Acrobat DC 安全性總覽

全球頂尖 PDF 解決方案，符合建立、編輯與管理文件之所需

目錄

當您將公司的資訊交由協力廠商應用程式託管時，安全性至關重要。Adobe 率先推行 PDF 及數位簽名標準，引領安全數位文件發展超過 20 年。全球成千上萬的組織已製作了數十億份的 PDF 文件，因為這些組織非常放心讓 Adobe Acrobat 軟體和 Adobe PDF 協助他們準備、保護和共用其最重要的日常文件。

Adobe Acrobat DC 搭配 Adobe Document Cloud 服務，堪稱是適用於現今行動互聯世界的完整 PDF 解決方案。這個解決方案將 Acrobat 桌面軟體與 Adobe Acrobat Reader 行動應用程式相結合，並輔以高階的行動功能及 Document Cloud 服務，在確保所有裝置間文件安全性的同時，協助各組織建立更明智的文件工作流程，並滿足用戶對行動解決方案的需求。有了 Acrobat DC，您就能隨時掌握並存取可依排程部署的最新安全性更新及最新功能。

本文涵蓋 Adobe 處理 Acrobat DC 相關之安全性的完整措施 (包括文件、應用程式及雲端安全性)，以協助保護您的資訊和獲得更好的體驗。

文件安全性

文件作者可以使用 Acrobat DC 軟體，建立 PDF 文件和套用許多安全性措施 (包括加密、存取控制、認證簽名)，以及透過密文工具永久移除文字和影像。Acrobat DC 中便利的「動作」功能可用來定義一組安全性工作，即使用戶未經正式訓練或不使用特殊工具也能輕鬆套用，讓各組織能夠輕鬆維持資訊的私密性和機密性。

加密

Acrobat DC 支援的安全性標準：

- 256 位元進階加密標準 (AES)
- 歐洲電信標準協會 (ETSI) 支援的標準

存取控制

輕鬆套用密碼和權限來控制存取或防止變更任何 PDF 文件、限制列印、複製或修改文件，讓您可放心共用文件。

電子簽名和數位簽名

Acrobat DC 中有兩種不同的工具可供用戶選擇，以便安全地使用簽名：「Send for Signature」和「認證」。

Send for Signature 可讓用戶管理端對端簽署流程，這些程序遵循美國、歐盟及全球大多數工業化國家的電子簽名法律。用戶可使用此工具來向他人索取簽名、追蹤簽署流程，以及自動封存已簽署文件和稽核記錄。整個過程都在安全管控中，而且文件與稽核記錄會經由 Adobe 認證並加上防竄改封印。Send for Signature 是由 Adobe Sign 提供支援，這是一個經獨立認證的 Adobe Document Cloud 解決方案，符合嚴苛的安全性標準，包括 ISO 27001、SOC 2 Type 2、HIPAA 及 PCI DSS。

認證工具可讓您使用 Adobe 認可的信任清單 (AATL) 或歐盟信任清單 (EUTL) 中所列的信任服務提供者核發的認證式數位 ID 來簽署文件。使用受信任第三方認證授權機構所核發的認證 ID 來簽署，是對文件進行電子簽署的最安全方法之一。此 ID 只會與簽署者本人連結，並且可以識別其身分。簽署者的認證會在簽署階段使用唯有該簽署者持有的私密金鑰，以密碼編譯方式繫結至文件。Acrobat DC 會自動與認證授權機構連線，以驗證他們的簽名 (及其所簽署之文件的真確性)。此類型的簽名符合 PDF 電子簽名標準，包括 PDF 進階電子簽名 (PAdES) 第 2、3 和 4 部分，以及美國國防部聯合互通測試司令部 (JITC) 使用密碼編譯及 PKI (採 AES-256/RSA-4096/SHA-512 演算法) 的方式。此認證工具也可讓您在文件上加入時間戳記，並提供防竄改封印以資證明。

若要進一步了解電子簽名和數位簽名，請參閱「使用電子簽名和數位簽名解決方案轉變業務流程」白皮書。

真實密文

Acrobat DC 提供一組可協助您保護敏感或機密資訊的密文工具。在分發文件之前，您可以先永久刪除文件中的文字和影像。您甚至可以根據模式 (例如電話、信用卡號碼和電子郵件地址) 搜尋和標記密文。您選取的資訊會從檔案中完全移除，不像其他工具或方法只是遮蔽而已。

