白皮書

網路會議：為您帶來安全、實時協作的優勢

本報告的重點為思科 WebEx Meeting Center、思科 WebEx Training Center、思科 WebEx Support Center 和思科 WebEx Event Center 的安全資訊。

簡介

思科 WebEx® 線上方案有助全球的員工和虛擬團隊以實時方式見面和協作，就像是在同一個房間工作一樣。事實上，線上協作比面對面的協作更加有成本效益，節省出行的時間和開支，甚至可以無需會議室空間。全球的企業、機構和政府都使用思科 WebEx® 方案來簡化業務流程，提高銷售、營銷、培訓、項目管理和技術支援團隊的工作成果。

對於所有這些企業和機構來說，資料安全是一項最需要關注的基本元素。從排定會議，到認證參加者，以至檔案共用，線上協作都必須提供到多重安全保障。

思科在設計、部署和維護網路、平台和應用程式時，視安全為最重要的考慮元素。您可以放心在商務程序中使用 WebEx® 解決方案，我們的服務能夠符合您的嚴格安全要求。

了解思科 WebEx 線上應用程式的安全功能，以及當中所包含的通訊基礎架構思科 WebEx Cloud，從而成為您在投資決策中重要的一部分。

思科 WebEx Cloud 基礎架構

思科 WebEx Meetings 是一套以思科 WebEx Cloud 傳送的軟體即服務（SaaS）解決方案，此方案是一項有優質安全性的服務平台，兼具領先業界的卓越性能、可擴展性及可用性。思科 WebEx Cloud 為您帶來易於部署和方便易用的程式，除可降低總購置成本外，亦同時帶來最高等級的企業安全。

切換架構

思科部署了分布全球的專用網路，帶來高速的會議交流。透過思科 WebEx Cloud，從主講者電腦到達參加者電腦上的會議階段作業資料會予以切換，不會永久儲存。[1]

資料中心

思科 WebEx Cloud 是一項用於實時網路通訊的基礎技術。WebEx 會議階段作業使用多個位於世界各地的資料中心來切換裝置。這些資料中心經過特別部署，以放置在靠近主要互聯網接入點的位置，並使用全球各地的專用高頻寬光纖來路由流量。思科在思科 WebEx Cloud 中運作整個基礎架構。來自美國的資料會留在美國地區，而在歐洲內的資料則會留在歐洲地區。

此外，思科營運網路提供點 (PoP) 地點，以增強主幹連線、互聯網對等、全球站點備份和緩存技術，提升最終使用者的操作表現和可用性。思科人員提供全天候的後勤安全、操作和變更管理支援。

[1] 當使用者啟用網路錄製（NBR）功能，便會將會議錄製和儲存下來。除 NBR 外，WebEx 也會儲存使用者設定檔資料和使用者檔案。

高度安全的 WebEx 會議體驗概述

WebEx 會議體驗包括：

- 會議站點配置
- 在排定中使用的安全選項
- 開始及加入 WebEx 會議的選項
- 加密技術
- 傳輸層安全性
- 防火牆兼容性
- 會議資料隱私
- 會議安全性
- 單次登入
- 第三方認證資格（獨立審核驗證的思科 WebEx 安全性）

「WebEx 會議」和「思科 WebEx 會議階段作業」是指所有使用思科 WebEx 線上產品的整合音訊會議、網路音訊會議以及單人及多人視訊會議。這些產品包括：

- 思科 WebEx Meeting Center
- 思科 WebEx Training Center
- 思科 WebEx Event Center
- 思科 WebEx Support Center（包括思科 WebEx Remote Support 和思科 WebEx Remote Access）

除非另有指明，本文件中所描述的安全功能乃等同於上述所有的 WebEx 應用程式。

WebEx Meeting 的角色

WebEx 會議的四個角色為主持人、候補主持人、主講者和出席者。以下部分將描述每個角色的安全權限。

主持人

主持人可排定及開始一場 WebEx 會議。主持人可控制會議體驗。從安全的角度考慮，主持人可以將主講者權限授予給出席者。主持人還可以鎖定會議和驅逐出席者。

候補主持人

主持人可任命候補主持人，以代替主持人開始已排定的 WebEx 會議。從安全的角度考慮，候補主持人擁有主持人相同的權限。

主講者

主講者可以共用簡報、指定的應用程式或整個桌面。主講者可控制會議註解工具。從安全的角度考慮，主講者可以授予和撤銷共用應用程式的遠端控制予個別出席者。

出席者

出席者沒有任何安全職責和權限。

WebEx 網站管理模組

WebEx 網站管理模塊允許獲授權的管理員在各個會議期間，為主持人和主講者的權限進行管理和執行安全措施。例如，您可以自行定制每個階段作業的配置，在個別網站或個別使用者的基礎上禁止主講者共用應用程式或傳輸檔案。

