支援) 及 MuleSoft Anypoint Platform。

- 使用者裝置、作業系統和瀏覽器必須支援 FIDO2 WebAuthn 標準。
- 非 Chromium 版的 Edge 瀏覽器不支援內建驗證器。
- 若要使用生物識別驗證，裝置必須包含內建驗證服務支援的指紋、虹膜或臉部識別掃描器。
- 對 MFA 註冊此類型驗證器之前，必須先啟用並設定使用者的內建驗證器服務，才能透過生物特徵、PIN 或密碼驗證其身分。
- 登入 Salesforce 行動應用程式時無法使用內建驗證器。
- 內建驗證器不適用於 Experience Cloud 網站。
- 透過 API 存取 Salesforce 的使用者無法使用內建驗證器來驗證其身分。

 **備註:** 此類驗證方法會與使用者的特定裝置綁定。如果使用者從多台電腦 (例如桌上型電腦和筆記型電腦) 登入，則必須在每個系統上都註冊內建驗證器。如果並非所有的使用者系統皆支援內建驗證器，則這些驗證器也應註冊替代驗證方法。

若要深入瞭解，請參閱 [FIDO2：Web 驗證 \(WebAuthn\)](#) 或使用者內建驗證器的文件。

內建驗證器在登入時的運作方式

此類方法提供最簡單的 MFA 登入體驗。使用者輸入 Salesforce 使用者名稱和密碼之後，內建驗證器會提示其使用生物識別、PIN 或密碼識別碼。接著便可登入。

背景

註冊內建驗證器會建立對使用者帳戶唯一的私人和公用金鑰組。私人金鑰會安全地儲存在使用者的桌面或行動裝置上，並由使用者的生物識別資料保護。私人金鑰與使用者的生物識別資料一律不會離開使用者的裝置，且一律不會與 Salesforce 共用。當使用者登入其帳戶時，瀏覽器會呼叫裝置的作業系統，以啟動使用者註冊的內建驗證器。根據使用者瀏覽器和作業系統，使用者可使用如 Touch ID、Face ID 或 Windows Hello 等驗證器來驗證其身分。

符合 WebAuthn 的內建驗證器可抵抗網路釣魚和中間人攻擊。其主要原因是因為使用者的私人金鑰繫結到與使用者帳戶相關聯的網域。例如，假設使用者遭到誘騙使用惡意網站。當網站提示內建驗證器批准登入要求時，驗證器會識別網站的網域並非預期網域，並阻止使用者登入。

多因素驗證的評估選項和要求

啟用多因素驗證 (MFA) 的步驟很簡單直接。在深入瞭解前，請用一些時間來瞭解現有的驗證系統，並識別 MFA 解決方案的要求。如果您從評估期間開始，您可以收集配合主管要求所需的資料，並開發專案計畫。

檢閱 Salesforce 目前具備的驗證解決方案

開始規劃多因素驗證 (MFA) 實作之前，請瞭解目前使用 Salesforce 產品的驗證方式。您可能要讓 MFA 配合或整合您已經使用的其他驗證解決方案，例如單一登入 (SSO)。

預覽多因素驗證

作為評估流程的一部分，查看多因素驗證 (MFA) 的運作方式與使用者體驗對您很有幫助。透過為您的幾位 Salesforce Champion 開啟 MFA，然後收集其回饋意見來取得預覽。這些意見可協助您預測其他的使用者使用 MFA 時會有何感受，以及您是否應計畫如何運用行銷與教育來降低使用者的抗拒。您的 Champion 也可以對訓練和上線支援的類型提供回饋意見，這些回饋意見可在您更大範圍地推出 MFA 時協助使用者成功完成。此外，另一個優點是您可以確切瞭解實作 MFA 所需的作業，這有助於告知您推出與實作計畫。

決定 MFA 的業務及使用者要求

若要定義最適合您公司的多因素驗證 (MFA) 實作，請決定業務要求。並且瞭解您的使用者對正面且具生產力體驗的要求。這些條件有助於您瞭解實作中應支援的 MFA 驗證方法。

針對 MFA 實作執行使用者清點

透過清點所有 Salesforce 使用者來瞭解多因素驗證 (MFA) 專案的工作層級。識別現有的使用者和角色類型，例如業務使用者、管理員、承包商、合作夥伴和非人類帳戶。並將對指派給每個使用者的權限進行分類。

評估組織和使用者對 MFA 的整備狀況

找出是否有任何您必須在啟用多因素驗證 (MFA) 前先處理的相依性、先決條件或阻礙因素。預先解決這些問題，或在 MFA 專案的實作階段中計畫解決問題。

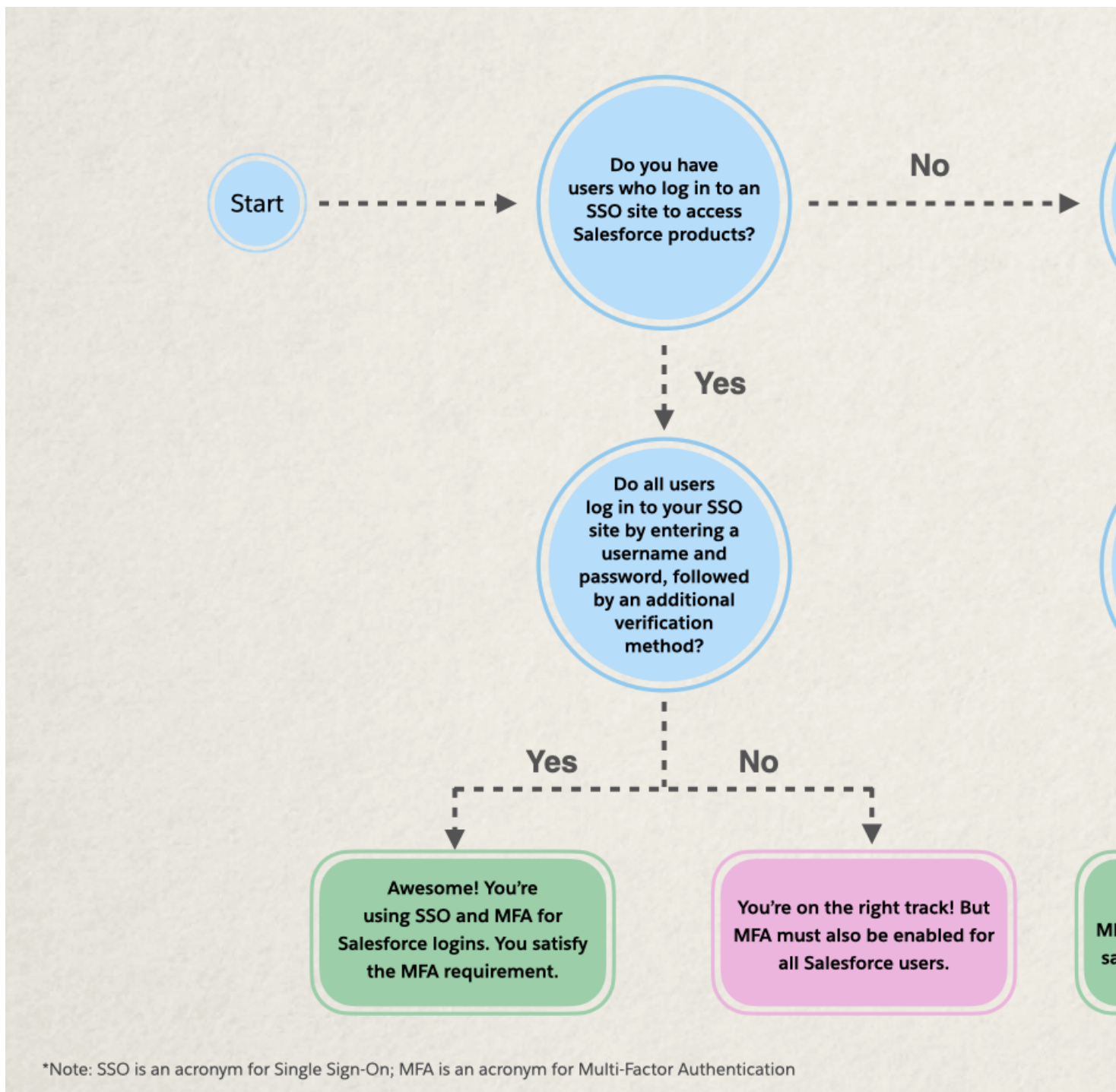
說服使用 MFA 的理由

當您完成評估多因素驗證 (MFA) 的選項和需求時，請與主管及受影響的專案關係人分享結果。以解決目前威脅形勢風險作為理由，說服他們使用 MFA。同時說明為 Salesforce 登入增加另一層防護，可讓公司和客戶獲得哪些好處和投資報酬率。您需要此群組支援為 MFA 計畫開綠燈，並為工作分配資源。

檢閱 Salesforce 目前具備的驗證解決方案

開始規劃多因素驗證 (MFA) 實作之前，請瞭解目前使用 Salesforce 產品的驗證方式。您可能要讓 MFA 配合或整合您已經使用的其他驗證解決方案，例如單一登入 (SSO)。

使用此圖表來開始評估您的組態。如果您已為所有使用者啟用 MFA，那麼您做得很好！



 **小祕訣:** 想要瞭解您目前或計畫的 MFA 實作是否符合 2022 年 2 月 1 日起生效的 MFA 需求？請查看 MFA Salesforce 客戶網站上的 [MFA Requirement Checker \(MFA 要求檢查工具\)](#)。

請注意，MFA 有時候會與名為身分驗證 (或裝置啟用) 的功能混為一談。若使用此功能，使用者從無法辨識的瀏覽器或裝置存取 Salesforce 時，系統會要求使用者提供驗證方法。但 MFA 可提供更好的保護，因為其會要求使用者在每次登入時提供強大的驗證方法。

SSO 是改善使用者登入體驗的絕佳選項，也可降低某些與低強度或重複使用之密碼相關的風險。但 SSO 本身不會提供您透過 MFA 取得的保護。單獨依賴使用者認證的 SSO 實作，可能會讓使用者帳戶受到常見的攻擊 (例如網路釣魚或認證填充)。如果您目前對 Salesforce 登入使用 SSO，請確定已對所有 Salesforce 使用者啟用 MFA：

- 如果是建立在 Salesforce Platform 上的產品，您可以[使用 Salesforce 中提供的 MFA 功能](#)，或使用 SSO 提供者的 MFA 服務。
- 如果是所有其他的 Salesforce 產品，請使用 SSO 提供者的 MFA 服務。

滿足 MFA 需求的最佳全方位選項是將 MFA 與 SSO 合併，讓您能夠提供 MFA 的增強安全性，以及 SSO 的便利性和易用性。。

預覽多因素驗證

作為評估流程的一部分，查看多因素驗證 (MFA) 的運作方式與使用者體驗對您很有幫助。透過為您的幾位 Salesforce Champion 開啟 MFA，然後收集其回饋意見來取得預覽。這些意見可協助您預測其他的使用者使用 MFA 時會有何感受，以及您是否應計畫如何運用行銷與教育來降低使用者的抗拒。您的 Champion 也可以對訓練和上線支援的類型提供回饋意見，這些回饋意見可在您更大範圍地推出 MFA 時協助使用者成功完成。此外，另一個優點是您可以確切瞭解實作 MFA 所需的作業，這有助於告知您推出與實作計畫。