使用「淨化文件」功能來移除隱藏資訊和非圖形物件，例如可能顯示於 PDF 的中繼資料。

Acrobat DC 中改進的安全性功能有助於防範某些攻擊，這些攻擊嘗試利用 PDF 檔案格式，在您的系統中安裝惡意程式碼及 / 或從系統擷取敏感資料。

應用程式安全性

在 Adobe，安全性做法已深植於我們的文化、軟體開發，以及工程設計流程。我們採用業界對於存取管理、資料保密和文件完整性等方面的標準安全性做法，精心打造 Acrobat DC 和 Acrobat Reader，以協助保護您的文件、資料和個人資訊。

安全工程

Adobe DC 應用程式的工程設計採用 Adobe 安全產品生命週期 (SPLC) 流程，其中包括數百項涵蓋軟體開發實務、程序及工具的嚴格安全性活動。Adobe SPLC 已整合至 Acrobat DC 產品生命週期的數個階段，從設計與開發到品質保證、測試和部署，環環相扣。如需 Adobe 安全性程序、社群參與和 Adobe SPLC 的詳細資訊，請參閱 www.adobe.com/security。

Adobe Acrobat Reader DC 中的保護模式

惡意程式碼會利用 PDF 格式來寫入或讀取電腦的檔案系統；為了保護您個人和組織不受此威脅，Adobe 提供尖端沙盒技術的實作，這項技術已在 Adobe Reader X 中採用，稱為「保護模式」。

Acrobat Reader DC 的「保護模式」不僅防禦嘗試在電腦系統上安裝惡意程式碼的駭客，現在也封鎖存取及擷取電腦或公司網路敏感性資料和智慧財產之惡意個人。

當您啟動 Acrobat Reader DC 時，「保護模式」預設為啟用。它會限制授予程式的存取權等級，確保執行 Microsoft Windows® 之系統的安全，以避免惡意的 PDF 檔案寫入或讀取電腦的檔案系統、刪除檔案或修改系統資訊。Reader 保護模式 (在 Windows 8.1 和更高版本中) 現在可以在 AppContainer 中執行。若要進一步了解 AppContainer，請參閱：https://msdn.microsoft.com/en-us/library/windows/desktop/mt595898(v=vs.85).aspx。

除了公司持續透過 SPLC 流程努力將安全性整合至產品生命週期的多個階段之外，Adobe 還會在此過程中定期審核現有程式碼並適時進行強化，進一步改善應用程式安全性，並在您使用 Adobe 產品時增強個人資料的安全。

Acrobat DC 中的保護檢視

「保護檢視」類似 Acrobat Reader DC 的「保護模式」是 Acrobat DC 豐富功能集的沙盒技術實作。在 Acrobat DC 中，Adobe 擴充「保護檢視」功能，不僅封鎖嘗試使用 PDF 檔案格式在電腦系統上執行惡意程式碼的寫入式攻擊，也封鎖嘗試透過 PDF 檔案竊取敏感性資料或智慧財產的讀取式攻擊。

