GFI 產品手冊

GFI LanGuard™

評估工具指南 - 有助於最大程度地利用 GFI LanGuard 試用版

文件版本：12.0

最近更新（年/月/日）：14/04/2016

目錄

1 介紹 4

1.1 GFI LanGuard 概覽 4
1.2 客戶為什麼購買 GFI LanGuard？ 4
1.3 取得評估金鑰 8

2 執行安全性掃描 9

2.1 無代理程式安全性掃描 9
2.2 以代理程式為主的稽核 13
2.3 稽核智慧手機和平板電腦 15
2.4 掃描設定檔 16
2.5 從儀表板觸發掃描 17

3 分析掃描結果 19

3.1 儀表板 19
3.2 如何從您的網路中檢視相關安全性變更 21
3.3 如何新增/檢視儀表板中的更多裝置 22
3.4 如何篩選裝置 22
3.5 如何對裝置分組 23
3.6 如何搜尋電腦 25
3.7 全文檢索搜尋 26
3.8 報告 27

4 補救安全性問題 29

4.1 部署缺少的軟體更新 29
4.2 解除安裝未經授權的應用程式 32
4.3 部署自訂軟體 35
4.4 傳送電子郵件通知給行動裝置擁有者 36
4.5 其他補救作業 37

5 自動執行工作 39

5.1 自動探索網路中的新裝置 39
5.2 自動稽核安全性 40
5.3 自動下載修補程式 42
5.4 自動補救作業 43
5.5 自動產生報告 48

6 詞彙表 49

7 索引 57

1 介紹

感謝您評估 GFI LanGuard。本指南的目標是協助您從 GFI LanGuard 試用獲得最大效益。

在接下來的章節中，我們的指引將協助您證明本產品對於您以及參與決策的任何其他人的利益。

本章節主題：

1.1 GFI LanGuard 概覽 4

1.2 客戶為什麼購買 GFI LanGuard？ 4

1.3 取得評估金鑰 8

1.1 GFI LanGuard 概覽

GFI LanGuard 是全面性的網路管理解決辦法。它作為虛擬安全顧問，可在下列方面提供協助：

» 修補程式管理

» 弱點評估

» 網路和軟體稽核

» 資產清查

» 行動裝置管理

» 風險分析

» 合規

GFI LanGuard 掃描、分析，並協助補救您的網路。

» 不管是以代理程式為主安裝還是無代理程式安裝，GFI LanGuard 都會掃描網路中的安全性問題，並收集相關的安全資訊。它會收集有關安全性弱點、缺少的修補程式、缺少的 Service Pack、開啟的連接埠、開放共用、使用者和群組、安裝的應用程式、員工使用的智慧手機和平板電腦，以及硬體清查的資訊。GFI LanGuard 可以與超過 4,000 種安全應用程式整合，例如防毒軟體、反間諜軟體或防火牆及其狀態報告。

» 利用掃描結果，您可以分析網路的狀態。GFI LanGuard 提供功能強大的儀表板，供瀏覽和研究掃描結果。如果偵測到問題，將觸發安全感測器。弱點等級是根據稽核結果，對每個掃描電腦的評級。GFI LanGuard 並提供報告和結果比較。

» 掃描和分析完成後，GFI LanGuard 可協助補救安全性問題，並盡可能自動完成該過程。

» 建立基準掃描後，您可以確定網路中的所有電腦的安全和電腦組態的不同和變更。例如，可以決定部署缺少的 Microsoft 和非 Microsoft 安全(以及非安全) 更新、回復更新、部署自訂軟體和指令碼、解除安裝未經授權的應用程式、開啟到所掃描電腦的遠端桌面連線的動作。所有這些動作將協助確保您的網路是最新的，並且套用最新修補程式。

1.2 客戶為什麼購買 GFI LanGuard？

根據我們的經驗，GFI 客戶購買 GFI LanGuard 的五大原因包括：

1. 透過以下步驟大幅降低安全風險：

» 掃描網路中的安全與弱點問題

» 自動偵測並解除安裝任何未經授權的應用程式

» 稽核網路中的軟體(哪些 PC 安裝了什麼軟體) 和硬體裝置

» 接收有關網路安全環境的警示和報告

2. 自動化修補程式管理過程 - 為 Microsoft、Mac OS、Linux 系統和其他協力廠商應用程式偵測和部署缺少的修補程式

3. 執行網路稽核和網路健康監視

4. 協助遵守要求定期弱點評估和修補程式管理的安全規範(例如 PCI DSS、HIPAA、SOX、GLBA、PSN CoCo)

5. 評估和管理員工用來存取公司資訊和應用程式的智慧手機和平板電腦的安全性

下列主題提供真實案例及更多對於使用 GFI LanGuard 的深入見解：

1.2.1 使用 GFI LanGuard 進行弱點評估

GFI LanGuard 可利用弱點檢查資料庫(例如 OVAL 和 SANS Top 20) 對您的作業系統、虛擬環境、網路裝置和已安裝的應用程式執行超過 50,000 個弱點檢查。

本節提供關於如何實現弱點評估和安全性問題補救的準則，以保證您電腦是安全的且是最新的。

» 保證 GFI LanGuard 是最新的

» 確保安裝 GFI LanGuard 的電腦可存取網際網路。GFI LanGuard 每天執行檢查，以獲得有關弱點和修補程式的更新的資訊。

» 如果使用 Proxy 伺服器，可以在 **GFI LanGuard 使用者介面 > 主功能表 > 組態 > Proxy 設定...** 中進行設定。

» 如果安裝 GFI LanGuard 的電腦無法存取網際網路，可以設定本產品從其他位置獲得更新。如需詳細資訊，請按一下此處。

» 定期執行安全稽核

» 每天都會發現新的安全性問題。對這些問題的補救需要一些前瞻性的規劃，盡早注意到安全性問題能夠更有效地進行排程，獲得有效的補救。

» 建議設定本產品每天或每星期自動稽核網路。

» 首先部署缺少安全性更新

» 確保每台電腦上的所有修補程式和 Service Pack 都是最新的，即可補救大部分的安全性問題。

» Service Pack 包含許多安全補救，因此建議您先套用這些 Service Pack。

» 部署 Service Pack 之後，我們建議再次掃描網路(將更新您網路的修補程式狀態)

» 在重新掃描後，部署所有缺少的修補程式

» 本產品可以設定為自動部署缺少安全性更新，前提是經過管理員預先核准。

» 尋找和補救其他安全性問題

» 弱點評估結果包含對偵測到的安全性問題的詳細描述，以及對外部網站的參考，可獲得額外資訊。

» GFI LanGuard 隨附的工具可協助透過遠端解除安裝(未經授權的) 軟體解決弱點、啟用防毒軟體/反間諜軟體/防火牆、觸發防毒軟體/反間諜軟體的定義更新、部署自訂軟體和指令碼，或者開啟電腦的遠端桌面連線。

» 如何檢查網路安全性狀態

» 使用**儀表板 > 概覽**可獲得網路安全性狀態的總體概覽，包括最易受攻擊的電腦、弱點分佈和弱點趨勢

» GFI LanGuard 提供了網路弱點等級，該等級是基於每台電腦的各個弱點等級計算的。每台電腦都有基於在其上偵測到的安全性問題計算的弱點等級。根據 NVD 計算的 CVSS 評分系統，安全性問題被歸類為具有高、中、低嚴重性。

» 使用**儀表板 > 歷程記錄**可獲得偵測到的新安全性問題清單，以及在網路中進行的其他安全敏感組態變更清單。

» 使用**儀表板 > 弱點**取得在網路中偵測到的弱點的詳細檢視

» 使用**儀表板 > 修補程式**取得網路修補程式狀態的詳細檢視

» 使用**報告 > 網路安全概覽**報告，取得網路安全性狀態的總體概覽

» 使用**報告 > 弱點狀態**報告，取得網路安全性狀態的詳細概覽

» 使用**報告 > 補救歷程記錄**報告，可獲得安全性問題是否已使用 GFI LanGuard 補救的歷程記錄

»
使用**報告 > 行動裝置稽核**報告可獲得連線到公司的 Microsoft Exchange 伺服器的智慧手機和平板電腦的概覽，並且偵測它們是否有過期的作業系統和已知的安全性問題

» 可以設定報告定期產生

1.2.2 使用 GFI LanGuard 進行修補程式管理

GFI LanGuard 提供依需求或自動偵測、下載和部署缺少的更新，覆寫：

» Microsoft 作業系統和應用程式

» Apple OS X 作業系統和應用程式

» Linux 作業系統和應用程式。支援下列 Linux 發行版本： Red Hat Enterprise Linux、Fedora、Ubuntu、Suse、OpenSuse、CentOS 和 Debian

» Windows 平台上執行的最常見和對安全敏感的協力廠商應用程式，包括所有主要的 Web 瀏覽器、Adobe 產品、Java 執行時等。如需完整清單，請按一下此處。

» 安全和非安全修補程式

» 修補程式回復

» 自訂軟體和指令碼(可以使用 GFI LanGuard 部署的可無訊息模式執行的軟體的任何部分) 的網路範圍部署

1.2.3 使用 GFI LanGuard 進行資產追蹤

未受管理或被遺忘的裝置具安全風險。使用 GFI LanGuard 可找到您不清楚的裝置：

» 伺服器和工作站

» 虛擬機器

» 以 IP 為主的裝置，例如路由器、印表機、存取點、交換器等。

» 行動裝置，例如 iPad、iPhone 和 Android 手機

如需詳細資訊，請參閱 部署自訂軟體 (page 35)。

1.2.4 使用 GFI LanGuard 進行網路和軟體稽核

GFI LanGuard 提供對網路中發生的活動的詳細分析 - 哪些應用程式或預設組態正帶來安全風險，以及瞭解您的網路所需的全部資訊，例如：

» 作業系統

» 虛擬機器

» 已安裝的硬體和軟體

» CPU資訊

» HDD 空間

» 無線裝置

» 網路介面卡

» 服務

» 稽核原則

» 使用者和群組

» 共用

» 開啟的 TCP 和 UDP 連接埠

» 連線到公司的 Microsoft Exchange 伺服器、Office 365、Google Apps 或 Apple Profiles Manager 等服務的智慧型手機與平板電腦

使用**儀表板 > 軟體**可獲得網路中安裝的所有應用程式的詳細檢視。

使用**儀表板 > 硬體**可檢查網路的硬體清查。

使用**儀表板 > 系統資訊**可檢視有關網路中存在的系統的安全敏感資訊。

使用**儀表板 > 歷程記錄**可獲得在網路中發生的安全敏感變更清單

使用**報告 > 軟體稽核**可產生有關網路中安裝的應用程式的全面報告。

使用**報告 > 行動裝置稽核**報告可獲得連線到公司的 Microsoft Exchange 伺服器、Office 365、Google Apps 或 Apple Profiles Manager 等服務的智慧手機和平板電腦的概覽，並且偵測它們是否有過期的作業系統和已知的安全性問題。

GFI LanGuard 可用來標記、偵測和移除網路中未經授權的應用程式。

GFI LanGuard 可與下列類別超過 4,000 種關鍵安全應用程式整合：防毒軟體、反間諜軟體、防火牆、防網路釣魚軟體、備份用戶端、VPN 用戶端、URL 篩選、修補程式管理、Web 瀏覽器、即時訊息、對等、磁碟加密、預防資料遺失和裝置存取控制。提供它們的狀態報告，並且透過允許諸如啟用防毒軟體或防火牆、觸發防毒軟體或反間諜軟體的定義更新、解除安裝對等應用程式等操作，補救問題。

1.2.5 使用 GFI LanGuard 以遵循法規

如今出現越來越多的法律法規，要求企業實施特定安全作法。提供金融服務和醫療保健的政府機構、企業受這些規定的影響最大，最新發展趨勢是所有企業都需要足夠安全，以保護他們的員工、客戶和合作夥伴的隱私和資料。違反這些法規可能導致遺失機會、遭受法律和經濟處罰，甚至可能停止營業。

以下是這些規範所要求的常見安全項目以及 GFI LanGuard 能夠協助的地方：

» 定期執行弱點評估

» 保證系統安裝了全部修補程式

» 確保網路中的所有系統都安裝並執行防毒軟體和反間諜軟體而且是最新的

» 確保網路中的每個系統都安裝並開啟個人防火牆

» 確保整個網路皆已安裝加密軟體

GFI LanGuard 可以與其他 GFI 軟體產品整合，進而形成一組產品套件而有助於法規遵循：

» GFI EventsManager® – 記錄管理解決辦法

» GFI EndPointSecurity™ – 裝置封鎖解決辦法

GFI LanGuard 隨附一套現成的預先定義報告，可用來遵循 PCI DSS、HIPAA、SOX、GLBA 和 PSN CoCo 等規範。如需 PCI DSS 的詳細資訊，請按一下此處。

以下是與 IT 基礎設施安全相關的一些最重要的標準清單：

» 支付卡行業資料安全標準 (PCI DSS)

» 健康保險流通與責任法案 (HIPAA)

» 沙賓法案 (SOX)

- 金融服務業現代化法案 (GLB/GLBA)
- 聯邦資訊安全管理法案 (FISMA)
- 家庭教育權和隱私權法案 (FERPA)
- 兒童網路保護法 (CIPA)
- 公用部門網路 – 連線法規 (PSN CoCo)
- 歐洲聯盟網路資料暨隱私保護綱領
- 關於隱私和電子通訊的歐盟綱領

1.2.6 使用 GFI LanGuard 管理行動裝置

GFI LanGuard 能夠偵測連線到公司服務的智慧型手機和平板電腦，公司服務則例如 Microsoft Exchange 伺服器、Office 365、Google Apps 或 Apple Profiles Manager 以及：

- 依照使用者、製造商、裝置型號、作業系統、上次連線時間來對裝置分類
- 執行對裝置作業系統的弱點評估。支援 Android、iOS 和 Windows Phone。
- 有關可用的作業系統更新的報告
- 向裝置擁有者傳送自訂電子郵件通知

1.3 取得評估金鑰

如果您尚未下載 GFI LanGuard，開始之前，請從此處下載試用版。

若要啟動評估版的 GFI LanGuard，請輸入免費評估金鑰。評估金鑰將使您獲得產品的全部功能，但是限於 25 個 IP 位址，25 個行動裝置，為期 30 天。該金鑰傳送到在您下載產品時註冊的電子郵件地址。

如果您無法存取包含該金鑰的原始電子郵件，可以按一下此處免費索取新評估金鑰。

如果需要評估較長時間或者超過 25 個 IP 位址和 25 個行動裝置，可以在此提交您的要求。

2 執行安全性掃描

在 Windows 系統上，GFI LanGuard 可以執行無代理程式和以代理程式為主的安全性掃描。目前，只有無代理程式掃描適用於非 Windows 系統（ Linux、Mac OS、網路裝置、智慧手機和平板電腦）。以下是選擇要使用的掃描方法時需要考慮的事項：

無代理程式掃描：

» 用戶端電腦上無安裝

» 所有處理都是由中央伺服器完成的，不需要用戶端電腦的資源

» 在不支援代理程式的系統中工作

以代理程式為主的掃描：

» 由於在用戶端之間分配負載，所以有更好的效能

» 由於伺服器和用戶端之間的通訊比無代理程式掃描時的通訊量少，所以能夠在低頻寬環境下更好地工作

» 由於代理程式在離線時也可繼續工作，所以可更好地支援筆記型電腦。當它們上線後，就會與伺服器進行同步

» 由於本機掃描可以比遠端掃描存取詳細資訊，所以可提高結果的準確性

本章節主題：

2.1 無代理程式安全性掃描 9

2.2 以代理程式為主的稽核 13

2.3 稽核智慧手機和平板電腦 15

2.4 掃描設定檔 16

2.5 從儀表板觸發掃描 17

2.1 無代理程式安全性掃描

2.1.1 觸發掃描並即時追蹤進度

使用**掃描**索引標籤可立即觸發無代理程式掃描，並且即時追蹤進度。掃描目標可以是下列各項的任意組合：

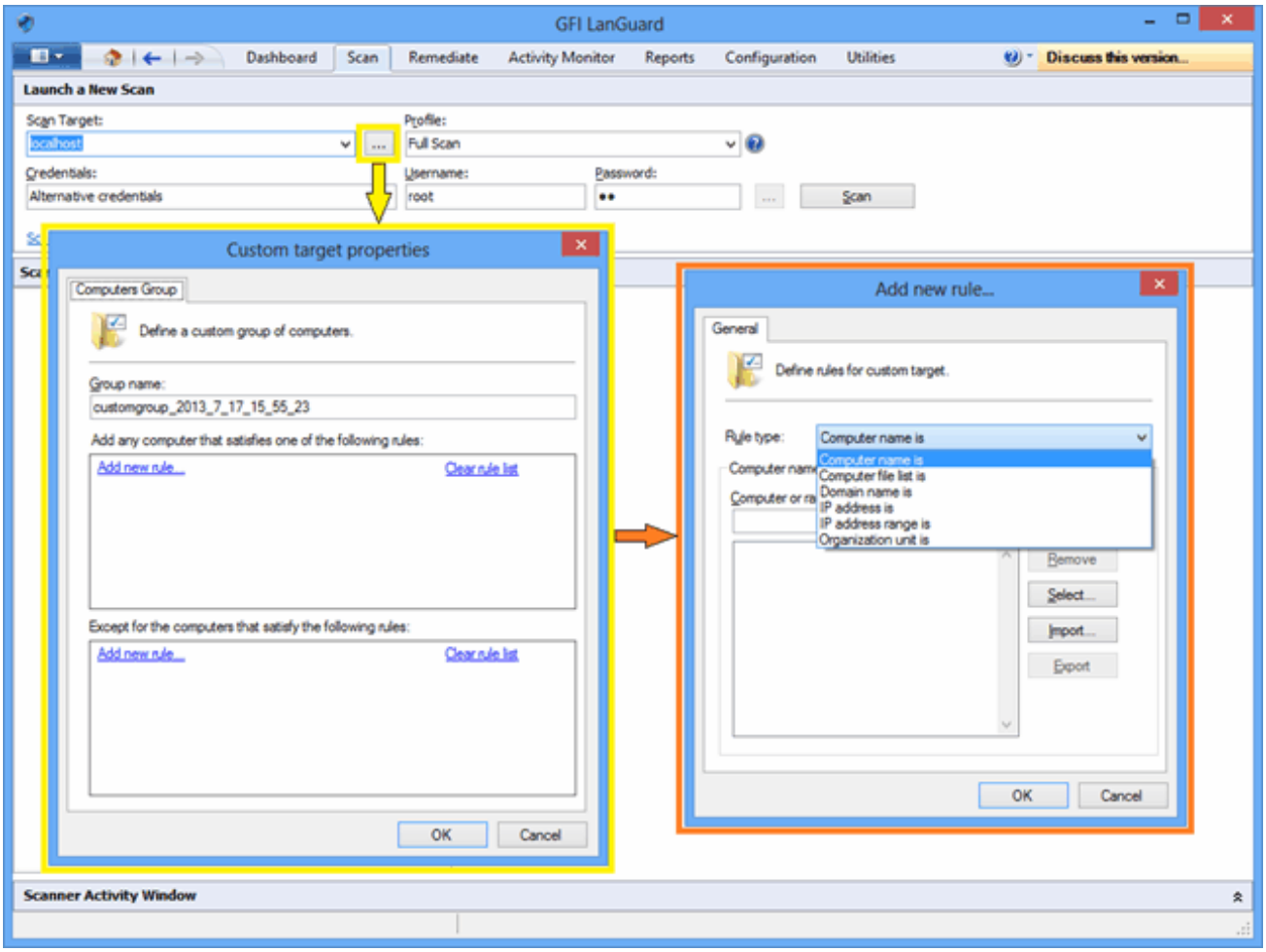
» 電腦名稱

» 包含電腦名稱的文字檔

» 單一 IP 位址和 IP 位址範圍

» 網域或工作群組和組織單位

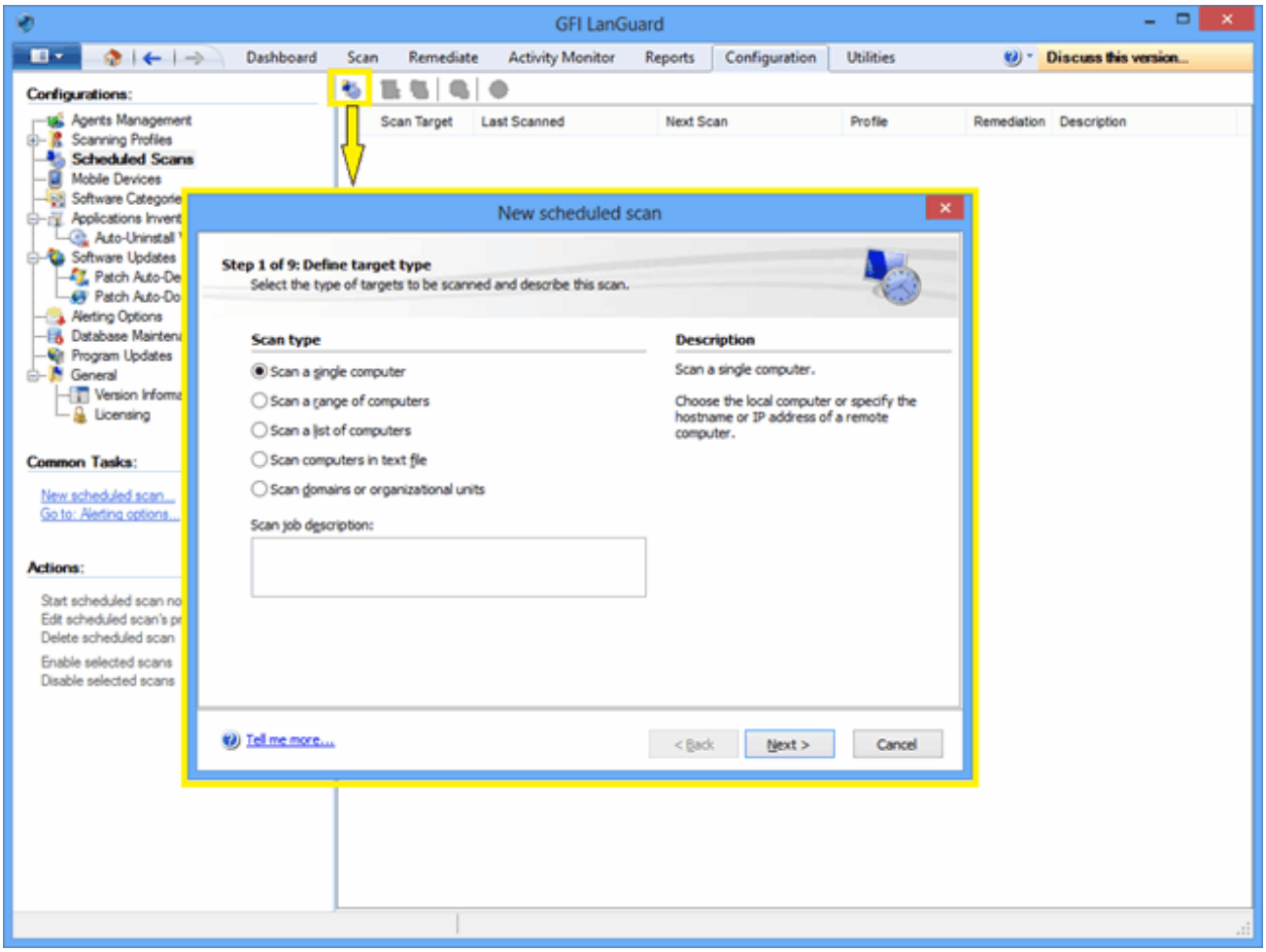
> **附註：**
> 需要對遠端電腦具有系統管理存取權，才可以獲得全面性的安全稽核結果。