- 選擇您的 **Salesforce Champion**：選取一或多個 Salesforce 使用者參與早期預覽或試用版 MFA。Champion 是您的超級使用者一也就是對於 Salesforce 懷抱熱情且定期提供改善建議的人。若缺乏人選，請選擇能直言表達如何改善您業務流程的人，或第一個採用新技術的人。
- 幫您的 **Champion** 做好準備：說明當啟用 MFA 時登入流程如何運作，並提供註冊 MFA 驗證方法的指引。建議使用 Salesforce Authenticator 行動應用程式，因為其不但免費且易於設定。但如果您計畫要在實作中支援安全性金鑰或其他方法，請要求您的 Champion 也註冊這些方法。
- 為您的 **Champion** 啟用 **MFA**：針對每個 Salesforce 產品，遵循步驟以為特定使用者啟用 MFA，[為您的租戶啟用](#)
 - [在 Salesforce Platform 上建立的產品](#) (包括 Sales Cloud 和 Service Cloud)
 - [B2C Commerce Cloud](#)
 - [Heroku](#)
 - [Marketing Cloud 參與](#) (由電子郵件、傳訊和旅程支援)
 - [Marketing Cloud Intelligence](#) (由 Datorama 提供技術支援)
 - [Marketing Cloud Social](#)
 - [MuleSoft Anypoint 平台](#)
 - [Quip 產品](#)
 - [Tableau Online](#)
- 取得回饋意見：與您的 Champion 談一談他們的體驗。他們是否瞭解如何註冊 MFA 的驗證方法？他們在使用其註冊方法登入時是否順利？他們對登入流程的變更有何感想？

- 在規劃階段中使用洞察：將學習到的知識納入推出和變更管理計畫，包括要建立的訓練和上線資源類型。請參閱[計畫多因素驗證推出](#)以取得詳細資訊。

另請參照：

[使用 MFA 首展套件取得可自訂的範本](#)

決定 MFA 的業務及使用者要求

若要定義最適合您公司的多因素驗證 (MFA) 實作，請決定業務要求。並且瞭解您的使用者對正面且具生產力體驗的要求。這些條件有助於您瞭解實作中應支援的 MFA 驗證方法。

以下是要考慮的一些潛在要求。

現有的驗證解決方案	貴公司是否針對其他系統使用現有的 MFA 解決方案，例如 Okta 或 Duo？如果您的 Salesforce 使用者已經使用 MFA 登入其他應用程式，請查看您是否可以使用相同的解決方案整合 Salesforce 產品。這麼做可縮減實作 MFA 時的時程表和成本。而且可將摩擦和變更管理需求降到最低，因為使用者已針對 MFA 登入進行訓練。 您的 Salesforce 產品是否與 SSO 解決方案整合？如果您對 Salesforce 登入使用 SSO，請確定已為所有 Salesforce 使用者啟用 MFA。 - 如果是建立在 Salesforce Platform 上的產品，您可以使用 Salesforce 中提供的 MFA 功能，或使用 SSO 提供者的 MFA 服務。 - 如果是所有其他的 Salesforce 產品，請使用 SSO 提供者的 MFA 服務。
安全性需求	與您的安全性及 IT 小組合作，瞭解 MFA 可如何配合您公司的安全性目標及需求。瞭解是否有任何企業要求，以及您必須遵循哪種應用程式測試或評估流程。
法律與法規要求	當使用者向系統進行驗證時，您公司對客戶和其他專案關係人的法律承諾為何？ 也請考慮當地和其他法規需求及這些需求如何影響 MFA 實作。例如，一些法規需求可能包含對將應用程式下載到特定裝置的限制。
合規要求	哪種審核要求會受 MFA 實作影響或觸發？您是否會在未來 12 個月內開始實施可能受到 MFA 影響的任何新合規制度？
裝置需求	考量您產業或公司的行動裝置原則是否會對 MFA 實作產生任何限制。例如，以應用程式為基礎的行動解決方案是否有效，或是您必須提供實體安全性金鑰給使用者？ 如果可以選擇使用行動應用程式，貴公司是否會提供公司裝置？或者您是否必須在自攜裝置 (BYOD) 原則中整合 MFA 資料的使用情形和補償指導方針？
使用者考量	瞭解 MFA 會如何影響貴公司的各種角色和小組。例如： 您的使用者是否在連線能力有限的位置出差或辦公？

	- 您的使用者 (例如有存取需求的協力廠商電話服務中心工作人員或員工) 在驗證方法上是否有特殊需求或限制？ - 哪些驗證方法對您的使用者工作流程來說最沒有侵害性？ 我們建議您的實作中應支援多個驗證方法，如此每個人員都可以選擇最適合他們的選項。
預算考量事項	將 MFA 實作的成本考量在內相當實用，此外也需要推出後作業及使用者支援功能的預算。 您不需支付額外的費用，Salesforce 產品就已提供 MFA，且 Salesforce Authenticator 應用程式也是免費的。但是如果部分或所有使用者不能使用行動應用程式選項，則應考量購買及分配安全性金鑰的費用。

定義 MFA 實作的使用需求

當您找出您的需求並瞭解使用者的需求後，請利用這些條件來決定您 MFA 實作所要包含的驗證方法。我們知道您的使用者和使用個案千變萬化，所以我們支援數種不同類型的強大驗證方法。請參閱[多因素驗證的驗證方法](#)，以取得每個方法的優點及考量比較。

 **小祕訣：**您可以將每個人都使用的一種方法標準化，或是您可以支援多個選項，並讓使用者選擇。在決定要採取的方法時請考量代價。當每個人都使用相同的方法時，即可簡化您的上線與每日管理責任。讓使用者挑選最適合他們的方法，即無需尋找一體適用的解決方案。並且可輕鬆地符合您所有需求。此外，如果使用者為他們自己設定多個驗證方法，就比較不會被鎖在 Salesforce 之外。

另請參照：

[計畫多因素驗證首展](#)

針對 MFA 實作執行使用者清點

透過清點所有 Salesforce 使用者來瞭解多因素驗證 (MFA) 專案的工作層級。識別現有的使用者和角色類型，例如業務使用者、管理員、承包商、合作夥伴和非人類帳戶。並將對指派給每個使用者的權限進行分類。

此演練有幾個好處。您可以：

- 識別所有擁有特權的使用者，包含 Salesforce 管理員和具有高層級應用程式和敏感資料存取權的員工。當您推出 MFA 時，這些使用者是您最先考慮的優先對象，因為如果他們遭到入侵，則會構成最大的風險。
- 決定使用者的邏輯群組 (如果您計畫分階段推出 MFA)。
- 評估對使用者帳戶套用「最低特權」原則的應用情形。安全性最佳作法就是限制使用者擁有執行其工作所需的最小權限集。如此一來，如果攻擊者取得帳戶存取權，對您環境造成傷害的風險就會比較低。使用者清點會顯示可降低權限的部分，進而減少具有特權的使用者數量。我們建議每季執行一次此演練。如果距演練已經過一段時間，則您的 MFA 專案就是立即排程檢閱的重要理由。

 **小祕訣：** 從[可下載的 MFA 首展套件](#)中取得使用者庫存範本。

另請參照：

[針對在 Salesforce Platform 上建立的產品識別有特權的使用者](#)

[計畫多因素驗證首展](#)

針對在 Salesforce Platform 上建立的產品識別有特權的使用者

當您評估組織多因素驗證 (MFA) 時，清點 Salesforce 使用者是相當實用的作法。此步驟可協助您識別誰是有特權的使用者、提供您規劃階段性推出的資料，以及提供專案工作量的洞察。推出 MFA 時，Salesforce 管理員和其他特權使用者是最優先的對象。您可使用數種工具來清點使用者群。

僅適用於：在 Salesforce Platform 上建立的產品，包括 Sales Cloud、Service Cloud、Analytics Cloud、B2B Commerce Cloud、Marketing Cloud—Audience Studio、Marketing Cloud—Account Engagement、Experience Cloud、Platform、產業產品 (Consumer Goods Cloud、Financial Services Cloud、Government Cloud、Health Cloud、Manufacturing Cloud、Philanthropy Cloud) 及 Salesforce Essentials

提供版本：**Essentials、Group、Professional、Enterprise、Performance、Unlimited、Developer 及 Contact Manager Edition**

 **小祕訣：** 若要瞭解此演練的優點，請參閱[為您的 MFA 實作執行使用者清點](#)。

從[可下載的 MFA 首展套件](#)中取得使用者庫存範本。

特權使用者為：

- Salesforce 管理員 (定義為具有「自訂應用程式」和「修改所有資料」使用者權限的使用者)
- 具有下列任一使用者權限的使用者：
 - 自訂應用程式
 - 管理使用者
 - 修改所有資料
 - 全部檢視

以下是可用來識別組織的管理員和其他特權使用者的一些工具。

- [Salesforce Optimizer](#)
- [Salesforce AppExchange 中的設定檔和權限集協助程式](#)
- [查詢設定檔和權限集物件](#)

使用 Salesforce Optimizer 尋找 Salesforce 管理員

Optimizer 是識別組織中所有管理員的最簡易方式。

1. 進入 Lightning Experience 中的「設定」，在「快速尋找」方塊中輸入 *Optimizer*，然後選取「**Optimizer**」。
2. 在「Salesforce Optimizer 應用程式」區段中，按一下「開啟 **Optimizer**」。

3. 按一下「執行 **Optimizer**」。Optimizer 需要一點時間來產生結果。
4. 在「功能」資料欄中，按一下「管理員權限」。
5. 檢閱目前有管理員權限的使用者清單。

使用「設定檔和權限集協助程式」來尋找所有特權使用者

使用 AppExchange 中的「設定檔和權限集協助程式」工具來識別組織中所有特權使用者。該工具會針對特定使用者權限來搜尋您組織的設定檔和權限集，然後顯示擁有該權限的所有使用者。

1. 從 AppExchange 下載及安裝[設定檔和權限集協助程式](#)封裝。
2. 從 App Launcher 選取「權限集協助程式」。
3. 按一下「權限分析器」索引標籤。
4. 在側列中執行這些設定：

依欄位分析	選取「權限」
權限類型欄位	選取「使用者」
權限欄位	選取下列其中一個特權：自訂應用程式、管理使用者、修改所有資料或全部檢視

應用程式會顯示所有已獲派所選權限的使用者 (無論是透過權限集或設定檔)。

重複這些步驟以搜尋每一個特殊使用者權限。

查詢您組織的資料

您可以直接透過 API 和 SOQL 來清點權限集和設定檔中獲派的使用者權限。此方法提供最具彈性的資料匯出和分析方式。

若要透過設定檔查詢獲派下列四個特權中任一項的所有使用者：

```
SELECT Id,Username, Profile.Name, Profile.PermissionsCustomizeApplication,
Profile.PermissionsModifyAllData, Profile.PermissionsManageUsers,
Profile.PermissionsViewAllData
FROM User
WHERE IsActive = true and (Profile.PermissionsModifyAllData=true
OR Profile.PermissionsCustomizeApplication=true
OR Profile.PermissionsManageUsers=true)
```

