TREND MICRO™

TREND MICRO™ Remote Manager™

版本：2018 年 4 月

管理手冊

Security Management

文件編號：APTMS8225/180330

發行日期：2018 年 4 月

受美國專利保護，專利編號： 專利申請中。

本文件介紹了服務的主要功能，並/或提供作業環境的安裝說明。在安裝或使用本服務前，請先閱讀此文件。

如需有關如何使用服務特定功能的詳細資訊，請參閱趨勢科技線上說明中心和/或趨勢科技常見問題集。

趨勢科技十分重視文件品質的提升。如果您對於本文件或其他趨勢科技文件有任何問題、意見或建議，請與我們聯絡，電子郵件信箱為 docs@trendmicro.com。

請至下列網站並給予您對此文件的評估意見：

http://www.trendmicro.com/download/documentation/rating.asp

隱私權資料和個人資料蒐集披露

趨勢科技產品中所提供的部分功能會蒐集與產品使用和偵測相關的資訊，並建議傳送回饋給趨勢科技。少數資訊在部分司法管轄權和法規下會視為個人資料。如果您不希望趨勢科技蒐集您的個人資訊，則建議您務必詳細瞭解並確認是否要關閉相關功能。

以下連結列出 Remote Manager 將蒐集的資料類型，並提供有關如何關閉特定資訊回饋功能的詳細說明。

https://success.trendmicro.com/data-collection-disclosure

趨勢科技所蒐集的資料將遵循趨勢科技隱私權政策中的規定：

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

目錄

部分 III：管理趨勢科技產品

第 4 章：Remote Manager 中的 Cloud App Security

第 5 章：Remote Manager 中的 Cloud Edge

第 6 章：Remote Manager 中的 Hosted Email Security

第 7 章：Remote Manager 中的 InterScan Web Security as a Service

第 8 章：Remote Manager 中的 Worry-Free Business Security

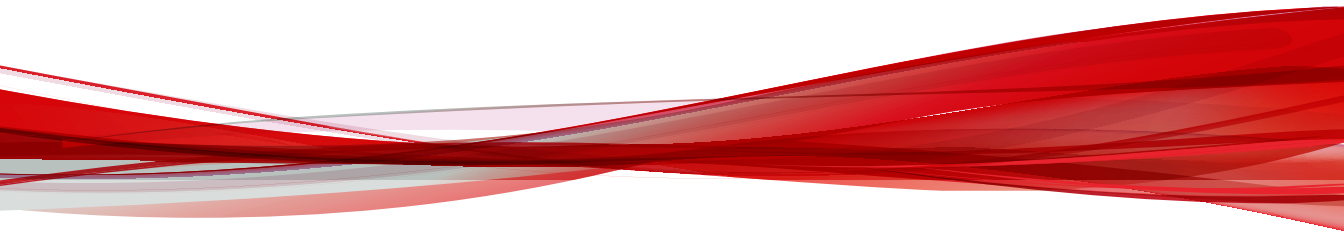
第 9 章：Remote Manager 中的 Worry-Free Business Security Services

部分 IV：整合第三方解決方案

第 10 章：AutoTask 支援

部分 I

Remote Manager 簡介



第 1 章

簡介

本節包含下列主題：

Trend Micro™Remote Manager™

Trend Micro™Remote Manager™ 是一個功能健全的主控台，與 Trend Micro Licensing Management Platform™ 配合工作，來為中小型企業提供受管理安全服務。

Trend Micro Remote Manager 可讓您透過多個受管理產品與服務，監控多個受管理網路的健康狀況。Trend Micro Remote Manager 可讓經銷商管理員發出命令，以管理網路安全的關鍵方面。

Trend Micro Remote Manager 裝載於區域性趨勢科技資料中心伺服器上，經銷商可從這些伺服器取得帳號。經銷商可使用 Trend Micro Remote Manager 建立客戶帳號、監控客戶網路，以及使用 Trend Micro Remote Manager Web 主控台管理安全性。

Remote Manager 提供客戶網路的結構化檢視，並可讓經銷商發出命令並管理網路安全的以下方面：

- 元件更新以及受管理伺服器更新
- 弱點評估
- 損害清除及復原
- 自動疫情爆發回應
- 防火牆和即時掃瞄設定
- 手動掃瞄

Trend Micro Remote Manager 還支援全面的報告功能，可讓經銷商為個人訂閱自動產生的報告。

新增功能

發行日期：2018 年 4 月

下表概述了 Trend Micro™Remote Manager™ 包含的新功能和增強功能。

功能	說明
Worry-Free Business Security 10.0 相容性	新增對 Worry-Free Business Security 10.0 新功能的支援，包括 Machine Learning 偵測、記錄查詢等。 如需詳細資訊，請參閱 Remote Manager 中的 Worry-Free Business Security 第 8-1 頁。
API 金鑰產生	自動 API 金鑰產生功能可讓您將 Trend Micro Remote Manager 與協力廠商程式整合。 如需詳細資訊，請參閱產生 API 金鑰 第 17-17 頁。
Worry-Free Business Security Services 加強掃瞄支援	Worry-Free Business Security Services 整合可提供更深入的掃瞄選項和惡意程式防護移除功能，以增強在裝置層級的安全威脅防護。 如需詳細資訊，請參閱管理 Worry-Free Business Security Services 第 9-5 頁。

發行日期：2018 年 1 月

下表概述了 2018 年 1 月版 Trend Micro™Remote Manager™ 的新功能和增強功能。

功能	說明
ConnectWise Manage 整合增強功能	升級的整合支援 RESTful API 和嵌入式 Remote Manager 主控台。 如需詳細資訊，請參閱 ConnectWise Manage 支援 第 11-1 頁。
Worry-Free Services Plug-in for ConnectWise Automate 增強功能	升級的嵌入程式支援 Security Agent 自動部署、程式檔執行重試，以及針對不成功的命令送出票證。 如需詳細資訊，請參閱 ConnectWise Automate 支援 第 12-1 頁。
Worry-Free Services Plug-in for Kaseya 增強功能	升級的嵌入程式支援範本指派、命令執行狀態、Security Agent 自動部署、程式檔執行重試，以及針對不成功的命令送出票證。 如需詳細資訊，請參閱 Kaseya 支援 第 13-1 頁。

功能	說明
Remote Manager 主控台組態設定選項	• 可設定 Remote Manager 主控台的作業階段逾時 • 「通知中心」的新事件類型過濾器 • 「客戶」畫面會儲存您的排序喜好設定，並在您下次查看該畫面時顯示

功能

Trend Micro Remote Manager 提供以下功能：

表 1-1. Remote Manager 功能

功能	說明
整合的平台	Remote Manager 與 Trend Micro™ Licensing Management Platform 並行運作，但具有更健全的介面。您可以從 Remote Manager 入口網站執行以下作業： • 建立新帳號 • 為個人帳號續約使用授權 • 新增更多授權 Remote Manager 還會與在受管理的伺服器上執行的 Remote Manager Agent 通訊，從單一主控台監控和管理多個受保護的網路。此外，Remote Manager 還根據主要安全指標提供事件監控。
資訊中心 Widget	在資訊中心頁面上自訂 Widget 這些 Widget 可告知您是否需要續約使用授權、新增更多配置的授權，甚或告知您哪些客戶遇到的安全威脅最多。
新帳號的可自訂設定	建立帳號時，您可以自訂新帳號依預設將使用的基本預設設定，或從您已設定並儲存的範本中選取設定。
安全狀態	Remote Manager「事件」畫面會針對您所有客戶的整合產品，提供安全威脅偵測和策略違規計數。

功能	說明
	Remote Manager 提供詳細資訊，例如中毒電腦和病毒/惡意程式事件的數目。經銷商管理員還可以查看詳細資訊，包括中毒電腦或安全威脅的名稱。
系統狀態	經銷商管理員可以在 Remote Manager「事件」畫面上查看系統相關事件資訊，例如元件更新狀態、裝置資源使用率及上線狀態。
使用授權狀態	經銷商管理員可以檢視以下使用授權相關詳細資訊： • 購買的授權總數 • 使用中的授權數目 • 已到期的使用授權，包括到期日期 • 即將到期的使用授權，包括到期剩餘天數
網路管理	Remote Manager 提供受管理網路的結構化檢視，並可讓經銷商管理員發出命令並管理網路安全的以下關鍵方面： • 元件更新以及受管理伺服器更新 • 弱點評估 • 自動疫情爆發回應 • 損害清除及復原 • 防火牆和即時掃瞄設定 • 手動掃瞄
報告	除了安全事件的通知之外，Remote Manager 還可以定期自動產生並傳送報告。您可以根據客戶、產品、頻率和內容產生報告，並採用多種格式儲存。
與第三方工具整合	使用第三方工具（包括 Autotask™、Kaseya™ 或 ConnectWise™）啟用記錄監控，以標準化您監控的工作和處理程序。
意見反應提交	趨勢科技希望為使用者提供最好且最有用的平台。但是，趨勢科技不知道哪些服務或功能對您重要。為此，Remote Manager 歡迎您透過「提交意見反應」按鈕，提供您的意見反應和建議；此按鈕顯示在橫幅上。然後，趨勢科技可以處理並確定哪些功能對大多數使用者有幫助。

瀏覽器需求

- 連線至 Internet
- 趨勢科技的 Remote Manager 帳號資訊
- 支援的瀏覽器：
  - 最新版 Google™Chrome™（建議）
  - 最新版 Firefox™
  - Microsoft Edge
  - Internet Explorer™ 11

支援的產品

下表列出 Trend Micro Remote Manager 可以監控的趨勢科技產品和產品版本。

產品	支援的版本
Trend Micro Cloud App Security	最新版本 如需詳細資訊，請參閱 Remote Manager 中的 Cloud App Security 第 4-1 頁。
Trend Micro Cloud Edge	最新版本 如需詳細資訊，請參閱 Remote Manager 中的 Cloud Edge 第 5-1 頁。
Trend Micro Hosted Email Security™	最新版本 如需詳細資訊，請參閱 Remote Manager 中的 Hosted Email Security 第 6-1 頁。
Trend Micro InterScan Web Security as a Service™	最新版本 如需詳細資訊，請參閱 Remote Manager 中的 InterScan Web Security as a Service 第 7-1 頁。

產品	支援的版本
Worry-Free Business Security™ Standard（之前稱為 Client Server Suite）。	6.x、7.x、8.x、9.x、10.x 如需詳細資訊，請參閱 Remote Manager 中的 Worry-Free Business Security 第 8-1 頁。
Worry-Free Business Security Advanced（之前稱為 Client Server Messaging Suite）。	6.x、7.x、8.x、9.x、10.x 如需詳細資訊，請參閱 Remote Manager 中的 Worry-Free Business Security 第 8-1 頁。
Worry-Free Business Security Services	最新版本 如需詳細資訊，請參閱 Remote Manager 中的 Worry-Free Business Security Services 第 9-1 頁。

Trend Micro Remote Manager 還可與以下第三方工具整合，以提供管理趨勢科技產品的替代方法：

第三方工具	參考資料
Autotask™	AutoTask 支援 第 10-1 頁
ConnectWise Automate™	ConnectWise Automate 支援 第 12-1 頁
ConnectWise Manage™	ConnectWise Manage 支援 第 11-1 頁
Kaseya™	Kaseya 支援 第 13-1 頁

整體基礎架構

Trend Micro Remote Manager 包含三個基本部分：

- 合作夥伴
- 趨勢科技資料中心

- 客戶網路

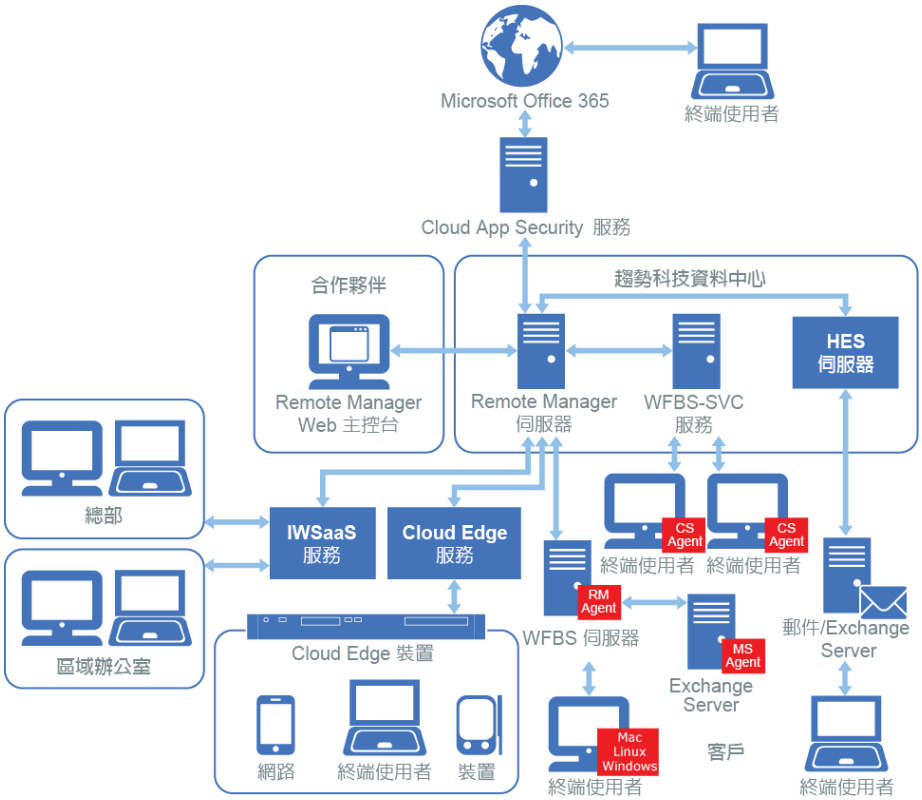


圖 1-1. Remote Manager 總體架構

合作夥伴藉由 Internet，透過 Remote Manager Web 主控台存取 趨勢科技 資料中心（目前位於不同的大陸）。合作夥伴不需要安裝任何元件就可以使用此產品。合作夥伴必須先在 Remote Manager Web 主控台新增並設定每個客戶，然後才能管理客戶帳號。

每部 Worry-Free Business Security Standard 和 Advanced 受管理的伺服器都已安裝 Remote Manager Agent，這實現與 Remote Manager 伺服器的通訊。Remote Manager Agent（可以從 Remote Manager Web 主控台安裝），在客戶網路內的

Worry-Free Business Security Standard 和 Advanced 受管理伺服器上執行。Remote Manager Agent 將資訊傳送至 Remote Manager 伺服器，您可以使用 Internet 連線，透過主控台全天候從此伺服器存取資料。

Worry-Free Business Security Services (WFBS-SVC) 和 Hosted Email Security (HES) 都託管在 趨勢科技 資料中心。InterScan Web Security as a Service (IWSaaS)、Cloud App Security (CAS) 和 Cloud Edge (CE) 都託管在雲端。WFBS-SVC、HES、IWSaaS、CAS 和 CE 全部會將資料直接傳送至 Remote Manager 伺服器。

主要術語

瞭解以下術語可以協助您更高效地使用 Remote Manager：

條款	定義
Agent	此程式安裝在 Worry-Free Business Security Standard 和 Advanced 伺服器上，可讓 Remote Manager 監控和管理 Worry-Free Business Security Standard 和 Advanced。
評估	對從客戶網路收集的資料執行的定期檢查，以確定受監控網路的健康情況。這些檢查使用稱為「評估指標」的主要指標。
評估指標	安全評估的基礎；經銷商管理員可以單獨自訂這些指標，來控制評估間隔、範圍和通知。
用戶端安全等級 Agent (CSA)	報告至 Worry-Free Business Security 伺服器的 Agent。CSA 會即時傳送事件狀態資訊。Agent 會報告事件，例如安全威脅偵測、Agent 啟用、Agent 關機、掃瞄開始以及更新完成。CSA 提供三種掃瞄方法：即時掃瞄、預約掃瞄、手動掃瞄。您可以從 Web 主控台設定 Agent 上的掃瞄設定。
資訊中心	Remote Manager 中的資訊中心是顯示 Web 主控台和 Widget 的主要畫面（「首頁」標籤）。
偵測	發現安全威脅；偵測並不表示系統感染，而僅指示惡意程式已進入電腦。在不同電腦上偵測到同一安全威脅則表示疫情爆發。
事件	在受監控的網域發生的狀況。

條款	定義
全域唯一識別碼 (GUID) 或啟用碼	在電腦軟體中做為識別碼的唯一參考號碼。
感染	安全威脅能夠在電腦中執行其裝載的狀況；當防毒掃瞄程式偵測到病毒/惡意程式，並且無法清除、刪除或隔離安全威脅時，Remote Manager 便認為已發生感染。如果只有重新啟用電腦才能完全清除間諜程式/可能的資安威脅程式，則表示已感染間諜程式/可能的資安威脅程式。
受管理的產品/服務	Remote Manager 支援的任何趨勢科技產品或服務
Messaging Security Agent (MSA)	位於 Microsoft Exchange Server 上，並報告至 Client Server Messaging 和 Worry-Free Business Security Advanced 伺服器的 Agent。此 Agent 會防禦病毒/惡意程式、特洛伊木馬程式、蠕蟲和其他電子郵件產生的安全威脅。還提供垃圾郵件封鎖、內容過濾和附件封鎖。
經銷商	一般術語，表示在 Remote Manager 中直接向客戶提供安全監控和管理服務的組織。
經銷商管理員	經銷商方使用 Remote Manager.執行服務相關工作的管理員。
趨勢科技資料中心	趨勢科技監控和管理中心，用於主控 Remote Manager（和 Hosted Email Security）伺服器並向經銷商管理員提供支援。
安全伺服器	Worry-Free Business Security Standard 和 Advanced 伺服器電腦。
病毒警訊	TrendLabs℠ 宣告的警惕狀態，讓客戶做好網路防範準備工作，防止病毒爆發；TrendLabs 警訊與趨勢科技產品不同，它提供預防性解決方案，讓 IT 管理員可以在病毒碼可用之前守護好第一道防線。
病毒爆發	病毒安全威脅快速散播到其他電腦和網路；根據安全威脅的普遍性，病毒爆發的範圍可以是內部、區域或全域。

部分 II

管理客戶

第 2 章

Remote Manager 客戶

本節包含下列主題：

客戶總覽

「客戶」畫面提供您公司管理的所有先前設定的客戶清單。您可以使用此畫面檢視客戶的基本聯絡資訊，並識別客戶是否需要立即關注值得注意的安全威脅、系統或授權事件。

秘訣

您可以使用清單右側的搜尋窗格過濾「客戶」清單。

如需詳細資訊，請參閱過濾客戶清單 第 2-5 頁。

下表概述了「客戶」畫面上的可用工作。

工作	說明	適用對象
新增客戶	按一下「新增客戶」可設定公司簡介和使用者帳號、指派服務計畫，以及設定預設產品設定。 如需詳細資訊，請參閱新增客戶 第 2-5 頁。	• Customer Licensing Portal 帳號 • Licensing Management Platform 帳號
刪除現有的客戶	選取現有的客戶並按一下「刪除」，可從「客戶」清單中移除客戶帳號。 注意 必須先從選取的客戶中移除所有產品，才能刪除客戶。 警告! 客戶帳號被刪除後，就無法復原。	• Customer Licensing Portal 帳號

工作	說明	適用對象
將預設產品範本指派給現有客戶	選取現有客戶並按一下「指派範本」，可從預先設定的產品設定中進行選擇。 注意 Remote Manager 僅支援 Worry-Free Business Security Services 和 Cloud Edge 的預設產品範本。 如需詳細資訊，請參閱將預設設定範本指派給現有客戶 第 2-9 頁。	• Licensing Management Platform 帳號
將策略設定部署至多個客戶	選取現有客戶並按一下「策略設定」，可從可用 Worry-Free Business Security Services 策略（您可以套用至所有選取的客戶）中進行選取。 如需詳細資訊，請參閱多個客戶的大量策略更新 第 2-10 頁。	• Licensing Management Platform 帳號
更新 Cloud Edge 裝置韌體	選取現有 Cloud Edge 客戶，然後按一下「更新韌體」。Remote Manager 會通知選取的所有需要更新韌體的 Cloud Edge 客戶，以取得更新套件。	• Licensing Management Platform 帳號
續約產品使用授權	選取現有 Cloud Edge 客戶，然後按一下「續約使用授權」。Remote Manager 可讓您續約使用授權已到期的任何客戶。 如需詳細資訊，請參閱續約使用授權 第 3-14 頁。	• Licensing Management Platform 帳號
匯出客戶資訊	• 選取客戶並按一下「匯出」，可將選取的客戶資訊儲存為 CSV 檔案 • 按一下「全部匯出」，可將所有顯示的客戶資訊儲存為 CSV 檔案	• Customer Licensing Portal 帳號 • Licensing Management Platform 帳號
變更 Remote Manager「客戶」檢視設定	按一下「設定」可將 Remote Manager 變更為向所有擁有 Licensing Management Platform 帳號的客戶顯示，還是僅向產品受 Remote Manager 管理的客戶顯示。	• Licensing Management Platform 帳號

客戶資料

「客戶」畫面向您提供客戶的基本資訊，並顯示影響您客戶的重要事件彙總計數。

重要

若要修改個別客戶資訊，您必須使用 Licensing Management Platform 帳號登入，然後按一下畫面右上角的「Licensing Management Platform」連結。您無法直接從 Remote Manager 主控台修改客戶資訊。

表 2-1. 客戶資料

項目	說明
公司	在 Licensing Management Platform 中設定的公司名稱 按一下「公司」名稱可管理個別客戶和授權設定。 如需詳細資訊，請參閱個別客戶設定 第 3-1 頁。
聯絡人	在 Licensing Management Platform 中設定的公司聯絡人姓名
電話	在 Licensing Management Platform 中設定的公司聯絡人電話號碼
產品	公司授權的所有產品的逗號分隔清單
安全威脅和系統事件	目前影響客戶的所有「需要採取處理行動」（紅色）和「警告」（黃色）安全威脅或系統事件的彙總計數 按一下計數可開啟「<客戶>」畫面，並可檢視有關事件類型的特定詳細資訊。 如需詳細資訊，請參閱受管理的產品事件 第 15-3 頁。
使用授權事件	目前影響客戶的所有「需要採取處理行動」（紅色）和「警告」（黃色）授權事件的彙總計數 按一下計數可開啟「<客戶>」畫面，並可檢視有關事件類型的特定詳細資訊。 如需詳細資訊，請參閱續約使用授權 第 3-14 頁。

項目	說明
上次交易	客戶上次發生事件變更（例如，使用授權交易或系統安全威脅）的日期和時間。

過濾客戶清單

使用畫面右側的搜尋窗格過濾客戶清單。

程序

1. 移至「客戶」。
2. 在右側，從搜尋窗格中選取一或多個選項。

   注意

   下拉式功能表中的「安全威脅類別」、「系統事件」和「使用授權事件」選項，不會根據您的「產品」選擇動態更新。如果不存在您選取的產品對應的事件選項，可能會顯示其他產品的結果。

   例如，選取「產品 > Hosted Email Security (HES)」和「系統事件 > 雲端電子郵件掃瞄」，會傳回任何產品的所有 Hosted Email Security (HES) 事件和所有「雲端電子郵件掃瞄」事件。

3. （選用）按一下「匯出」，以產生您過濾出的客戶的 CSV 檔案。

新增客戶

建立客戶帳號之前，您應該識別基本客戶資訊。需要注意的欄位包括：「名字」和「姓氏」（將顯示在報告和通知中）、「時區」（客戶所屬時區）和「語言」（客戶收到的報告和通知將使用的語言）。在您新增客戶並在受管理伺服器上安裝 Agent 之前，請確保您已獲得書面核可，可以執行工作以存取、監控和管理客戶的資源。

程序

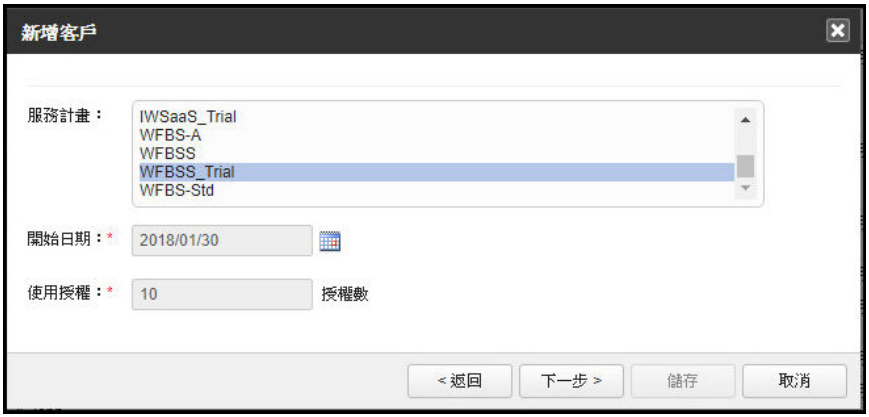
1. 從 Remote Manager Web 主控台橫幅中，按一下「新增客戶」。

> **注意**
> 您可以從標題區域或「客戶」標籤，按一下「新增客戶」。

2. 提供客戶資訊。

圖 2-1. 客戶資訊畫面

3. 按「下一步 >」。
4. 指派服務計畫、使用授權開始日期和每個使用授權的單位數量。



5. 設定此帳號的產品預設設定。這些設定包括：

注意

此功能僅適用於 Worry-Free Business Security Services 和 Cloud Edge。

- 「基本」：僅在此畫面上設定新客戶帳號將使用的設定。

圖 2-2. 基本產品設定

- 「範本」：使用此選項選取預設設定範本。從「管理 > 設定預設設定範本」，設定相關設定。

6. 確認所有資訊，然後按一下「儲存」。

注意

新增客戶後，僅可從 Trend Micro Licensing Management Platform 變更描述檔。

將預設設定範本指派給現有客戶

僅當 Trend Micro Remote Manager 與 Licensing Management Platform 整合後，才會提供預設設定範本。

您可以指派已啟用「行為監控」的預設範本，將預設設定範本指派給現有客戶，以啟用勒索軟體防護。

如需關於可設定之設定的詳細資訊，請參閱產品文件。

http://docs.trendmicro.com/zh-tw/smb/worry-free-business-security-services.aspx

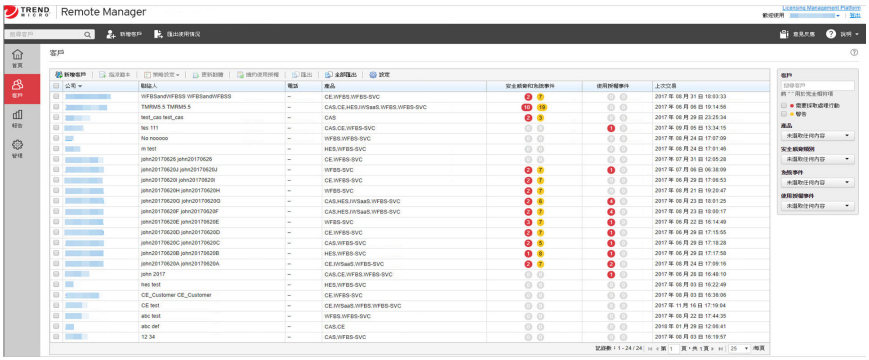
注意

僅可將範本指派給使用 Worry-Free Business Security Services 的公司。

程序

1. 移至「客戶」。

   隨即顯示「客戶」畫面。



2. 從「公司」清單中選取一個或多個客戶。
3. 按一下「指派範本」標籤。

   隨即顯示「指派範本」畫面。

4. 從清單中選取範本。
5. 按「下一步 >」。

   隨即顯示確認畫面，並僅列出擁有支援產品的公司。

6. 按一下「指派」。

   範本將成功指派給選取的客戶。

多個客戶的大量策略更新

透過 Remote Manager，您能夠設定單一 Worry-Free Business Security Services 策略，並能夠在一個批次部署中將設定部署給多個客戶。根據策略類型，您可以將策略部署至每個客戶的特定裝置群組，或更新客戶的全域設定供日後使用。將策略部署給多個客戶和客戶裝置群組，可減少為每個客戶單獨手動設定清單的負荷。

Remote Manager 提供以下大量策略部署選項：

設定核可/封鎖的 URL 清單

您可以為您的 Worry-Free Business Security Services 客戶設定核可/封鎖的 URL 清單，並將該清單部署到多個客戶或裝置群組，或在全域設定層級進行部署。

注意

將核可/封鎖的 URL 清單策略設定部署到特定裝置群組，會自動在 Security Agent 上啟用自訂核可/封鎖的 URL 清單。

如需詳細資訊，請參閱《*Worry-Free Business Security Services 線上說明*》。

注意

- 核可的 URL 清單的策略設定適用於網頁信譽評等服務和 URL 過濾功能。
- 封鎖的 URL 清單的策略設定僅適用於 URL 過濾功能。

程序

1. 移至「客戶」。
2. 從「公司」清單中選取一個或多個客戶。
3. 按一下「策略設定」並選取「核可/封鎖的 URL 清單」。

   隨即顯示「核可/封鎖的 URL 清單」畫面。

4. 為策略設定選取「目標」。

   - 「客戶 (全域設定)」：僅將變更套用至清單中所選客戶的全域設定

     重要

     對全域設定所做的任何變更都不會套用至任何預先存在的裝置群組。您必須選取「裝置群組」，才能將變更立即套用至現有的裝置群組。

   - 「裝置群組」：將變更套用至清單中的所選裝置群組

     注意

     若要選取特定類型的裝置群組，請使用「選取群組」下拉按鈕，從策略設定中選取或移除裝置群組。依預設，Remote Manager 會選取所有客戶的所有裝置群組。

5. 按一下「設定策略 >」。

6. 設定例外清單和封鎖清單的策略設定。

   a. 使用下拉方塊指定變更會如何影響每個清單。

      - 「選取處理行動」：這是預設設定，不會將任何變更套用至目前的策略設定
      - 「附加」：Remote Manager 會將指定的項目新增至現有清單
      - 「刪除」：Remote Manager 會從現有清單中移除指定的項目

        注意

        如果 Remote Manager 在現有清單中找不到指定的項目，則 Remote Manager 不會對清單執行任何動作。

      - 「覆寫」：Remote Manager 會刪除現有清單中的所有項目，並使用指定的項目取代此清單

        警告!

        您無法復原此動作。如果您選擇取代整個清單，則無法還原之前的清單項目。

b. 輸入要套用至策略的 URL。

注意

如果新增至核可/封鎖的 URL 清單的項目較多，造成清單超出允許的最大值，則清單部署會失敗。

使用空格字元、逗號 (,)、分號 (;) 或 ENTER 鍵，可指定多個項目。

URL 可使用星號 (*) 做為萬用字元（星號可匹配零或多個字元）。

7. 按一下「部署策略設定」。

Remote Manager 會將變更部署到指定的客戶或裝置群組。您可以從「管理記錄檔」監控策略部署的狀態。

如需詳細資訊，請參閱檢視管理記錄檔 第 17-21 頁。

設定即時掃瞄的防毒例外清單

您可以為您的 Worry-Free Business Security Services 客戶設定防毒例外清單，並將該清單部署到多個客戶或裝置群組。

注意

啟用防毒例外清單會在受影響的 Security Agent 上自動啟用即時防毒和間諜程式防護掃瞄。

程序

1. 移至「客戶」。
2. 從「公司」清單中選取一個或多個客戶。
3. 按一下「策略設定」並選取「防毒例外清單」。

隨即顯示「防毒例外清單」畫面。

4. 選取您要設定的客戶或特定裝置群組。

   注意

   若要選取特定類型的裝置群組，請使用「選取群組」下拉按鈕，從策略設定中選取或移除裝置群組。依預設，Remote Manager 會選取所有客戶的所有裝置群組。

5. 按一下「設定策略 >」。

6. 使用下拉方塊指定變更會如何影響每個清單。

   - 「選取處理行動」：這是預設設定，不會將任何變更套用至目前的策略設定
   - 「啟用防毒例外清單」：Remote Manager 會在所選裝置群組上啟用防毒例外清單。

     隨即顯示「Windows 例外清單」和「Mac 例外清單」區段。
   - 「關閉防毒例外清單」：Remote Manager 會在所選裝置群組上關閉防毒例外清單。

7. 在「Windows 例外清單」和「Mac 例外清單」區段中：

   a. 使用下拉方塊指定變更會如何影響每個清單。

      - 「選取處理行動」：這是預設設定，不會將任何變更套用至目前的策略設定
      - 「附加」：Remote Manager 會將指定的項目新增至現有清單
      - 「刪除」：Remote Manager 會從現有清單中移除指定的項目

        注意

        如果 Remote Manager 在現有清單中找不到指定的項目，則 Remote Manager 不會對清單執行任何動作。

      - 「覆寫」：Remote Manager 會刪除現有清單中的所有項目，並使用指定的項目取代此清單

警告!

您無法復原此動作。如果您選擇取代整個清單，則無法還原之前的清單項目。

b. 在以下欄位中輸入必要例外：

- 「目錄路徑」：排除指定的目錄和所有子目錄

重要

Mac 裝置不支援目錄路徑清單。

注意

目錄路徑項目使用星號 (*) 做為萬用字元。

- 「檔案名稱或具有完整路徑的檔案名稱」：根據檔案名稱或具有完整路徑的檔案名稱，排除指定的檔案

注意

檔案名稱和具有完整路徑的檔案名稱項目可使用星號 (*) 做為萬用字元。

- 「副檔名」：排除所有具有指定副檔名的檔案

注意

請在欄位中輸入不含句點的副檔名。例如，輸入 txt 而不是 .txt。

使用分號 (;) 或 ENTER 鍵，可指定多個項目。

8. 按一下「部署策略設定」。

Remote Manager 會將變更部署到指定的客戶或裝置群組。您可以從「管理記錄檔」監控策略部署的狀態。

如需詳細資訊，請參閱檢視管理記錄檔 第 17-21 頁。

設定行為監控例外清單

您可以為您的 Worry-Free Business Security Services 客戶設定行為監控例外清單，並將該清單部署到多個客戶或裝置群組。

重要

部署行為監控例外清單設定時，請注意以下事項：

- 針對「裝置（預設）」群組，Security Agent 會自動啟用「行為監控」。
- 針對「伺服器（預設）」群組，Security Agent 會自動啟用「行為監控」和「未經授權的變更阻止服務」。
- 針對手動群組：
  - 桌面平台上安裝的 Security Agent 會自動啟用「行為監控」。
  - 伺服器平台上安裝的 Security Agent 會自動啟用「行為監控」，但您必須使用 Worry-Free Business Security Services 主控台手動啟用「未經授權的變更阻止服務」。

如需詳細資訊，請參閱《*Worry-Free Business Security Services 線上說明*》。

程序

1. 移至「客戶」。
2. 從「公司」清單中選取一個或多個客戶。
3. 按一下「策略設定」並選取「行為監控例外清單」。

   隨即顯示「行為監控例外清單」畫面。
4. 選取您要設定的客戶或特定裝置群組。

注意

若要選取特定類型的裝置群組，請使用「選取群組」下拉按鈕，從策略設定中選取或移除裝置群組。依預設，Remote Manager 會選取所有客戶的所有裝置群組。

5. 按一下「設定策略 >」。
6. 設定「核可的程式清單」和/或「封鎖的程式清單」的策略設定。
   a. 使用下拉方塊指定變更會如何影響每個清單。
      - 「選取處理行動」：這是預設設定，不會將任何變更套用至目前的策略設定
      - 「附加」：Remote Manager 會將指定的項目新增至現有清單
      - 「刪除」：Remote Manager 會從現有清單中移除指定的項目

      注意

      如果 Remote Manager 在現有清單中找不到指定的項目，則 Remote Manager 不會對清單執行任何動作。

      - 「覆寫」：Remote Manager 會刪除現有清單中的所有項目，並使用指定的項目取代此清單

      警告!

      您無法復原此動作。如果您選擇取代整個清單，則無法還原之前的清單項目。

   b. 輸入要套用至策略的完整程式路徑。

      使用分號 (;) 或 ENTER 鍵，可指定多個項目。
7. 按一下「部署策略設定」。

   Remote Manager 會將變更部署到指定的客戶或裝置群組。您可以從「管理記錄檔」監控策略部署的狀態。

   如需詳細資訊，請參閱檢視管理記錄檔 第 17-21 頁。

設定 Machine Learning 例外清單

您可以為您的 Worry-Free Business Security Services 客戶設定 Machine Learning 例外清單，並在全域設定層級將該清單部署到多個客戶。

重要

對全域設定所做的任何變更都不會套用至任何預先存在的裝置群組。

程序

1. 移至「客戶」。
2. 從「公司」清單中選取一個或多個客戶。
3. 按一下「策略設定」並選取「Machine Learning 例外清單」。

   隨即顯示「Machine Learning 例外清單」畫面。
4. 選取您要設定的客戶。
5. 按一下「設定策略 >」。
6. 設定 Machine Learning 例外清單的策略設定。
   a. 使用下拉方塊指定變更會如何影響清單。
      - 「選取處理行動」：這是預設設定，不會將任何變更套用至目前的策略設定
      - 「附加」：Remote Manager 會將指定的項目新增至現有清單
      - 「刪除」：Remote Manager 會從現有清單中移除指定的項目

        注意

        如果 Remote Manager 在現有清單中找不到指定的項目，則 Remote Manager 不會對清單執行任何動作。
      - 「覆寫」：Remote Manager 會刪除現有清單中的所有項目，並使用指定的項目取代此清單

警告!

您無法復原此動作。如果您選擇取代整個清單，則無法還原之前的清單項目。

b. 輸入要套用至策略的 SHA-1 檔案雜湊。

使用分號 (;) 或 ENTER 鍵，可指定多個項目。

7. 按一下「部署策略設定」。

Remote Manager 會將變更部署到指定的客戶。您可以從「管理記錄檔」監控策略部署的狀態。

如需詳細資訊，請參閱檢視管理記錄檔 第 17-21 頁。

設定 Machine Learning 設定

您可以為您的 Worry-Free Business Security Services 客戶設定「Machine Learning 設定」清單，並將該清單部署到多個客戶或裝置群組。

注意

Machine Learning 需要 Internet 連線正常運作，才能連線至主動式雲端截毒技術。

程序

1. 移至「客戶」。
2. 從「公司」清單中選取一個或多個客戶。
3. 按一下「策略設定」並選取「Machine Learning 設定」。

隨即顯示「Machine Learning 設定」畫面。

4. 選取您要設定的客戶或特定裝置群組。

注意

若要選取特定類型的裝置群組，請使用「選取群組」下拉按鈕，從策略設定中選取或移除裝置群組。依預設，Remote Manager 會選取所有客戶的所有裝置群組。

5. 按一下「設定策略 >」。

6. 選取要套用至策略的「處理行動」。

   - 「選取處理行動」：這是預設設定，不會將任何變更套用至目前的策略設定
   - 「啟用 Machine Learning」：在所選裝置群組上啟用 Machine Learning

     隨即顯示「偵測設定」區段。
   - 「關閉 Machine Learning」：在所選裝置群組上關閉 Machine Learning

7. 在「偵測設定」下，選取偵測的類型以及「Machine Learning」採取的相關處理行動。

偵測類型	處理行動
檔案	• 隔離： 選取此項，即會自動依「Machine Learning」分析結果，將展現惡意程式相關特徵的檔案隔離 • 僅記錄檔： 選取此項，即會掃瞄未知檔案並記錄「Machine Learning」分析結果，以供內部進一步調查安全威脅
處理程序	• 終止：選取此項，即會自動依「Machine Learning」分析結果，將展現惡意程式相關行為的程序或程式檔終止 重要 Machine Learning 會嘗試將已執行惡意處理程序的檔案清除。如果清除處理行動不成功，則受管理產品會隔離受影響的檔案。 • 僅記錄檔：選取此項，即會掃瞄未知程序或程式檔並記錄「Machine Learning」分析結果，以供內部進一步調查安全威脅

8. 按一下「部署策略設定」。

   Remote Manager 會將變更部署到指定的客戶或裝置群組。您可以從「管理記錄檔」監控策略部署的狀態。

   如需詳細資訊，請參閱檢視管理記錄檔 第 17-21 頁。

設定勒索軟體設定

您可以為您的 Worry-Free Business Security Services 客戶設定勒索軟體設定，並將這些設定部署到多個客戶或裝置群組。

重要

部署勒索軟體設定時，請注意以下事項：

- 針對「裝置（預設）」群組，Security Agent 會自動啟用「行為監控」。
- 針對「伺服器（預設）」群組，Security Agent 會自動啟用「行為監控」和「未經授權的變更阻止服務」。
- 針對手動群組：
  - 桌面平台上安裝的 Security Agent 會自動啟用「行為監控」。
  - 伺服器平台上安裝的 Security Agent 會自動啟用「行為監控」，但您必須使用 Worry-Free Business Security Services 主控台手動啟用「未經授權的變更阻止服務」。

如需詳細資訊，請參閱《*Worry-Free Business Security Services 線上說明*》。

程序

1. 移至「客戶」。
2. 從「公司」清單中選取一個或多個客戶。
3. 按一下「策略設定」並選取「勒索軟體設定」。

   隨即顯示「勒索軟體設定」畫面。

4. 選取您要設定的客戶或特定裝置群組。

   注意

   若要選取特定類型的裝置群組，請使用「選取群組」下拉按鈕，從策略設定中選取或移除裝置群組。依預設，Remote Manager 會選取所有客戶的所有裝置群組。

5. 按一下「設定策略 >」。

6. 選取要套用至策略的「處理行動」。

   - 「選取處理行動」：這是預設設定，不會將任何變更套用至目前的策略設定
   - 「啟用勒索軟體防護」：在所選裝置群組上啟用勒索軟體防護

     隨即顯示「設定」區段。

   - 「關閉勒索軟體防護」：在所選裝置群組上關閉勒索軟體防護

7. 啟用勒索軟體防護時，請選取您要套用的勒索軟體防護功能。

   - 「啟用文件防護，以防止未經授權的加密或修改」：阻止潛在的勒索軟體安全威脅加密或修改文件內容
     - 「自動備份與還原可疑程式修改的檔案」：如果受管理產品偵測到勒索軟體安全威脅，則會為端點上要加密的檔案建立備份副本，以防任何資料遺失

       注意

       自動檔案備份需要用戶端端點上至少有 100 MB 的磁碟空間，而且僅會備份大小小於 10 MB 的檔案。

   - 「針對通常與勒索軟體相關聯的處理程序啟用封鎖」：在加密和修改文件之前，封鎖與已知勒索軟體安全威脅相關的處理程序
   - 啟動程式檢測，以偵測並封鎖遭到入侵的可執行檔：程式檢測可監控處理程序並執行 API 攔截，以判斷程式是否表現出非預期的行為。雖然此程序可提高對遭到入侵的可執行檔的整體偵測率，卻可能會導致系統效能降低。

8. 按一下「部署策略設定」。

   Remote Manager 會將變更部署到指定的客戶或裝置群組。您可以從「管理記錄檔」監控策略部署的狀態。

   如需詳細資訊，請參閱檢視管理記錄檔 第 17-21 頁。

在 Licensing Management Platform 中合併多個 Remote Manager 帳號

如果您管理其他尚未移轉至新 Licensing Management Platform 的 Trend Micro Remote Manager 帳號，可以將這些帳號與目前帳號合併。

程序

1. 登入已移轉至 Licensing Management Platform 的 Remote Manager 帳號。

   隨即顯示「資訊中心」畫面。

2. 按一下登入名稱旁邊的箭頭，然後按一下「合併另一帳號 > 是」。

   警告!

