SOPHOS

Cybersecurity made simple.

Sophos Central Device Encryption

管理員指南

目錄

1 關於 Sophos Central Device Encryption

Sophos Central Device Encryption 使您能夠透過 Sophos Central 管理 Windows 端點上的 BitLocker 驅動器加密和 Mac 端點上的 FileVault 加密。

對硬碟進行加密後，即使裝置丟失或被被盜，也可以保持資料安全。

本指南介紹如何設定和使用裝置加密。其還介紹了如何使用自助入口網站擷取修復金鑰。如需有關策略設定、警報和透過 Sophos Central 恢復的詳情，請參閱 Sophos Central 幫助。

相關資訊

Sophos Central 說明

2 管理 BitLocker 驅動器加密

本節介紹在網路中的 Windows 端點上使用 BitLocker 驅動器加密的先決條件，可用的各種驗證模式以及其如何與專有組策略設定進行互動。

2.1 轉移到 Sophos Central Device Encryption

如果您已經透過 BitLocker 驅動器加密或 Sophos 完整磁碟加密使用 SafeGuard Enterprise，本節將介紹如何轉移到 Sophos Central Device Encryption。

它包括：

- SafeGuard Enterprise 和 BitLocker
- SafeGuard Enterprise 和 Sophos Full Disk Encryption
- 有關轉移 Mac 端點的資訊，請參閱轉移到 Sophos Central Device Encryption (Mac)。

相關工作
轉移到 Sophos Central Device Encryption (Mac) （第 11 頁）
如果要使用 Sophos Central 管理已使用 FileVault 加密的 Mac 端點，則需要將 Sophos Central Device Encryption 策略套用於這些端點。

2.1.1 從 SafeGuard Enterprise BitLocker 轉移

請按照以下步驟轉移。

注意事項
如果您使用具有 SafeGuard Enterprise 版本 6.x 或 7.x 的 BitLocker，我們建議您首先升級到最新版本的 SafeGuard Enterprise。

如果您使用 SafeGuard Enterprise 版本 6.x 或 7.x，必須先按照 SafeGuard Enterprise 管理員幫助中的步驟解密系統磁碟，才能轉移到 Sophos Central Device Encryption。

若要從 SafeGuard Enterprise BitLocker Client（8.0 或更高版本）轉移到 Sophos Central Device Encryption：

1. 前往控制台 > 解除安裝程式，然後對 Sophos SafeGuard Client 按右鍵。
2. 從右鍵功能表中選取變更。
   Sophos SafeGuard Client 安裝精靈開啟。
3. 解除安裝 BitLocker 元件。

   注意事項
   移除 BitLocker 元件不會解密磁碟區或檔案。

4. 安裝 Sophos Central Device Encryption 軟體。
5. 確保 Sophos Central Device Encryption 策略分配到端點並啟用。

現在，您可以使用 Sophos Central 管理 BitLocker。您無須重新加密。將 Sophos Central Device Encryption 策略套用到端點後，修復金鑰更新並傳送到 Sophos Central。檔案加密功能保持不變。

相關資訊
SafeGuard Enterprise 管理員說明

2.1.2 從 SafeGuard Enterprise 完整磁碟加密轉移

請按照以下步驟轉移。

若要從 SafeGuard Enterprise 完整磁碟加密轉移：

1. 解除安裝 Sophos SafeGuard Client 軟體。
   加密的磁碟區將自動解密。加密的文件保持加密。
2. 安裝 Sophos Central Device Encryption 軟體。
3. 確保 Sophos Central Device Encryption 策略分配到端點並開啟。
4. 重新安裝所需的 SafeGuard Enterprise File Encryption 模組（同步加密或基於位置的檔案加密）。

現在，您可以使用 Sophos Central 管理 BitLocker。將 Sophos Central Device Encryption 策略套用到端點後，加密在背景啟動，且修復金鑰更新並傳送到 Sophos Central。

2.2 準備裝置加密

大多數系統驅動器預設為已為 BitLocker 做好準備。如果情況不是這樣，Sophos Central Device Encryption 會自動運行所需的 Microsoft 指令行工具 BdeHdCfg.exe 以準備驅動器。

這說明系統驅動器上要建立一個單獨的 BitLocker 分割磁區。

在安裝 Sophos Central Device Encryption 期間，將有一條訊息通知使用者準備系統驅動器時需要進行重新啟動。使用者可以選擇立即重新啟動計算機或延遲操作。僅有在計算機已進行重新啟動且系統驅動器準備成功之時裝置加密才會啟動。

裝置加密所需的 .NET Framework 版本自動安裝在端點上。

2.3 逐步給裝置加密

請按照以下步驟給裝置加密。

使用者開始之前：

- 必須在端點上安裝 Sophos Central 代理軟體。
- 必須在 Sophos Central 中設定並啟用裝置加密策略。
- 使用者必須交互式地登入他們的端點，並將它們連接至 Sophos Central 並與其同步。請注意，不支援遠端登入。
- 操作系統必須支援 BitLocker 驅動器加密。如欲瞭解更多詳情，請參閱準備裝置加密和裝置加密系統相容性。

這些指示會告訴您使用者將看到什麼內容以及他們需要做的事：

1. 如果尚未啟用 TPM 安全軟體，將觸發一個 BIOS 動作以啟用它。這需要進行重新啟動。使用者可以立即重新啟動也可以延遲進行重新啟動。
   在重新啟動期間，會提示使用者啟用 TPM。如果不能啟用 TPM 或者使用者未作出響應，將顯示一條訊息。
2. 如果 TPM 處於活動狀態並已啟用，但是尚未被持有，Sophos Central 代理軟體會自動生成並設定 TPM 擁有者資訊。如果此操作失敗，將向 Sophos Central 傳送一條警示。