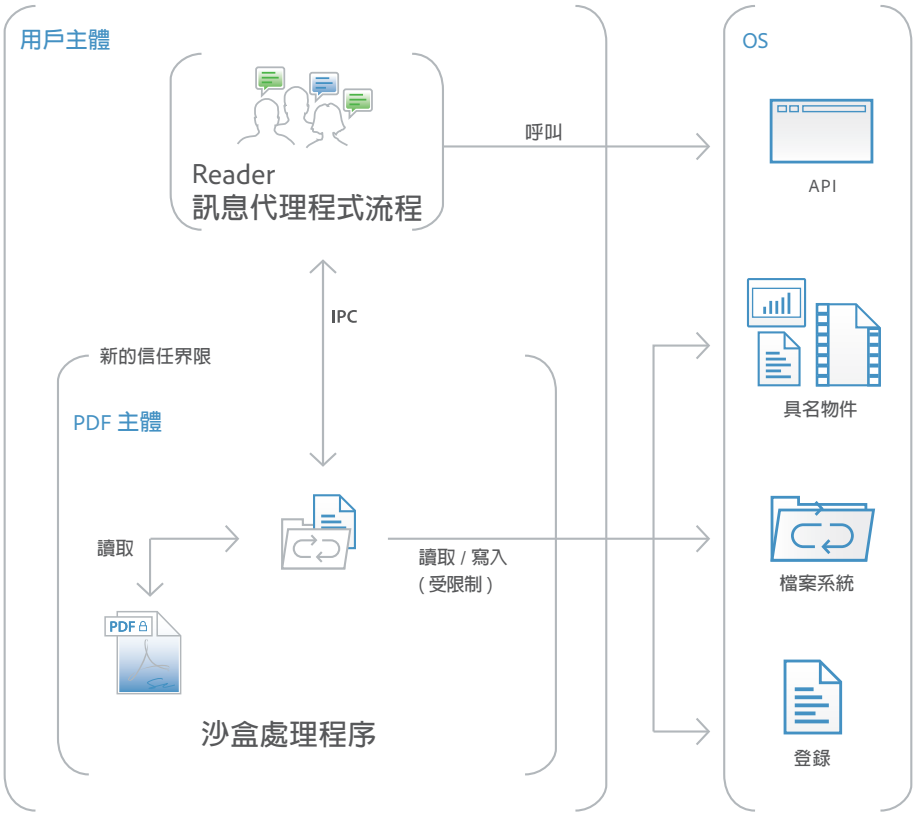
如同「保護模式」，「保護檢視」會將不受信任程式 (例如，任何 PDF 檔案和它所叫用的處理程序) 的執行侷限於沙盒，以避免使用 PDF 格式的惡意程式碼寫入或讀取電腦的檔案系統。

「保護檢視」假設所有 PDF 檔案都是潛在惡意檔案，並將處理侷限於沙盒，除非您明確指定檔案受信任。用戶在 Acrobat DC 獨立應用程式和在瀏覽器中開啟 PDF 文件的這兩種情況下都支援「保護檢視」。Windows 8 和更高版本中的「保護檢視」一律都在 AppContainer 中執行。如此可為啟用「保護檢視」的客戶提供更加穩固的鎖定環境。

當您在「保護檢視」中開啟可能有惡意的檔案時，Acrobat DC 會在檢視視窗頂端顯示黃色訊息列 (YMB)。YMB 指出檔案不受信任並提醒您現正處於「保護檢視」，藉此停用許多 Acrobat DC 功能及限制檔案內的用戶互動。基本上，檔案為「唯讀」模式，而且「保護檢視」會防止內嵌或標記 (tag-along) 惡意內容竄改您的系統。若要信任檔案及啟用所有 Acrobat DC 功能，您可以按一下 YMB 中的「啟用所有功能」按鈕。此動作會結束「保護檢視」，並透過將檔案加入至 Acrobat 授權位置清單，提供檔案的永久信任。後續每次開啟受信任的 PDF 檔案，都會停用「保護檢視」限制。

什麼是沙盒？

沙盒會建立受限制的執行環境，以便利用低權限來執行程式，因此受到安全性專業人員高度重視。沙盒協助保護用戶的系統，不受包含可執行程式碼之未受信任文件傷害。在 Acrobat Reader DC，未受信任的文件是任何 PDF 檔案和它所叫用的處理程序。Reader DC 將所有 PDF 檔案都視為可能發生損毀，並將 PDF 檔案叫用的所有處理程序侷限於沙盒。



JavaScript 執行

Acrobat DC 提供精密且細微的控制，可讓您跨越各種環境 (例如 Microsoft Windows 和 Macintosh) 將 JavaScript 執行列入安全清單和黑名單。Adobe JavaScript 安全清單架構會針對使用受信任認證所簽署的特定 PDF 檔案、網站、主機或文件，選擇性啟用 JavaScript。此外，Adobe JavaScript 黑名單架構可讓您在業務工作流程中使用 JavaScript，同時保護用戶和系統不受針對特定 JavaScript API 呼叫之攻擊的威脅。透過將特定 JavaScript API 呼叫加入至黑名單，您可以防止它執行，而不完全停用 JavaScript。您也可以防止個別用戶撤銷您封鎖特定 JavaScript API 呼叫的決定，協助保護整個企業不受惡意程式碼威脅。