   如果您將一個帳號合併至目前帳號，被合併帳號的所有資料都將移動。例如，如果您目前以 admin1 登入，並將 admin2 合併至 admin1 帳號，則 admin2 帳號中的所有資料都將從 admin2 帳號中刪除。此資料已與 admin1 帳號合併。您仍可以開啟 admin2 帳號，但所有資料都在 admin1 帳號中。

3. 輸入您要與目前帳號合併之帳號的使用者名稱和密碼。
4. 按一下「合併」。

   等待幾分鐘，讓資料合併。

接下來需執行的動作

合併帳號後，在新增客戶時您都會看到以下資訊：

- 「具有作用中的 Licensing Management Platform 帳號」：如果新客戶已擁有 Licensing Management Platform 帳號。
- 「透過需要連線至此帳號的現有產品伺服器」：如果新客戶擁有產品/服務，但帳號尚未合併至 Licensing Management Platform。

第 3 章

個別客戶設定

本節包含下列主題：

客戶資訊

「<客戶>」畫面包含多個標籤，可讓您檢視個別客戶的以下資訊：關聯產品、使用授權、公司資料、通知和 ConnectWise 設定。

表 3-1. 客戶標籤

標籤	說明
產品	提供客戶帳號的所有關聯產品的清單，並顯示可能需要立即注意的所有產品相關事件的清單 您可以使用「產品」標籤，設定個別產品設定。 **注意** 如果任何產品發生「需要採取處理行動」（紅色）和「警告」（黃色）事件，Remote Manager 會直接在該標籤上顯示摘要計數。 如需詳細資訊，請參閱客戶產品 第 3-3 頁。
使用授權	提供與客戶帳號關聯的所有產品和服務計畫的清單 **注意** 如果任何產品發生「已到期」（紅色）和「即將到期」（黃色）事件，Remote Manager 會直接在該標籤上顯示摘要計數。 如需詳細資訊，請參閱客戶使用授權 第 3-13 頁。
公司簡介	顯示在 Licensing Management Platform 中設定的公司一般資訊 如需詳細資訊，請參閱公司簡介 第 3-15 頁。
聯絡資訊	顯示在 Licensing Management Platform 中設定的客戶聯絡資訊 如需詳細資訊，請參閱聯絡資訊 第 3-16 頁。
通知	顯示客戶的所有通知組態設定 如需詳細資訊，請參閱客戶通知 第 3-17 頁。

標籤	說明
ConnectWise	顯示客戶的 ConnectWise 整合設定 如需詳細資訊，請參閱個別客戶的 ConnectWise 設定 第 3-18 頁。

客戶產品

客戶「產品」標籤顯示目前與客戶帳號關聯的所有產品，並列出所有相關事件通知。

秘訣

您可以使用表格上方的「檢視方式」下拉方塊，過濾「通知事件」清單。

下表概述了「產品」標籤上的可用工作。

工作	說明
新增產品	按一下「新增」按鈕，為客戶指派新產品和服務計畫。 如需詳細資訊，請參閱使用 Licensing Management Platform 帳號新增產品 第 3-8 頁或使用 Customer Licensing Portal 帳號新增產品 第 3-11 頁。

工作	說明
管理產品設定	在產品樹狀結構中選取產品，以顯示該產品特定的事件通知和組態設定。 如需詳細資訊，請參閱以下產品的特定產品設定資訊： • Cloud App Security 第 4-2 頁 • Cloud Edge 第 5-2 頁 • Hosted Email Security 第 6-2 頁 • InterScan Web Security as a Service 第 7-2 頁 • Worry-Free Business Security 第 8-2 頁 • Worry-Free Business Security Services 第 9-2 頁 如需關於產品樹狀結構中所顯示圖示的詳細資訊，請參閱網路樹狀結構狀態圖示 第 3-12 頁。
檢視安全威脅和系統事件通知	依預設，Remote Manager 會顯示與客戶帳號關聯之所有產品的所有事件通知。若要檢視特定產品的事件通知，請從產品樹狀結構中選取此產品。 如需詳細資訊，請參閱受管理的產品事件 第 15-3 頁。 若要檢視關於特定事件的詳細資訊，請按一下「出現次數」計數。

產品/服務資訊

資訊中心僅列出需要注意的客戶。若要取得任何產品（包括未在資訊中心中列出的產品）的詳細資訊，請移至「客戶」標籤並在客戶樹狀結構中存取產品。

按一下「客戶 > {客戶} > {產品}」，以顯示其他資訊。

注意

每個產品/服務顯示的選項各有不同。

產品	選項
Cloud App Security	• 「事件」：顯示系統和安全威脅事件 • 「使用者」：可讓您建立或刪除 Cloud App Security 使用者，以及重設使用者的密碼

Cloud Edge	• 對於服務計畫：
	  • 「事件」：顯示服務計畫中所有 Cloud Edge 裝置中的事件摘要
	  • 「韌體更新」：顯示每部裝置的目前韌體版本及最新可用版本，並提供手動更新韌體的選項
	  • 「裝置」：顯示每部已註冊裝置的名稱和產品序號
	• 對於已註冊裝置：
	  • 「事件」：顯示系統和安全威脅事件
	  • 「元件」：顯示每個元件的目前版本、最新可用版本以及上次更新日期
	  • 「網路」：顯示透過 Cloud Edge 裝置連線至網路之端點的使用者名稱、遠端 IP 位址和 MAC 位址
	  • 「VPN」：顯示透過虛擬私人網路和 Cloud Edge 裝置連線至網路之端點的使用者名稱、遠端 IP 位址和虛擬 IP 位址
	注意
	若要進行更詳細的變更，請存取 Cloud Edge 主控台。

產品	選項
Hosted Email Security	• 「即時狀態」：顯示最新的 Hosted Email Security 資訊。 • 「策略設定」：列出所有可用的策略。 • 「核可的寄件者」：列出不受 IP 信譽評等型垃圾郵件、網路釣魚或行銷郵件過濾制約的所有寄件者。 • 「封鎖的寄件者」：列出遭到封鎖而無法傳送郵件的所有位址或網域。 注意 若要進行更詳細的變更，請存取 Hosted Email Security 主控台。
InterScan Web Security as a Service	顯示最新的 InterScan Web Security as a Service 安全威脅和系統資訊。 注意 若要進行更詳細的變更，請存取 InterScan Web Security as a Service 主控台。

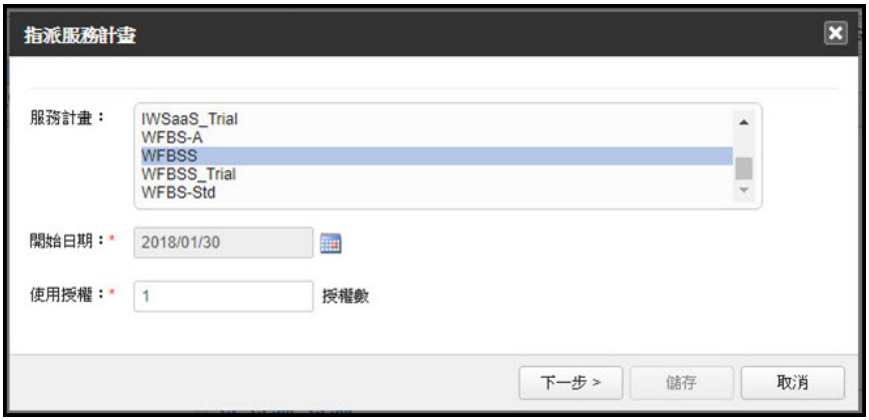
產品	選項
Worry-Free Business Security	• 「事件」：列出可能需要或不需要採取處理行動的系統和安全威脅事件。 • 「群組」：列出在伺服器上設定的不同群組。您可以從此處請求開始或停止掃瞄。 • 「網域設定」：設定整個網域的設定。 如需詳細資訊，請參閱 Trend Micro Worry-Free Business Security 文件： http://docs.trendmicro.com/zh-tw/smb/worry-free-business-security.aspx。 注意 無法從此處設定個別群組的安全設定。您將需要存取 Worry-Free Business Security，來進行這些變更。 • 「受管理的伺服器」：顯示伺服器的所有詳細資訊。您可以從此處請求更新伺服器和 Agent。 • 「TMRM Agent」：包含關於 Trend Micro Remote Manager Agent 的一般資訊，包括可用性、全域唯一識別碼 (GUID) 或啟用碼和 IP 位址。 • 「裝置」：列出掃瞄引擎、病毒碼檔案和平台的名稱、IP 位址、線上/離線狀態和詳細資訊。 注意 您可以在展開產品後查看「裝置」和「安全設定」，然後按一下「伺服器」或「桌面」。 • 「安全設定」：設定特定群組的安全設定（僅適用於 Worry-Free Business Security 6.0 及更新版本）。如需詳細資訊，請參閱 Trend Micro Worry-Free Business Security 文件。

產品	選項
Worry-Free Business Security Services	• 「事件」：列出可能需要或不需要採取處理行動的系統和安全威脅事件。 • 「群組」：列出已設定的群組和類型。 • 「裝置」：列出掃瞄引擎、病毒碼檔案和平台的名稱、IP 位址、線上/離線狀態和詳細資訊。 注意 您可以在展開產品後查看「裝置」和「安全設定」，然後按一下「伺服器」或「桌面」。 • 「安全設定」：設定 Worry-Free Business Security Services 的安全設定。如需詳細資訊，請參閱 Trend Micro Worry-Free Business Security Services 文件： http://docs.trendmicro.com/zh-tw/smb/worry-free-business-security-services.aspx 注意 若要進行更詳細的變更，請存取 Worry-Free Business Security Services 主控台。

使用 Licensing Management Platform 帳號新增產品

程序

1. 移至「客戶 > {客戶名稱} > 產品 > 新增」。



2. 指定服務計畫、開始日期和每個使用授權的單位數量。
3. 按「下一步>」或「儲存」。
4. 設定產品的預設設定。您可以選擇下列其中一項：

注意

僅在選取 Worry-Free Business Security Services 時，才會顯示此功能。

- 「基本」：僅設定顯示的設定。
  - 網頁信譽評等和 URL 過濾的例外清單

> **注意**
>
> 如果您將 URL 新增至例外清單，請確保它未新增至封鎖的清單，反之亦然。

- URL 過濾的封鎖的清單
- 伺服器和裝置的預約掃瞄

- 「範本」：移至「管理 > 設定預設設定範本」，以使用與 Worry-Free Business Security 類似的主控台設定更多設定。

5. 按一下「儲存」。

   會新增產品/服務，並顯示新增內容的詳細資訊。

注意

如果新增 Worry-Free Business Security 產品，請記下 Worry-Free Business Security 啟用碼，並在 Licensing Management Platform 主控台中完成安裝。

6. 按一下「連線」，以取得有關如何將產品/服務連線至主控台的資訊。

使用 Customer Licensing Portal 帳號新增產品

您僅可使用 CLP 帳號新增以下產品：

- Hosted Email Security
- Worry-Free Business Security
- Worry-Free Business Security Services

程序

1. 在 Remote Manager 主控台上，移至「客戶 > [客戶] > 產品 > 新增」。

   隨即顯示「新增產品」畫面。

2. 在「產品類型」下拉式清單中，選取您要註冊到客戶的產品。
3. 輸入「產品說明」。
4. 按一下「儲存」。

   隨即顯示一個確認畫面，其中包含詳細說明。

5. 複製授權碼或 GUID；必須使用該資訊才能將受管理產品註冊到 Remote Manager。
6. 在受管理產品主控台上，移至「管理 > Trend Micro Remote Manager」。
7. 在可用欄位中提供授權碼或 GUID。
8. 按一下「連線」。

   受管理產品會連線至 Remote Manager，並註冊到先前選取的客戶帳號。

   開啟 Remote Manager 主控台並檢視客戶產品清單，確認受管理產品已成功註冊。

網路樹狀結構狀態圖示

在「產品」標籤的左側，畫面顯示您的客戶產品的樹狀結構表示。

表 3-2. 網路樹狀結構物件

圖示	網路物件	說明
	產品/服務	此產品/服務未連線至 Remote Manager。
	產品/服務	此產品/服務已連線至 Remote Manager。
	裝置	此裝置處於離線狀態。
	裝置	此裝置處於線上狀態。
	群組	桌面群組
	群組	Worry-Free Business Security Services 裝置由不同的裝置類型組成。
	Exchange 伺服器	Exchange 伺服器電腦；此電腦執行 Messaging Security Agent (MSA)。
	群組	伺服器群組；此群組管理多個用戶端安全等級 Agent (CSA)。

客戶使用授權

客戶「使用授權」標籤顯示目前授權給客戶帳號的所有產品，以及每個使用授權的目前狀態。

下表概述了「使用授權」標籤上的可用工作。

工作	說明
續約使用授權	選取產品並按一下「續約使用授權按鈕，即可延長所選產品的授權期限。 如需詳細資訊，請參閱續約使用授權 第 3-14 頁。
修改授權配置	選取產品並按一下「修改授權配置按鈕，即可變更與每個服務計畫關聯的授權數。 如需詳細資訊，請參閱修改授權配置 第 3-15 頁。

下表概述了「使用授權」表格上顯示的資訊。

項目	說明
狀態圖示	狀態圖示可讓您快速識別使用授權問題 •  ：正常 •  ：即將到期 •  ：已到期 •  ：已超過配置
產品	指示產品名稱 按一下可用連結可登入產品主控台。
服務計畫	指示與產品關聯的服務計畫
已佈建	指示配置給產品的授權數
已使用	指示客戶已啟用的授權數
到期日	指示使用授權的到期日

項目	說明
自動續約	指示使用授權是否會自動延長授權期限

續約使用授權

為您管理的客戶續約使用授權。

注意

僅在您要使用已與 Trend Micro Licensing Management Platform 整合的帳號時，此功能才適用。

程序

1. 有多種方式可以查看「續約使用授權」視窗：
   - 從 Remote Manager Web 主控台：
     a. 按一下「客戶」。
     b. 選取使用授權已到期或即將到期的客戶。
     c. 按一下「使用授權」標籤。
     d. 按一下「續約使用授權」。
   - 從「使用授權管理」Widget 中：
     a. 按一下「已到期」或「即將到期」計數。
     b. 選取使用授權已到期或即將到期的客戶。
     c. 按一下「使用授權」標籤。
     d. 按一下「續約使用授權」。
   - 從電子郵件通知訊息中，按一下「續約」連結。
2. 指定使用授權期限的變更。

3. 按一下「提交」。

修改授權配置

每個經銷商都可以指定他們為每個客戶配置的授權數目。如果超過配置的授權數目，經銷商可以根據客戶新增更多授權。

注意

僅在您要使用已與 Trend Micro Licensing Management Platform 整合的帳號時，此功能才適用。

程序

1. 移至「客戶 > {客戶名稱} > 使用授權」。

秘訣

您還可以按一下已從「通知」Widget 請求更多授權的客戶數目，檢視需更多授權的客戶簡短清單。

2. 選取您要修改的產品。
3. 按一下「修改授權配置」。

   隨即顯示「修改授權配置」畫面。
4. 在「新授權」欄下，指定您想要為每個產品新增的新授權數目。
5. 按一下「提交」。

公司簡介

客戶的「公司簡介」標籤顯示 Licensing Management Platform 中儲存的客戶公司相關一般資訊。

下表概述了「公司簡介」標籤上的可用資訊。

項目	說明
公司名稱	客戶公司的名稱
地址	客戶公司的街道地址
城市	客戶公司所在城市
省/市	客戶公司所在省/市/地區
郵遞區號	客戶公司的郵遞區號
國家/地區	客戶公司所在國家/地區
登入 URL	客戶可用於登入 Licensing Management Platform 的 URL
公司標誌	客戶公司的自訂橫幅，可以顯示在支援的趨勢科技產品主控台上

聯絡資訊

客戶的「聯絡資訊」標籤顯示 Licensing Management Platform 中儲存的主要客戶聯絡人的相關資訊。

下表概述了「聯絡資訊」標籤上的可用資訊。

項目	說明
帳號	聯絡人的帳號名稱
使用者角色	指派給聯絡人的使用者角色
聯絡人姓名	主要聯絡人的姓名
聯絡號碼	主要聯絡人的電話號碼
電子郵件	主要聯絡人的電子郵件信箱
時區	聯絡人所在的時區
語言	聯絡人偏好的語言

客戶通知

客戶「通知」標籤可讓您設定 Remote Manager 傳送至設定的收件者的事件通知類型、第三方遠端管理與監控工具，以及傳送的電子郵件內容類型。

您可以接受全域通知設定，或針對每個客戶自訂相關設定。

如需有關全域通知設定的詳細資訊，請參閱設定全域通知設定 第 17-3 頁。

程序

1. 移至「客戶 > [客戶]」。
2. 按一下「通知」標籤。
3. 在「收件者」區段中，選取下列設定：
   - 「帳號管理員」：選取授權管理帳號做為管理客戶的代表
   - 「其他收件者」：輸入您希望 Remote Manager 通知客戶事件的任何其他人員的電子郵件信箱
4. 在「第三方通知」區段中，選取您已與 Remote Manager 整合的遠端管理與監控工具。
   - ConnectWise

     重要

     您必須先將 Remote Manager 與 ConnectWise 整合，並為每個客戶啟用個別 ConnectWise 設定，之後 Remote Manager 才能傳送通知。

     如需詳細資訊，請參閱整合 ConnectWise Manage™ 第 11-2 頁和個別客戶的 ConnectWise 設定 第 3-18 頁。
   - Kaseya

     如需詳細資訊，請參閱整合 Kaseya™ 第 13-2 頁。
   - Autotask

     如需詳細資訊，請參閱整合 Autotask™ 第 10-2 頁。

5. 在「郵件內容」區段中，接受全域設定的內容設定，或按一下「變更全域郵件內容設定」連結，以修改所有 Remote Manager 客戶的郵件內容。

6. 在「事件」區段中，選取下列設定：

   - 「使用全域通知事件設定」：將全域設定的事件設定套用至客戶

     按一下此連結可檢視全域設定，並進行將套用至所有 Remote Manager 客戶的任何必要修改。

   - 「使用自訂通知事件設定」：選取此選項，以顯示 Remote Manager 中所有產品的所有事件設定清單

     針對客戶的特定產品，啟用所需的通知事件類型並設定任何必要設定。

     如需有關可用事件類型的詳細資訊，請參閱：

     - Worry-Free Business Security Services 通知 第 17-10 頁
     - Worry-Free Business Security 通知 第 17-12 頁
     - Cloud App Security 通知 第 17-14 頁
     - Cloud Edge 通知 第 17-15 頁
     - InterScan Web Security as a Service 通知 第 17-17 頁

7. 按一下「儲存」。

個別客戶的 ConnectWise 設定

如果您想自動傳送 Remote Manager 通知，則必須在 Remote Manager 主控台上為每個趨勢科技客戶啟動 ConnectWise Manage 通知與整合。

如需有關全域 ConnectWise 整合設定的詳細資訊，請參閱整合 ConnectWise Manage™ 第 11-2 頁。

重要

若要開始在 ConnectWise 系統中接收通知，您必須先設定每個客戶的 ConnectWise 通知設定。

如需詳細資訊，請參閱客戶通知 第 3-17 頁。

程序

1. 移至「客戶 > [客戶]」。
2. 若要為此客戶整合 ConnectWise Manage 設定，請按一下「ConnectWise Manage」標籤。
3. 選取「啟用整合」。
4. 指定客戶的「ConnectWise 公司 ID」。

   注意

   按一下「確認」，確認 ConnectWise Manage 中有此公司 ID。

5. 按一下「儲存」。

   Trend Micro Remote Manager 會同步 ConnectWise Manage 中的客戶資訊，並載入任何可用合約資訊。隨即顯示以下畫面：

6. 在「合約」區段中，您可以將 ConnectWise Manage 合約指派給趨勢科技產品。

> **注意**
>
> 將合約指派給趨勢科技產品後，即可允許 ConnectWise Manage 為 Trend Micro Remote Manager 客戶提供自動帳單服務。

> **重要**
>
> - 如果您先前已使用「TMRM Management Solution」或「Managed Service」合約類型設定 ConnectWise Manage，則趨勢科技產品名稱旁邊會顯示「預設」。
> - 如果您先前未使用「TMRM Management Solution」或「Managed Service」合約類型設定 ConnectWise Manage，則可以將 ConnectWise Manage 合約指派給趨勢科技產品。

a. 按一下「設定」。

   隨即顯示「產品合約」畫面。

b. 針對每個產品，先選取合約類型，再選取合約名稱。

c. 按一下「確定」。

7. 選取以下任一整合設定：

- 選取「使用管理 > 設定第三方整合 > ConnectWise Manage 設定中的全域設定」，以套用全域整合設定。
- 選取「使用自訂設定」，以設定用於帳單和管理摘要的客戶特定通知。
  - 「在每月的 X 號將以下產品的帳單資訊傳送到 ConnectWise」：選取接收所選產品之帳單資訊的每月日期。

> **注意**
>
> 如果您選取了 29、30 或 31，而該月沒有該日，Remote Manager 會在該月的最後一天傳送通知。

- 「每 <日、週或月> 將來自 Hosted Email Security 的以下資訊傳送到 ConnectWise」：Remote Manager 會以指定的頻率從 Hosted Email Security 傳送選取的偵測資訊。

8. 按一下「儲存」。

部分 III

管理趨勢科技產品

第 4 章

Remote Manager 中的 Cloud App Security

本節包含下列主題：

Cloud App Security

Trend Micro Cloud App Security 為 Microsoft Office 365 服務、Box、Dropbox 和 Google 雲端硬碟提供進階防護服務，透過強大的企業級安全威脅和資料防護控管增強安全。Cloud App Security 可防禦網路釣魚詐騙手法、零時差和隱藏的惡意程式，以及未經授權的敏感資料傳輸。

Cloud App Security 將雲端對雲端功能與 Exchange Online、SharePoint Online、商務用 OneDrive、Box、Dropbox 和 Google 雲端硬碟進行整合，以維持高可用性和管理功能。

註冊 Cloud App Security

程序

1. 在 Remote Manager Web 主控台上新增客戶。
2. 將 Cloud App Security 新增至該客戶的服務計畫。

   如需詳細資訊，請參閱使用 Licensing Management Platform 帳號新增產品 第 3-8 頁。
3. 移至 Cloud App Security Web 主控台，以啟用使用授權。

注意

Cloud App Security 資料會自動與 Remote Manager 同步。

管理 Cloud App Security

Remote Manager 可讓您完成已註冊 Cloud App Security 安裝的以下工作。

表 4-1. Cloud App Security 管理工作

工作	說明
檢視事件	從「事件」標籤檢視 Cloud App Security 事件的清單。
管理使用者	從「使用者」標籤新增使用者、刪除使用者，以及重設密碼。
存取 Cloud App Security 主控台	按一下「開啟主控台」，存取 Cloud App Security 主控台。

Cloud App Security 事件

注意

如果發生多個「需要採取處理行動」和「警告」事件，Remote Manager 會針對最嚴重的安全威脅顯示 圖示。

表 4-2. 安全威脅事件

事件類別	詳細資訊	事件狀態
防毒	病毒偵測數超過	：在 1 小時內偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
檔案封鎖	檔案封鎖違規數超過	：在 1 小時內偵測到的檔案封鎖違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

事件類別	詳細資訊	事件狀態
沙盒虛擬平台	沙盒虛擬平台「高風險」偵測數超過	：在 1 小時內偵測到的「高風險」物件的沙盒虛擬平台偵測計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
	沙盒虛擬平台「中/低風險」偵測數超過	：在 1 小時內偵測到的「中/低風險」物件的沙盒虛擬平台偵測計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網頁信譽評等服務	URL 違規數超過	：在 1 小時內偵測到的網頁信譽評等服務違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

表 4-3. 系統事件

事件類別	詳細資訊	事件狀態
帳號同步問題	Box 存取 Token 無效	：無法存取指定的雲端儲存
	Dropbox 存取 Token 無效	：無法存取指定的雲端儲存
	Google 雲端硬碟存取 Token 無效	：無法存取指定的雲端儲存
	委派帳號的同步問題	：無法與委派帳號同步

Cloud App Security 通知

表 4-4. 安全威脅事件

事件	詳細資訊
防毒 - 病毒偵測數超過	：在 1 小時內偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

事件	詳細資訊
檔案封鎖 - 檔案封鎖違規數超過	：在 1 小時內偵測到的檔案封鎖違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
勒索軟體 - 勒索軟體偵測數超過	：在 1 小時內偵測到的勒索軟體計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
沙盒虛擬平台 - 沙盒虛擬平台偵測數超過	：在 1 小時內偵測到的「低風險」或「中風險」物件的沙盒虛擬平台偵測計數超過了設定的門檻值（如在受管理的產品主控台上所設定） ：在 1 小時內偵測到的「高風險」物件的沙盒虛擬平台偵測計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網頁信譽評等服務 - URL 違規數超過	：在 1 小時內偵測到的網頁信譽評等服務違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

表 4-5. 系統事件

事件	詳細資訊
帳號同步問題 - Box 存取 Token 無效	：無法存取指定的雲端儲存
帳號同步問題 - Dropbox 存取 Token 無效	：無法存取指定的雲端儲存
帳號同步問題 - Google 雲端硬碟存取 Token 無效	：無法存取指定的雲端儲存
帳號同步問題 - 委派帳號的同步問題	：無法與委派帳號同步

第 5 章

Remote Manager 中的 Cloud Edge

本節包含下列主題：

Cloud Edge

Cloud Edge 既具有新一代內部部署防火牆的優點，又具有受管理服務供應商的安全即服務的便利性。

藉由在內部或雲端對網路封包進行深度掃瞄和過濾，Cloud Edge 可以在閘道處制止安全威脅。Cloud Edge 智慧地結合了應用程式控管與使用者及通訊埠識別、零時差入侵偵測、惡意程式防護掃瞄、網頁信譽評等服務安全和 URL 過濾，可保護您的客戶免於發生網路侵害和業務中斷。VPN 支援還可保護行動裝置、公司網站和遠端員工的連線安全。

可將 Cloud Edge 內部部署裝置部署到世界上任何位置的客戶辦公室，然後透過直觀的雲端主控台或 Trend Micro Remote Manager，集中控制使用者存取和安全策略。Remote Manager 透過以下方式與 Cloud Edge 配合使用：提供單一入口點，來存取支援的裝置和趨勢科技產品的圖形報告與彙總資訊中心資料。您也可以使用 Remote Manager 管理多個客戶的授權與帳單。

在 Cloud Edge 裝置中註冊客戶

程序

1. 移至「客戶 > 新增客戶」。

   隨即顯示「選取新客戶」視窗。

2. 選取客戶類型。

   注意

   如果您要使用 Licensing Management Platform 帳號，則不會顯示「選取客戶類型」畫面。繼續執行步驟 4。

3. 按「下一步」。

   隨即顯示「輸入客戶資訊」畫面。

4. 輸入所需資訊。

5. 按「下一步」。

   隨即顯示「指派服務計畫」畫面。

6. 選取服務計畫和開始日期。

7. 輸入每個使用授權的裝置數目。

8. 選用：按一下「新增裝置」，然後輸入每部裝置的以下資訊。

   - 「裝置名稱」：輸入有別於公司名稱的裝置名稱。
   - 「產品序號」：產品序號不區分大小寫。

   
   注意

   裝置數目不得超過指定的授權計數。

9. 按「下一步」。

   隨即顯示「設定產品預設設定」畫面。

10. 選取預設設定範本。

11. 選用：根據需要變更預設範本。

    如需詳細資訊，請參閱設定 Cloud Edge 的預設設定範本 第 17-21 頁。

12. 按一下「儲存」。

    會關閉此畫面並出現「客戶」畫面。


注意

由於 Licensing Management Platform 已關聯您的 Cloud Edge 帳號，因此您無需輸入憑證即可登入 Cloud Edge。

管理 Cloud Edge

Remote Manager 可讓您完成已註冊 Cloud Edge 安裝的以下工作。

表 5-1. Cloud Edge 管理工作

工作	說明
將沙盒虛擬平台服務計畫指派給 Cloud Edge	按一下「新增」按鈕，然後選取沙盒虛擬平台服務計畫，以指派給現有 Cloud Edge 裝置。
檢視事件	從「事件」標籤檢視 Cloud Edge 事件的清單。
更新韌體	從「韌體更新」標籤更新過期的裝置。
註冊裝置	從「裝置」標籤註冊裝置。
存取 Cloud Edge 主控台	按一下「開啟主控台」，存取 Cloud Edge 主控台。

您還可以從「產品」樹狀結構選取已註冊的裝置，並檢視以下標籤來瞭解特定裝置的相關資訊：

- 事件
- 元件
- 網路
- VPN

Cloud Edge 事件

注意

Cloud Edge 中的某些安全威脅事件可能會顯示額外的途徑資訊。

表 5-2. 安全威脅事件

事件類別	詳細資訊	事件狀態
垃圾郵件防護	垃圾郵件偵測數	：過去一小時偵測到的垃圾郵件計數

事件類別	詳細資訊	事件狀態
防毒	病毒偵測數	：過去一小時偵測到的病毒/惡意程式計數
殭屍網路	殭屍網路偵測數	：過去一小時偵測到的殭屍網路計數
C&C 回呼	C&C 回呼數	：過去一小時偵測到的 C&C 回呼計數
IPS	IPS 偵測數	：過去一小時偵測到的 IPS 計數
Machine Learning	未知的安全威脅偵測數	：過去一小時偵測到的未知安全威脅計數
勒索軟體	勒索軟體偵測數	：過去一小時偵測到的勒索軟體計數
沙盒虛擬平台	沙盒虛擬平台偵測數	：過去一小時偵測到的沙盒虛擬平台偵測計數
網頁信譽評等服務	URL 違規數	：過去一小時偵測到的封鎖的 URL 計數
網頁安全威脅	網頁安全威脅偵測數 (包括 IPS、殭屍網路、防毒或網頁信譽評等服務違規數)	：過去一小時偵測到的網頁安全威脅計數

表 5-3. 系統事件

事件類別	詳細資訊	事件狀態
雲端電子郵件掃瞄	服務無法使用	：Cloud Edge 無法連線至雲端掃瞄服務
	在過去 24 小時內服務已變為暫時無法使用	：Cloud Edge 在過去 24 小時內暫時無法連線至雲端掃瞄服務
韌體更新	上一次韌體更新失敗。如需詳細資訊，請開啟 <Cloud Edge 雲端主控台>。	：Cloud Edge 韌體無法成功更新至最新的韌體版本
	過期的韌體	：Cloud Edge 韌體的目前版本已過期

事件類別	詳細資訊	事件狀態
離線	離線閘道。可能會影響策略部署和記錄檔分析。	：Cloud Edge 無法連線至閘道或執行掃瞄
離線 (過去 24 小時)	過去 24 小時內的離線閘道出現次數。可能已影響策略部署和記錄檔分析。	：Cloud Edge 超過 24 小時無法保持與所有註冊閘道的專用連線
資源短缺	偵測到 <數目> 個問題 • 磁碟空間使用率已超過 • CPU 使用率已超過 • 記憶體使用率已超過	：裝置上剩餘的資源量已低於設定的警訊門檻值。
資源短缺 (過去 24 小時)	偵測到 <數目> 個問題 • 磁碟空間使用率已超過 • CPU 使用率已超過 • 記憶體使用率已超過	：過去 24 小時內裝置上剩餘的資源量已低於設定的警訊門檻值，但已恢復
未註冊	無法執行雲端管理。此閘道未註冊到 Cloud Edge 雲端主控台。	：Cloud Edge 無法在閘道上執行掃瞄

Cloud Edge 通知

表 5-4. 安全威脅事件

事件	詳細資訊	警訊門檻值
網頁安全威脅 - 網頁安全威脅偵測數超過	：在 1 小時內偵測到的網頁安全威脅數計數超過了設定的門檻值（如在 Remote Manager 主控台上所設定）	請指定介於 1 到 300 之間的值。

事件	詳細資訊	警訊門檻值
C&C 回呼 - C&C 回呼偵測數超過	：在 1 小時內偵測到的 C&C 回呼計數超過了設定的門檻值（如在 Remote Manager 主控台上所設定）	請指定介於 1 到 100 之間的值。
勒索軟體 - 勒索軟體偵測數超過	：在 1 小時內偵測到的勒索軟體計數超過了設定的門檻值（如在 Remote Manager 主控台上所設定）	請指定介於 1 到 100 之間的值。

表 5-5. 系統事件

事件	詳細資訊	警訊門檻值
離線 - 偵測到離線閘道	：Cloud Edge 無法連線至閘道或執行掃瞄	指定 Remote Manager 何時傳送通知： • 「立即」：Cloud Edge 將事件報告至 Remote Manager 時立即觸發通知 • 「超過 X 天」：如果閘道在設定的天數內保持離線狀態，則觸發通知
離線 - 離線裝置復原	：Cloud Edge 已恢復離線裝置的連線	不適用
雲端電子郵件掃瞄 - 服務無法使用	：Cloud Edge 無法連線至雲端掃瞄服務	不適用
雲端電子郵件掃瞄 - 服務已復原	：Cloud Edge 已恢復至雲端掃瞄服務的連線	不適用
資源短缺 - CPU、記憶體或磁碟空間使用率超過	：裝置上剩餘的資源量已低於設定的警訊門檻值。	指定在 Remote Manager 觸發通知之前，可以使用的最大資源數（介於 80% 到 95% 之間）

第 6 章

Remote Manager 中的 Hosted Email Security

本節包含下列主題：

Hosted Email Security

Trend Micro™ Hosted Email Security 可在垃圾郵件、病毒、網路釣魚和其他電子郵件安全威脅入侵您的網路之前，將其封鎖。這是一種託管解決方案，無需安裝和維護硬體或軟體，可協助您節省 IT 員工的時間、提高使用者生產效率、頻寬、郵件伺服器儲存容量和 CPU 容量。

此外，趨勢科技的全球專家團隊會管理 Hot Fix、修補程式、更新和應用程式調校，以便解決方案效能得到持續最佳化。

注意

如需關於 Hosted Email Security 的資訊，請參閱以下文件：

http://docs.trendmicro.com

Trend Micro Remote Manager 會與位於趨勢科技資料中心的 Hosted Email Security 伺服器通訊，來監控和管理受 Hosted Email Security 保護的網路。

註冊 Hosted Email Security

1. 在 Remote Manager Web 主控台上新增客戶。
2. 新增客戶主要聯絡人。
3. 至少將一項服務新增至該客戶的帳號。
4. 在客戶的服務主控台上輸入授權碼。

從 Hosted Email Security 客戶連線至 Remote Manager Web 主控台

若要從 Trend Micro Remote Manager Web 主控台管理 Hosted Email Security，必須將客戶的 Hosted Email Security 帳號註冊到 Remote Manager。

注意

如果經銷商透過 Licensing Management Platform 將產品新增至您的帳號，則您不需要執行以下步驟。

程序

1. 新增產品至 Remote Manager Web 主控台，並儲存 GUID 或授權碼。
2. 登入客戶的 Hosted Email Security 帳號。
3. 移至「管理 > Remote Manager」。
4. 輸入 GUID 或授權碼，再按一下「連線」。

   輸入 GUID 或授權碼並按一下「連線」後，Hosted Email Security 需要十分鐘時間才能完成與 Remote Manager Web 主控台的連線。
5. 檢閱連線狀態。

   新的 Hosted Email Security 資料可能需要長達三小時時間，才能在 Remote Manager Web 主控台上更新。Hosted Email Security 客戶資訊每天更新一次。

從 Remote Manager Web 主控台中斷 Hosted Email Security 客戶的連線

若要從 Remote Manager Web 主控台中斷 Hosted Email Security 客戶的連線，請執行以下作業：

- 如果帳號已與 Licensing Management Platform 整合，則經銷商可以從 Licensing Management Platform Web 主控台刪除服務計畫。刪除服務計畫後，客戶將從 Remote Manager Web 主控台中斷連線。
- 對於其他帳號，客戶可以在 Hosted Email Security Web 主控台中開啟 Remote Manager 畫面，然後按一下「中斷連線」。

然後，會在 Hosted Email Security 主控台上通知客戶，此時按一下「確定」。

管理 Hosted Email Security

Remote Manager 可讓您完成已註冊 Hosted Email Security 安裝的以下工作。

表 6-1. Hosted Email Security 管理工作

工作	說明
檢視事件	從「即時狀態」標籤檢視 Hosted Email Security 事件的清單。
檢視策略	從「策略」標籤檢視 Hosted Email Security 策略的清單。
檢視「核可的寄件者」清單	從「核可的寄件者」標籤檢視核可的寄件者清單。
檢視「封鎖的寄件者」清單	從「封鎖的寄件者」標籤檢視封鎖的寄件者清單。
存取 Hosted Email Security 主控台	按一下「開啟主控台」，存取 Hosted Email Security 主控台。

第 7 章

Remote Manager 中的 InterScan Web Security as a Service

本節包含下列主題：

InterScan Web Security as a Service

簡單、快速、具成本效益的解決方案。

趨勢科技瞭解保護您網路的重要性，以及相應技術基礎架構所需的成本。因此，趨勢科技利用我們的專業雲端技術，建立了一款彈性雲端安全閘道產品 - InterScan Web Security as a Service (IWSaaS)。

這是一款雲端型應用程式，不需要在硬體和軟體方面有任何資本支出。使用 IWSaaS，您就可以專注於策略安全（例如策略和架構），而不必在管理網路基礎架構的運營工作方面分心。

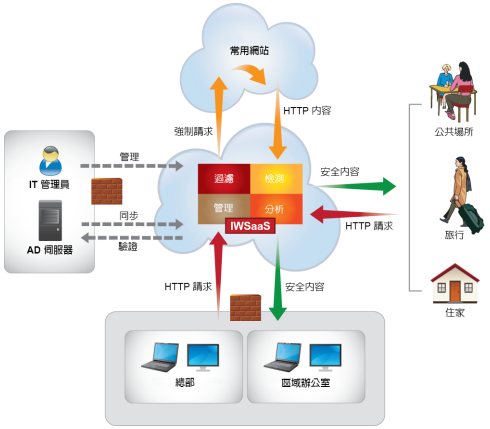
我們的雲端解決方案將協助您：

- 使用可自行設定的惡意程式防護技術，在上傳和下載檔案時防禦病毒或其他安全風險。此外，IWSaaS 會掃瞄許多類型的間諜程式、可能的資安威脅程式和其他風險類型。
- 封鎖網頁信譽評等服務 (WRS) 根據網站的信譽評分，確定為惡意網站的網站。
- 使用策略控制應用程式控管發現的 Internet 應用程式。
- 使用核可/封鎖的清單控制對任何特定網站的存取。
- 掃瞄依 URL 類別（例如「成人」和「賭博」）組織的流量。使用者使用 URL 過濾策略請求 URL、IWSaaS 時，先尋找該 URL 的類別，然後根據設定的策略允許、拒絕或監控存取。
- 使用資訊中心報告和記錄查詢功能，監控和分析 Web 流量狀態。

IWSaaS 的工作原理

下圖說明 IWSaaS 如何在雲端管理您的網路流量。使用者傳送 HTTP 請求時，不論請求位於防火牆內部還是外部，該使用者的流量都會路由過雲端。IWSaaS 會偵測請求，進行分析，然後根據管理員設定的策略進行過濾。如果允許此請求，使用者會登入 IWSaaS，然後 IWSaaS 會將安全的內容回傳給使用者。如果

不允許此請求（例如，請求禁止的 URL 類別），則 IWSaaS 會封鎖此請求並通知使用者。



按一下任何頁面上的藍色問號按鈕，可開啟該頁面的說明。會在一個面板中顯示頁面級說明。在此面板內，在畫面中填寫的必要資訊可在「步驟」標籤中找到，支援此程序的任何資訊可在「更多」標籤中找到。

您可以存取目錄型說明（位於主要橫幅的「說明」功能表中的說明內容），以及 Readme、開始使用說明和開始使用指南。

註冊 InterScan Web Security as a Service (IWSaaS)

1. 在 Remote Manager Web 主控台上新增客戶。
2. 將 IWSaaS 服務新增至該客戶的帳號。

   如需詳細資訊，請參閱使用 Licensing Management Platform 帳號新增產品 第 3-8 頁。

注意

由於 Licensing Management Platform 已關聯您的 IWSaaS 帳號，因此您不需要輸入憑證就可以登入 IWSaaS。

管理 InterScan Web Security as a Service

Remote Manager 可讓您完成已註冊 InterScan Web Security as a Service (IWSaaS) 安裝的以下工作。

表 7-1. IWSaaS 管理工作

工作	說明
檢視事件	檢視 IWSaaS 事件清單。
存取 IWSaaS 主控台	按一下「開啟主控台」，存取 IWSaaS 主控台。

InterScan Web Security as a Service 事件

表 7-2. 安全威脅事件

事件類別	詳細資訊	事件狀態
間諜程式防護	間諜程式/可能的資安威脅程式偵測	：過去 24 小時偵測到的間諜程式/可能的資安威脅程式計數
防毒	病毒偵測數	：過去 24 小時偵測到的病毒/惡意程式計數
應用程式控管	應用程式控管違規數	：過去 24 小時偵測到的應用程式控管違規計數
URL 過濾	URL 違規數	：過去 24 小時偵測到的 URL 過濾違規計數

事件類別	詳細資訊	事件狀態
網頁信譽評等服務	URL 違規數	：過去 24 小時偵測到的封鎖的 URL 計數

表 7-3. 系統事件

事件類別	詳細資訊	事件狀態
帳號同步問題	AD/LDAP 的同步問題	：無法與 AD/LDAP 同步

InterScan Web Security as a Service 通知

表 7-4. 系統事件

事件	詳細資訊
帳號同步問題 - AD/LDAP 的同步問題	：無法與 AD/LDAP 同步

第 8 章

Remote Manager 中的 Worry-Free Business Security

本節包含下列主題：

Worry-Free Business Security

趨勢科技™ Worry-Free Business Security Standard 和 Worry-Free Business Security Advanced 是適用於中小型企業的全面、集中式管理解決方案。

Worry-Free Business Security Standard 為桌面和伺服器提供用戶端防毒和防火牆防護。Worry-Free Business Security Advanced 提供的功能與 Worry-Free Business Security Standard 相同，但針對執行 Microsoft™ Exchange Server 的郵件伺服器提供垃圾郵件防護和電子郵件安全威脅解決方案。Worry-Free Business Security Standard 和 Advanced 包含伺服器端元件，用於從中心位置監控和管理用戶端防護。

Trend Micro Remote Manager 透過與 Worry-Free Business Security Standard 和 Advanced 伺服器上執行的 Agent 通訊，監控和管理受 Worry-Free Business Security Standard 和 Advanced 保護的網路。

如需關於 Worry-Free Business Security Standard 和 Advanced 的資訊，請參閱以下文件：

http://docs.trendmicro.com

註冊 Worry-Free Business Security Standard and Advanced

您可以使用 Worry-Free Business Security Web 主控台在 Remote Manager 中註冊 Worry-Free Business Security。註冊程序需要下列項目：

1. 根據您的帳號類型而定，記錄下列來自 Remote Manager 主控台的資訊：
   - Licensing Management Platform 帳號：未註冊 Worry-Free Business Security 伺服器的啟動碼
     a. 移至「客戶 > {客戶} > {Worry-Free Business Security 伺服器名稱}」。
     b. 複製出現在畫面上的啟動碼。

- OLR 帳號：現有 Worry-Free Business Security 客戶的 TMRM Agent GUID

  a. 移至「客戶 > {客戶} > {Worry-Free Business Security 伺服器名稱}」。

  b. 按一下「TMRM Agent」標籤。

  c. 複製出現在畫面上的 GUID。

2. 安裝 Trend Micro Remote Manager Agent 程式。

   您可以在 Worry-Free Business Security 伺服器上的安裝目錄中找到 Trend Micro Remote Manager Agent 程式。如需詳細資訊，請參閱《*Worry-Free Business Security 管理手冊*》。

檢查 Trend Micro Remote Manager Agent 連線

為確保 Trend Micro Remote Manager 能夠與 Worry-Free Business Security 伺服器正確通訊，請確認 Trend Micro Remote Manager Agent 程式的連線狀態。

程序

1. 在 Trend Micro Remote Manager 主控台上，移至「客戶 > {客戶} > {Worry-Free Business Security 伺服器名稱}」。
2. 按一下「TMRM Agent」標籤。
3. 確認連線狀態。

狀態	說明	解決辦法
線上	Agent 正在正常運作。	無
異常	Agent 似乎已離線且無法對 Remote Manager 伺服器做出回應，但尚未傳送登出請求。	如果受管理伺服器未正常關機，則可能會出現此狀態。請確保受管理伺服器管理員瞭解此狀況。如有必要，請聯絡管理員。

狀態	說明	解決辦法
已關閉	此狀態是從主控台手動設定的。Agent 處於已關閉狀態時，Agent 每 10 分鐘從伺服器查詢一次命令。	提交命令以啟動 Agent。
離線	Agent 在向 Remote Manager 伺服器傳送登出請求後正常關閉。通常，如果使用者已關閉 Agent 服務或受管理伺服器已關機，則 Agent 會處於此狀態。	請確保受管理伺服器管理員瞭解伺服器已關機。如有必要，請聯絡受管理伺服器管理員。
未知	Agent 未正常運作。	移除 Agent 並要求受管理伺服器管理員重新安裝 Agent。如果此問題仍然存在，請聯絡您的支援提供商。
嵌入程式錯誤	主控台已在 Agent 的服務嵌入程式元件中偵測到錯誤。	移除 Agent 並要求受管理伺服器管理員重新安裝 Agent。如果此問題仍然存在，請聯絡您的支援提供商。
未註冊	Agent 尚未註冊到 Remote Manager 伺服器。	Agent 可能尚未安裝，或尚無法與 Remote Manager 伺服器成功通訊。請聯絡受管理伺服器管理員。
版本不符	已偵測到以下任何元件的版本不相容： • Agent • Remote Manager • Worry-Free Business Security（Standard 和 Advanced）	升級 Agent 和受管理伺服器。如果無法解決問題，請向趨勢科技資料中心管理員報告此問題。

管理 Worry-Free Business Security 伺服器

在 Remote Manager 主控台上存取已註冊的 Worry-Free Business Security Standard 或 Advanced 伺服器（按一下「客戶 > {客戶} > {Worry-Free Business Security 伺服器名稱}」），以檢視事件資料、部署掃瞄設定、啟動特定功能，以及傳送更新至伺服器和 Security Agent。

下表概述了在「客戶 > {客戶}」畫面上選取已註冊的 Worry-Free Business Security Standard 或 Advanced 伺服器後可用的區段。

區段	說明
產品樹狀結構	顯示 Worry-Free Business Security 伺服器和相關的裝置群組 將游標懸停在產品樹狀結構中的 Worry-Free Business Security 伺服器名稱上，便會顯示齒輪圖示 ()。按一下該圖示並按一下「同步」，即可手動觸發 Remote Manager 的狀態更新。

「事件」標籤	顯示所選伺服器的安全威脅和系統事件
	• 可使用出現在表格上方的下拉方塊排序事件清單
	  • 檢視方式：依嚴重性顯示事件
	  • 安全威脅和系統：依類型顯示事件
	  • 狀態：依目前狀態顯示事件
	• 按一下「出現次數」計數以開啟記檔錄詳細資訊畫面，當中提供了有關所選事件的詳細資訊。
	• 在「狀態」欄中，您可以選擇對特定事件類型執行動作
	  • 解除：從 Remote Manager 和 Worry-Free Business Security 主控台移除事件通知
	  注意
	  解除事件不會刪除與事件相關的任何記錄資料。Remote Manager 僅會解除事件通知資訊。
	  • 立即更新：更新具有相關元件的受影響 Security Agent 和伺服器

「群組」標籤	可讓您針對所選的裝置群組開始或停止掃瞄 • 立即掃瞄：選取所需的裝置群組並按一下，將「手動掃瞄」命令傳送至 Security Agent • 停止掃瞄：選取所需的裝置群組並按一下，以通知所有選取的 Security Agent 停止任何進行中的掃瞄

區段	說明
「網域設定」標籤	可讓您在所有支援的 Security Agent 上啟動或關閉功能和服務 • 啟動：選取項目並按一下，以在所有 Security Agent 上啟動功能或服務 • 關閉：選取項目並按一下，以在所有 Security Agent 上關閉功能或服務 • 啟動弱點評估：按一下以評估 Security Agent 端點是否有已知的弱點  注意 僅適用於執行 9.5 版或更早版本的 Worry-Free Business Security 伺服器。 • 啟動損害清除及復原服務：按一下以開始掃瞄所有支援的 Security Agent，檢查其中是否有特洛伊木馬程式、蠕蟲和間諜程式  注意 僅適用於執行 9.5 版或更早版本的 Worry-Free Business Security 伺服器。
「受管理的伺服器」標籤	可讓您檢視有關 Worry-Free Business Security 伺服器的詳細資訊，以及執行更新工作 • 更新受管理的伺服器：按一下以將元件更新命令傳送至伺服器 • 更新 Security Agent：按一下以將元件更新命令傳送至所有 Security Agent • 檢視：按一下以檢視 Worry-Free Business Security 伺服器元件的目前版本和更新歷史記錄
「TMRM Agent」標籤	可讓您檢視有關 Trend Micro Remote Manager Agent 程式的詳細資訊，包括連線狀態和 GUID
伺服器資訊	可讓您儲存有關 Worry-Free Business Security 伺服器的資訊，包括「名稱」、「URL」和任何重要的「附註」。