WebEx 網站管理模組可管理以下安全功能：

帳戶管理

- 達到某個設定次數的失敗登入後鎖定帳戶
- 在指定時間間隔自動解除鎖定帳戶
- 停用在特定期間內沒有活動的帳戶

特定使用者的帳戶操作

- 要求使用者在下次登入時更改密碼
- 鎖定或解鎖使用者帳戶
- 啟動或停用使用者帳戶

帳戶建立

- 新帳戶申請需要填寫安全文字
- 新帳戶申請需要電郵確認
- 新帳戶申請允許自助登記（註冊）
- 設置新帳戶申請的規則

帳戶密碼

強制使用安全性強的帳戶密碼，其中包括：

- 混合使用大小寫
- 最短長度
- 最少需要的數字字符數
- 最少需要的英文字母數
- 最少需要的特殊符號數
- 相同的字符不得重複三次或以上
- 不得重用之前用過的密碼指定次數
- 不得使用動態文字（網站名稱、主持人名稱、使用者名稱）
- 不得使用設定清單的密碼（例如「password」）
- 更改密碼前的最短時間間隔
- 主持人在指定的時間間隔需要更改帳戶密碼
- 所有使用者在下次登入時需要更改帳戶密碼

個人會議室

個人會議室是使用個人化網址和密碼來進入。在這些會議室中，主持人可以列出已排定和正在進行的會議，開始及加入會議，以及與出席者共用檔案。管理員可以為個人會議室設定安全相關的功能，其中包括：

- 在個人會議室共用檔案的選項
- 在個人會議室存取檔案密碼的要求

WebEx 網站管理的其他安全相關功能

- 主持人或出席者可以選擇儲存名字和電郵地址，令安排或加入新會議變得更簡單。
- 主持人可以將錄製檔重新指派給其他主持人。
- 藉著要求所有主持人和出席者驗證身份，以限制網站存取。需要取得認證以存取任何網站資料，如已公開的會議、以及取得會議的存取權。
- 強密碼規則可以套用在 WebEx Access Anywhere 中。
- 所有會議都可以選為不公開。
- 可按需要批准「忘記密碼？」請求。
- 可以按需要來重設帳戶密碼，無需以使用者身份重新進入。

排定 WebEx 會議的安全選項

- 個別主持人可以得到指定會議存取安全的能力（在網站管理層級（不可予以覆寫）中所設定的參數內）。
- 可以選擇不公開某個會議，使其不在行事曆上顯示。
- 主持人加入會議前，可以容許出席者先加入會議。
- 主持人加入會議前，出席者可以存取音訊。
- 只有在 WebEx 網站上擁有帳戶的出席者，才可加入會議。
- 電話會議資訊可以在會議中顯示。
- 設定如果只剩下一位出席者，會議可依設置的時間自動結束。
- 可要求出席者加入會議室時輸入他們的電郵地址。

公開或不公開的會議

主持人可以選擇在 WebEx 網站的行事曆中公開列出會議。或者排定會議為不公開，讓其不在行事曆上顯示。主持人需要明確地告知出席者關於那些不公開的會議，他可選擇以電郵邀請向出席者發送鏈結，或要求出席者在加入會議頁面時輸入提供的會議號碼。

內部或外部會議

主持人可以限制會議只能由在自訂 WebEx 網站上擁有帳戶的出席者加入，並以是否能夠登入網站來予以驗證。

會議密碼

主持人可以設定會議密碼，然後選擇在會議邀請電郵裡是否加入密碼。

註冊

- 主持人可以使用註冊功能來限制會議的存取。主持人可建立一個「存取控制清單」，只允許曾註冊過及獲得主持人明確批核的使用者加入會議。
- 可以透過在 WebEx Training Center 和 WebEx Event Center 阻止重用註冊 ID ，以確保會議的安全度。任何出席者嘗試重用已被使用的註冊 ID，均會被阻止加入會議。這方法可以防止多個出席者共用 ID。
- 另外，主持人可以限制參加者的存取和驅逐參加者，以確保會議的安全性。

