

Change Auditor for Exchange

適用於 Exchange 和 Exchange Online 的即時稽核

電子郵件已成為組織內部及組織之間通訊的主要商務工具。因此，電子郵件可作為資訊的存放庫，其中包含部分敏感且容易遭人濫用的資訊。許多組織原則違規情形往往不會被發現，因為大多數的安全性動作並未接受稽核。而這可能導致生產力喪失和系統停機時間，任何組織都不該承擔這樣的風險。

現今的公司行號需要適用於 Microsoft Exchange Server 和 Office 365 安全性與法規遵循的深入稽核和報告功能，以證明符合法規並提高效率。

Quest® Change Auditor for Exchange 可主動稽核 Exchange 環境中發生的活動、防止他人存取重要信箱，以及在發生重大變更時提供即時的詳細警示。持續掌握最新狀況可協助您證明符合法規、強化安全性及改善連續運作時間，同時主動稽核對 Exchange Server 和

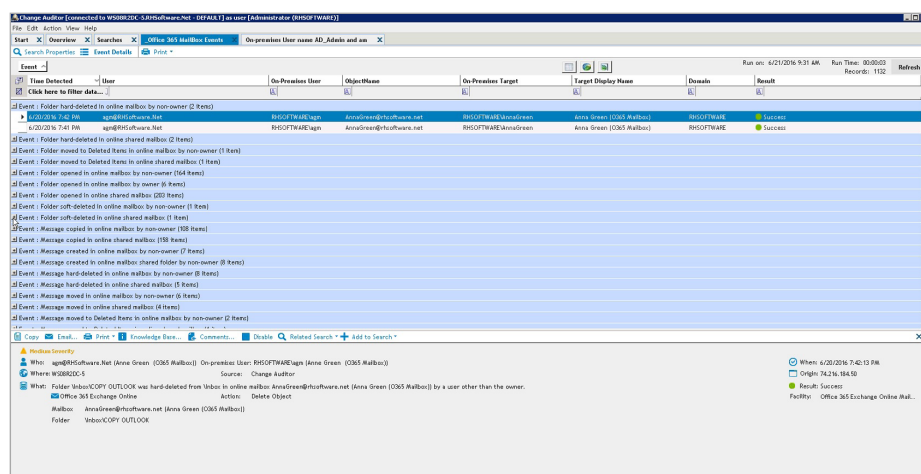
Exchange Online 設定與權限所做的變更。您將能夠針對 Exchange 和 Exchange Online 安全性與原則設定展開追蹤、發佈警示及產生報告，以及透過主動收集與重大變更相關的所有資訊 (包括原始與最新數值)，對其他問題快速進行故障診斷。

稽核所有重大變更

Change Auditor for Exchange 可針對 Exchange Server 和 Office 365 託管 Exchange 元件的所有重大變更，包括管理群組、信箱原則、公用及私人資訊存放區稽核、組織變更 (例如 ActiveSync 信箱原則變更、發佈清單變更等)，提供豐富且可自訂的稽核和報告功能。您將能依時間順序充分掌握所有變更，並獲得深入解析的鑑識情報，瞭解變更的人員、內容、位置、時間、原因以及來自哪個工作站，包括任何相關事件的詳細資料以及變更前後的值。此外，透過對所有裝置發佈

優點：

- 只需幾分鐘即可完成安裝；可快速收集事件資訊，立即分析 Exchange 和 Exchange Online 環境
- 可從單一用戶端，執行涵蓋整個企業的稽核與法規遵循工作
- 防止存取敏感或重要信箱，並限制授權使用者的控制能力，藉此強化內部控制
- 透過對所有裝置傳送即時警示，做出立即的回應，以降低安全性風險
- 消除不明安全疑慮，透過追蹤所有事件以及與特定事件相關的變更，確保能夠持續存取 Exchange 和 Exchange Online 設定、信箱以及使用者
- 主動對原則和 Exchange 公用資料夾的變更進行故障診斷，以提高可用性
- 不使用原生稽核方式來收集事件資訊，以降低對伺服器效能的影響，並省下儲存資源
- 簡化內部原則和外部規範 (包括 GDPR、SOX、PCI DSS、HIPAA、FISMA 及 SAS 70 等) 的合規報告
- 將資訊轉為深入解析的鑑識情報，供稽核人員和管理階層使用



Change Auditor for Exchange 概觀畫面

Exchange 使用者在數個月內即可獲得投資報酬率

69% 的受訪 IT 部門選擇 Change Auditor for Exchange 後，在六至九個月或更短的時間內即成功回收其投資。

TechValidate 問卷調查

系統需求

如需詳細需求的完整清單，請參閱版本說明指南。

即時警示，您將能隨時保持警戒，並在發生重大原則變更時有效因應，以降低日常修改所產生的相關風險。

追蹤使用者活動及保護敏感信箱

Change Auditor for Exchange 可針對使用者帳戶和交付限制變更，追蹤使用者和系統管理員活動，以協助強化整個企業的稽核與法規遵循原則。Change Auditor 還可防止未經授權的使用者存取信箱，並提供有關已存取其他使用者信箱之系統管理員和使用者的資訊。您將可實際看到哪些人員存取、刪除、複製、移動或建立了該信箱中的電子郵件。透過 24 小時全年無休的即時警示、深入分析及報告功能，保護您的 Exchange 和 Exchange Online 基礎架構免於受到可疑行為的影響和未經授權的存取行為，並且始終符合企業與政府的標準。

使用 ACTIVESYNC 稽核行動裝置

使用 Microsoft 的 ActiveSync 技術稽核行動裝置，並追蹤電子郵件和行事曆存取、裝置註冊等。

將不相關的資料轉換為具有意義的資訊，藉此提高安全性和法規遵循成效

Change Auditor for Exchange 會追蹤 Exchange 和 Exchange Online 環境的重大變更，然後將原始資料轉譯為具有意義的情報資料，協助保障基礎架構的安全性和合規性。多虧 Change Auditor 的高效能稽核引擎，稽核限制已成為歷

史，現在您不需要原生稽核記錄，即可更快地得出結果並節省儲存資源。

整合式事件轉送

輕鬆與 SIEM 解決方案整合，將 Change Auditor 事件轉送至 Splunk、ArcSight 或 QRadar。此外，Change Auditor 可整合 Quest® InTrust®，以 20:1 的壓縮率儲存事件，並透過對可疑事件的警示和自動化回應動作，集中收集、剖析及分析原生或第三方紀錄。

自動報告以符合企業與政府規範

運用 Microsoft 的 SQL Reporting Services (SRS)，Change Auditor for Exchange 可即時提供簡潔且具有意義的安全性和法規遵循報告。利用內建的法規遵循資料庫，以及建立專屬自訂報告的功能，證明符合一般資料保護規範 (GDPR)、沙賓法案 (SOX)、支付卡產業資料安全標準 (PCI DSS)、健康保險可攜性及責任法案 (HIPAA)、美國聯邦資訊安全管理法案 (FISMA)、稽核標準第 70 號準則 (SAS 70) 等標準的法規要求，變得易如反掌。

關於 QUEST

Quest 為快速變遷的企業 IT 世界提供軟體解決方案。我們協助簡化資料暴增、雲端擴張、混合式資料中心、安全威脅和法規要求所帶來的挑戰。我們的產品組合包含用於資料庫管理、資料保護、統一端點管理、身分識別與存取權管理，以及 Microsoft 平台管理的解決方案。