若要透過權限集查詢獲派下列四個特權中任一項的所有使用者：

```
SELECT Assignee.Id, Assignee.Username, Assignee.Profile.Name, PermissionSet.Label,
PermissionSet.PermissionsCustomizeApplication,
PermissionSet.PermissionsModifyAllData, PermissionSet.PermissionsManageUsers,
PermissionSet.PermissionsViewAllData
FROM PermissionSetAssignment
WHERE Assignee.IsActive = true AND PermissionSet.IsOwnedByProfile=false AND
(PermissionSet.PermissionsModifyAllData=true
```

```
OR PermissionSet.PermissionsCustomizeApplication=true
OR PermissionSet.PermissionsManageUsers=true)
```

評估組織和使用者對 MFA 的整備狀況

找出是否有任何您必須在啟用多因素驗證 (MFA) 前先處理的相依性、先決條件或阻礙因素。預先解決這些問題，或在 MFA 專案的實作階段中計畫解決問題。

備註： 啟用 MFA 前，務必解決任何使用中共用帳戶或認證的問題。儘管 Salesforce 原則禁止共用使用者認證，但這種情況仍會發生。然而，此作法與 MFA 不相容，因為每個使用者必須將唯一的驗證方法與其 Salesforce 帳戶相連才能登入。如果多個使用者共用單一帳戶，則在 MFA 啟用後，僅其中一人能夠登入該帳戶。

如果您在為存取 Salesforce 的每個人員設定唯一帳戶時需要他人協助，請連絡帳戶主管或銷售小組。或者請參閱[管理帳戶的 Salesforce Checkout](#) 和[自助式服務](#)。

說服使用 MFA 的理由

當您完成評估多因素驗證 (MFA) 的選項和需求時，請與主管及受影響的專案關係人分享結果。以解決目前威脅形勢風險作為理由，說服他們使用 MFA。同時說明為 Salesforce 登入增加另一層防護，可讓公司和客戶獲得哪些好處和投資報酬率。您需要此群組支援為 MFA 計畫開綠燈，並為工作分配資源。

若要向使用者說明原因並取得其對 MFA 推出的贊同：

- 說明未使用 MFA 時對業務造成的風險和潛在影響。提供資料說明常見安全性威脅的風險和後果，尤其是對您的市場和產業來說。
- 說明您公司能夠從 MFA 新增的安全性中實現的好處和投資報酬率 (ROI)。
- 討論您對於 MFA 實作的建議。
- 用能夠引起受眾共鳴的術語來闡述問題，並談論其優先任務。

小祕訣： Salesforce 委託 Forrester Consulting 進行 [Salesforce 多因素驗證的整體經濟影響 \(Total Economic Impact™\)](#) 研究，以協助客戶瞭解採用 MFA 的好處。使用此研究，有利於您的領導階層與專案關係人瞭解 MFA 如何為您的損益底線帶來價值。想要預告結果嗎？組織可在 3 年內達成高達 164% 的 MFA 投資報酬率，並在 6 個月內獲得收益。



討論到 MFA 的好處時，請考慮下列幾點：

資料保護	MFA 可透過讓攻擊者難以盜用使用者的認證來協助您保護極度珍貴的 Salesforce 資料。
客戶安全性	身為客戶資料的管理者，使用強大的安全性控制措施(例如 MFA)，有助於降低業務的下游影響風險。您可以向客戶保證您的安全狀況。
安全性最佳作法	使用 MFA 表示您符合全球公認的常見產業趨勢，此趨勢被視為降低安全性風險的最佳作法。
公司責任	隨著業務不斷發展，您必須為客戶、專案關係人和員工負起保護產品資訊和業務的責任。
業務價值	說明 MFA 如何提升客戶信心、保護公司聲譽、避免網站或應用程式停機，以及防止因資料洩漏造成的成本和責任，藉此將「改善的安全性」等 IT 好處轉換為業務價值。

示範 MFA 可如何協助達成其他業務優先任務或目標也相當重要。例如：

法律要求	您是否有驗證、使用者安全性或治理業務的資料遺失要求、您對繼承安全性之客戶的承諾，或是您對專案關係人的承諾？MFA 是達成這些目標的有效方式。
合規要求	您的組織可能在某種審查結構下運行，而許多這些結構都包含驗證要求。您也可能具有必須遵循的安全性原則，您可以透過 MFA 來符合這些原則。
未來和不斷演進的要求	考量在未來 12 個月內的業務目標。您是否計畫將業務擴大到新的客群或是需要增強安全性的市場？計畫的變更是否可從 MFA 中受益？ 也請考量您的安全性目標。MFA 實作是否協助您符合目前或新興的企業安全性要求？MFA 可能是最強大的降低新興風險的選項，或是計畫安全性目標的解決方案。



小祕訣：如需協助建立個案，請查看[可下載的 MFA 首展套件](#)中包含的可自訂 MFA 簡報組。

另請參照：

[決定 MFA 的業務及使用者要求](#)

[計畫多因素驗證首展](#)

計畫多因素驗證首展

在完成評估期間以瞭解您對多因素驗證 (MFA) 的選項和要求後，您就可以擬定自己的專案計畫。

為了確保順利推出，我們建議解決這些問題。

- 專案小組的角色和責任。
- 如何以及何時向使用者推出 MFA 的策略。

- 在整個專案中要採用的變更管理策略。
- 如何在 MFA 啟用後支援使用者。
- 設定和測試實作的要求、接受條件和排程。

 **小祕訣:** 如需協助計畫 MFA 首展，請查看[可下載的 MFA 首展套件](#)中的可自訂範本和指南。

組成 MFA 專案小組

您需要組成小組，才能推出任何 Salesforce 專案。如需多因素驗證 (MFA) 推廣活動，請讓小組立即開始作業。讓整個組織的人員都參與在內，包含安全性和 IT 小組、業務專案關係人，甚至可能是您公司的通訊部門。

組成一個由執行贊助者帶領的專案小組，該贊助者不僅支援 Salesforce 實作，還瞭解保護帳戶存取權的重要性。確保納入貴公司中所有受影響的部門領導者。這個步驟很重要，因為您需要執行支援來協助定義願景，最終得以批准和支援該專案。

設想您的安全性和 IT 小組在專案中扮演的角色。例如，您的實作工作是否需要批准和登出？或者，也許這些小組中的某人可以積極參與計畫和實作階段。

 **小祕訣:** 提早並經常納入正確的專案關係人，可確保所有客群都涵蓋在內。

若要協助定義和實作策略與專案計畫，請考量這些小組成員：

- 關鍵業務使用者可作為擁護者，並提供「客戶的聲音」
- Salesforce 管理員
- 安全性與 IT 合作夥伴
- 變更管理商機
- 報告商機
- 產品、工程和技術寫作商機

定義 MFA 首展策略

決定您將如何建立結構與執行多因素驗證 (MFA) 推出。擬定適用於您公司規模、業務目標，以及您使用之 Salesforce 產品的策略。

 **備註:** 在此主題中的指導方針不適用於單一登入 (SSO) 登入、API 登入，或是為存取您 Salesforce Experience Cloud 網站或電子商務網站的客戶設定 MFA 需求。

向使用者推出 MFA 的策略

執行推出的方法有兩種。同時為所有使用者開啟 MFA。或是在經過數天、數週或數月後為一群使用者開啟 MFA。

- 如果您只有少數 Salesforce 使用者，則最有效率的作法可能是在同一天向所有人推出 MFA。
- 如果您的使用者群夠大，以至於無法同時為所有人啟用 MFA，或是如果為所有使用者準備單一啟動日期會延遲您可以開始啟用 MFA 的時間，則我們建議您採取分階段的方法。

若您尚未使用您的某些 Salesforce Champion 預覽 MFA，請考慮使用小型試用版來開始推出。如此一來，您就可以測試推出流程和使用者的體驗。收集回饋意見，瞭解哪些是有效的、哪些需要調整，以及在資源或支援方面存在的差

距，好讓正式推出順利進行。您可以將試驗重點放在管理員使用者上，或是針對小組間的跨區段使用者進行試驗，以確認所有受眾都能正常使用。

瞭解您的使用者是誰

開始您的推出策略之前(尤其是當您採用分階段方法時)，請先清點現有使用者，包括其目前的權限和角色。使用此演練來識別您的管理員和其他特權使用者，並取得其他洞察來協助您定義邏輯推出群組。如需相關祕訣，請參閱[為您的 MFA 實作執行使用者清點](#)。

決定誰先進行 MFA

針對分階段的首展，計算您需要多少群組。然後找出每個群組要包含的人員。請記住，自 2022 年 2 月 1 日起，登入使用者介面的所有使用者，包括管理員、公司使用者、承包商、合作夥伴和外部廠商，都必須使用 MFA。

- 您的第一優先事項是為擁有特權的使用者新增 MFA 要求，因為如果攻擊者能夠存取這些類型的帳戶，您將會面臨更高的風險。從對所有 Salesforce 管理員推出 MFA 開始，然後是任何可存取敏感資料或可變更產品操作方式的使用者。這類使用者通常都擁有 Salesforce 專業知識，因此您可以比其他人更快地將這些使用者上線。
- 接下來，對有重要角色或功能的使用者啟用 MFA。會因為失去 Salesforce 存取權而可能影響您業務的任何使用者，也是前期群組的最佳候選人。
- 考量如何與何時應對必須存取 Salesforce 產品的承包商、合作夥伴和其他外部使用者啟用。
- 最後，對剩下的使用者推出 MFA。尋找邏輯群組，例如特定小組上的所有使用者，或是業務單位或地理位置中的任何人。

這裡提供一些額外考量事項：

- 如果您已實作單一登入 (SSO)，請將 MFA 需求新增至當 SSO 無法使用時管理員使用的直接登入備用帳戶。
- 如果您會與需要 Salesforce 環境存取權的協力廠商電話服務中心、創意機構或諮詢公司合作，請制定如何將 MFA 要求套用到外部使用者的計畫。

另請參照：

[決定 MFA 的業務及使用者要求](#)

[評估組織和使用者對 MFA 的整備狀況](#)

[針對 MFA 實作執行使用者清點](#)

[預覽多因素驗證](#)

決定 MFA 變更管理策略

忙碌的使用者不一定能接受變更。變更管理策略有助於協助使用者瞭解多因素驗證 (MFA) 的價值，並協助其做好進行 MFA 登入的準備。您需要制訂計畫來預先推廣認知，以及讓使用者上線。在計畫階段期間奠定基礎，可以為您提供藍圖，讓您在開始變更管理活動時可以遵循。



小祕訣：如需協助開發變更管理計畫，請查看[可下載的 MFA 首展套件](#)。其提供詳細的變更管理指南，以及各種變更管理範本，可協助您進行通訊、行銷、訓練和上線。