3. 如果 TPM 的簽注金鑰丟失，Sophos Central 代理軟體將會自動建立這些金鑰。如果此操作失敗，將向 Sophos Central 傳送一條警示。
4. 如果 Device Encryption 策略未指定需要安裝驗證，則硬碟的加密會自動開始。在本情況下，使用者無需執行任何動作。您可以跳到第 8 步。
5. 如果 Device Encryption 未指定需要安裝驗證，則使用者可參閱 Sophos Device Encryption 對話方塊。

    - 如果 Device Encryption 策略要求 PIN 碼或密碼以進行驗證，則使用者需要按照螢幕上的指示操作以定義 PIN 碼或密碼。如果使用 TPM+PIN，系統磁碟的加密金鑰將儲存在 TPM 中。

      注意事項
      設定密碼時，使用者需要謹慎。預先開機環境僅支援美式英語鍵盤配置。如果他們現在使用特殊字元設定 PIN 碼或密碼，則當他們稍後輸入該 PIN 碼或密碼登入時，可能需要使用不同的金鑰。

    - 如果 Device Encryption 策略要求 USB 金鑰進行驗證，使用者需要將 USB 快閃磁碟連接至其電腦。USB 快閃磁碟機必須是 NTFS、FAT 或 FAT32 格式。
6. 使用者按一下重新啟動並加密之後，電腦會重新啟動並檢查 Device Encryption 是否在運作。使用者可以選擇稍後再做以關閉對話。但是，當使用者下次登入，或者當您變更加密策略時，它將再次顯示。
7. 如果使用者無法輸入正確的 PIN 碼/密碼，他們可以按 Esc 鍵。由於尚未套用加密，此時系統可以正常啟動。登入後將再次要求使用者嘗試輸入 PIN 碼/密碼。
8. 您可以看到哪些使用者尚未啟用加密。這意味著他們尚未重新啟動其電腦或者尚未完成螢幕上的說明。查看 Sophos Central 中的報告。
9. 如果預先開機測試成功，Sophos Central 代理軟體將啟動固定磁碟的加密。加密將在背景環境下進行，允許使用者如平常一樣使用他們的計算機。
   如果硬體測試失敗，則系統會重新啟動，並且將不會執行加密。將會向 Sophos Central 傳送一個事件以通知您。
10. Sophos Central 代理為系統磁碟區加密之後，資料卷的加密已啟動（如果在策略中指定）。這些卷的保護儲存在系統磁碟區中，因此資料卷在安裝之後將自動可用。這說明當使用者登入他們的計算機之後，無需進行任何進一步的使用者互動即可存取資料卷。卸除式資料卷，例如 USB 快閃磁碟機，將不會進行加密。

您可以在端點上的 %ProgramData%\Sophos\Sophos Data Protection\Logs 下找到兩個日誌檔案 - CDE.log 和 CDE_trace.xml。

相關概念

準備裝置加密 （第 3 页）
大多數系統驅動器預設為已為 BitLocker 做好準備。如果情況不是這樣，Sophos Central Device Encryption 會自動運行所需的 Microsoft 指令行工具 BdeHdCfg.exe 以準備驅動器。

裝置加密系統相容性 （第 4 页）
以下表格概述了哪個平台支援哪種保護類型。套用的保護類型取決於使用的 Windows 版本和 TPM 安全硬體是否可用。

TPM+PIN （第 6 页）
TPM+PIN 模式使用計算機的 TPM 安全硬體和 PIN 碼作為驗證方式。

2.4 裝置加密系統相容性

以下表格概述了哪個平台支援哪種保護類型。套用的保護類型取決於使用的 Windows 版本和 TPM 安全硬體是否可用。

括號中的數字描述了具體保護類型的優先權。

(*) 啟用需要安裝驗證時，僅限 TPM 保護的安裝將不可用，因此 TPM+PIN 為首選項。

	Win 7 無 TPM	Win 7 有 TPM	Win 8.1 無 TPM	Win 8.1 有 TPM	Win 10 無 TPM	Win 10 有 TPM
僅限 TPM	-	可以 (1*)	-	可以 (1*)	-	可以 (1*)
TPM+PIN	-	可以 (2)	-	可以 (2)	-	可以 (2)
密碼	-	-	可以 (1)	可以 (3)	可以 (1)	可以 (3)
USB 金鑰	可以 (1)	可以 (3)	-	-	-	-

當您使用 Central Device Encryption 時，可能需要在端點電腦上配置 TPM 。

如果您使用的是 TPM 2.0 或更新版本，則必須將硬碟格式變更為 GPT，且 BIOS 必須處於 UEFI 模式。

如果您使用的是 TPM 1.2，則必須在 BIOS/UEFI 中啓用 TPM，並保證 TPM 隨時可用。您可使用 TPM.MSC 來檢查此項。

建議您在安裝 Central Device Encryption 之前，先將端點電腦更新為最新的 BIOS/UEFI 版本。

啟用 Windows FIPS Mode 時，BitLocker 加密僅受 Windows 8.1 或 Windows 10 系統的支援。如需 Windows 7 上的 BitLocker 在 FIPS 模式下的詳細資訊，請參閱FIPS 相容的恢復密碼無法儲存至 Windows 7 或 Windows Server 2008 R2 中 BitLocker 的 AD DS 。