檢視裝置群組資訊

下表概述了在「客戶 > {客戶}」畫面上，選取已註冊 Worry-Free Business Security Standard 或 Advanced 伺服器上的個別裝置群組後可用的區段。

區段	說明
「裝置」標籤	顯示有關指派至所選群組的所有 Security Agent 端點的基本資訊。
「安全設定」標籤	針對指派至所選群組的 Security Agent，顯示掃瞄方法以及功能或服務的「已啟動」或「已關閉」狀態

Worry-Free Business Security 事件

表 8-1. 安全威脅事件

事件類別	詳細資訊	事件狀態
垃圾郵件防護	收到的所有郵件中的垃圾郵件偵測數超過	：在 1 小時內偵測到的垃圾郵件數與所收到總郵件數的比率超過了設定的門檻值（如在受管理的產品主控台上所設定）
間諜程式防護	需要重新啟用裝置的偵測數	：顯示感染受管理產品無法完全清除而需要客戶重新啟用端點才能完成清除程序的間諜程式/可能的資安威脅程式的端點數
	間諜程式/可能的資安威脅程式偵測數超過	：在 1 小時內偵測到的間諜程式/可能的資安威脅程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

事件類別	詳細資訊	事件狀態
防毒	端點已關閉即時掃瞄	：已關閉即時掃瞄的 Security Agent 無法保護端點免於新建立或執行之檔案中的病毒/惡意程式侵害
	Exchange 伺服器已關閉即時掃瞄	：已關閉即時掃瞄的 Exchange 伺服器可允許傳送電子郵件中的所有附件，使得客戶網路容易受到大量郵件蠕蟲攻擊。
	未解決的安全威脅	：不成功的動作表示病毒或惡意程式已成功規避防毒並已使端點中毒。 注意 Remote Manager 假設未成功清除、隔離或刪除病毒或惡意程式的電腦已中毒。
	端點上的病毒偵測數超過	：在 1 小時內在端點上偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
	Exchange 伺服器上的病毒偵測數超過	：在 1 小時內在 Exchange 伺服器上偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
行為監控	行為監控違規數超過	：在 1 小時內偵測到的行為監控違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
週邊設備存取控管	週邊設備存取控管違規數超過	：在 1 小時內偵測到的週邊設備存取控管違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網路病毒	網路病毒偵測數超過	：在 1 小時內偵測到的網路病毒計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

事件類別	詳細資訊	事件狀態
疫情爆發防範	疫情爆發防範已啟用	：已在桌面/伺服器平台上啟用疫情爆發防範，來應對異常安全威脅活動
	疫情爆發防範已關閉	：已在桌面/伺服器平台上關閉疫情爆發防範，並已恢復正常的網路狀況
Machine Learning	超過未知的安全威脅偵測數	：在 1 小時內偵測到的未知安全威脅數計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
URL 過濾	URL 違規數超過	：在 1 小時內偵測到的 URL 過濾違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網頁信譽評等服務	URL 違規數超過	：在 1 小時內偵測到的網頁信譽評等服務違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

表 8-2. 系統事件

事件類別	詳細資訊	事件狀態
資源短缺	剩餘如下磁碟空間	：伺服器上剩餘的磁碟空間量已低於設定的警訊門檻值。
主動式雲端截毒技術服務	服務無法使用	：Worry-Free Business Security 主控台無法連線至雲端截毒伺服器
更新	過期的 Agent	：超過 <數目> 個 Security Agent 在過去一小時內未收到最新的防毒病毒碼
	過期的 Exchange 伺服器	：在 Exchange 伺服器上偵測到過期的元件

Worry-Free Business Security 通知

表 8-3. 安全威脅事件

事件	詳細資訊
垃圾郵件防護 - 收到的所有郵件中的垃圾郵件偵測數超過	：在 1 小時內偵測到的垃圾郵件數與所收到總郵件數的比率超過了設定的門檻值（如在受管理的產品主控台上所設定）
間諜程式防護 - 需要重新啟用裝置的偵測數	：顯示感染受管理產品無法完全清除而需要客戶重新啟用端點才能完成清除程序的間諜程式/可能的資安威脅程式的端點數
間諜程式防護 - 間諜程式/可能的資安威脅程式偵測數超過	：在 1 小時內偵測到的間諜程式/可能的資安威脅程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
防毒 - 關閉即時掃瞄的端點數	：已關閉即時掃瞄的 Security Agent 無法保護端點免於新建立或執行之檔案中的病毒/惡意程式侵害
防毒 - 關閉即時掃瞄的 Exchange 伺服器數	：已關閉即時掃瞄的 Exchange 伺服器可允許傳送電子郵件中的所有附件，使得客戶網路容易受到大量郵件蠕蟲攻擊。
防毒 - 未解決的安全威脅	：不成功的動作表示病毒或惡意程式已成功規避防毒並已使端點中毒。 注意 Remote Manager 假設未成功清除、隔離或刪除病毒或惡意程式的電腦已中毒。
防毒 - 端點上的病毒偵測數超過	：在 1 小時內在端點上偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
防毒 - Exchange 伺服器上的病毒偵測數超過	：在 1 小時內在 Exchange 伺服器上偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

事件	詳細資訊
行為監控 - 行為監控違規數超過	：在 1 小時內偵測到的行為監控違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
週邊設備存取控管 - 週邊設備存取控管違規數超過	：在 1 小時內偵測到的週邊設備存取控管違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網路病毒 - 網路病毒偵測數超過	：在 1 小時內偵測到的網路病毒計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
Machine Learning - 超過未知的安全威脅偵測數	：在 1 小時內偵測到的未知安全威脅數計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
URL 過濾 - URL 違規數超過	：在 1 小時內偵測到的 URL 過濾違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網頁信譽評等服務 - URL 違規數超過	：在 1 小時內偵測到的網頁信譽評等服務違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

表 8-4. 系統事件

事件	詳細資訊
資源短缺 - 剩餘如下磁碟空間	：伺服器上剩餘的磁碟空間量已低於設定的警訊門檻值。
主動式雲端截毒技術服務 - 服務無法使用	：Worry-Free Business Security 主控台無法連線至雲端截毒伺服器
更新 - 過期的 Exchange 伺服器	：在 Exchange 伺服器上偵測到過期的元件
更新 - 過期的 Agent	：超過 <數目> 個 Security Agent 在過去一小時內未收到最新的防毒病毒碼

第 9 章

Remote Manager 中的 Worry-Free Business Security Services

本節包含下列主題：

Worry-Free Business Security Services

趨勢科技™ Worry-Free Business Security Services 是適用於中小型企業的全面、集中式管理解決方案。

Worry-Free Business Security Services 具有 Worry-Free Business Security Standard 的大部分優點。由於 Worry-Free Business Security Services 是一項託管服務，因此您可以隨處集中管理安全事宜，完全不需要新增、安裝、設定或維護伺服器。趨勢科技的安全專家會主控並持續為您更新服務。

Trend Micro Remote Manager 可監控和管理位於趨勢科技資料中心的 Worry-Free Business Security Services 伺服器。

如需關於 Worry-Free Business Security Services 的資訊，請參閱以下文件：

http://docs.trendmicro.com

註冊 Worry-Free Business Security Services

程序

1. 移至「客戶 > 新增客戶」。

   隨即顯示「選取新客戶」視窗。

2. 選取客戶類型。

   注意

   如果您要使用 Licensing Management Platform 帳號，則不會顯示「選取客戶類型」畫面。繼續執行步驟 4。

3. 按「下一步」。

   隨即顯示「輸入客戶資訊」畫面。

4. 輸入所需資訊。
5. 按「下一步」。

   隨即顯示「指派服務計畫」畫面。
6. 選取服務計畫和開始日期。
7. 輸入每個使用授權的裝置數目。
8. 按「下一步」。

   隨即顯示「設定產品預設設定」畫面。
9. 選取預設設定範本。
10. 選用：根據需要變更預設範本。

    如需詳細資訊，請參閱設定 Worry-Free Business Security Services 的預設設定範本 第 17-19 頁。
11. 按一下「儲存」。

    會關閉此畫面並出現「客戶」畫面。

注意

由於 Licensing Management Platform 已關聯您的 Worry-Free Business Security Servies 帳號，因此您不需要輸入憑證就可以登入 Worry-Free Business Security Services。

將 Worry-Free Business Security Services 客戶連線至 Remote Manager Web 主控台

若要將 Worry-Free Business Security Services 客戶連線至 Trend Micro Remote Manager Web 主控台：

注意

如果經銷商透過 Licensing Management Platform 將產品新增至您的帳號，則您不需要執行以下步驟。

程序

1. 新增產品至 Remote Manager Web 主控台，並儲存 GUID 或授權碼。

   如需詳細資訊，請參閱使用 Licensing Management Platform 帳號新增產品 第 3-8 頁。

2. 登入客戶的 Worry-Free Business Security Services 帳號。

3. 移至「管理 > Trend Micro Remote Manager」。

4. 輸入授權碼，再按一下「連線」。

從 Remote Manager Web 主控台中斷 Worry-Free Business Security Services 客戶的連線

若要從 Remote Manager Web 主控台中斷 Worry-Free Business Security Services 的連線，請執行以下作業：

- 如果帳號已與 Licensing Management Platform 整合，則經銷商可以從 Licensing Management Platform Web 主控台刪除服務計畫。刪除服務計畫後，客戶將從 Remote Manager Web 主控台中斷連線。
- 對於其他帳號，客戶可以在 Worry-Free Business Security Services Web 主控台中開啟 Remote Manager 畫面，然後按一下「中斷連線」。

然後，將在 Worry-Free Business Security Services 主控台中通知客戶。

管理 Worry-Free Business Security Services

Remote Manager 可讓您完成已註冊 Worry-Free Business Security Services 安裝的以下工作：

表 9-1. Worry-Free Business Security Services 管理工作

工作	說明
檢視事件	從「事件」標籤檢視 Worry-Free Business Security Standard 事件的清單。
管理群組	使用「群組」標籤上的「掃瞄」下拉按鈕，以執行下列掃瞄動作： • 開始正常掃瞄：開始掃瞄 Mac 和 Windows 端點 正常掃瞄支援 Windows Security Agent 5.3 版或更新版本，以及 Mac Security Agent 1.7.2801 版或更新版本。 • 開始加強掃瞄：開始進階掃瞄，以分析和清除正常掃瞄無法移除的安全威脅 加強掃瞄支援 Windows Security Agent 6.3 版或更新版本。 • 停止掃瞄：停止掃瞄 Windows 端點 停止掃瞄支援 Windows Security Agent 5.3 版或更新版本。 您也可以執行下列工作： • 立即更新：更新所選群組中 Security Agent 上的元件 • 複製設定：從選取的群組複製 Security Agent 設定，並且讓您將相同的設定指派給其他群組或客戶 從表格中選取群組類型，然後按一下所需的工作按鈕。
存取 Worry-Free Business Security Services 主控台	按一下「開啟主控台」，存取 Worry-Free Business Security Services 主控台。

您也可以檢視個別裝置群組資訊、傳送掃瞄命令給個別 Agent，以及在選取向所選的 Worry-Free Business Security Services 伺服器回報的特定群組後，部署群組策略設定。

如需詳細資訊，請參閱：

- 檢視 Worry-Free Business Security Services 裝置群組資訊 第 9-6 頁
- Worry-Free Business Security Services 的安全設定 第 9-7 頁

檢視 Worry-Free Business Security Services 裝置群組資訊

下表概述了在「客戶 > {客戶}」畫面上選取個別 Worry-Free Business Security Services 裝置群組後，「裝置」標籤上的可用資訊。

區段	說明
掃瞄下拉按鈕	選取一或多個 Security Agent 並按下列其中一項： • 開始正常掃瞄：開始掃瞄 Mac 和 Windows 端點 正常掃瞄支援 Windows Security Agent 5.3 版或更新版本，以及 Mac Security Agent 1.7.2801 版或更新版本。 • 開始加強掃瞄：開始進階掃瞄，以分析和清除正常掃瞄無法移除的安全威脅 加強掃瞄支援 Windows Security Agent 6.3 版或更新版本。 • 停止掃瞄：停止掃瞄 Windows 端點 停止掃瞄支援 Windows Security Agent 5.3 版或更新版本。
裝置表	顯示有關指派至所選群組的所有 Security Agent 端點的基本資訊。

Worry-Free Business Security Services 的安全設定

功能	說明
掃瞄方法	• 「雲端截毒掃瞄」：用戶端使用本身的掃瞄引擎，但主要依賴「掃瞄伺服器」上的病毒碼檔案（而非僅使用本機病毒碼檔案）來識別安全威脅。 • 「標準掃瞄」：用戶端使用本身的掃瞄引擎和本機病毒碼檔案來識別安全威脅。
防毒/間諜程式防護	• 「啟用即時防毒/間諜程式防護」：即時掃瞄提供對檔案型安全威脅的防護。

防火牆	• 「啟用防火牆」：防火牆能在用戶端和網路之間建立一道屏障，以封鎖或允許特定類型的網路流量。此外，防火牆會辨識網路封包中可能攻擊用戶端的行為模式。
	  • 簡易模式：以趨勢科技的預設設定啟用防火牆
	  • 進階模式：設定安全層級、IDS、通知和例外。
	
	  重要
	  選取進階模式後，您必須使用 Worry-Free Business Security Services 主控台設定進階設定。

功能	說明
網頁信譽評等服務	• 「啟用網頁信譽評等服務」：網頁信譽評等服務可加強對於惡意網站的防護。「網頁信譽評等服務」利用趨勢科技的龐大 Web 安全資料庫，來檢查用戶端嘗試存取的 URL 或內嵌在電子郵件中而且會聯絡網站的 URL 的信譽。 • 高：封鎖以下網頁： • 危險：已驗證為詐騙網頁或已知的安全威脅來源 • 非常可疑：疑似詐騙網頁或可能的安全威脅來源 • 可疑：與垃圾郵件相關或可能遭到破壞 • 未測試的：雖然趨勢科技會主動測試網頁以確保安全，但使用者仍可能會在造訪新的或較不熱門的網站時遇到未測試的網頁。封鎖對於未測試網頁的存取，可以提高安全性，但也會讓人無法存取某些安全的網頁 • 中：封鎖以下網頁： • 危險：已驗證為詐騙網頁或已知的安全威脅來源 • 非常可疑：疑似詐騙網頁或可能的安全威脅來源 • 「低 (預設值)」：封鎖以下頁面： • 危險：已驗證為詐騙網頁或已知的安全威脅來源
URL 過濾	• 「啟用 URL 過濾」：URL 過濾可協助您控制網站的存取以減少員工上班打混摸魚的時間、減少 Internet 頻寬用量，同時建立更安全的 Internet 環境。您可以選擇想要的 URL 過濾保護層級，或是自訂要過濾的網站類型。 • 「高」：封鎖已知或潛在的安全威脅、不適當或可能令人不悅的內容，或是封鎖可能會影響產能或頻寬的內容，以及未分級的頁面 • 「中」：封鎖已知的安全威脅與不適當的內容 • 「低 (預設值)」：封鎖已知的安全威脅 • 「自訂」：選取您的個人類別，以及您是否想要在上班時間或休閒時間封鎖這些類別。

功能	說明
行為監控	• 「啟用行為監控」：「行為監控」可保護用戶端的作業系統、登錄項目、其他軟體或檔案和資料夾免於遭到未經授權的變更。 • 啟用所有勒索軟體防護功能 • 對未經授權的加密或修改啟用文件保護：防止對文件進行未經授權的變更。 注意 啟動此選項將停止用於重新命名、修改和刪除檔案的處理程序，然後隔離正在執行這些處理程序的程式。 • 自動備份與還原可疑程式修改的檔案：如果已啟用文件保護，則會自動備份由可疑程式修改的檔案。 • 對通常與勒索軟體相關聯的處理程序啟用封鎖：封鎖通常與綁架嘗試相關聯的處理程序，來防止端點遭受勒索軟體攻擊。 • 啟動程式檢測以偵測和封鎖已遭到破壞的可執行檔：監控處理程序是否有類似勒索軟體的行為，以增強偵測。 • 啟動 Intuit QuickBooks 防護：可防止其他程式對所有 Intuit QuickBooks 檔案和資料夾進行未經授權的變更。啟動此功能將不會影響從 Intuit QuickBooks 程式內部進行的變更，而只會防止檔案遭其他未經授權的應用程式變更。

功能	說明

Machine Learning	• 「啟用 Machine Learning」：Machine Learning 可透過進階檔案特徵分析與主動程序監控，保護您的網路免受新的、過去未識別或是未知安全威脅的侵襲。
	  • 檔案
	  • 隔離： 選取此項，即會自動依「Machine Learning」分析結果，將展現惡意程式相關特徵的檔案隔離
	  • 僅記錄檔： 選取此項，即會掃瞄未知檔案並記錄「Machine Learning」分析結果，以供內部進一步調查安全威脅
	  • 處理程序
	  • 終止：選取此項，即會自動依「Machine Learning」分析結果，將展現惡意程式相關行為的程序或程式檔終止
	  重要
	「Machine Learning」會嘗試將已執行惡意程序或程式檔的檔案清除。如果清除處理行動不成功，Machine Learning 會將受影響的檔案隔離。
	  • 僅記錄檔：選取此項，即會掃瞄未知程序或程式檔並記錄「Machine Learning」分析結果，以供內部進一步調查安全威脅

郵件掃瞄	• 「啟用 POP3 郵件掃瞄」：「POP3 郵件掃瞄」嵌入程式可即時保護用戶端，避免用戶端受到透過 POP3 電子郵件訊息傳送的安全威脅和垃圾郵件的侵擾。

如需詳細資訊，請參閱 Worry-Free Business Security Services 線上說明。

Worry-Free Business Security Services 事件

表 9-2. 安全威脅事件

事件類別	詳細資訊	事件狀態
間諜程式防護	需要重新啟用裝置的偵測數	：顯示感染受管理產品無法完全清除而需要客戶重新啟用端點才能完成清除程序的間諜程式/可能的資安威脅程式的端點數
	間諜程式/可能的資安威脅程式偵測數超過	：在 1 小時內偵測到的間諜程式/可能的資安威脅程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
防毒	即時掃瞄已關閉	：已關閉即時掃瞄的 Security Agent 無法保護端點免於新建立或執行之檔案中的病毒/惡意程式侵害
	未解決的安全威脅	：不成功的動作表示病毒或惡意程式已成功規避防毒並已使端點中毒。 注意 Remote Manager 假設未成功清除、隔離或刪除病毒或惡意程式的電腦已中毒。
	病毒偵測數超過	：在 1 小時內偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
應用程式控管	應用程式控管違規數超過	：在 1 小時內偵測到的應用程式控管違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

事件類別	詳細資訊	事件狀態
行為監控	行為監控違規數超過	：在 1 小時內偵測到的行為監控違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
週邊設備存取控管	週邊設備存取控管違規數超過	：在 1 小時內偵測到的週邊設備存取控管違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網路病毒	網路病毒偵測數超過	：在 1 小時內偵測到的網路病毒計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
疫情爆發防範	疫情爆發防範已啟用	：已在桌面/伺服器平台上啟用疫情爆發防範，來應對異常安全威脅活動
	疫情爆發防範已關閉	：已在桌面/伺服器平台上關閉疫情爆發防範，並已恢復正常的網路狀況
Machine Learning	超過未知的安全威脅偵測數	：在 1 小時內偵測到的未知安全威脅數計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
URL 過濾	URL 違規數超過	：在 1 小時內偵測到的 URL 過濾違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網頁信譽評等服務	URL 違規數超過	：在 1 小時內偵測到的網頁信譽評等服務違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

表 9-3. 系統事件

事件類別	詳細資訊	事件狀態
主動式雲端截毒技術服務	中斷連線的 Agent 數目	：Security Agent 無法連線至主動式雲端截毒技術

事件類別	詳細資訊	事件狀態
更新	過期的 Agent	：防毒病毒碼發佈的兩個小時後過期的病毒碼超過門檻值的 Security Agent 數

Worry-Free Business Security Services 通知

重要

對於具有可設定門檻值的事件，您必須在 Worry-Free Business Security Services 主控台上單獨為每個客戶設定門檻值。

表 9-4. 安全威脅事件

事件	詳細資訊
防毒 - 未解決的安全威脅	：不成功的動作表示病毒或惡意程式已成功規避防毒並已使端點中毒。 注意 Remote Manager 假設未成功清除、隔離或刪除病毒或惡意程式的電腦已中毒。
防毒 - 即時掃瞄已關閉	：已關閉即時掃瞄的 Security Agent 無法保護端點免於新建立或執行之檔案中的病毒/惡意程式侵害
防毒 - 病毒偵測數超過	：在 1 小時內偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
間諜程式防護 - 需要重新啟用裝置的偵測數	：顯示感染受管理產品無法完全清除而需要客戶重新啟用端點才能完成清除程序的間諜程式/可能的資安威脅程式的端點數

事件	詳細資訊
間諜程式防護 - 間諜程式/可能的資安威脅程式偵測數超過	：在 1 小時內偵測到的間諜程式/可能的資安威脅程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網頁信譽評等服務 - URL 違規數超過	：在 1 小時內偵測到的網頁信譽評等服務違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
URL 過濾 - URL 違規數超過	：在 1 小時內偵測到的 URL 過濾違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
Machine Learning - 超過未知的安全威脅偵測數	：在 1 小時內偵測到的未知安全威脅數計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
行為監控 - 行為監控違規數超過	：在 1 小時內偵測到的行為監控違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網路病毒 - 網路病毒偵測數超過	：在 1 小時內偵測到的網路病毒計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
週邊設備存取控管 - 週邊設備存取控管違規數超過	：在 1 小時內偵測到的週邊設備存取控管違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
應用程式控管 - 應用程式控管違規數超過	：在 1 小時內偵測到的應用程式控管違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

表 9-5. 系統事件

事件	詳細資訊
更新 - 過期的 Agent	：防毒病毒碼發佈的兩個小時後過期的病毒碼超過門檻值的 Security Agent 數
主動式雲端截毒技術服務 - Agent 已中斷連線	：Security Agent 無法連線至主動式雲端截毒技術

部分 IV

整合第三方解决方案

第 10 章

AutoTask 支援

本節介紹如何將 Remote Manager 與 Autotask 整合，以及趨勢科技產品和服務所支援的事件通知。

包含下列主題：

整合 Autotask™

設定以下設定，以將 Autotask™ 與 Remote Manager 整合：

將 Remote Manager 與 Autotask 整合

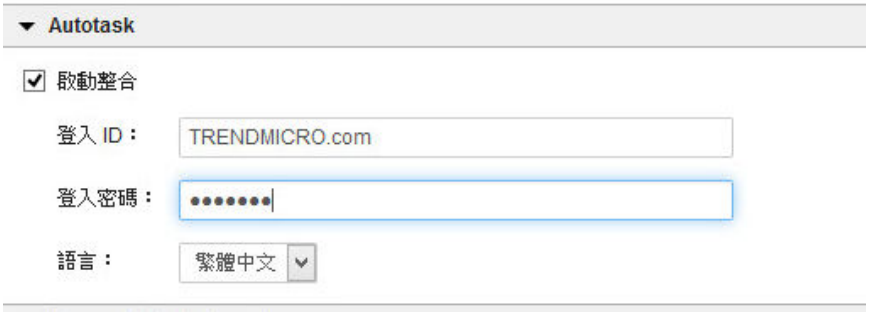
程序

1. 登入 Autotask Web 主控台，網址為 https://ww2.autotask.net。
2. 移至「Autotask Logo Menu > ADMIN」。

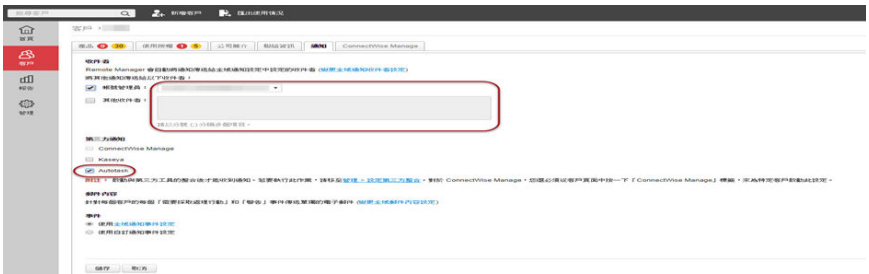
   隨即顯示「ADMIN」畫面。
3. 展開「APPLICATION-WIDE (SHARED) FEATURES」，然後按一下「Incoming Email Processing」。

   隨即顯示「INCOMING EMAIL PROCESSING」畫面。
4. 將游標懸停在「Add Ticket Email Service (ATES)」功能表圖示 () 上，然後按一下「Edit」。

   隨即顯示「EMAIL PROCESSING MAILBOX - ADD TICKET EMAIL SERVICE (ATES)」畫面。
5. 記錄下您的「Service Provider ID」和「Service Provider Password」，以便您可以稍後輸入這些詳細資訊。
6. 登入 Remote Manager Web 主控台。
7. 移至「管理 > 設定第三方整合」。
8. 在「Autotask」區段中，選取「啟用整合」，然後輸入您之前記錄下的「登入 ID」和「登入密碼」。從「語言」下拉式功能表中，選取您的慣用語言。



9. 按一下「儲存」。
10. 移至「客戶」畫面。
11. 選取您想要從其接收 Autotask 通知的公司。
12. 按一下「通知」標籤。
13. 選取「我」做為收件者，以確保您將收到電子郵件通知。如有必要，請在「其他收件者」欄位中輸入收件者的電子郵件信箱，以新增其他收件者。
14. 從「第三方通知」清單中選取「Autotask」。



15. 請選取下列其中一個選項：
    - 使用預設即時電子郵件通知設定
    - 使用自訂設定

允許 Autotask 顯示 Remote Manager 通知

程序

1. 登入 Autotask Web 主控台，網址為 https://ww2.autotask.net。
2. 移至「Autotask Logo Menu > ADMIN」。

   隨即顯示「ADMIN」畫面。
3. 展開「SERVICE DESK (TICKETS)」，然後移至「Issue & Sub-Issue Types > Managed Services Alert」。
4. 將以下欄位新增至票證系統：
   - 趨勢科技安全威脅事件
   - 趨勢科技系統事件
   - 趨勢科技使用授權事件
5. 按一下「Save & Close」。
6. 移至「Autotask Logo Menu」，以返回「ADMIN」頁面。
7. 展開「APPLICATION-WIDE (SHARED) FEATURES」，然後移至「Incoming Email Processing」。

   隨即顯示「INCOMING EMAIL PROCESSING」畫面。
8. 將游標懸停在「Add Ticket Email Service (ATES)」功能表圖示 () 上，然後按一下「Edit」。

   隨即顯示「EMAIL PROCESSING MAILBOX - ADD TICKET EMAIL SERVICE (ATES)」畫面。
9. 按一下「Ticket」標籤。
10. 從「Sub-Issue Type」下拉式功能表，選取「Trend Micro Threat Events」。
11. 按一下「Save & Close」。
12. 移至「Autotask Logo Menu」，以返回「ADMIN」頁面。

13. 展開「APPLICATION-WIDE (SHARED) FEATURES」，然後移至「USER-DEFINED FIELDS > + New」。

    隨即顯示「USER-DEFINED FIELDS」畫面。

14. 在「Name」欄位中鍵入 `Trend Micro Site ID`，然後選取「Required」。

15. 按一下「Save & Close」。

讓 Autotask 產生帳號票證

程序

1. 移至「Autotask Logo Menu > CRM」。

   隨即顯示「ACCOUNT SEARCH」畫面。

2. 按一下「+ New Account」。在開啟的新快顯視窗中，輸入帳號資訊，包括「Trend Micro Site ID」。

   注意

   「Trend Micro Site ID」是從 Remote Manager 匯出的唯一 ID。您可以透過以下方式找到此 ID：登入至 Remote Manager 主控台，然後移至「客戶 > 全部匯出」。在匯出的 `.csv` 檔案中，「唯一 ID」位於「公司」名稱的右側。

3. 按一下「Save & Close」。

4. 移至「CRM > My Account Tickets」（位於「Reports」下），以檢視您的帳號票證。

Autotask 中支援的趨勢科技產品事件

Remote Manager 可以將以下事件通知傳送至 Autotask 系統。

產品	事件	
Cloud Edge	• 殭屍網路 • 入侵防護系統 (IPS)	• 網頁信譽評等服務 • 病毒
Hosted Email Security	• 電子郵件總流量 • 接受的電子郵件大小 • 安全威脅摘要	• 收到垃圾郵件最多的前幾名收件者 • 收到病毒最多的前幾名收件者
InterScan Web Security as a Service	• 防毒 • 間諜程式防護 • 網頁信譽評等服務	• URL 過濾 • 應用程式控管
Worry-Free Business Security Standard 和 Advanced	• Agent 異常 • 疫情爆發防範 • 防毒 • 間諜程式防護 • 網頁信譽評等服務 • 行為監控 • 網路病毒 • 垃圾郵件防護 • 過期的受管理伺服器	• 異常系統事件 • 使用授權到期 • URL 過濾 • 週邊設備存取控管 • Exchange 伺服器關機 • Active Directory 同步問題 • Worry-Free Business Security Standard 和 Advanced 伺服器關機
Worry-Free Business Security Services	• Agent 異常 • 疫情爆發防範 • 防毒 • 間諜程式防護 • 網頁信譽評等服務 • 行為監控 • 網路病毒	• 過期的受管理伺服器 • 異常系統事件 • 使用授權到期 • URL 過濾 • Exchange 伺服器關機 • Active Directory 同步問題

第 11 章

ConnectWise Manage 支援

本節介紹如何將 Remote Manager 與 ConnectWise Manage 整合，以及趨勢科技產品和服務所支援的事件通知。

包含下列主題：

整合 ConnectWise Manage™

ConnectWise Manage 是一項專業服務自動化 (PSA) 及遠端監控和管理 (RMM) 解決方案，為受管理服務供應商和經銷商提供即時資訊中心和報告、事件管理、服務資產和設定管理以及自動帳單服務。

Remote Manager 可以將事件資訊以電子郵件的形式傳送至 ConnectWise Manage，電子郵件會轉換為 ConnectWise Manage 票證。若要如此，您必須將通知收件者新增至 Remote Manager Web 主控台，並將多個欄位新增至 ConnectWise Manage 票證系統。

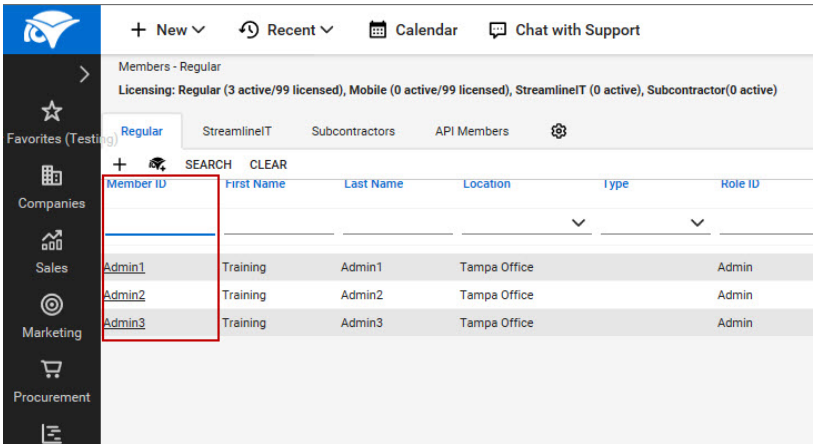
若要成功整合 Remote Manager、開始接收通知並在 ConnectWise Manage 中產生帳號票證，請您務必完成所需的整合步驟。

整合 ConnectWise Manage 與 Remote Manager 客戶

在 ConnectWise Manage 中針對 Trend Micro Remote Manager 客戶開始設定帳單期間、監控垃圾郵件統計資料或接收通知之前，您必須先辨識 ConnectWise Manage 客戶並與對應的 Trend Micro Remote Manager 客戶連線。

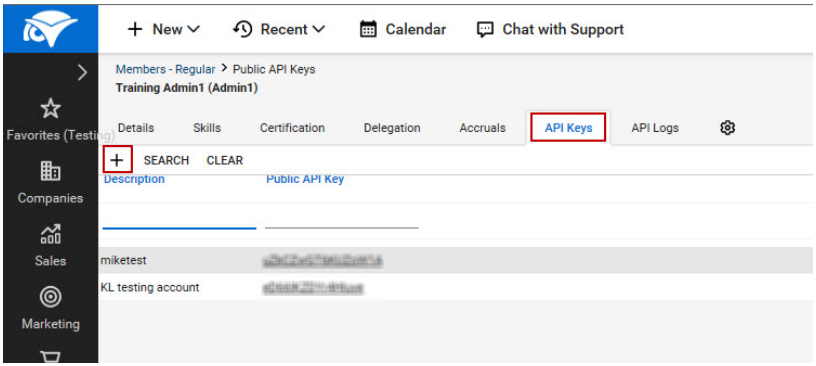
程序

1. 使用 ConnectWise Manage 主控台取得 ConnectWise Manage 與 Trend Micro Remote Manager 之間通訊所需的 API 金鑰。
   a. 開啟 ConnectWise Manage 主控台。
   b. 移至「System > Members」。



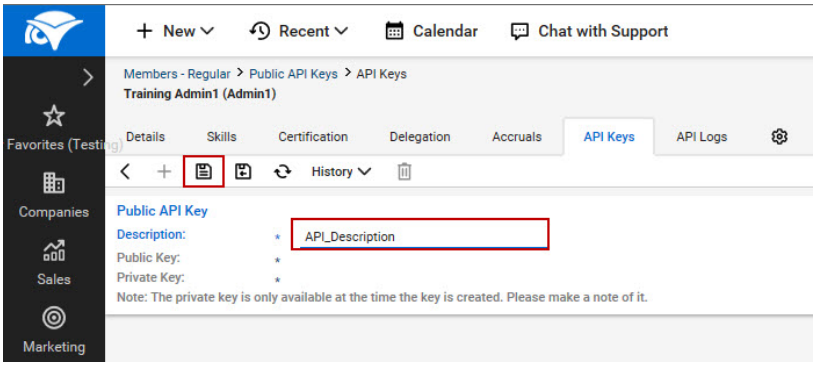
c. 按一下負責 API 金鑰的 Member ID。

d. 按一下「API Keys」標籤。



e. 按一下「New Item (➕)。

f. 輸入 API 金鑰的「Description」。



g. 按一下「Save」。

重要

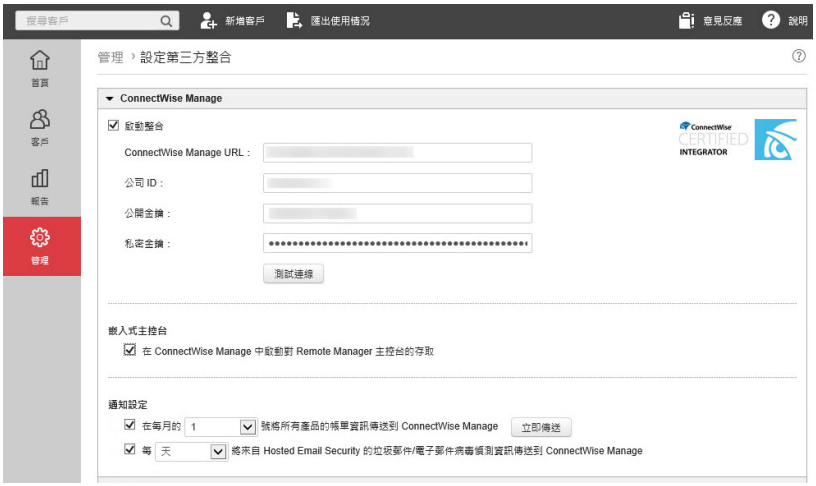
ConnectWise Manage 會為新項目指派「Public Key」和「Private Key」。「Private Key」只會顯示一次。務必謹慎複製「Private Key」。若遺失金鑰，就無法再次復原「Private Key」，而且必須建立新的項目並重新設定 Remote Manager 伺服器。

2. 在 Trend Micro Remote Manager 主控台上設定全域 ConnectWise Manage 整合設定。

   a. 開啟 Trend Micro Remote Manager 主控台。

   b. 移至「管理 > 設定第三方整合」。

隨即顯示「設定第三方整合」畫面。



c. 在「ConnectWise Manage」區段中，選取「啟用整合」，以允許 ConnectWise Manage 從 Trend Micro Remote Manager 接收通知。

- ConnectWise Manage URL：輸入 ConnectWise Manage URL 或 FQDN。

  注意

  依預設，Trend Micro Remote Manager 會自動使用 HTTPS 與 ConnectWise Manage 伺服器進行通訊。如果您公司需要使用 HTTP 通訊，則必須指定 URL，而非 FQDN。

- 公司 ID：輸入您用來登入 ConnectWise Manage 主控台的公司名稱。
- 公開金鑰：指定 ConnectWise Manage 公開金鑰，Trend Micro Remote Manager 會用它加密對 ConnectWise Manage 的通訊。
- 私密金鑰：指定 ConnectWise Manage 私密金鑰，用於解密來自 Trend Micro Remote Manager 的通訊

d. 按一下「測試連線」，驗證與 ConnectWise Manage 之間的連線。

> **注意**
>
> 如果您未按一下「測試連線」，Trend Micro Remote Manager 會在您按一下「儲存」按鈕時，自動驗證與 ConnectWise Manage 之間的連線。

e. 按一下「儲存」。

3. 辨識個別 Trend Micro Remote Manager 客戶，並於 Trend Micro Remote Manager 主控台上與 ConnectWise Manage 客戶建立關聯。

   a. 開啟 Trend Micro Remote Manager 主控台。

   b. 移至「客戶 > [客戶]」。

   c. 若要為此客戶整合 ConnectWise Manage 設定，請按一下「ConnectWise Manage」標籤。

   d. 選取「啟用整合」。

   e. 指定客戶的「ConnectWise 公司 ID」。

      存取 ConnectWise Manage 主控台，可找出特定客戶的公司 ID。

      > **秘訣**
      >
      > 按一下「確認」，確認 ConnectWise Manage 中有此公司 ID。

   f. 按一下「儲存」。

   g. 針對每個 ConnectWise Manage 客戶重複上述步驟。

您可以使用 Trend Micro Remote Manager 和 ConnectWise Manage 主控台執行以下作業：

- 監控 Hosted Email Security 垃圾郵件統計資訊 第 11-9 頁
- 管理客戶帳單 第 11-15 頁
- 監控客戶通知 第 11-25 頁

新增趨勢科技產品至 ConnectWise Manage

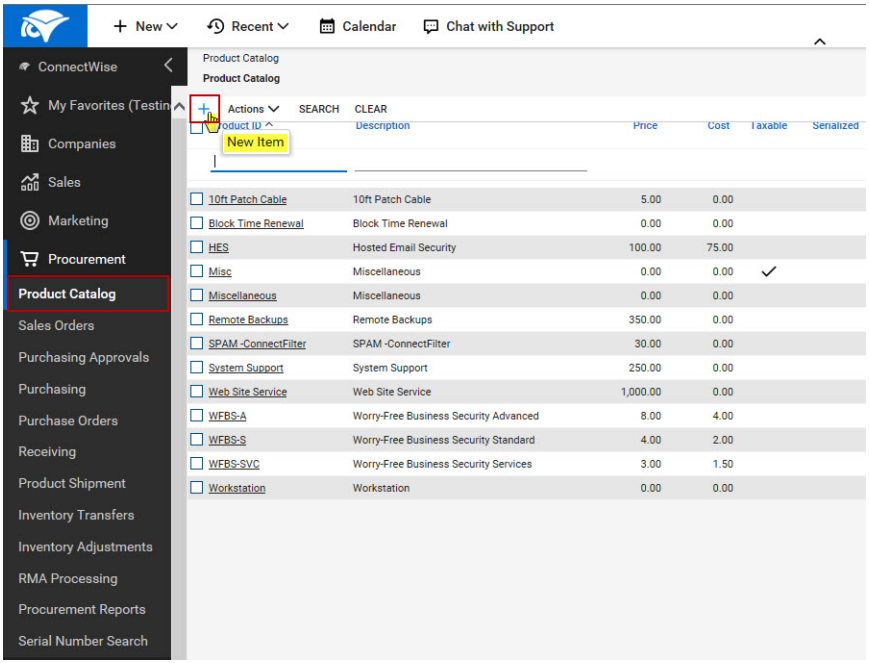
為便於傳送帳單，趨勢科技將以下 Trend Micro Remote Manager 產品/服務與 ConnectWise Manage 整合：

- Worry-Free Business Security Standard
- Worry-Free Business Security Advanced
- Worry-Free Business Security Services
- Hosted Email Security

程序

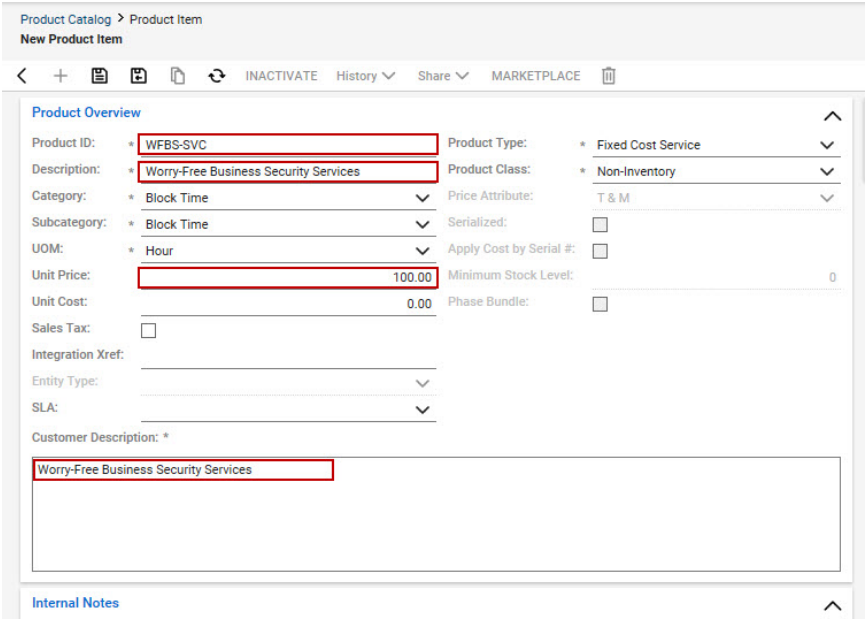
1. 從 ConnectWise Manage 主控台，移至「Procurement > Product Catalog」。

   隨即顯示「Product Catalog」畫面。



2. 按一下「New Item」(➕)，以新增產品。

   隨即顯示「New Product Item」畫面。



3. 在「Product ID」欄位中，輸入必要的 Trend Micro Remote Manager 受管理產品/服務產品 ID。

   表 11-1. 可與 ConnectWise Manage 整合的趨勢科技產品 ID

產品/服務	產品 ID
Worry-Free Business Security Standard	WFBS-S
Worry-Free Business Security Advanced	WFBS-A
Worry-Free Business Security Services	WFBS-SVC
Hosted Email Security	HES

4. 指定下列資訊：

- 說明
- Unit Price
- Customer Description

5. 按一下「Save」。

   ConnectWise Manage 會將新產品新增至「Product Catalog」。

監控 Hosted Email Security 垃圾郵件統計資訊

您必須先整合 ConnectWise Manage 客戶與 Trend Micro Remote Manager，才能開始監控 Hosted Email Security 客戶的垃圾郵件統計資訊。