變更影響評估

從執行[變更影響評估](#)開始。您可以使用此步驟來瞭解使用者對MFA的想法。您也可以深入瞭解人們對於每次登入Salesforce時的額外驗證步驟有何感想。

使用此評估中的結果來計算當您推出MFA時，遭到使用者拒絕的機率。使用者可能會將額外的驗證步驟視為不方便的動作，而不是感謝加強帳戶安全帶來的好處。掌握使用者對此主題的心態，就能瞭解需要投資多少行銷和教育才能讓每個人都投入MFA。

變更管理策略

將您的發現轉變為變更管理策略，專注於獲得Salesforce使用者的認同，並使MFA快速流暢地整合至每日生活。可靠的措施包含這些元素。

溝通和行銷活動	推廣認知並讓使用者感到安全且有所幫助，而不是感到不便。
訓練及上線資源	讓使用者更清楚瞭解必須做的事、必須執行的時間，以及在他們卡住時如何取得協助。
啟動日支援	讓支援小組做好準備，以協助使用者處理啟動日問題和進行疑難排解。
成功度量	定義MFA專案是否成功的測量方式。與主管和專案關係人合作，以決定用來衡量使用者採用情況的度量。

另請參照：

[讓使用者做好使用多因素驗證的準備](#)

建立 MFA 支援計畫

多因素驗證 (MFA) 專案不會在您的啟動日結束。您需要可處理啟動後工作的支援計畫，包括管理 MFA 作業及協助使用者解決驗證問題。建立這些責任的擁有者也很重要。

以下是 MFA 支援計畫的一些建議和考量。

支援小組	設想誰會有須每日進行的作業，例如服務台或協力廠商服務提供者。找出支援小組中的正確連絡人，並邀請他們在您的專案計畫中提供意見。
原則與流程	定義並記錄支援小組處理常見問題的方式，例如： - 解決失敗的驗證嘗試和帳戶鎖定的登入問題。 - 如果使用者遺失或忘記其驗證方法，請協助他們復原存取權。 - 為新使用者啟用 MFA。 更新使用者上線流程，讓新進員工在第一天上班時就能使用 MFA。確保新進員工上線流程中包含 MFA 註冊協助。
訓練	決定將 MFA 知識授與支援小組的方式。考量舉辦訓練會議。優先建立支援工作人員需要的文件，以針對使用者問題進行疑難排解和解決問題。

操作預算	制定管理 MFA 實作的預算。針對啟動 MFA 後前幾週可能會有較多支援個案的情況制定計畫。 如果您使用安全性金鑰，請考量維護這些裝置供應的成本，以及將替代金鑰分送給使用者的成本。
------	--

存取復原流程

有些使用者可能會在某些時間點遺失或遺忘其驗證方法。詳細記載的復原流程是 MFA 支援計畫的重要部分 (對於管理員和一般使用者來說都是如此)。建立可降低方法遺失相關風險的流程，並快速還原使用者的 Salesforce 存取權。

 **小祕訣:** 請將復原流程設定得簡單好用，而且不會讓使用者感到被責備，如此使用者就會放心地即時回報其遺失裝置或驗證方法。

請考慮將這些步驟建置到復原流程中：

- 結束使用者目前的工作階段。
- 中斷與遺失驗證方法的連接。
- 重新建立登入存取權。
- 審查使用者的帳戶活動來監看任何異常活動。
- 如果使用者驗證方法遺失或遭到竊取，請指引他們完成取得替代方案的流程。

此外也具備 Salesforce 管理員適用的存取復原計畫！

確定您的存取復原計畫考量到 Salesforce 管理員有可能遭到鎖定或失去對其驗證方法的存取權。如果您是 Salesforce 環境中的唯一管理員，您必須具備一個針對您制定的特殊復原計畫！請考慮下列最佳作法：

- 每位管理員應註冊至少兩個驗證方法。
- 將備份安全性金鑰保留在工作場所中安全的地方。
- 除了您自己，請確定至少還有另一位值得信任的使用者擁有管理使用者和 MFA 設定的權限 (包括「管理使用者介面中的多因素驗證」使用者權限)。如此一來，如果您遭到鎖定，另一位使用者也可以還原您的存取權。

另請參照：

[準備好支援您的 MFA 實作](#)

[支援 MFA 實作](#)

[復原 MFA 已啟用使用者的存取權 \(適用於在 Salesforce Platform 上建立的產品\)](#)

定義 MFA 實作和測試計畫

以下是有助於在多因素驗證 (MFA) 中定義實作及測試步驟的一些建議和指引。

專案排程	挑選您的啟動日 (如果您是分階段推出的話，則會有多個日期)。然後為您的 MFA 專案建立排程。包括將驗證方法和上線文件分配給使用者的里程碑。 查看 Salesforce 藍圖，避免和可能與您推出動作競爭的任何專案同時啟動。與領導階層小組合作來清除障礙，像是與可能奪走焦點或竊取資源的非 Salesforce 專案。
支援的驗證方法	選擇您在實作中計畫要支援的驗證方法。記錄將這些方法散佈給使用者的流程和時程表。 如果您支援實體安全性金鑰，請在啟動日前保留足夠的時間，讓使用者接收金鑰。
啟用步驟和需求	定義解決以下項目的方式：任何您在專案的評估階段期間找到的相依性、先決條件或阻礙因素。 記錄為使用者開啟 MFA 將採取的步驟。請參閱為使用者啟用 MFA 第 34 頁來取得詳細資料。
測試計畫和接收條件。	建立接收條件，並記錄您測試 MFA 實作的方式。 建議您在計畫中執行啟用步驟。然後為每個驗證方法完成註冊流程，以確保您可以成功地連線到 Salesforce 帳戶並登入。  小祕訣： 使用測試環境或帳戶來避免將任何人鎖在生產環境之外的可能性。如果無法使用測試環境，我們建議為測試使用者或是在生產環境中的非關鍵角色啟用 MFA。接著執行測試步驟。 從可下載的 MFA 首展套件取得測試計畫範本。 驗證您的復原流程能如預期般運作也是個好主意。執行您在 MFA 支援計畫中定義的流程。

另請參照：

[決定 MFA 的業務及使用者要求](#)

首展階段：準備啟動多因素驗證

隨著專案計畫準備就緒並與專案關係人保持一致，下一步就是展開工作，以向 Salesforce 使用者提供多因素驗證 (MFA)。現在是時候讓使用者準備好使用 MFA 登入，並制定實作和測試計畫。如此您就做好啟動 MFA 的準備。如果您正逐步向使用者群組推出 MFA，請在此階段重複一些活動，直到每個人都使用 MFA 為止。

[讓使用者做好使用多因素驗證的準備](#)

若沒有適當的環境，忙碌的使用者可能會覺得多因素驗證 (MFA) 會拖慢他們，而不是增加價值。實作您的變更管理策略來協助使用者瞭解 MFA 的重要性，並提供流暢的上線體驗。您的目標是透過溝通、訓練甚至是一些行銷來讓每個人參與及接受訓練。

實作多因素驗證

除了執行變更管理活動，現在正是開始多因素驗證 (MFA) 實作的時機。啟用 MFA 會自動將驗證挑戰新增至登入流程，因此您想要將該步驟延後至排程的啟動日。讓我們看一看我們在這個階段建議的其他實作相關活動。

啟動多因素驗證

當重要的日子來臨時，請為使用者啟用多因素驗證 (MFA)。然後發起啟動日活動來確保每個人都能獲得所需的支援。如果您要全面使用 MFA，請針對所有使用者將其開啟。如果您採取的是分階段方法，請立即為第一個群組啟用該使用者或角色，然後為後續的群組執行這些步驟。

讓使用者做好使用多因素驗證的準備

若沒有適當的環境，忙碌的使用者可能會覺得多因素驗證 (MFA) 會拖慢他們，而不是增加價值。實作您的變更管理策略來協助使用者瞭解 MFA 的重要性，並提供流暢的上線體驗。您的目標是透過溝通、訓練甚至是一些行銷來讓每個人參與及接受訓練。

開始您為專案識別的變更管理活動，並在所有使用者順利採用 MFA 前讓這些活動保持運作。我們建議使用以下活動類型的多方策略：

- 溝通和行銷活動
- 訓練
- 啟動日上線及支援



小祕訣：如需有關這些活動的協助，請查看[可下載的 MFA 首展套件](#)。其中包含可自訂的範本，可協助您執行電子郵件行銷活動、訓練使用者使用 MFA，以及在啟動日透過上線範本進行支援。

使用通訊和促銷行銷活動與使用者互動

提早且頻繁地與 Salesforce 使用者通訊，並使用多個管道來確保您能與每個人聯繫。說明什麼是多因素驗證 (MFA)、您何時啟動此驗證，使用者必須做好哪些準備，以及他們可以在哪裡找到指示和支援。透過強調 MFA 是使用者帳戶、其資料和客戶健康的重要防護機制的概念來解釋使用者為何應多加留意。透過在專案前期建立這些詳細資料，您就可以減少使用者的反彈並避免採用封鎖程式。

這裡提供與使用者互動的幾個想法：

通訊論壇	建立如 Slack 管道或 Chatter 群組等中心地點來進行公告、提問與回答及同儕協同合作。這裡也是依照啟動排程定期共用更新的絕佳平台。
行銷活動	執行為期一週的電子郵件行銷活動來建立認知，向使用者宣傳 MFA 的價值，並提供祕訣，讓使用者為您的發行日做好準備。這也是說明如何註冊驗證方法和使用 MFA 登入的絕佳管道。
視覺提醒	透過在走廊和休息室張貼海報來強化認知。制定主題或發明流行語來吸引使用者並為其賦能，像是「安全從您開始！」或「使用 MFA 全程保護您的安全」。您是否有創意的一面？試著用一些方式，讓海報彈出時帶有色彩或是引人注目的意象。

 **小祕訣:** 將存取 Salesforce 環境的外部使用者 (例如合作夥伴、承包商和電話服務中心服務) 納入所有通訊和行銷活動中。

對使用者進行 MFA 基礎知識的訓練

當使用者在啟用 MFA 後登入時，會出現一系列的提示，帶領其完成註冊和使用驗證方法的步驟。但，請勿完全依賴此體驗。提供一些與 MFA 基礎知識相關的正式訓練，對於順利推出而言很重要。

此處提供幾個您可以採用的訓練方法。

選隨訓練	建立可讓使用者隨時存取的資源，例如影片。或者，要求使用者完成 Trailhead 中的 使用者驗證 課程模組。
面對面式訓練	建立網路研討會或午餐學習會議等即時訓練機會。

在您的訓練資料中包含以下詳細資料：

- 什麼是 MFA，為何對您的公司與客戶如此重要。
- 可在您實作中支援的驗證方法，以及使用者必須採取以進行註冊的步驟。
- 如何使用您支援的每種驗證方法來登入。
- 使用者在登入後工作階段保持啟用的時間長短，以及若工作階段到期，應如何重新驗證。
- 如果使用者在註冊方法、登入時遇到問題，或是當他們忘記或遺失驗證方法時，可在哪裡獲得協助。