螢幕擷取畫面 1: 無代理程式安全性掃描

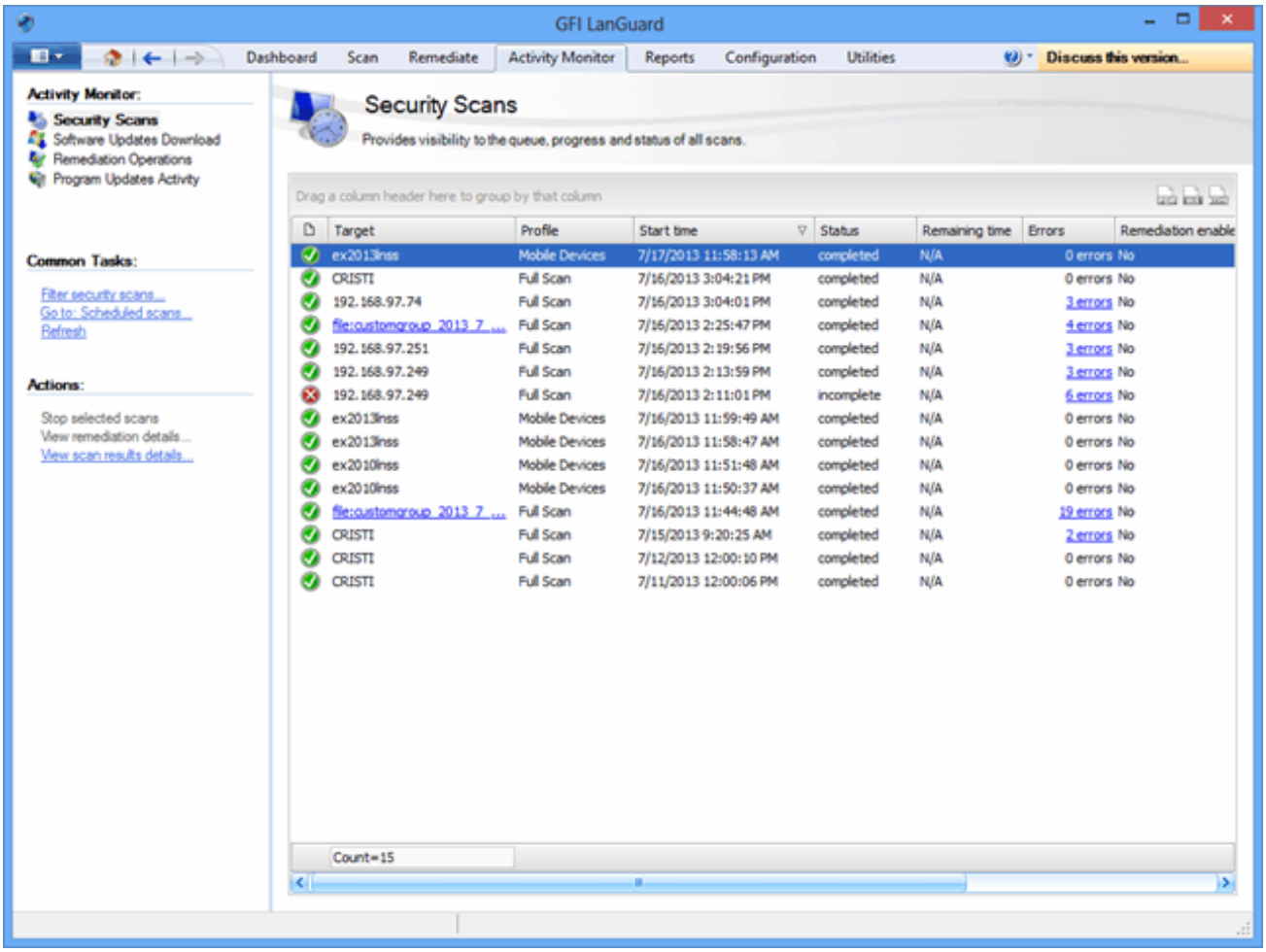
2.1.2 排程掃描

1. 若要排程無代理程式掃描定期執行，請按一下**組態 > 排程的掃描**，並選擇要掃描的目標類型。



螢幕擷取畫面 2: 新排程掃描

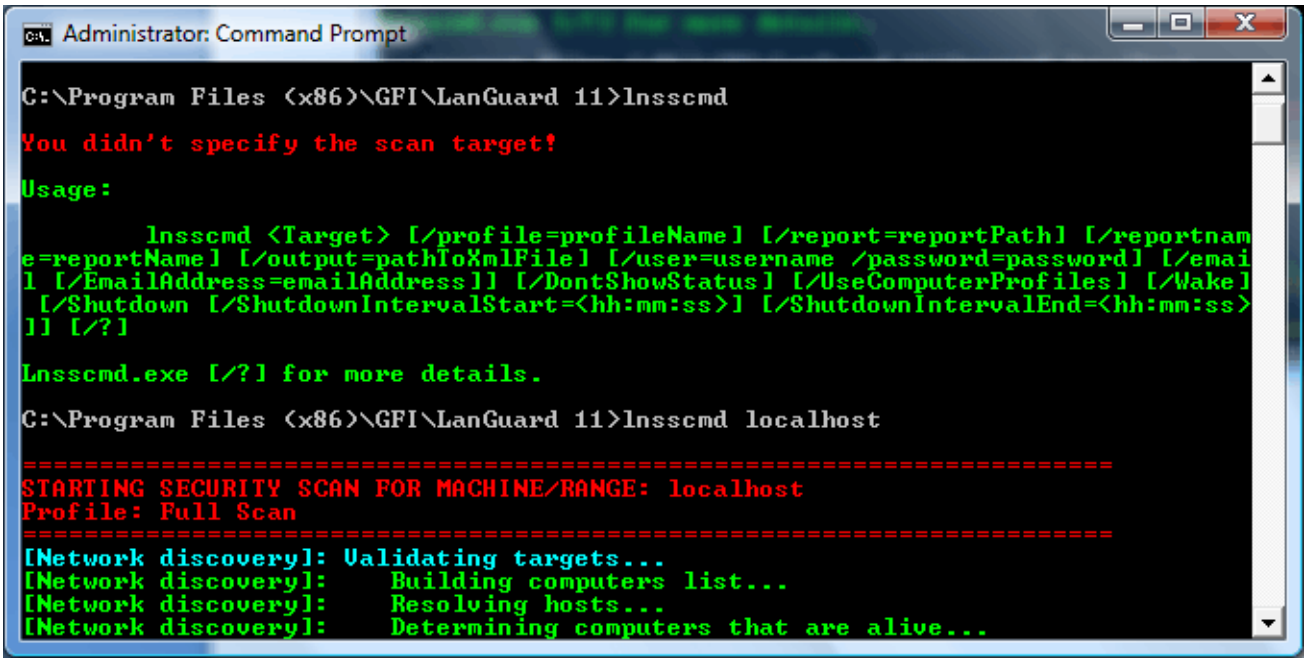
2. 可以使用**活動監視器 > 安全性掃描**來追蹤排程掃描的進度：



螢幕擷取畫面 3: 安全性掃描

2.1.3 命令列掃描

1. 若要執行命令列掃描，請使用 lnsscmd.exe 工具



螢幕擷取畫面 4: 命令列掃描

2.2 以代理程式為主的稽核

啟用代理程式的步驟很簡單。只需設定需要部署代理程式的電腦清單、網域或組織單位，並提供對遠端電腦具有系統管理存取權的認證。

GFI LanGuard 將處理部署操作。

代理程式的功能是：

» GFI LanGuard 在選擇的電腦上自動安裝代理程式

» 代理程式只能安裝在 Microsoft Windows 系統上

» 預設情況下，代理程式每天對其主機執行一次完全掃描，但是可以設定頻率、掃描時間和掃描設定檔

» 代理程式需要大概 25 MB RAM 和 600 MB 磁碟空間

» 代理程式只有在稽核主機時才會佔用 CPU。稽核每天只需要幾分鐘的時間，而且處理程序的優先順序低於正常值，因此不會干擾該電腦上執行的操作。

» 可以從 GFI LanGuard 解除安裝代理程式。預設情況下，代理程式如果有 60 天與伺服器無聯繫，則將自動解除安裝。此天數可以設定。

» GFI LanGuard 代理程式使用 TCP 連接埠 1070 將其狀態傳送到 GFI LanGuard 伺服器。此連接埠號碼可以設定。

» 可以設定 GFI LanGuard 在網域或組織單位自動執行網路探索，並且在新發現的電腦上自動安裝代理程式。

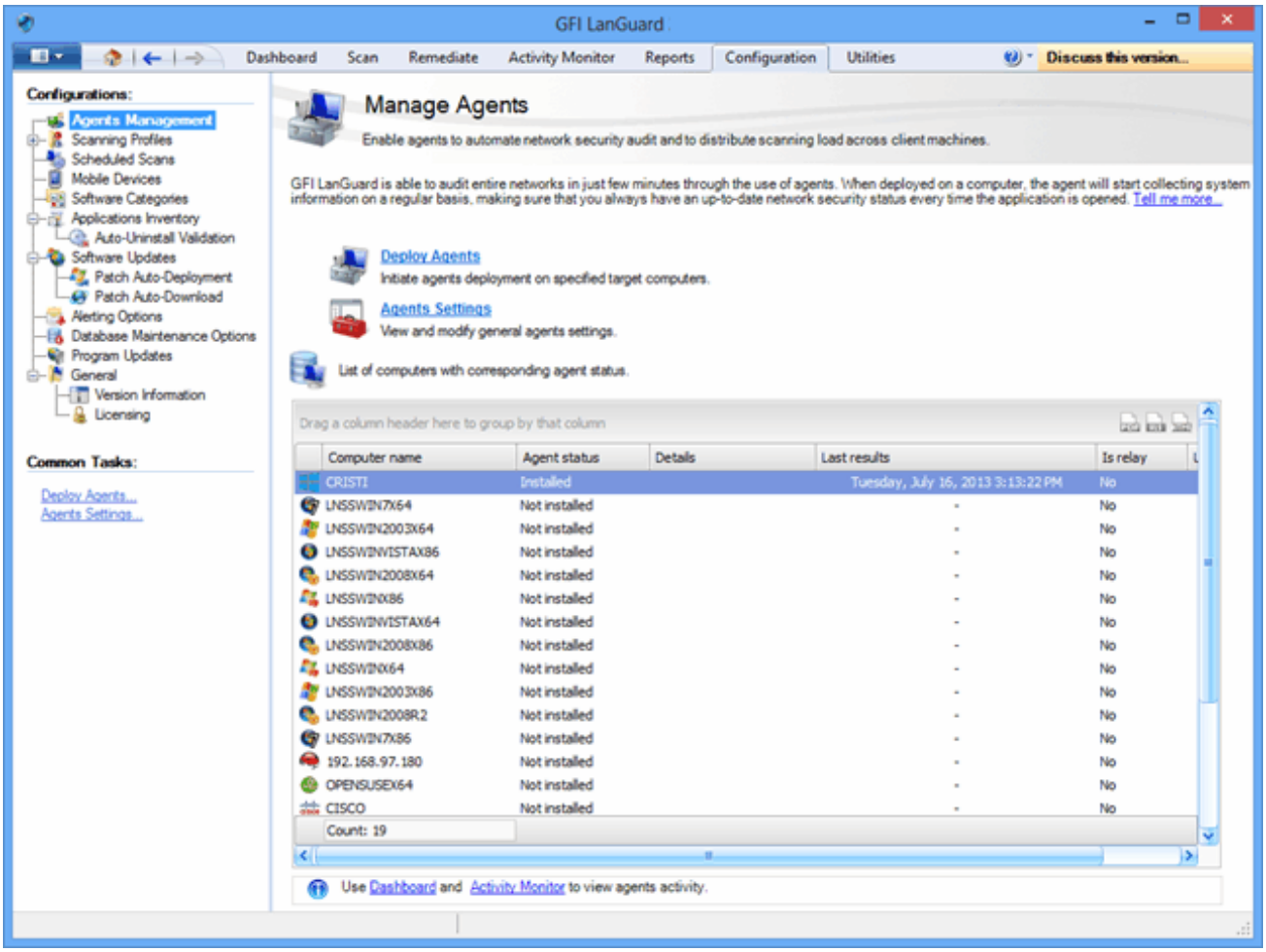
» GFI LanGuard 會自動處理代理程式遭到意外刪除或者需要升級的情況。

重要事項：
可以為代理程式指定轉送代理程式，對於多網站或大型網路來說，這樣可以更有效地執行補救，並且少佔用網路頻寬。轉送代理程式會儲存修補程式資料的本機複本(通常儲存在 GFI LanGuard 伺服器上) ，用來補救附近的電腦。

附註：
有關轉送代理程式的詳細資訊，請參閱 管理員指南，可以從此處下載。

要啟用代理程式：

1. 按一下**組態 > 管理代理程式**

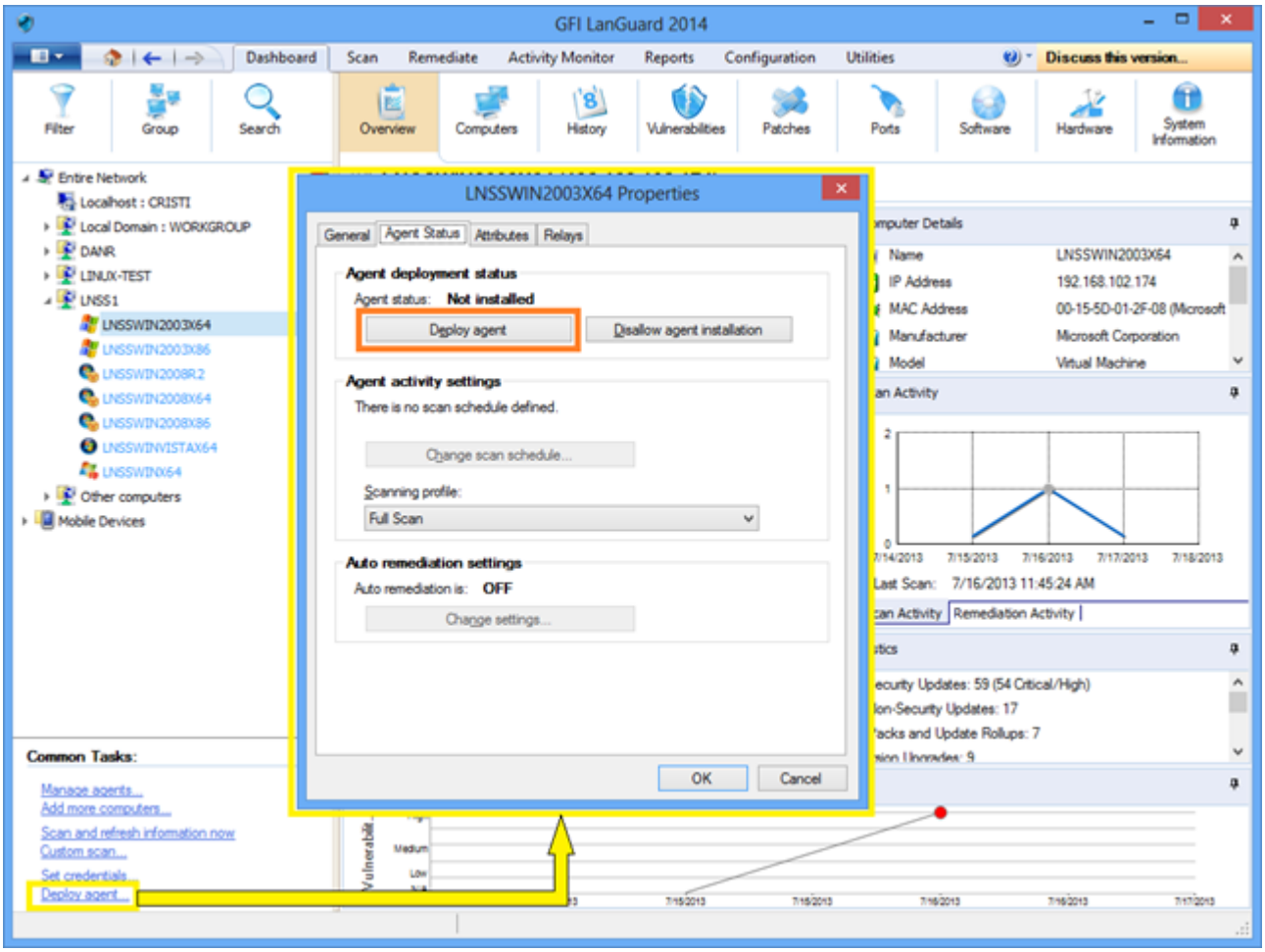


螢幕擷取畫面 5: 管理代理程式

2.2.1 代理程式部署錯誤疑難排解

如需導致 GFI LanGuard 無法在某些電腦上部署代理程式的可能原因清單，請按一下此處

要啟用和設定代理程式，請按一下**儀表板 > 概覽**，並選擇**一般工作**下的**部署代理程式...**：



螢幕擷取畫面 6: 部署代理程式

2.2.2 觸發以代理程式為主的依需求掃描

以代理程式為主的掃描通常按照已設定的稽核排程，自動在遠端電腦的背景執行（ 預設情況下代理程式一天執行一次掃描） 。

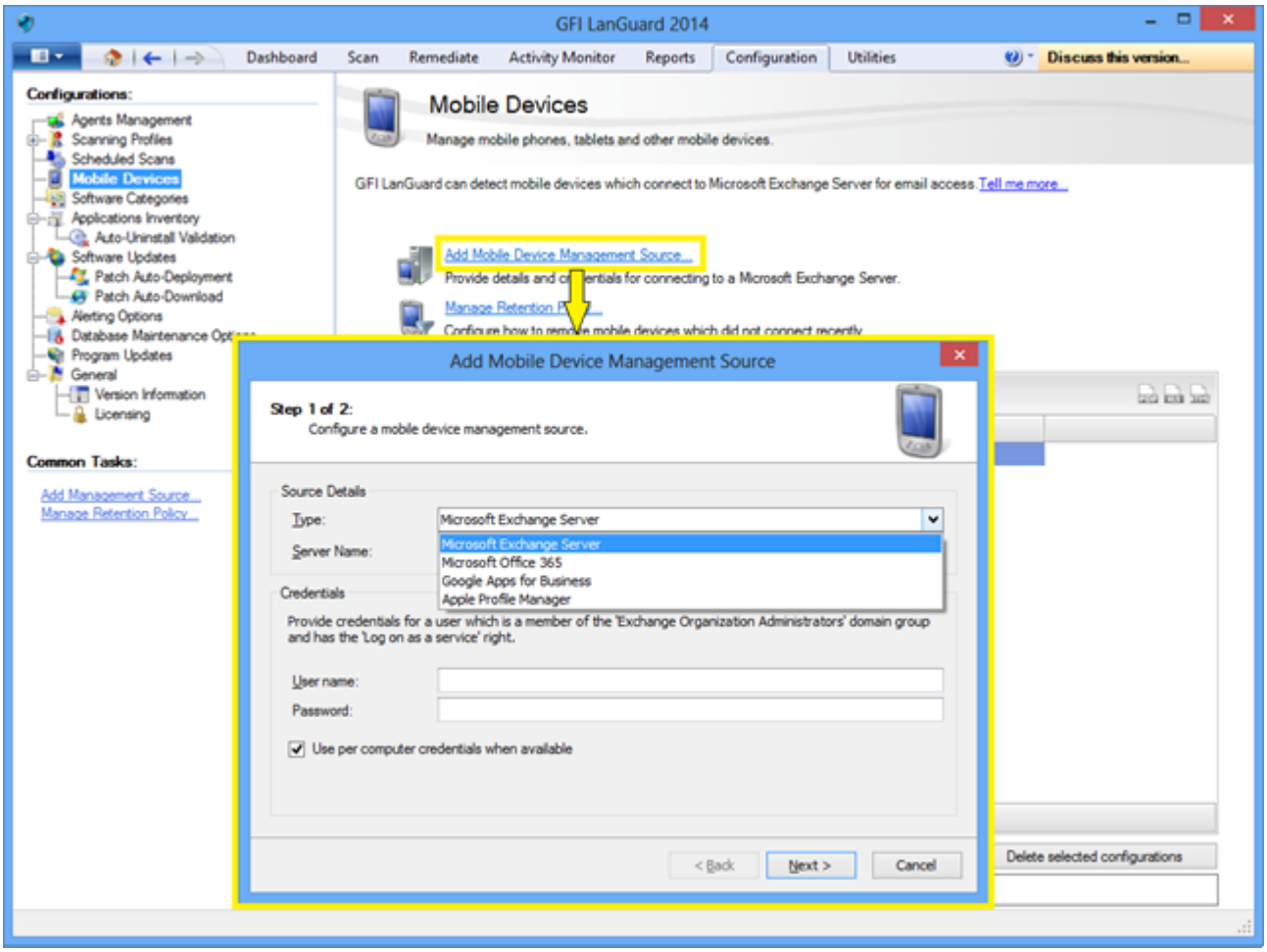
> **附註：**
> 如需重新整理安全資訊，可以使用**儀表板**中的**立即掃描和重新整理**選項，觸發依需求代理程式掃描。

2.3 稽核智慧手機和平板電腦

GFI LanGuard 可以稽核連線到公司的 Microsoft Exchange、Office 365、Google Apps 和 Apple Profiles Manager 等服務的智慧型手機與平板電腦。使用此功能可瞭解您的員工使用哪些行動裝置、這些裝置有什麼安全性問題，以及是否有可補救這些安全性問題的作業系統更新。

> **附註：**
> 行動裝置稽核是無代理程式的。支援的系統有： Google Android、Apple iOS 和 Windows Phone。

使用**組態 > 行動裝置**可新增或編輯行動裝置管理來源。



螢幕擷取畫面 7: 管理行動裝置

可以使用**活動監視器 > 安全性掃描**來監視行動裝置掃描。可以在儀表板中或透過產生報告來檢視行動裝置的掃描結果。行動裝置稽核報告是專門為智慧手機和平板電腦擷取的掃描結果。