這些排定選項的組合可以任意進行調整，以符合安全政策。

開始及加入 **WebEx 會議**

主持人的用戶 ID 和密碼在您自訂的 WebEx 網站中通過認證後，WebEx 會議即可開始。主持人是會議的首要控制者，並也是會議的首位主講者。主持人可以向其他出席者授予或撤回主持或主講的權力、驅逐指定的出席者，或在任何時候終止階段作業。

主持人可以指定後補主持人，讓他們在主持人無法參加會議或失去網路連線的時候開始或控制會議。這樣可以提高會議的安全度，防止主持人的職務隨機分配給任何未經授權的出席者。

您可以設定由您自訂的 WebEx 網站，以允許出席者在主持人加入前參加會議，包括音訊部分，並限制出席者在提早加入會議時可使用的聊天和音訊功能。

如出席者首次參加 WebEx 會議，其電腦會自動下載並安裝 WebEx 客戶端軟件。WebEx 客戶端軟件擁有 VeriSign 公司頒發的數碼簽名。在之後的會議中，WebEx 應用程式只會下載並安裝具有更改或更新的檔案。出席者可以使用電腦作業系統的取消安裝功能輕鬆移除 WebEx 檔案。

加密技術

WebEx 會議的設計目的是讓每個 WebEx 會議階段作業的參加者，都可以在安全的環境中參與實時及有豐富媒體內容的會議。當主講者共用檔案或簡報時，內容將會受到 Cisco® 專利的通用通訊格式 (UCF) 技術編碼，從而優化共用的資料。在 iPad、iPhone 和 BlackBerry 行動裝置上也可以使用 WebEx 會議應用程式，當中採用的加密機制和電腦客戶端類似。

WebEx 會議提供以下加密機制：

- 在電腦和行動裝置的 WebEx 會議中，資料會採用 128 位元的安全套接字層（SSL）技術，從客戶轉移到 Cisco WebEx Cloud。
- 終端到終端（E2E）加密技術是 Cisco WebEx Meeting Center 的其中一個選項。這個方法使用高級加密標準（AES），以終端到終端的方式加密所有會議內容，並採用主持人電腦隨機建立的 256 位元密鑰，將其分發給出席者作為公開密鑰。E2E 技術和在 Cisco WebEx Cloud 一方終止的 SSL 加密技術不同，它可以為所有 Cisco WebEx Cloud 基礎架構的會議內容加密。只有在出席者電腦上才會顯示清晰的文字會議內容。[2]
- 如使用者選擇有關的「記住我」選項，儲存在電腦及行動裝置上的 WebEx 會議使用者登入 ID 和密碼將會使用 128 位元 AES 加密。

網站管理員和會議主持人可以在「會議類型」選項中選擇 E2E 加密技術。E2E 方案所提供的安全性比單獨使用 AES 更強（雖然 E2E 加密技術亦有使用 AES 負載加密），全因該密鑰只有會議主持人和出席者知道。

每一個從 WebEx 會議客戶端到 WebEx Cloud 的連線都會採用加密代幣驗證，所以只有合資格使用者才可以加入特定的會議。

[2] 請留意，啟用 E2E 加密技術時，NBR 技術將無法使用。此技術只在 WebEx Meeting Center 中提供。

傳輸層安全性

在應用程式層面的安全保障上，所有會議資料的傳輸都使用 128 位元 SSL。SSL 使用防火牆端口 443（用於 HTTPS 流量），而非使用防火牆端口 80（用於標準 HTTP 互聯網流量）來穿越防火牆。

連接到 Cisco WebEx Cloud 的 WebEx 會議出席者會使用應用程式的邏輯連接 /presentation/session 層面。出席者電腦之間將沒有點對點的連線。

防火牆兼容性

WebEx 會議應用程式與 Cisco WebEx Cloud 之間的通訊使用 HTTPS（443 端口），以建立了可靠及極度安全的連線。因此，您的防火牆不需要特定的設定來啟用 WebEx 會議。

會議資料隱私

所有 WebEx 會議內容（聊天、音訊、視訊、桌面或檔案共用）都是暫時的（只會在會議期間存在）。在預設的情況下，會議內容不會儲存在任何一部思科雲端或參加者的電腦中。思科只會保留兩類會議資料，包括：