開發上線資料並計畫您的啟動日

訓練很重要，但不要期望使用者提前記住他們學到的一切。啟動日到來時，使用者可借助說明及展開應用程式內註冊提示的簡單資源。上線資料在協助使用者開始與執行方面 (以及降低您呼叫支援小組的可能性) 有很大的幫助。

在啟用 MFA 前，請考慮建立快速入門網頁或複合速查表，以快速散佈給使用者。專注在逐步指示，以取得和註冊驗證方法，接著使用此方法來登入。確保在使用者卡住或感到困惑時能夠明確地知道如何獲得協助。

擬定流程和撰寫文件，以快速解決使用者在啟動日遭遇的任何問題。

- 透過建立自助資料 (包含對使用者在啟動日最可能遭遇之問題的疑難排解資訊)，將呼叫轉移至支援小組。
- 計畫安排營業時間，或是為啟動日設立專屬的現場服務台。確保負責這些資源的人員都經過訓練，並可存取 MFA 疑難排解文件。如果您進行模擬啟動日情形的演練，則實際啟動時應能進行得比較順利。
- 考慮為在遭遇問題時需要優先協助的主管和業務使用者考慮建立 SOS 流程。

最後，設想在啟動日上製造一點樂趣。運用一些創意和一點預算，您就能打造引人入勝的上線事件。這裡提供一些想法：

- 舉辦抽獎活動，獎品包含禮品卡、一天的休假或與高階主管共進午餐。
- 用杯子蛋糕主辦啟動。
- 分發贈品或品牌項目。

- 舉辦競賽，以 MFA 來順利登入的前幾名使用者 (由您決定數量) 可收到獎品。在公開公司論壇中為得獎者慶祝。人員會因認可和獎品而獲得激勵，不論認可多微小或獎品多便宜都是如此！

另請參照：

[決定 MFA 變更管理策略](#)

實作多因素驗證

除了執行變更管理活動，現在正是開始多因素驗證 (MFA) 實作的時機。啟用 MFA 會自動將驗證挑戰新增至登入流程，因此您想要將該步驟延後至排程的啟動日。讓我們看一看我們在這個階段建議的其他實作相關活動。

處理 MFA 相依性和阻礙因素

現在正是處理必須處理之問題的時機，如此您才能夠繼續啟用 MFA。

準備好支援您的 MFA 實作

實施多因素驗證 (MFA) 支援計畫，以確保支援小組獲得訓練且具有資源，能解決 MFA 相關問題。指派 MFA 管理權限，使小組可在使用者遺失或忘記其驗證方法時，協助其復原存取權。

準備部署 MFA 的安全性金鑰和內建驗證器 (選用)

針對 Salesforce Platform 上建立的產品，管理員必須先啟用安全性金鑰和內建驗證器，使用者才能將這些選項註冊為多因素驗證 (MFA) 的驗證方法。如果您在 MFA 實作時使用安全性金鑰，請在啟動日之前保留足夠的時間以購買並將其散佈給使用者。建議您保存一些額外的金鑰以作為備用。

測試您的 MFA 實作

執行測試計畫來確保多因素驗證 (MFA) 實作如預期般運作。針對每個支援的驗證方法完成註冊及登入流程。並針對使用者沒有方法時的情況測試復原流程。

協助使用者取得和註冊 MFA 的驗證方法

當您啟用多因素驗證 (MFA) 後，使用者必須至少有一個已註冊的驗證方法，才能登入。註冊流程會與使用者 Salesforce 帳戶的登入方法連線。在接近啟動日時，就是將驗證方法 (包括註冊流程的指示) 分配給使用者的時候。

處理 MFA 相依性和阻礙因素

現在正是處理必須處理之問題的時機，如此您才能夠繼續啟用 MFA。

例如：

- 透過確保登入 Salesforce 的每個人都有自己的使用者授權和帳戶，以免除共用帳戶或認證。如需協助，請連絡帳戶主管或銷售小組。或者請參閱[管理帳戶的 Salesforce Checkout](#) 和 [自助式服務](#)。
- 如果您使用的是 B2C Commerce Cloud，而您尚未執行以上建議，則請將業務經理使用者移轉至客戶經理。如需步驟式說明，請參閱[業務經理統一驗證的常見問題](#)和[業務經理的 B2C Commerce 統一驗證](#)研討會錄影檔。

-  **小祕訣:** 如果您先前已執行使用者清點，並且發現任何其擁有的權限超過所需權限的使用者，請考慮執行一些使用者管理清理作業。移除非必要的權限可協助降低安全風險。

另請參照：

[評估組織和使用者對 MFA 的整備狀況](#)

準備好支援您的 MFA 實作

實施多因素驗證 (MFA) 支援計畫，以確保支援小組獲得訓練且具有資源，能解決 MFA 相關問題。指派 MFA 管理權限，使小組可在使用者遺失或忘記其驗證方法時，協助其復原存取權。

以下是一些最佳作法。

記錄 MFA 原則和流程	建立知識文章或其他支援人員可用來解決個案問題的文件。建議您說明下列主題： - 使用驗證方法註冊和登入的指示 - 適用於連線問題、失敗的驗證嘗試和帳戶鎖定的疑難排解資料 - 驗證方法遺失或遭竊的復原流程
教育支援人員	安排網路研討會或面對面式訓練課程。保留示範及問與答的時間。
加快 MFA 個案解決速度	如果您使用 Salesforce 來處理支援詢問，請透過設定 快速文字 和 巨集 ，並在 MFA 資料夾中進行組織來簡化常見問題的回應。

將 MFA 管理權限指派給支援小組

您可以將與遺失或忘記驗證法相關的管理員任務委派給支援小組。將「管理使用者介面中的多因素驗證」權限指派給適當的使用者。此使用者權限可讓工作人員處理如產生臨時驗證碼、中斷與驗證方法的連接，及更換遺失安全性金鑰等活動。請參閱[委派多因素驗證管理工作](#)來獲得詳細資料。

-  **備註:** 委派 MFA 管理員工作僅適用於在 [Salesforce Platform 上建立的產品](#)。

另請參照：

[支援 MFA 實作](#)

[復原 MFA 已啟用使用者的存取權 \(適用於在 Salesforce Platform 上建立的產品\)](#)

[建立 MFA 支援計畫](#)

準備部署 MFA 的安全性金鑰和內建驗證器 (選用)

針對 Salesforce Platform 上建立的產品，管理員必須先啟用安全性金鑰和內建驗證器，使用者才能將這些選項註冊為多因素驗證 (MFA) 的驗證方法。如果您在 MFA 實作時使用安全性金鑰，請在啟動日之前保留足夠的時間以購買並將其散佈給使用者。建議您保存一些額外的金鑰以作為備用。

若要為您的 MFA 實作設定這些選項：

- [針對身分驗證啟用 U2F 或 WebAuthn 安全性金鑰](#)
- [針對身分驗證啟用內建驗證器](#)

另請參照：

[多因素驗證的驗證方法](#)

測試您的 MFA 實作

執行測試計畫來確保多因素驗證 (MFA) 實作如預期般運作。針對每個支援的驗證方法完成註冊及登入流程。並針對使用者沒有方法時的情況測試復原流程。

測試實作的建議會因 Salesforce 產品而有所不同。

- [在 Salesforce Platform 上建立的產品](#) (包括 Sales Cloud 和 Service Cloud)
- [B2C Commerce Cloud](#)
- [Marketing Cloud 參與](#) (由電子郵件、傳訊和旅程支援)



小祕訣： 從[可下載的 MFA 首展套件](#)取得可自訂測試計畫範本。

測試 MFA (適用於在 Salesforce Platform 上建立的產品)

在測試環境中啟用和驗證多因素驗證 (MFA)，之後再於 Salesforce 生產組織中推出事項。確認使用每一個支援的驗證方法進行的註冊和登入都能如預期運作。

僅適用於：在 Salesforce Platform 上建立的產品，包括 Sales Cloud、Service Cloud、Analytics Cloud、B2B Commerce Cloud、Marketing Cloud、Marketing Cloud—Pardot、Experience Cloud、Platform、產業產品 (Consumer Goods Cloud、Financial Services Cloud、Government Cloud、Health Cloud、Manufacturing Cloud、Philanthropy Cloud)，及 Salesforce Essentials

提供版本：**Essentials、Group、Professional、Enterprise、Performance、Unlimited、Developer 及 Contact Manager Edition**

您可以使用 [Sandbox 環境](#)或註冊 [Developer Edition 組織](#)。

若要測試驗證方法，建議您使用不具管理員權限的測試使用者。以測試使用者身分登入，然後為每個方法完成註冊流程，並確認您可以成功地連線到 Salesforce 並登入。



備註： 避免在 MFA 測試中使用管理員帳戶，如此您就不會不小心將自己鎖在帳戶之外。

另請參照：

[Sandbox 環境的多因素驗證考量事項](#)
[定義 MFA 實作和測試計畫](#)

測試 MFA (適用於 B2C Commerce Cloud)

客戶經理沒有可測試客戶經理設定的隔離環境。建議您使用信任的使用者或使用測試使用者帳戶來驗證多因素驗證 (MFA) 實作。

僅適用於：B2C Commerce Cloud

若要測試 MFA，請對僅具有少數指派使用者的測試角色或非關鍵角色 [啟用此功能](#)。如此一來，您可以在不影響大多數使用者的情況下驗證實作。

登入測試使用者帳戶，或使用指派給已啟用角色的使用者。確認使用者可使用每一個支援的驗證方法進行註冊和登入。

 **備註：** 避免在 MFA 測試中使用管理員帳戶，如此您就不會不小心將自己鎖在帳戶之外。

如果您發現無法快速解決或處理的任何問題，您可以隨時為該角色停用 MFA。

另請參照：

[定義 MFA 實作和測試計畫](#)

測試 MFA (適用於 Marketing Cloud 參與)

「MarketingCloud 參與」(由電子郵件、傳訊和旅程支援)沒有測試環境，因此我們建議您使用測試使用者帳戶來驗證多因素驗證 (MFA) 實作。

僅適用於：Marketing Cloud 參與 (由電子郵件、傳訊和旅程支援)

若要測試 MFA，請從 [為您的租戶啟用此功能](#) 開始。建議您使用預設的啟用選項，這可讓使用者選擇其開始使用 MFA 的時間。如此一來，開啟 MFA 時，就不會有人立即受到影響。

然後，登入測試使用者帳戶 (或使用測試的使用者)，確認您可以使用每一個支援的驗證方法來註冊及登入。

 **備註：** 避免在 MFA 測試中使用管理員帳戶，如此您就不會不小心將自己鎖在帳戶之外。

如果您發現您無法快速解決或處理的任何問題，您可以 [停用 MFA](#)。

另請參照：

[定義 MFA 實作和測試計畫](#)

協助使用者取得和註冊 MFA 的驗證方法

當您啟用多因素驗證 (MFA) 後，使用者必須至少有一個已註冊的驗證方法，才能登入。註冊流程會與使用者 Salesforce 帳戶的登入方法連線。在接近啟動日時，就是將驗證方法 (包括註冊流程的指示) 分配給使用者的時候。