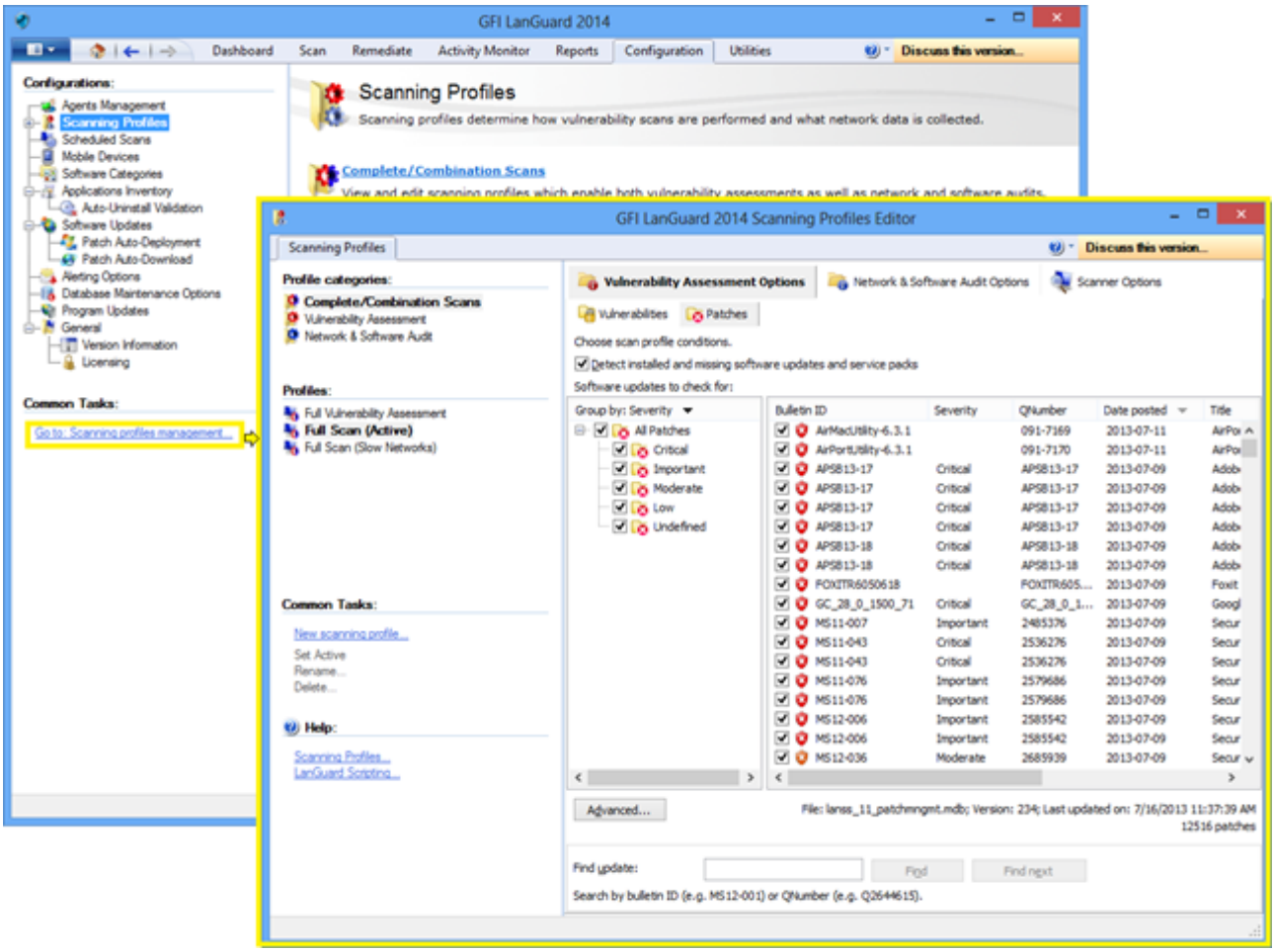
> **附註：**
> 可以向行動裝置擁有者傳送電子郵件通知，告知他們適用於其裝置的作業系統安全性更新。

2.4 掃描設定檔

掃描設定檔決定如何執行安全性掃描：要檢查的安全性問題以及要收集的網路資料。GFI LanGuard 隨附預先定義的掃描設定檔詳盡清單，供您開箱即用。

要檢視、修改或建立新的自訂掃描設定檔：

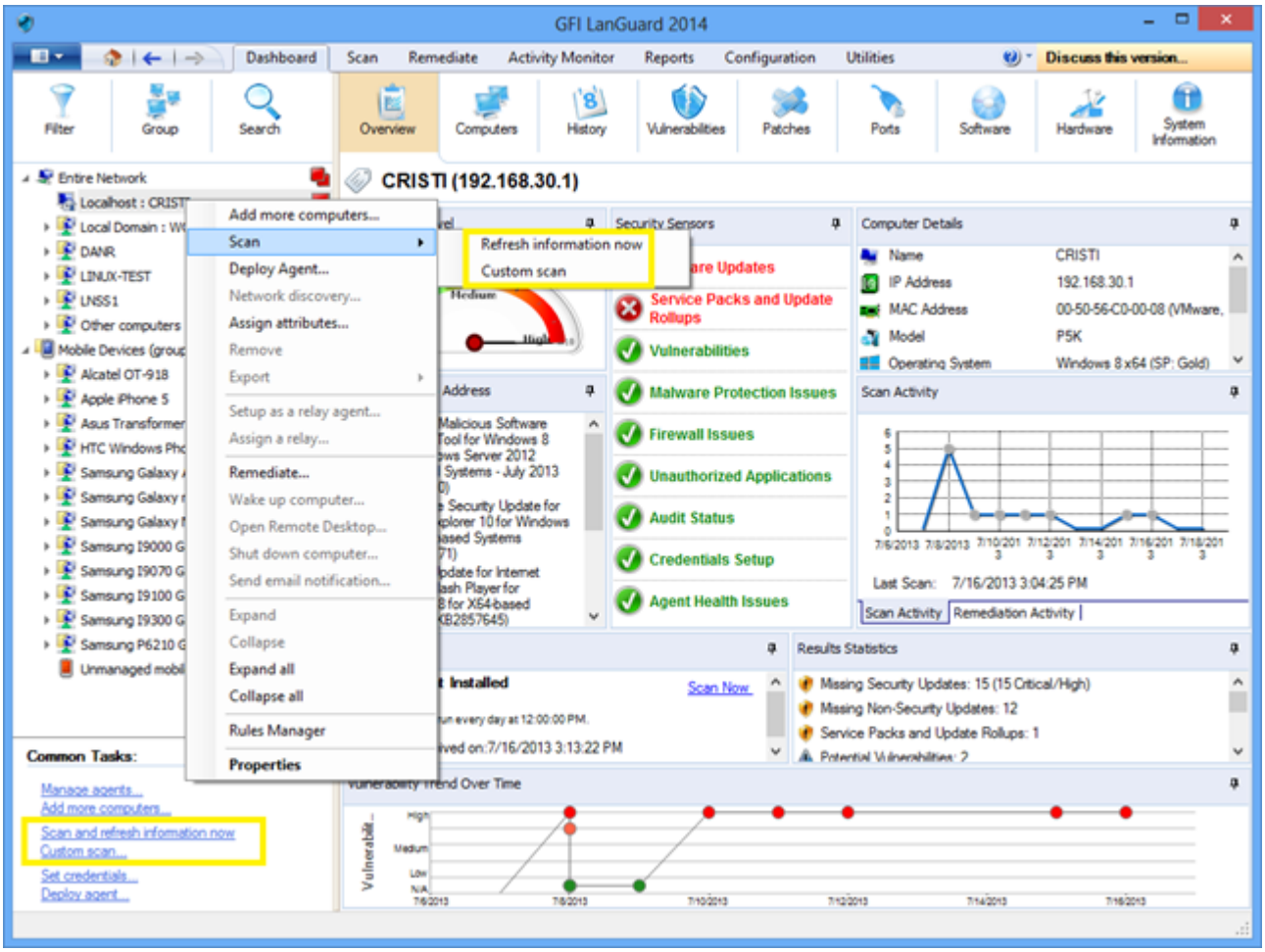
從**組態**中選擇**掃描設定檔**。



螢幕擷取畫面 8: 掃描設定檔

2.5 從儀表板觸發掃描

觸發安全稽核的一個簡單方法是使用**儀表板**。只需從**儀表板**樹選擇電腦/網域/組織單位清單，然後按一下**立即掃描和重新整理資訊**或者**自訂掃描**選項。這兩個選項都在**一般工作**區域，或者以右鍵按一下選擇的電腦。



螢幕擷取畫面 9: 從儀表板觸發掃描

功能	描述
立即掃描和重新整理資訊	此選項可為選擇的電腦立即觸發在背景執行的安全稽核。在安裝代理程式的電腦上，將由代理程式執行掃描，並且在為該代理程式定義的掃描設定檔下執行掃描。對於沒有代理程式的電腦，排程使用**完全掃描**設定檔在背景執行無代理程式掃描。使用**活動監視器 > 安全性掃描**可監視以代理程式為主的掃描和無代理程式的排程的掃描。
自訂掃描	此選項將選擇**掃描**索引標籤，以及用在**儀表板**中選擇的電腦清單預先填入的掃描目標。

3 分析掃描結果

本章節主題：

3.1 儀表板 19
3.2 如何從您的網路中檢視相關安全性變更 21
3.3 如何新增/檢視儀表板中的更多裝置 22
3.4 如何篩選裝置 22
3.5 如何對裝置分組 23
3.6 如何搜尋電腦 25
3.7 全文檢索搜尋 26
3.8 報告 27

3.1 儀表板

儀表板彙總所有掃描的結果，與掃描設定檔無關，與掃描是以代理程式為主還是無代理程式的也無關。目標是立即顯示網路安全性狀態的完整概覽。

另外，執行摘要顯示最易受攻擊的電腦、突出的安全性問題、弱點趨勢。使用者還可以向下鑽研到特定電腦和問題。

左側的電腦樹狀結構顯示按使用者組織的網域和組織單位和行動裝置清單。在右側，儀表板區段為您提供多個檢視，其中包含基於稽核過程中取得的資料的全面安全資訊。另外，儀表板還可讓您判斷目前網路弱點等級、最易受攻擊的的電腦和資料庫中的電腦數量。

- 概覽、
- 電腦、歷程記錄、
- 弱點、
- 修補程式、
- 連接埠、
- 軟體、
- 硬體
- 系統資訊。

螢幕擷取畫面 10: 儀表板

區段	描述
1	此部分提供下列相關資訊： » 按照大量條件來篩選樹狀結構中的裝置，包括作業系統、弱點等級和上次掃描時間等。 » 按照網域和組織單位、作業系統或其他自訂的屬性對電腦分組。可以按照使用者、作業系統或裝置型號對行動裝置進行分組。 » 按照名稱搜尋裝置，或者尋找包含特定關鍵字的掃描結果
2	本部分提供如何檢視和管理 GFI LanGuard 掃描和保護的裝置的相關資訊： » 在**整個網路**節點下列出了伺服器和工作站，以及虛擬機器和以 IP 為主的網路裝置，例如路由器、交換機、印表機等。 » 在**行動裝置**節點下列出了連線到公司的 Microsoft Exchange 伺服器以檢查工作電子郵件的智慧手機和平板電腦 » 樹狀結構右側的圖示指示弱點等級或者稽核是否正在進行中 » 藍色文字的電腦為虛擬電腦 » 使用 **<CTRL> + 按一下**可以選擇多台電腦
3	此區段可讓使用者為在樹狀結構中選擇的裝置觸發動作。
4	此區段可讓使用者為在樹狀結構中選擇的裝置選擇不同的檢視，以顯示統計資訊和掃描結果。
5	此區段可讓使用者檢視目前選擇的裝置。
6	此區段提供檢視在樹狀結構中選擇的裝置的統計資訊和掃描結果的相關資訊： » 安全感測器表示有多少裝置受不同安全性問題的影響 » 從儀表板概覽區域按一下安全感測器或圖表，可向下鑽研到更具體的資料

3.2 如何從您的網路中檢視相關安全性變更

GFI LanGuard 會在下列情況下通知使用者：

» 發現新裝置

» 偵測到新的安全性弱點

» 安裝或移除應用程式

» 啟動或停止服務

» 開啟新連接埠

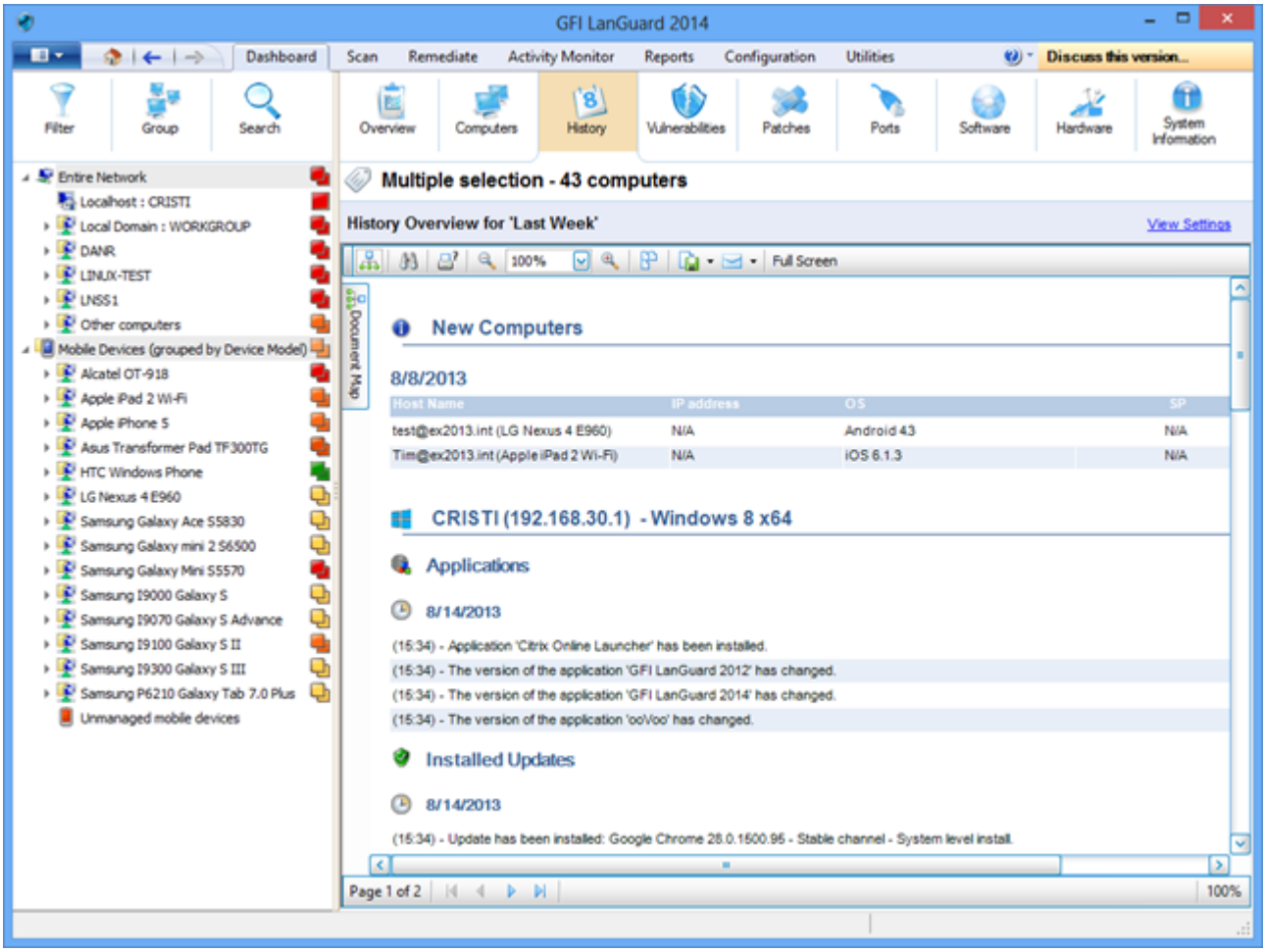
» 建立新共用

» 建立新使用者

» 偵測到硬體變更

要檢視您網路中的相關安全性變更：

1. 按一下**儀表板 > 歷程記錄**。



螢幕擷取畫面 11: 檢視網路中的安全性變更

> **附註：**
> 如果在**警示選項**組態中設定了有效的電子郵件收件者，GFI LanGuard 將預設傳送包含過去 24 小時內整個網路歷程記錄檢視的 每日摘要報告。

3.3 如何新增/檢視儀表板中的更多裝置

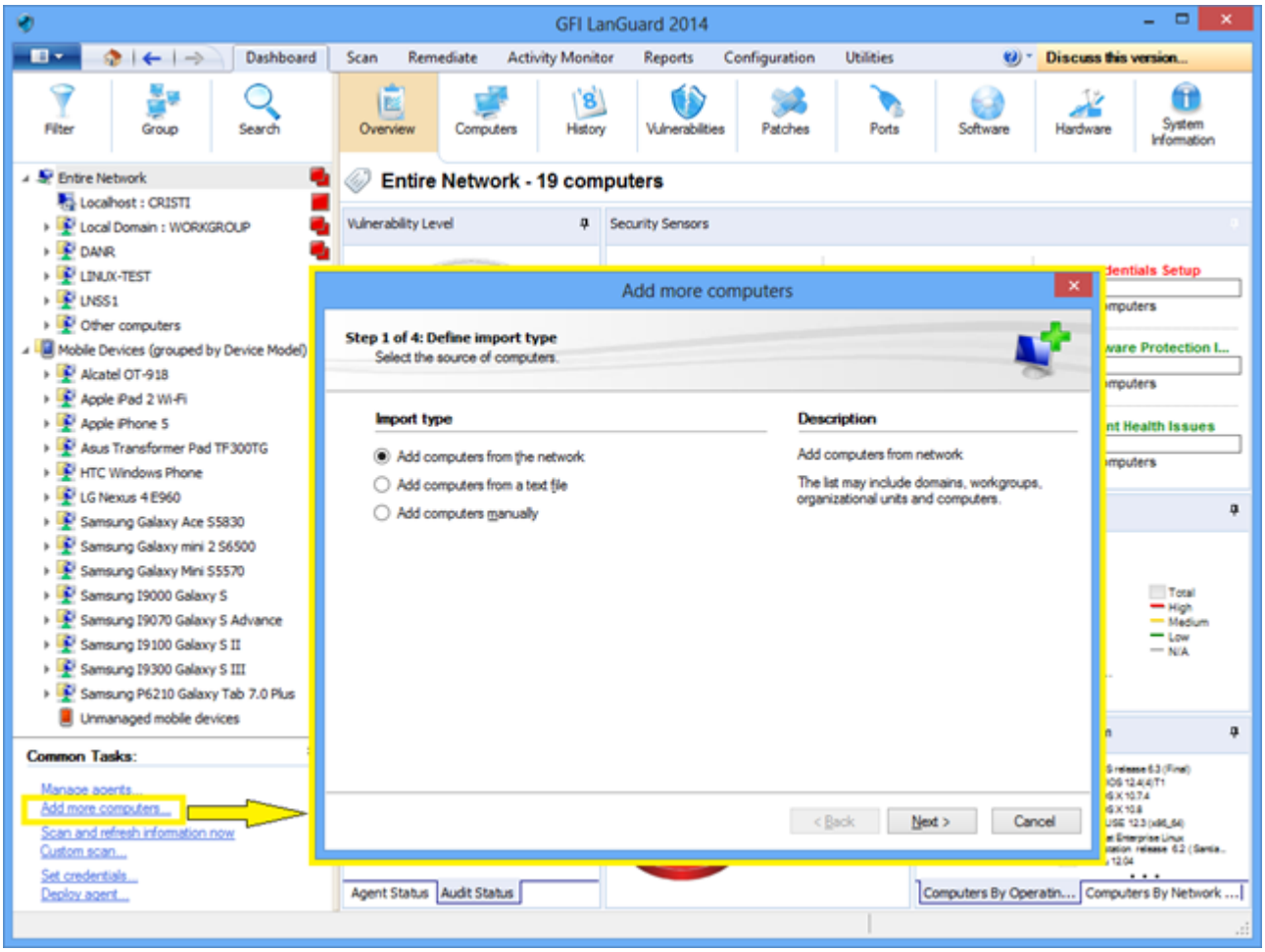
除非進行篩選，否則儀表板樹狀結構將顯示 GFI LanGuard 管理的所有裝置。這表示本產品發現或全部掃描所有裝置。