如需詳細資訊，請參閱整合 ConnectWise Manage 與 Remote Manager 客戶 第 11-2 頁。

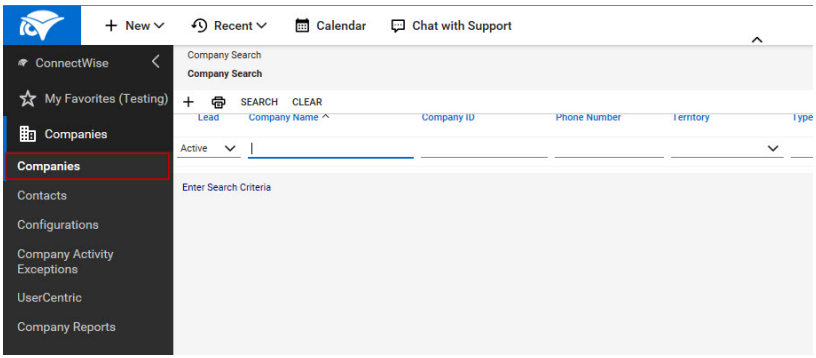
整合兩種產品並建立客戶帳號的關聯後，就可以設定客戶的垃圾郵件統計資訊設定。

程序

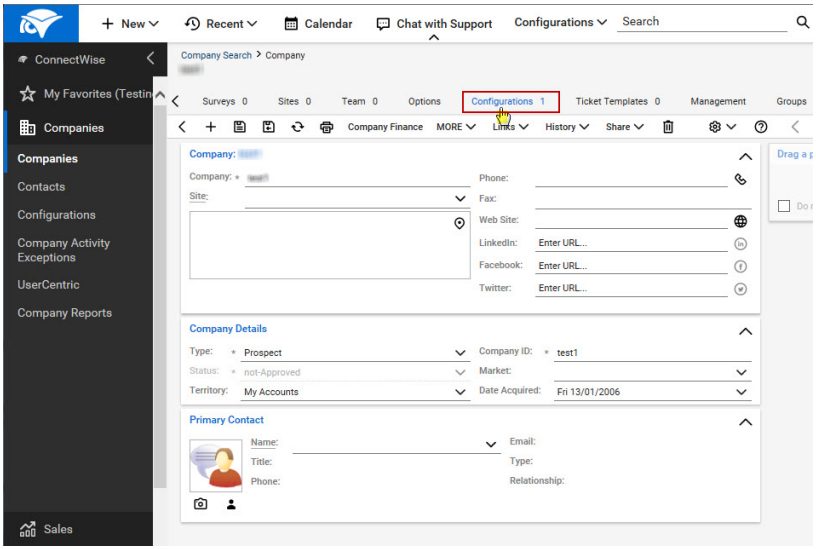
1. 設定 ConnectWise Manage 客戶監控垃圾郵件統計資訊。

   a. 從 ConnectWise Manage 主控台，移至「Companies > Companies」。

      隨即顯示「Company Search」畫面。



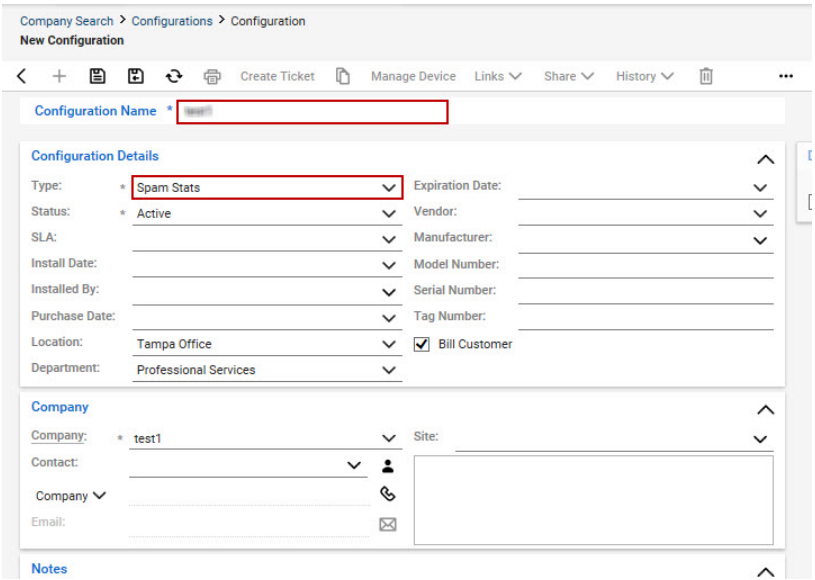
b. 在「Company Name」欄位中輸入公司名稱，然後按一下「Search」。隨即顯示「{公司}」畫面。



c. 按一下「Configurations」標籤。

d. 按一下「New Item」(➕)，以建立新的設定。

隨即顯示「New Configuration」畫面。



e. 在「Configuration Name」欄位中輸入公司 ID。

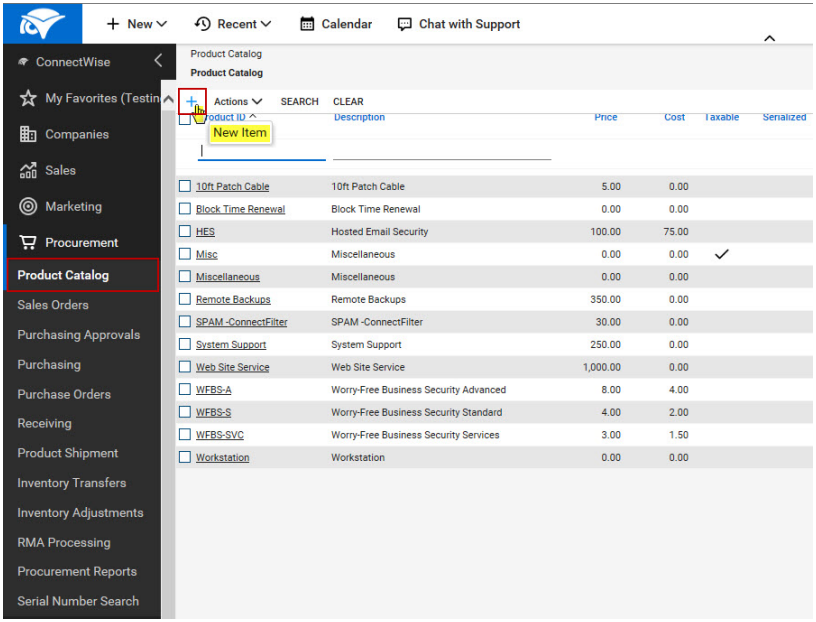
f. 從「Type」下拉式清單中選取「Spam Stats」。

g. 按一下「Save」。

2. 確認您已將 Hosted Email Security 產品新增至 ConnectWise Manage 主控台。

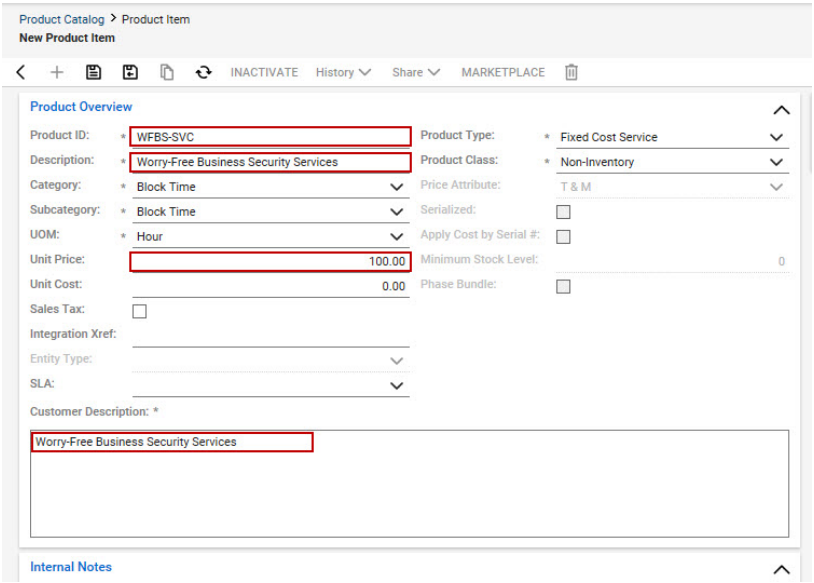
   a. 從 ConnectWise Manage 主控台，移至「Procurement > Product Catalog」。

隨即顯示「Product Catalog」畫面。



b. 按一下「New Item」(➕)，以新增產品。

隨即顯示「New Product Item」畫面。



c. 在「Product ID」欄位中，輸入必要的 Trend Micro Remote Manager 受管理產品/服務產品 ID。

   Hosted Email Security 的產品 ID 為 `HES`。

d. 指定下列資訊：

   - Description
   - Unit Price
   - Customer Description

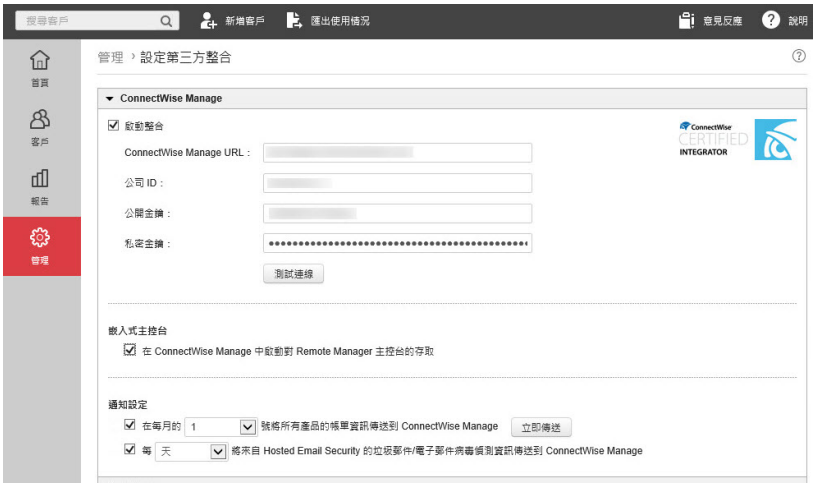
e. 按一下「Save」。

3. 在 Trend Micro Remote Manager 主控台上設定全域第三方整合設定，以將 Hosted Email Security 偵測情況傳送給 ConnectWise Manage 客戶。

   a. 開啟 Trend Micro Remote Manager 主控台。

b. 移至「管理 > 設定第三方整合」。

隨即顯示「設定第三方整合」畫面。



c. 在「通知設定」區段中：

- 啟用「每 ___將來自 Hosted Email Security 的垃圾郵件/電子郵件病毒偵測資訊傳送到 ConnectWise Manage」，對 Hosted Email Security 客戶執行自動安全報告。

d. 按一下「儲存」。

4. 在 Trend Micro Remote Manager 主控台上設定客戶特定的 ConnectWise Manage 設定，以將 Hosted Email Security 偵測情況傳送給特定 ConnectWise Manage 客戶。

a. 開啟 Trend Micro Remote Manager 主控台。

b. 若要讓 Remote Manager 向 ConnectWise Manage 傳送通知，請移至「客戶 > {公司}」。

c. 按一下「通知」標籤。

隨即顯示以下畫面：

d. 在「第三方通知」區段中，選取「ConnectWise Manage」。

e. 按一下「儲存」。

f. 按一下「ConnectWise Manage」標籤。

g. 在「通知設定」區段中：

- 選取「使用管理 > 設定第三方整合 > ConnectWise Manage 設定中的全域設定」，以套用全域整合設定。
- 選取「使用自訂設定」，以設定用於帳單和管理摘要的客戶特定通知。
  - 啟用「每 ___將來自 Hosted Email Security 的垃圾郵件/電子郵件病毒偵測資訊傳送到 ConnectWise Manage」，對 Hosted Email Security 客戶執行自動安全報告。

h. 按一下「儲存」。

管理客戶帳單

您必須先整合 ConnectWise Manage 客戶與 Trend Micro Remote Manager，才能開始管理客戶帳單。

如需詳細資訊，請參閱整合 ConnectWise Manage 與 Remote Manager 客戶 第 11-2 頁。

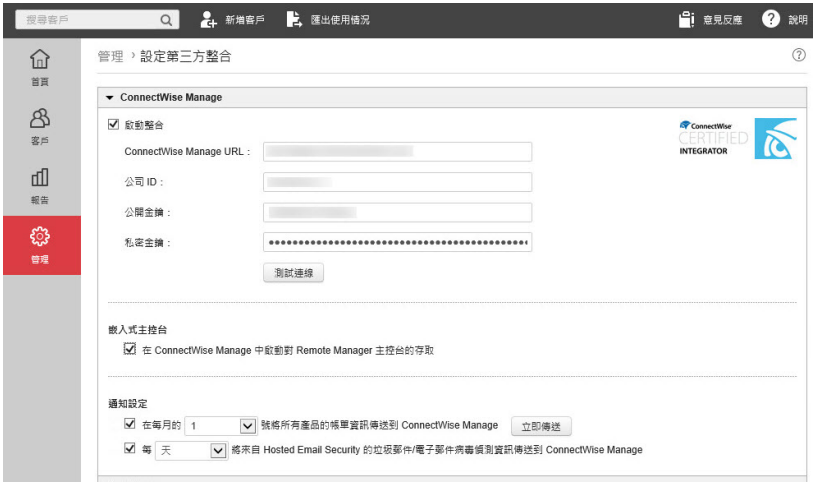
整合兩種產品並建立客戶帳號的關聯後，就可以設定客戶的帳單設定。

程序

1. 在 Trend Micro Remote Manager 主控台上設定全域帳單排程。

   a. 移至「管理 > 設定第三方整合」。

      隨即顯示「設定第三方整合」畫面。



   b. 在「通知設定」區段中：

      - 啟用「在每月的 __ 號將所有產品的帳單資訊傳送到 ConnectWise Manage」，針對所有 ConnectWise Manage 客戶的所有趨勢科技產品自動傳送帳單。

      注意

      - 按一下「立即傳送」，立即將目前帳單傳送給 ConnectWise Manage 客戶。
      - 如果您選取了 29、30 或 31，而該月在設定的日期前結束，Remote Manager 會在該月的最後一天傳送帳單資訊。

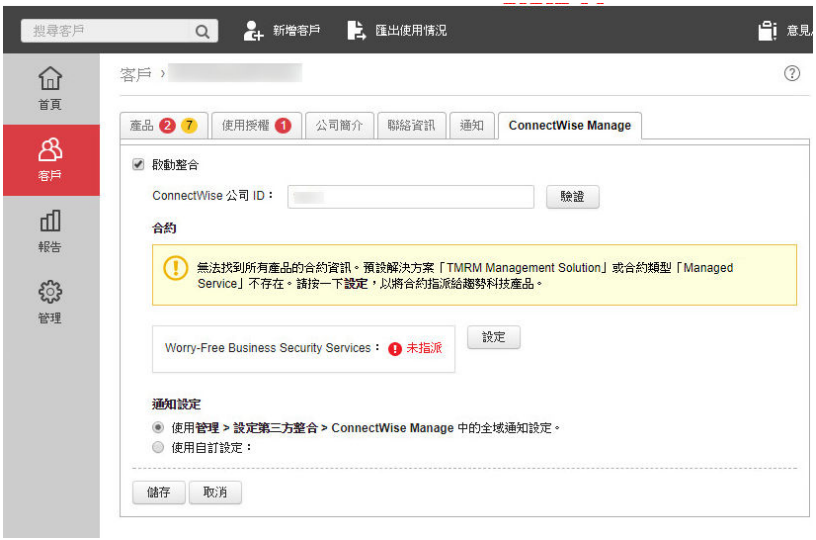
c. 按一下「儲存」。

ConnectWise Manage 現在可以從 Remote Manager 接收通知。

2. 在 Remote Manager 主控台上設定合約，並視需要修改個別 Remote Manager 客戶的帳單排程。

a. 若要讓 Remote Manager 將帳單資訊傳送至 ConnectWise Manage，請移至「客戶 > {公司}」。

b. 若要為此客戶整合 ConnectWise Manage 設定，請按一下「ConnectWise Manage」標籤。



c. 在「合約」區段中，您可以將 ConnectWise Manage 合約指派給趨勢科技產品。

注意

將合約指派給趨勢科技產品後，即可允許 ConnectWise Manage 為 Trend Micro Remote Manager 客戶提供自動帳單服務。

重要

Trend Micro Remote Manager 只能顯示您在 ConnectWise Manage 中的「Companies > Companies > {公司} > Agreements（標籤）」上設定的合約。

如果您先前已使用「TMRM Management Solution」或「Managed Service」合約類型設定 ConnectWise Manage，則趨勢科技產品名稱旁邊會顯示「預設」。

如需有關 ConnectWise Manage 中管理解決方案帳單設定的詳細資訊，請參閱建立管理解決方案 第 11-18 頁和建立交互參考 第 11-22 頁。

d. 按一下「設定」。

隨即顯示「產品合約」畫面。

e. 針對每個產品，先選取合約類型，再選取合約名稱。

f. 按一下「確定」。

g. 選取以下任一整合設定：

- 選取「使用管理 > 設定第三方整合 > ConnectWise Manage 設定中的全域設定」，以套用全域整合設定。
- 選取「使用自訂設定」，以設定用於帳單和管理摘要的客戶特定通知。

h. 按一下「儲存」。

建立管理解決方案

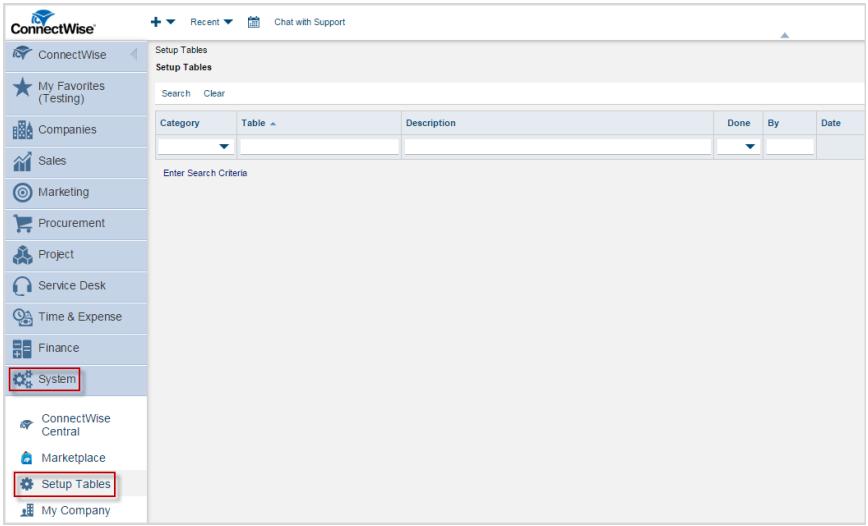
注意

此程序會顯示來自 ConnectWise Manage 2015.1 的畫面。畫面可能會因使用的 ConnectWise Manage 版本而異。

程序

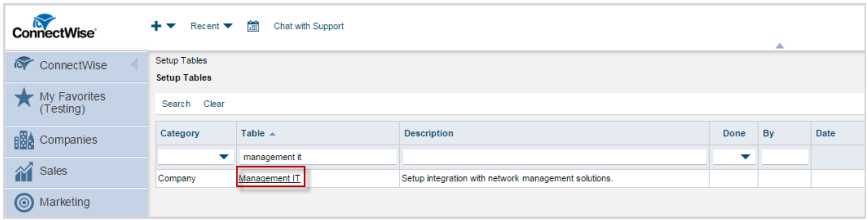
1. 從 ConnectWise Manage 主控台，移至「System > Setup Tables」。

   隨即顯示「Setup Tables」畫面。



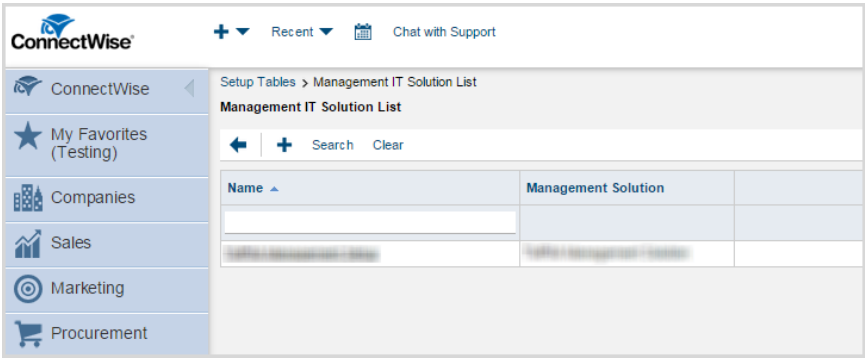
2. 在「Table」欄位中輸入「`management it`」，然後按一下「Search」。

   隨即顯示「Management IT」設定表格。



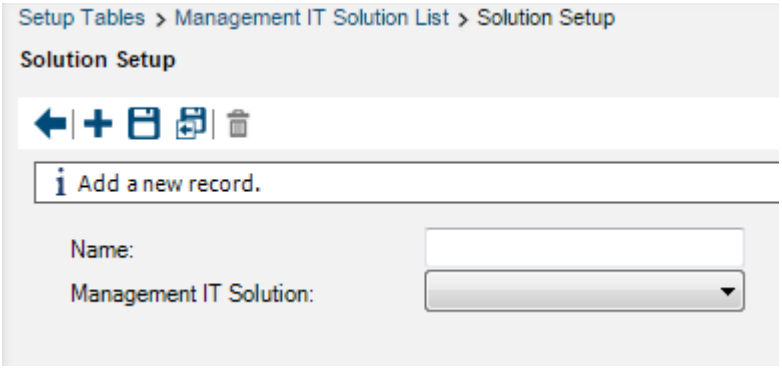
3. 按一下「Management IT」設定表格。

隨即顯示「Management IT Solution List」。



4. 按一下「New Item」(➕)，以建立新管理解決方案。

   隨即顯示「Solution Setup」畫面。



5. 指定下列資訊：

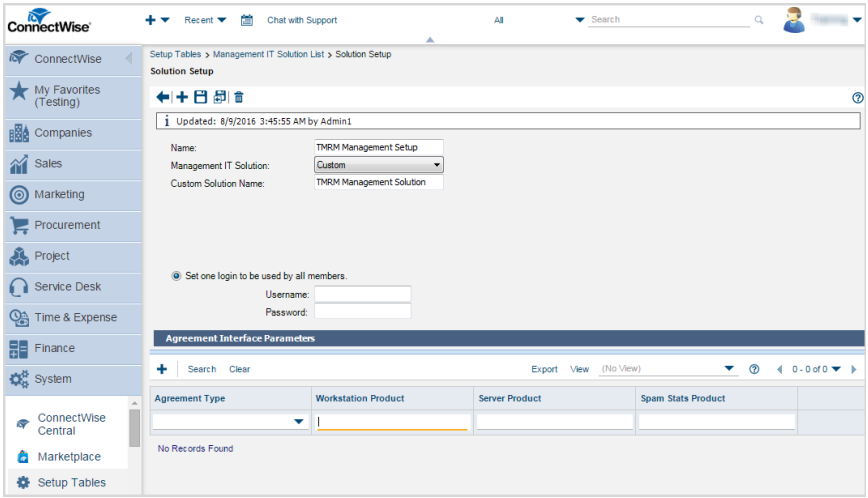
   - 「Name」：輸入 `TMRM Management Setup`。
   - 「Management IT Solution」：選取「Custom」。
   - 「Custom Solution Name」：輸入 `TMRM Management Solution`。

重要

Trend Micro Remote Manager 要求指定的值與提供的範例完全相同。

6. 按一下「Save」。

   ConnectWise Manage 會將該管理解決方案新增至「Management IT Solution List」。



7. 將該管理解決方案與趨勢科技客戶關聯。

   a. 移至趨勢科技客戶的「Company」畫面。

   b. 按一下「Management」標籤。

   c. 在「Management Solutions」旁邊，按一下「New Item」(➕)。

   d. 從「Solution」下拉式清單中，選取「TMRM Management Solution/TMRM Management Setup」。

   e. 指定「Managed ID」。

   f. 按一下「Save」。

      該管理解決方案已可供使用。

8. 對於使用 ConnectWise 管理解決方案的客戶： 建立交互參考 第 11-22 頁

建立交互參考

建立交互參考，以將 Remote Manager 產品/服務與 ConnectWise Manage 關聯。

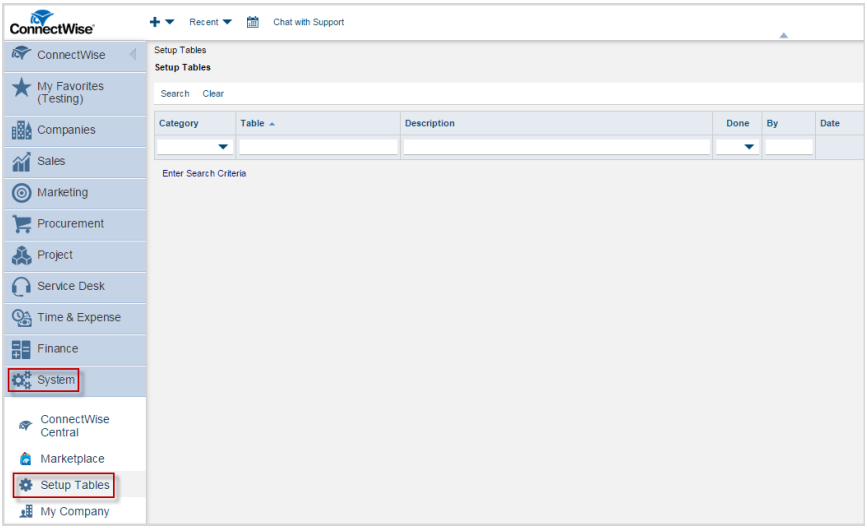
注意

此程序會顯示來自 ConnectWise Manage 2015.1 的畫面。畫面可能會因使用的 ConnectWise Manage 版本而異。

程序

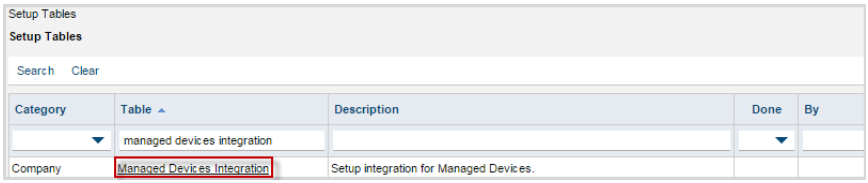
1. 從 ConnectWise Manage 主控台，移至「System > Setup Tables」。

   隨即顯示「Setup Tables」畫面。



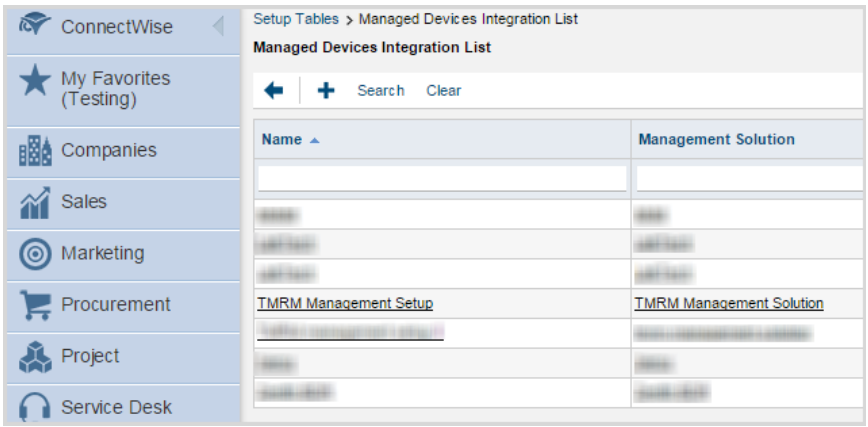
2. 在「Table」欄位中輸入「`managed devices integration`」，然後按一下「Search」。

隨即顯示「Managed Devices Integration」設定表格。



3. 按一下「Managed Devices Integration」設定表格。

   隨即顯示「Managed Devices Integration List」。

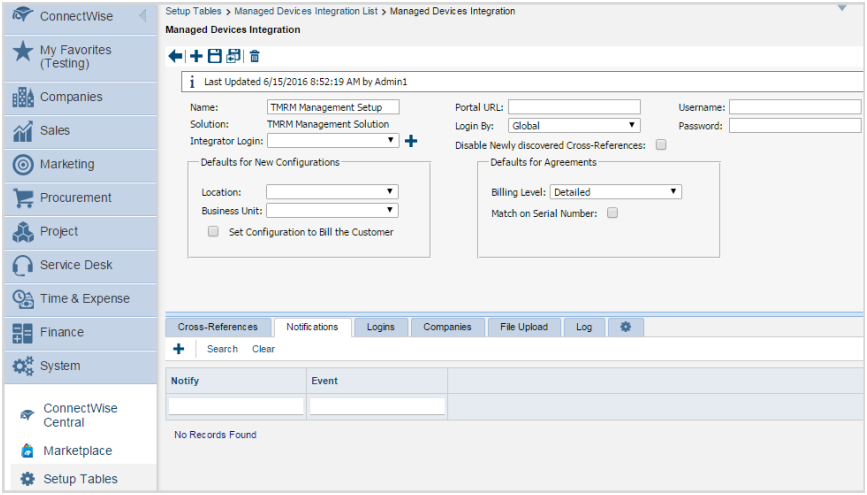


4. 按一下「Management Solution」欄中的「TMRM Management Solution」。

注意

如需有關建立管理解決方案的詳細資訊，請參閱建立管理解決方案 第 11-18 頁。

隨即顯示「Managed Devices Integration」畫面。



5. 按一下「Cross-References」標籤。
6. 按一下「New Item」(➕)，以建立產品。
7. 為您的每個 Remote Manager 受管理產品/服務指定所需的設定。

產品/服務	設定
Worry-Free Business Security Standard	• 「Type」：`REG_SZ` • 「Level」：`Standard` • 「Product」：`WFBS-S` • 「Configuration Type」：`Spam Stats`
Worry-Free Business Security Advanced	• 「Type」：`T-WFBS-A` • 「Level」：`Advanced` • 「Product」：`WFBS-A` • 「Configuration Type」：`Spam Stats`

產品/服務	設定
Worry-Free Business Security Services	• 「Type」：`T-WFBSS` • 「Level」：`Standard` • 「Product」：`WFBSS` • 「Configuration Type」：`Spam Stats`
Hosted Email Security	• 「Type」：`T-HES` • 「Level」：`Standard` • 「Product」：`HES` • 「Configuration Type」：`Spam Stats`

8. 按一下「Save」。

   ConnectWise Manage 會將該產品/服務新增至「Cross-References」。

監控客戶通知

您必須先整合 ConnectWise Manage 客戶與 Trend Micro Remote Manager，才能開始從 Trend Micro Remote Manager 接收客戶通知。

如需詳細資訊，請參閱整合 ConnectWise Manage 與 Remote Manager 客戶 第 11-2 頁。

整合兩種產品並建立客戶帳號的關聯後，就可以設定開始接收客戶通知。

程序

1. 在 Trend Micro Remote Manager 主控台上設定個別 Trend Micro Remote Manager 客戶的通知設定。

   a. 若要讓 Remote Manager 向 ConnectWise Manage 傳送通知，請移至「客戶 > {公司}」。

   b. 按一下「通知」標籤。

隨即顯示以下畫面：

c. 在「第三方通知」區段中，選取「ConnectWise Manage」。

d. 選取應傳送至 ConnectWise Manage 的產品通知事件。

- 使用全域通知設定：選取此項以使用「管理 > 設定通知」畫面中的設定。
- 使用自訂通知事件設定：選取此項，並選擇 Trend Micro Remote Manager 針對此客戶傳送至 ConnectWise Manage 系統的通知事件。

如需詳細資訊，請參閱：

- 使用授權通知 第 17-10 頁
- Worry-Free Business Security Services 通知 第 17-10 頁
- Cloud App Security 通知 第 17-14 頁
- Cloud Edge 通知 第 17-15 頁

e. 按一下「儲存」。

2. 在 ConnectWise Manage 主控台上監控客戶通知。

a. 從 ConnectWise Manage 主控台，移至「Service Desk > Service Board」。

重要

如果您要從舊版 ConnectWise Manage 移轉並使用「TMRM Event Notifications」服務面板，則必須設定服務面板的預設服務團隊，才能收到通知。

第 12 章

ConnectWise Automate 支援

本節介紹如何將 Remote Manager 與 ConnectWise Automate 整合，以及趨勢科技產品和服務所支援的事件通知。

包含下列主題：

整合 ConnectWise Automate™

以下主題包含關於 ConnectWise Automate 與 Remote Manager 整合的資訊：

安裝 Trend Micro Worry-Free Services Plug-in for ConnectWise Automate

此嵌入程式可讓 Remote Manager 與 ConnectWise Automate 同步 Worry-Free Business Security Services 客戶和偵測資料。

秘訣

您可以從 ConnectWise Automate Solution Center 下載 Trend Micro Worry-Free Services Plug-in for ConnectWise Automate。

重要

- 使用 Customer Licensing Portal 帳號的客戶不支援 Trend Micro Worry-Free Services Plug-in for ConnectWise Automate。
- Worry-Free Services Plug-in for Automate 需要最新版 Worry-Free Business Security Services。將您的所有 Security Agent 更新至最新版本，以確保完全支援所有新功能。

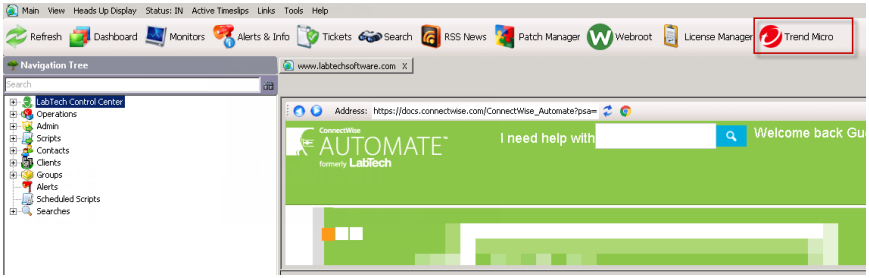
注意

此程序會顯示來自 ConnectWise Automate 11 的畫面。畫面可能會因使用的 ConnectWise Automate 版本而異。

程序

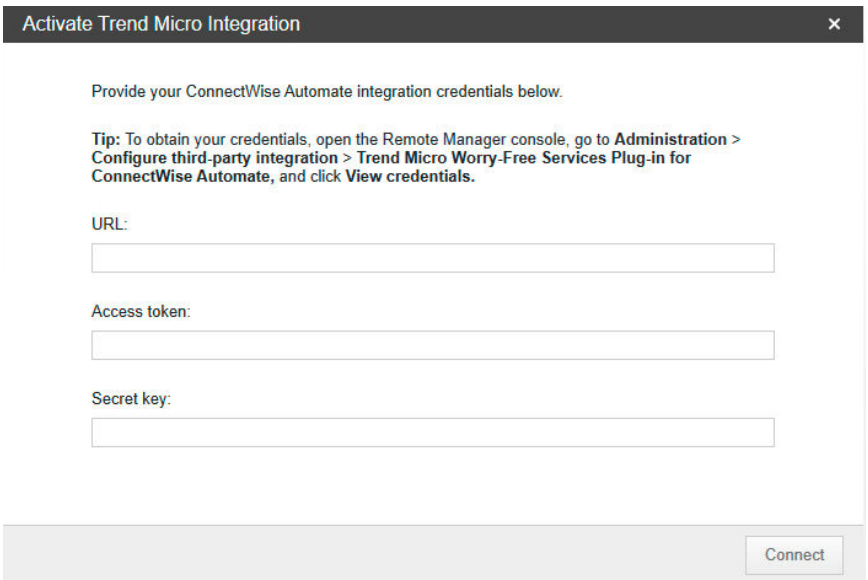
1. 從 Automate Solution Center 安裝 Trend Micro Worry-Free Services Plug-in for ConnectWise Automate。
2. 返回「Automate Control Center」畫面。

「Trend Micro」圖示會新增至工具列。



3. 按一下工具列中的「Trend Micro」按鈕。

   隨即顯示「Activate Trend Micro Integration」畫面。



4. 提供 Remote Manager 啟用憑證。

   - URL

- Access token
- Secret key

秘訣

若要尋找啟用憑證，請執行以下作業：

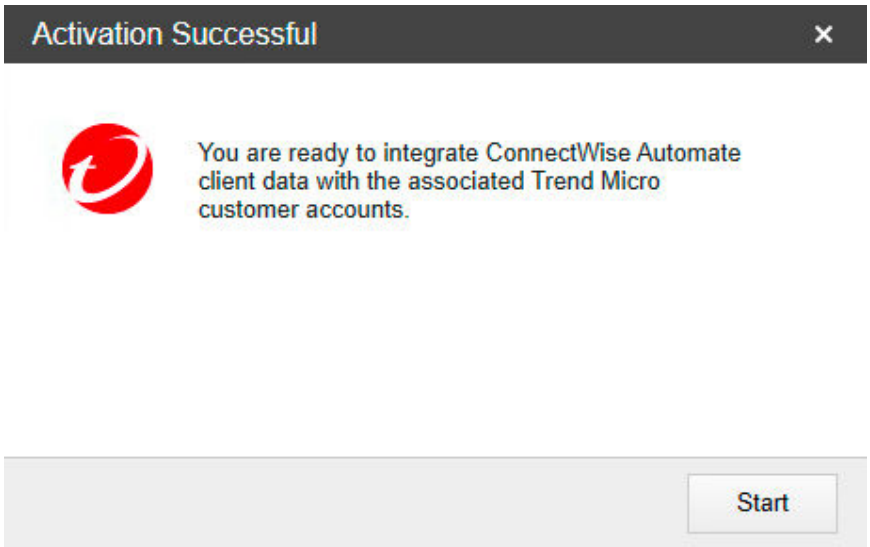
a. 開啟 Remote Manager 主控台，然後移至「管理 > 設定第三方整合 > ConnectWise Automate」。

b. 按一下「檢視憑證」。

5. 按一下「Connect」。

隨即顯示「Activation Successful」畫面。您可以按一下「Start」，開始將 ConnectWise Automate 客戶資料與趨勢科技帳號整合。

如需詳細資訊，請參閱匯入 ConnectWise Automate 客戶 第 12-8 頁。



注意

若要之後整合帳號，請按一下工具列中的「Trend Micro」按鈕，然後移至「Non-Trend Micro Customers」。

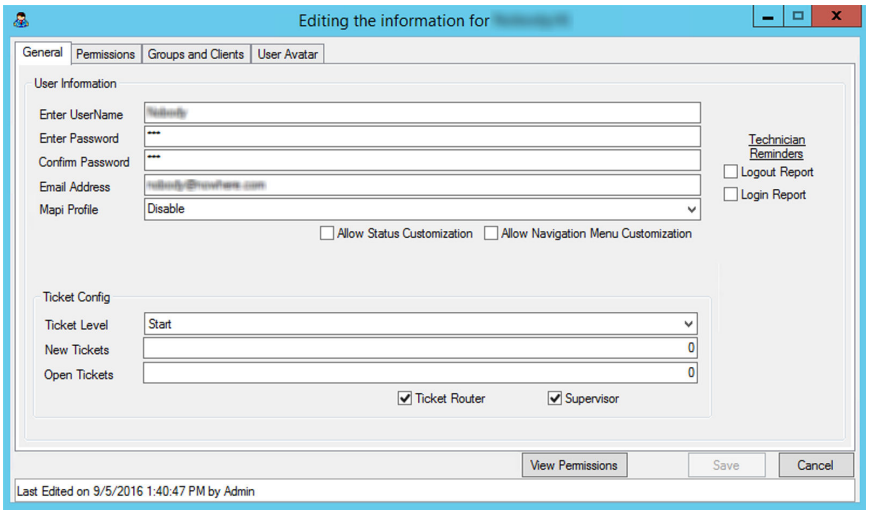
在 ConnectWise Automate 中指派趨勢科技使用者權限

安裝 Trend Micro Worry-Free Business Services Plug-in for Automate 後，您必須指派權限給 ConnectWise Automate 使用者，之後使用者才能存取全部嵌入程式功能。

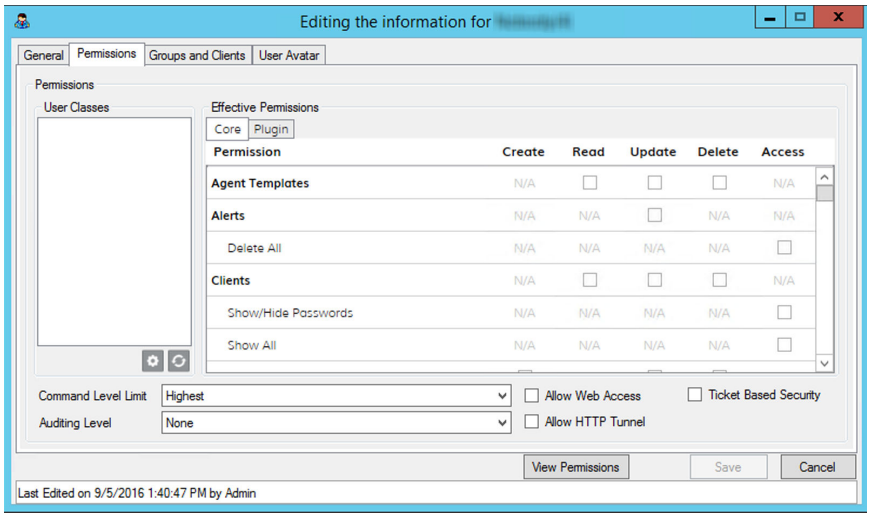
程序

1. 在 Automate Control Center 瀏覽樹狀結構中，移至「Admin > Users」，然後按兩下您要指派權限的使用者。

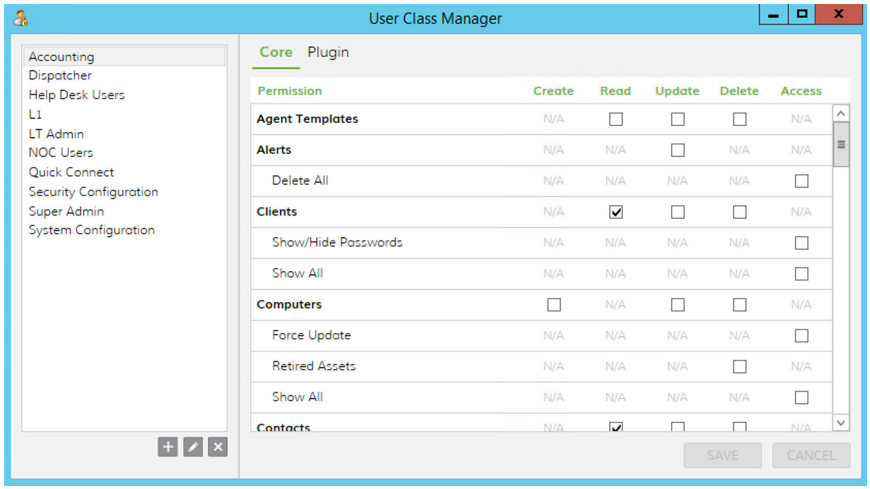
   隨即顯示「Editing the information for {使用者}」畫面。



2. 按一下「Permissions」標籤。



3. 在「User Classes」欄位下，按一下「Open User Class Manager」( ) 圖示。隨即顯示「User Class Manager」畫面。



4. 選取以下核取方塊，以指派適當的權限。

權限	類型
Clients	Read
Contacts	Read
Database	Access
Scripts	Read

5. 按一下「SAVE」。
6. 按一下「Plugin」標籤。
7. 在「Trend Micro Worry-Free Services Plug-in for ConnectWise Automate」旁邊，選取「Access」核取方塊。
8. 按一下「儲存」。

   ConnectWise Automate 使用者現在可以存取 Trend Micro Worry-Free Services Plug-in for ConnectWise Automate 功能。

在 ConnectWise Automate 中管理趨勢科技客戶

啟用 Trend Micro Worry-Free Services Plug-in for Automate 後，您可以開始將 ConnectWise Automate 客戶與趨勢科技帳號關聯，並直接從 ConnectWise Automate 主控台管理客戶關聯。

- 匯入 ConnectWise Automate 客戶：將目前的 ConnectWise Automate 客戶與預先存在的或新的趨勢科技帳號關聯

  如需詳細資訊，請參閱匯入 ConnectWise Automate 客戶 第 12-8 頁。

- 客戶摘要畫面：顯示關聯的趨勢科技客戶和未與趨勢科技帳號關聯的 ConnectWise Automate 客戶

如需詳細資訊，請參閱客戶摘要 第 12-13 頁。

匯入 ConnectWise Automate 客戶

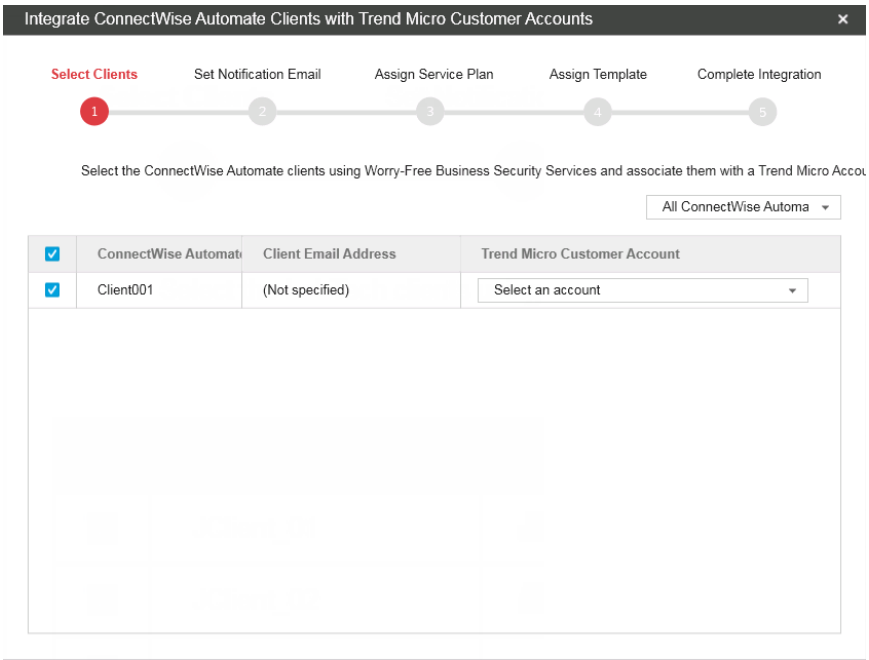
程序

1. 移至「Integrate Automate Clients with Trend Micro Accounts」畫面。
   - 在 Automate 控制中心中：
     a. 按一下工具列中的「Trend Micro」按鈕，然後移至「Non-Trend Micro Customers」。
     b. 選取要匯入的 ConnectWise Automate 客戶旁邊的核取方塊。
     c. 按一下「Import to Trend Micro」。
   - 首次啟用 ConnectWise Automate 嵌入程式後，從「Activation Successful」畫面中按一下「Start」。

重要

您必須在顯示的「Integrate Automate Clients with Trend Micro Accounts: Select Clients」畫面中，選取您想要與趨勢科技帳號關聯之 ConnectWise Automate 客戶旁邊的核取方塊。

隨即顯示「Integrate Automate Clients with Trend Micro Accounts: Select Clients」畫面。



2. 在「Trend Micro Customer Account」下拉式清單中：

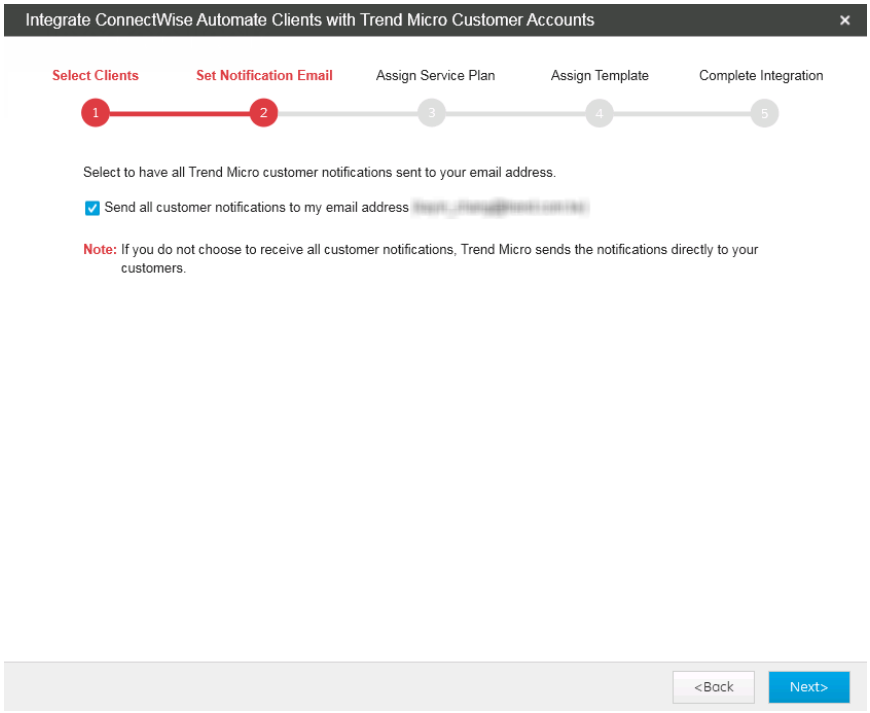
   - 與 Remote Manager 客戶帳號相符的任何 ConnectWise Automate 客戶都會顯示在清單中。如果相符的記錄不正確，請選取其他公司帳號，或建立新的趨勢科技帳號。
   - 選取「+ Create a new Trend Micro Account」，以使用 ConnectWise Automate 客戶名稱做為公司名稱，在 Remote Manager 中自動註冊新的客戶帳號。
   - 從尚未指派給其他帳號的現有 Remote Manager 客戶中進行選取。