建議您在開啟 MFA 的一到兩週前開始分配方法。使用者也可以隨時自行註冊驗證方法。建議每個人至少在啟動日的一個月前進行註冊，以避免在使用 MFA 時造成登入延遲。我們建議使用者設定多個驗證方法，這樣即使使用者忘記或遺失其中一個選項，也不會被鎖在帳戶之外。

 **小祕訣：** 想要提前提供上線說明來協助您的使用者進行註冊流程？請查看 [可下載的 MFA 首展套件](#)。其針對 Salesforce 產品支援的每種驗證方法提供可自訂的上線範本。

每個驗證方法的註冊步驟會有些微差異。而且使用者啟動自我註冊流程的方式，也會因為Salesforce產品不同而有所差異。使用這些資源來取得逐步詳細資料。

- [在 Salesforce Platform 上建立的產品](#) (包括 Sales Cloud 和 Service Cloud)
- [B2C Commerce Cloud](#)
- [Heroku](#)
- [Marketing Cloud 參與](#) (由電子郵件、傳訊和旅程支援)
- [Marketing Cloud Intelligence](#) (由 Datorama 提供技術支援)
- [Marketing Cloud Social](#)
- [MuleSoft Anypoint 平台](#)
- [Tableau Online](#)

 **備註:** 如果使用者在MFA開啟前尚未準備好方法，則其會在下一次登入時自動進行註冊流程。畫面上的提示會引導使用者執行步驟。

當您準備要分配驗證方法時，請考慮下列原則。

- 在啟動日之前舉辦幾個註冊會議或安排營業時間，讓使用者可以在需要時獲得協助。
- 針對驗證器應用程式：
 - 為確保行動驗證應用程式 (例如 Salesforce Authenticator 或 Google Authenticator) 的安全性，使用者必須在其行動裝置上設定 PIN 或生物識別因素。(請注意，使用者必須先保護行動裝置的安全，才能註冊 B2C 商務的行動驗證應用程式。)
- 針對安全性金鑰：
 - 請保留足夠的時間，能在啟動日期之前將其傳送給使用者。決定您是否要親自交付金鑰，或是使用者必須前往指定的位置領取金鑰。如果您有遠端使用者或位於不同區域的辦公室，請為貨運延遲保留緩衝時間。
 - 請在啟動日準備一副額外的安全性金鑰，以免有些使用者收到故障的金鑰，或是不能準時拿到金鑰。
- 針對內建驗證器：
 - 註冊此類型驗證器之前，必須啟用並設定使用者的內建驗證器服務 (例如 TouchID、FaceID 或 Windows Hello)，才能驗證其身分。

另請參照：

[多因素驗證的驗證方法](#)

[讓使用者做好使用多因素驗證的準備](#)

啟動多因素驗證

當重要的日子來臨時，請為使用者啟用多因素驗證 (MFA)。然後發起啟動日活動來確保每個人都能獲得所需的支援。如果您要全面使用 MFA，請針對所有使用者將其開啟。如果您採取的是分階段方法，請立即為第一個群組啟用該使用者或角色，然後為後續的群組執行這些步驟。

對使用者啟用 MFA

準備好上線時，即可啟用多因素驗證 (MFA)。請記得，開啟 MFA 會對 Salesforce 登入流程自動新增驗證挑戰，因此請先確定您的使用者已準備就緒，再採取此步驟。

在 MFA 啟動日支援使用者

使用建議的最佳作法來成功推出多因素驗證 (MFA)。例如，發起使用者支援活動，以協助使用者快速疑難排解和解決問題，例如辦公室服務時間或是專屬說明中心。

對使用者啟用 MFA

準備好上線時，即可啟用多因素驗證 (MFA)。請記得，開啟 MFA 會對 Salesforce 登入流程自動新增驗證挑戰，因此請先確定您的使用者已準備就緒，再採取此步驟。

啟用 MFA 的步驟取決於 Salesforce 產品。

- [在 Salesforce Platform 上建立的產品](#) (包括 Sales Cloud 和 Service Cloud)
- [B2C Commerce Cloud](#)
- [Heroku](#)
- [Marketing Cloud 參與](#) (由電子郵件、傳訊和旅程支援)
- [Marketing Cloud Intelligence](#) (由 Datorama 提供技術支援) 第 頁 35
- [Marketing Cloud Social](#)
- [MuleSoft Anypoint 平台](#)
- [Quip 產品](#)
- [Tableau Online](#)

啟用 MFA (適用於在 Salesforce Platform 上建立的產品)

為一些或所有使用者啟用多因素驗證 (MFA)。當使用者登入 Salesforce 使用者介面時，MFA 會要求他們提供其他驗證因素。

僅適用於：在 Salesforce Platform 上建立的產品，包括 Sales Cloud、Service Cloud、Analytics Cloud、B2B Commerce Cloud、Marketing Cloud、Marketing Cloud—Pardot、Experience Cloud、Platform、產業產品 (Consumer Goods Cloud、Financial Services Cloud、Government Cloud、Health Cloud、Manufacturing Cloud、Philanthropy Cloud)，及 Salesforce Essentials

提供版本：**Essentials、Group、Professional、Enterprise、Performance、Unlimited、Developer 及 Contact Manager Edition**

有兩種方法可以啟用 MFA。

對每個人啟用 MFA

若要同時為每個人開啟 MFA，請為對 Salesforce 組織設定進行的所有直接 UI 登入使用「需要多因素驗證 (MFA)」。
請參閱[針對整個組織啟用 MFA](#)來取得詳細資料。



小祕訣：想要觀看流程的實際運作嗎？請觀看[啟動 Salesforce 的多因素驗證影片](#)。

有一些使用者類型免受 MFA 需求的約束。當您使用 MFA 組織設定時，系統會自動將大部分的使用者類型排除在 MFA 之外。然而，有一些 MFA 免除的使用者類型必須手動排除，這應在使用此選項之前完成。若要查看您組織中是否有免除的使用者類型，以及瞭解如何將其從 MFA 排除，請參閱[從 MFA 排除例外使用者](#)。

分階段啟用 MFA

若要隨著時間向使用者群組推出 MFA，請使用「使用者介面登入的多因素驗證」使用者權限。請參閱[針對特定使用者啟用 MFA](#) 來取得詳細資料。

以下是一些注意事項：

- 要對選取的一群使用者或標準設定檔使用者推出試驗用的 MFA 嗎？請建立包含 MFA 使用者權限的權限集。接著將權限集套用給想要的使用者。
- 準備好將 MFA 推出到經指派至特定自訂設定檔的每個人嗎？將 MFA 使用者權限新增至設定檔，以為使用者大量啟用 MFA。

MFA 啟用時的使用者體驗

為使用者開啟 MFA 時，他們必須擁有可存取 Salesforce 且已註冊的驗證方法。如果使用者未在啟動日之前自行註冊方法，下一次使用者登入時，畫面上的提示會引導其完成該流程。針對所有後續登入，使用者除了要提供使用者名稱和密碼以外，還須提供該驗證方法。

啟用 MFA (適用於 B2C Commerce Cloud)

自 2022 年 5 月起，已針對 B2C Commerce 客戶啟用並強制執行 MFA，現在 MFA 已成為登入體驗的永久部分。如果 Salesforce 尚未為您的組織強制執行 MFA，但您已準備好開始使用，請連絡 Salesforce 客戶支援。

僅適用於：B2C Commerce Cloud

另請參照：

[使用多因素驗證確認您的身分](#)

啟用 MFA (適用於 Marketing Cloud Intelligence)

自 2022 年 10 月起，已針對 Marketing Cloud Intelligence (由 Datorama 技術支援) 啟用並強制執行 MFA，現在 MFA 已成為登入體驗的永久部分。如果 Salesforce 尚未為您的組織強制執行 MFA，但您已準備好開始使用，請連絡 Salesforce 客戶支援。

僅適用於：Marketing Cloud Intelligence

在 MFA 啟動日支援使用者

使用建議的最佳作法來成功推出多因素驗證 (MFA)。例如，發起使用者支援活動，以協助使用者快速疑難排解和解決問題，例如辦公室服務時間或是專屬說明中心。

 **小祕訣：**若要在 MFA 上線時支援您的使用者，請查看[可下載的 MFA 首展套件](#)中提供的可自訂通訊和上線資源。

透過通訊來開始啟動	當重要的日子來臨時，請確保整個公司都能收到正式的通訊，其中標示 MFA 的啟動資訊。與執行贊助者、安全性小組或 CISO 合作來傳送公告，讓每個人都能瞭解推廣活動的重要性。
讓您的支援小組做好準備	即使有具有主動式進階變更管理活動，但有些使用者在註冊驗證方法或使用 MFA 進行驗證時仍會遇到問題。為了快速協助使用者解決問題，請確定已編制支援小組人員來處理與 MFA 相關的通話和個案。
針對啟動日問題提供直接支援	啟動您為啟動日規劃的特殊支援後勤。例如： - 配置現場說明中心或營業時間的人員，讓使用者可以獲得現場的幫助。 - 為需要優先獲得協助的主管和業務使用者建立 SOS 流程。
來辦一場活動吧！	雖然我們必須謹慎看待過程，但為何不透過將啟動日變成活動來為推出增添一些樂趣和刺激呢？這裡提供一些想法： - 舉辦抽獎活動，獎品包含禮品卡、一天的休假或與高階主管共進午餐。 - 用杯子蛋糕主辦啟動。 - 分發贈品或品牌項目。 - 舉辦競賽，以 MFA 來順利登入的前幾名使用者可收到獎品。在公開公司論壇中為得獎者慶祝。人員會因認可和獎品而獲得激勵，不論認可多微小或獎品多便宜都是如此！

另請參照：

[決定 MFA 變更管理策略](#)

管理階段：維護及增強多因素驗證

恭喜，您已為 Salesforce 使用者啟用多因素驗證 (MFA)！但請勿只「設定好就遺忘」。請透過持續關注每個人體驗 MFA 的方式來確保專案順利進行。在此階段中，請估量 MFA 推出的成效，並以每天持續進行的作業來支援使用者。這也是尋找方法來最佳化 MFA 實作及整體安全狀況的好時機。

測量多因素驗證推出的成功與否

在推出多因素驗證(MFA)後，確認您是否獲得使用者的認同並達成目標。收集回饋意見以瞭解哪些可行與哪些不可行。並且監控與用量模式相關的度量和 MFA 降低風險的程度，以瞭解實作的運作狀況。

支援 MFA 實作

啟用多因素驗證(MFA)會產生某些新管理員的責任以支援使用者和維護作業。根據您的支援計畫，您可能會與服務台或外部服務等支援小組分擔部分或所有活動。

最佳化多因素驗證實作及其他

當您向所有 Salesforce 使用者推出多因素驗證 (MFA) 時，請考量是否有可以對 MFA 實作和整體 Salesforce 安全性進行的增強。

測量多因素驗證推出的成功與否

在推出多因素驗證 (MFA) 後，確認您是否獲得使用者的認同並達成目標。收集回饋意見以瞭解哪些可行與哪些不可行。並且監控與用量模式相關的度量和 MFA 降低風險的程度，以瞭解實作的運作狀況。