要在**儀表板**中檢視電腦，需要執行下列操作之一：

1. 透過按一下**掃描**索引標籤，**組態 > 排程的掃描**或命令列掃描，掃描無代理程式的電腦。

2. 按一下**組態 > 代理程式管理**，在電腦上啟用代理程式。

3. 從**儀表板**，按一下**一般工作**下的**新增更多電腦...**，可新增整個網域/工作群組和組織單位或特定電腦清單。

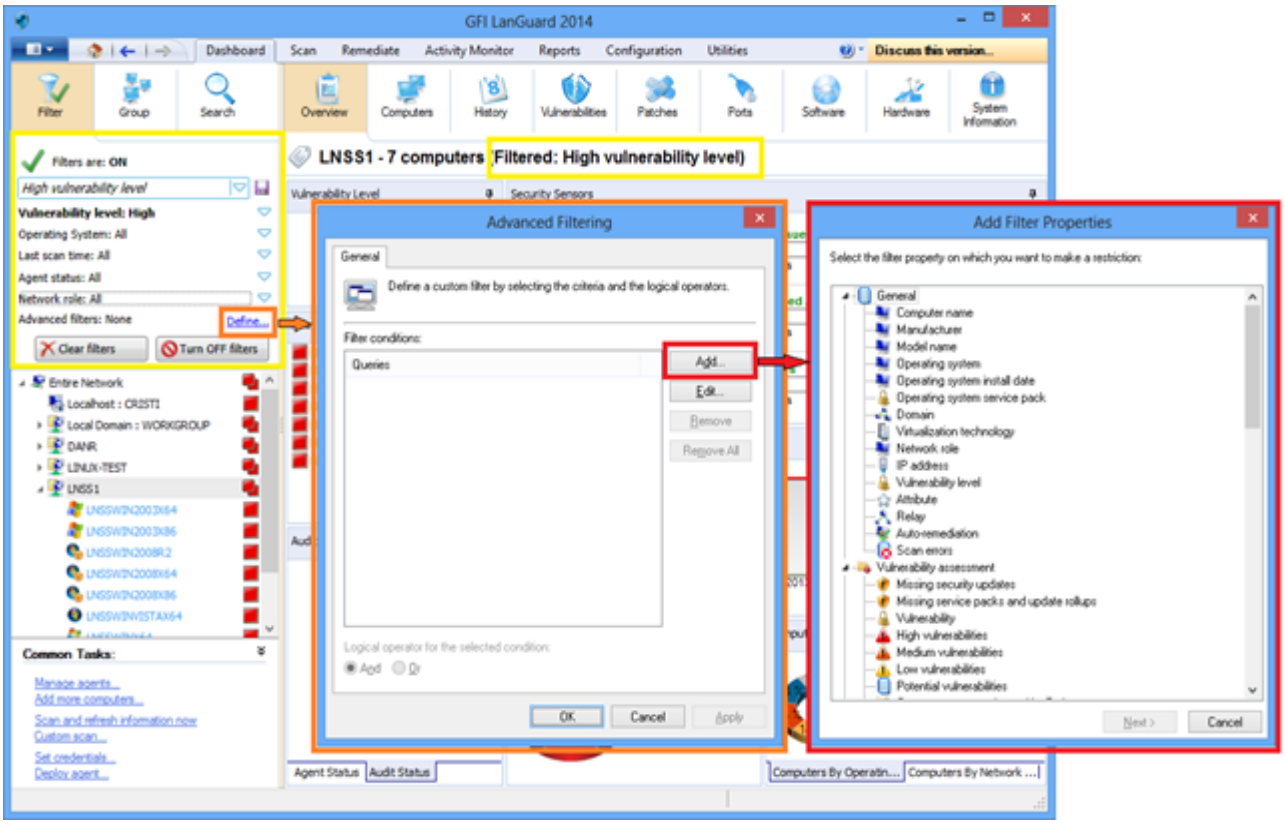


螢幕擷取畫面 12: 從儀表板新增和檢視電腦

若要稽核智慧手機和平板電腦，請使用**組態 > 行動裝置**新增或編輯行動裝置管理來源（ 提供有關 Microsoft Exchange 伺服器的詳細資訊） 。

3.4 如何篩選裝置

使用**儀表板**、**補救**和**報告**檢視中的篩選區域，可篩選在螢幕左側的樹中顯示的裝置：

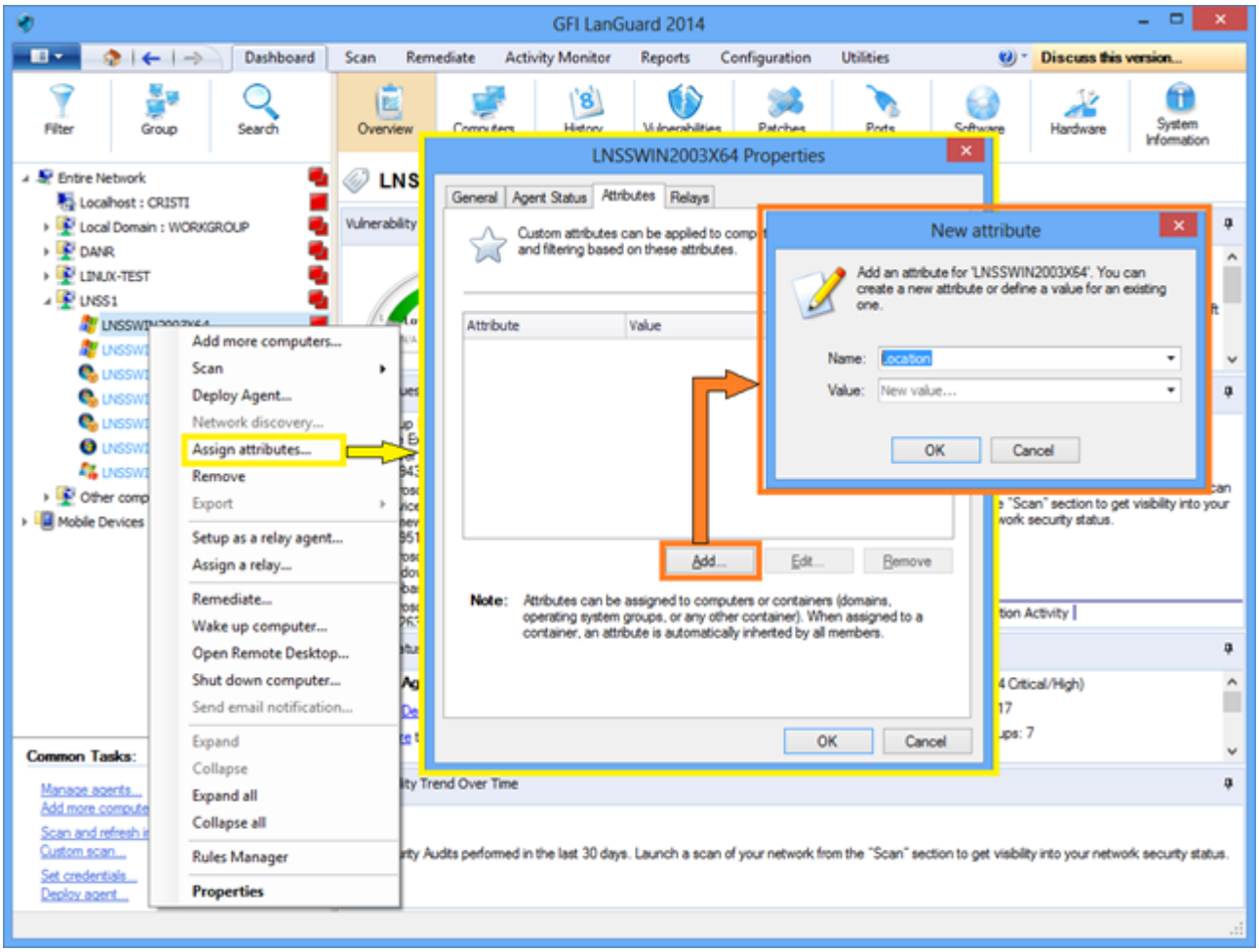


螢幕擷取畫面 13: 篩選電腦

3.5 如何對裝置分組

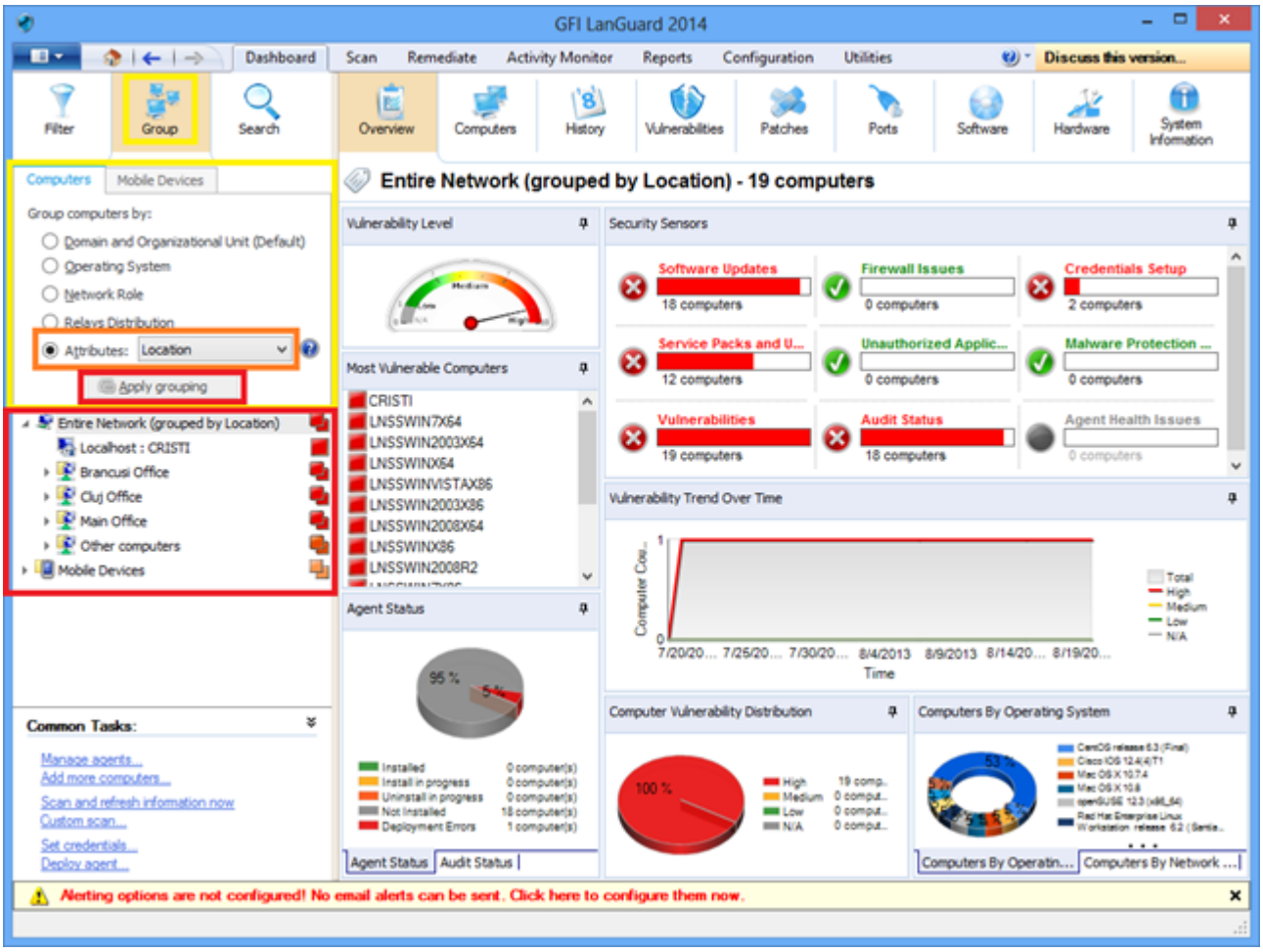
可以按照預先定義的條件對樹中的電腦進行分組，例如按照網域和組織單位(預設分組) 、作業系統、網路角色、轉送分佈或使用者定義的自訂屬性。可以按照使用者(預設分組) 、作業系統、裝置型號和自訂屬性對行動裝置進行分組。

3.5.1 定義自訂屬性



螢幕擷取畫面 14: 定義自訂屬性

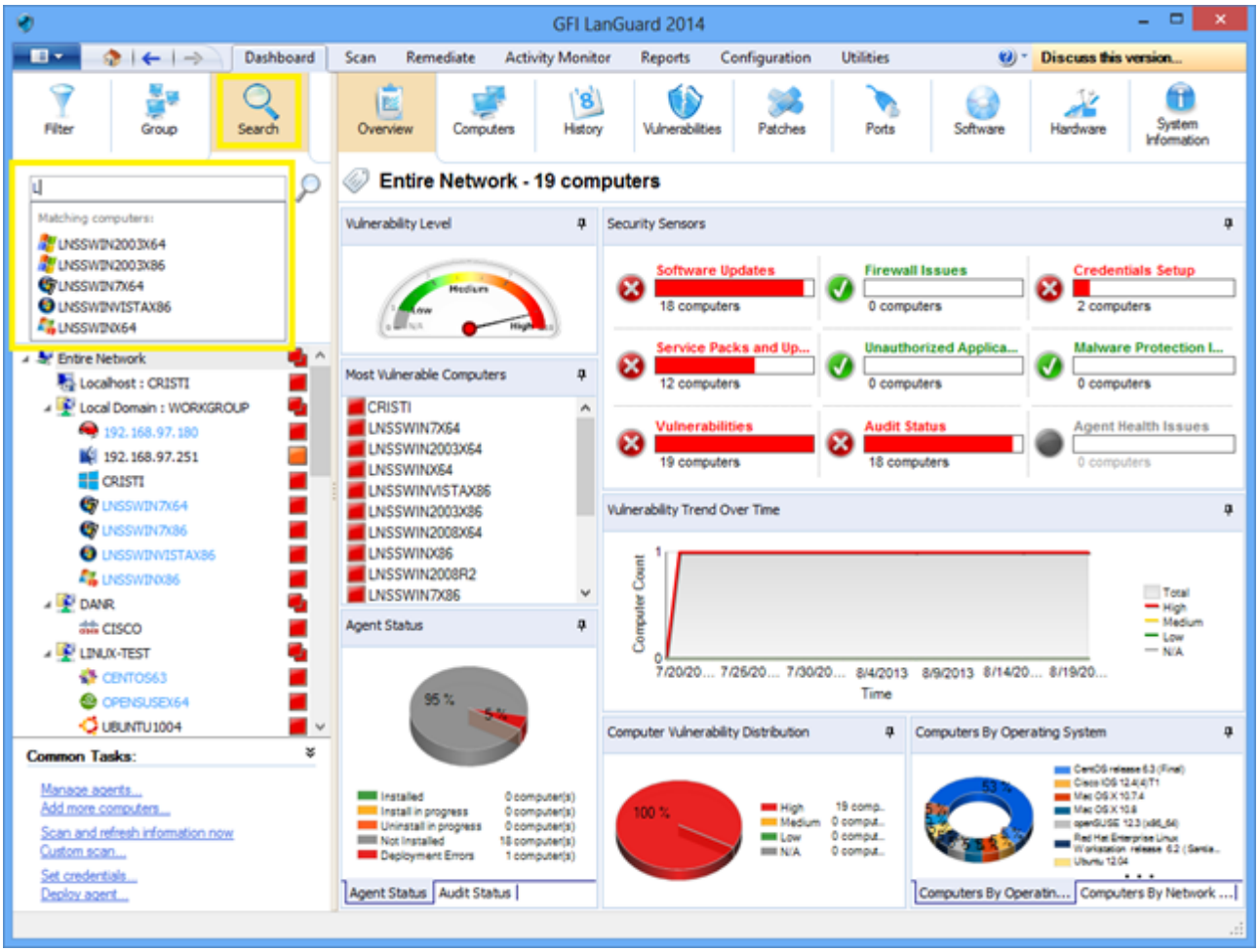
3.5.2 按定義的屬性檢視電腦



螢幕擷取畫面 15: 按定義的屬性檢視電腦

3.6 如何搜尋電腦

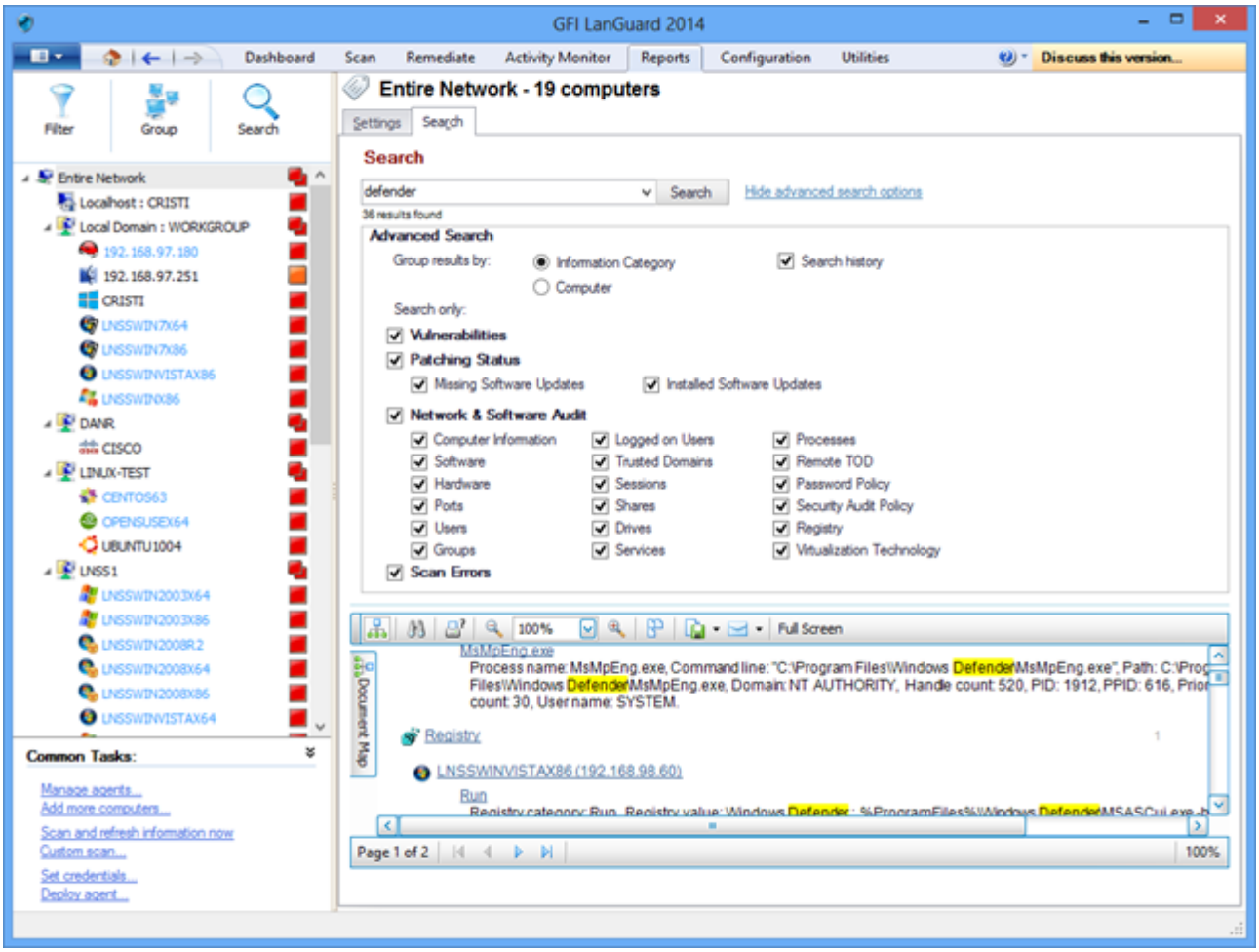
如果管理大量裝置，在樹狀結構中尋找裝置可能會很費時。使用**儀表板**、**補救**和**報告**檢視中的搜尋區域，可立即找到裝置。



螢幕擷取畫面 16: 搜尋電腦

3.7 全文檢索搜尋

使用**儀表板**、**補救**和**報告**檢視的搜尋區域，可根據關鍵字立即在掃描結果中尋找資訊。



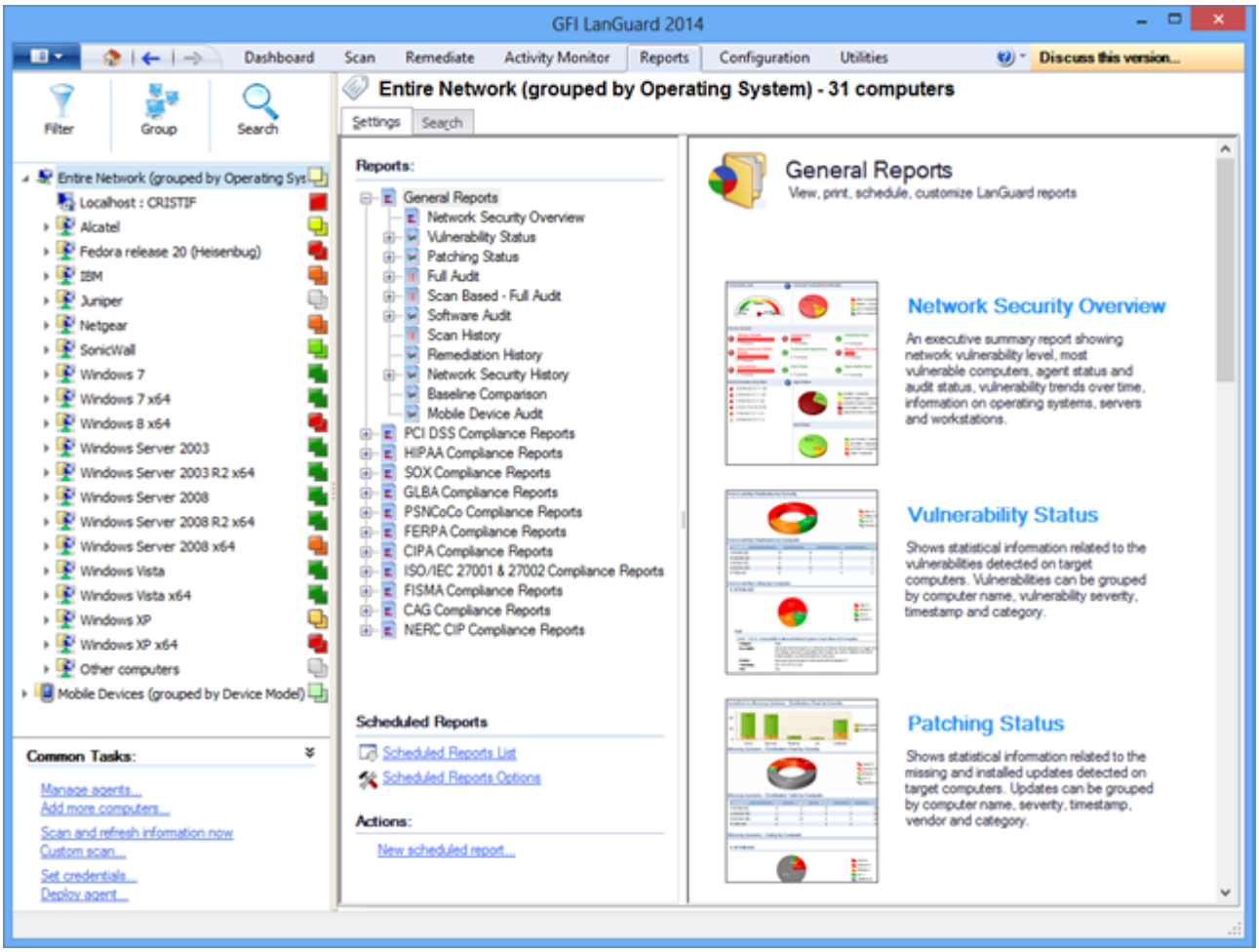
螢幕擷取畫面 17: 全文檢索搜尋

可以按特定類別組織搜尋結果。還可以排除在其他類別中找到的結果。

3.8 報告

GFI LanGuard 包含大量預先定義的執行、技術和統計報告。所有報告都可以自訂、更名、排程定期產生，並且匯出為各種常見格式，如 PDF、HTML、RTF、XLS。

此外，GFI LanGuard 隨附一套專門用來遵守各種標準和法律的報告，其中包括 PCI DSS、HIPAA、SOX、GLBA 和 PSN CoCo 規範。


GFI LanGuard 2014
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
Entire Network (grouped by Operating System) - 31 computers
Settings
Search
Reports:
General Reports
Network Security Overview
Vulnerability Status
Patching Status
Full Audit
Scan Based - Full Audit
Software Audit
Scan History
Remediation History
Network Security History
Baseline Comparison
Mobile Device Audit
PCI DSS Compliance Reports
HIPAA Compliance Reports
SOX Compliance Reports
GLBA Compliance Reports
PSNCoCo Compliance Reports
FERPA Compliance Reports
CIPA Compliance Reports
ISO/IEC 27001 & 27002 Compliance Reports
FISMA Compliance Reports
CAG Compliance Reports
NERC CIP Compliance Reports
Scheduled Reports
Scheduled Reports List
Scheduled Reports Options
Actions:
New scheduled report...
General Reports
View, print, schedule, customize LanGuard reports
Network Security Overview
An executive summary report showing network vulnerability level, most vulnerable computers, agent status and audit status, vulnerability trends over time, information on operating systems, servers and workstations.
Vulnerability Status
Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by computer name, vulnerability severity, timestamp and category.
Patching Status
Shows statistical information related to the missing and installed updates detected on target computers. Updates can be grouped by computer name, severity, timestamp, vendor and category.
Entire Network (grouped by Operating Sys...
Localhost : CRISTIF
Alcatel
Fedora release 20 (Heisenbug)
IBM
Juniper
Netgear
SonicWall
Windows 7
Windows 7 x64
Windows 8 x64
Windows Server 2003
Windows Server 2003 R2 x64
Windows Server 2008
Windows Server 2008 R2 x64
Windows Server 2008 x64
Windows Vista
Windows Vista x64
Windows XP
Windows XP x64
Other computers
Mobile Devices (grouped by Device Model)
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...