您可以使用帶有 Sophos Central Device Encryption 的加密硬碟。有關詳細資訊，請參閱加密硬碟。

Central Device Encryption 支援預佈建的 BitLocker。

相關資訊

FIPS 相容的恢復密碼無法儲存至 Windows 7 或 Windows Server 2008 R2 中 BitLocker 的 AD DS

加密硬碟

2.5 裝置加密驗證模式

您可以使用裝置加密設定中的需要安裝驗證開關進行控制，無論使用者在登入其計算機時是否需要進行驗證。

電腦上安裝的驗證模式因系統、BitLocker 群組策略設定以及已配置的裝置加密策略而異。根據裝置加密系統相容性，將在端點上安裝以下其中一種驗證模式：

- TPM+PIN
- 複雜密碼
- 僅限 TPM
- USB 金鑰

在已經使用 BitLocker 加密的端點上，將透過一條訊息告知使用者所需的步驟。

當您打開需要安裝驗證時，會提示使用者定義 PIN 碼/複雜密碼/ USB 金鑰並點選套用。此後，他們每次啟動計算機時都必須使用這個 PIN 碼/複雜密碼/ USB 金鑰。相反地，如果您將需要安裝驗證關

閉，將自動套用僅限 TPM 模式，且無需額外的驗證。將告知使用者他們的計算機會在其啟動時自動解鎖裝置。

Sophos 裝置加密能夠自動配置組策略對象 (GPO)，因此允許所有的驗證模式，如果相應的設定已設定為未配置。當您手動配置設定時，軟體將不會覆寫這些定義。如需更多資訊，請參閱 BitLocker 群組策略設定。

使用者可以決定延遲安裝驗證模式。在此情況下，將不會進行加密。無論使用者何時重新登入 Windows，或者在您部署新的加密策略時，系統都會提示使用者重新啟動計算機。重新啟動之後，將安裝驗證模式並啟動裝置加密。此後使用者將無法解密他們的裝置。

相關概念

裝置加密系統相容性 （第 4 页）
以下表格概述了哪個平台支援哪種保護類型。套用的保護類型取決於使用的 Windows 版本和 TPM 安全硬體是否可用。

BitLocker 組策略設定 （第 7 页）
Sophos Central 自動定義了一些組策略設定，因此管理員無需在進行裝置加密時準備計算機。

2.5.1 TPM+PIN

TPM+PIN 模式使用計算機的 TPM 安全硬體和 PIN 碼作為驗證方式。

使用者必須在每次啟動計算機時在 Windows 預先開機環境中輸入此 PIN 碼。

TPM+PIN 需要準備就緒的 TPM，而系統的 GPO 設定必須允許 TPM+PIN 模式。

如果符合全部條件，將會顯示 TPM+PIN 設定對話，還將提示使用者定義一個 PIN 碼。使用者可以按一下重新啟動與加密以立即重新啟動計算機並開始加密。

如果啟用 GPO 設定允許在安裝時使用增強的 PIN 碼，PIN 碼可能要包含數字、字母或特殊字元。否則，只允許使用數字。

BitLocker 的 PIN 碼長度在 4 到 20 個字元之間。您可以透過組策略定義一個更長的最小長度。Sophos Central 代理軟體設定組策略以允許增強的 PIN 碼。對話會告知使用者可以輸入哪些字元，以及所允許的最小/最大長度是什麼。

注意事項
特定 Windows 計算機的所有使用者都需要使用相同的 PIN 碼來解除鎖定系統磁碟。隨後，使用他們的個人憑證登入作業系統。Windows 計算機不支援單一登入。