取得有關 MFA 實作的使用者回饋意見

定期使用 Salesforce 使用者報到，以掌握事情的進展。衡量整體滿意度，並瞭解具體的難題。透過與使用者談話所獲得的洞察有助於協助您瞭解可以在哪些方面微調 MFA 體驗，特別是當您讓新使用者加入公司時。

監控和分析 MFA 用量

監控多因素驗證 (MFA) 用量模式和度量來全面瞭解使用者遇到的常見問題。使用此資料來評估用於改善的選項。

取得有關 MFA 實作的使用者回饋意見

定期使用 Salesforce 使用者報到，以掌握事情的進展。衡量整體滿意度，並瞭解具體的難題。透過與使用者談話所獲得的洞察有助於協助您瞭解可以在哪些方面微調 MFA 體驗，特別是當您讓新使用者加入公司時。

這裡提供收集回饋意見的一些想法。

投票	舉辦投票。例如，建立非正式的 Chatter 投票或使用線上投票應用程式來詢問特定問題。
調查	使用調查應用程式來進行正式的書面調查，以測量滿意度和問題領域。
重點群組	排程重點群組，以與重要使用者和小組進行對話。
問與答工作階段	主辦公開的「問題和答案」會議，以聽取對 MFA 原則造成之任何衝擊的疑慮。

監控和分析 MFA 用量

監控多因素驗證 (MFA) 用量模式和度量來全面瞭解使用者遇到的常見問題。使用此資料來評估用於改善的選項。

以下是要追蹤的一些事項。

- 檢查支援票證和日誌來追蹤失敗的登入嘗試及使用者註冊驗證方法的問題。同時追蹤暫存驗證代碼的要求數量。
- 查看使用者訓練或上線資料的差異，這些差異可能會導致使用者不正確設定或誤用驗證方法。
- 監控和分析 MFA 用量模式。例如，使用者是否需要比以前花更多時間才能登入？是否需要嘗試更多次才能順利登入？如果是這樣，您是否可以看到模式，其顯示某些驗證方法比其他方法更適合使用者？使用者是否像您推出 MFA 前那樣頻繁放棄或不登入 Salesforce？

視您的 Salesforce 而定，我們會提供您用來監視 MFA 使用情況的工具。

- 針對[在 Salesforce Platform 上建立的產品](#) (包括 Sales Cloud 和 Service Cloud)

- 針對 [Marketing Cloud 參與](#) (由電子郵件、傳訊和旅程支援)

另請參照：

[取得有關 MFA 實作的使用者回饋意見](#)

監控 MFA 用量 (適用於在 Salesforce Platform 上建立的產品)

您可以使用多種工具來監視及報告組織中的多因素驗證 (MFA) 使用模式。選項包括 Lightning Usage 應用程式、Salesforce Labs 中的全面性 MFA 顯示面板，以及使用清單檢視與現成的「身分驗證方法」報告。

僅適用於：在 Salesforce Platform 上建立的產品，包括 Sales Cloud、Service Cloud、Analytics Cloud、B2B Commerce Cloud、Marketing Cloud、Marketing Cloud—Pardot、Experience Cloud、Platform、產業產品 (Consumer Goods Cloud、Financial Services Cloud、Government Cloud、Health Cloud、Manufacturing Cloud、Philanthropy Cloud)，及 Salesforce Essentials

提供版本：**Essentials、Group、Professional、Enterprise、Performance、Unlimited、Developer** 及 **Contact Manager Edition**

Lightning Usage 應用程式

使用 Lightning Usage 應用程式中的「登入度量」來監視組織中的登入。您可以追蹤有多少使用者利用貴組織的各種身分識別服務 (包括多因素驗證 (MFA) 和單一登入 (SSO)) 登入。如需完整的詳細資料，請參閱[使用 Lightning Usage 應用程式監視登入](#) 第 39 頁。

Salesforce Labs 中的 MFA 顯示面板應用程式

Salesforce Labs 中的多因素驗證顯示面板是開始使用 MFA 後，監視及報告 MFA 使用模式的絕佳選項。這是免費的應用程式。您可從 [Salesforce AppExchange](#) 下載及安裝該封裝。

 **備註：** 在 Winter '21 版本之前，此封裝稱為雙因素驗證顯示面板。

此封裝包含：

- MFA 檢視：查看誰已註冊 MFA 驗證方法。您也可以追蹤誰已產生暫存驗證碼，以及誰已撤銷任何已註冊的驗證方法。
- 顯示面板和報告：審查組織中的 MFA 驗證活動，並追蹤方法註冊進度。

安裝封裝之後，請在 Salesforce 中選取「顯示面板」。然後開啟 MFA 顯示面板資料夾並選取「**MFA 顯示面板**」。

MFA 清單檢視和身分驗證方法報告

您可以自訂清單檢視來查看誰已註冊 MFA 的驗證方法。此外，「設定」中的身分驗證方法報告可監視和審查使用者過去六個月內的身分驗證嘗試。使用此報告瞭解使用者使用 MFA 的方式和時機。

如需完整的詳細資料，請參閱[查看使用者如何驗證身分](#)和[監控身分驗證歷程記錄](#)。

另請參照：

[監控和分析 MFA 用量](#)

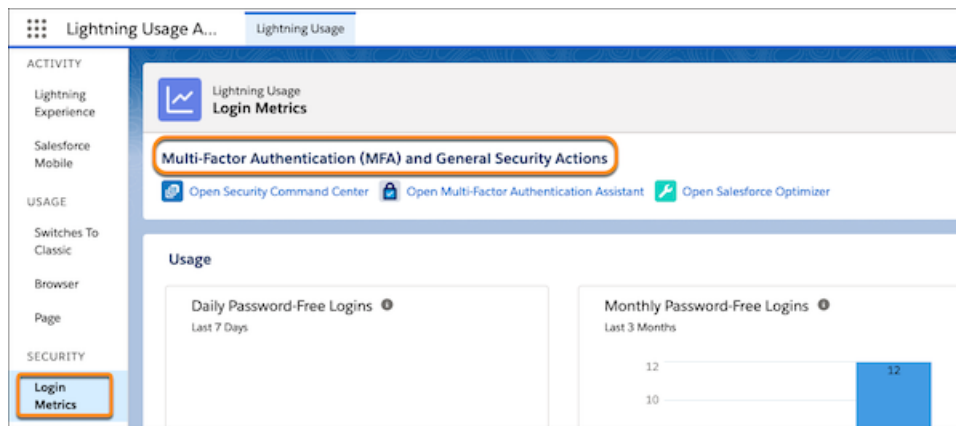
使用 Lightning Usage 應用程式監視登入

使用 Lightning Usage 應用程式中的「登入度量」來監視組織中的登入。查看有多少使用者利用您組織的各種身分識別服務登入，包括多因素驗證 (MFA) 和單一登入 (SSO)。

如果您在組織中實作 MFA，您可以使用登入度量來查看使用者是否使用 MFA 來登入。監視多個登入方法可讓您瞭解趨勢、偵測任何異常的登入或發現使用者仍未使用 MFA 來登入。

若要從 App Launcher (⋮) 存取 Lightning Usage 應用程式，請尋找並開啟「**Lightning Usage**」。在應用程式中，按一下頁面左側「安全性」底下的「登入度量」，以檢視相關資料。「登入度量」頁面會顯示過去 7 天及過去 3 個月中，免密碼單一登入 (SSO) 及使用者名稱和密碼登入方法 (使用及不使用 MFA) 的登入資料。如需更多 MFA 和安全性資源，請按一下「多因素驗證 (MFA)」和「一般安全性動作」底下的任一連結。

- 「免密碼登入」會追蹤以憑證為基礎的登入、Lightning 登入及無密碼登入。
- 「單一登入」會追蹤 Salesforce 或協力廠商透過同盟 SSO 執行的登入，包括 SAML 和 OpenID Connect 開放標準。
- 您可以在「使用者名稱和密碼」登入度量下追蹤委派驗證登入。
- 「使用 MFA 登入」只會追蹤 Salesforce MFA 登入。



監視 MFA 用量 (適用於 Marketing Cloud 參與)

當您為「Marketing Cloud 參與」(由電子郵件、傳訊和旅程支援) 租戶啟用多因素驗證 (MFA) 後，即可使用「MFA 事件」記錄追蹤所有註冊和驗證嘗試。

如需完整的詳細資料，請參閱[檢視 Marketing Cloud 中的 MFA 事件](#)。

支援 MFA 實作

啟用多因素驗證 (MFA) 會產生某些新管理員的責任以支援使用者和維護作業。根據您的支援計畫，您可能會與服務台或外部服務等支援小組分擔部分或所有活動。

一般支援和作業活動包括：

- 疑難排解和解決登入和驗證問題，包含帳戶鎖定。
- 如果使用者遺失或忘記其驗證方法，請協助其復原存取權。
- 在新進人員上線流程中為新員工啟用 MFA。

- 如果您支援此類型的驗證方法，請保存並散佈安全性金鑰。

存取復原

如果使用者忘記或遺失 Salesforce 產品相關的慣用驗證方法，則您可使用該選項協助使用者。

管理員產生的臨時驗證碼

針對部分產品，管理員可以產生臨時驗證碼以允許使用者在無驗證方法的情況下登入。下列是支援此選項的產品步驟：

- [在 Salesforce Platform 上建立的產品 \(包括 Sales Cloud 和 Service Cloud\)](#) 第 頁 40
- [Marketing Cloud 參與 \(由電子郵件、傳訊和旅程支援\)](#)
- [Marketing Cloud Social](#)

使用者產生的復原碼

在部分產品中，使用者可以產生十個一次性復原碼的清單，並將其保存在安全位置以備不時之需。作為上線活動的一部分，請要求您的使用者在開始使用 MFA 時產生復原碼。以下是具有此選項的產品步驟：

- [Heroku](#)
- [Marketing Cloud Intelligence \(由 Datorama 提供技術支援\)](#)
- [Marketing Cloud Social](#)
- [Tableau Online](#)

重設 MFA

針對 MuleSoft Anypoint Platform，管理員可以為遺失或忘記其驗證方法的使用者 [重設 MFA](#)。使用者便會收到提示，在下一一次登入時註冊新的方法。

 **備註：** 如果您是產品的唯一管理員且遭到鎖定，請連絡 Salesforce 客戶支援。

另請參照：

[建立 MFA 支援計畫](#)

[準備好支援您的 MFA 實作](#)

[復原 MFA 已啟用使用者的存取權 \(適用於在 Salesforce Platform 上建立的產品\)](#)

復原 MFA 已啟用使用者的存取權 (適用於在 Salesforce Platform 上建立的產品)

啟用 MFA 之後，存取問題通常分為兩個種類：使用者的 MFA 驗證方法與其 Salesforce 帳戶之間的連線未運作，或者使用者遺失、更換或忘記其 MFA 驗證方法。使用臨時驗證碼可讓使用者立即重新取得存取權。處理中斷的連線或缺少驗證方法時，撤銷連線並協助使用者設定新方法。