螢幕擷取畫面 18: 報告

4 補救安全性問題

本章節主題：

4.1 部署缺少的軟體更新 29
4.2 解除安裝未經授權的應用程式 32
4.3 部署自訂軟體 35
4.4 傳送電子郵件通知給行動裝置擁有者 36
4.5 其他補救作業 37

4.1 部署缺少的軟體更新

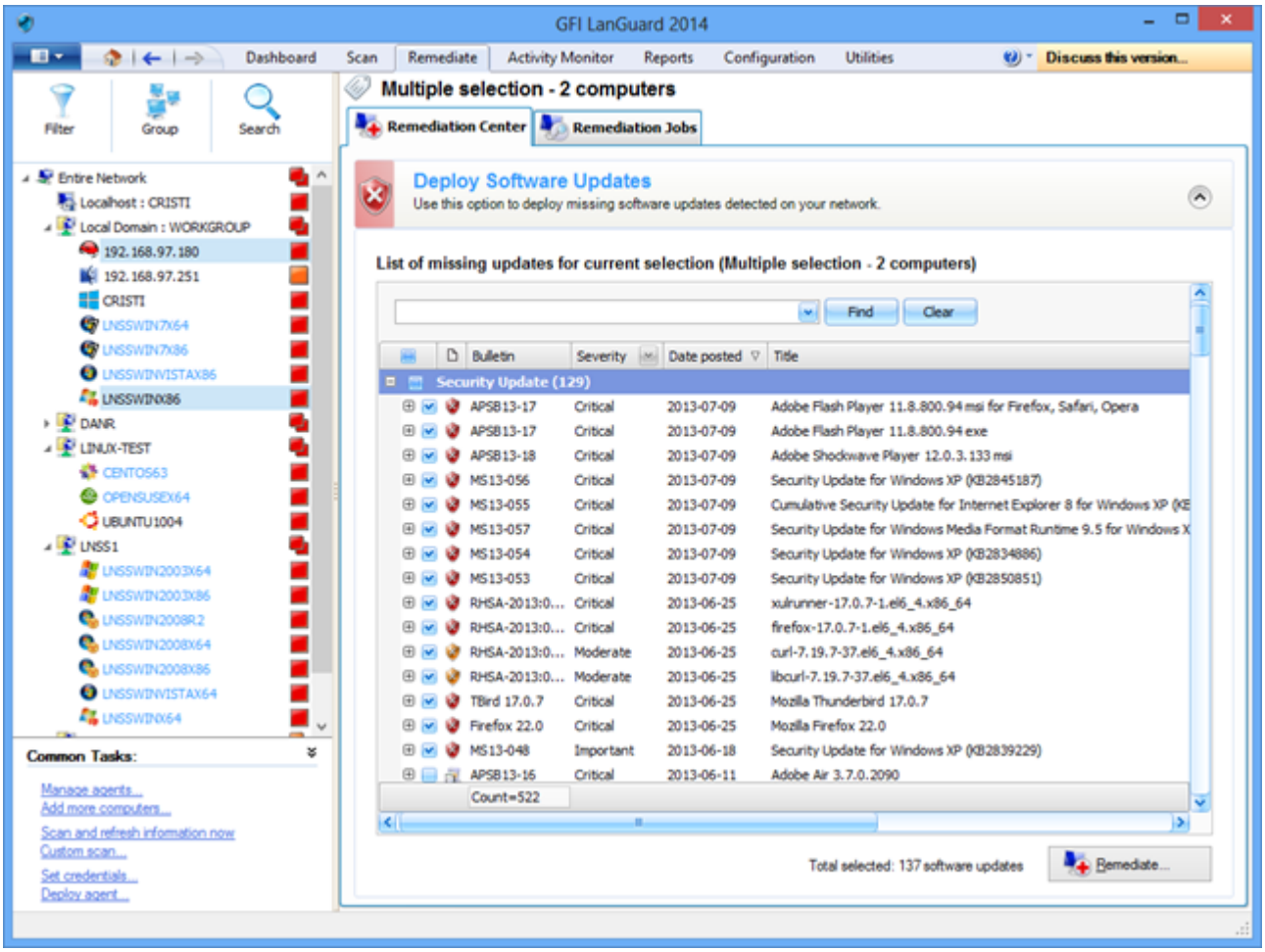
要部署缺少的安全性和非安全性更新：

1. 按一下**補救 > 補救中心 > 部署軟體更新**
2. 從螢幕左側部分的電腦樹狀結構中選擇需要部署的電腦或電腦群組修補程式。

附註：

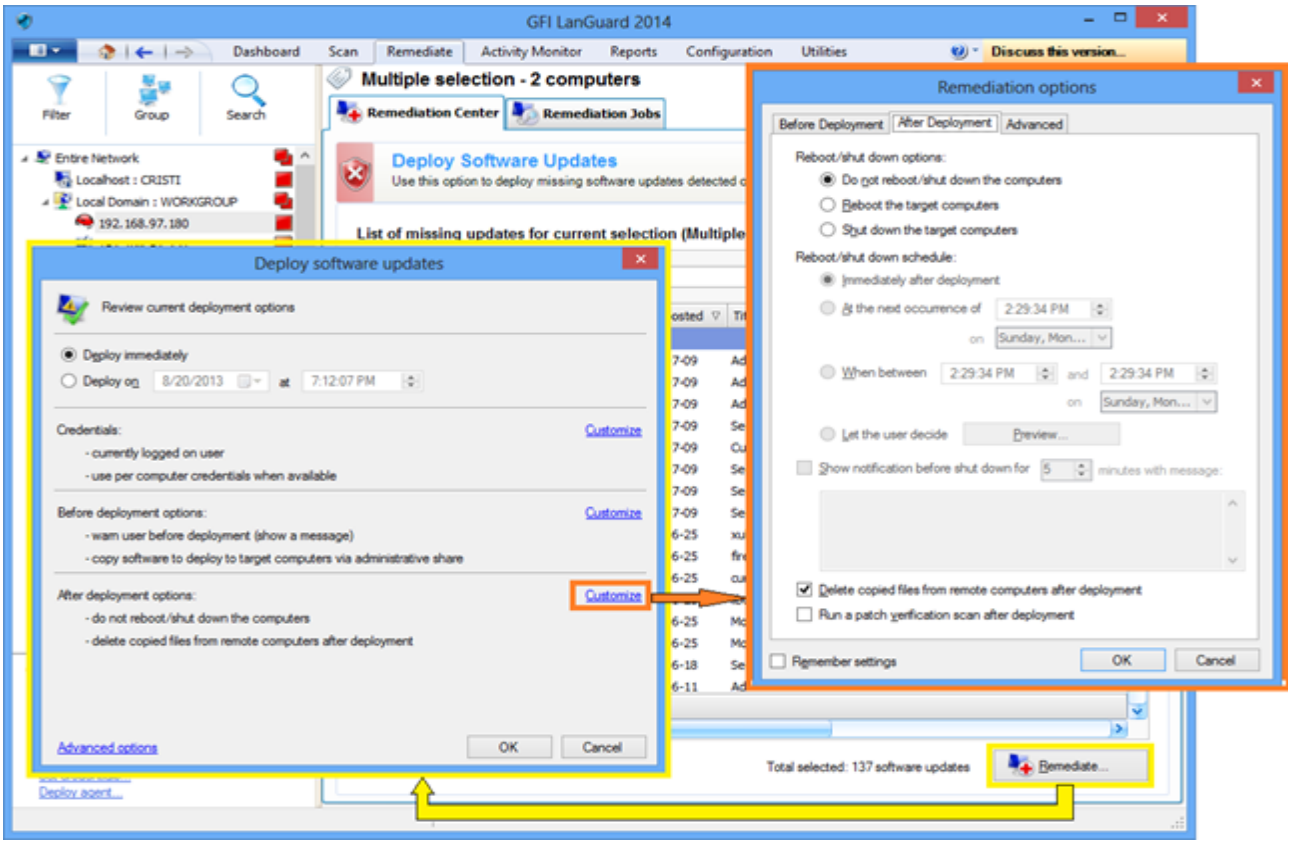
» 使用 <CTRL> + **按一下**可以在電腦樹狀結構中選擇多個項目。

» 要在大型網路中輕鬆找到電腦，可以按照大量條件來篩選樹狀結構中的電腦。如需詳細資訊，請參閱 如何篩選裝置 (page 22)。



螢幕擷取畫面 19: 部署軟體更新

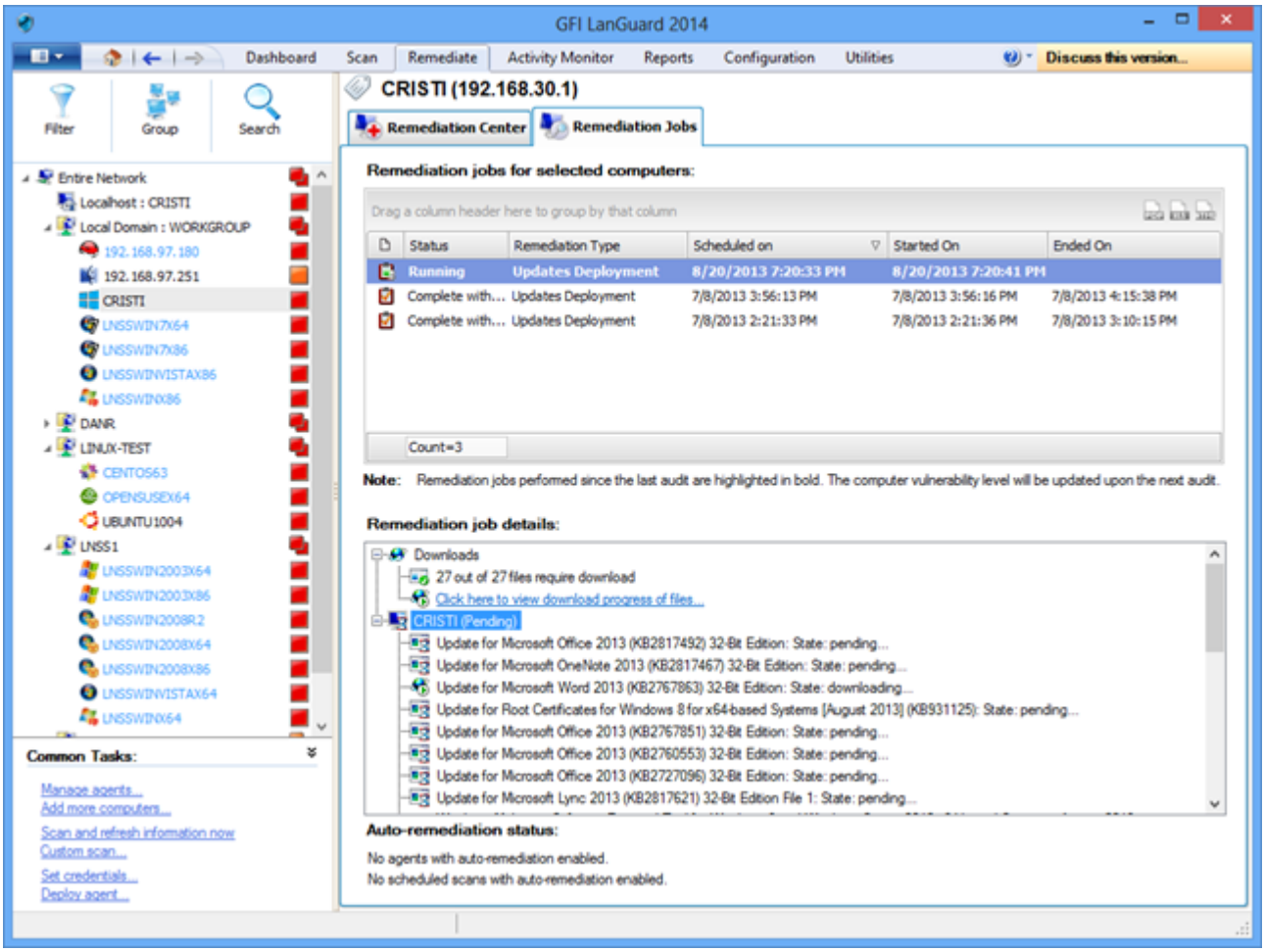
在**部署軟體更新**螢幕，可以檢視所選電腦所有缺少的更新，以及每個更新的詳細資訊。透過選擇或取消選擇修補程式或電腦，可以對部署進行微調。



螢幕擷取畫面 20: 補救選項

要開始部署操作：

1. 從**補救**中選擇**補救作業**。
2. 從**部署軟體選項**精靈設定部署排程
3. 從**補救選項**精靈選擇重新開機選項，並按一下**確定**。



螢幕擷取畫面 21: 電腦重新掃描

4. 完成部署後，重新掃描電腦以取得其安全性狀態。

附註：

» 大量的更新需要重新啟動目標電腦才能完成部署。

» 如果在部署作業之後仍缺少更新，請確定機器已重新開機。

附註：

可以設定 GFI LanGuard 自動部署缺少的更新。如需詳細資訊，請參閱 自動補救作業 (page 43)。

4.2 解除安裝未經授權的應用程式

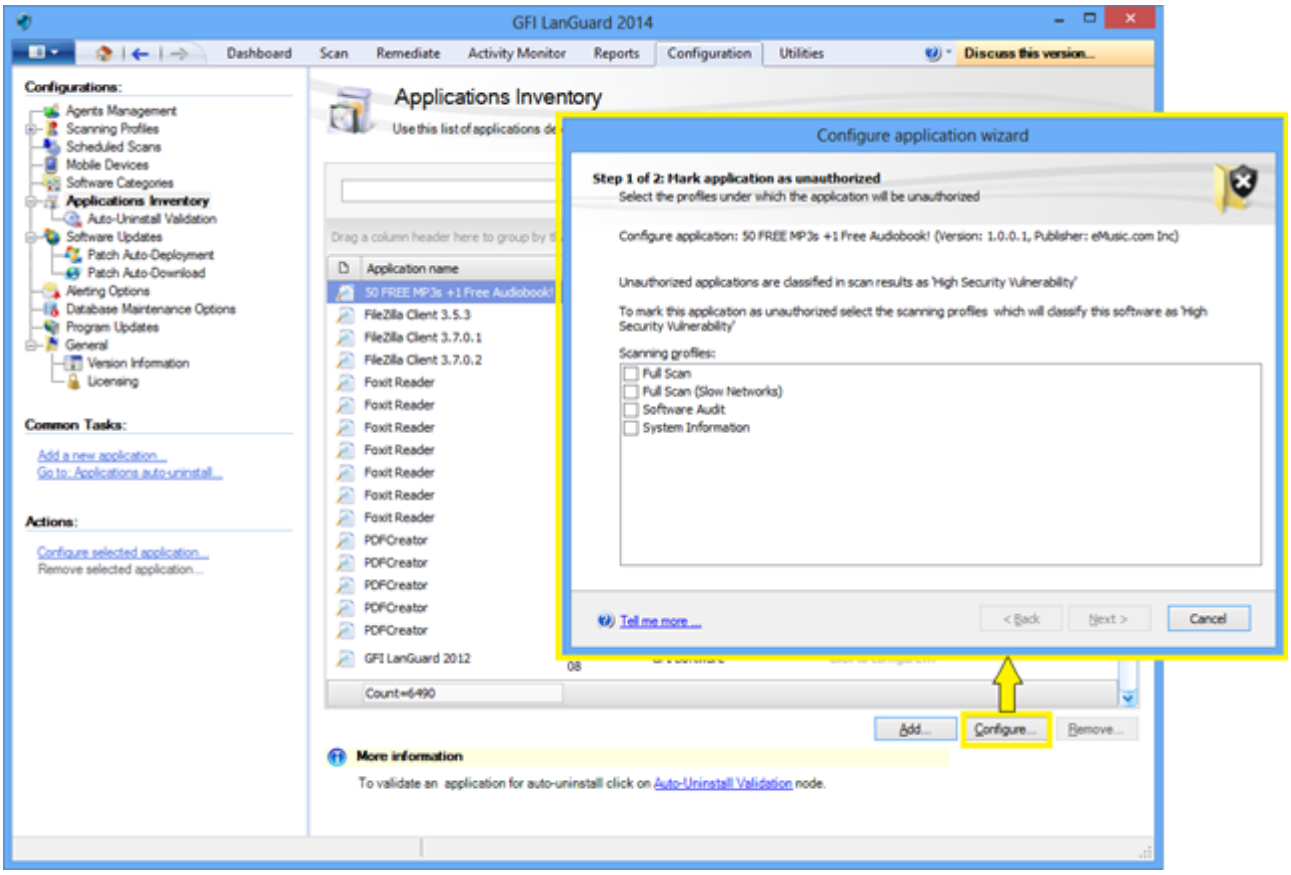
對網路執行全面稽核或軟體稽核，以獲得安裝應用程式的清查。如需詳細資訊，請參閱 執行安全性掃描 (page 9)。

附註：

即使未偵測到網路上安裝的未授權應用程式，但仍可使用 **新增...** 」按鈕新增這些應用程式。

若要標記未經授權的應用程式，請執行以下操作：

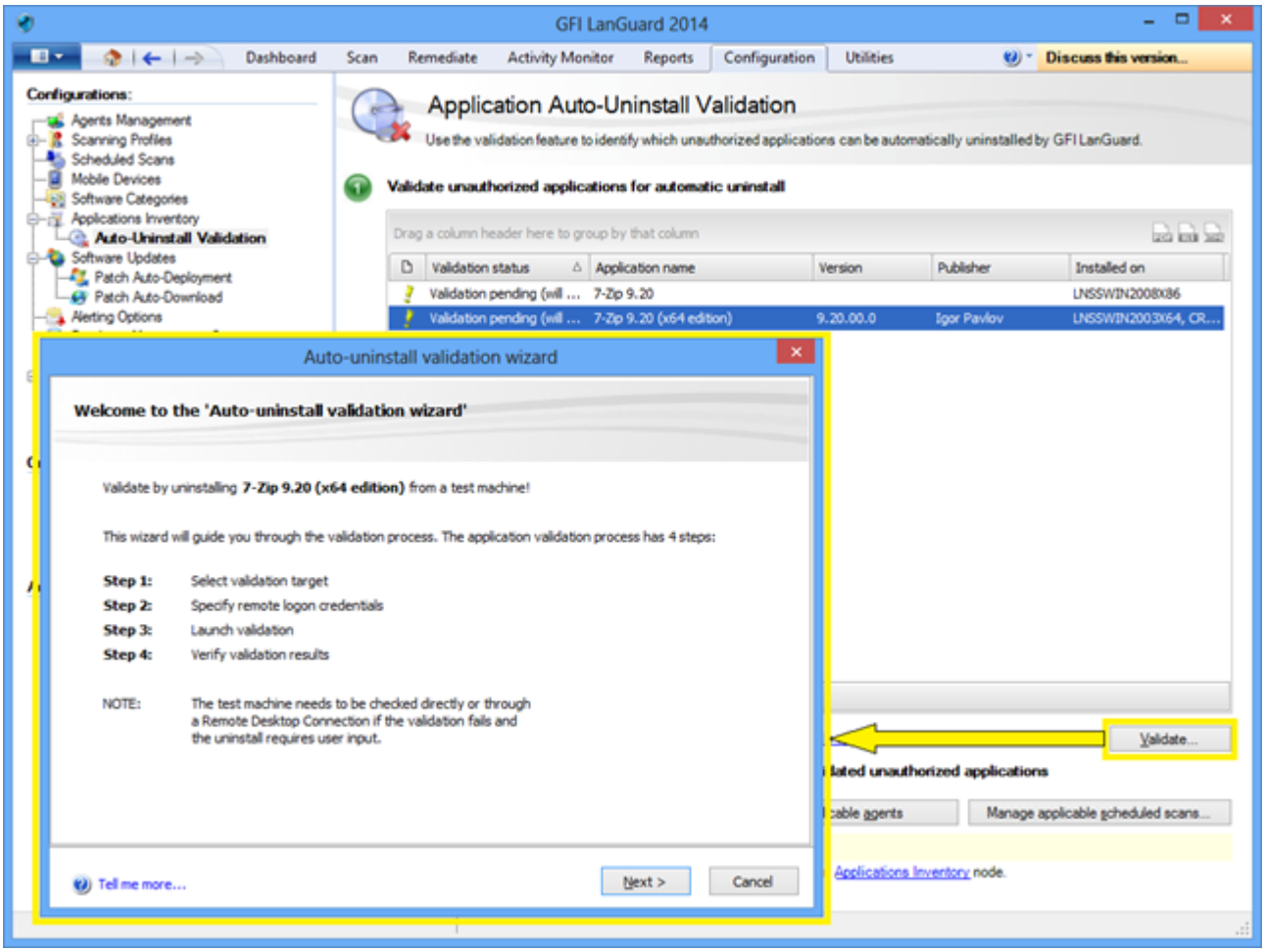
1. 按一下**組態 > 應用程式清查。**



螢幕擷取畫面 22: 標記未經授權的應用程式

2. 使用**組態 > 自動解除安裝驗證**」可測試 GFI LanGuard 能否成功自動解除安裝未經授權的應用程式。

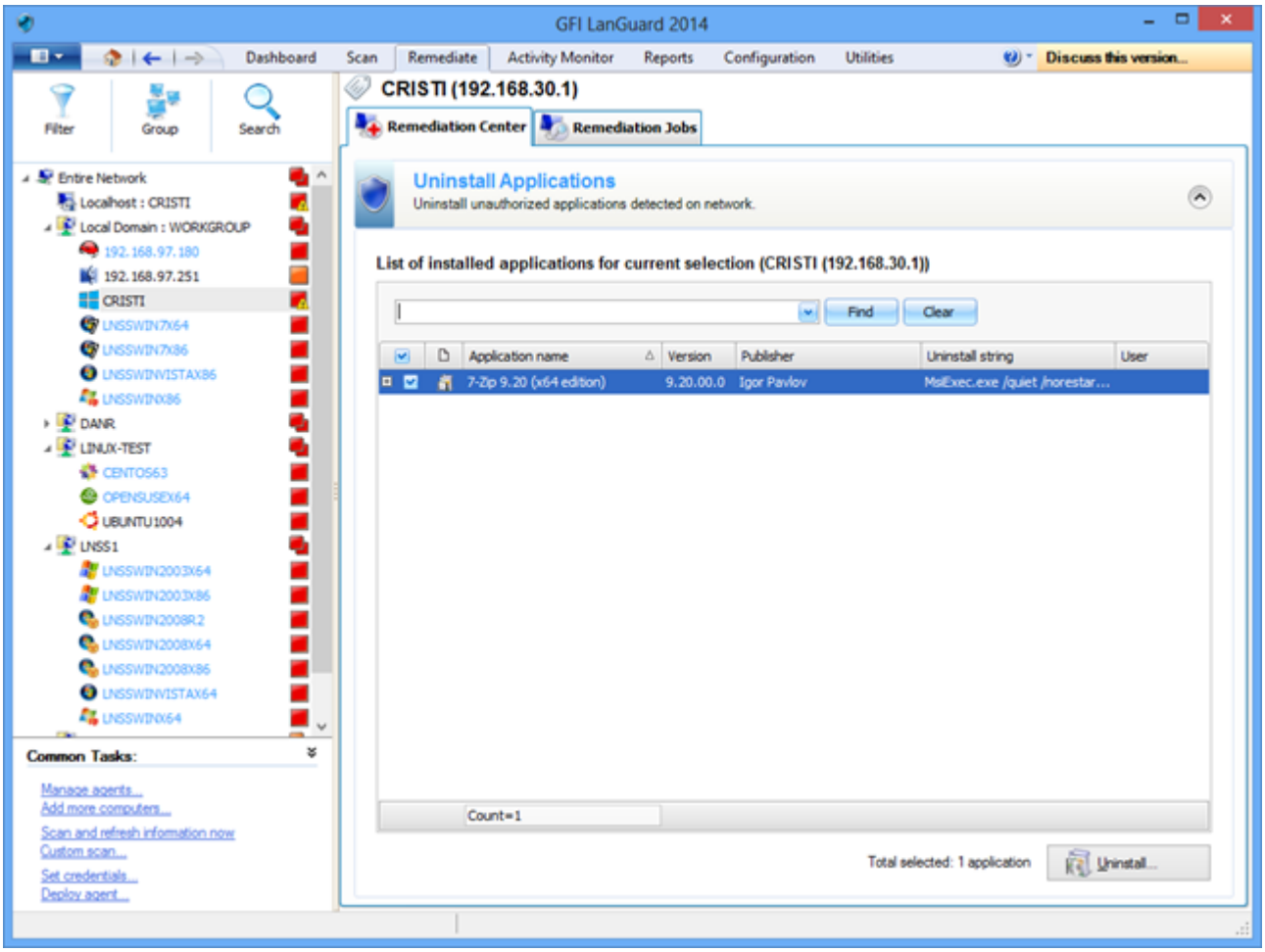
> **附註：**
> 部分應用程式不支援自動解除安裝，它們無法透過 GFI LanGuard 刪除，因為解除安裝過程將對目標電腦的最終使用者顯示對話方塊，並等待他們的輸入，這樣會干擾他們的工作。