安全清單架構

使用授權位置將文件列入安全清單，以便選擇性針對您信任的工作流程啟用 JavaScript，這可讓您根據 Microsoft Windows 安全性區域、已認證文件，或藉由新增特定檔案、檔案夾或主機來授予信任。

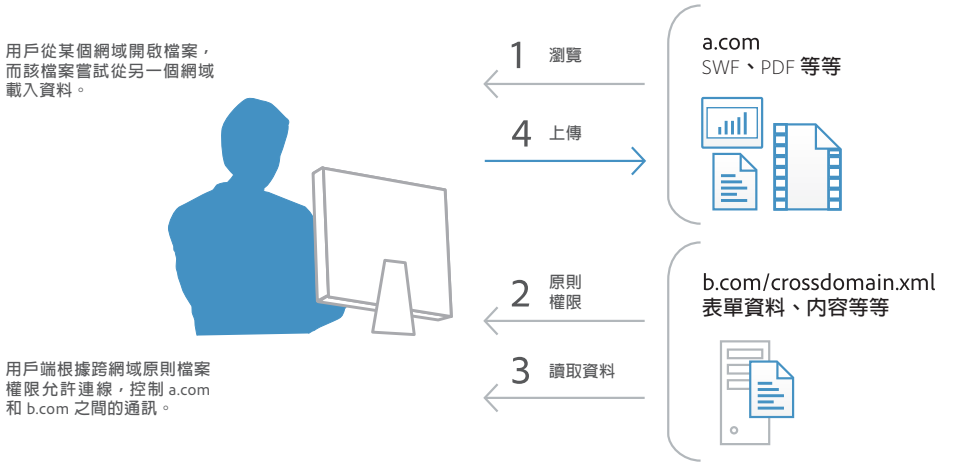
跨網域組態

根據預設，Acrobat DC 會停用 Windows 和 Mac OS X 用戶端的無限制跨網域存取，防止攻擊者利用豐富型 PDF 檔案來存取另一個網域的資源。

透過運用伺服器式、跨網域原則檔案的內建支援，您可以允許 Acrobat DC 和 Acrobat Reader DC 處理跨網域資料。此跨網域原則檔案 (XML 文件) 是裝載於遠端網域上，它會授予對來源網域的存取權，並允許 Acrobat DC 或 Acrobat Reader DC 繼續交易。

您可以在下列情況下啟用 Adobe 跨網域支援：

- 您需要選擇性的跨網域存取並想要運用其他功能，例如根據數位簽章的辨識功能。
- 您想要從單一伺服器位置，集中管理跨網域存取權限。
- 您需要實作包含多個網域之資料要求的工作流程，以傳回表單資料、SOAP 要求、串流媒體參照和 .NET HTTP 要求。



用戶易於辨識的安全性警告

除了 Adobe 事件回應流程和安全性警告之外，Acrobat DC 還會透過 YMB 實作用戶易於辨識的安全性警告方法。當您已啟用增強保全，而 PDF 檔案未設定為經授權或受信任的位置時，如果 PDF 檔案嘗試執行類似下列具潛在風險的動作，YMB 就會出現：

- 叫用跨網域存取
- 執行具特殊權限的 JavaScript
- 叫用 JavaScript 所叫用的 URL
- 呼叫已列入黑名單的 JavaScript API
- 注入資料
- 注入指令碼
- 播放內嵌的舊版多媒體

在 Acrobat DC 和 Reader DC 中，YMB 會出現在文件頂端並顯示警告或錯誤訊息。用戶可以選擇一次或永遠信任文件。選擇永遠會將文件新增至應用程式的授權文件清單中。

「選項」按鈕可讓用戶設定即時、一次或永遠信任。您也可以預先設定信任整個企業的檔案、資料夾和主機，讓受信任的企業工作流程中永不出現 YMB。

雲端安全性

Adobe 持續監控和改善雲端服務、系統及流程，以協助客戶因應日益增長的資料保全需求與挑戰。Document Cloud 服務 (包括 Acrobat DC 所使用的 Adobe Sign 和 PDF 服務) 是專為協助您確保文件機密性、完整性和可用性而設計。Document Cloud 服務遵循 ISO 27001、PCI DSS 和 SOC 2 Type 2 規範，並符合許多產業特定的其他合規性認證、標準及法規。如需我們雲端安全性措施的詳細資訊，請參閱「Adobe Document Cloud 安全性總覽」。