- **活動詳細錄製（EDR）：**思科使用 EDR 作計費和報告用途。您可以使用您的主持人 ID 登入自行定制的 WebEx 網站，以查看活動的詳情資料。一旦驗證獲得通過，您還可以從 WebEx 網站下載，或者使用 WebEx API 來存取這些資料。EDR 包括基本的會議出席資料，包括何人（使用者名稱和電郵）加入了甚麼會議（會議 ID）以及時間（加入和離開時間）。
- **網路錄製（NBR）檔：**如主持人選擇錄製一個 WebEx 會議階段作業，錄製檔將會儲存在 Cisco WebEx Cloud 中，並可以到您自行定制的 WebEx 網站中 MyRecordings 部分存取檔案。只有在會議主持人於會議期間啟用 NBR，或選擇整個網站選項來錄製整場會議，系統才會建立這個檔案。NBR 可以透過 URL 鏈結來存取。每個鏈結都包含一個不可預測的代幣。主持人能全權控制 NBR 檔案的存取，包括刪除、共用或新增密碼來保護檔案。NBR 為可選功能，並可由管理員選擇關閉。

單次登入

思科使用安全聲明標記語言（SAML）1.1 及 2.0 和 WS-Federation 1.0 協定，來支援使用者單次登入（SSO）的聯合身份驗證。正逐步淘汰對 SAML 1.1 的支援。使用聯合驗證需要您將公共密鑰 X.509 證書上傳到您自定的 WebEx 網站。然後，您可建立包含使用者屬性的 SAML 聲明，並以相符的隱私密鑰以數碼方式簽署聲明。WebEx 認證使用者之前，會先行利用預載的公共密鑰證書，以對比方式驗證 SAML 聲明的簽名。

第三方報告

除了自身嚴格的內部程序外，思科的安全部門會與多個獨立第三方合作，以針對思科內部策略、程序及應用程式履行縝密的審查。這些審計的目的，是為商業和政府應用程式驗證關鍵任務的安全需求。

第三方安全評估

思科使用第三方供應商進行持續、深入、設有代碼輔助的滲透測試和服務評估。在合作中，第三方會執行以下安全性評估：

- 識別關鍵的應用程式及/或服務漏洞，並提出解決方案
- 建議改善架構的一般範疇
- 識別編碼錯誤，並為編碼實行的改進提供指引
- 直接與 WebEx 工程人員合作，解釋調查結果和為工作提供指引

安全港證書

思科於 2012 年 3 月獲得客戶及合作夥伴資料的安全港證書（有關員工資料的安全港證書已經在 2011 年獲得）。該證書是思科全面隱私合規計劃的一個附加組件，雖然沒有任何政府或標準委員會的要求規管，但公司深明客戶對此證書的重視。

歐盟資料保護指令禁止將歐盟公民的個人資料，轉移至不符合歐盟隱私保護「適當性」標準的非歐盟國家。美國商業部為求與歐盟委員會的要求一致，制定了安全港架構，讓美國企業遵守一系列安全港隱私原則指令。公司需要在美國商務網站上證明會遵守這些原則。該框架於 2000 年獲得歐盟認可，並使公司有一致的原則，讓歐盟確保歐盟公民有「足夠」的隱私保護。

SSAE16

普華永道會計師事務所按照註冊會計師美國研究所建立的標準，執行鑑證業務第 16 號（SSAE16）聲明的年度審計。更多 SSAE16 的資料，請參考：http://www.ssae16.com。

ISO 27001 及 27002

思科已於 2012 年 10 月為 WebEx 服務取得 ISO 27001 認證。認證每三年更新一次，並每年接受中期外部審計。ISO 27001 是一套由國際標準化組織（ISO）頒布的資料安全標準，當中提供了資料安全管理系統（ISMS）的最佳實踐建議。ISMS 是一套政策和程序框架，當中包括組織在資料風險管理程序中的所有法律、行政、物理和技術控制。根據文件，ISO 27001 的開發乃「為建立、實行、運作、監控、審查、維護和改進資料安全管理系統提供示範。」點按以下鏈結以查看 ISO 27001 和 27002 的更多資訊：http://www.27000.org/。

瞭解更多資訊

更多有關思科 WebEx 解決方案的資訊，請瀏覽 www.cisco.com/c/zh_hk/products/conferencing/index.html，或聯絡您的銷售代表。

美洲總部
Cisco Systems, Inc.
加州聖荷西市

亞太區總部
Cisco Systems (USA) Pte. Ltd.
新加坡

歐洲總部
Cisco Systems International BV 荷蘭
阿姆斯特丹

思科在全球擁有 200 多個辦公室。思科網站（**www.cisco.com/go/offices**）列有地址、電話號碼以及傳真號碼。

美國印製 C11-709579-01 04/14