2.5.2 密碼

如需在沒有 TPM 安全硬體的端點進行驗證，則可以使用密碼。

使用者必須在每次啟動計算機時在 Windows 預先開機環境中輸入此密碼。

密碼保護需要 Windows 8.0 或更高版本，而系統的 GPO 設定必須允許密碼模式。

如果符合全部條件，將會顯示密碼設定對話，還將提示使用者定義一個長度為 8-100 個字元的密碼。使用者可以按一下重新啟動與加密以立即重新啟動計算機並開始加密。

2.5.3 僅限 TPM

僅限 TPM 模式使用計算機的 TPM 安全硬體，無需任何 PIN 碼驗證。

這意味著使用者可以無需在 Windows 預先開機環境中獲得 PIN 碼的提示即可啟動計算機。

僅限 TPM 需要準備就緒的 TPM，且必須啟用裝置加密策略設定的需要安裝驗證功能。此外，系統的 GPO 設定必須允許僅限 TPM 保護。

如果符合全部條件，將顯示僅限 TPM 保護安裝對話。使用者可以按一下重新啟動與加密以立即重新啟動計算機並開始加密。

2.5.4 USB 金鑰

USB 金鑰模式使用儲存在 USB 快閃磁碟機上的金鑰進行驗證。

每次安裝，USB 快閃磁碟機都必須與計算機進行連接。

如果 TPM 不可用或者已透過 GPO 將其禁用，USB 金鑰保護將在 Windows 7 端點上使用。

USB 快閃磁碟機必須是 NTFS、FAT 或 FAT32 格式。exFAT 格式不受支援。此外，USB 快閃磁碟機必須是可寫入的。

如果符合全部條件，將會顯示 USB 金鑰保護安裝對話，使用者必須選擇一個已連接的 USB 快閃磁碟機，用於儲存金鑰。

使用者可以按一下重新啟動與加密以立即重新啟動計算機並開始加密。

2.6 BitLocker 組策略設定

Sophos Central 自動定義了一些組策略設定，因此管理員無需在進行裝置加密時準備計算機。

如果管理員已經定義了設定，則將不會覆寫已配置的值。

在計算機配置 > 管理樣本 > Windows 元件 > BitLocker 驅動器加密 > 操作系統驅動器下的本地組策略編輯器中，您可以找到以下策略：

原則	設定	Sophos Central 設定的值	註解
允許啟動時網路解除鎖定		已啟用	啟用 Central Device Encryption 後，您可以允許預先設定的 BitLocker 網路解鎖以繼續工作。
啟動時需要其他驗證	在不含相容 TPM 的情形下允許使用 BitLocker	已勾選	如果沒有可用的 TPM，將在 Windows 8 上進行這一步設定以允許在安裝時使用密碼解鎖系統磁碟。
啟動時需要其他驗證	設定 TPM 啟動 PIN	允許啟動 PIN 搭配 TPM	如果已設定裝置加密策略設定為需要安裝驗證且系統具有 TPM，那麼此組策略設定將設定為允許透過 TPM 保護系統磁碟機，同時要求使用者輸入 PIN 碼。
允許用於啟動的增強 PIN	無	已啟用	設定該功能以允許使用字母數字 PIN 保護帶有 TPM 的系統驅動器。如果無法設定，將僅允許使用數字。
配置預先開機復原訊息和 URL	選擇預先開機復原訊息的選項	使用預設復原訊息和 URL	這將設為使用 Sophos 的預設訊息和 URL。

原則	設定	Sophos Central 設定的值	註解
配置預先開機復原訊息和 URL	自訂復原訊息選項	沒有恢復金鑰？請聯絡 IT 服務台或前往自助入口網站： https://sophos.com/ssp	
配置預先開機復原訊息和 URL	自訂復原 URL 選項		
為固定的資料磁碟機配置使用基於硬體的加密	無	已停用	這將設為執行軟體型加密。但是，若現有 BitLocker 群組策略設定要求使用基於硬體的加密，則該策略設定不會被覆寫。
為作業系統磁碟機配置使用基於硬體的加密	無	已停用	這將設為執行軟體型加密。但是，若現有 BitLocker 群組策略設定要求使用基於硬體的加密，則該策略設定不會被覆寫。

- 要使用的加密算法：預設條件下，Sophos Central Device Encryption 使用 AES-256。有一種組策略設定可用於選擇 AES-128。
- PIN/密碼要求：有一種組策略設定可用於設定最小 PIN/密碼長度並需要使用複雜的密碼。
- 加密全部資料或僅加密已使用的空間：如果將開機卷和/或資料卷的組策略設定為需要進行完整加密，其覆蓋僅允許加密已使用空間的 Sophos Central 策略。

有些組策略設定可能與 Sophos Central 相衝突，因此加密無法啟用。在這種情況下，將向 Sophos Central 傳送事件。

- 需要智慧卡：如果組策略需要為 BitLocker 使用智慧卡，那麼 Sophos Central 不支援此種情況，同時會生成錯誤事件。
- 加密全部資料或僅加密已使用的空間：如果將開機卷和/或資料卷的組策略設定為僅加密已使用的空間，但 Sophos Central 策略需要進行完整加密，那麼這種情況下會生成錯誤事件。

如果要對平板電腦裝置（例如 MS Surface Pro）進行加密，並使用安裝驗證，則需要啟用以下組策略設定：

啟用需要平板電腦開機前鍵盤輸入使用 BitLocker 驗證

如欲瞭解更多詳情，請參閱知識庫文章 125772。

如需更多有關 BitLocker 和 TPM 群組策略設定的一般資訊，請參閱 BitLocker 群組策略設定和可信平台模塊服務群組策略設定。

相關概念

加密方法和報告 （第 9 页）
您可採用基於軟體或基於硬體的加密方式對磁區加密。

相關資訊

BitLocker 組策略設定
TPM 群組策略設定
知識庫文章 125772

2.7 限制

動態磁碟

BitLocker 不支援動態磁碟。端點向 Sophos Central 傳送事件，以通知您加密失敗。這是因為動態磁碟上的系統磁碟區無法加密。動態磁碟上的資料卷僅被忽略。

遠端桌面

在透過安裝有 Sophos Central 代理軟體的遠端桌面使用 Windows 端點時，如果部署了加密策略，將不會顯示任何對話，也不會執行裝置加密。啟用加密將帶來一個重新啟動序列，用於驗證硬體的相容性。使用者需要能夠在預先開機環境中輸入 PIN 碼/密碼，這不能透過遠端桌面完成。

2.8 加密方法和報告

您可採用基於軟體或基於硬體的加密方式對磁區加密。

裝置加密對新磁區一律使用基於軟體的加密，即使磁碟機支援基於硬體的加密。

若磁碟機使用基於硬體的加密，則不予變更。

若 BitLocker 群組策略設定要求使用基於硬體的加密，則不予變更。

在 電腦 頁面上，您可以根據電腦的加密狀態（例如加密方法或未加密的電腦）來篩選電腦。

電腦的詳細資料頁面會顯示磁區使用的加密方法和演算法。

對於 Windows 電腦，您還可參閱 加密開始日期。顯示的資訊取決於裝置。

- 對於已使用 Sophos Central Device Encryption 加密的電腦，它顯示電腦升級至 Sophos Central Device Encryption 2.1 版的日期和時間。
- 對於使用其他加密產品加密的電腦，它顯示安裝 Sophos Central Device Encryption 的日期和時間。
- 對於使用 Sophos Central Encryption 2.1（或更高版本）加密的新電腦，它顯示加密的日期和時間。