注意

如果您已指派所有客戶，則不會在清單中顯示任何客戶資訊。

3. 按一下「Next >」。

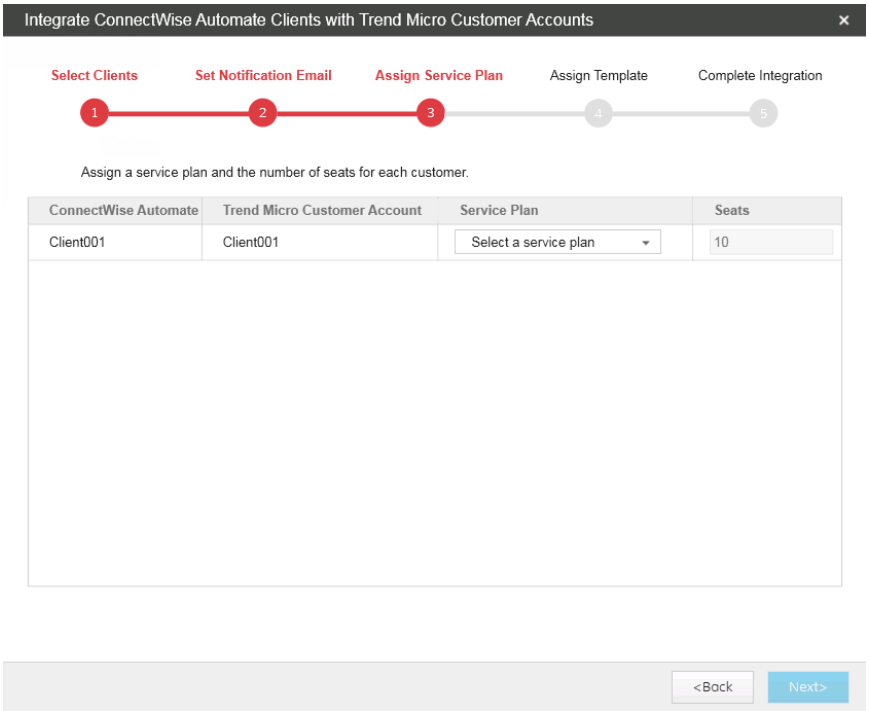
   隨即顯示「Set Notification Email」畫面。



4. 如果您想將所選客戶環境的所有電子郵件通知傳送至您註冊的電子郵件信箱，請選取「Send all customer notifications to my email address」。

5. 按一下「Next >」。

隨即顯示「Assign Service Plan」畫面。



6. 如果您已為任何 ConnectWise Automate 客戶選取「+ Create a new Trend Micro Account」，請為每個客戶指定以下內容：

   a. Service Plan

   b. 「Seats」：依預設，Remote Manager 會佈建比客戶在 ConnectWise Automate 中所註冊端點數多 20% 的授權（每個客戶至少 10 個授權）。

注意

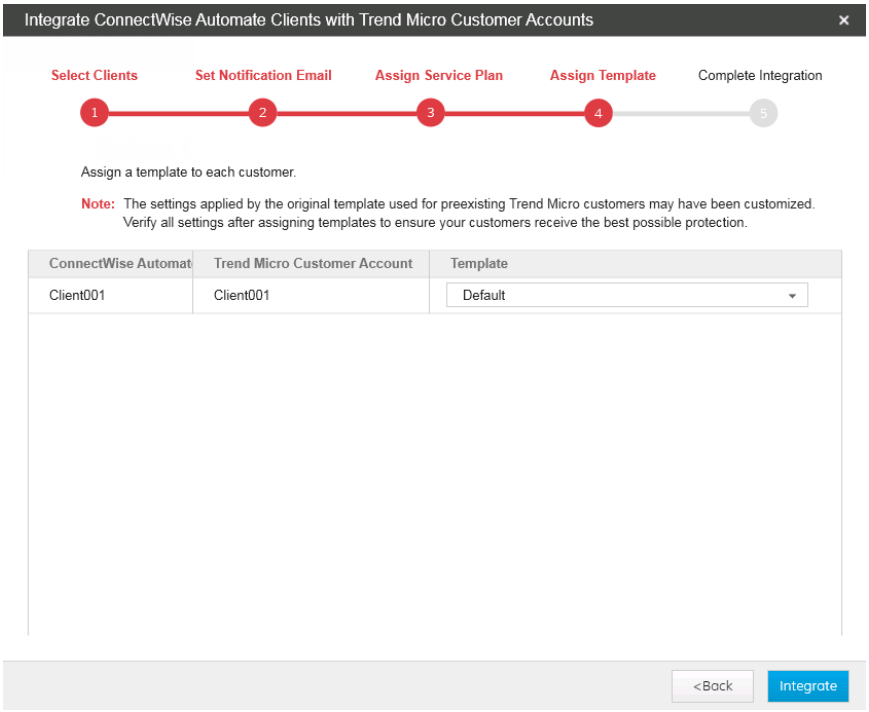
您無法修改預先存在之使用者的設定。

7. 按一下「Next >」，將選取的客戶新增至清單。

重要

您必須在 Licensing Management Platform 中提供足夠的使用授權，以供選取的 ConnectWise Automate 客戶使用。如果提供的使用授權不足，則嵌入程式僅會匯入清單中有使用授權的前幾個客戶。

隨即顯示「Assign Template」畫面。



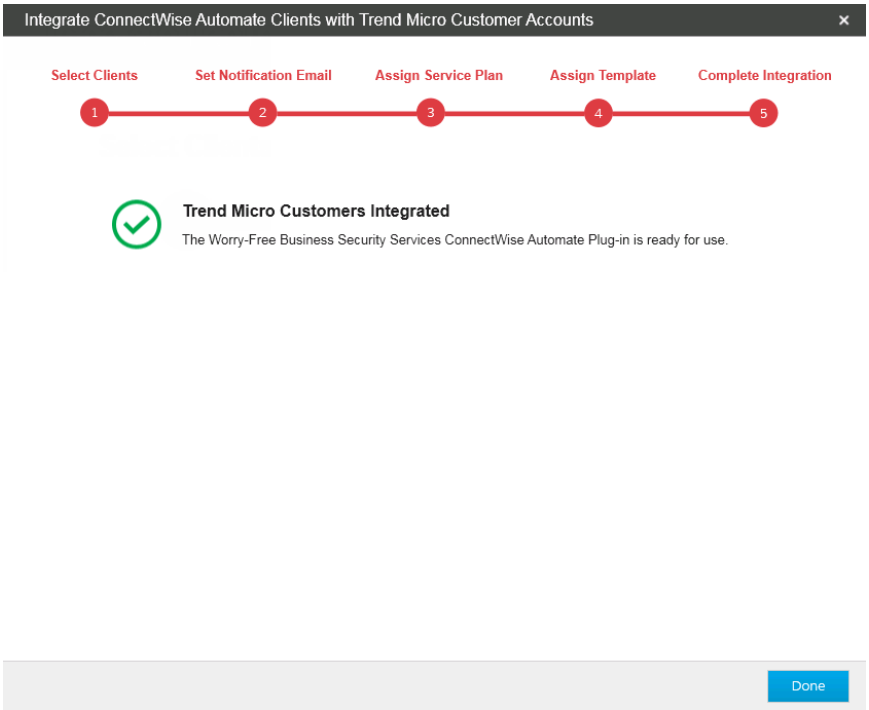
8. 在「Template」下拉式清單中，為每個客戶指派一個範本。

重要

供預先存在的趨勢科技客戶使用的原始範本套用的設定可能已自訂。請在指派範本後確認所有設定，以確保您的客戶獲得最佳防護。

9. 按一下「Integrate」。

   隨即顯示「Complete Integration」畫面。



10. 按一下「Done」，以結束設定精靈。

客戶摘要

按一下工具列中的「Trend Micro」按鈕，或按一下客戶樹狀結構中的「Trend Micro Customers」節點後，會顯示「Trend Micro Customers」畫面。您可以在此畫面中檢視您的所有具有趨勢科技帳號的 ConnectWise Automate 客戶，以及與先前透過趨勢科技帳號設定的 ConnectWise Automate 客戶中斷連線。

下表概述了「Trend Micro Customers」畫面的主要區段。

區段	說明
客戶摘要	提供透過 ConnectWise Automate 管理的所有趨勢科技帳號的總覽 • 「Clients」：按一下此計數可在「Clients」標籤中檢視表格中的所有趨勢科技帳號 • 「Action required」：按一下此計數可在「Clients」標籤中檢視表格中需要注意的所有趨勢科技帳號 • 「Managed machines」：顯示已安裝 Worry-Free Business Services Security Agent 的電腦總數 • 「Unmanaged machines」：顯示已與趨勢科技帳號關聯，但未安裝 Security Agent 的電腦總數

區段	說明
「Clients」標籤	顯示一個表格，概述 ConnectWise Automate 客戶的趨勢科技帳號資訊，以及客戶是否需要立即注意 • 「Automate Client」：按一下客戶名稱，開啟該客戶的 Worry-Free Business Security Services 主控台 • 「Action Required」：按一下紅色的反白顯示儲存格，在「Statistics」標籤上顯示「Action Required Events」Widget • 「Disconnect Client from Trend Micro Account」：如果 ConnectWise Automate 客戶不再是趨勢科技客戶，請選取表格中 ConnectWise Automate 客戶名稱旁邊的核取方塊，然後按一下「Disconnect Client from Trend Micro Account」，以從清單中移除客戶。 **注意** 中斷 ConnectWise Automate 客戶與趨勢科技的連線時，不會從客戶的受管理端點解除安裝 Security Agent。 • 「Automatic Deployment」：啟動後會以每小時一次的頻率，將 Security Agent 自動部署到指派至 ConnectWise Automate 客戶的未受保護端點 **重要** 在啟動自動部署之前，請確保 ConnectWise Automate 客戶擁有足夠的使用授權。雖然在沒有使用授權的情況下，Trend Micro Worry-Free Services Plug-in 仍會部署 Security Agent，但是沒有使用授權的 Security Agent 就無法向 Worry-Free Business Security Services 主控台回報，並且會保留在未受管理的端點清單中。
「Statistics」標籤	顯示一個資訊中心，其中包含多個 Widget，提供透過 ConnectWise Automate 管理的所有趨勢科技帳號的總覽 可用的 Widget： • 「需要採取處理行動的事件」Widget 第 12-21 頁 • 「安全威脅管理」Widget 第 12-22 頁

在 ConnectWise Automate 中管理 Worry-Free Security Agent

Trend Micro Worry-Free Security Services Plug-in for ConnectWise Automate 透過 ConnectWise Automate 主控台，提供對 Security Agent 的部分有限控制。

從 ConnectWise Automate 主控台，您可以執行以下 Worry-Free Business Security Agent 工作：

- 管理趨勢科技 ConnectWise Automate 客戶 第 12-16 頁
- 在 ConnectWise Automate 中使用趨勢科技程式檔 第 12-19 頁

管理趨勢科技 ConnectWise Automate 客戶

客戶資訊畫面提供基本的 ConnectWise Automate 客戶摘要資訊，包括 Worry-Free Business Security Services 的主要客戶聯絡人、電子郵件信箱和目前的使用授權狀態。

重要

Worry-Free Services Plug-in for Automate 需要最新版 Worry-Free Business Security Services。將您的所有 Security Agent 更新至最新版本，以確保完全支援所有新功能。

使用「Endpoints」和「Unmanaged Endpoints」標籤，將命令傳送至 Worry-Free Security Services Security Agent，或將 Agent 部署至端點。

注意

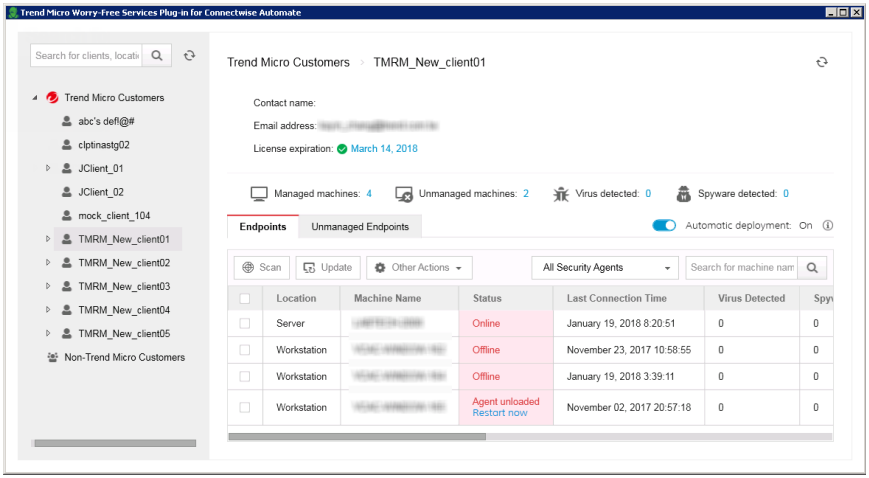
- 您可以選擇在客戶樹狀結構「Trend Micro Customers」節點下的任何層級，檢視特定客戶/端點資訊。
- 常用 Worry-Free Business Security Services Agent 命令也可使用 ConnectWise Automate 程式檔提供。

  如需詳細資訊，請參閱 在 ConnectWise Automate 中使用趨勢科技程式檔 第 12-19 頁

程序

1. 開啟 Automate Control Center，移至「Trend Micro > Trend Micro Customers」，然後在瀏覽樹狀結構中選取客戶。

   所顯示畫面的標題取決於在客戶樹狀結構中選取的客戶資訊層級。下圖顯示「Trend Micro Customers > {客戶}」畫面。



2. 從 Remote Manager 中按一下使用授權到期日，檢視關於可用 Worry-Free Business Security Services 使用授權的詳細資訊。

3. 按一下以下任何計數，檢視特定端點：

   - 「Managed machines」：在「Endpoints」標籤中顯示已安裝 Worry-Free Business Services Security Agent 的電腦清單
   - 「Unmanaged machines」：在「Unmanaged Endpoints」標籤中顯示未安裝 Worry-Free Business Services Security Agent 的電腦清單
   - 「Viruses detected」：在「Endpoints」標籤上顯示具有病毒偵測的 Worry-Free Business Services Security Agent 清單
   - 「Spyware detected」：在「Endpoints」標籤上顯示具有間諜程式偵測的 Worry-Free Business Services Security Agent 清單

秘訣

對於在「Endpoints」標籤上顯示大量 Worry-Free Business Services Security Agent 的客戶，您可以使用端點表格上方下拉式控制中的狀態資訊進一步過濾結果。

4. 啟動「Automatic Deployment」後，會以每小時一次的頻率，將 Security Agent 自動部署到指派至 ConnectWise Automate 客戶的未受保護端點。

重要

在啟動自動部署之前，請確保 ConnectWise Automate 客戶擁有足夠的使用授權。雖然在沒有使用授權的情況下，Trend Micro Worry-Free Services Plug-in 仍會部署 Security Agent，但是沒有使用授權的 Security Agent 就無法向 Worry-Free Business Security Services 主控台回報，並且會保留在未受管理的端點清單中。

5. 在「Endpoints」標籤上，選取您要管理的端點的核取方塊，然後按一下清單上方的按鈕，以傳送必要的命令。

- 「Scan」：觸發選取的端點上的 Security Agent，以在下次伺服器同步期間執行手動掃瞄
- 「Update」：觸發 Security Agent，以檢查在下次伺服器同步期間是否有元件更新
- 「Other Actions」：顯示以下命令：
  - 「Unload Agent」：在下次伺服器同步期間的指定時間段內，從選取的端點上傳 Security Agent
  - 「Remove Agent」：在下次伺服器同步期間，從選取的端點解除安裝 Security Agent

    警告!

    移除 Security Agent 可能會讓端點容易受到安全威脅攻擊。

注意

您必須確認您想要將命令傳送至選取的 Security Agent。

在 Remote Manager 下次與 Worry-Free Business Security Services 同步時，端點會收到此命令。預設同步時間是五分鐘。

6. 在「Unmanaged Endpoints」標籤上：

   - 選取您想要以 CSV 格式另存為清單的未受管理的端點，然後按一下「Export」。
   - 選取您想要在其上安裝 Security Agent 的未受管理的端點，然後按一下「Deploy Agent」。

     注意

     您必須確認您想要將命令傳送至選取的端點。

     在 Remote Manager 下次與 Worry-Free Business Security Services 同步時，端點會收到此命令。預設同步時間是五分鐘。

在 ConnectWise Automate 中使用趨勢科技程式檔

Worry-Free Business Security Service ConnectWise Automate 嵌入程式提供以下程式檔，可透過「Scripts > Anti-Virus > Trend Micro」右鍵功能表存取。

重要

您必須先指派存取每個程式檔所需的特定 ConnectWise Automate 使用者類別權限，然後才會顯示右鍵程式檔項目。

您只能存取與趨勢科技帳號關聯的 ConnectWise Automate 客戶的右鍵程式檔功能表。若要將 ConnectWise Automate 客戶與趨勢科技帳號關聯，請參閱 匯入 ConnectWise Automate 客戶 第 12-8 頁

- 「Deploy Security Agent」：將 Security Agent 部署至選取的端點

- 「Remove Security Agent」：從選取的端點解除安裝 Security Agent

> **警告!**
> 移除 Security Agent 可能會讓端點容易受到安全威脅攻擊。

- 「Restart Security Agent」：在選取的端點上重新啟用 Security Agent
- 「Scan Now」：觸發所選端點上的 Security Agent，以執行手動掃瞄
- 「Unload Security Agent」：從選取的端點卸載 Security Agent
- 「Update Now」：觸發 Security Agent 以檢查是否有元件更新

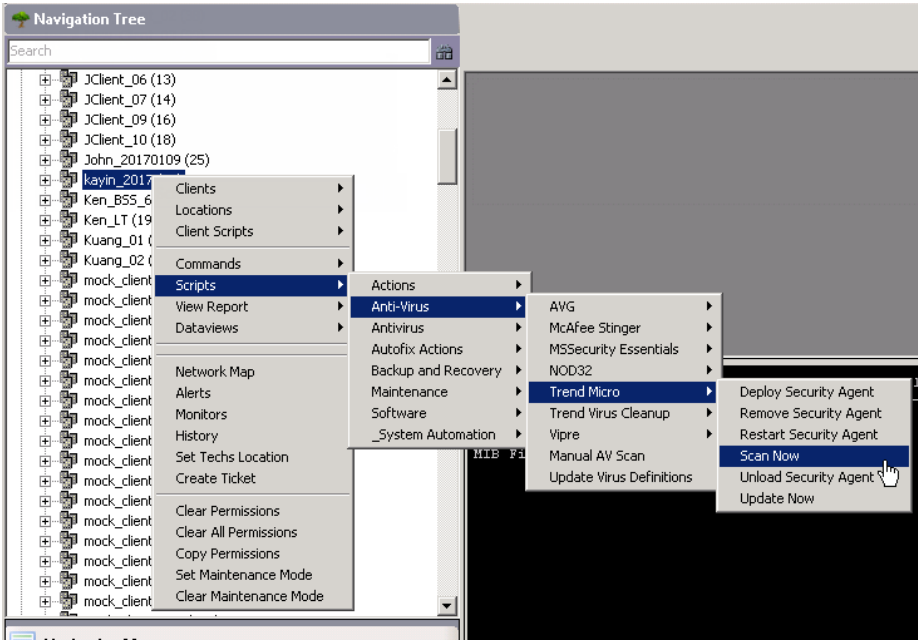


圖 12-1. 趨勢科技 ConnectWise Automate 程式檔

注意

- 在 Remote Manager 下次與 Worry-Free Business Security Services 同步時，端點會收到此命令。預設同步時間是五分鐘。
- 這些命令僅在有效的端點上執行。例如，如果選取的端點未安裝 Security Agent，則無法執行「Scan Now」功能。

監控 Worry-Free Business Security Services Agent

「統計資料」提供一種簡單的方式來檢視需要進一步採取處理行動，或已使用「需要採取處理行動事件」和「安全威脅管理」Widget 偵測到安全事件的所有趨勢科技客戶。

「需要採取處理行動的事件」Widget

「需要採取處理行動的事件」Widget 列出了有端點需要注意的客戶。

事件	說明
中毒處理行動不成功	按一下「出現次數」，移至 Worry-Free Business Security Services 主控台，並檢視客戶端點上的不成功掃瞄結果。
即時掃瞄已關閉	按一下「裝置」，移至 Worry-Free Business Security Services 主控台，並檢視即時掃瞄已關閉的端點。
需要重新啟用	按一下「出現次數」，移至 Worry-Free Business Security Services 主控台，並檢視需要重新啟用以完成間諜程式/可能的資安威脅程式清除的端點。
需要更新	按一下「裝置」，移至 Worry-Free Business Security Services 主控台，並檢視需要更新的端點。

按一下 ConnectWise Automate 客戶名稱，在 Remote Manager 主控台上檢視資訊。

「安全威脅管理」Widget

檢視具有不同安全偵測類型的客戶數目。按一下這些連結可在 Remote Manager 主控台上檢視詳細資訊。

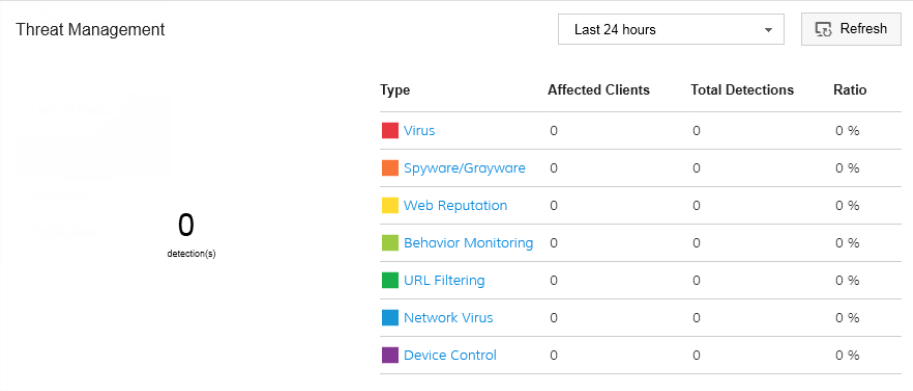


圖 12-2. 「安全威脅管理」Widget

Worry-Free Business Security Services 票證

下表概述了 Worry-Free Security Services 嵌入程式所產生的 ConnectWise Automate 票證。

命令類型	票證主旨	可能原因
Scan	[Action Required] Unsuccessful scan command - <machine_name> of <client_name> - Worry-Free Business Security Services	• 選取的端點未安裝 Security Agent • 選取的端點上安裝的 Security Agent 已損毀 • 選取的端點處於離線狀態，或 Security Agent 已卸載 • Security Agent 正在執行更新 • 發生內部錯誤
Update Agent	[Action Required] Unsuccessful update command - Security Agent for <machine_name> of <client_name> - Worry-Free Business Security Services	• 選取的端點未安裝 Security Agent • 選取的端點上安裝的 Security Agent 已損毀 • 選取的端點處於離線狀態，或 Security Agent 已卸載 • Security Agent 正在執行掃瞄 • 發生內部錯誤
Deploy Agent	[Action Required] Unsuccessful deployment command - Security Agent for <machine_name> of <client_name> - Worry-Free Business Security Services	• 伺服器未完成產生 Security Agent 安裝套件 • 下載 Security Agent 安裝套件時發生錯誤 • Security Agent 目前正在選取的端點上安裝，或已安裝完成
	[Action Required] Exceeded seat allocation for <machine_name> of <client_name> - Worry-Free Business Security Services	• Security Agent 已部署，但仍處於未受管理狀態，因為客戶所剩的使用授權不足

第 13 章

Kaseya 支援

本節介紹如何將 Remote Manager 與 Kaseya 整合，以及趨勢科技產品和服務所支援的事件通知。

包含下列主題：

整合 Kaseya™

以下主題包含關於 Kaseya 與 Remote Manager 整合的資訊：

在 Remote Manager 中設定 Kaseya 通知設定

程序

1. 移至「管理 > 設定第三方整合」。

   隨即顯示「設定第三方整合」畫面。

圖 13-1.「Kaseya」區段

2. 在「Kaseya」區段中，選取「啟用整合」。
3. 輸入「Kaseya 電子郵件信箱」。
4. 按一下「儲存」。

   隨即顯示「成功」通知。

5. 移至「客戶 > {公司} > 通知」。

隨即顯示以下畫面：

6. 如果您想接收通知電子郵件，請選取「帳號管理員」做為收件者。
7. 在「其他收件者」欄位中，輸入需要通知電子郵件的任何其他收件者的電子郵件信箱。
8. 從第三方通知清單中選取「Kaseya」。
9. 選取應傳送至 Kaseya 的產品通知事件。
   - 使用全域通知設定：選取此項以使用「管理 > 設定通知」畫面中的設定。
   - 使用自訂通知事件設定：選取此項，並選擇 Trend Micro Remote Manager 針對此客戶傳送至 Kaseya 系統的通知事件。

   如需詳細資訊，請參閱：
   - 使用授權通知 第 17-10 頁
   - Worry-Free Business Security Services 通知 第 17-10 頁
   - Cloud App Security 通知 第 17-14 頁
   - Cloud Edge 通知 第 17-15 頁
10. 按一下「儲存」。

11. 針對每個客戶重複步驟 6 到 10。

在 Kaseya 中設定通知設定

程序

1. 在 Kaseya 中，將以下欄位新增至票證系統，以顯示 Trend Micro Remote Manager 通知。

   - Worry-Free Business Security

欄位名稱	用途
TM_CreateTime	事件產生時間
TM_ProductName	產品名稱
TM_AgentGUID	Remote Manager Agent GUID
TM_CustomerName	客戶/公司名稱
TM_EventName	事件名稱
TM_ServerName	Worry-Free Business Security 伺服器名稱
TM_MASClientName（選用）	Exchange 伺服器名稱（僅會影響 Exchange 伺服器關機事件）

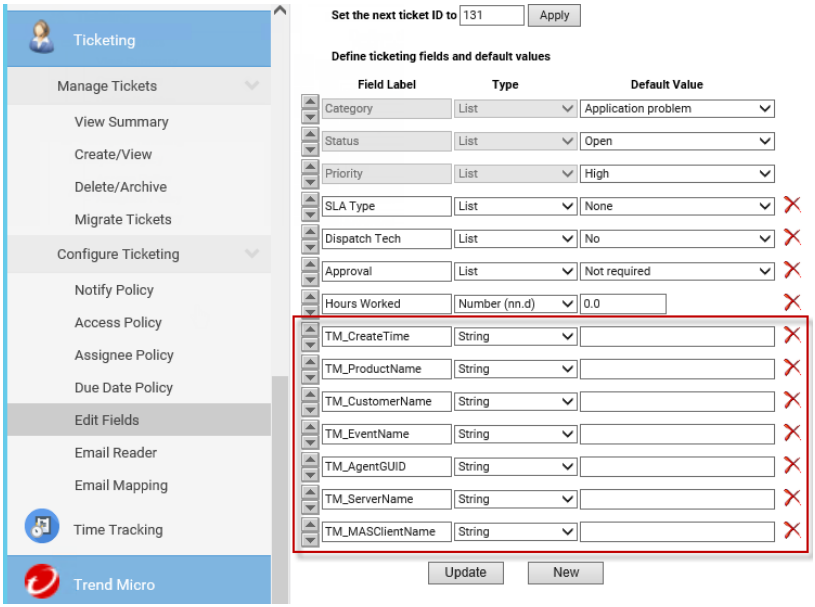


圖 13-2. Kaseya 票證欄位

- Worry-Free Business Security Services

欄位名稱	用途
TM_CreateTime	事件產生時間
TM_ProductName	產品名稱
TM_CustomerName	客戶/公司名稱
TM_EventName	事件名稱

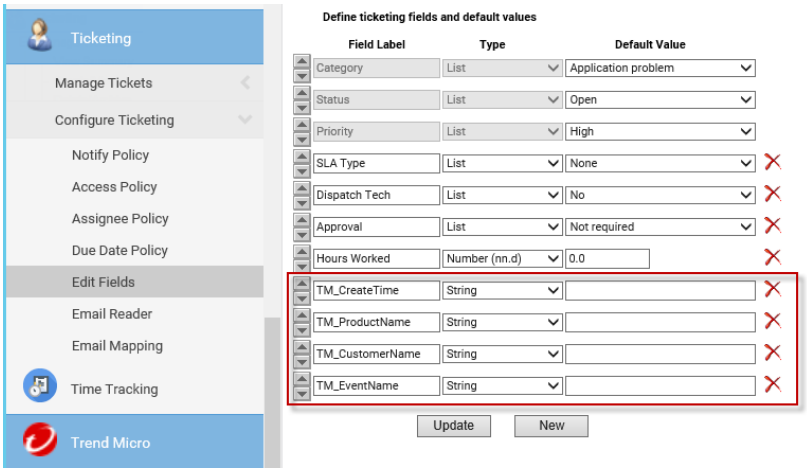


圖 13-3. Kaseya 票證欄位

2. 確保電子郵件設定正確無誤，如以下畫面所示：

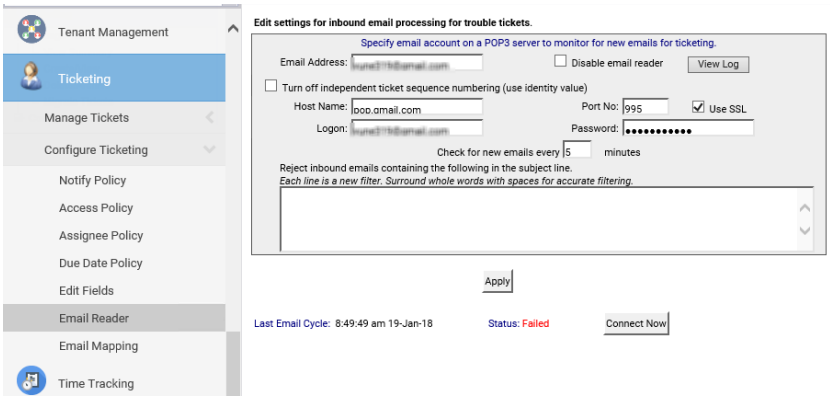


圖 13-4. Kaseya 電子郵件設定

在事件被觸發時，Kaseya 將收到票證：

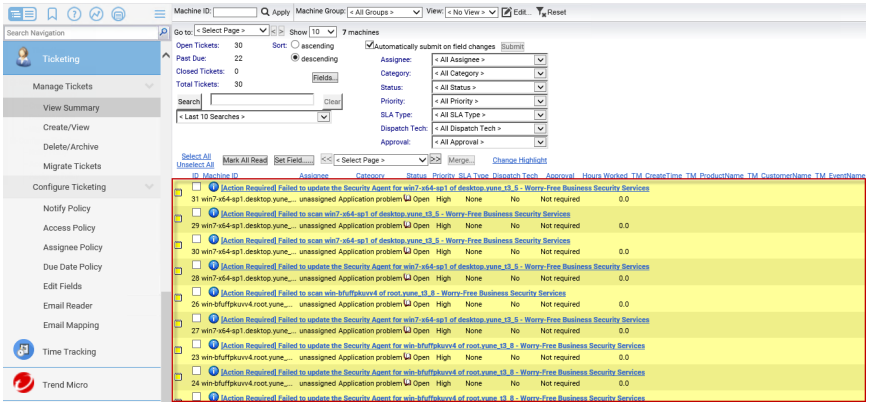


圖 13-5. Kaseya 事件票證

安裝 Trend Micro Worry-Free Services Plug-in for Kaseya

此嵌入程式可讓 Remote Manager 與 Kaseya 同步 Worry-Free Business Security Services 客戶和偵測資料。

注意

使用 Customer Licensing Portal 帳號的客戶不支援 Trend Micro Worry-Free Services Plug-in for Kaseya。

程序

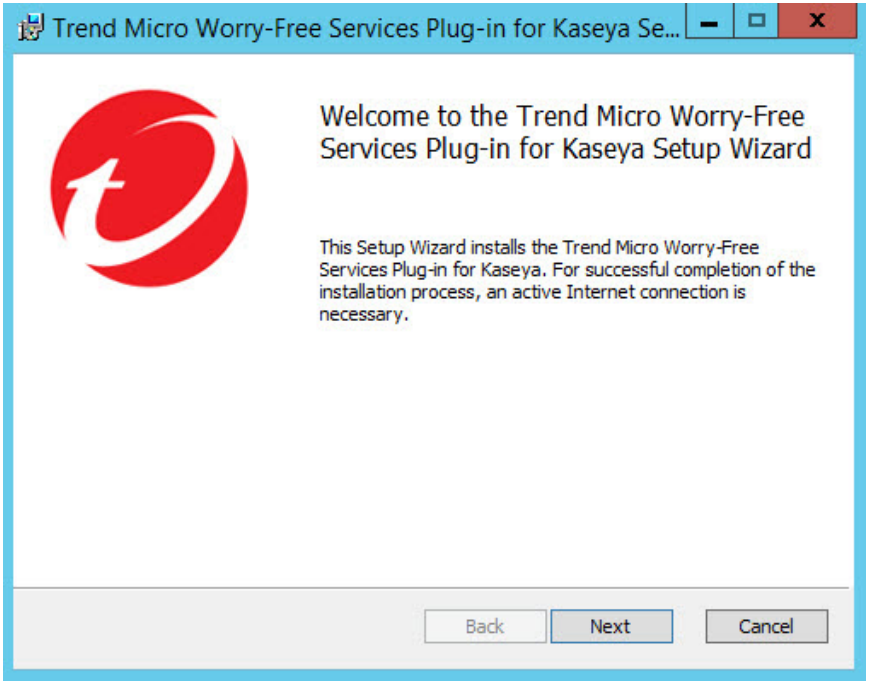
1. 開啟 Remote Manager 主控台，然後移至「管理 > 設定第三方整合」。

   隨即顯示「設定第三方整合」畫面。

2. 移至「Kaseya」區段。

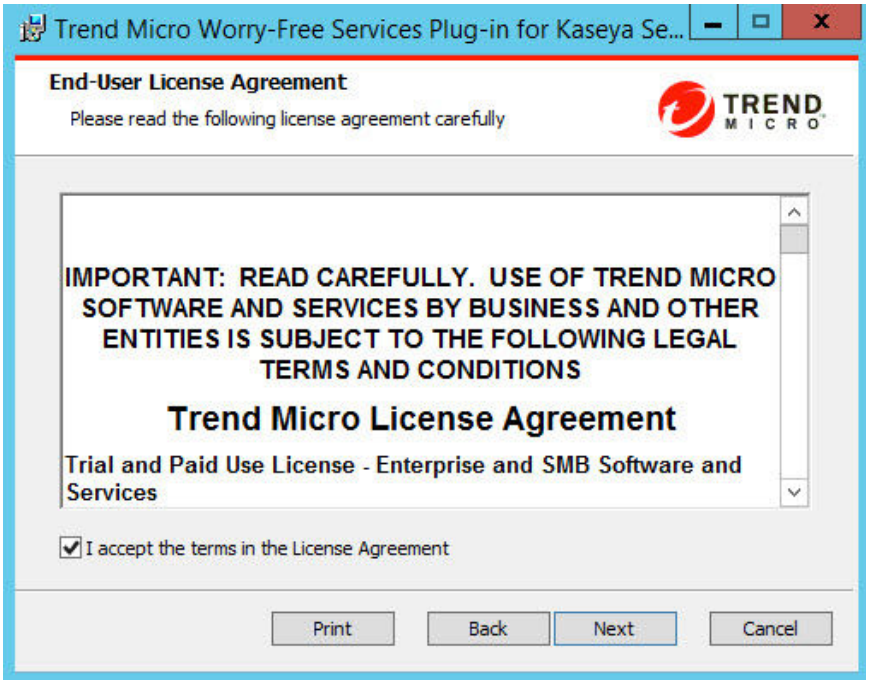
3. 在「Worry-Free Services Plug-in for Kaseya」下，按「下載」以儲存此嵌入程式。
4. 在 Kaseya VSA 伺服器上儲存檔案。
5. 執行 `TrendMicroWorryFreeServicesPluginForKaseya_X.X.X.msi` 檔案。

   隨即顯示歡迎畫面。



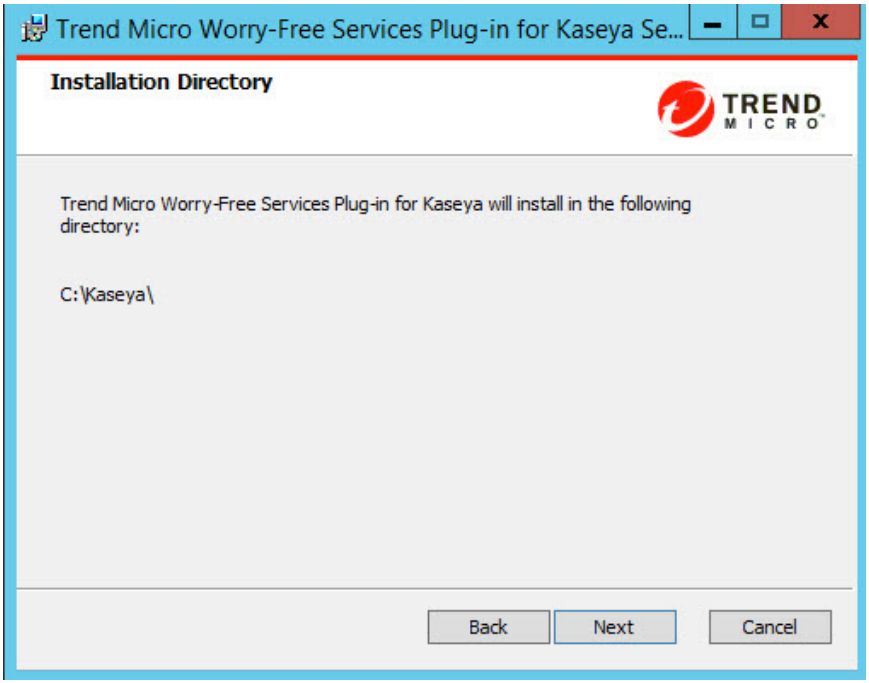
6. 按一下「Next」。

隨即顯示「End-User License Agreement」畫面。



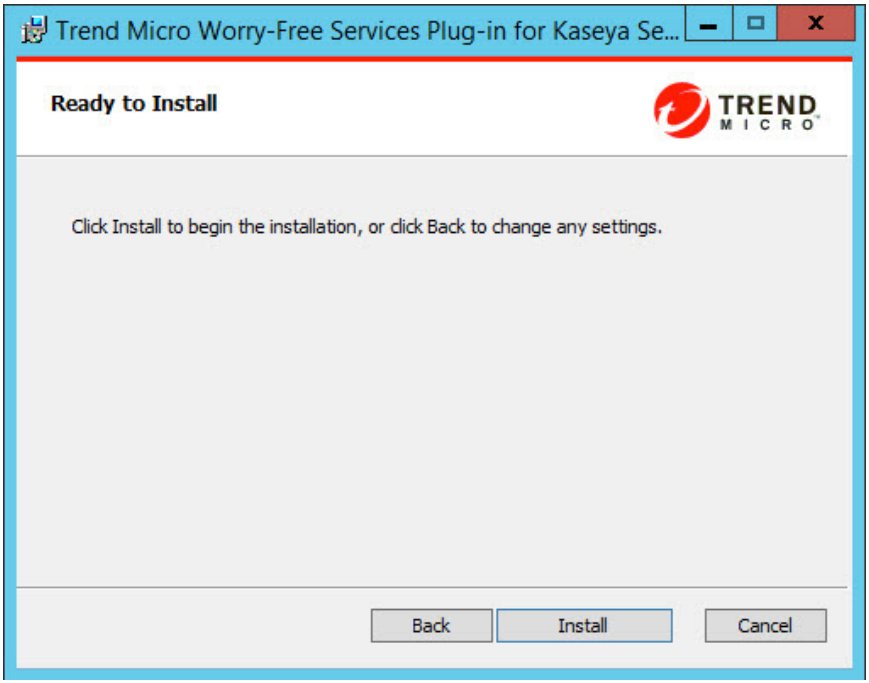
7. 如果您同意授權合約中的條款，請選取「I accept the terms in the License Agreement」核取方塊。
8. 按一下「Next」。

隨即顯示「Installation Directory」畫面。



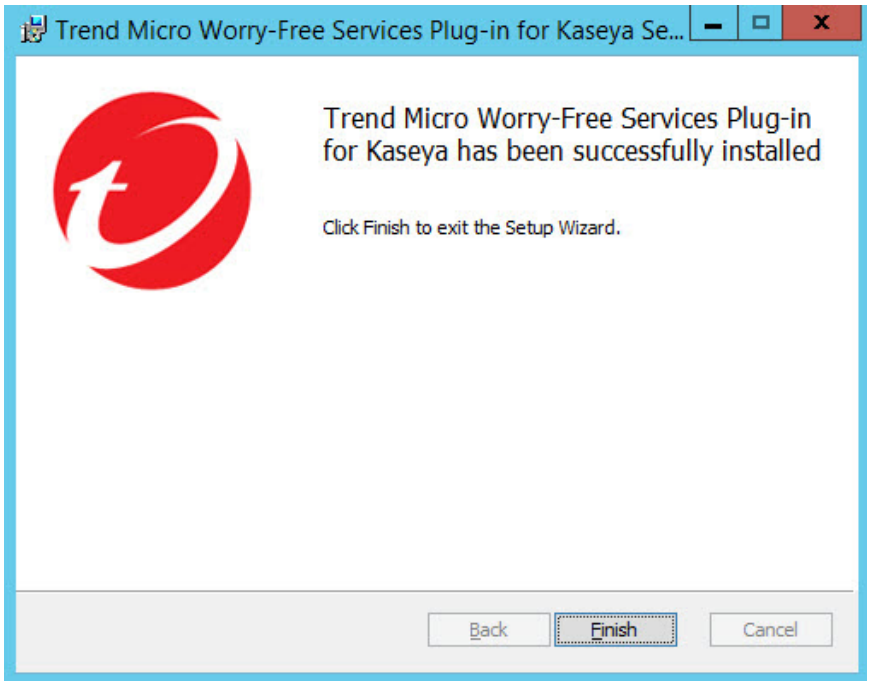
9. 確認 Kaseya 安裝資料夾，然後按一下「Next」。

隨即顯示「Ready to Install」畫面。



10. 按一下「Install」。

安裝完成後，隨即顯示「Trend Micro Worry-Free Services Plug-in for Kaseya has been successfully installed」畫面。



注意

在安裝過程中，Kaseya 會開啟一個瀏覽器視窗，其中顯示關於整合進度的資訊。

11. 按一下「Finish」。
12. 開啟 Kaseya Web 主控台，移至「Trend Micro > Worry-Free Services」。

隨即顯示以下畫面：

13. 提供 Remote Manager 啟用憑證。
    - URL（含 https）
    - Access token
    - Secret key

注意

若要尋找啟用憑證，請執行以下作業：

a. 開啟 Remote Manager 主控台並移至「管理 > 設定第三方整合」，然後移至「Kaseya」區段。

b. 在「步驟 3.在 Kaseya 主控台中，移至趨勢科技 > Worry-Free Services 並啟用嵌入程式。」下，按一下「檢視憑證」。

c. 複製啟用憑證並貼至 Kaseya Web 主控台。

---

14. 按一下「Connect」。

隨即顯示「Activation Successful」精靈，可讓您將現有的 Kaseya 客戶匯入至 Trend Micro Worry-Free Services Plug-in for Kaseya。

如需詳細資訊，請參閱匯入 Kaseya 客戶 第 13-20 頁。

更新 Trend Micro Worry-Free Services Plug-in for Kaseya

更新 Trend Micro Worry-Free Services Plug-in for Kaseya 後，您就可以使用所有新功能和增強功能。更新後的版本會自動套用所有先前設定的設定，包括客戶和 Security Agent 端點資訊。

秘訣

您也可以直接從 Kaseya 主控台下載 Trend Micro Worry-Free Services Plug-in for Kaseya 更新套件。只要有可用的更新，所有 Trend Micro Worry-Free Services Plug-in for Kaseya 畫面頂端都會出現一條資訊列。按一下「Download Now」取得套件。