螢幕擷取畫面 23: 應用程式自動解除安裝驗證

3. 再次重新掃描您的網路以偵測所有未經授權的應用程式。

4. 使用**補救 > 補救中心 > 解除安裝應用程式**刪除網路中的未授權應用程式



螢幕擷取畫面 24: 解除安裝應用程式

5. 解除安裝完成後，重新掃描電腦以獲得其安全性狀態。

附註：
GFI LanGuard 可設定為自動偵測和刪除網路中的任何未授權應用程式。如需詳細資訊，請參閱 自動補救作業 (page 43)。

4.3 部署自訂軟體

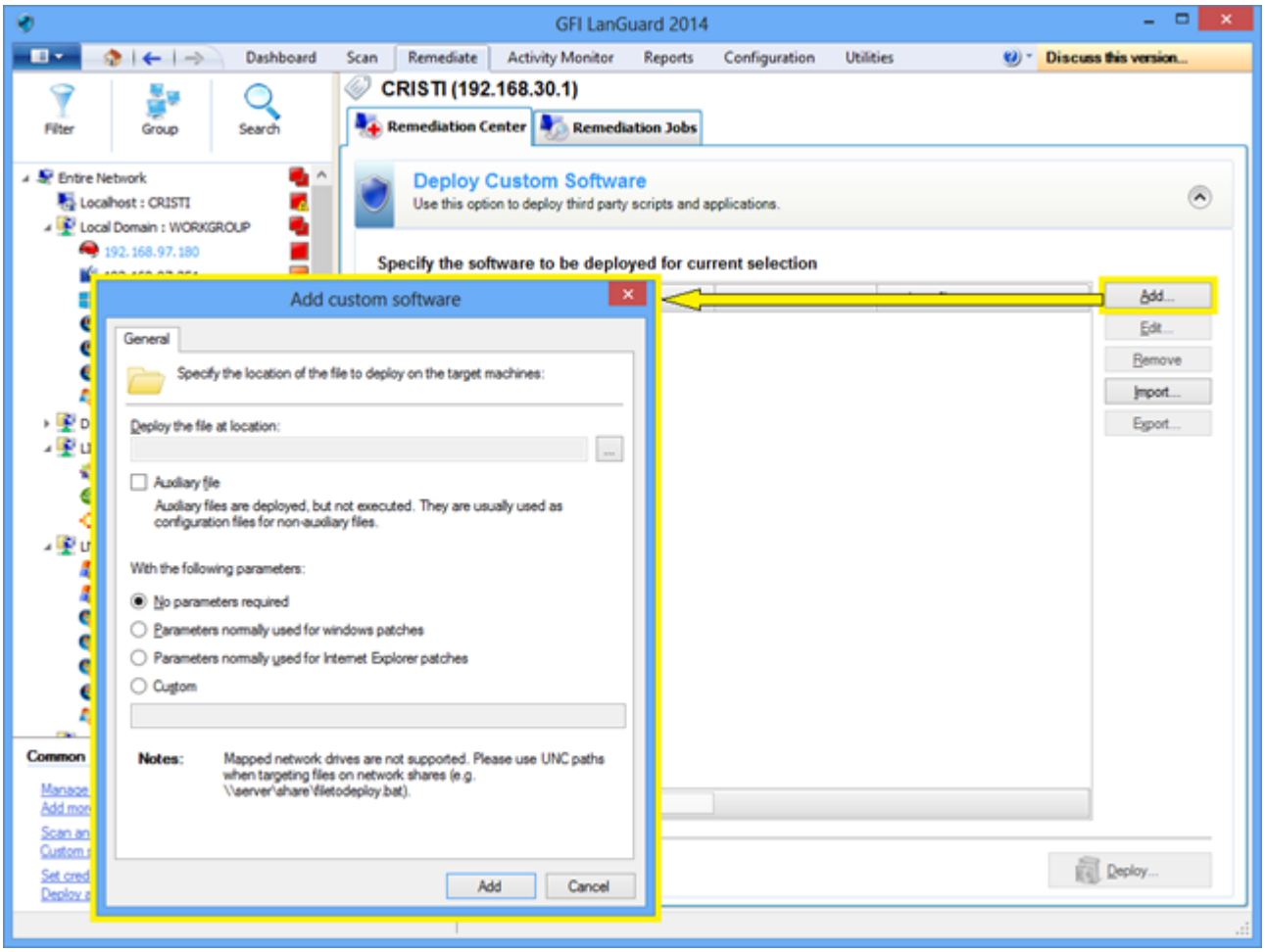
GFI LanGuard 可以在網路範圍內部署自訂軟體和指令碼。可用無訊息模式執行的軟體的幾乎任何部分都可以使用 GFI LanGuard 部署。

要將自訂軟體和指令碼部署到您的網路中：

1. 按一下**補救 > 補救中心 > 部署自訂軟體**

2. 從螢幕左側部分的電腦樹狀結構中選擇需要部署的電腦或電腦群組修補程式。

附註：
必須手動指定自訂軟體，並且根據需要，指定用於無訊息模式安裝的參數和組態檔。

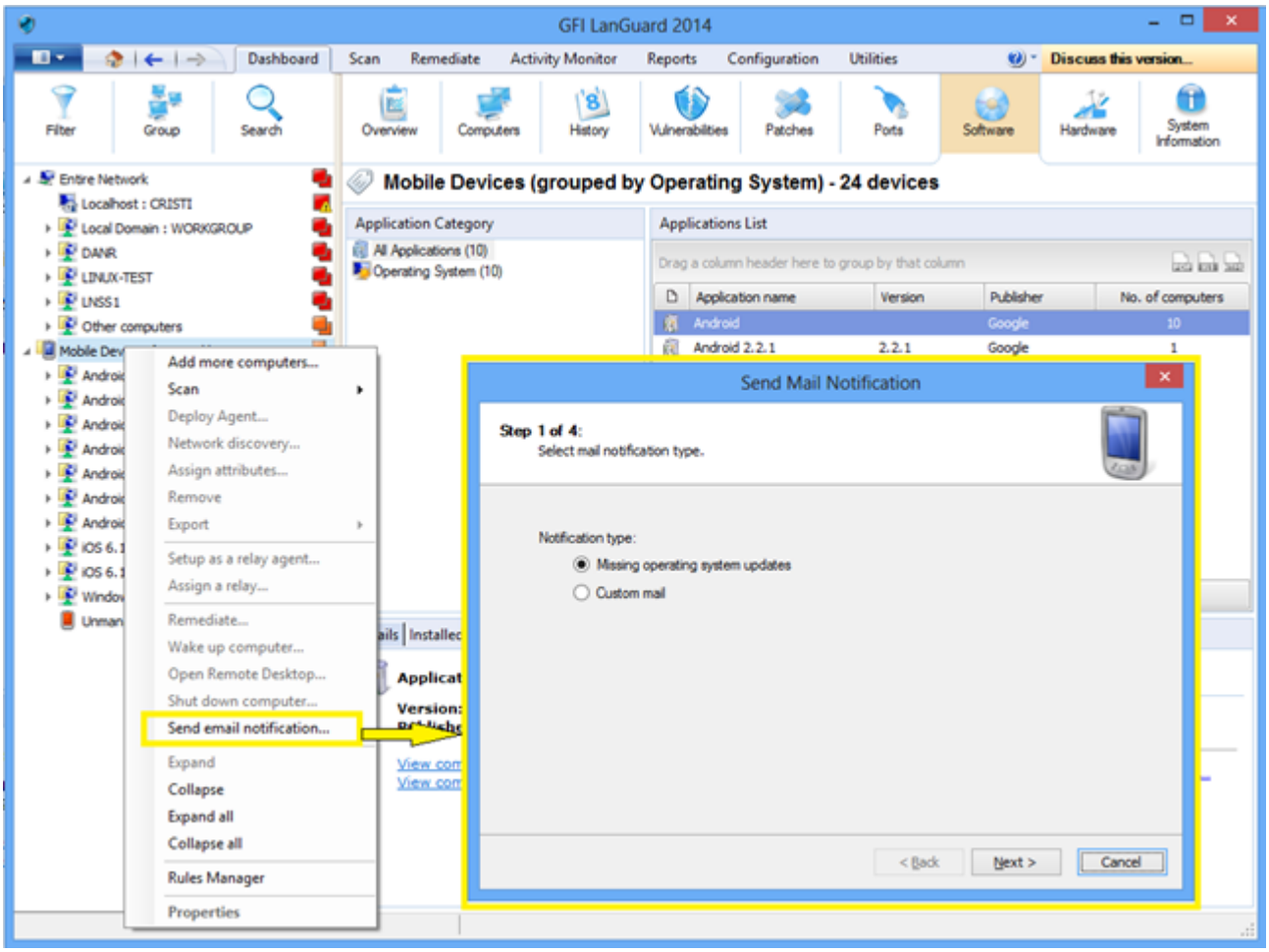


螢幕擷取畫面 25: 部署自訂軟體

4.4 傳送電子郵件通知給行動裝置擁有者

IT 管理員可以使用 GFI LanGuard 向連線到公司的 Microsoft Exchange、Office 365、Google Apps 或 Apple Profiles Manager 等服務的智慧型手機與平板電腦擁有者傳送自訂電子郵件通知。可以使用預先定義的電子郵件範本來通知裝置擁有者在其裝置上安裝的作業系統的最新更新。

在儀表板樹狀結構中以右鍵按一下行動裝置或行動裝置群組，選擇**傳送電子郵件通知**選項，以向行動裝置擁有者傳送電子郵件訊息。



螢幕擷取畫面 26: 傳送電子郵件通知

4.5 其他補救作業

若要檢視 GFI LanGuard 內可用的所有補救作業：

1. 從**補救**中選擇**補救中心**

GFI LanGuard 允許諸如下列補救作業：

» 回復修補程式 – 此選項在安裝的安全性更新干擾您的業務環境時非常有用

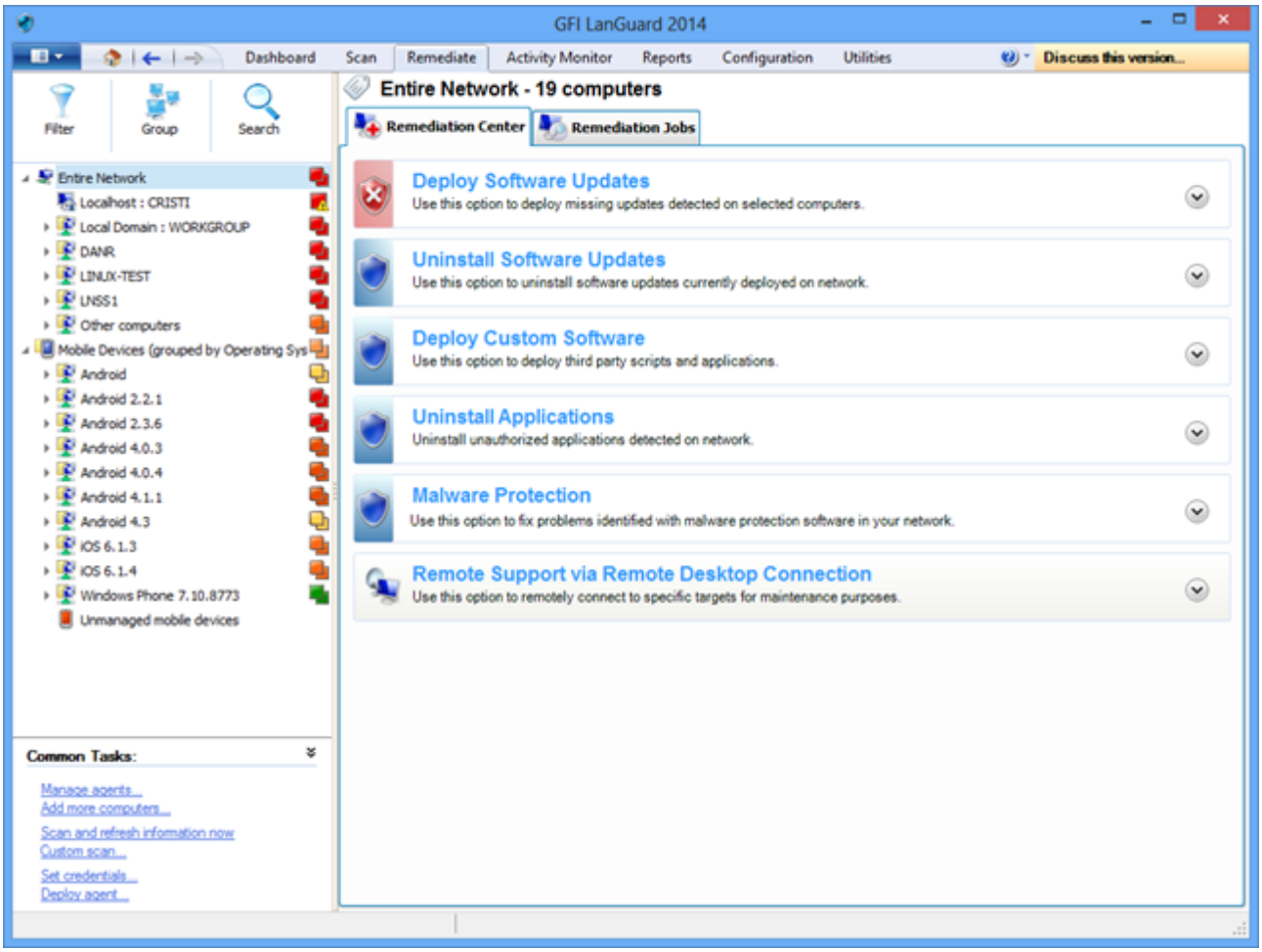
» 觸發防毒軟體和反間諜軟體的定義更新

» 在遠端電腦上觸發防毒軟體和反間諜軟體掃描

» 啟用防毒和反間諜軟體解決辦法的即時保護

» 開啟防火牆

» 在目標電腦上開啟遠端桌面連線，以迅速解決無法自動補救的安全性問題



螢幕擷取畫面 27: 其他補救作業

5 自動執行工作

本章節主題：

5.1 自動探索網路中的新裝置 39
5.2 自動稽核安全性 40
5.3 自動下載修補程式 42
5.4 自動補救作業 43
5.5 自動產生報告 48

5.1 自動探索網路中的新裝置

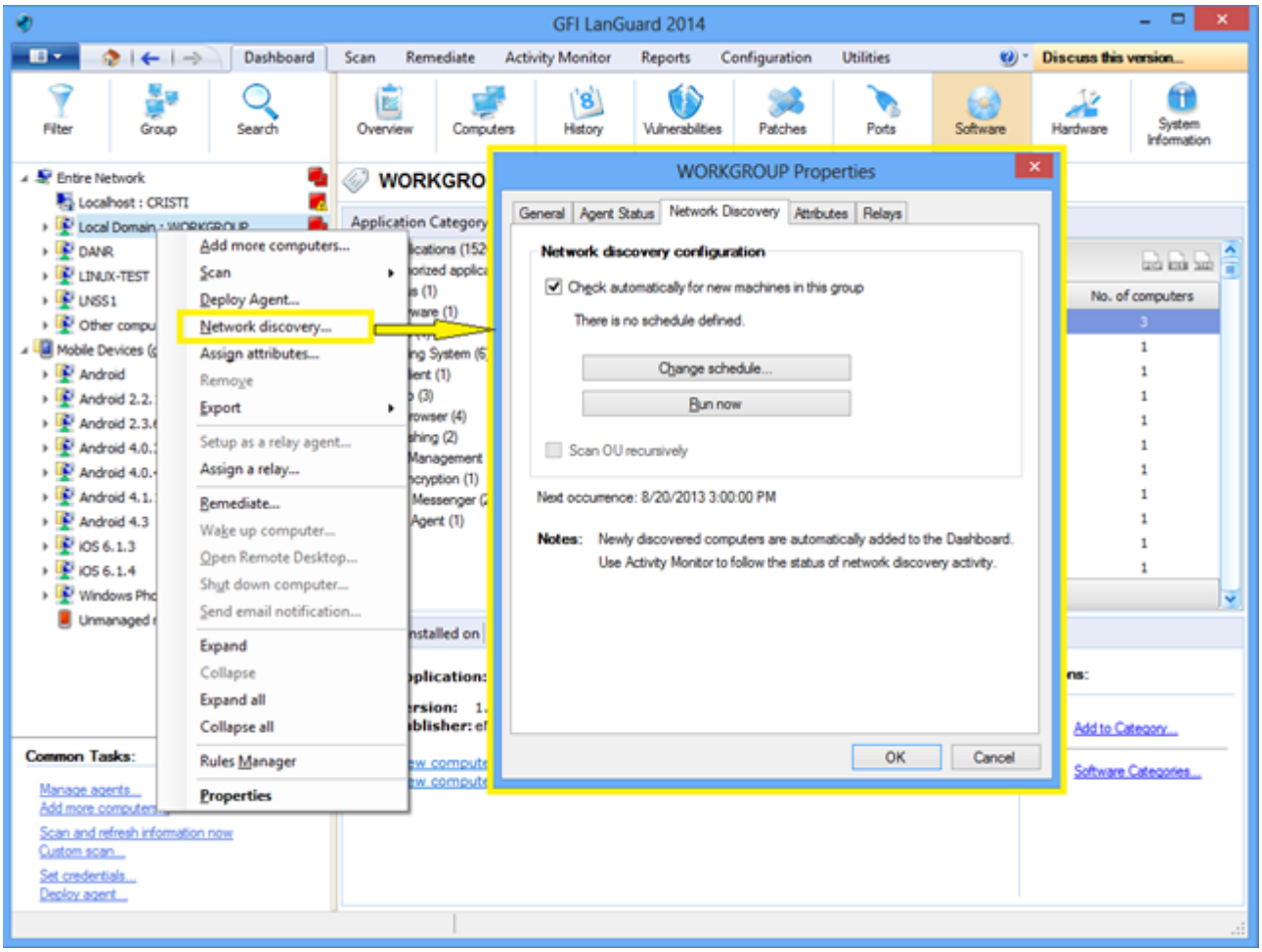
附註：

» GFI LanGuard 中的所有重要工作均可設定為定期自動執行。

» 若要監視網路上的新的活動裝置，應排程對網路探索設定檔執行定期掃描。

若要自動偵測新電腦何時新增到特定的網域或組織單元，請執行以下操作：

1. 在**儀表板**中，以右鍵按一下電腦樹狀結構中的網域或組織單元，並選擇**網路探索**...