僅適用於：在 Salesforce Platform 上建立的產品，包括 Sales Cloud、Service Cloud、Analytics Cloud、B2B Commerce Cloud、Marketing Cloud、Marketing Cloud—Pardot、Experience Cloud、Platform、產業產品 (Consumer Goods Cloud、Financial Services Cloud、Government Cloud、Health Cloud、Manufacturing Cloud、Philanthropy Cloud)，及 Salesforce Essentials

提供版本：**Essentials、Group、Professional、Enterprise、Performance、Unlimited、Developer 及 Contact Manager Edition**

以下是常見 MFA 相關存取問題的建議復原步驟。

使用者的驗證方法未運作或已更換

如果使用者已註冊驗證方法，但在嘗試登入時該方法沒有作用，請使用這些存取復原步驟。如果使用者因為其新的行動裝置、安全性金鑰或電腦內建驗證服務，而必須註冊驗證方法，這些步驟也適用。

1. 向使用者發出臨時驗證碼，讓他們可以在您解決其問題時登入。請參閱[產生暫時身分驗證代碼](#)。
2. 中斷使用者現有驗證方法的連線。請參閱[中斷與使用者驗證方法的連接](#)。
3. 協助使用者重新註冊其驗證方法或設定新方法。參閱[註冊多因素驗證的驗證方法](#)。
4. 當不再需要使用者臨時驗證碼時使其到期。請參閱[使暫存驗證代碼到期](#)。

使用者的驗證方法遺失或遭竊

1. 移除使用者目前的工作階段並重新驗證使用者。請參閱[使用者工作階段](#)。
2. 向使用者發出臨時驗證碼，讓他們可以在您解決其問題時登入。請參閱[產生暫時身分驗證代碼](#)。
3. 中斷使用者現有驗證方法的連線。請參閱[中斷與使用者驗證方法的連接](#)。
4. 審查使用者的帳戶活動來查看是否有任何異常活動。請參閱[您的使用者如何驗證其身分](#)。
5. 指引使用者完成流程來獲得更換裝置。當他們具備驗證方法時，協助他們重新註冊其驗證方法或設定新方法。參閱[註冊多因素驗證的驗證方法](#)。
6. 當不再需要使用者臨時驗證碼時使其到期。請參閱[使暫存驗證代碼到期](#)。

使用者忘記其驗證方法

1. 向使用者發出臨時驗證碼，讓他們可以登入並完成當天的工作。請參閱[產生暫時身分驗證代碼](#)。
2. 當不再需要使用者臨時驗證碼時使其到期。請參閱[使暫存驗證代碼到期](#)。

另請參照：

[建立 MFA 支援計畫](#)

[準備好支援您的 MFA 實作](#)

最佳化多因素驗證實作及其他

當您向所有 Salesforce 使用者推出多因素驗證 (MFA) 時，請考量是否有可以對 MFA 實作和整體 Salesforce 安全性進行的增強。

[精簡 MFA 使用者體驗](#)

計畫多因素驗證 (MFA) 實作的定期檢閱，以確認其是否仍符合您的需求。

[檢閱並增強 Salesforce 安全性策略](#)

多因素驗證 (MFA) 只是整體 Salesforce 安全性策略中的其中一個面向。若要保護客戶和資料的安全，請考慮最佳作法、工具和技術來改善現有的深度防護策略。

精簡 MFA 使用者體驗

計畫多因素驗證 (MFA) 實作的定期檢閱，以確認其是否仍符合您的需求。

這裡提供一些建議。

- 在新的驗證方法技術可供使用時檢閱該技術。尋找簡化或改善目前使用者體驗的機會。
- 維護讓 Salesforce 帳戶存取保持安全的公司承諾。
- 透過後續追蹤訓練會議或營業時間來繼續教育使用者，以加強正確的行為。

啟用 Lightning Login (適用於在 Salesforce Platform 上建立的產品)

僅適用於：在 Salesforce Platform 上建立的產品，包括 Sales Cloud、Service Cloud、Analytics Cloud、B2B Commerce Cloud Marketing Cloud、Marketing Cloud—Pardot、Experience Cloud、Platform、產業產品 (Consumer Goods Cloud、Financial Services Cloud、Government Cloud、Health Cloud、Manufacturing Cloud、Philanthropy Cloud)，及 Salesforce Essentials

提供版本：**Essentials**、**Group**、**Professional**、**Enterprise**、**Performance**、**Unlimited**、**Developer** 及 **Contact Manager Edition**

啟用 Lightning Login 來增強 MFA 使用者體驗。此功能可讓使用者快速、方便、安全且不用密碼地存取其 Salesforce 帳戶。其藉由要求 Salesforce Authenticator (使用者具備的應用程式) 及在其行動裝置上 (使用者具備的裝置) 設定 PIN 或生物識別掃描來符合 MFA 標準。請參閱[針對免密碼登入啟用 Lightning Login](#)。

檢閱並增強 Salesforce 安全性策略

多因素驗證 (MFA) 只是整體 Salesforce 安全性策略中的其中一個面向。若要保護客戶和資料的安全，請考慮最佳作法、工具和技術來改善現有的深度防護策略。

增強登入安全性	針對登入實作 IP 範圍限制之類的控制項。
考量替代的身分安全性解決方案	單一登入 (SSO) 是改善使用者登入體驗的絕佳選項。如果您的使用者會在每天行程中定時存取多個應用程式，建議您使用身分提供者 (IdP) 為所有應用程式 (包括 Salesforce) 增強存取安全性。妥善實作 SSO 策略後，您就可以降低密碼相關的風險、改善驗證流程，以及讓使用者更輕鬆地登入經常使用的應用程式。 若要符合 MFA 需求，請為您的 SSO 身分提供者啟用 MFA。
將 MFA 套用至 API 登入	將「最低權限」原則套用至 API 使用者。將強大的管理層級權限提供給 API 使用者是一種常見的不良作法，因為真正需要的是相關物件的存取權。審核 API 使用者目前擁有的權限，並查看您可以刪除非必要權限的部分。 考量您的 API 使用者是否也具有該使用者介面的存取權。如果非必要，請只限制對 API 的存取權。

如果您使用在 [Salesforce Platform 上建立的產品](#)，您可以使用內建工具來檢視整體的 Salesforce 安全性設定，以及尋找解決任何現有風險的方法。

- 使用[安全健康檢查](#)來找出和修正安全性設定中的風險。
- 使用[Salesforce Shield](#)，在業務關鍵的應用程式中建立新層級的信任、透明度、合規和監管。

多因素驗證詞彙

熟悉與多因素驗證 (MFA) 和合約 MFA 要求相關的常用術語。

自動啟用 MFA

Salesforce 會代表客戶為直接登入 Salesforce 產品 UI 的所有使用者啟用 MFA。先前未使用 MFA 的使用者會收到提示，要求他們在下一次登入時註冊否則便無法繼續。已使用 MFA 登入的使用者不會受到影響。針對部分產品，MFA 會在強制執行前幾個月自動啟用。在此期間，如果使用者尚未準備好使用 MFA，管理員可以暫時停用 MFA。請查看「[強制執行 MFA](#)」和「[註冊 MFA](#)」。

驗證

在允許使用者登入帳戶、執行動作或存取資訊之前，驗證使用者所聲稱身分的過程。

啟用 MFA

客戶管理員為其組織/租戶/領域啟用 MFA 所採取的動作。取決於 Salesforce 產品，管理員可以針對使用者群組或逐個使用者在組織層級啟用 MFA。

強制執行 MFA

當 Salesforce 為 Salesforce 產品強制執行 MFA 時，MFA 將永久成為該產品登入程序的一部分。在強制執行期間，Salesforce 會為所有未使用 MFA 直接登入的使用者自動啟用 MFA。同時，Salesforce 也會移除所有客戶使用者 (包括管理員) 停用 MFA 的選項。

最低權限

使用者完成工作所需擁有的最少權限的概念。這可限制使用者存取資訊或執行其角色不應被允許動作的風險、限制使用者錯誤的影響，並減少在發生攻擊時認證遭盜用的損害。

多因素驗證 (MFA)

一種安全措施，用於加強對存取使用者帳戶的保護。MFA 要求使用者在登入時出示兩個以上的證據或因素，以證明他們就是所聲稱的身分。這些證據必須至少分為兩個不同的類別 (使用者知道、擁有或其本身的東西)。廣為人知的 MFA 工作範例是從 ATM 提款所需的兩個因素。若要提款，您必須出示 ATM 卡片 (您擁有的東西)，接著您必須輸入 PIN 碼 (您知道的東西)。另請參閱「[驗證方法](#)」。

特權使用者

具有高層級應用程式和敏感資料存取權的管理員和使用者。

針對在 Salesforce Platform 上建立的產品，特權使用者為 Salesforce 管理員 (定義為具有「自訂應用程式」和「修改所有資料」使用者權限的使用者)，或具有下列任一使用者權限的使用者：自訂應用程式、管理使用者、修改所有資料或全部檢視。

註冊 MFA

每個使用者將驗證方法連接到其帳戶的過程，以便他們在登入時可以使用該方法驗證自己的身分。啟用 MFA 時，使用者必須註冊一個方法才能登入。使用者可以註冊多個方法，如此便有備用選項，以防他們丟失或忘記主要的方法。

安全性金鑰

通過儲存和檢索某種個人資訊，以電子方式驗證個人身分的實體裝置。安全性金鑰可能有許多不同的尺寸規格，包括 USB、Lightning 和 NFC。也稱為安全性權杖或驗證權杖。

強大驗證方法

更能抵禦網路攻擊的驗證方法，例如網路釣魚和中間人攻擊。這些類型的方法有助於對存取 Salesforce 產品的使用者身分提供高度保證。另請參閱「[驗證方法](#)」。

時間型一次性密碼 (TOTP)

一次性密碼，可用作對使用者與其帳戶進行驗證的方法。若要使用 TOTP，使用者必須使用 TOTP 驗證器應用程式，它會產生一次性密碼。當使用者對其帳戶進行驗證時，產生器會實施演算法以根據目前時間建立一次性密碼。一旦向使用者顯示，此密碼會在有限的時間內有效，直到過期後便不能再用於登入，而使用者必須要求新密碼。

雙因素驗證 (2FA)

多因素驗證 (MFA) 的一個子集，只需要兩個因素即可登入。2FA 和 MFA 都透過要求使用者提供多個因素來驗證其身分來防止未經授權的存取。兩者的差異在於登入所需的因素數量。有些 MFA 解決方案可能要求三、四或更多個因素組合，但 2FA 只要求兩個。

驗證方式

使用者在登入以驗證其身分時出示的證據。也稱為因素或驗證因素。

Salesforce 產品支援多種類型的驗證方法，包括 Salesforce Authenticator、第三方 TOTP 驗證器應用程式 (例如 Google Authenticator 或 Authy)、實體安全性金鑰和內建驗證器 (例如 Windows Hello、TouchID 或 FaceID)。另請參閱「[強大驗證方法](#)」。

索引

M

MFA 首展套件 [6](#)

T

TOTP 驗證器應用程式 [11](#)