加密狀態 報告會顯示您電腦的加密狀態。

您可查看哪些電腦已加密，哪些磁碟區類型已加密，以及哪些電腦符合您的加密策略。您也可瞭解電腦的驗證方式及加密方式。

相關概念

BitLocker 組策略設定 （第 7 页）
Sophos Central 自動定義了一些組策略設定，因此管理員無需在進行裝置加密時準備計算機。

電腦

電腦摘要

2.9 關於解密

通常，您不需要解密。如果您需要將加密的端點從加密中排除，可以透過先移除策略中的所有使用者再將加密關閉的方式完成解密。

在 Windows Explorer（在端點上）中，在系統磁碟上按滑鼠右鍵並選擇「管理 BitLocker」。在「BitLocker 驅動器加密」對話中，按一下「關閉 BitLocker」。只有 Windows 管理員可執行此操作。

如果套用了加密策略，且具有管理權限的使用者嘗試手動解密他們的硬碟，Sophos Central 會覆蓋使用者的指令，磁碟將仍然處於加密狀態。

2.10 恢復 Windows 端點

如果使用者忘記了 BitLocker PIN 碼或密碼，他們可以使用兩種方式重新獲取對電腦的存取權。

- 使用者可前往 Sophos 自助入口網站，請參閱透過自助服務入口擷取修復金鑰。Windows 10 使用者收到 BitLocker 修復螢幕上的說明。
- 您可以幫助他們存取其電腦。這些說明會告訴您使用者將看到什麼內容以及他們需要做的事。他們必須：

1. 重新啟動電腦，並在 BitLocker 登入螢幕中按下 Esc 鍵。
2. 在 BitLocker 修復螢幕中，找到修復金鑰識別碼。
3. 呼叫管理員，並將修復金鑰識別碼告訴他們。
   您可以將修復金鑰給他們。有關檢索一位使用者的金鑰的幫助，請參閱 Sophos Central 幫助。
4. 使用者必須輸入修復金鑰，然後遵循螢幕上的指示建立新 PIN 碼或密碼。
   在執行 Windows 7 的電腦上，使用者將看不到任何說明。他們需要手動重設其 PIN 碼/密碼。

使用者可以重新存取其電腦。通常，只要使用者可以存取開機卷，資料卷就會自動解鎖。如果不是這種情況，您可以在 Sophos Central 中獲得資料卷的修復金鑰，方法與開機卷相同。

相關工作

透過自助服務入口擷取恢復密鑰 （第 18 页）
如果使用者無法登入到他們的計算機（忘記 BitLocker PIN 碼、macOS 密碼等），他們可以使用 Sophos 自助入口網站來擷取修復金鑰。

相關資訊

自助服務入口網站
Sophos Central 說明

3 管理 FileVault 加密

用於 Mac 的 Sophos Central Device Encryption 可管理 Mac 上 FileVault 的完整磁碟加密功能。使用者僅需使用他們的 macOS 登入密碼，即可加密和存取其資料。

3.1 轉移到 Sophos Central Device Encryption (Mac)

如果要使用 Sophos Central 管理已使用 FileVault 加密的 Mac 端點，則需要將 Sophos Central Device Encryption 策略套用於這些端點。

注意事項
如果將 FileVault 與 SafeGuard Enterprise 配合使用，則必須先解除安裝 Sophos SafeGuard Device Encryption 軟體。

使用者開始之前：

- 您必須在端點上安裝 Sophos Central 代理軟體。
- 您必須在 Sophos Central 中設定和開啟裝置加密原則。
- 使用者必須登入其端點。其必須連線到 Sophos Central 並與之同步。請注意，不支援遠端登入。

這些指示會告訴您使用者將看到什麼內容以及他們需要做的事：

1. 當使用者登入，或在使用者登入時套用 Sophos Central Device Encryption 策略時，將通知使用者已設定裝置加密以保護其計算機。
2. 若要開啟 Sophos Central Device Encryption，使用者必須輸入其登入密碼，然後點選創建金鑰。為了恢復，創建並集中儲存新修復金鑰。如果存在其他未加密的內部磁碟，則這些磁碟也將加密。您不需要為其建立單獨的磁碟密碼。
3. 如果有已使用磁碟密碼加密的內部磁碟，使用者必須輸入磁碟密碼，然後按一下繼續。現在，磁碟密碼由 Sophos Central 控制。在安裝期間，磁碟會自動解除鎖定。

現在，端點由 Sophos Central Device Encryption 管理。

3.2 逐步給裝置加密 (Mac)

請按照以下步驟給 Mac 加密。

使用者開始之前：

- 您必須在端點上安裝 Sophos Central 代理軟體。
- 您必須在 Sophos Central 中設定和開啟裝置加密原則。
- 使用者必須登入其端點。其必須連線到 Sophos Central 並與之同步。請注意，不支援遠端登入。