程序

1. 開啟 Remote Manager 主控台，然後移至「管理 > 設定第三方整合」。

   隨即顯示「設定第三方整合」畫面。

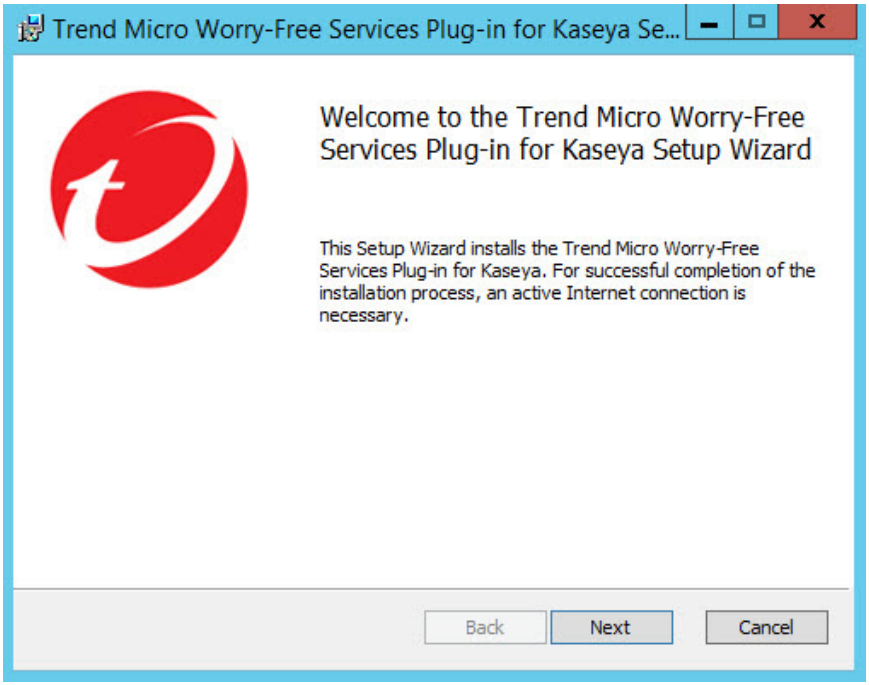
2. 移至「Kaseya」區段。

3. 在「Worry-Free Services Plug-in for Kaseya」下，按「下載」以儲存此嵌入程式。

4. 在 Kaseya VSA 伺服器上儲存檔案。

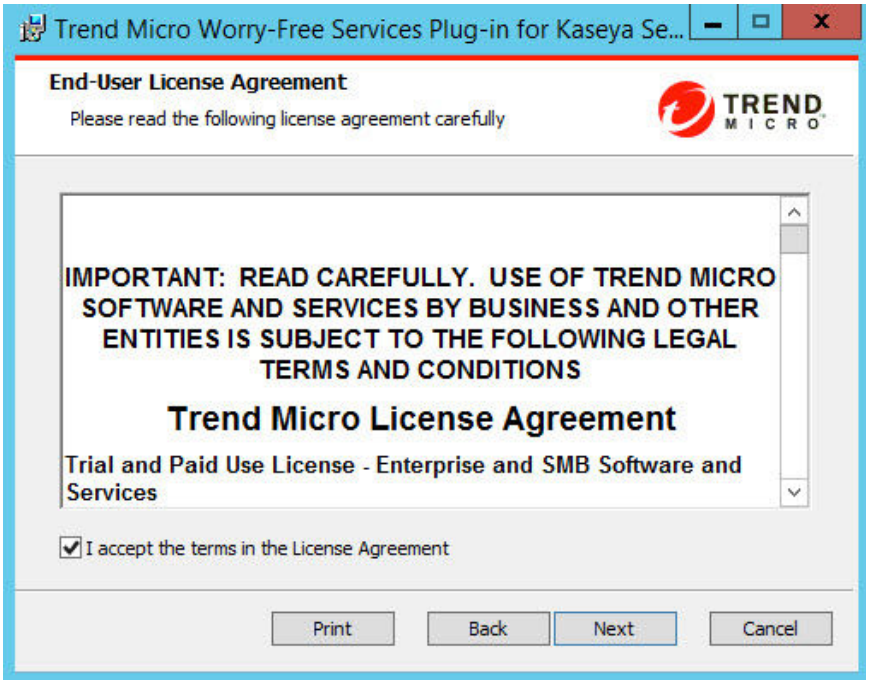
5. 執行 `TrendMicroWorryFreeServicesPluginForKaseya_X.X.X.msi` 檔案。

隨即顯示歡迎畫面。



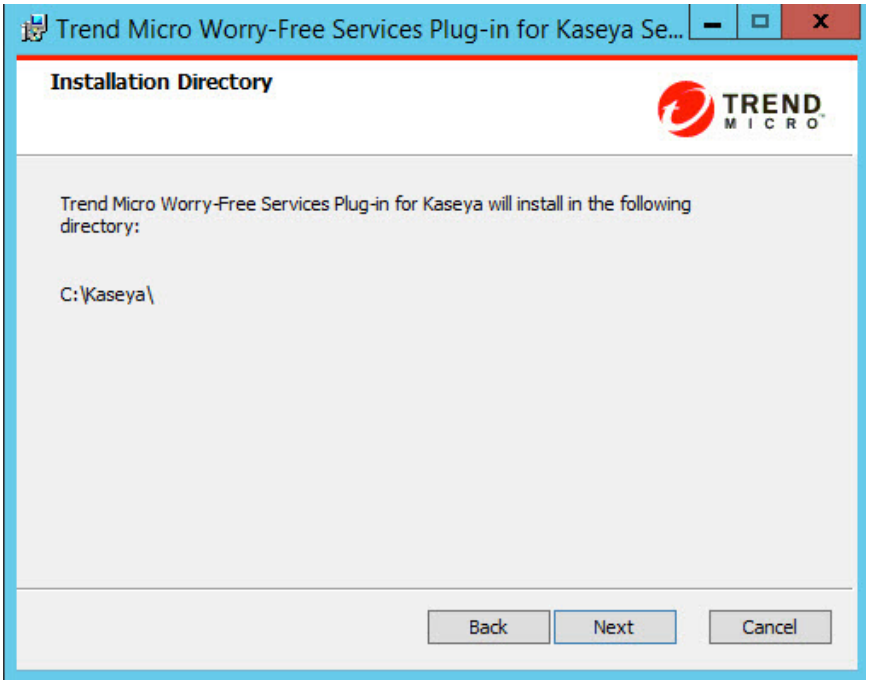
6. 按一下「Next」。

隨即顯示「End-User License Agreement」畫面。



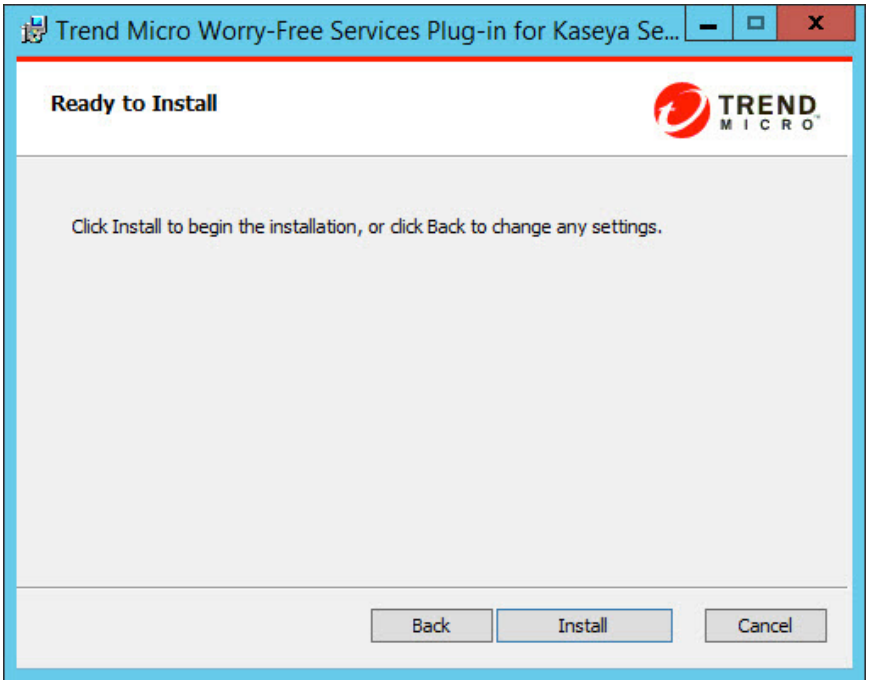
7. 如果您同意授權合約中的條款，請選取「I accept the terms in the License Agreement」核取方塊。
8. 按一下「Next」。

隨即顯示「Installation Directory」畫面。



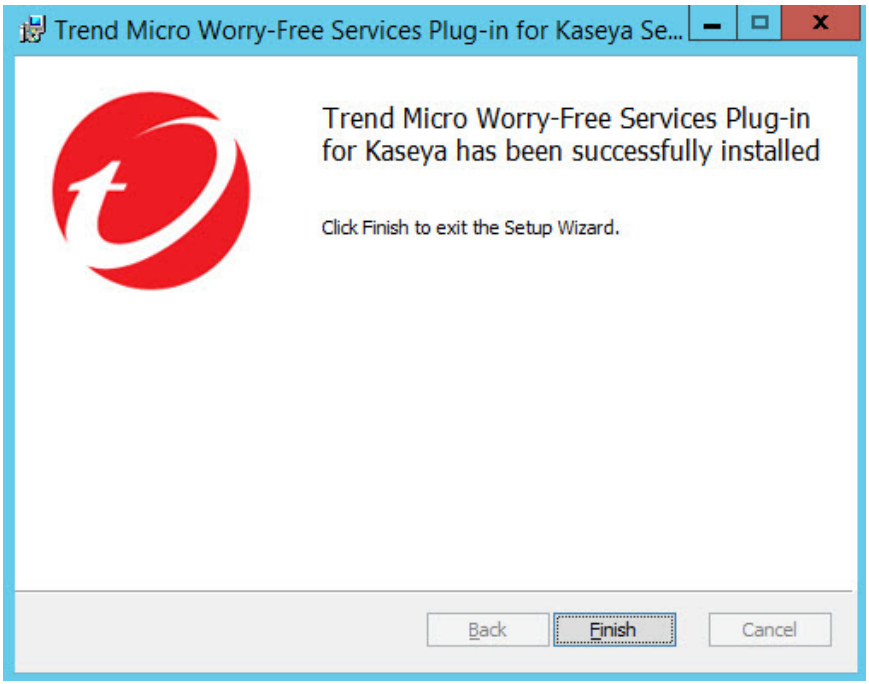
9. 確認 Kaseya 安裝資料夾，然後按一下「Next」。

隨即顯示「Ready to Install」畫面。



10. 按一下「Install」。

安裝完成後，隨即顯示「Trend Micro Worry-Free Services Plug-in for Kaseya has been successfully installed」畫面。



注意

在安裝過程中，Kaseya 會開啟一個瀏覽器視窗，其中顯示關於整合進度的資訊。

11. 按一下「Finish」。

    Trend Micro Worry-Free Services Plug-in for Kaseya 已更新。

在 Kaseya 中管理趨勢科技客戶

啟用 Trend Micro Worry-Free Services Plug-in for Kaseya 後，您可以開始將 Kaseya 客戶與趨勢科技帳號關聯，並直接從 Kaseya 主控台管理客戶關聯。

- 匯入 Kaseya 客戶：將目前的 Kaseya 客戶與預先存在的或新的趨勢科技帳號關聯

  如需詳細資訊，請參閱匯入 Kaseya 客戶 第 13-20 頁。

- 客戶摘要畫面：顯示關聯的趨勢科技客戶和未與趨勢科技帳號關聯的 Kaseya 客戶

  如需詳細資訊，請參閱客戶摘要 第 13-24 頁。

匯入 Kaseya 客戶

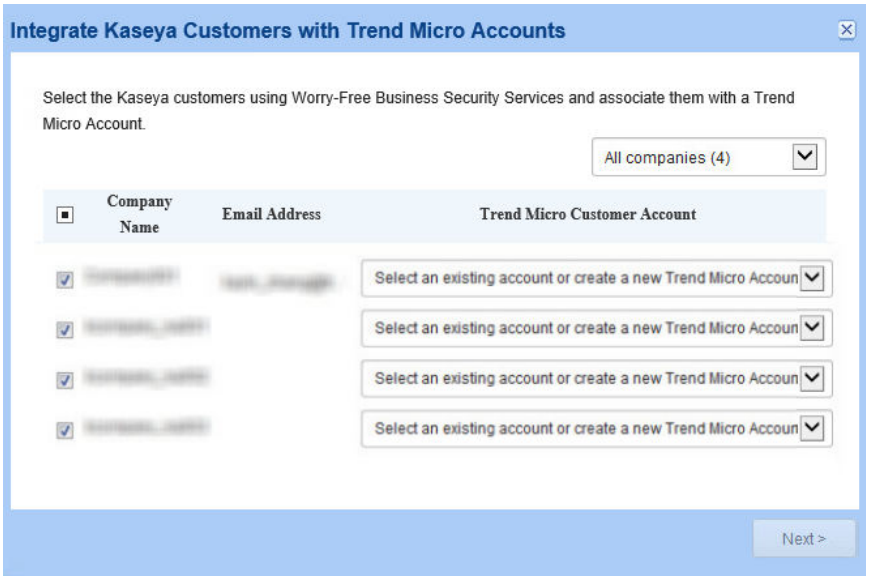
程序

1. 移至「Integrate Kaseya Customers with Trend Micro Accounts」畫面。
   - 從 Kaseya 瀏覽樹狀結構中：
     a. 移至「Trend Micro > Worry-Free Services > Customers」。
     b. 按一下「Non-Trend Micro Customers」標籤。
     c. 選取您想要與趨勢科技帳號關聯之客戶旁邊的核取方塊。
     d. 按一下「Import to Trend Micro」。
   - 首次啟用 Kaseya 嵌入程式後，從「Activation Successful」畫面中按一下「Start」。

   重要

   您必須在顯示的「Integrate Kaseya Customers with Trend Micro Accounts」畫面中，選取您想要與趨勢科技帳號關聯之 Kaseya 客戶旁邊的核取方塊。

隨即顯示「Integrate Kaseya Customers with Trend Micro Accounts」畫面。



2. 在「Trend Micro Customer Account」下拉式清單中：

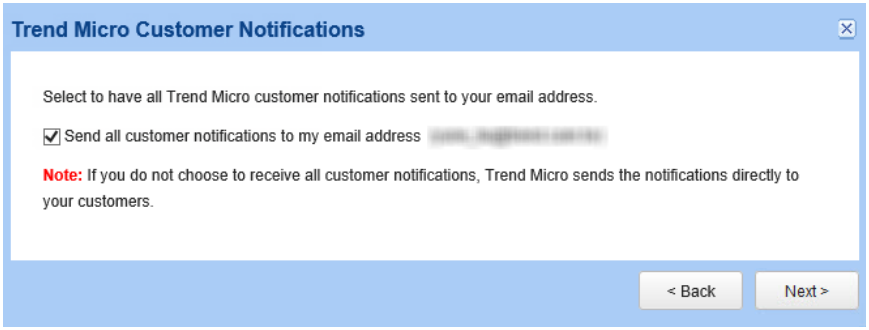
   - 選取「+ Create a new Trend Micro Account」，以在 Licensing Management Platform 中註冊新客戶
   - 從尚未指派給其他帳號的現有 Licensing Management Platform 客戶中進行選取

注意

如果您的所有客戶都已指派，則清單中不會顯示任何客戶資訊。

3. 按一下「Next >」。

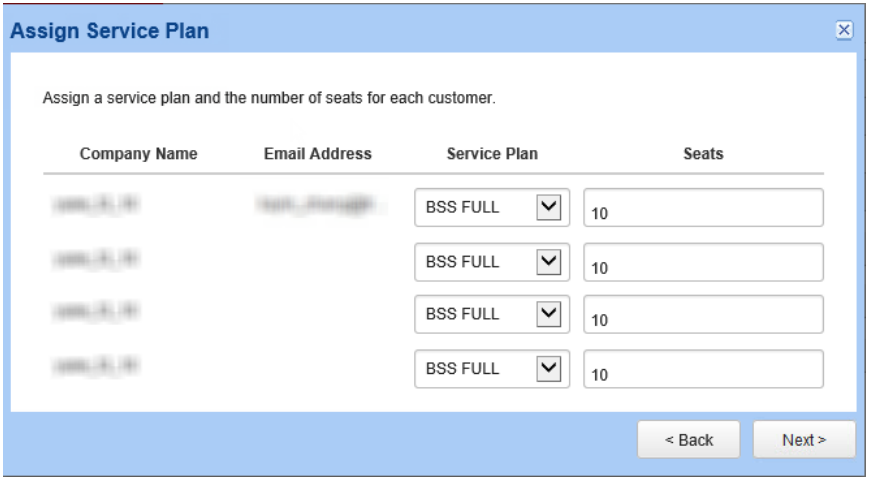
隨即顯示「Trend Micro Customer Notifications」畫面。



4. 如果您想將所選客戶環境的所有電子郵件通知傳送至您註冊的電子郵件信箱，請選取「Send all customer notifications to my email address」。

5. 按一下「Next >」。

   隨即顯示「Assign Service Plan」畫面。



6. 為每個客戶選取「Service Plan」。

7. 確認為每個客戶配置的「Seats」數量正確，然後按一下「Next >」將所選客戶新增至清單。

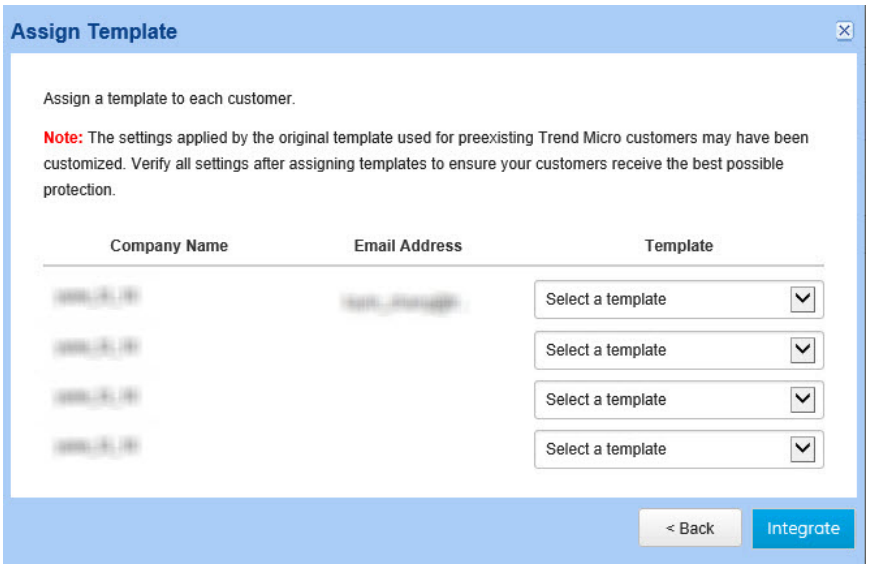
注意

依預設，Remote Manager 會佈建比客戶在 Kaseya 中所註冊端點數多 20% 的授權（每個客戶至少 10 個授權）。

重要

您必須在 Licensing Management Platform 中提供足夠的使用授權，以供選取的 Kaseya 客戶使用。如果提供的使用授權不足，則嵌入程式僅會匯入清單中有使用授權的前幾個客戶。

隨即顯示「Assign Template」畫面。



8. 在「Template」下拉式清單中，為每個客戶指派一個範本。

重要

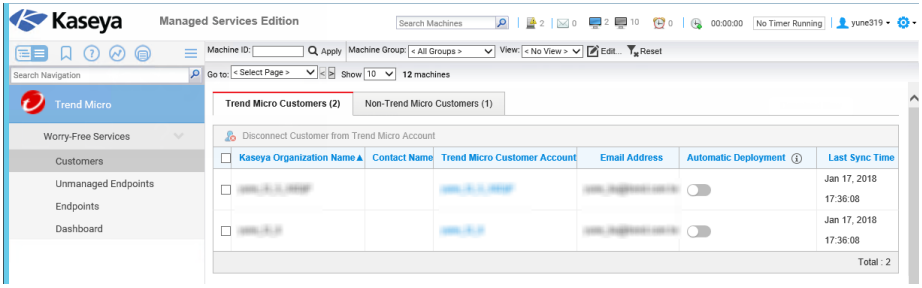
供預先存在的趨勢科技客戶使用的原始範本套用的設定可能已自訂。請在指派範本後確認所有設定，以確保您的客戶獲得最佳防護。

9. 按一下「Integrate」。

   隨即顯示「Complete Integration」畫面。

客戶摘要

「Customers」畫面提供有關 Kaseya 客戶的資訊，包括 Kaseya 組織名稱、主要客戶聯絡人、趨勢科技客戶帳號、聯絡人電子郵件信箱、自動部署狀態，以及上次與 Worry-Free Business Security Services 同步的時間。



下表概述了「Customers」畫面的主要區段。

區段	說明
「Trend Micro Customers」標籤	顯示一個表格，其中概述了 Kaseya 客戶的趨勢科技帳號資訊 啟動「Automatic Deployment」後，會以每小時一次的頻率，將 Security Agent 自動部署到指派至 ConnectWise Automate 客戶的未受保護端點。 重要 在啟動自動部署之前，請確保 Kaseya 客戶擁有足夠的使用授權。雖然在沒有使用授權的情況下，Trend Micro Worry-Free Services Plug-in 仍會部署 Security Agent，但是沒有使用授權的 Security Agent 就無法向 Worry-Free Business Security Services 主控台回報，並且會保留在未受管理的端點清單中。
「Non-Trend Micro Customers」標籤	顯示一個表格，其中概述了未連線至趨勢科技帳號的 Kaseya 客戶的帳號資訊 注意 若要部署 Trend Micro Security Agent，請選取您要管理之端點旁的核取方塊，然後按一下「Deploy Agent」。 如需詳細資訊，請參閱匯入 Kaseya 客戶 第 13-20 頁。

在 Kaseya 中管理 Worry-Free Security Agent

「Endpoints」畫面提供有關目前已安裝 Security Agent 之 Kaseya 客戶端點的資訊。

下表概述了「Endpoints」畫面的主要區段。

區段	說明
命令互動	顯示數個可在所選取端點的 Security Agent 上執行的命令互動。 • 「Scan」：在選取的端點上執行掃瞄 如需詳細資訊，請參閱掃瞄 Worry-Free Security Agent 第 13-29 頁。 • 「Update」：在選取的端點上更新 Security Agent 如需詳細資訊，請參閱更新 Worry-Free Security Agent 第 13-32 頁。 • 「Unload Agent」：從選取的端點卸載 Security Agent 如需詳細資訊，請參閱卸載 Worry-Free Security Agent 第 13-31 頁。 • 「Remove Agents」：從選取的端點移除 Security Agent 如需詳細資訊，請參閱移除 Worry-Free Security Agent 第 13-28 頁。
端點摘要	顯示一份表格，當中概述 Kaseya 客戶的端點資訊，並指出端點是否需要立即注意 注意 離線 Security Agent 將在「狀態」欄中顯示紅色背景。 「狀態」欄會指出 Security Agent 的連線狀態，以及傳送至 Security Agent 的命令狀態。

如需有關未受管理端點的詳細資訊，請參閱將 Security Agent 部署至未受管理的端點 第 13-26 頁。

將 Security Agent 部署至未受管理的端點

「未受管理的端點」畫面可讓您檢視目前未安裝 Security Agent 的所有客戶端點的 Kaseya 清單。

重要

Kaseya 需要 Agent Procedure 程式檔，才能將 Security Agent 部署至端點。

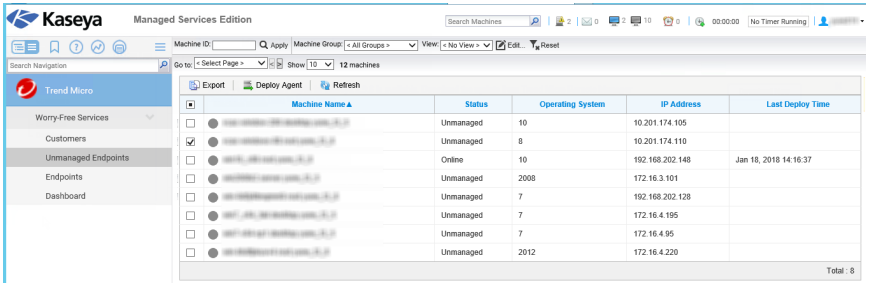
秘訣

您可以採用 CSV 格式匯出未受管理之端點的清單，以供進一步評估。

程序

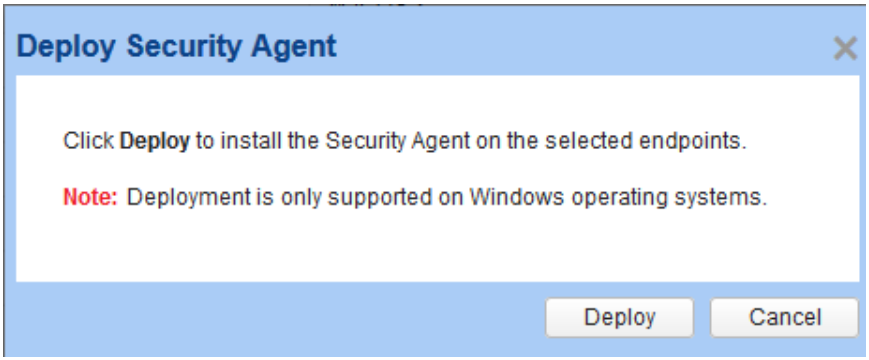
1. 開啟 Kaseya Web 主控台，移至「Trend Micro > Worry-Free Services > Unmanaged Endpoints」。

   隨即顯示以下畫面：



2. 使用 Kaseya 搜尋列過濾搜尋結果。
3. 選取您想要部署 Worry-Free Business Security Agent 之電腦旁邊的核取方塊。
4. 按一下「Deploy Agent」。

會顯示「Deploy Security Agent」畫面。



5. 按一下「Deploy」。

注意

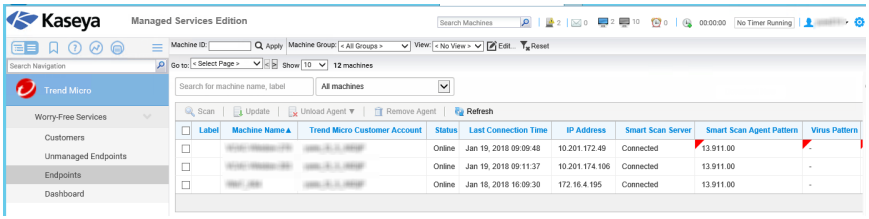
在 Remote Manager 下次與 Worry-Free Business Security Services 同步時，端點會收到此命令。預設同步時間是五分鐘。僅會在尚未安裝 Security Agent 的端點上進行安裝。

移除 Worry-Free Security Agent

程序

1. 開啟 Kaseya Web 主控台，移至「Trend Micro > Worry-Free Services > Endpoints」。

   隨即顯示以下畫面：



2. 使用下拉式清單過濾端點：
   - All machines
   - Online
   - Offline
   - Outdated
   - With virus detections
   - With spyware detections
3. 選取所需端點旁邊的核取方塊，然後按一下「Remove Agent」。

   隨即顯示確認畫面。
4. 按一下「Remove」。

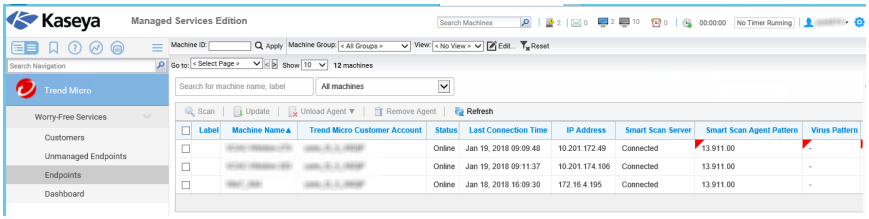
   所選端點上會立即進行 Security Agent 程式的解除安裝作業。

掃瞄 Worry-Free Security Agent

程序

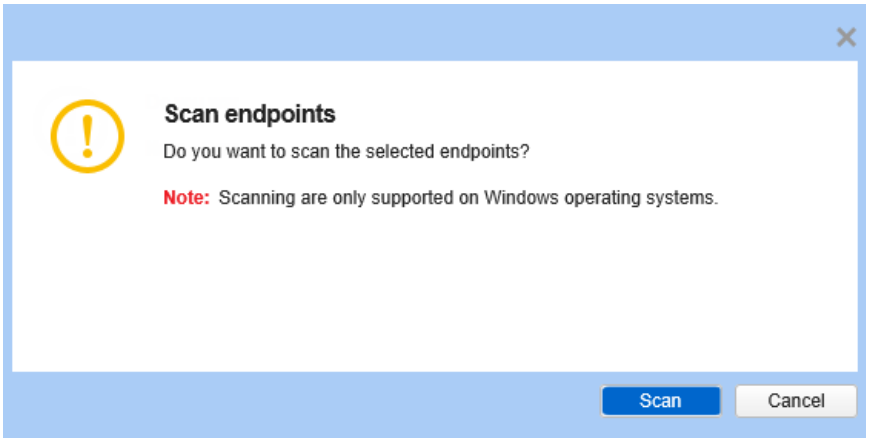
1. 開啟 Kaseya Web 主控台，移至「Trend Micro > Worry-Free Services > Endpoints」。

   隨即顯示以下畫面：



2. 使用下拉式清單過濾端點：
   - All machines
   - Online
   - Offline
   - Outdated
   - With virus detections
   - With spyware detections
3. 選取您想要掃瞄的端點旁邊的核取方塊，然後按一下「掃瞄」。

   隨即顯示確認畫面。



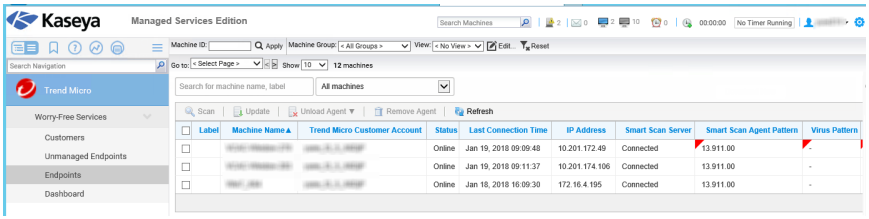
4. 按一下「Scan」。

卸載 Worry-Free Security Agent

程序

1. 開啟 Kaseya Web 主控台，移至「Trend Micro > Worry-Free Services > Endpoints」。

   隨即顯示以下畫面：



2. 使用下拉式清單過濾端點：

   - All machines
   - Online
   - Offline
   - Outdated
   - With virus detections
   - With spyware detections

3. 選取您想要卸載的端點旁邊的核取方塊，然後按一下「Unload Agent」。在出現的下拉式清單中，選取應卸載所選 Security Agent 的時間長度。

   隨即顯示確認畫面。

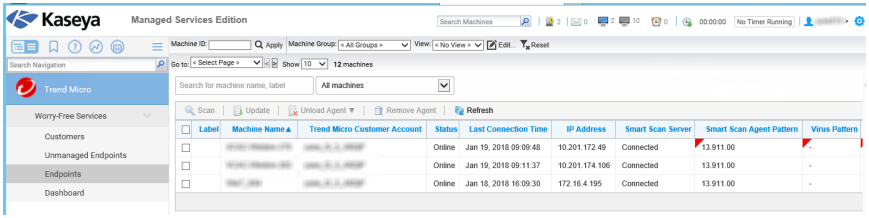
4. 按一下「Unload」。

更新 Worry-Free Security Agent

程序

1. 開啟 Kaseya Web 主控台，移至「Trend Micro > Worry-Free Services > Endpoints」。

   隨即顯示以下畫面：



2. 使用下拉式清單過濾端點：
   - All machines
   - Online
   - Offline
   - Outdated
   - With virus detections
   - With spyware detections
3. 選取您想要更新的端點旁邊的核取方塊，然後按一下「Update」。

   隨即顯示確認畫面。
4. 按一下「Update」。

趨勢科技資訊中心

使用「資訊中心」快速檢視您的 Kaseya 客戶的安全狀態，以及 Worry-Free Business Security Services 偵測到的安全威脅總數。

「資訊中心」提供以下 Widget：

- 「需要採取處理行動的事件」Widget 第 13-33 頁
- 「安全威脅管理」Widget 第 13-33 頁

「需要採取處理行動的事件」Widget

「需要採取處理行動的事件」Widget 列出了有端點需要注意的客戶。

事件	說明
中毒處理行動不成功	按一下「出現次數」，移至 Worry-Free Business Security Services 主控台，並檢視客戶端點上的不成功掃瞄結果。
需要即時掃瞄	按一下「端點」，移至 Worry-Free Business Security Services 主控台，並檢視即時掃瞄已關閉的端點。
需要重新啟用	按一下「出現次數」，移至 Worry-Free Business Security Services 主控台，並檢視需要重新啟用以完成間諜程式/可能的資安威脅程式清除的端點。
需要更新	按一下「端點」，移至 Worry-Free Business Security Services 主控台，並檢視需要更新的端點。

按一下「公司」名稱，在 Remote Manager 主控台上檢視資訊。

「安全威脅管理」Widget

檢視具有不同安全偵測類型的客戶數目。按一下安全威脅「類型」可在 Remote Manager 主控台上檢視詳細資訊。

Kaseya 中的 Worry-Free Business Security Services 票證

下表概述了 Worry-Free Security Services 嵌入程式所產生的 Kaseya 票證。

命令類型	票證主旨	可能原因
Scan	[Action Required] Unsuccessful scan command - <machine_name> of <client_name> - Worry-Free Business Security Services	• 選取的端點未安裝 Security Agent • 選取的端點上安裝的 Security Agent 已損毀 • 選取的端點處於離線狀態，或 Security Agent 已卸載 • Security Agent 正在執行更新 • 發生內部錯誤
Update Agent	[Action Required] Unsuccessful update command - Security Agent for <machine_name> of <client_name> - Worry-Free Business Security Services	• 選取的端點未安裝 Security Agent • 選取的端點上安裝的 Security Agent 已損毀 • 選取的端點處於離線狀態，或 Security Agent 已卸載 • Security Agent 正在執行掃瞄 • 發生內部錯誤
Deploy Agent	[Action Required] Unsuccessful deployment command - Security Agent for <machine_name> of <client_name> - Worry-Free Business Security Services	• 伺服器未完成產生 Security Agent 安裝套件 • 下載 Security Agent 安裝套件時發生錯誤 • Security Agent 目前正在選取的端點上安裝，或已安裝完成

命令類型	票證主旨	可能原因
Automatic Deployment	[Action Required] Exceeded seat allocation for <machine_name> of <client_name> - Worry-Free Business Security Services	• Security Agent 已部署，但仍處於未受管理狀態，因為客戶所剩的使用授權不足

部分 V

监控客戶

第 14 章

瞭解資訊中心

Trend Micro Remote Manager 具有監控資訊中心，提供所有客戶的安全、系統和使用授權狀態的快速檢視。

本節包含下列主題：

資訊中心狀態畫面

資訊中心是用於檢閱監控網路之狀態的中心畫面。資訊中心僅列出狀態不正常的產品。例如，如果客戶的 Worry-Free Business Security Services 使用授權即將到期，或者如果客戶具有太多安全威脅，這些客戶將在此列出。

若要存取資訊中心，請開啟相容的瀏覽器，然後登入您所在地區的 Trend Micro Remote Manager 網站。

資訊中心中的大多數項目都已加入連結，以協助您解決問題。按一下某個項目（圖形、連結、號碼），以解決相應問題。

如需詳細資訊，請參閱產品/服務資訊 第 3-4 頁。

使用標籤和 Widget

標籤為 Widget 提供了容器。「首頁」畫面上的每個標籤可以容納最多 20 個 Widget。「首頁」畫面本身最多支援 30 個標籤。

Widget 是資訊中心的核心元件。Widget 提供有關各種安全或使用授權相關事件的特定資訊。某些 Widget 可讓您執行特定工作。

Widget 顯示以下出處的資訊：

- Cloud App Security
- Cloud Edge 伺服器和用戶端
- Hosted Email Security 服務
- InterScan Web Security as a Service
- Worry-Free Business Security 伺服器和用戶端
- Worry-Free Business Security Services 伺服器

標籤工作

下表列出所有標籤相關工作：

工作	步驟
新增標籤	按一下「首頁」畫面頂端的新增圖示 (+)。會顯示一個新標籤。
重新命名標籤	將游標懸停在標籤名稱上並按一下向下箭頭 ( )，然後按一下「重新命名」。輸入標籤的新名稱。
標記標籤版面配置	將游標懸停在標籤名稱上並按一下向下箭頭 ( )，然後按一下「變更版面配置」。會開啟「變更版面配置」視窗。 如需詳細資訊，請參閱「變更版面配置」視窗 第 14-4 頁。
刪除標籤	將游標懸停在標籤名稱上並按一下向下箭頭 ( )，然後按一下「刪除」。按一下「確定」以刪除標籤。
播放標籤投影片放映	按一下標籤顯示右側的「設定」按鈕 ( )，然後按一下「標籤投影片放映」滑桿。在滑桿下的下拉式功能表中，選擇選取的標籤應顯示的時間間隔。

工作	步驟
移動標籤	使用拖放功能變更標籤的位置。 注意 並非所有瀏覽器都支援拖放功能。 如需有關建議的瀏覽器的詳細資訊，請參閱瀏覽器需求 第 1-6 頁。

「變更版面配置」視窗

當您在標籤的下拉式功能表 (▽) 中按一下「變更版面配置」時，會開啟「變更版面配置」視窗。

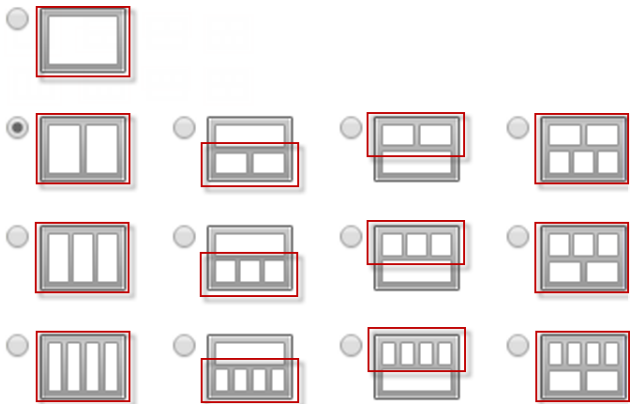
秘訣

趨勢科技建議的最低畫面解析度如下，具體取決於您的版面配置選擇：

- 2 欄：800 x 600 或更高
- 3 欄：1280 x 720 或更高
- 4 欄：1680 x 1050 或更高

Widget 工作

下表列出 Widget 相關工作：

工作	步驟
新增 Widget	開啟一個標籤，然後按一下標籤右上角的「新增 Widget」。將顯示「新增 Widget」畫面。
重新整理 Widget 資料	按一下重新整理圖示（ ）。
檢視說明	按一下「說明」(?)。
刪除 Widget	按一下「關閉 Widget」( )。此處理行動會從包含此 Widget 的標籤中將其移除，但不會從包含此 Widget 的其他標籤中或「新增 Widget」畫面中的 Widget 清單中將其移除。
移動 Widget	使用拖放功能將 Widget 移動到標籤內的不同位置。
調整 Widget 的大小	若要調整 Widget 的大小，請將游標指向此 Widget 的右側。顯示粗垂直線和箭頭（如下圖所示）時，請按住游標，然後移動到左側或右側。  只能調整多欄標籤上的 Widget。具有任何以下版面配置和反白顯示區段的標籤包含可以調整大小的 Widget。 

Remote Manager Widget

資訊中心會顯示下列 Remote Manager Widget：

「客戶通知中心」Widget

此 Widget 提供目前具有「需要採取處理行動」或「警告」事件狀態的 Remote Manager 客戶計數。

將游標懸停在客戶計數上可檢視最近受影響客戶的排名靠前的事件類別。

若要開啟「通知中心」並檢視有關目前狀態的更多詳細解釋，請按一下特定「類別」的「出現次數」計數，或按一下「在通知中心中檢視所有通知」以檢視所有受影響的客戶。

如需詳細資訊，請參閱通知中心 第 14-32 頁。

「安全威脅事件統計中心」Widget

此 Widget 提供選取的時間範圍內，偵測到的所有安全威脅與策略違規的總覽。

將滑鼠游標暫留在安全威脅或違規總數上，可檢視每個群組中特定偵測類型的明細。

若要切換檢視，請按一下右上角的表格圖示或橫條圖圖示。若要在表格檢視中檢視特定特徵的記錄檔，請按一下右側的總數。若要在橫條圖檢視中檢視特定特徵的記錄檔，請按一下右側的橫條圖。

表 14-1. 偵測類別

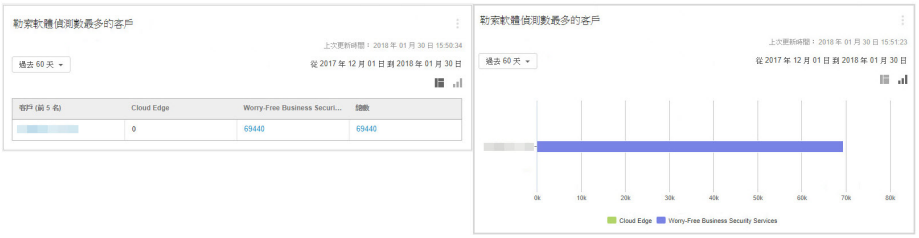
類別	說明
已知的安全威脅	顯示所有會偵測趨勢科技已確認之安全威脅的特徵 • 殭屍網路 • C&C 回呼 • 檔案封鎖 • IPS • 網路病毒 • 垃圾郵件 • 病毒/惡意程式 • 間諜程式/可能的資安威脅程式 • 網頁信譽評等服務
未知的安全威脅	顯示所有會使用進階邏輯分析、分析或特徵建模來偵測潛在安全威脅的特徵 • Machine Learning • 行為監控 • 沙盒虛擬平台
策略違規	顯示所有包含您企業安全標準特定策略違規的特徵 • 應用程式控管 • 週邊設備存取控管 • URL 過濾

「需要最多關注的客戶」Widget

顯示具有最多需要立即採取處理行動或回應的事件之客戶的最新數目。資料以表格和圓餅圖顯示。您可以按一下顯示圖示 ( )，在表格和圓餅圖之間切換。

- 如果特定狀態的客戶數目大於或等於 1，您可以按一下該數值來檢視產品樹狀結構中的事件。
- 按一下客戶名稱可檢視此客戶的所有事件，或者展開客戶名稱來查看特定類別的事件。
- 「需要採取處理行動」下的事件數目是應儘快處理之事件的數目。
- 「警告」下的事件數目是緊急程度低於「需要採取處理行動」下的事件，但也需要儘快處理之事件的數目。

「勒索軟體偵測數最多的客戶」Widget



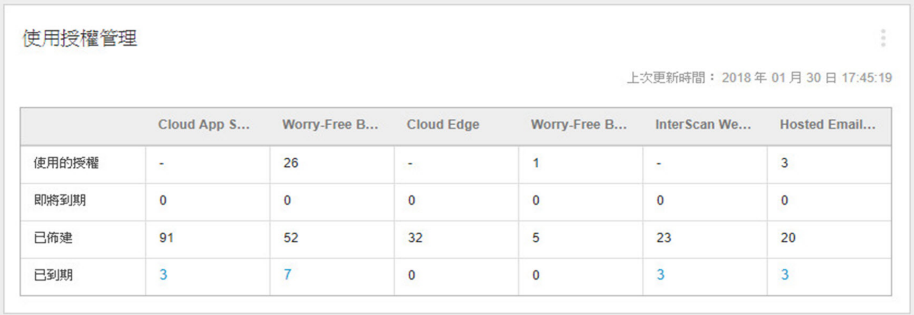
此 Widget 顯示在選取的時間範圍內勒索軟體偵測數最高的 Cloud Edge 和 Worry-Free Business Security Services 客戶。

若要切換檢視，請按一下右上角的表格圖示或橫條圖圖示。

檢視	選項
表格	• 按一下「客戶」名稱可開啟「客戶 **>** **[客戶]**」畫面。 • 按一下任何偵測計數可檢視事件記錄。
橫條圖	• 將游標懸停在橫條圖上可檢視針對特定客戶和產品的偵測數。 • 按一下任何橫條圖可檢視事件記錄。

「使用授權管理」Widget

顯示客戶使用之使用授權的目前狀態。



	Cloud App S...	Worry-Free B...	Cloud Edge	Worry-Free B...	InterScan We...	Hosted Email...
使用的授權	-	26	-	1	-	3
即將到期	0	0	0	0	0	0
已佈建	91	52	32	5	23	20
已到期	3	7	0	0	3	3

顯示客戶和產品的以下使用授權相關詳細資訊：

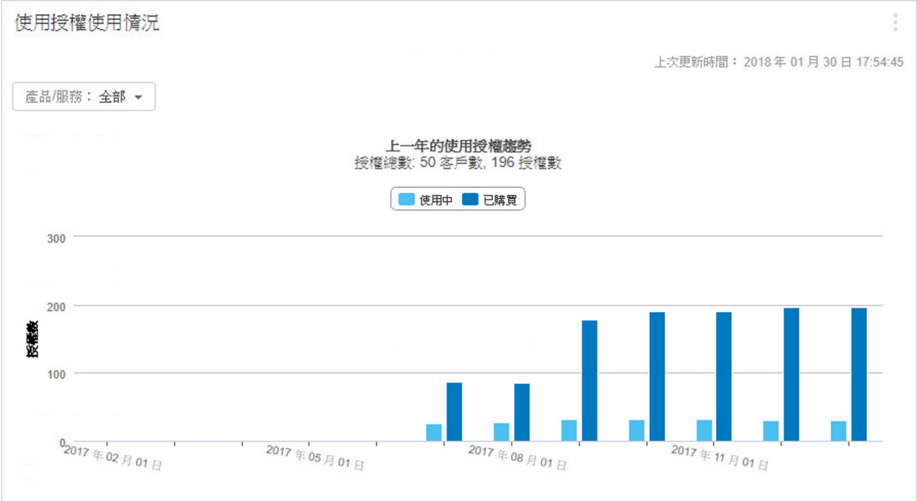
- 「即將到期」：尚未到期但即將到期的使用授權數目。
- 「已到期」：已到期的使用授權。