資料中心安全性

裝載 PDF 服務及檔案儲存空間的 Document Cloud 資料中心，現今位於由我們信任的雲端服務提供者 Amazon Web Services (AWS) 所管理的美國國家標準局 (ANSI) 層級 4 資料中心。AWS 在資料中心存取、容錯、環境控制和安全性方面，都保持極其嚴格的控制。只有獲核准、經授權的 Adobe 員工、雲端服務提供者員工，以及承攬有執照之合法業務的承包商，才能存取位於美國維吉尼亞州的受保護網站。如需 AWS 資料中心安全性的詳細資訊，請參閱 https://aws.amazon.com/security/。

資料加密和隱私權

Adobe 產品和服務 (包括 Document Cloud 服務) 在設計時已將隱私權考慮在內。Document Cloud 使用美國國家標準與技術局 (NIST) 進階加密標準 (AES) 256 位元加密來將閒置文件及資產加密，並在傳輸層安全性 (TLS) 所加密的連線中支援超文字傳輸通訊協定 (HTTP)，以確保傳輸中的資料也能受到充份保護。

Document Cloud 員工和受信任的廠商只能存取客戶資料來執行特定的 (或依法規定的) 業務及支援功能。Adobe 不會讓任何政府機構直接或有計畫地存取我們所儲存的客戶資料。如需 Adobe 隱私權政策的詳細資訊，請參閱 www.adobe.com/privacy。

與作業系統架構整合

永不間斷的安全性

Acrobat DC 運用 Windows 和 Mac OS X 作業系統中永不間斷的內建安全性防護，為您提供多一層的防護，防範攻擊者嘗試控制桌面系統或破壞記憶體。

「資料執行防止」(DEP) 會限制將資料或危險程式碼置入定義為受 Windows 作業系統保護之記憶體位置的行為。Apple 針對 Mac OS X Lion 提供類似的保護功能，包括堆疊 DEP 和堆積式 DEP，並將此延伸至 32 位元和 64 位元應用程式，讓所有應用程式更能抵抗攻擊。

位址空間配置隨機化 (ASLR) 會隱藏系統元件的記憶體和分頁檔位置，讓攻擊者難以找到和鎖定這些元件。Windows 和 Mac OS X Lion 都使用 ASLR。在 Mac OS X Lion 中，ASLR 已延伸至 32 位元和 64 位元應用程式。

登錄層級和 plist 組態

Acrobat DC 為您提供多種工具來管理安全性設定，包括登錄層級 (Windows) 和 plist (Mac OS) 偏好設定。使用這些設定，您可以在部署前後設定用戶端，以執行下列動作：

- 開啟或關閉增強式安全性
- 開啟或關閉授權位置
- 指定預先定義的授權位置
- 鎖定某些功能並停用應用程式用戶介面，讓用戶無法變更設定
- 停用、啟用或設定幾乎所有其他安全性相關的功能

更輕鬆的部署和管理

軟體安全性強化

安全性增強功能 (例如保護檢視) 只是 Adobe 在強化 Acrobat DC 不受威脅方面所做的大量工程投資範例之一。只要建立更健全不受攻擊威脅的軟體，Adobe 就可以減少或甚至免除非常態安全性更新的需求，並降低定期排定更新的緊急性。這些全都能提高作業彈性並降低整體擁有成本 (TCO)，在安全性保證需求很高的大型環境中，效果尤其顯著。

支援 Citrix 和應用程式虛擬化

您可以透過 Citrix XenApp、Citrix XenDesktop、VMware Horizon 及 Microsoft App-V 的指名用戶授權支援，讓用戶安全地從遠端存取所需的 Acrobat 功能。