這些指示會告訴您使用者會看到什麼內容以及他們需要做的事。

1. 啟動 Mac 後，輸入他們的登入密碼。

   這會開啟 Sophos Device Encryption。
2. 點選加密以開始加密系統磁碟，或者點選延遲以稍後開始該進程。

使用者輸入其登入密碼並按一下加密時，修復金鑰會儲存在本機金鑰鏈以及 Sophos Central 中。

端點的所有現有使用者都會自動新增到 FileVault。

在運行 macOS 10.12 或早期版本的端點上，每位使用者需要單獨登入才能被新增至 FileVault。

系統磁碟加密後，內部資料磁碟區會自動加密。電腦啟動時，已加密的磁碟會自動解鎖。

通知會告訴使用者各個磁碟的加密狀態。

3.2.1 新增新的 FileVault 使用者

如果使用者未自動新增至 FileVault，這些說明會告訴您新的使用者會看到什麼內容以及他們需要做的事。

他們必須：

1. 輸入其登入密碼並點選繼續。
   使用者通常可以使用其 macOS 登入密碼存取其 Mac 並使用 FileVault。
2. 如果 Sophos Central 中尚未存儲修復金鑰，則新使用者必須選取可授權此任務的現有 FileVault 用戶。
3. 然後，現有的 FileVault 使用者需要輸入其登入密碼，並點選繼續。

現在，新使用者可以使用其 macOS 登入密碼存取其 Mac 並使用 FileVault。

3.3 恢復 Mac 端點

請依照下列步驟恢復 Mac 端點。

如果使用者忘記了登入密碼，有幾種方法可用於重新獲得電腦的存取權。

- 如果使用者是最後登入電腦的人員，他們可以使用 Sophos 自助入口網站，請參閱透過自助服務入口擷取修復金鑰。
- 使用者可以使用外部 Mac 安裝磁碟啟動電腦，然後使用 Terminal 命令解除鎖定磁碟。
- 使用者可以在目標磁碟模式中啟動其電腦，然後使用 Terminal 命令解除鎖定磁碟 。
- 使用者可以使用 macOS 恢復啟動其電腦，然後使用 Terminal 命令解除鎖定磁碟 。

  如需有關使用 Terminal 命令的資訊，請參閱使用 Terminal 命令解除鎖定 HFS+ 磁碟區和使用 Terminal 命令解除鎖定 APFS 磁碟區。

您可以幫助使用者重新獲取存取權。這些說明會告訴您使用者將看到什麼內容以及他們需要做的事。他們必須：

1. 打開端點電腦，然後等待，直至顯示修復金鑰識別碼。
   修復金鑰識別碼僅會顯示幾分鐘。要使其再次顯示，使用者必須重新啟動其計算機。
2. 呼叫管理員，並將修復金鑰識別碼告訴他們。
   您可以將修復金鑰給他們。有關檢索一位使用者的金鑰的幫助，請參閱 Sophos Central 幫助。
3. 點選密碼欄位中的問號圖示。
   顯示消息。
4. 點選訊息旁邊的箭頭圖示以切換到修復金鑰欄位。
5. 輸入恢復金鑰。

   對於從 Active Directory 中匯入的使用者，您需要執行以下額外步驟：

   - 重設 Active Directory 中的現有密碼。然後生成一個初始密碼，並將其提供給使用者。

- 告訴使用者按一下重設密碼對話方塊中的取消，然後輸入初始密碼。

6. 遵循螢幕上的說明以建立新密碼。
7. 如果出現提示，點選建立新金鑰鏈。

使用者可再次重新存取其計算機的開機卷。

在運行 macOS 10.12 或早期版本的端點上，新修復金鑰將會建立並儲存在 Sophos Central 中。一個修復金鑰僅能使用一次。如果稍後需要再次恢復電腦，您將需要擷取新的修復金鑰。

在運行 macOS 10.13 及 Apple 檔案系統 (APFS) 的端點上，不會建立新修復金鑰。現有的修復金鑰仍然有效。

相關工作

透過自助服務入口擷取恢復密鑰 （第 18 页）
如果使用者無法登入到他們的計算機（忘記 BitLocker PIN 碼、macOS 密碼等），他們可以使用 Sophos 自助入口網站來擷取修復金鑰。

使用 Terminal 命令解除鎖定 HFS+ 磁碟區 （第 13 页）
您可以使用 Terminal 命令來解鎖加密磁碟區。本節中的命令適用於具有格式為 HFS+ 的磁碟區的運行 macOS 10.12 或早期版本的端點。

使用 Terminal 命令解除鎖定 APFS 磁碟區 （第 13 页）
您可以使用 Terminal 命令來解鎖加密磁碟區。本節中的命令適用於運行 macOS 10.13 和 Apple 檔案系統 (APFS) 的端點。

相關資訊

關於 macOS 復原
如何選取不同的安裝磁碟
Sophos Central 說明

3.3.1 使用 Terminal 命令解除鎖定 HFS+ 磁碟區

您可以使用 Terminal 命令來解鎖加密磁碟區。本節中的命令適用於具有格式為 HFS+ 的磁碟區的運行 macOS 10.12 或早期版本的端點。

這些說明會告訴您使用者將看到什麼內容以及他們需要做的事。他們必須：

1. 打開 Terminal 應用程式並運行 diskutil corestorage list。
   將顯示所有連接的磁碟區的清單。
2. 搜尋要恢復的磁碟區名稱（LV 名稱），並注意邏輯磁碟區識別碼。
3. 請使用邏輯磁碟區識別碼作為修復金鑰 ID 呼叫管理員並請求修復金鑰。
   您將修復金鑰給他們。有關檢索一位使用者的金鑰的幫助，請參閱 Sophos Central 幫助。
4. 在磁碟密碼對話方塊中輸入修復金鑰以解除鎖定磁碟。
   或者，使用者可以使用命令 diskutil corestorage unlockVolume，並在 Terminal 應用程式中輸入修復金鑰來解除鎖定磁碟。