螢幕擷取畫面 28: 探索裝置

2. 從**儀表板**選擇**歷程記錄**，以檢視偵測到了網路上的哪些新裝置，以及初次探索的時間。

> **附註：**
> 定義行動裝置管理來源後，將定期自動偵測新行動裝置。如需詳細資訊，請參閱稽核智慧手機和平板電腦一節。

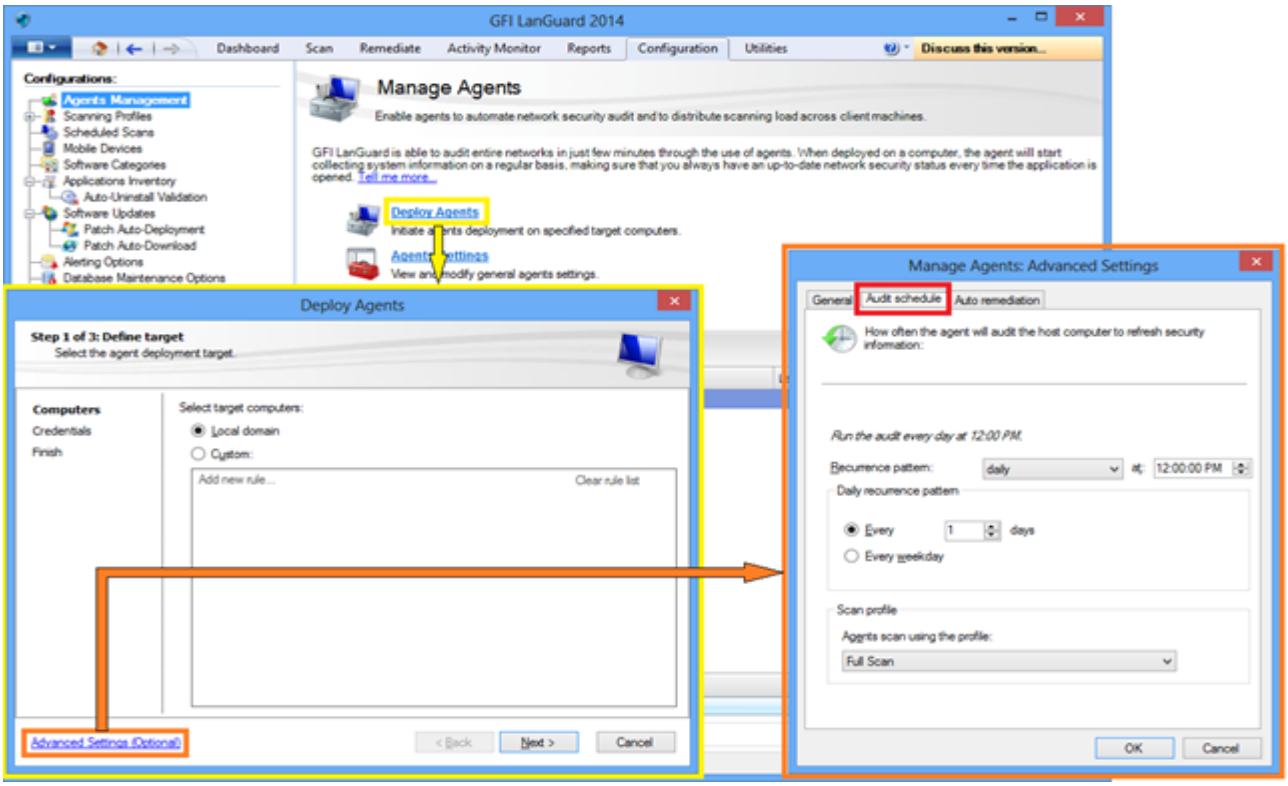
5.2 自動稽核安全性

安全稽核可透過以下兩種方式自動執行：

1. 設定無代理程式的排程掃描，以定期在背景執行

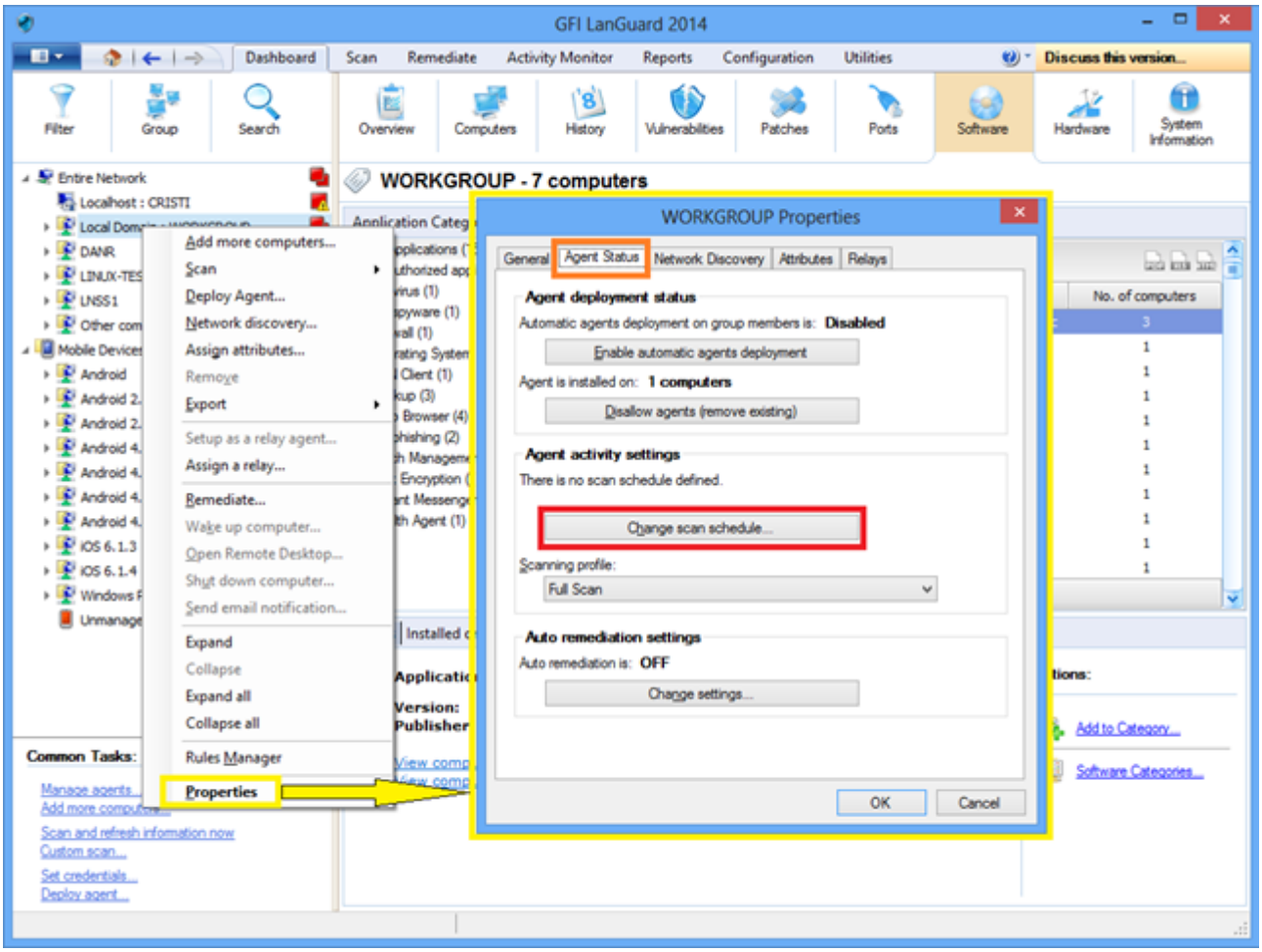
2. 部署目標電腦上的代理程式。預設情況下，代理程式每天稽核主機一次，但可自訂稽核排程。

5.2.1 部署代理程式時自訂稽核排程



螢幕擷取畫面 29: 自訂稽核排程 - 部署代理程式

5.2.2 使用儀表板自訂代理程式的稽核排程



螢幕擷取畫面 30: 自訂稽核排程 - 使用儀表板

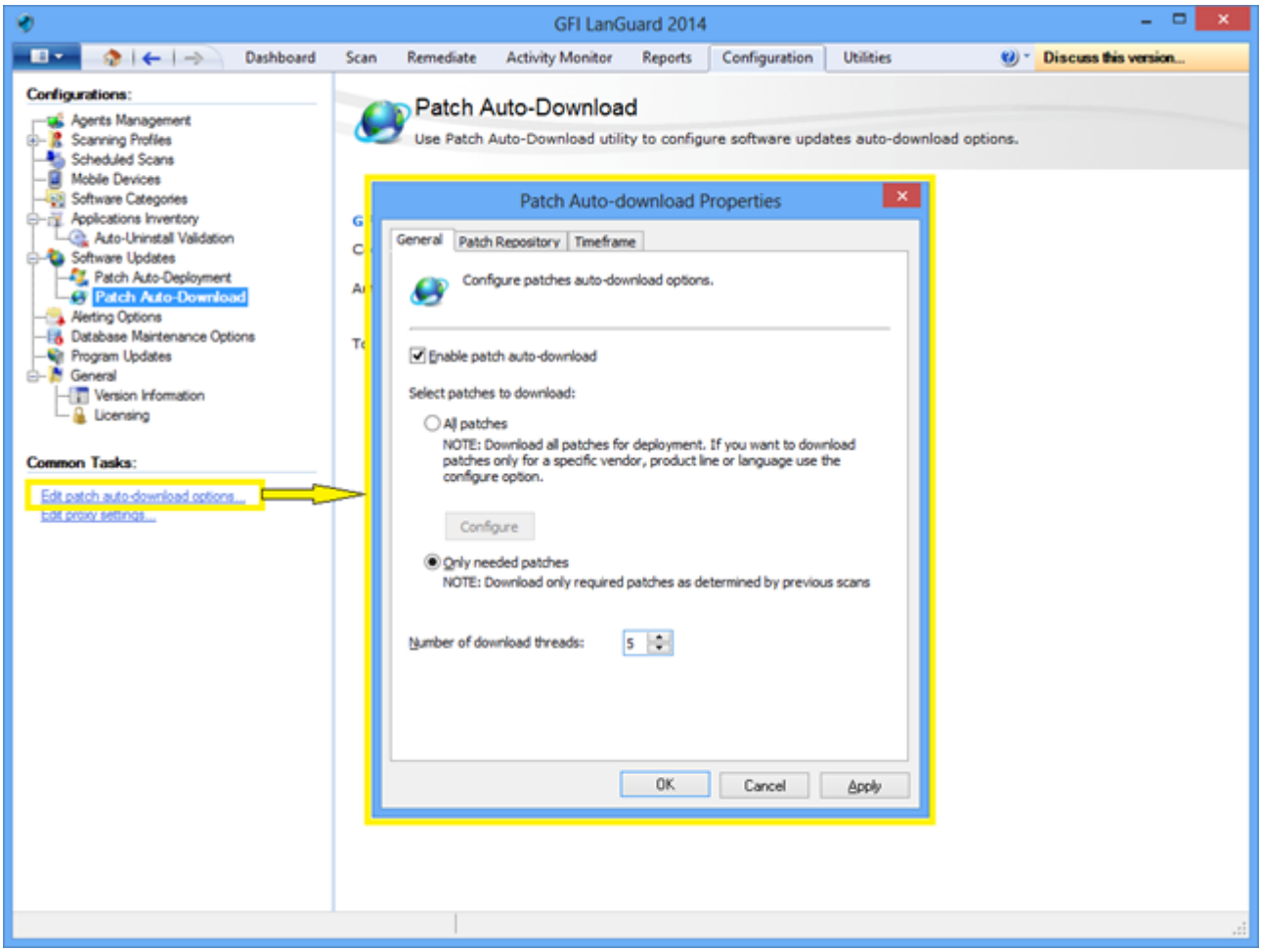
5.3 自動下載修補程式

使用 **設定 > 修補程式自動下載**，將產品設定為自動下載更新，當佈署作業開始時即可使用更新。可用的選項有：

» 自動下載所有修補程式

» 只自動下載 GFI LanGuard 所偵測到缺少的修補程式

» 自動下載特定廠商、產品或語言的修補程式。



螢幕擷取畫面 31: 自動下載修補程式

5.4 自動補救作業

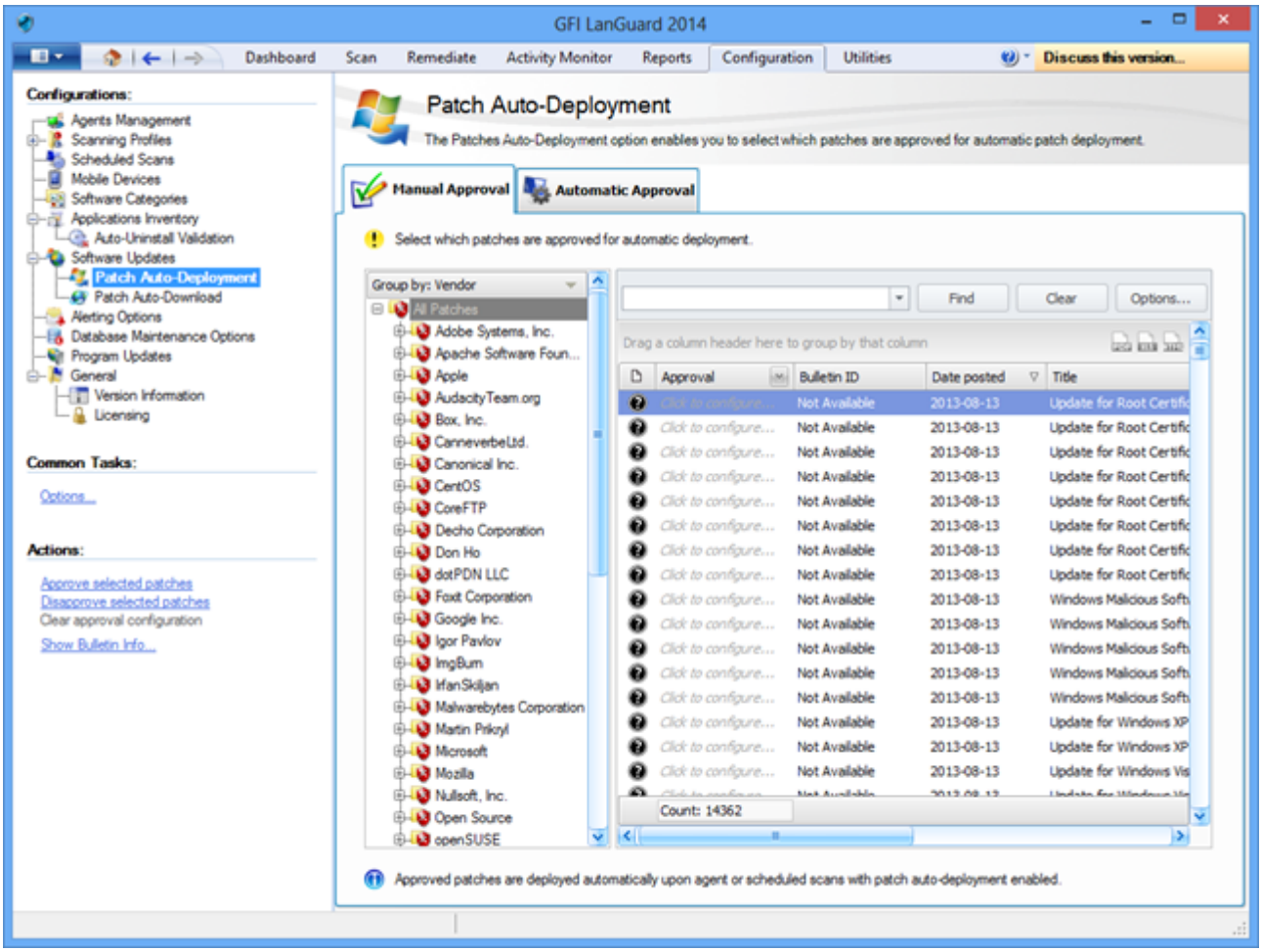
GFI LanGuard 可設定為自動補救特定的安全性問題，例如部署更新和解除安裝未經授權的應用程式(當被無代理程式的排程掃描或以代理程式為主的掃描偵測到時) 。

> **附註：**
> 只有先定義未經授權的應用程式並核准安全性更新以自動部署，才能繼續。

若要核准安全性更新，請執行以下操作：

1. 從**組態**中選擇**自動部署修補程式**。

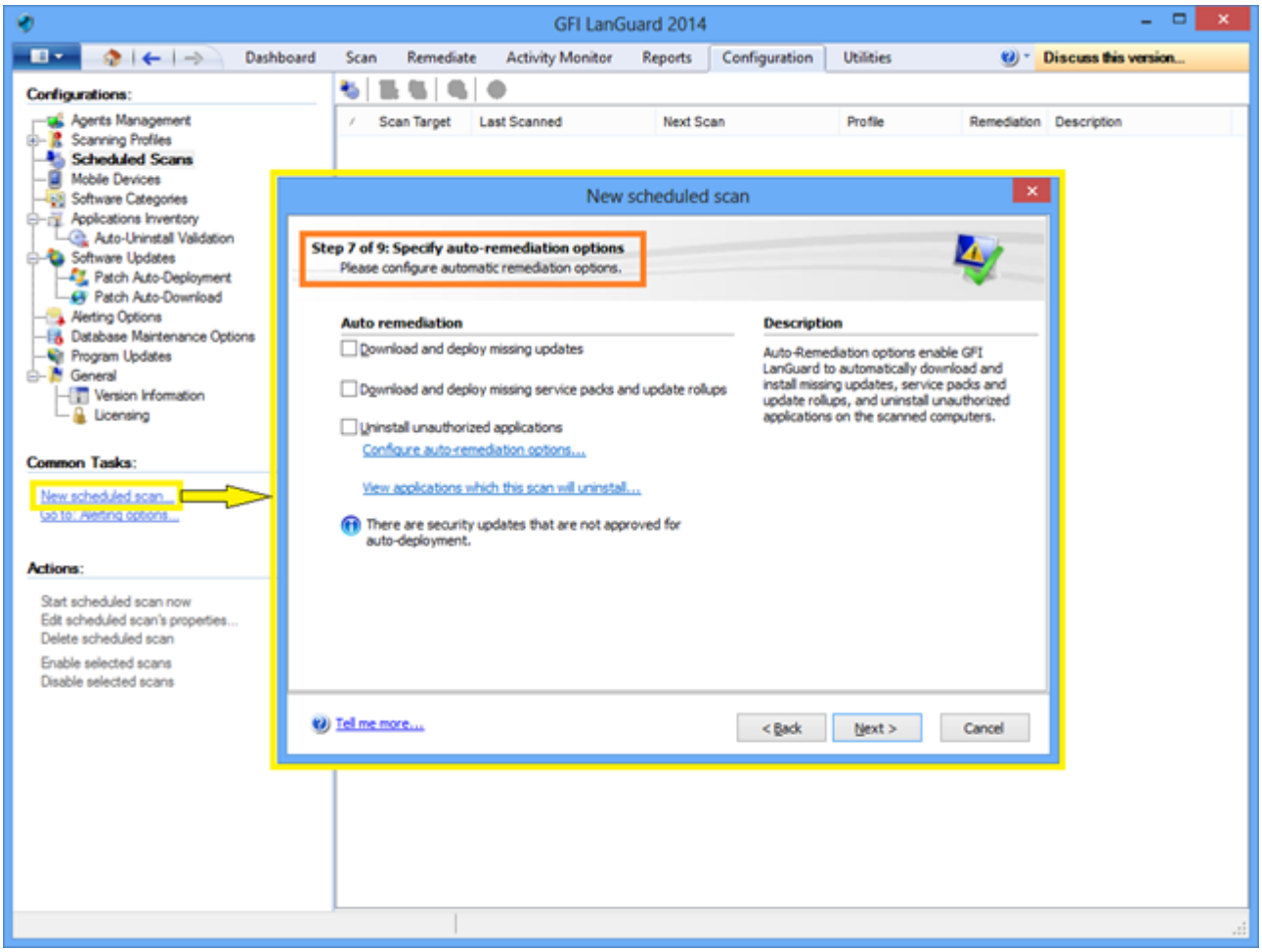
2. 從清單中選擇修補程式。



螢幕擷取畫面 32: 核准安全性更新

對於新的無代理程式排程的掃描，要啟用自動補救，請執行以下操作：

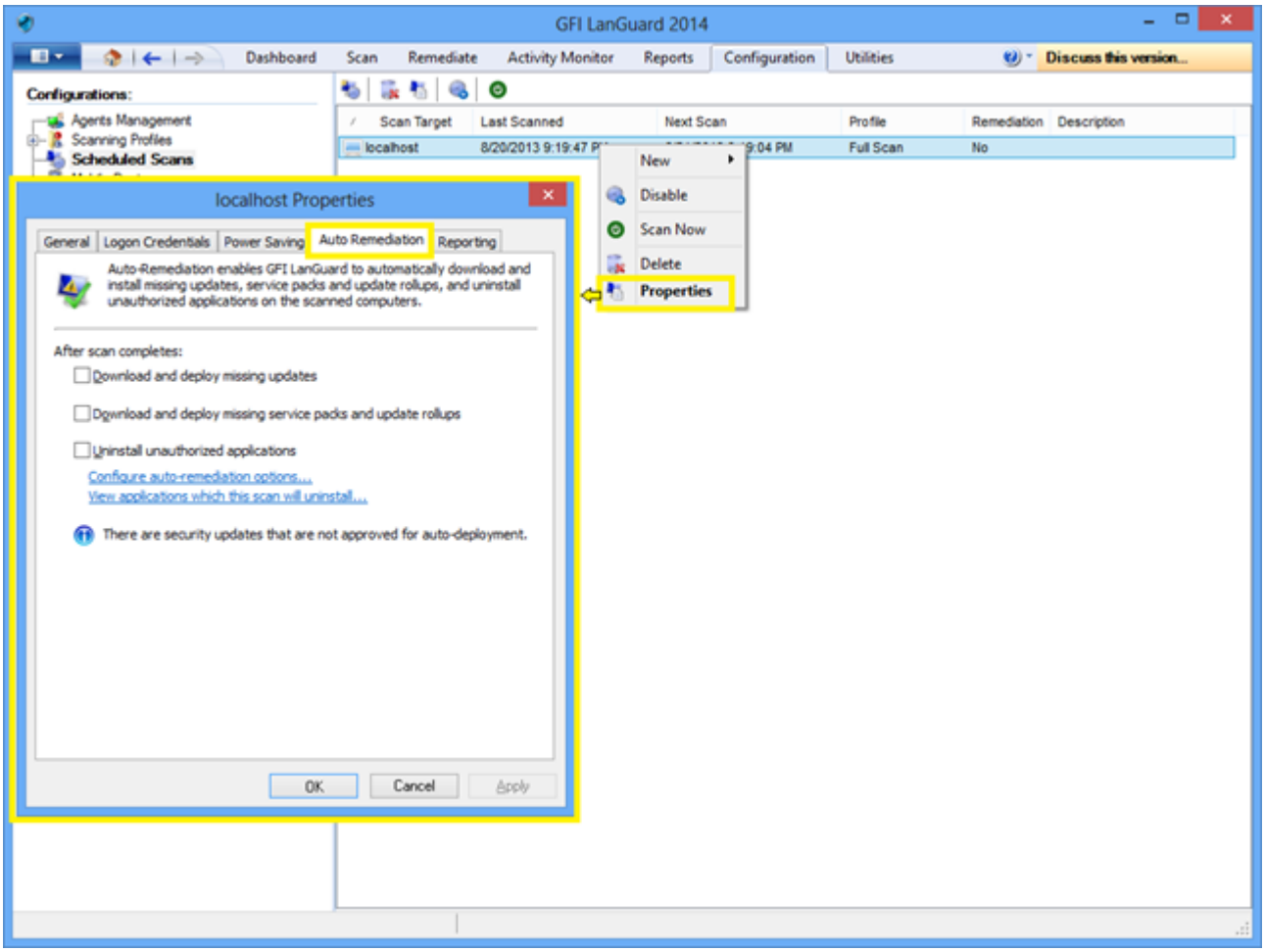
1. 從**組態 > 排程的掃描 > 一般工作**選擇**新增排程的掃描**。
2. 從精靈選擇自動補救組態選項，然後按一下**完成**。