> **注意**
> 趨勢科技建議儘快續約這些使用授權。

- 「使用的授權」：目前正在使用的授權數目。
- 「已佈建」：客戶已佈建的授權數目。

「使用授權使用情況」Widget

顯示一年內已配置授權和實際購買授權的圖形分析。這可協助確定您應增加還是減少授權配置。

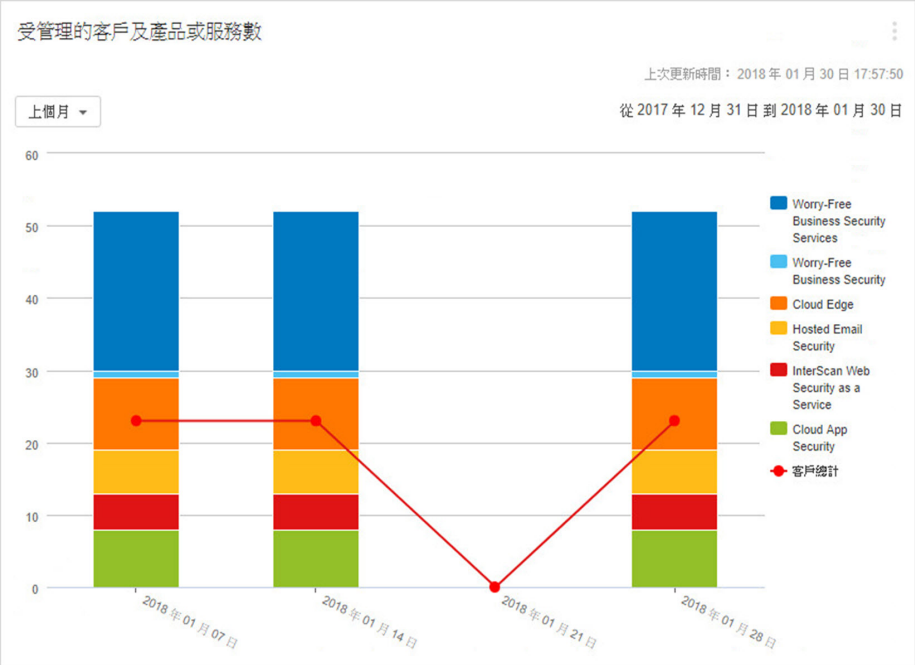


您可以選取以下選項，變更產品/服務：

- 全部
- Hosted Email Security
- Worry-Free Business Security
- Worry-Free Business Security Services
- Cloud Edge
- InterScan Web Security as a Service
- Cloud App Security

「受管理的客戶及產品或服務數」Widget

顯示指定時間段內每個產品的受管理客戶數目。



- 您可以選取以下選項，變更所顯示資料的時間範圍：
  - 上個月（預設）
  - 過去 3 個月
  - 過去 6 個月
  - 去年
- 您可以在右側按一下已註冊產品的名稱，以在圖形中新增或移除資料。

- 每個橫條圖表示一個週或一個月。
- 橫條圖顯示產品/服務的總數目。

「勒索軟體偵測數」Widget

顯示 Cloud App Security、Hosted Email Security、Worry-Free Business Security Services、Cloud Edge、InterScan Web Security as a Service 和 Worry-Free Business Security 中的勒索軟體偵測資料。

- 您可以選取以下選項，變更所顯示資料的時間範圍：
  - 過去 24 小時（預設）
  - 過去 7 天
  - 過去 30 天
- 您可以按一下以下計數，檢視勒索軟體事件記錄：

- 「感染嘗試次數」：顯示依出現次數排序的勒索軟體事件記錄。
- 「偵測到勒索軟體的客戶數」：顯示依公司名稱排序的勒索軟體事件記錄。

- 展開資訊方塊 (ⓘ) 以檢視「最大化 Worry-Free Business Security Services 的勒索軟體防護」連結。按一下此連結可為您的所有客戶啟用勒索軟體防護。

  如需關於在 Remote Manager 中設定勒索軟體防護的詳細資訊，請參閱最大化勒索軟體防護常見問題 第 18-11 頁。

「所有客戶的勒索軟體偵測數」Widget

此 Widget 顯示選取的時間範圍內，受支援產品的勒索軟體總偵測數。您可以自訂此 Widget，以顯示單一客戶的資料。

按一下任何偵測計數可檢視事件記錄。

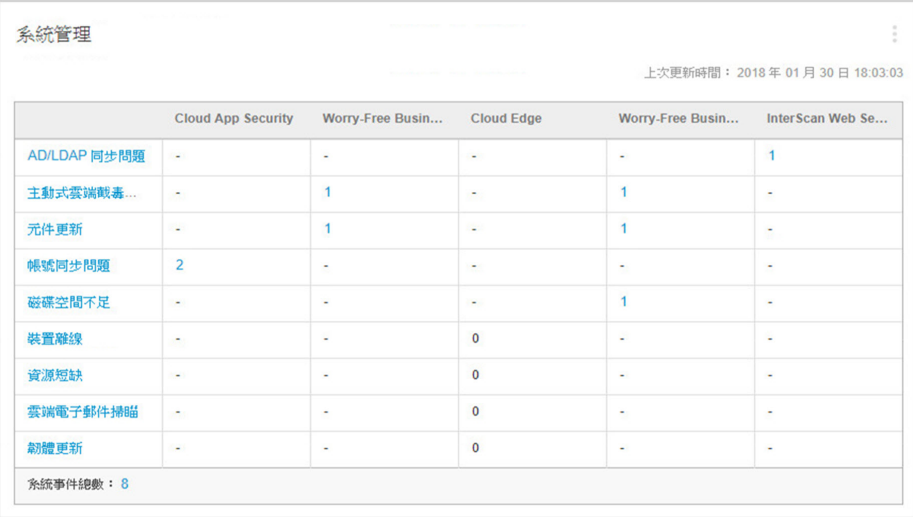
若要檢視特定客戶的資料，請按一下「顯示特定客戶的資料」連結，並選取您想要顯示的客戶和產品。您還可以變更此 Widget 的標題。

表 14-2. 防護層

防護層	說明
Internet	「Internet」層包含的產品會在安全威脅到達使用者的閘道之前，從雲端中對其進行偵測。 在此層運作的產品包括： • Cloud App Security • Hosted Email Security • InterScan Web Security as a Service 將游標懸停在圓形產品圖示上，以顯示該產品偵測到的勒索軟體嘗試次數資料。
閘道	「閘道」層包含保護路由器、伺服器和其他閘道裝置的產品。 在此層運作的產品包括： • Cloud Edge 將游標懸停在圓形產品圖示上，以顯示該產品偵測到的勒索軟體嘗試次數資料。
Intranet	「Intranet」層包含保護閘道內端點的產品。 在此層運作的產品包括： • Worry-Free Business Security • Worry-Free Business Security Services 將游標懸停在圓形產品圖示上，以顯示該產品偵測到的勒索軟體嘗試次數資料。

「系統管理」Widget

顯示已註冊產品的所有系統事件的目前數目。您可以使用此 Widget 確定硬體問題、伺服器或 Agent 事件。



如果特定類別的事件數目大於等於 1，您可以按一下該數值來檢視事件記錄。

「安全威脅管理」Widget

顯示所有已註冊產品的安全威脅事件計數。

	Cloud App Se...	Worry-Free B...	Cloud Edge	Worry-Free B...	InterScan We...	Hosted Email ...
C&C 回呼	-	-	0	-	-	-
IPS	-	-	0	-	-	-
Machine Lear...	-	230	0	-	-	-
URL 過濾	-	460	-	0	0	-
勒索軟體	1380	1150	0	45	0	380
周邊設備存取...	-	92	-	60	-	-
垃圾郵件防護	-	-	0	-	-	323
應用程式控管	-	230	-	-	0	-
檔案封鎖	276	-	-	-	-	-
殭屍網路	-	-	0	-	-	-
沙盒虛擬平台	828	-	0	-	-	-
病毒/惡意程式	552	460	0	75	0	399
網路病毒	-	230	-	32	-	-
網頁信譽評等...	552	230	0	0	0	-
行為監控	-	460	-	45	-	-
間諜程式/可能...	-	230	-	60	0	-

安全威脅事件總數：8779

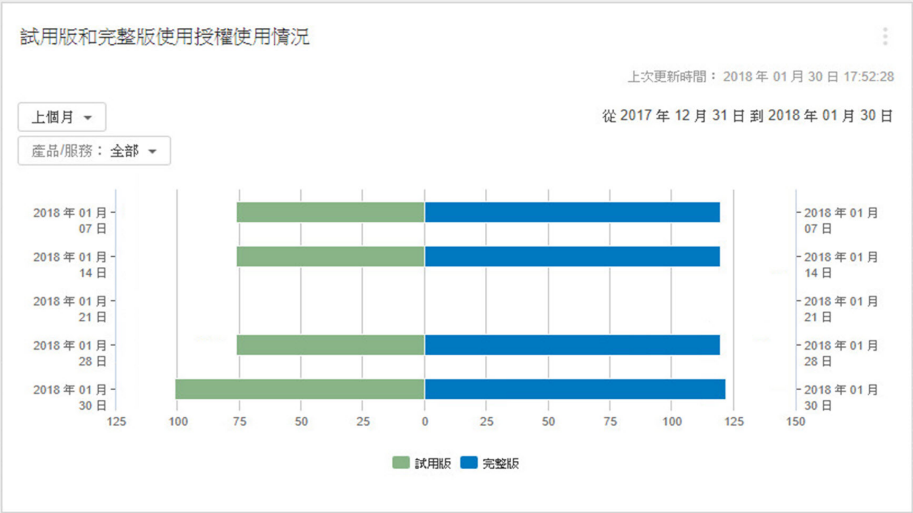
- 您可以選取以下選項，變更所顯示資料的時間範圍：
  - 過去 24 小時（預設）

- 過去 7 天
- 過去 30 天

- 如果特定類別的事件數目大於等於 1，您可以按一下該數值來檢視事件記錄。

「試用版和完整版使用授權使用情況」Widget

顯示已註冊產品使用的試用版或完整版使用授權數目。



您可以選取以下選項，變更所顯示資料的時間範圍：

- 上個月（預設）
- 過去 3 個月
- 過去 6 個月
- 去年

您可以選取以下選項，變更產品/服務：

- 全部
- Hosted Email Security
- Worry-Free Business Security
- Worry-Free Business Security Services
- Cloud Edge
- InterScan Web Security as a Service
- Cloud App Security

檢視特定產品的事件

特定產品的事件顯示即時事件的清單。

程序

1. 移至「客戶 > {公司名稱} > {產品}」。
2. 請根據選取的產品執行下列其中一項動作。

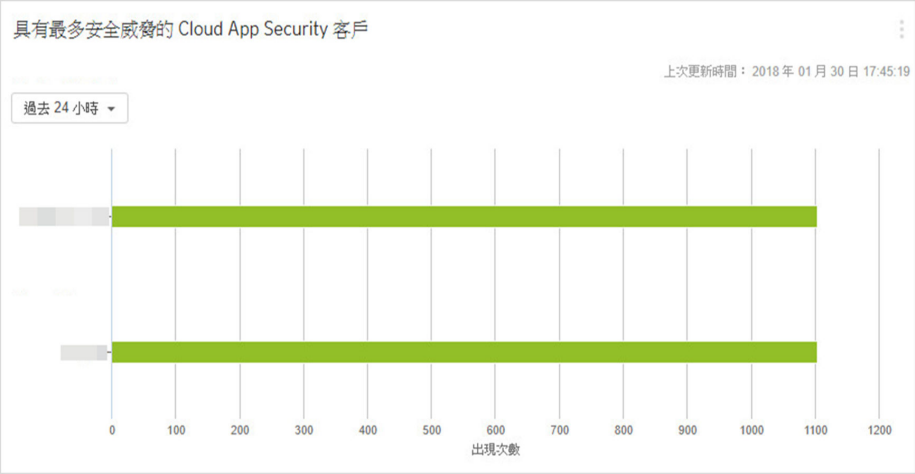
產品	步驟
Cloud App Security	移至「事件」標籤。
Cloud Edge	移至「事件」標籤。
InterScan Web Security as a Service	從網路樹狀結構中選取 IWSaaS 產品時，會自動顯示事件清單。
Worry-Free Business Security	移至「事件」標籤。
Worry-Free Business Security Services	移至「事件」標籤。

Cloud App Security Widget

資訊中心會顯示下列 Cloud App Security Widget：

「具有最多安全威脅的 Cloud App Security 客戶」Widget

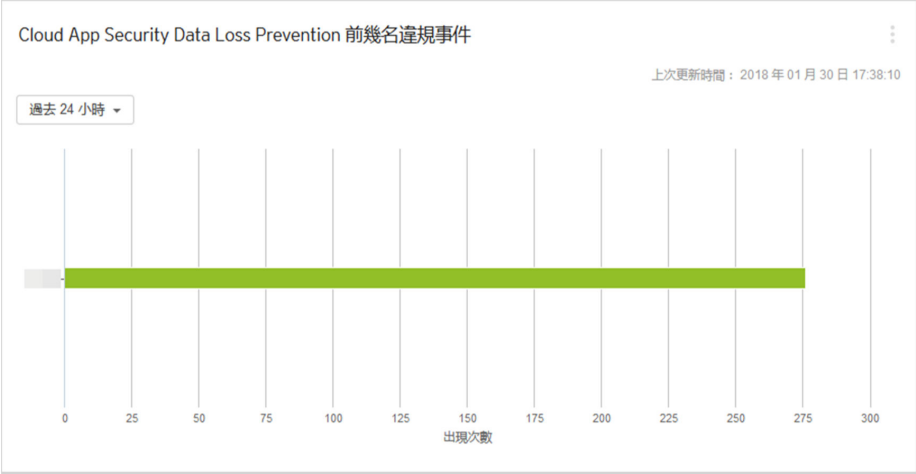
顯示安全威脅事件數最多的 Cloud App Security 客戶。



按一下橫條可檢視事件記錄檔。

「Cloud App Security Data Loss Prevention 前幾名違規事件」Widget

顯示 Data Loss Prevention 範本違規數最多的 Cloud App Security 客戶。

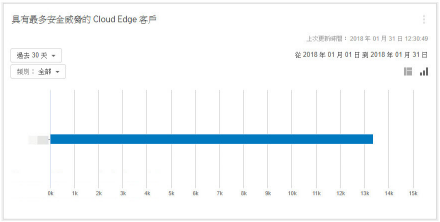


按一下橫條可檢視事件記錄檔。

Cloud Edge Widget

資訊中心會顯示下列 Cloud Edge Widget：

「具有最多安全威脅的 Cloud Edge 客戶」Widget



此 Widget 顯示安全威脅事件數最多的 Cloud Edge 客戶。

資料以表格和橫條圖顯示。若要切換檢視，請按一下右上角的表格圖示或橫條圖圖示 ( )。

- 按一下右邊的計數，即可檢視 Cloud Edge 主控台中的安全威脅詳細資訊。
- 按一下「客戶」名稱可開啟「客戶 > [客戶]」畫面。
- 選取以下選項即可變更所顯示資料的類別：
  - 全部
  - 殭屍網路
  - C&C 回呼
  - IPS
  - Machine Learning
  - 勒索軟體 (電子郵件途徑)
  - 勒索軟體 (網路途徑)
  - 勒索軟體 (Web 途徑)
  - 垃圾郵件
  - 沙盒虛擬平台

- 病毒 (電子郵件途徑)
- 病毒 (Web 途徑)
- 網頁信譽評等服務

「具有最多安全威脅的 Cloud Edge 裝置」Widget

此 Widget 顯示安全威脅事件數最多的 Cloud Edge 裝置。

- 按一下右邊的計數，即可檢視 Cloud Edge 主控台中的安全威脅詳細資訊。
- 按一下「客戶」名稱可開啟「客戶 > [客戶]」畫面。
- 選取以下選項即可變更所顯示資料的類別：
  - 全部
  - 殭屍網路
  - C&C 回呼
  - IPS
  - Machine Learning
  - 勒索軟體 (電子郵件途徑)
  - 勒索軟體 (網路途徑)
  - 勒索軟體 (Web 途徑)

- 垃圾郵件
- 沙盒虛擬平台
- 病毒 (電子郵件途徑)
- 病毒 (Web 途徑)
- 網頁信譽評等服務

「單一客戶的 C&C 回呼數最多的裝置」Widget

此 Widget 顯示在選取的時間範圍內，特定客戶的前幾名 C&C 回呼偵測數最高的裝置。這些裝置透過伺服器位址以及裝置名稱（如果可行）識別。

重要

您必須先選取要監控的客戶，然後才能顯示 C&C 回呼偵測資料。

您可以按一下其中一個客戶選取連結，來選取要監控的客戶。在出現的「Widget 設定」畫面上，您可以選取要監控的客戶、變更 Widget 的標題，以及選擇要顯示的前幾名裝置數目。

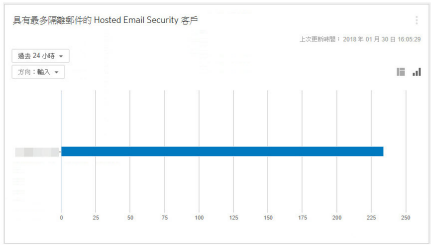
按一下「C&C 回呼偵測數」計數檢視事件記錄，或者按一下客戶名稱開啟「客戶 > [客戶]」畫面。可以按一下「請選取其他客戶」連結來選取新客戶。

Hosted Email Security Widget

資訊中心會顯示下列 Hosted Email Security Widget：

具有最多隔離郵件的 Hosted Email Security 客戶

顯示隔離郵件數最多的 Hosted Email Security 客戶。資料以表格和圓餅圖顯示。您可以按一下顯示圖示 ( )，在表格和圓餅圖之間切換。



- 您可以選取以下選項，變更所顯示資料的時間範圍：
  - 過去 24 小時

- 過去 7 天
- 過去 30 天（預設）

- 您可以選取以下選項，變更所顯示資料的方向類型：
  - 輸入
  - 輸出
- 按一下客戶名稱可檢視客戶資訊。
- 按一下郵件計數可檢視事件記錄。

具有最多安全威脅的 Hosted Email Security 客戶

顯示安全威脅事件數最多的 Hosted Email Security 客戶。資料以表格和圓餅圖顯示。您可以按一下顯示圖示 ( )，在表格和圓餅圖之間切換。

- 您可以選取以下選項，變更所顯示資料的時間範圍：
  - 過去 24 小時
  - 過去 7 天
  - 過去 30 天（預設）
- 您可以選取以下選項，變更所顯示資料的安全威脅類型：
  - 垃圾郵件

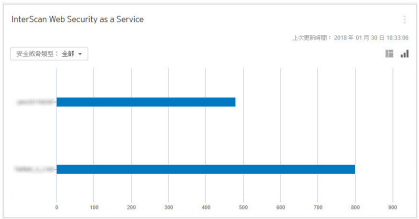
  - 病毒
  - 全部（預設）
- 您可以選取以下選項，變更所顯示資料的方向類型：
  - 輸入
  - 輸出
- 按一下客戶名稱可檢視客戶資訊。
- 按一下安全威脅計數可檢視事件記錄檔。

InterScan Web Security as a Service Widget

資訊中心會顯示下列 InterScan Web Security as a Service Widget：

「InterScan Web Security as a Service」Widget

顯示安全威脅事件數最多的 InterScan Web Security as a Service (IWSaaS) 客戶。資料以表格和橫條圖顯示。您可以按一下顯示圖示 ( )，在表格和橫條圖之間切換。



- 您可以選取以下選項，變更所顯示資料的安全威脅類型：
  - 全部
  - 間諜程式防護
  - 防毒
  - 應用程式控管
  - URL 過濾
  - 網頁信譽評等服務
- 按一下客戶名稱可檢視客戶資訊。

Worry-Free Business Security Services Widget

資訊中心會顯示下列 Worry-Free Business Security Services Widget：

Worry-Free Business Security Services Agent 狀態

此 Widget 顯示已離線或無法完成掃瞄一個月以上的 Worry-Free Business Security Services 裝置。

注意

此裝置計數僅包含已啟用預約掃瞄設定的 Worry-Free Business Security Services Agent。

按一下任何裝置計數可檢視事件記錄。

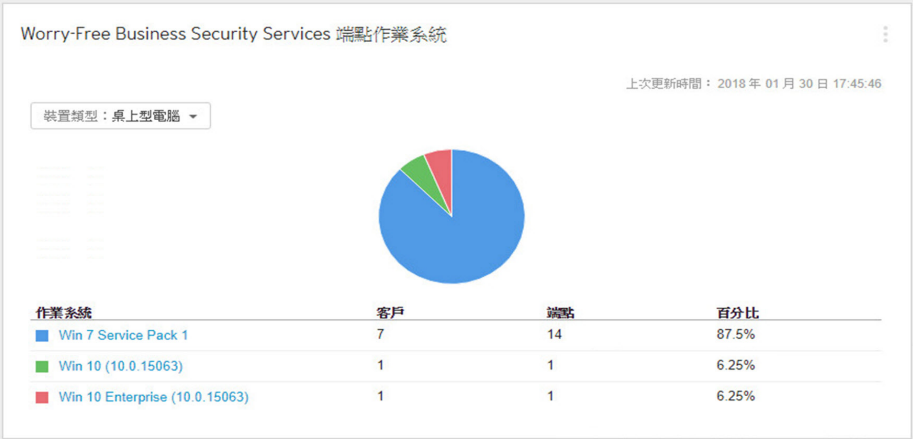
「具有最多安全威脅的 Worry-Free Business Security Services 客戶」Widget

此 Widget 顯示安全威脅事件數最多的 Worry-Free Business Security Services 客戶。

若要切換檢視，請按一下右上角的表格圖示或橫條圖圖示 ( )。

檢視	選項
表格	• 按一下「客戶」名稱可開啟「客戶 > [客戶]」畫面。
橫條圖	• 將游標懸停在橫條圖上可檢視針對特定客戶和產品的偵測數。 • 按一下任何橫條圖可檢視事件記錄。

Worry-Free Business Security Services 端點作業系統



此 Widget 顯示 Worry-Free Business Security Services 端點上使用的作業系統。

- 選取以下選項即可變更所顯示資料的裝置類型：
  - 桌上型電腦
  - 伺服器
  - 行動裝置
- 按一下表格或圓餅圖上的作業系統版本可檢視事件記錄檔。

通知中心

「通知中心」提供一種快速的方法來識別具有「需要採取處理行動」和「警告」事件的客戶。

透過「客戶通知中心」Widget 存取「通知中心」。

如需詳細資訊，請參閱「客戶通知中心」Widget 第 14-7 頁。

下表概述了「通知中心」畫面中，「需要採取處理行動」和「警告」標籤中提供的選項。

選項	說明
全部匯出	按一下此選項可匯出一個 CSV 檔案，裡面包含與有事件的客戶相關的所有資料。
解除	當您採取手動動作解決端點中受管理產品無法直接解決的問題後，會解除通知。 為支援的受管理產品選取一或多個事件，然後按一下「解除」，以從「通知中心」、相關的 Remote Manager Widget 和以下受管理的產品主控台（如果適用）移除事件資料： • Worry-Free Business Security • Worry-Free Business Security Services 注意 解除事件不會刪除與事件相關的任何記錄資料。Remote Manager 僅會解除事件通知資訊。
設定通知	按一下此選項可開啟「管理 > 設定通知」畫面，並可在 Remote Manager 中設定全域通知設定。 如需詳細資訊，請參閱設定全域通知設定 第 17-3 頁。
類型	選取表格中顯示的事件類型。 • 全部：顯示所有事件類型的通知 • 使用授權：只顯示使用授權通知 • 系統：只顯示系統通知 • 安全威脅：只顯示安全威脅通知
公司	按一下表格中的公司名稱，可開啟「客戶 > [客戶]」畫面，並可檢視與該特殊客戶相關的所有事件。 如需詳細資訊，請參閱客戶產品 第 3-3 頁。

選項	說明
出現次數	按一下「出現次數」計數可檢視特定事件的更多詳細資訊。 根據受管理的產品，事件詳細資訊顯示如下： • Worry-Free Business Security（Standard 或 Advanced）：會出現快顯畫面，概述特定事件所有出現次數的詳細資訊 • Worry-Free Business Security Services：隨即顯示「事件詳細資訊」畫面，顯示關於事件和建議的解析度動作的其他資訊。 如需詳細資訊，請參閱事件詳細資訊 第 14-34 頁。 • 所有其他受管理的產品：Remote Manager 會開啟受管理的產品主控台，您可以在這裡尋找關於事件的詳細資訊。

事件詳細資訊

「事件詳細資訊」畫面提供影響 Worry-Free Business Security Services 客戶的安全威脅和系統事件的更深入檢視。

下表概述了在「事件詳細資訊」畫面上提供的資訊。

資訊	說明
事件類型	顯示以下事件類型的圖示和說明： • 需要採取處理行動 • 警告
事件類別	介紹顯示的特定事件和子類別
說明	介紹與事件通知相關的問題和任何門檻值設定
建議的處理行動	提供對受管理產品無法直接解決之事件的建議

資訊	說明
動作按鈕	可用的動作因特定事件而異 可能的動作包括： • 「解除通知」：當您採取手動動作解決端點中受管理產品無法直接解決的問題後，會解除通知。 解除事件通知後，Remote Manager 會從「通知中心」、相關的 Remote Manager Widget 和 Worry-Free Business Security Services 主控台移除事件資料。 注意 解除事件不會刪除與事件相關的任何記錄資料。Remote Manager 僅會解除事件通知資訊。 • 「下載工具」：如果另一趨勢科技工具可用於協助解決安全威脅，請按一下以取得軟體套件。 注意 您必須在受影響的端點上手動執行此工具，才能解決安全威脅。 • 「啟用即時掃瞄」：按一下可在受影響的端點上自動啟用即時掃瞄服務。 • 「更新 Security Agent」：按一下可在受影響的過期端點上觸發更新程序。
受影響的端點清單	顯示受影響的端點清單以及與事件類別相關的特定事件資料

事件記錄檔

按一下資訊中心上顯示的各個 Widget 的計數後，會顯示「事件記錄檔」畫面。「事件記錄檔」提供特定客戶的受管理產品所報告偵測的詳細檢視。

您可以按一下「出現次數」計數，以取得關於特定事件類型的詳細資訊。視受管理產品而異，按一下「出現次數」計數會執行以下作業：

- 針對 Worry-Free Business Security 和 Worry-Free Business Security Services 事件：顯示「記錄查詢」畫面

  如需詳細資訊，請參閱執行記錄查詢 第 14-36 頁。

- 對於所有其他受管理的產品：開啟受管理的產品主控台，您可以在其中檢視受影響客戶的產品特定記錄

執行記錄查詢

Remote Manager 可讓您進一步調查下列產品的個別客戶事件記錄：

- Worry-Free Business Security (WFBS)
- Worry-Free Business Security Services (WFBSS)

程序

1. 移至「首頁」。
2. 按一下任何可用 Widget 上的事件偵測計數以顯示「事件記錄」畫面。
3. 按一下任何 Worry-Free Business Security 或 Worry-Free Business Security Services 客戶的「出現次數」計數。

   「記錄查詢」畫面會出現，顯示相關事件類別的詳細偵測資訊。

   注意

   按一下任何其他產品的「出現次數」計數會開啟受管理產品主控台，您可以在其中檢視受影響客戶的產品特定記錄。

4. （選用）檢視客戶的其他事件記錄資料。

   a. 從「期間」下拉式清單中，指定偵測資料的資料範圍。

   b. 從「類別」下拉式清單中，從可用的安全威脅類別中選取。如果已選取「勒索軟體」類別，則從可用的感染途徑中選取。

   c. 根據選取的「類別」而定，選取要檢視的「感染途徑」。

d. 按一下「顯示記錄檔」。

5. （選用）按一下「全部匯出」，以將資料儲存為 CSV 檔案。

第 15 章

管理事件

本節包含下列主題：

瞭解事件

Remote Manager 將事件定義為任何需要管理員注意的活動。提供的資訊因選取的產品和事件類型而異。

Remote Manager 提供兩種類型的事件清單。

表 15-1. Remote Manager 事件清單

清單	說明
事件記錄檔	顯示來自 Widget 的事件清單 Remote Manager 根據指定的範圍顯示所選取 Widget 的事件清單。根據 Widget，您可以選擇顯示過去 24 小時、7 天或 30 天的資訊。 如需詳細資訊，請參閱事件記錄檔 第 14-35 頁。
產品特定事件	顯示即時事件的清單 Remote Manager 與支援的產品同步，每 5 分鐘會重新整理清單。 注意 如需詳細資訊，請參閱檢視特定產品的事件 第 14-21 頁。

事件嚴重性

產品特定事件可能具有以下任一嚴重性層級。

- 需要採取處理行動：需要立即注意的事件。
- 警告：發出警告但不需要立即注意的通知。

事件狀態

產品特定事件可能具有以下任一狀態。

- 未解決：需要注意的事件。
- 解除/立即更新：已解決但仍需要產品或服務更新的事件。

受管理的產品事件

Remote Manager 事件因每個受管理產品/服務而異。

- Cloud App Security 事件 第 15-3 頁
- Cloud Edge 事件 第 15-4 頁
- InterScan Web Security as a Service 事件 第 15-7 頁
- Worry-Free Business Security 事件 第 15-7 頁
- Worry-Free Business Security Services 事件 第 15-10 頁

Cloud App Security 事件

注意

如果發生多個「需要採取處理行動」和「警告」事件，Remote Manager 會針對最嚴重的安全威脅顯示 圖示。

表 15-2. 安全威脅事件

事件類別	詳細資訊	事件狀態
防毒	病毒偵測數超過	：在 1 小時內偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
檔案封鎖	檔案封鎖違規數超過	：在 1 小時內偵測到的檔案封鎖違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

事件類別	詳細資訊	事件狀態
沙盒虛擬平台	沙盒虛擬平台「高風險」偵測數超過	：在 1 小時內偵測到的「高風險」物件的沙盒虛擬平台偵測計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
	沙盒虛擬平台「中/低風險」偵測數超過	：在 1 小時內偵測到的「中/低風險」物件的沙盒虛擬平台偵測計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網頁信譽評等服務	URL 違規數超過	：在 1 小時內偵測到的網頁信譽評等服務違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

表 15-3. 系統事件

事件類別	詳細資訊	事件狀態
帳號同步問題	Box 存取 Token 無效	：無法存取指定的雲端儲存
	Dropbox 存取 Token 無效	：無法存取指定的雲端儲存
	Google 雲端硬碟存取 Token 無效	：無法存取指定的雲端儲存
	委派帳號的同步問題	：無法與委派帳號同步

Cloud Edge 事件

注意

Cloud Edge 中的某些安全威脅事件可能會顯示額外的途徑資訊。

表 15-4. 安全威脅事件

事件類別	詳細資訊	事件狀態
垃圾郵件防護	垃圾郵件偵測數	：過去一小時偵測到的垃圾郵件計數
防毒	病毒偵測數	：過去一小時偵測到的病毒/惡意程式計數
殭屍網路	殭屍網路偵測數	：過去一小時偵測到的殭屍網路計數
C&C 回呼	C&C 回呼數	：過去一小時偵測到的 C&C 回呼計數
IPS	IPS 偵測數	：過去一小時偵測到的 IPS 計數
Machine Learning	未知的安全威脅偵測數	：過去一小時偵測到的未知安全威脅計數
勒索軟體	勒索軟體偵測數	：過去一小時偵測到的勒索軟體計數
沙盒虛擬平台	沙盒虛擬平台偵測數	：過去一小時偵測到的沙盒虛擬平台偵測計數
網頁信譽評等服務	URL 違規數	：過去一小時偵測到的封鎖的 URL 計數
網頁安全威脅	網頁安全威脅偵測數 (包括 IPS、殭屍網路、防毒或網頁信譽評等服務違規數)	：過去一小時偵測到的網頁安全威脅計數

表 15-5. 系統事件

事件類別	詳細資訊	事件狀態
雲端電子郵件掃瞄	服務無法使用	：Cloud Edge 無法連線至雲端掃瞄服務
	在過去 24 小時內服務已變為暫時無法使用	：Cloud Edge 在過去 24 小時內暫時無法連線至雲端掃瞄服務

事件類別	詳細資訊	事件狀態
韌體更新	上一次韌體更新失敗。如需詳細資訊，請開啟 <Cloud Edge 雲端主控台>。	：Cloud Edge 韌體無法成功更新至最新的韌體版本
	過期的韌體	：Cloud Edge 韌體的目前版本已過期
離線	離線閘道。可能會影響策略部署和記錄檔分析。	：Cloud Edge 無法連線至閘道或執行掃瞄
離線 (過去 24 小時)	過去 24 小時內的離線閘道出現次數。可能已影響策略部署和記錄檔分析。	：Cloud Edge 超過 24 小時無法保持與所有註冊閘道的專用連線
資源短缺	偵測到 <數目> 個問題 • 磁碟空間使用率已超過 • CPU 使用率已超過 • 記憶體使用率已超過	：裝置上剩餘的資源量已低於設定的警訊門檻值。
資源短缺 (過去 24 小時)	偵測到 <數目> 個問題 • 磁碟空間使用率已超過 • CPU 使用率已超過 • 記憶體使用率已超過	：過去 24 小時內裝置上剩餘的資源量已低於設定的警訊門檻值，但已恢復
未註冊	無法執行雲端管理。此閘道未註冊到 Cloud Edge 雲端主控台。	：Cloud Edge 無法在閘道上執行掃瞄

InterScan Web Security as a Service 事件

表 15-6. 安全威脅事件

事件類別	詳細資訊	事件狀態
間諜程式防護	間諜程式/可能的資安威脅程式偵測	：過去 24 小時偵測到的間諜程式/可能的資安威脅程式計數
防毒	病毒偵測數	：過去 24 小時偵測到的病毒/惡意程式計數
應用程式控管	應用程式控管違規數	：過去 24 小時偵測到的應用程式控管違規計數
URL 過濾	URL 違規數	：過去 24 小時偵測到的 URL 過濾違規計數
網頁信譽評等服務	URL 違規數	：過去 24 小時偵測到的封鎖的 URL 計數

表 15-7. 系統事件

事件類別	詳細資訊	事件狀態
帳號同步問題	AD/LDAP 的同步問題	：無法與 AD/LDAP 同步

Worry-Free Business Security 事件

表 15-8. 安全威脅事件

事件類別	詳細資訊	事件狀態
垃圾郵件防護	收到的所有郵件中的垃圾郵件偵測數超過	：在 1 小時內偵測到的垃圾郵件數與所收到總郵件數的比率超過了設定的門檻值（如在受管理的產品主控台上所設定）

事件類別	詳細資訊	事件狀態
間諜程式防護	需要重新啟用裝置的偵測數	：顯示感染受管理產品無法完全清除而需要客戶重新啟用端點才能完成清除程序的間諜程式/可能的資安威脅程式的端點數
	間諜程式/可能的資安威脅程式偵測數超過	：在 1 小時內偵測到的間諜程式/可能的資安威脅程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
防毒	端點已關閉即時掃瞄	：已關閉即時掃瞄的 Security Agent 無法保護端點免於新建立或執行之檔案中的病毒/惡意程式侵害
	Exchange 伺服器已關閉即時掃瞄	：已關閉即時掃瞄的 Exchange 伺服器可允許傳送電子郵件中的所有附件，使得客戶網路容易受到大量郵件蠕蟲攻擊。
	未解決的安全威脅	：不成功的動作表示病毒或惡意程式已成功規避防毒並已使端點中毒。 注意 Remote Manager 假設未成功清除、隔離或刪除病毒或惡意程式的電腦已中毒。
	端點上的病毒偵測數超過	：在 1 小時內在端點上偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
	Exchange 伺服器上的病毒偵測數超過	：在 1 小時內在 Exchange 伺服器上偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
行為監控	行為監控違規數超過	：在 1 小時內偵測到的行為監控違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

事件類別	詳細資訊	事件狀態
週邊設備存取控管	週邊設備存取控管違規數超過	：在 1 小時內偵測到的週邊設備存取控管違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網路病毒	網路病毒偵測數超過	：在 1 小時內偵測到的網路病毒計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
疫情爆發防範	疫情爆發防範已啟用	：已在桌面/伺服器平台上啟用疫情爆發防範，來應對異常安全威脅活動
	疫情爆發防範已關閉	：已在桌面/伺服器平台上關閉疫情爆發防範，並已恢復正常的網路狀況
Machine Learning	超過未知的安全威脅偵測數	：在 1 小時內偵測到的未知安全威脅數計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
URL 過濾	URL 違規數超過	：在 1 小時內偵測到的 URL 過濾違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網頁信譽評等服務	URL 違規數超過	：在 1 小時內偵測到的網頁信譽評等服務違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

表 15-9. 系統事件

事件類別	詳細資訊	事件狀態
資源短缺	剩餘如下磁碟空間	：伺服器上剩餘的磁碟空間量已低於設定的警訊門檻值。
主動式雲端截毒技術服務	服務無法使用	：Worry-Free Business Security 主控台無法連線至雲端截毒伺服器

事件類別	詳細資訊	事件狀態
更新	過期的 Agent	：超過 <數目> 個 Security Agent 在過去一小時內未收到最新的防毒病毒碼
	過期的 Exchange 伺服器	：在 Exchange 伺服器上偵測到過期的元件

Worry-Free Business Security Services 事件

表 15-10. 安全威脅事件

事件類別	詳細資訊	事件狀態
間諜程式防護	需要重新啟用裝置的偵測數	：顯示感染受管理產品無法完全清除而需要客戶重新啟用端點才能完成清除程序的間諜程式/可能的資安威脅程式的端點數
	間諜程式/可能的資安威脅程式偵測數超過	：在 1 小時內偵測到的間諜程式/可能的資安威脅程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
防毒	即時掃瞄已關閉	：已關閉即時掃瞄的 Security Agent 無法保護端點免於新建立或執行之檔案中的病毒/惡意程式侵害
	未解決的安全威脅	：不成功的動作表示病毒或惡意程式已成功規避防毒並已使端點中毒。 注意 Remote Manager 假設未成功清除、隔離或刪除病毒或惡意程式的電腦已中毒。
	病毒偵測數超過	：在 1 小時內偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

事件類別	詳細資訊	事件狀態
應用程式控管	應用程式控管違規數超過	：在 1 小時內偵測到的應用程式控管違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
行為監控	行為監控違規數超過	：在 1 小時內偵測到的行為監控違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
週邊設備存取控管	週邊設備存取控管違規數超過	：在 1 小時內偵測到的週邊設備存取控管違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網路病毒	網路病毒偵測數超過	：在 1 小時內偵測到的網路病毒計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
疫情爆發防範	疫情爆發防範已啟用	：已在桌面/伺服器平台上啟用疫情爆發防範，來應對異常安全威脅活動
	疫情爆發防範已關閉	：已在桌面/伺服器平台上關閉疫情爆發防範，並已恢復正常的網路狀況
Machine Learning	超過未知的安全威脅偵測數	：在 1 小時內偵測到的未知安全威脅數計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
URL 過濾	URL 違規數超過	：在 1 小時內偵測到的 URL 過濾違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網頁信譽評等服務	URL 違規數超過	：在 1 小時內偵測到的網頁信譽評等服務違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

表 15-11. 系統事件

事件類別	詳細資訊	事件狀態
主動式雲端截毒技術服務	中斷連線的 Agent 數目	：Security Agent 無法連線至主動式雲端截毒技術
更新	過期的 Agent	：防毒病毒碼發佈的兩個小時後過期的病毒碼超過門檻值的 Security Agent 數

檢視特定產品的事件

特定產品的事件顯示即時事件的清單。

程序

1. 移至「客戶 > {公司名稱} > {產品}」。
2. 請根據選取的產品執行下列其中一項動作。

產品	步驟
Cloud App Security	移至「事件」標籤。
Cloud Edge	移至「事件」標籤。
InterScan Web Security as a Service	從網路樹狀結構中選取 IWSaaS 產品時，會自動顯示事件清單。
Worry-Free Business Security	移至「事件」標籤。
Worry-Free Business Security Services	移至「事件」標籤。

第 16 章

管理報告

本節包含下列主題：

報告總覽

Trend Micro Remote Manager 可讓您產生、下載並自動傳送報告。報告提供使用授權狀態、評估結果、安全威脅事件、重大安全威脅，以及客戶網路中大部分受影響的電腦、檔案和電子郵件信箱的總覽。

報告包括 Worry-Free Business Security（全部）和 Hosted Email Security 中的統計資料範圍。Remote Manager 允許報告描述檔、一次性和定期報告、日期範圍和多個電子郵件收件者。Remote Manager 會儲存 30 份最新的每日報告、10 份最新的每週報告和 5 份最新的每月報告。一般報告適合經銷商和客戶。詳細報告適合經銷商和合作夥伴。

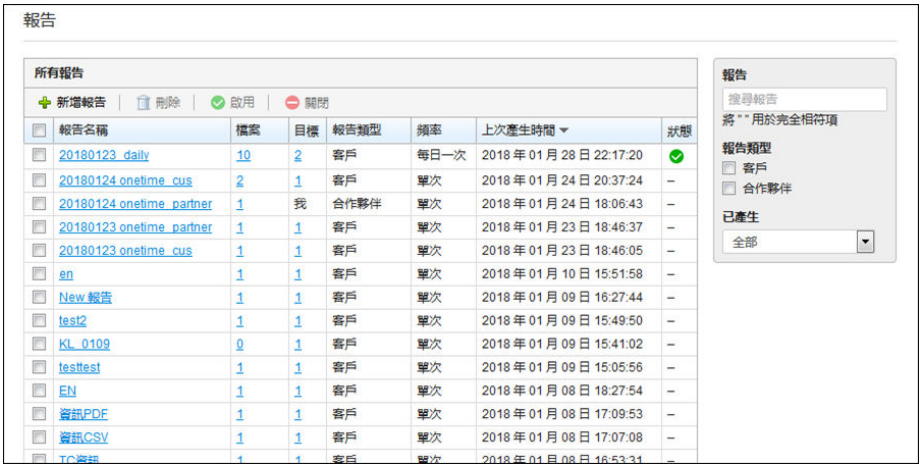


圖 16-1. 報告頁面

報告描述檔可讓您透過單一描述檔建立多個報告。例如，今天建立一個一次性報告、產生該報告，明天變更某些選項並重新產生，而不必重新建立整個報告。Remote Manager 目前支援一般報告和詳細報告。

建立報告

Trend Micro Remote Manager 提供以下報告範本建立方法：

- 按一下現有報告、修改該報告，然後按一下畫面底部的「儲存」。
- 建立新報告範本。如需詳細資訊，請參閱建立報告範本 第 16-3 頁。

建立報告範本

程序

1. 移至「報告 > 新增報告」。

「新增報告」視窗隨即開啟。

2. 指定下列項目：
   - 報告名稱
   - 「報告類型」：如需詳細資訊，請參閱報告總覽 第 16-2 頁。
3. 選取日期範圍：
   - 一次性報告

選項	說明
過去 24 小時	使用午夜 12 點到產生報告時（根據所選時區）所收到的資料計算報告。 注意 報告使用的時區為經銷商在建立描述檔時所選取的時區。該時區並非由客戶電腦所確定。
過去 7 天	使用過去 7 天的資料（不包括當日的資料）計算報告。
過去 30 天	使用過去 30 天的資料（不包括當日的資料）計算報告。
自訂範圍	「開始」日期不得早於上個月的第一天（Remote Manager 僅儲存上個月和當月的資料）；「結束」日期不得晚於當日日期。

- 週期性報告

選項	說明
每日報告	結束日期必須晚於當日日期。然後會在指定日期範圍內的每天，根據前一日的資料產生報告。 例如，如果設定的範圍是 2009 年 1 月 27 日至 2009 年 1 月 29 日，則： • 在 27 日，Remote Manager 會根據 26 日的資料產生報告 • 在 28 日，Remote Manager 會根據 27 日的資料產生報告 • 在 29 日，Remote Manager 會根據 28 日的資料產生報告
每週報告	Remote Manager 會在每個月使用上一週的資料產生每週報告。因此，若要產生本週的報告，請至少將結束日期設定為下週的星期一。

選項	說明
每月報告	Remote Manager 會在每個月結束第二天使用上個月的資料產生每月報告。因此，若要產生本月的報告，請至少將結束日期設定為下個月的第二天。

4. 指定以下報告格式元素：

選項	說明
報告格式	報告可以匯出為 PDF 或 CSV 檔案。
報告語言	Trend Micro Remote Manager 支援英文、法文、德文、義大利文、日文、簡體中文和西班牙文。
附註	此資訊僅供內部使用，不會顯示在報告中。

5. 按「下一步」。

   隨即顯示「選取報告資料」畫面。

6. 選取報告範本和要產生的資料。

   注意

   如果經銷商未連線至客戶的伺服器，或資料無法使用，則不會向客戶顯示資料。

7. 按「下一步」。

   隨即顯示「為特定客戶產生報告」畫面。

8. 選取將產生此報告的客戶。

9. 指定電子郵件報告詳細資訊。「郵寄地址」選項下的收件者來自公司聯絡人清單。您也可以新增電子郵件信箱，來接收所產生的報告。

   注意

   選取的每位客戶都將具有不同的電子郵件收件者。您可以根據客戶新增或刪除電子郵件收件者。

10. 選用：選取「啟用」以顯示客戶的標誌。
11. 按一下「完成」。

    Remote Manager 會將該範本新增至報告範本清單。

檢視報告

報告必須至少已產生一次，才能檢視。

移至「報告 > {報告名稱} > 報告檔案（標籤） > {檢視下的檔案}」。

如需詳細資訊，請參閱報告總覽 第 16-2 頁。

編輯報告

移至「報告 > {報告名稱}」。

如需詳細資訊，請參閱建立報告範本 第 16-3 頁。

下載並傳送報告

您可以下載報告並傳送給收件者。雖然收件者在您定義報告時指定，但可以修改收件者。

程序

1. 移至「報告 > {報告文件下的項目或項目數} > {檢視下的報告}」。
2. 選取您要傳送或下載的報告。
3. 按一下「傳送」或「下載」。

如需詳細資訊，請參閱訂閱報告 第 16-8 頁。

訂閱報告

程序

1. 移至「報告 > {報告名稱} > 目標受眾（標籤） > 新增目標」。
2. 選取客戶報告。

注意

建立報告時的電子郵件收件者清單來自「聯絡人」詳細資訊。

3. 根據需要修訂主旨行。
4. 按一下「儲存」。

部分 VI

管理 Remote Manager

第 17 章

管理 Remote Manager

注意

如需關於第三方產品整合的資訊，請參閱部分 IV：整合第三方解決方案。

本節包含下列主題：

管理設定

使用「管理」畫面，您可以設定全域客戶設定、Remote Manager 主控台設定、檢視和設定第三方軟體整合，以及檢視系統記錄檔。

區段	說明
系統設定	• 「設定通知」：可讓您設定全域通知設定 秘訣 趨勢科技建議您在設定全域通知設定時，將這些設定套用至您的大多數客戶。全域設定可以快速設定個別客戶的通知，雖然您也可以針對每個客戶自訂通知設定。 如需詳細資訊，請參閱設定全域通知設定 第 17-3 頁。 • 「主控台設定」：可讓您變更 Remote Manager 主控台上顯示的橫幅影像 如需詳細資訊，請參閱設定主控台設定 第 17-17 頁。
第三方整合	• 檢視與第三方軟體整合之 Remote Manager 功能的目前狀態 • 「設定第三方整合」：可讓您啟用與支援的第三方軟體的整合，並設定全域整合設定 如需詳細資訊，請參閱部分 IV：整合第三方解決方案 第 1 頁。 • 產生 API 金鑰：讓您產生或撤銷 API 金鑰（存取 Token 和機密金鑰），用來整合 Remote Manager 與第三方程式 如需詳細資訊，請參閱產生 API 金鑰 第 17-17 頁。