現在，可以在 Finder 中存取磁碟。

相關資訊

Sophos Central 說明

3.3.2 使用 Terminal 命令解除鎖定 APFS 磁碟區

您可以使用 Terminal 命令來解鎖加密磁碟區。本節中的命令適用於運行 macOS 10.13 和 Apple 檔案系統 (APFS) 的端點。

這些說明會告訴您使用者將看到什麼內容以及他們需要做的事。他們必須：

1. 打開 Terminal 應用程式並運行 diskutil apfs list。
   將顯示所有連接的磁碟區的清單。
2. 搜尋要恢復的磁碟區名稱，並記下磁碟區識別碼，如 Volume disk1s1。
3. 呼叫管理員並使用磁碟區識別碼作為修復金鑰 ID 請求修復金鑰。
   您將修復金鑰給他們。有關檢索一位使用者的金鑰的幫助，請參閱 Sophos Central 幫助。
4. 在磁碟密碼對話方塊中輸入修復金鑰以解除鎖定磁碟。
   或者，使用者可以使用命令 diskutil apfs unlockVolume，並在 Terminal 應用程式中輸入修復金鑰來解除鎖定磁碟。

現在，可以在 Finder 中存取磁碟。

相關資訊
Sophos Central 說明

3.3.3 錯誤：無法儲存修復金鑰

在極少數情況下，系統可能無法在本機（在金鑰鏈中）或 Sophos Central 中儲存修復金鑰。

這表示著如果使用者忘記密碼，機器將無法修復。為減輕此風險，將顯示修復金鑰的錯誤訊息，並提示使用者製作修復金鑰的副本。

系統將重複嘗試將修復金鑰儲存在 Sophos Central 中。一旦成功，將通知使用者現在由 Sophos Central 管理新修復金鑰，而他們可以銷毀其修復金鑰的副本。

3.4 裝置加密狀態（Mac）

使用者可以使用 Sophos Device Encryption 應用程式存取關於加密狀態的資訊。其安裝到應用程式目錄，並且可以透過 Finder、Launchpad 或 Spotlight 啟動。

Sophos Device Encryption 應用程式提供以下資訊：

- 策略狀態：第一行告訴使用者他們的端點是否由 Sophos Device Encryption 管理。
- 使用者狀態：第二行告訴使用者可以做及不可以做的事項。
- 磁碟狀態：將顯示所有內部磁碟的清單。如果磁碟名稱顯示為灰色，則說明磁碟當前未掛接。磁碟名稱旁邊的圖示表示磁碟的狀態。以下為可用的狀態：
  - 綠色：磁碟已完全加密，修復金鑰集中儲存。
  - 黃色：磁碟已完全加密，但修復金鑰未儲存在 Sophos Central 中。Sophos Central 當前無法連線時，可能會發生這種情況。如果不需要加密磁碟，則修復金鑰可能根本不存在。通常情況下，磁碟不是由 Sophos Central Device Encryption 管理，並且是使用作業系統工具加密。
  - 黃色 + 驚歎號標示：磁碟已完全加密，存在要求磁碟加密的策略，但沒有可用的修復金鑰。
  - 紅色：磁碟未加密，但要求磁碟必須加密的策略處於活動狀態。
  - 灰色：磁碟未加密，策略不需要加密或根本沒有策略。
  - 狀態列 + 正在加密：磁碟當前正在加密。
  - 狀態列 + 正在解密：磁碟當前正在解密。

注意事項
在 Mac 端點，具有管理權限的使用者可嘗試在套用加密策略時手動解密他們的硬碟，Sophos Central 無法覆蓋該指令，磁碟將解密。解密完成後，會要求使用者輸入其密碼以啟用 FileVault，並且磁碟將再次加密。

- 恢復狀態：在視窗底部，將通知使用者修復金鑰是否可用於其磁碟。

或者，您可以透過命令列工具存取有關裝置加密狀態的資訊。工具安裝在：/usr/local/bin/seadmin。以下為可用的命令：

- help: 顯示可用命令的清單。
- status: 顯示加密軟體的最後一次同步和同步間隔。
- --device-encryption: 顯示當前加密策略，以及所有內部磁碟的加密和恢復狀態。

4 用於安全共用的密碼保護檔案

您可在裝置加密策略中開啟此功能。

注意事項
該功能僅可用於 Central Device Encryption 2.0 或更新版本。這僅適用於 Windows。

您最多可以保護 50MB 的文件。

啟用按右鍵內容功能表：若您開啟此選項，建立受密碼保護的檔案選項就會顯示在右鍵功能表中。使用者傳送敏感資料給貴企業網路以外的收件人時，可在電子郵件中附加受密碼保護的檔案。檔案會包含在內容加密的新 HTML 檔案中。

收件人雙擊檔案並輸入密碼後，即可開啟檔案。他們可以將收到的檔案寄回，亦可用相同密碼或新密碼保護檔案，或者建立新的受密碼保護檔案。

啟用 Outlook 載入項：此選項會將電子郵件加密附件新增至 Outlook。使用者可在 Outlook 功能區選擇保護附件，對附件進行保護。所有未受保護的附件，會包含在內容加密的新 HTML 附件中，並寄出電子郵件。