螢幕擷取畫面 33: 對新的無代理程式安全性掃描啟用自動補救

對於現有的無代理程式排程的掃描，若要啟用自動補救，請執行以下操作：

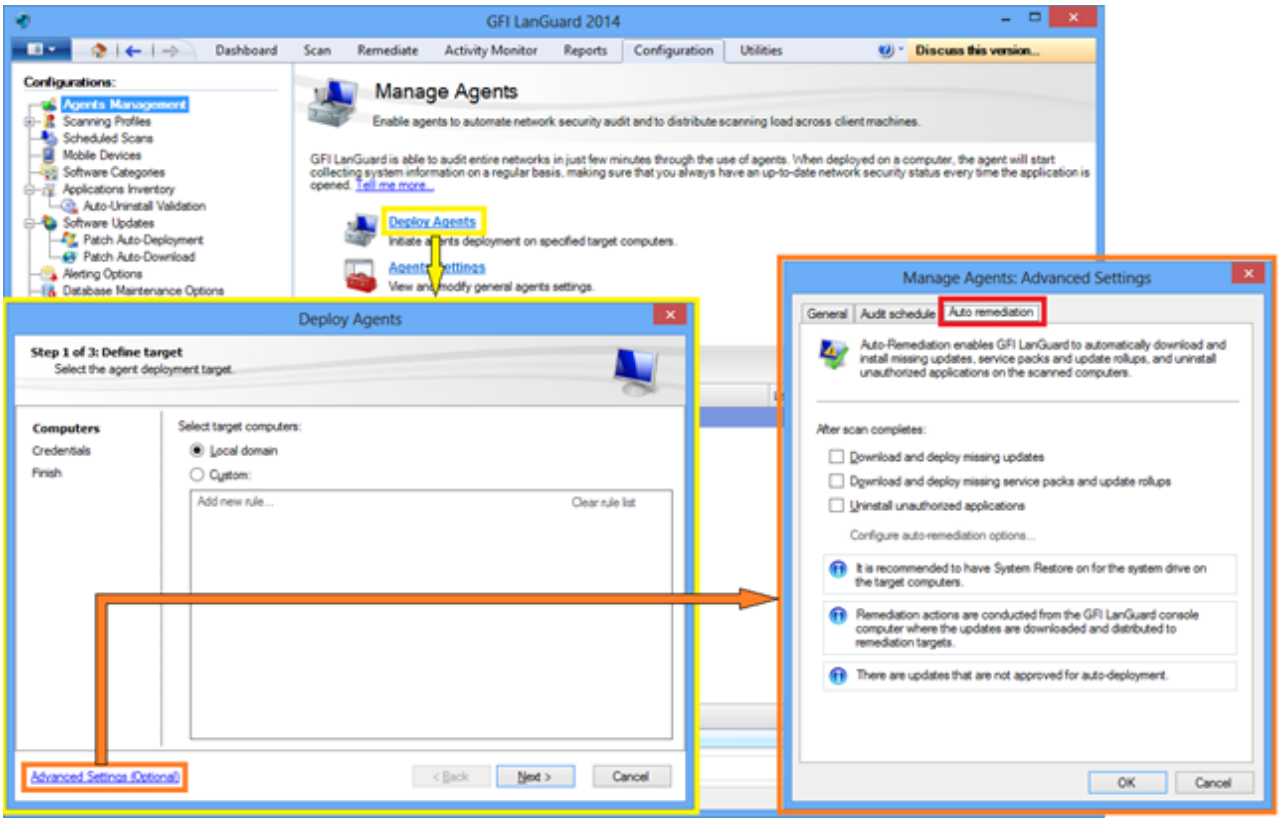
1. 從**組態 > 排程的掃描**」選擇掃描目標。
2. 以右鍵按一下選定的目標，然後按一下**屬性**。這將開啟目標**屬性**對話方塊。
3. 在**自動補救**索引標籤中，從**掃描完成後**區域選擇選項，並按一下**確定**。



螢幕擷取畫面 34: 對現有的無代理程式安全性掃描啟用自動補救

對於部署上的代理程式，要啟用自動補救，請執行以下操作：

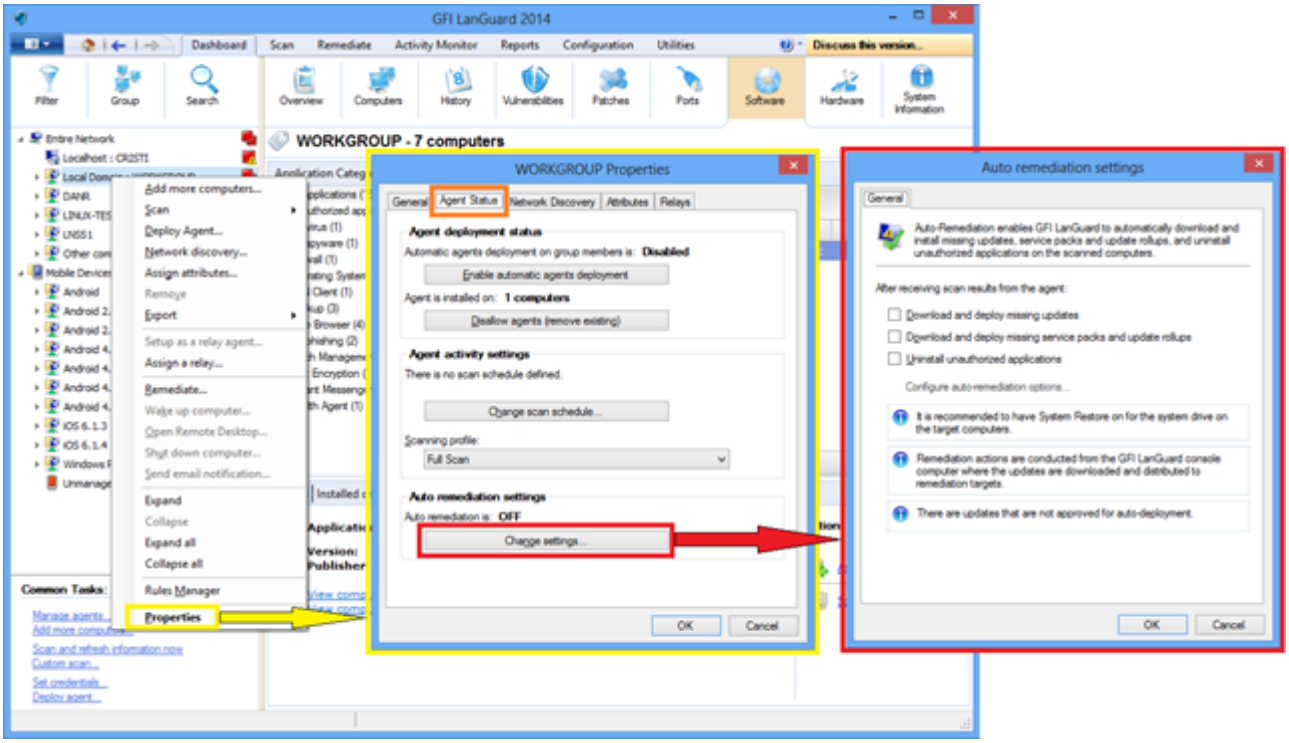
1. 從**組態 > 代理程式管理** 選擇 **部署代理程式**。
2. 從**部署代理程式**精靈中，選擇**進階設定**。
3. 按一下**自動補救**索引標籤，然後從**掃描完成後**區域選擇選項，並按一下**確定**。



螢幕擷取畫面 35: 在部署期間對代理程式啟用自動補救

要啟用代理程式稽核的自動補救，請使用**儀表板**：

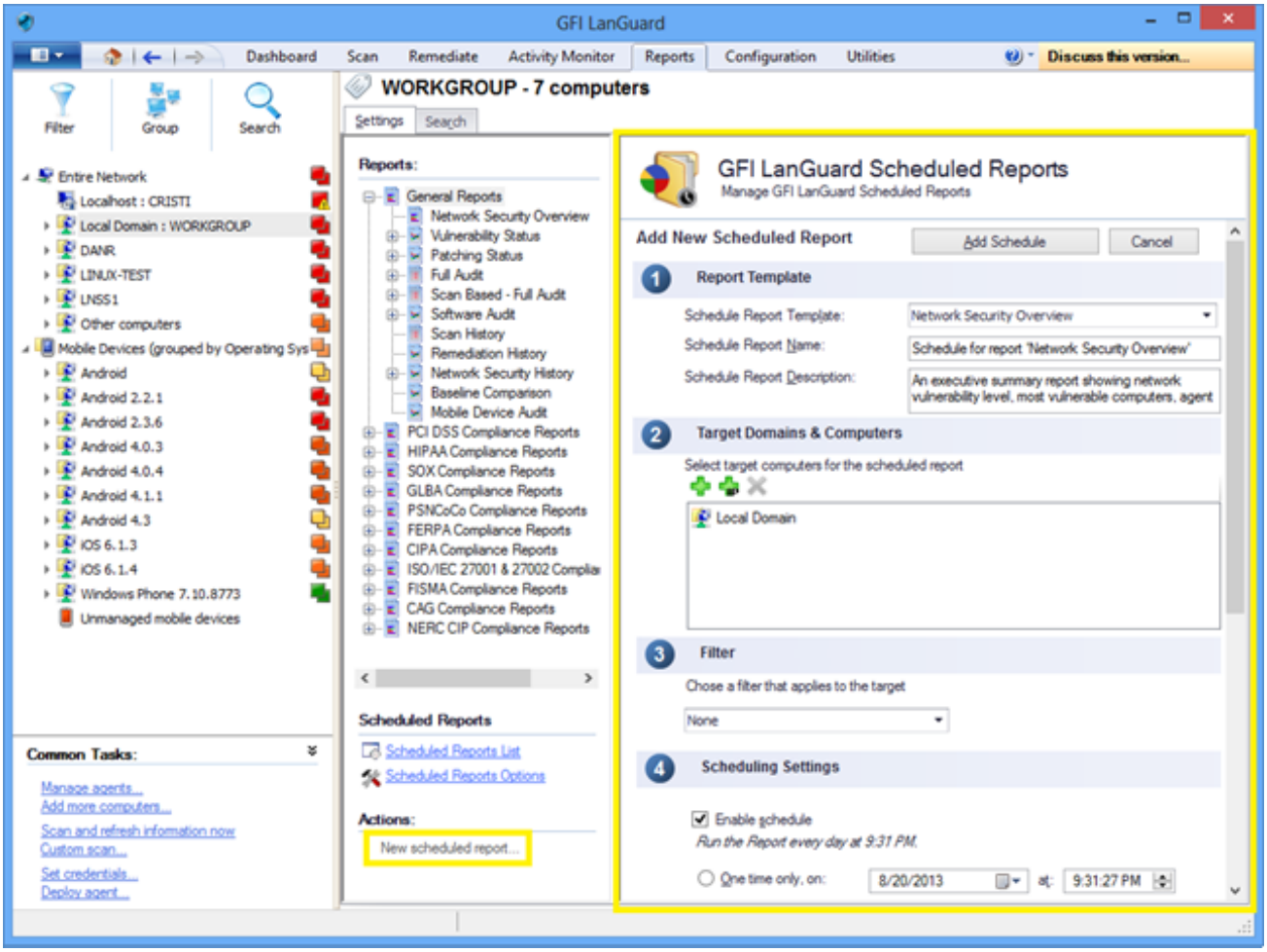
1. 從**儀表板**以右鍵按一下代理程式，然後按一下**屬性**
2. 從**屬性**對話方塊選擇**代理程式狀態**索引標籤
3. 按一下**變更設定**，然後從**接收代理程式的掃描結果後**區域選擇選項，然後按一下**確定**



螢幕擷取畫面 36: 使用儀表板啟用自動補救

5.5 自動產生報告

所有 GFI LanGuard 報告均可設定為定期產生，並自動儲存到指定位置的磁碟中，或傳送給某電子郵件收件者。



螢幕擷取畫面 37: 自動產生報告

6 詞彙表

A

Access™

A Microsoft® 桌面關聯式資料庫管理系統，包含在 Microsoft® Office 套件內。Access™ 通常用於小型資料庫。

Active Directory™ (AD)

提供各種網路服務（包括諸如 LDAP 這樣的目錄服務）的一種技術。

Apache web 伺服器

Apache 軟體基金會開發和維護的開放原始碼 HTTP 伺服器物件。

D

deploycmd.exe

GFI LanGuard 命令列工具，用於部署目標電腦上的 Microsoft® 修補程式和協力廠商軟體。

DMZ

網路的一部分，但不是內部網路的一部分，也不是網際網路的直接部分。其目的通常是用作內部網路和網際網路之間的閘道。

DNS

TCP/IP 網路使用的資料庫，可以將主機名稱轉換為 IP 號並提供其他網域相關的資訊。

DNS 查閱工具

將網域名稱解析為對應的 IP 位址並從目標網域擷取特定資訊的公用程式。

F

FTP

用於在網路電腦之間傳輸檔的通訊協定。

G

GFI EndPointSecurity

GFI 開發的有助於組織透過阻止未授權存取來維護資料完整性，並從卸除式裝置傳輸的安全解決辦法。

GPO

控制哪些使用者可以/不可以在電腦網路上執行操作的 Active Directory 集中管理和配置系統。

I

ICMP pings

網際網路控制訊息通訊協定（ICMP）是網際網路通訊協定套件的其中一個核心通訊協定。網路電腦的作業系統用它傳送錯誤訊息指示，例如，要求的服務不可用或無法聯繫到主機或路由

器。ICMP 還可以用於轉送查詢訊息。

impex.exe
命令列工具，用於從 GFI LanGuard 匯入和匯出設定檔和弱點。

L

Linux
屬於 Unix 作業系統系列一部分的開放原始碼作業系統。

lnsscmd.exe
允許對網路目標執行弱點檢查的 GFI LanGuard 命令列工具。

M

Microsoft® Access™ 資料庫
A Microsoft® 桌面關聯式資料庫管理系統，包含在 Microsoft® Office 套件內。Microsoft® Access™ 通常用於小型資料庫。

Microsoft® IIS
由 Microsoft® Corporation 建立的一套網際網路服務，適用於網際網路伺服器。

Microsoft® Windows Service Pack
Microsoft® 提供的用於增強應用程式或作業系統的更新集和修補程式集。

Microsoft® WSUS
Microsoft® Windows 伺服器更新服務的首字母縮寫。該服務使管理員能夠管理 Microsoft® 更新到網路電腦的分配。

N

NETBIOS
網路基本輸入/輸出的首字母縮寫。該系統提供的服務使網路中不同電腦上的應用程式能夠相互通訊。

Netscape
最初由 Netscape Communications Corporation 開發的 Web 瀏覽器。

O

OVAL
一套標準，可提高開放和公用安全內容可用性，並對此資訊在整個安全工具和服務範圍內進行標準化轉換。

P

Python 指令碼處理
高階電腦程式設計指令碼語言。

S

SANS

系統管理、網路和安全搜尋組織的英文首字母縮寫。共用系統和安全警示解決辦法的一個協會。

SNMP

簡易網路管理通訊協定的英文首字母縮寫，一種用於監視網路裝置（例如路由器、集線器和交換機）的技術。

SNMP Walk 工具

用於探測網路節點並擷取 SNMP 資訊的工具。

SNMP 稽核工具

該工具透過使用預設字典中儲存的值執行字典攻擊，以報告弱式 SNMP 社群字串。

SQL Server 稽核工具

此工具用於測試 -sa- 帳戶（即 root 管理員）以及在 SQL Server® 上設定的任何其他 SQL 使用者帳戶的密碼弱點。

SQL Server®

Microsoft® 關聯式資料庫管理系統。Microsoft® 包含 SQL Server® 的額外功能（事務控制、異常處理和安全），因此 Microsoft SQL Server® 可支援大型組織。

SSH 模組

該模組用於判定對執行的指令碼產生的控制台（文字）資料檢查的弱點結果。這意味著您可以使用目標 Linux/UNIX 作業系統支援的、將結果以文字格式輸出到控制台的任何指令碼方法建立自訂 Linux/UNIX 弱點檢查。

T

TCP 連接埠

傳輸控制通訊協定的英文首字母縮寫。該通訊協定開發的目的在於，使應用程式能夠經由網際網路使用已知的電腦連接埠傳輸和接收資料。

U

UDP 連接埠

用於在裝置之間傳輸 UDP 資料的使用者封包通訊協定的英文首字母縮寫。在該通訊協定中，不確認接收的封包。

URL

統一資源定位符是全球資訊網的網頁位址。

V

VBScript

Visual Basic Scripting 語言是 Microsoft® 開發的高階程式設計語言。

W

Web 伺服器

使用 HTTP通訊協定為用戶端瀏覽器提供 web 頁面的伺服器。

Whois 工具

用於在特定網域或 IP 位址尋找資訊的工具。

Wi-Fi/無線 LAN

廣泛用於區域網路的一種技術。網路節點使用透過無線電波而不是電纜傳輸的資料進行互相通訊。

X

XML

用於定義資料格式的開放文字標準。GFI LanGuard 使用此標準匯入或匯出掃描的已儲存結果和組態。

一

一般弱點和暴露 (CVE)

弱點和其他資訊安全暴露的標準名稱清單。CVE 的目標是將所有公認的弱點和安全暴露的名稱標準化。

修

修補代理程式

處理目標電腦上的修補程式、Service Pack 和軟體更新部署的背景服務。

儀

儀表板

指示目前可能處於使用中狀態的或排程的各種操作狀態的圖形展示。

公

公告資訊

包含修補程式或 Microsoft® 更新的資訊集。在 GFI LanGuard 中用於提供有關安裝的修補程式或更新的詳細資訊。資訊包括：公告 ID、標題、說明、URL 和檔案大小。

列

列舉使用者工具

使您能夠從您的網域/工作群組中擷取使用者和使用者資訊的工具。

列舉電腦工具

識別網路中的網域和工作群組的公用程式。

反

反間諜功能軟體

一種軟體對策，用於偵測未經過使用者許可而安裝到電腦上的間諜軟體。

可

可擴展標記文字(XML)

用於定義資料格式的開放文字標準。GFI LanGuard 使用此標準匯入或匯出掃描的已儲存結果和組態。

後

後門程式

用於透過網路存取電腦或電腦資料的替代方法。

惡

惡意程式碼

由惡意和軟體部分組成，惡意程式碼是一般術語，用於針對危害電腦系統所開發的所有軟體。病毒、蠕蟲和特洛伊特洛伊程式程式是所有類型的惡意程式碼。

應

應用程式自動解除安裝

能夠自動解除安裝應用程式的動作，支援從 GFI LanGuard 自動解除安裝。

批

批次檔

測試檔，包含將由作業系統或應用程式執行的指令集。

指

指令碼偵錯工具

一個 GFI LanGuard 模組，用於使用 VBScript 相容語言寫入並偵錯自訂指令碼。

掃

掃描設定檔

決定識別了哪些弱點以及將從掃描的目標擷取哪些資訊的弱點檢查集合。

本

本機主機

在網路中，本機主機是目前正在使用的電腦。您可以透過使用保留的 IP 位址(127.0.0.1) 參考本機主機。在本手冊中，本機主機是安裝 GFI LanGuard 的電腦。

檔

檔案傳輸通訊協定

用於在網路電腦之間傳輸檔的通訊協定。

特

特洛伊特洛伊程式程式

一種惡意程式碼，包含將會損壞電腦的隱藏應用程式。

病

病毒

會感染電腦的一種惡意程式碼。病毒的目的是透過損壞檔和應用程式損壞電腦。病毒是一個自我複製的程式，可自行複製到整個電腦系統。

白

白名單

不認為具有危險性的 USB 或網路裝置名稱的清單。如果在掃描網路時 USB/網路裝置名稱包含白名單項目，GFI LanGuard 將忽略該裝置並將其看做是安全來源。

簡

簡易網路管理通訊協定(SNMP)

簡易網路管理通訊協定是用於監測網路裝置(如路由器、集線器和交換機) 的一種技術。

終

終端服務

該服務允許連線到目標電腦並管理其安裝的應用程式和儲存的資料。

統

統一資源定位器(URL)

統一資源定位符是全球資訊網的網頁位址。

網

網域名稱系統

TCP/IP 網路使用的資料庫，可以將主機名稱轉換為 IP 號並提供其他網域相關的資訊。

網際網路控制訊息通訊協定(ICMP)

網際網路控制訊息通訊協定(ICMP) 是網際網路通訊協定套件的其中一個核心通訊協定。網路電腦的作業系統用它傳送錯誤訊息指示，例如，要求的服務不可用或無法聯繫到主機或路由器。ICMP 還可以用於轉送查詢訊息。

網際網路資訊服務(IIS)

由 Microsoft® Corporation 建立的一套網際網路服務，適用於網際網路伺服器。

群

群組原則物件(GPO)
控制哪些使用者可以/不可以在電腦網路上執行操作的 Active Directory 集中管理和配置系統。

自

自動下載
在所有的 38 種語言中自動下載缺失的修補程式和 Service Pack 的 GFI LanGuard 技術。

自動修補程式管理
自動下載缺少的 Microsoft ® 更新並透過網路進行部署的 GFI LanGuard 技術。

自動補救
自動下載和部署缺少的修補程式的 GFI LanGuard 技術。如果應用程式列在 GFI LanGuard 的黑名單中，自動補救將在排程操作期間從目標電腦中解除安裝該應用程式。

藍

藍牙
支援裝置之間資料交換的開放無線通訊和介面通訊協定。

路

路徑追蹤工具
該工具用於識別 GFI LanGuard 搜尋目標電腦的路徑。

通

通用序列匯流排(USB)
廣泛用於連接裝置和主機電腦的串列匯流排標準。

通用閘道介面(CGI)
Web 伺服器使用的用於向用戶端網際網路瀏覽器傳輸資料的通訊指令碼。

遠

遠端桌面通訊協定
Microsoft® 開發的使用戶端能夠與遠端電腦介面相連接的通訊協定。

郵

郵件伺服器
管理和儲存用戶端電子郵件的伺服器。

開

開放式弱點和評估語言 (OVAL)

一套標準，可提高開放和公用安全內容可用性，並對此資訊在整個安全工具和服務範圍內進行標準化轉換。

間

間諜軟體

一種旨在收集電腦資訊而不通知使用者的惡意形式。

防

防毒

一種軟體對策，用於監測未經過使用者許可而安裝到電腦上的惡意程式碼。

非

非軍事化區(DMZ)

網路的一部分，但不是內部網路的一部分，也不是網際網路的直接部分。其目的通常是用作內部網路和網際網路之間的閘道。

黑

黑名單

被認為有危險的 USB 或網路裝置名稱的清單。在掃描網路時，如果 USB\網路裝置名稱包含黑名單項目，則 GFI LanGuard 會將裝置報告為安全威脅(高安全性弱點) 。

7 索引

L

lnsscmd.exe 12

O

OVAL 5

P

PCI DSS 5, 7, 27

Proxy 5

W

Web 瀏覽器 6

反

反間諜軟體 5, 7

全

全文檢索搜尋 26

共

共用 7

合

合規 4

安

安全性掃描 16

伺

伺服器 7-8

每

每日摘要 21

系

系統資訊 7, 19

修

修補程式管理 4

弱

弱點狀態 6

弱點評估 4

掃

掃描設定檔 16

排

排程掃描 10

軟

軟體 19

軟體稽核 7

連

連接埠 7, 13, 19

部

部署自訂軟體 35

部署軟體更新 30

硬

硬體 19

補

補救中心 29, 34-35, 37

補救作業 31

補救歷程記錄 6

解

解除安裝應用程式 35

網

網路和軟體稽核 4

網路裝置 9

儀

儀表板 5, 7, 14, 19, 21-22, 25-26, 39, 47

警

警示選項 21

屬

屬性 45