區段	說明
產品/服務的預設設定	「設定預設設定範本」：可讓您設定整個受管理產品/服務主控台設定，以便套用至新客戶或現有客戶 秘訣 設定範本可以預先設定受管理產品的安全策略和例外清單，供您稍後套用至多個客戶，有助於節省您的時間。 重要 Remote Manager 僅支援 Worry-Free Business Security Services 和 Cloud Edge 的預設設定範本。 如需詳細資訊，請參閱預設設定範本 第 17-18 頁。
系統記錄檔	「管理記錄檔」：顯示使用者對 Remote Manager 主控台所做變更的相關設定 如需詳細資訊，請參閱檢視管理記錄檔 第 17-21 頁。

設定全域通知設定

設定全域通知，以監控可能需要注意的常見事件。Remote Manager 透過電子郵件、「客戶通知中心」Widget 或您的第三方軟體提供通知。

秘訣

趨勢科技建議您在設定全域通知設定時，將這些設定套用至您的大多數客戶。全域設定可以快速設定個別客戶的通知，雖然您也可以針對每個客戶自訂通知設定。

程序

1. 移至「管理」。
2. 在「系統設定」區段中，按一下「設定通知」。

隨即顯示「管理 > 設定通知」畫面。

3. 在「電子郵件設定」區段中，指定接收通知電子郵件的「收件者」。

   - 「帳號管理員」：選取授權管理帳號做為應接收所有客戶之電子郵件通知的主要 Remote Manager 管理員。
   - 「其他收件者」：手動輸入 Remote Manager 應聯絡之其他人員的電子郵件信箱。

   注意

   請使用分號 (;) 分隔多個項目。

4. 在「電子郵件設定」區段中，指定通知電子郵件中顯示的「郵件內容」。

選項	說明	可能的通知
向所有客戶各傳送一封包含所有「需要採取處理行動」和所有「警告」事件的合併電子郵件	Remote Manager 會合併所有客戶的所有「需要採取處理行動」事件和所有「警告」事件，並在 Remote Manager 伺服器每次與受管理產品伺服器通訊時，針對每個安全層級以及所有事件的摘要傳送一封電子郵件。 **注意** 按一下「編輯主旨序言」，可指定要顯示為電子郵件主旨行開頭文字的自訂序言。	• 向每個受管理產品的所有客戶各傳送一封包含所有「需要採取處理行動」事件的合併電子郵件 • 向每個受管理產品的所有客戶各傳送一封包含所有「警告」事件的合併電子郵件 • 根據「事件通知設定」中的設定，針對所有使用授權事件傳送單獨的電子郵件

選項	說明	可能的通知
針對所有「警告」事件傳送一封合併電子郵件，但針對每個客戶的每個「需要採取處理行動」事件傳送單獨的電子郵件	Remote Manager 會合併所有客戶的所有「警告」事件，並在 Remote Manager 伺服器每次與受管理產品伺服器通訊時，針對所有「警告」事件的摘要傳送一封電子郵件。Remote Manager 還會在受管理產品每次報告任何客戶的「需要採取處理行動」事件時，傳送一封新電子郵件。 **注意** 按一下「編輯警告主旨序言」，可針對合併的「警告」事件郵件，指定要顯示為電子郵件主旨行開頭文字的自訂序言。	• 針對每個客戶的每個「需要採取處理行動」事件傳送單獨的電子郵件 • 向每個受管理產品的所有客戶各傳送一封包含所有「警告」事件的合併電子郵件 • 根據「事件通知設定」中的設定，針對所有使用授權事件傳送單獨的電子郵件
針對每個客戶的每個「需要採取處理行動」和「警告」事件傳送單獨的電子郵件	Remote Manager 會在受管理產品每次報告任何客戶的「警告」或「需要採取處理行動」事件時，傳送一封新電子郵件。	• 針對每個客戶的每個「需要採取處理行動」事件傳送單獨的電子郵件 • 針對每個客戶的每個「警告」/「資訊」事件傳送單獨的電子郵件 • 根據「事件通知設定」中的設定，針對所有使用授權事件傳送單獨的電子郵件

重要

您可以針對每個 Worry-Free Business Security Services 和 Cloud Edge「警告」事件和「需要採取處理行動」事件，自訂個別電子郵件內容，方法是在選取此選項後，在「事件通知設定」中按一下事件名稱。

5. 在「電子郵件設定」區段中的「語言」下，選取 Remote Manager 在傳送電子郵件通知時所使用的語言。

6. 在「電子郵件設定」區段中的「每日通知摘要」下，啟用「傳送每日通知摘要」選項，以便接收每日電子郵件報告，其中彙總了所有客戶每日的所有使用授權事件、系統事件和安全威脅事件。

秘訣

按一下「檢視範例」連結，以顯示 Remote Manager 所傳送圓餅圖和表格資料的預覽。

7. 在「事件通知設定」區段中，設定 Remote Manager 如何傳送特定產品和事件類型的通知。

- 一般設定：
  - 「在通知中顯示」：選取該核取方塊，以在「客戶通知中心」Widget 和「通知中心」畫面中顯示通知事件
  - 「電子郵件」：選取該核取方塊，讓 Remote Manager 在每次發生事件時傳送電子郵件（依據「郵件內容」設定）
  - 「警訊門檻值」：如果可以，請指定事件的門檻值設定

注意

請使用每個客戶的 Worry-Free Business Security Services Web 主控台，設定 Worry-Free Business Security Services 的門檻值設定。

- 通知產品和事件類型：通知事件因每個產品和事件類型而異。請參閱以下清單，瞭解與每個區段相關的特定資訊：

區段	說明
所有使用授權事件	從提供的清單中選取您想監控的特定事件類型。 注意 Remote Manager 會傳送一封單獨的合併電子郵件，其中包含所有客戶的所有使用授權通知。 如需有關通知事件的詳細資訊，請參閱使用授權通知 第 17-10 頁。

區段	說明
Worry-Free Business Security Services	從提供的清單中選取您想監控的特定事件類型。 如需有關通知事件的詳細資訊，請參閱 Worry-Free Business Security Services 通知 第 17-10 頁。 重要 啟用「請不要將受管理產品中的通知傳送給 Remote Manager 收件者」，以減少「電子郵件設定」中的「收件者」區段中指定的收件者所收到的重複電子郵件數量。Remote Manager 會比較「電子郵件設定」中的收件者與在 Worry-Free Business Security Services 主控台上針對每個客戶設定的收件者。如果電子郵件信箱同時顯示在兩個清單中，則 Remote Manager 會封鎖傳送至重複電子郵件信箱的 Worry-Free Business Security Services 通知。 秘訣 如果您在「郵件內容」區段中，選取針對「警告」或「需要採取處理行動」事件接收單獨的電子郵件，可以按一下事件名稱以自訂電子郵件內容。 如需詳細資訊，請參閱自訂電子郵件通知內容 第 17-8 頁。
Worry-Free Business Security	您僅可針對「安全威脅」與「系統」事件類型，選取是否接收通知。 如需有關通知事件的詳細資訊，請參閱 Worry-Free Business Security 通知 第 17-12 頁。
Cloud App Security	您僅可針對「安全威脅」與「系統」事件類型，選取是否接收通知。 如需有關通知事件的詳細資訊，請參閱 Cloud App Security 通知 第 17-14 頁。

區段	說明
Cloud Edge	從提供的清單中選取您想監控的特定事件類型。 如需有關通知事件的詳細資訊，請參閱 Cloud Edge 通知 第 17-15 頁。 重要 對於「資訊」事件類型，Remote Manager 會根據在「郵件內容」區段中設定的「警告」事件設定傳送通知。 秘訣 如果您在「郵件內容」區段中，選取針對「警告」或「需要採取處理行動」事件接收單獨的電子郵件，可以按一下事件名稱以自訂電子郵件內容。 如需詳細資訊，請參閱自訂電子郵件通知內容 第 17-8 頁。
InterScan Web Security as a Service	您僅可針對「系統」事件類型，選取是否接收通知。 如需有關通知事件的詳細資訊，請參閱 InterScan Web Security as a Service 通知 第 17-17 頁。

8. 按一下「儲存」。

注意

按一下「還原成預設值」，即可將所有全域通知設定還原成預設設定。

自訂電子郵件通知內容

如果您在「郵件內容」區段中，選取針對「警告」或「需要採取處理行動」事件接收單獨的電子郵件，可以按一下事件名稱以自訂電子郵件內容。

如需詳細資訊，請參閱設定全域通知設定 第 17-3 頁。

重要

自訂電子郵件範本僅可用於 Worry-Free Business Security Services 和 Cloud Edge 事件。

秘訣

按一下「預覽範例」連結，以在開始自訂通知內容之前瞭解通知郵件的配置。

程序

1. 在「主旨」欄位中：
   - 從「變數清單」中拖放欄位，以新增動態更新的資料。

     重要

     僅在使用 Chrome 或 Firefox 瀏覽器時支援拖放功能。
   - 手動鍵入靜態文字，以提高可讀性。
2. 在「內容」欄位中：
   - 從「變數清單」清單中拖放欄位，以新增動態更新的資料。
   - 手動鍵入靜態文字，以提高可讀性。
   - 使用可用的編輯工具列按鈕格式化郵件內容。
3. 按一下「儲存」。

使用授權通知

事件	頻率	警訊門檻值
使用授權 - 即將到期	選取下列選項： • 「每 7 天」：自到期前 14 天開始，系統每 7 天傳送一次電子郵件通知。 • 「每 14 天」：自到期前 28 天開始，系統每 14 天傳送一次電子郵件通知。 • 「每 30 天」：自到期前 60 天開始，系統每 30 天傳送一次電子郵件通知。	Remote Manager 會根據「頻率」設定顯示「警訊門檻值」： • 「每 7 天」：使用授權將在 14 天後到期 • 「每 14 天」：使用授權將在 28 天後到期 • 「每 30 天」：使用授權將在 60 天後到期
使用授權 - 已到期	依事件 如果有已過期的使用授權，則會傳送通知	不適用
使用授權 - 已超過配置	依事件 如果已使用授權所佔的百分比超過已佈建的授權數目，則會傳送通知	配置超過 (%)：<數目> 注意 您可以指定超過客戶所佈建授權數的已使用授權的百分比。這可以是介於 100 到 120 之間的任何值。

Worry-Free Business Security Services 通知

重要

對於具有可設定門檻值的事件，您必須在 Worry-Free Business Security Services 主控台上單獨為每個客戶設定門檻值。

表 17-1. 安全威脅事件

事件	詳細資訊
防毒 - 未解決的安全威脅	：不成功的動作表示病毒或惡意程式已成功規避防毒並已使端點中毒。 注意 Remote Manager 假設未成功清除、隔離或刪除病毒或惡意程式的電腦已中毒。
防毒 - 即時掃瞄已關閉	：已關閉即時掃瞄的 Security Agent 無法保護端點免於新建立或執行之檔案中的病毒/惡意程式侵害
防毒 - 病毒偵測數超過	：在 1 小時內偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
間諜程式防護 - 需要重新啟用裝置的偵測數	：顯示感染受管理產品無法完全清除而需要客戶重新啟用端點才能完成清除程序的間諜程式/可能的資安威脅程式的端點數
間諜程式防護 - 間諜程式/可能的資安威脅程式偵測數超過	：在 1 小時內偵測到的間諜程式/可能的資安威脅程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網頁信譽評等服務 - URL 違規數超過	：在 1 小時內偵測到的網頁信譽評等服務違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
URL 過濾 - URL 違規數超過	：在 1 小時內偵測到的 URL 過濾違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
Machine Learning - 超過未知的安全威脅偵測數	：在 1 小時內偵測到的未知安全威脅數計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
行為監控 - 行為監控違規數超過	：在 1 小時內偵測到的行為監控違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網路病毒 - 網路病毒偵測數超過	：在 1 小時內偵測到的網路病毒計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

事件	詳細資訊
週邊設備存取控管 - 週邊設備存取控管違規數超過	：在 1 小時內偵測到的週邊設備存取控管違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
應用程式控管 - 應用程式控管違規數超過	：在 1 小時內偵測到的應用程式控管違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

表 17-2. 系統事件

事件	詳細資訊
更新 - 過期的 Agent	：防毒病毒碼發佈的兩個小時後過期的病毒碼超過門檻值的 Security Agent 數
主動式雲端截毒技術服務 - Agent 已中斷連線	：Security Agent 無法連線至主動式雲端截毒技術

Worry-Free Business Security 通知

表 17-3. 安全威脅事件

事件	詳細資訊
垃圾郵件防護 - 收到的所有郵件中的垃圾郵件偵測數超過	：在 1 小時內偵測到的垃圾郵件數與所收到總郵件數的比率超過了設定的門檻值（如在受管理的產品主控台上所設定）
間諜程式防護 - 需要重新啟用裝置的偵測數	：顯示感染受管理產品無法完全清除而需要客戶重新啟用端點才能完成清除程序的間諜程式/可能的資安威脅程式的端點數
間諜程式防護 - 間諜程式/可能的資安威脅程式偵測數超過	：在 1 小時內偵測到的間諜程式/可能的資安威脅程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
防毒 - 關閉即時掃瞄的端點數	：已關閉即時掃瞄的 Security Agent 無法保護端點免於新建立或執行之檔案中的病毒/惡意程式侵害

事件	詳細資訊
防毒 - 關閉即時掃瞄的 Exchange 伺服器數	：已關閉即時掃瞄的 Exchange 伺服器可允許傳送電子郵件中的所有附件，使得客戶網路容易受到大量郵件蠕蟲攻擊。
防毒 - 未解決的安全威脅	：不成功的動作表示病毒或惡意程式已成功規避防毒並已使端點中毒。 注意 Remote Manager 假設未成功清除、隔離或刪除病毒或惡意程式的電腦已中毒。
防毒 - 端點上的病毒偵測數超過	：在 1 小時內在端點上偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
防毒 - Exchange 伺服器上的病毒偵測數超過	：在 1 小時內在 Exchange 伺服器上偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
行為監控 - 行為監控違規數超過	：在 1 小時內偵測到的行為監控違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
週邊設備存取控管 - 週邊設備存取控管違規數超過	：在 1 小時內偵測到的週邊設備存取控管違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網路病毒 - 網路病毒偵測數超過	：在 1 小時內偵測到的網路病毒計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
Machine Learning - 超過未知的安全威脅偵測數	：在 1 小時內偵測到的未知安全威脅數計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
URL 過濾 - URL 違規數超過	：在 1 小時內偵測到的 URL 過濾違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
網頁信譽評等服務 - URL 違規數超過	：在 1 小時內偵測到的網頁信譽評等服務違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

表 17-4. 系統事件

事件	詳細資訊
資源短缺 - 剩餘如下磁碟空間	：伺服器上剩餘的磁碟空間量已低於設定的警訊門檻值。
主動式雲端截毒技術服務 - 服務無法使用	：Worry-Free Business Security 主控台無法連線至雲端截毒伺服器
更新 - 過期的 Exchange 伺服器	：在 Exchange 伺服器上偵測到過期的元件
更新 - 過期的 Agent	：超過 <數目> 個 Security Agent 在過去一小時內未收到最新的防毒病毒碼

Cloud App Security 通知

表 17-5. 安全威脅事件

事件	詳細資訊
防毒 - 病毒偵測數超過	：在 1 小時內偵測到的病毒/惡意程式計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
檔案封鎖 - 檔案封鎖違規數超過	：在 1 小時內偵測到的檔案封鎖違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
勒索軟體 - 勒索軟體偵測數超過	：在 1 小時內偵測到的勒索軟體計數超過了設定的門檻值（如在受管理的產品主控台上所設定）
沙盒虛擬平台 - 沙盒虛擬平台偵測數超過	：在 1 小時內偵測到的「低風險」或「中風險」物件的沙盒虛擬平台偵測計數超過了設定的門檻值（如在受管理的產品主控台上所設定） ：在 1 小時內偵測到的「高風險」物件的沙盒虛擬平台偵測計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

事件	詳細資訊
網頁信譽評等服務 - URL 違規數超過	：在 1 小時內偵測到的網頁信譽評等服務違規計數超過了設定的門檻值（如在受管理的產品主控台上所設定）

表 17-6. 系統事件

事件	詳細資訊
帳號同步問題 - Box 存取 Token 無效	：無法存取指定的雲端儲存
帳號同步問題 - Dropbox 存取 Token 無效	：無法存取指定的雲端儲存
帳號同步問題 - Google 雲端硬碟存取 Token 無效	：無法存取指定的雲端儲存
帳號同步問題 - 委派帳號的同步問題	：無法與委派帳號同步

Cloud Edge 通知

表 17-7. 安全威脅事件

事件	詳細資訊	警訊門檻值
網頁安全威脅 - 網頁安全威脅偵測數超過	：在 1 小時內偵測到的網頁安全威脅數計數超過了設定的門檻值（如在 Remote Manager 主控台上所設定）	請指定介於 1 到 300 之間的值。
C&C 回呼 - C&C 回呼偵測數超過	：在 1 小時內偵測到的 C&C 回呼計數超過了設定的門檻值（如在 Remote Manager 主控台上所設定）	請指定介於 1 到 100 之間的值。

事件	詳細資訊	警訊門檻值
勒索軟體 - 勒索軟體偵測數超過	：在 1 小時內偵測到的勒索軟體計數超過了設定的門檻值（如在 Remote Manager 主控台上所設定）	請指定介於 1 到 100 之間的值。

表 17-8. 系統事件

事件	詳細資訊	警訊門檻值
離線 - 偵測到離線閘道	：Cloud Edge 無法連線至閘道或執行掃瞄	指定 Remote Manager 何時傳送通知： • 「立即」：Cloud Edge 將事件報告至 Remote Manager 時立即觸發通知 • 「超過 X 天」：如果閘道在設定的天數內保持離線狀態，則觸發通知
離線 - 離線裝置復原	：Cloud Edge 已恢復離線裝置的連線	不適用
雲端電子郵件掃瞄 - 服務無法使用	：Cloud Edge 無法連線至雲端掃瞄服務	不適用
雲端電子郵件掃瞄 - 服務已復原	：Cloud Edge 已恢復至雲端掃瞄服務的連線	不適用
資源短缺 - CPU、記憶體或磁碟空間使用率超過	：裝置上剩餘的資源量已低於設定的警訊門檻值。	指定在 Remote Manager 觸發通知之前，可以使用的最大資源數（介於 80% 到 95% 之間）

InterScan Web Security as a Service 通知

表 17-9. 系統事件

事件	詳細資訊
帳號同步問題 - AD/LDAP 的同步問題	：無法與 AD/LDAP 同步

設定主控台設定

主控台設定可決定客戶在橫幅中看見的標誌，以及離線使用者的自動逾時頻率。

程序

1. 按一下「管理 > 主控台設定」。
2. 選取您想要在橫幅中使用的影像。

   重要

   標誌必須為 .png、.jpg、.bmp 或 .gif 影像，且建議的大小為 600 x 60（寬 x 高）。

3. 選取「作業階段逾時」頻率，Remote Manager 會使用此頻率自動將離線使用者登出。
4. 按一下「儲存」。

產生 API 金鑰

您可以使用 API 讓 Remote Manager 與第三方程式整合。包含產生的「存取 Token」和「機密金鑰」，以驗證與第三方程式之間的通訊。

如需有關可用 API 的詳細資訊，請參閱《雲端服務平台整合指南》。

注意

只有以管理權限登入的使用者才能產生和撤銷 API 金鑰。所有其他使用者角色具有唯讀權限。

程序

1. 按一下「管理 > 產生 API 金鑰」。
2. 按一下「產生」以顯示 API 整合所需的「存取 Token」和「機密金鑰」。
3. 如果您因故需要變更 API 金鑰，請按一下「撤銷」，然後按一下「產生」以取得新的「存取 Token」和「機密金鑰」。

警告!

您無法復原此動作。如果您撤銷現有金鑰，Remote Manager 將不再接受任何使用已撤銷金鑰的 API。

預設設定範本

預設設定範本包含特定客戶或群組的預先設定的設定。這些範本僅可用於 Worry-Free Business Security Services 和 Cloud Edge，且僅在 Trend Micro Remote Manager 與 Licensing Management Platform 整合時可用。

Trend Micro Remote Manager 提供的主控台類似於用於範本設定的 Worry-Free Business Security Services 和 Cloud Edge 主控台。在範本設定主控台設定的設定不影響註冊的產品。

如需關於可設定之設定的詳細資訊，請參閱產品文件。

http://docs.trendmicro.com/zh-tw/smb/worry-free-business-security-services.aspx

http://docs.trendmicro.com/zh-tw/smb/cloud-edge.aspx

設定 Worry-Free Business Security Services 的預設設定範本

僅當 Trend Micro Remote Manager 與 Licensing Management Platform 整合後，才會提供預設設定範本。

如需關於可設定之設定的詳細資訊，請參閱產品文件。

http://docs.trendmicro.com/zh-tw/smb/worry-free-business-security-services.aspx

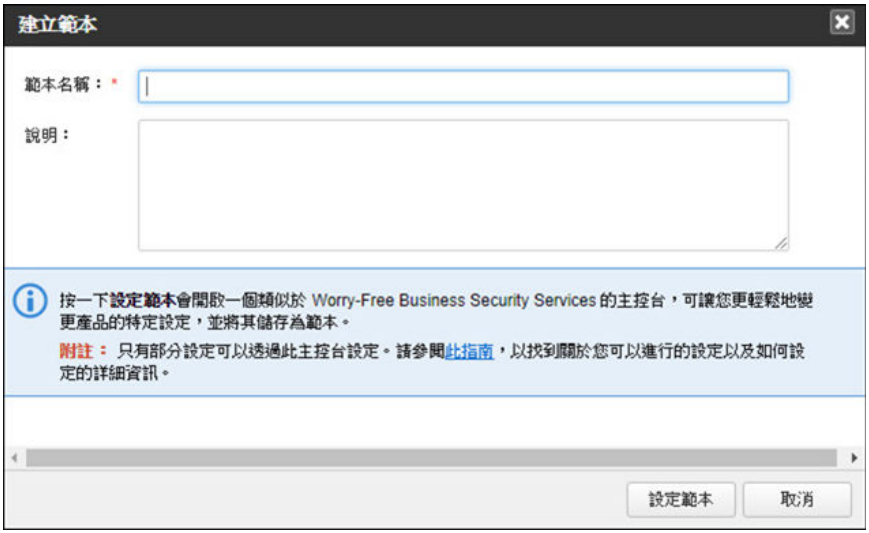
---

程序

1. 移至「管理 > 設定預設設定範本」。

   隨即顯示「設定預設設定範本」畫面。

2. 在「Worry-Free Business Security Services」下，按一下「建立」。



3. 輸入範本的名稱和說明。

4. 按一下「設定範本」。

   一個類似於 Worry-Free Business Security Services 主控台的主控台隨即開啟。

   重要

   在此主控台上進行的設定不會影響已註冊的產品。

5. 設定所需設定。

   重要

   設定以下任何設定之後，務必要按一下「儲存」將變更套用至每個畫面。

設定	LOCATION
策略	• 若是伺服器平台：裝置 > 伺服器（預設） > 設定策略 • 若是桌面平台：裝置 > 裝置（預設） > 設定策略
掃瞄設定	• 掃瞄 > 手動掃瞄（標籤） • 掃瞄 > 預約掃瞄（標籤） • 掃瞄 > 弱點掃瞄（標籤）
通知設定	• 管理 > 通知（標籤）
全域設定	• 管理 > 全域設定 > 安全設定（標籤） • 管理 > 全域設定 > 核可/封鎖的設定（標籤） • 管理 > 全域設定 > Agent 控管（標籤） • 管理 > 全域設定 > 裝置管理（標籤）

6. 按一下「完成」儲存範本設定。

設定 Cloud Edge 的預設設定範本

僅當 Trend Micro Remote Manager 與 Licensing Management Platform 整合後，才會提供預設設定範本。

如需關於可設定之設定的詳細資訊，請參閱產品文件。

http://docs.trendmicro.com/zh-tw/smb/cloud-edge.aspx

程序

1. 移至「管理 > 設定預設設定範本」。

   隨即顯示「設定預設設定範本」畫面。

2. 在「Cloud Edge」下，按一下「建立」。

   「建立範本」視窗隨即開啟。

3. 輸入範本的名稱和說明。

4. 按一下「設定範本」。

   一個類似於 Cloud Edge 雲端主控台的主控台隨即開啟。

   注意

   在此主控台上進行的設定不會影響已註冊的產品。

5. 進行所需的設定，然後按一下「儲存」。

6. 按一下「完成」儲存範本設定。

檢視管理記錄檔

管理記錄檔列出 Remote Manager 管理員執行的動作。

程序

1. 移至「管理 > 系統記錄檔」。
2. 按一下「管理記錄檔」。
3. 使用下拉式清單或透過行事曆指定日期，來指定日期範圍。
4. 按一下「顯示記錄檔」。

   將出現「管理記錄檔」表格。
5. 對於策略部署記錄檔，按一下「說明」欄中的連結，檢視關於成功或不成功策略部署動作的詳細資訊。

部分 VII

取得說明

第 18 章

疑難排解和常見問題

本節包含下列主題：

疑難排解

如果您在使用 Remote Manager 時遇到問題，請嘗試找到以下問題的解決步驟：

Trend Micro Remote Manager Web 主控台問題

以下主題介紹與 Trend Micro Remote Manager Web 主控台相關的疑難排解資訊：

存取問題

使用者無法登入 Trend Micro Remote Manager。

解決辦法

造成此問題的可能原因有兩個：

- 瀏覽器已關閉 JavaScript。Remote Manager 需要啟用此選項。請參閱瀏覽器說明文件，以取得相關指示。
- 描述檔尚未同步。如果您剛註冊 Trend Micro Licensing Management Platform 並且無法登入，請等待數分鐘，讓資訊同步。

不一致的狀態圖示

在資料收集的初始階段（Agent 註冊到伺服器後立即開始），Remote Manager 可能會顯示與顯示的病毒和垃圾郵件事件數目不一致的防毒和垃圾郵件防護狀態圖示。

註冊到伺服器之後，Agent 會立即從 Worry-Free Business Security（全部）傳輸目前的防毒和垃圾郵件防護狀態，但不傳輸這些狀態依據的歷史資料。因此，例如，它可能會顯示紅色狀態符號，但不顯示任何事件。

解決辦法

Remote Manager 會在 Worry-Free Business Security（全部）偵測到事件後，立即顯示正確的圖示和資料。

樹狀結構中無法展開的節點

如果按一下網域樹狀結構中的節點（「客戶」標籤下）時其不展開，則 Worry-Free Business Security 伺服器上的群組和客戶資訊與 Trend Micro Remote Manager 伺服器可能不同步。

若要解決此問題：

1. 移至「客戶 > [客戶]」畫面。
2. 將游標懸停在「產品」標籤中不展開的節點上。
3. 按一下「設定」圖示 ()。
4. 按一下「同步」。

   Trend Micro Remote Manager 會指示 Worry-Free Business Security 伺服器重新傳送群組資訊。

無法顯示網頁

嘗試開啟 Trend Micro Remote Manager 伺服器 URL 時顯示「無法顯示網頁」。在以下情況下會發生這種狀況：

- URL 不正確。
- Trend Micro Remote Manager 伺服器的 URL 不是 Internet Explorer 信任的網站。

解決辦法

1. 確保 Trend Micro Remote Manager 伺服器的 URL 是 Internet Explorer 信任的網站。
   a. 開啟 Internet Explorer。
   b. 按一下「工具 > 網際網路選項 > 安全性 > 信任的網站 > 網站」。
   c. 檢查 Trend Micro Remote Manager 伺服器 URL 是否在清單中。如果不在清單中，請在清單中輸入，然後按一下「確定」。

Agent 問題

將滑鼠懸停在系統匣圖示上時，系統會顯示狀態訊息來指示 Agent 是否在正常運作。

表 18-1. Agent 系統匣圖示顯示的狀態訊息

訊息	說明
遇到未知錯誤。請檢查系統或重新啟動 Agent。	遇到未知錯誤。請檢查系統或重新啟動 Agent。 有未預期的錯誤（通常是系統錯誤）造成 Agent 無法正常運作。 解決辦法： 檢查受管理伺服器是否發生記憶體不足或其他系統問題。

訊息	說明
無法在遠端伺服器中註冊。	您提供的 GUID 可能不正確，或可能發生網路問題。 解決辦法 有兩種狀況可能會造成此問題： • 確認您使用的 GUID 是否正確。請參閱管理 Worry-Free Business Security 伺服器 第 8-4 頁，以在 Remote Manager Web 主控台上找到正確的 GUID。 • 如果網路發生問題，Agent 也無法連線至伺服器。請檢查 Worry-Free Business Security（Standard 和 Advanced）伺服器與 Trend Micro Remote Manager 伺服器之間的網路連線。
無法連線至遠端伺服器。	受管理伺服器可能遇到 Internet 連線問題。 解決辦法 檢查受管理伺服器上的 Internet 連線。此外，請檢查 Agent 的 Proxy 設定，以及指定的伺服器位址和通訊埠。
Agent 已透過 Remote Manager 關閉	Agent 已透過 Remote Manager Web 主控台暫時關閉。 解決辦法 透過 Remote Manager Web 主控台啟用 Agent。
Agent 與 Client Server Messaging Security (CSM) 不相符。	Client Server 或 Client Server Messaging Security Suite 與 Agent 版本不相符。 解決辦法 將 Client Server 或 Client Server Messaging Security Suite 伺服器升級至最新版本，並安裝最新的 Agent。
Agent 服務已停止。	Agent 已從 Remote Manager 登出。 解決辦法 啟用 Agent 服務：以滑鼠右鍵按一下 Agent 系統匣圖示，然後按一下「啟用服務」。

訊息	說明
無法載入元件。您可能需要重新安裝 Agent。	Agent 在載入某些元件時發生問題。 解決辦法 首先嘗試重新啟用 Agent 服務：以滑鼠右鍵按一下 Agent 系統匣圖示，然後按一下「重新啟用服務」或「啟用服務」。如果無法解決問題，則解除安裝 Agent 再重新安裝。請務必使用相同的 GUID。

受管理的產品或第三方軟體連線問題

- 與 Hosted Email Security 的連線問題 第 18-6 頁
- 無法連線至 ConnectWise 客戶 第 18-7 頁

與 Hosted Email Security 的連線問題

如果您無法連線或中斷連線 Hosted Email Security，則頁面底部可能會顯示以下任何訊息：

訊息	解決辦法
無法連線至 Remote Manager 伺服器。請檢查網路連線和 Remote Manager 狀態。	檢查網路連線和 Remote Manager 狀態，然後再試一次。
授權碼無效	確認 GUID。如果 GUID 不正確。請刪除 Agent，然後再次嘗試連線。
授權碼重複	確認 GUID。如果 GUID 不正確。請刪除 Agent，然後再次嘗試連線。
無法連線至 Remote Manager 伺服器。請檢查網路連線和 Remote Manager 伺服器狀態。	檢查網路連線和 Remote Manager 狀態，然後再試一次。
伺服器內部錯誤	請與您的支援提供商聯絡。

無法連線至 ConnectWise 客戶

如果 ConnectWise 伺服器上的公司 ID 發生更新，則 Remote Manager 無法連線至 ConnectWise 客戶資訊。

若要解決此問題：

從 ConnectWise 中的 Remote Manager Customer 畫面，更新為新公司 ID。

常見問題

以下部分概述了關於 Remote Manager 設定的常見問題：

Web 主控台常見問題

我的 Customer Licensing Portal 帳號變更多長時間後，才會顯示在 MyAccount 畫面上？

變更 Customer Licensing Portal 帳號資訊後，系統最多可能需要 2 個小時與 Remote Manager Web 主控台同步變更。

為什麼在更新設定後，Remote Manager 主控台不立即顯示更新後的狀態？

需要幾分鐘時間，資料才能在所有服務間同步。延遲變更的一些範例包括更新使用授權或授權、重設計數器等。

我在嘗試開啟 Worry-Free Business Security Services 主控台時，為何收到登入錯誤？

如果 Worry-Free Business Security Services 停機維護，或 Licensing Management Platform 出現問題，則會發生這種情況。請稍等片刻，然後再次嘗試存取主控台。

在 Licensing Management Platform 建立新客戶後，客戶為何不顯示在 Remote Manager 中？

需要幾分鐘時間，資料才能在所有服務間同步。

我如何將新產品新增至現有 Remote Manager 客戶帳號？

將產品新增至現有 Remote Manager 客戶帳號的方法，會因您使用的趨勢科技帳號的類型而異。

- Licensing Management Platform 帳號：您可以直接從 Remote Manager Web 主控台，將新產品新增至現有 Remote Manager 客戶帳號。

  如需詳細資訊，請參閱使用 Licensing Management Platform 帳號新增產品 第 3-8 頁。

- 線上註冊入口網站帳號：使用以下方法，僅可將 Worry-Free Business Security、Worry-Free Business Security Services 和 Hosted Email Security 產品新增至現有 Remote Manager 客戶：接收受管理產品的授權碼，然後從受管理產品主控台註冊產品。

  如需詳細資訊，請參閱使用 Customer Licensing Portal 帳號新增產品 第 3-11 頁。

我如何從 Remote Manager 存取受管理產品主控台？

在 Remote Manager Web 主控台上，移至「客戶 > [客戶] > 產品」，然後在樹狀結構檢視中按一下產品名稱。

在表格的右上角，應顯示「開啟主控台」連結。按一下此連結以開啟受管理產品主控台。

Remote Manager 是否支援以角色為基礎的管理？

不支援。Remote Manager 僅支援使用完整功能的管理員帳號。

Remote Manager 中的 Licensing Management Platform 帳號和 Customer Licensing Portal 帳號存在哪些區別？

下表概述了使用不同帳號類型時，Remote Manager 中的功能差異。

功能	LICENSING MANAGEMENT PLATFORM 帳號	CUSTOMER LICENSING PORTAL 帳號
客戶管理 - 刪除客戶	不支援	支援
產品管理 - 刪除產品	不支援	支援
產品說明 - 編輯	不支援	支援
支援的產品	• Cloud App Security • Cloud Edge • Hosted Email Security • InterScan Web Security as a Service • Worry-Free Business Security（Standard 和 Advanced） • Worry-Free Business Security Services	• Hosted Email Security • Worry-Free Business Security（Standard 和 Advanced） • Worry-Free Business Security Services
第三方嵌入程式支援	• Autotask • ConnectWise Automate • ConnectWise Manage • Kaseya	• Autotask • ConnectWise Manage
範本管理	支援： • Cloud Edge • Worry-Free Business Security Services	不支援

功能	LICENSING MANAGEMENT PLATFORM 帳號	CUSTOMER LICENSING PORTAL 帳號
新客戶的範本指派	支援： • Cloud Edge • Worry-Free Business Security Services	不支援
現有客戶的範本指派	支援： • Cloud Edge • Worry-Free Business Security Services	不支援
我的帳號資訊	不支援	支援
Remote Manager 中的產品註冊	支援透過服務計畫指派自動註冊	需要授權碼
合併 OLR 帳號	支援	不適用
Licensing Management Platform 存取	支援	不支援
長 Beta 版本	支援	不支援
使用授權續約和授權配置	支援	不支援

最大化勒索軟體防護常見問題

- 當我按一下「首頁」畫面上的「最大化勒索軟體防護」按鈕時，會發生什麼？ 第 18-12 頁
- 我如何確定是否已啟用所有勒索軟體相關設定？ 第 18-12 頁
- 啟用勒索軟體防護有何風險？ 第 18-15 頁

當我按一下「首頁」畫面上的「最大化勒索軟體防護」按鈕時，會發生什麼？

隨即顯示「最大化所有客戶的 Worry-Free Business Security Services 勒索軟體防護」畫面。

按一下「全部啟用」會為除「伺服器（預設）」群組之外的所有群組中的所有客戶自動啟用以下功能：

- 行為監控
  - 勒索軟體防護
- 網頁信譽評等服務
- 新發現的程式偵測

我如何確定是否已啟用所有勒索軟體相關設定？

請在「客戶」畫面中的「安全設定」標籤中，確認所有勒索軟體相關設定均已啟用。

重要

您只能開啟 Worry-Free Business Security Services 主控台，來確認新發現的程式偵測功能是否已啟用。

程序

1. 移至「客戶 > {公司}」。

   隨即顯示「{公司}」畫面。

2. 在「產品」標籤上，在產品樹狀結構中展開 Worry-Free Business Security Services 產品計畫。

3. 選取「裝置（預設）」。

   隨即顯示「裝置」和「安全設定」標籤。

4. 按一下「安全設定」標籤。

隨即顯示以下畫面：


裝置
安全設定
掃瞄方法
雲端截毒掃瞄
標準掃瞄
防毒軟體/防間諜程式
啟動即時防毒/間諜程式防護
防火牆
啟動防火牆
簡易模式：以趨勢科技的預設設定啟動防火牆
進階模式：設定安全層級、IDS、通知和例外。
網頁信譽評等服務
啟動網頁信譽評等服務
高
中
低 (預設值)
URL 過濾
啟動 URL 過濾
高
中
低 (預設值)
自訂
行為監控
啟動行為監控
啟動所有勒索軟體防護功能
啟動 Intuit™ QuickBooks™ 防護
Machine Learning
啟動 Machine Learning
類型
處理行動
檔案
僅記錄檔
處理程序
終止

5. 在「網頁信譽評等服務」下，確認以下功能已啟用：
   - 啟用網頁信譽評等服務
6. 在「行為監控」下，確認以下功能已啟用：
   - 啟用行為監控
   - 啟用所有勒索軟體防護功能
7. 按一下「儲存」。

   會通知 Agent 進行變更。

啟用勒索軟體防護有何風險？

啟用勒索軟體防護功能可能會帶來以下任何風險：

- 啟用行為監控和勒索軟體防護可能會導致某些應用程式的一些相容性問題。

  若要解決此問題，請將這些應用程式新增至例外清單，或關閉行為監控和勒索軟體防護。

  如果此問題仍然存在，請洽詢您的支援提供商。
- 啟用勒索軟體防護的自動備份功能需要額外的 100MB 儲存空間。
- 啟用程式檢測會提升對已遭到入侵的可執行檔的偵測及整體偵測率，但可能會降低系統效能。

Hosted Email Security 常見問題

為什麼處於「即時狀態」時不顯示最近 3 小時的資料？

在 Hosted Email Security 伺服器上，資料收集需要超過兩個小時的時間。為了確保 Remote Manager 伺服器已整合來自 Hosted Email Security 伺服器的資料，資料收集會延遲 3 個小時。

為什麼在客戶樹狀結構中的 Hosted Email Security 上按一下右鍵時，「與伺服器同步」和「移至客戶主控台」呈灰色？

Hosted Email Security 處於離線狀態的可能原因有三個。

- Hosted Email Security 尚未連線至 Remote Manager。
- 客戶已終止連線。請參閱從 Hosted Email Security 客戶連線至 Remote Manager Web 主控台 第 6-2 頁。
- 可能需要重新整理客戶樹狀結構。

客戶將 Hosted Email Security 連線至 Remote Manager 後，當我嘗試重新導向至客戶的 Hosted Email Security 主控台時，為什麼會收到錯誤訊息「您的 Hosted Email Security 客戶尚未連線至 Remote Manager 或 Hosted Email Security 已中斷與客戶的連線。請聯絡您的管理員。」？

輸入 GUID 或授權碼並按一下「連線」後，可能需要十分鐘時間，Hosted Email Security 才能完成與 Remote Manager Web 主控台的連線。如果此問題仍然存在，請聯絡趨勢科技客戶服務部門。

為什麼 Hosted Email Security 客戶的啟用碼 (AC) 和到期日在 Remote Manager Web 主控台上顯示「無」？

如果 Hosted Email Security 客戶未將 Hosted Email Security 服務連線至 Remote Manager，或已中斷連線，則 Remote Manager 無法擷取資料。另一原因是 Hosted Email Security 找不到此客戶的有效啟用碼和到期日。很少會發生這種狀況。

報告常見問題

可儲存的報告是否有數目限制？

有。Remote Manager 會限制儲存報告的數目。達到配額後，會自動刪除較舊的報告。所儲存報告的數目為：

- 每日報告：最多儲存 30 份報告。
- 每周報告：最多儲存 10 份報告。

- 每月報告：最多儲存 5 份報告。

為什麼建立一次性報告描述檔後，在報告記錄中沒有新報告產生？

請在建立報告描述檔後等待一到兩分鐘。報告將顯示在報告記錄中。如果仍無法產生報告，請開啟報告描述檔並重新儲存。如果此問題仍然存在，請聯絡趨勢科技客戶服務部門。

為什麼報告記錄中有報告，但我卻收不到每日/每周/每月報告？

請確保客戶的電子郵件信箱有效，且在報告描述檔收件者清單中。如果這兩方面都沒有問題，則可能是網路問題。

在產生的報告中，為什麼不根據我所在時區顯示資料時間？

報告使用的時區為經銷商在建立描述檔時所選取的時區。而非由客戶的電腦確定。

建立一次性報告後，「無」表示甚麼？

對於一次性報告，狀態欄會永遠顯示「無」。發生這種情況是因為一次性報告沒有狀態（無法關閉、啟用、暫停等）。

使用 SSL (HTTPS) 連線時無法檢視報告。

「不要將加密的網頁存到磁碟」是 Internet Explorer 的一項安全設定，處理 SSL (HTTPS) 連線時會出現這種情況。如果核取此設定，則不會將任何內容儲存至快取記憶體，您將無法開啟或下載報告。

為了在 Internet Explorer 11.0 中修復此問題，請按一下「工具 > 網際網路選項 > 進階 > 安全性」，然後關閉「不要將加密的網頁存到磁碟」選項。

第 19 章

技術支援

瞭解下列主題：

聯絡支援

使用支援入口網站

趨勢科技支援入口網站是全年無休的線上資源，包含有關常見和不常見問題的最新資訊。

程序

1. 造訪 https://success.trendmicro.com/business-support。
2. 使用「Search Support」文字方塊搜尋可用的解決方案或關鍵字。
3. 按一下「All Products」下拉式清單，並選取您的產品。
4. 如果未找到解決方案，請按一下「Contact Support」，然後選取所需的支援類型。

   秘訣

   若要線上提交支援案例，請造訪下列 URL：

   http://esupport.trendmicro.com/zh-tw/srf/twbizmain.aspx

   趨勢科技支援工程師會在 24 小時或更短時間內調查案例並進行回應。

加速支援要求

為了提高解決問題的速度，現已提供下列資訊：

- 問題模擬的步驟

- 裝置或網路資訊
- 電腦品牌、型號以及連接的任何其他硬體或裝置
- 記憶體大小和可用硬碟空間
- 作業系統和 Service Pack 版本
- 安裝的 Agent 版本
- 產品序號或啟動碼
- 安裝環境的詳細說明
- 已接收的任何錯誤訊息的確切文字

將可疑內容傳送到趨勢科技

有多個選項可供將可疑內容傳送到趨勢科技，以便進一步分析。

電子郵件信譽評等服務

查詢特定 IP 位址的信譽評等，並指定一個訊息轉移用戶端，以將其包含在全域例外清單中：

https://ers.trendmicro.com/

請參閱下列「常見問題集」項目，將訊息範例傳送給趨勢科技：

http://esupport.trendmicro.com/solution/zh-TW/1112106.aspx

檔案信譽評等服務

收集系統資訊並將可疑檔案內容提交到趨勢科技：

http://esupport.trendmicro.com/solution/zh-tw/1059565.aspx

記錄案例編號以供追蹤。

網頁信譽評等服務

查詢疑似網路釣魚網站的 URL 的安全分級和內容類型，或其他所謂「病媒」（間諜程式和惡意程式等 Internet 威脅的蓄意來源）：

http://global.sitesafety.trendmicro.com/

如果指定的分級不正確，請傳送重新分類要求到趨勢科技。

疑難排解資源

聯絡技術支援之前，請考慮造訪下列趨勢科技線上資源。

安全威脅百科全書

現今的大多數惡意程式都包含混合安全威脅（合併了兩種或更多種技術），以略過電腦安全通訊協定。趨勢科技會使用建立自訂防範政策的產品來抵禦此複雜惡意程式。安全威脅百科全書提供了多種混合性安全威脅的名稱和癥狀的完整清單，包括已知惡意程式、垃圾郵件、惡意 URL 和已知弱點。

移至 http://about-threats.trendmicro.com/threatencyclopedia.aspx?language=tw&tab=malware 以瞭解更多資訊：

- 目前正在使用中或「擴散中」的惡意程式和惡意可攜式程式碼。
- 用於形成完整網頁攻擊過程的關聯安全威脅資訊頁面
- 有關目標攻擊和安全威脅的 Internet 安全威脅諮詢
- 網頁攻擊和線上趨勢資訊
- 每週惡意程式報告

下載專區

有時，趨勢科技可能會針對報告的已知問題發行修補程式，或是發行適用於特定產品或服務的升級。如果要瞭解是否有適用的修補程式，請移至：

http://downloadcenter.trendmicro.com/index.php?regs=tw

如果未套用修補程式（修補程式已過期），請開啟 Readme 檔以判斷其是否與您的環境相關。Readme 檔還包含安裝說明。

文件意見反應

趨勢科技始終力求改善其文件。如果您對本文件或趨勢科技的任何文件有任何疑問、意見或建議，請透過

docs@trendmicro.com 聯絡我們。

索引

趨勢科技股份有限公司
台北市敦化南路二段 198 號 8 樓
電話：(886) 2-23789666
傳真：(886) 2-23780993
info@trendmicro.com

www.trendmicro.tw
項目編號：APTMS8225/180330