始終詢問如何處理附加檔案：若您開啟此選項，使用者必須選擇在訊息中含有附件時，應如何傳送附件。可選擇以受密碼保護或未受保護兩種方式傳送。

您可輸入 始終詢問如何處理附加檔案 選項不適用的排除網域，例如您的組織網域。若收件人屬於該網域，就不會詢問寄件人希望如何處理附件。

僅限輸入完整的網域名稱，並以英文逗號分隔。

相關資訊
Device Encryption 策略

5 提示使用者變更其密碼/PIN

有兩種方法可提示使用者變更其密碼。

注意事項
此選項僅適用於 Windows。

- 使用加密策略中的 需要使用者提供新的驗證密碼/ PIN 選項。

  此選項預設為關閉。在指定時間後強制變更 BitLocker 密碼或 PIN。使用者變更其密碼或 PIN 後，會記錄此事件。

  注意事項
  該功能僅可用於 Central Device Encryption 2.0 或更新版本。

- 使用電腦詳細資料頁面的 摘要 標籤上的 觸發密碼/ PIN 的變更 選項。

  要求使用者立即變更 BitLocker 密碼或 PIN。成功傳送要求後，會顯示一則訊息。

在端點上，會提示使用者設定新的 BitLocker 密碼或 PIN。若使用者未輸入新密碼或 PIN 就關閉對話方塊，對話方塊會在 30 秒後再度出現。直到輸入新值為止。使用者關閉對話方塊五次且未變更密碼或 PIN 之後，會記錄警示。

相關資訊
Device Encryption 策略
電腦摘要

6 透過自助服務入口擷取恢復密鑰

如果使用者無法登入到他們的計算機（忘記 BitLocker PIN 碼、macOS 密碼等），他們可以使用 Sophos 自助入口網站來擷取修復金鑰。

有了修復金鑰，他們便可再次存取其電腦。

若要讓使用者能夠在自主入口網站中恢復其計算機，請前往 Sophos Central > 人員 > 使用者，選取一名或多名使用者，然後點選電子郵件設定連結按鈕。在以下對話方塊內，選取 Sophos Central 自助歡迎/設定電子郵件，以便向使用者傳送啟用連結。當使用者按照電子郵件中的指示操作時，他們可以使用 Sophos 自助入口網站來恢復其計算機。

這些說明會告訴您使用者將看到什麼內容以及他們需要做的事。他們必須：

1. 使用另一台計算機登入 Sophos 自助服務入口。
2. 前往裝置加密頁面。
   會顯示最後一個登入的使用者的所有計算機的清單。如果其他人同時登入計算機，使用者將無法透過自助服務入口對該電腦重新進行存取。
3. 從清單中選取電腦并在「修復金鑰」欄位下按「擷取」按鈕。
   將顯示一個帶有恢復金鑰的對話。
4. 啟動他們自己的計算機，然後前往恢復頁面。
   - Windows：按 Esc 鍵以切換至 BitLocker 恢復螢幕。
   - Mac：點選密碼欄位中的問號圖示，以便切換到 FileVault 恢復頁面。
5. 輸入恢復金鑰。

使用者可以重新存取其電腦。

相關資訊
自助服務入口網站

7 附加讀物

Windows

- 常見問題：知識庫文章 124819
- BitLocker 常見問題 (FAQ)
- BitLocker 群組策略設定
- TPM 基本功能
- TPM 群組策略設定：
- 受信任平台模塊管理技術概觀

Mac

- 常見問題：知識庫文章 125982
- FileVault 設定：使用 FileVault 將 Mac 上的啟動磁碟加密
- FileVault 修復金鑰：為您機構中的電腦設定 FileVault 修復金鑰
- 密碼重設：更改或重置 macOS 使用者帳號的密碼

相關資訊
BitLocker 常見問題 (FAQ)
BitLocker 組策略設定
TPM 群組策略設定
TPM 基本功能
受信任平台模塊管理技術概觀
使用 FileVault 將 Mac 上的啟動磁碟加密
為機構內的電腦設定 FileVault 復原密鑰
更改或重置 macOS 使用者帳號的密碼
知識庫文章 124819
知識庫文章 125982

8 支援的網頁瀏覽器

以下為當前支援的瀏覽器：

- Microsoft Internet Explorer 11 和 Microsoft Edge。
- Google Chrome。
- Mozilla Firefox。
- Apple Safari（僅限 Mac）。

我們建議您安裝或升級到以上清單中的支援版本，並且始終執行最新版本。我們的目標是支援最新版本和之前版本的 Google Chrome、Mozilla Firefox 和 Apple Safari。如果偵測到不受支援的瀏覽器，會將您重新導向 https://central.sophos.com/unsupported。

注意事項
行動裝置上不支援 Sophos Central Admin。

9 取得其他說明

若要 Sophos 支援獲取幫助：

1. 點選使用者介面右上角的說明，然後選取 建立支援票證。
2. 填寫表單。請儘量準確填寫，以便支援能夠有效地幫助您。
3. 或者，選擇讓支援可以直接存取您的 Sophos Central 工作階段的選項，以便 Sophos 更好地幫助您。
4. 按一下 傳送。

Sophos 將在 24 小時內聯絡您。

注意事項
如果選擇了讓支援可以存取您的 Sophos Central 工作階段的選項，則點擊 傳送 時會啟用此功能。遠端協助將在 72 小時後自動停用。若要更快將其停用，請點選您的帳戶名稱（使用者介面右上角），選取 帳戶詳細資訊，然後點選 Sophos 支援 標籤。

送出意見反應

若要向 Sophos 支援送出意見反應或建議：

1. 點選使用者介面右上角的 說明，然後選取進行意見反應。
2. 填寫表單。
3. 按一下 送出。

附加說明

您還可以按如下所述找到技術支援：

- 造訪 community.sophos.com/ 內的 Sophos 社群，尋找其他遭遇到相同問題的使用者。
- 造訪 www.sophos.com/zh-tw/support.aspx 內的 Sophos 技術支援知識庫。

10 法律聲明