支援企業行動力管理 (EMM) 解決方案

Adobe 在保護企業安全性及合規性的同時，也致力於協助企業客戶滿足對行動企業生產力解決方案的需求。Acrobat Reader 和 Adobe Sign 行動應用程式都支援 Android for Work EMM 平台，而適用於 Microsoft Intune 的 Adobe Acrobat Reader 則提供 iOS 和 Android 版本。Acrobat Reader 也支援 AppConfig 平台。進一步了解 IT 資源。

支援 Windows Server 群組原則物件和 Microsoft Active Directory

Windows Server 群組原則物件 (GPO) 和 Microsoft Active Directory 可讓您自動化電腦系統的一對多管理。Adobe 已在 Acrobat DC 中新增已認證 Microsoft Active Directory Administrative (ADM) 群組原則範本的支援，讓您提供隨選軟體安裝和應用程式自動修復。當您需要在部署後進一步設定應用程式時，可以使用 ADM 範本在整個組織中傳播必要的設定。

支援 Microsoft SCCM 和 SCUP

在 Acrobat DC，您可以有效率地透過 Microsoft System Center Configuration Manager (SCCM) 匯入和發佈更新，以確保受管理的 Windows 桌面永遠維持最新的安全性修補程式與更新程式。

Microsoft System Center Updates Publisher (SCUP) 目錄支援可讓您自動化整個組織的 Acrobat DC 軟體更新作業，並能簡化初始軟體部署。SCUP 會自動匯入 Adobe 發佈的任何更新，讓您更新 Acrobat DC 部署時更輕鬆並提高效率。與 SCCM 和 SCUP 整合可協助降低您擁有 Adobe 軟體的 TCO，因為您可以在全組織更輕鬆快速推出修補程式。

支援 Apple Package Installer 和 Apple Remote Desktop

在 Acrobat DC，Adobe 已實作 Mac OS X 所提供的標準 Apple Package Installer，而不是專屬 Adobe Installer。在企業中部署 Acrobat 軟體到 Macintosh 桌面更輕鬆，因為您現在可以使用 Apple Remote Desktop 管理軟體，從中央位置管理初始軟體部署和後續升級與修補。

累積、定期排定的更新與修補

為協助您更新軟體，Adobe 主動提供定期排程的更新，其中包含功能更新和安全性修補程式。為快速因應零時差攻擊，Adobe 也會視需要不定期提供修補程式。Adobe 會盡量運用累積修補，以降低保持系統最新狀態所需的心力和成本。Adobe 在發行前也會積極測試安全性修補程式，以協助確保現有安裝和工作流程的相容性。

每個計劃更新的日期將預先公佈於 Adobe 產品安全性事件回應團隊 (PSIRT) 部落格，網址是 blogs.adobe.com/psirt。

若要檢視 Adobe 產品的最新安全性公告和建議，請造訪 www.adobe.com/support/security。如需 Adobe 產品和安全性功能的詳細資訊，請造訪 Adobe Security Library，網址是 www.adobe.com/go/learn_acr_appsecurity_en。

Adobe 自訂精靈和企業工具組

為協助您進一步控制整個企業的部署，Adobe 提供下列工具：

- **Adobe** 自訂精靈—免費下載的公用程式，讓您在部署之前先自訂 Acrobat 安裝程式並設定應用程式功能。
- 適用於 **Acrobat** 和 **Windows** 的 **Adobe** 企業工具組 **(ETK)**—自動更新且可自訂的 Adobe 應用程式，包含 Adobe 偏好設定參照 (Preference Reference)。Adobe ETK 還包含一份仍在增加中的資源清單，可供企業管理員參考。

若要進一步了解這些工具，請造訪 IT 資源。

總結

Adobe 藉由 Acrobat DC 將 PDF 文件和個人資料的安全性帶入全新境界。我們所做的努力，從擴展應用程式安全性，到協助保護公司敏感資料和智慧財產免遭盜用，以及從封鎖危險的惡意程式碼使之無法安裝在電腦系統，到整合可讓全企業部署比以往更容易管理的工具，歷歷可見：Acrobat DC 以低於任何舊版 Acrobat DC 的 TCO 提供更高層級的安全性。

進一步了解
解決方案詳細資訊：
www.adobe.com/security

Adobe
Adobe
香港鋼鑼灣希慎道 33 號
利園大廈 4102 室
www.adobe.com

7/17