

2025台灣二版

企業操作課程-ESET PROTECT 進階篇

議程大綱

ESET PROTECT 進階篇

- ESET PROTECT On-Prem/ ESET PROTECT
Cloud版本更新資訊
- ESET PROTECT On-Prem/ ESET PROTECT
Cloud管理
- Q&A



ESET PROTECT On-Prem管理

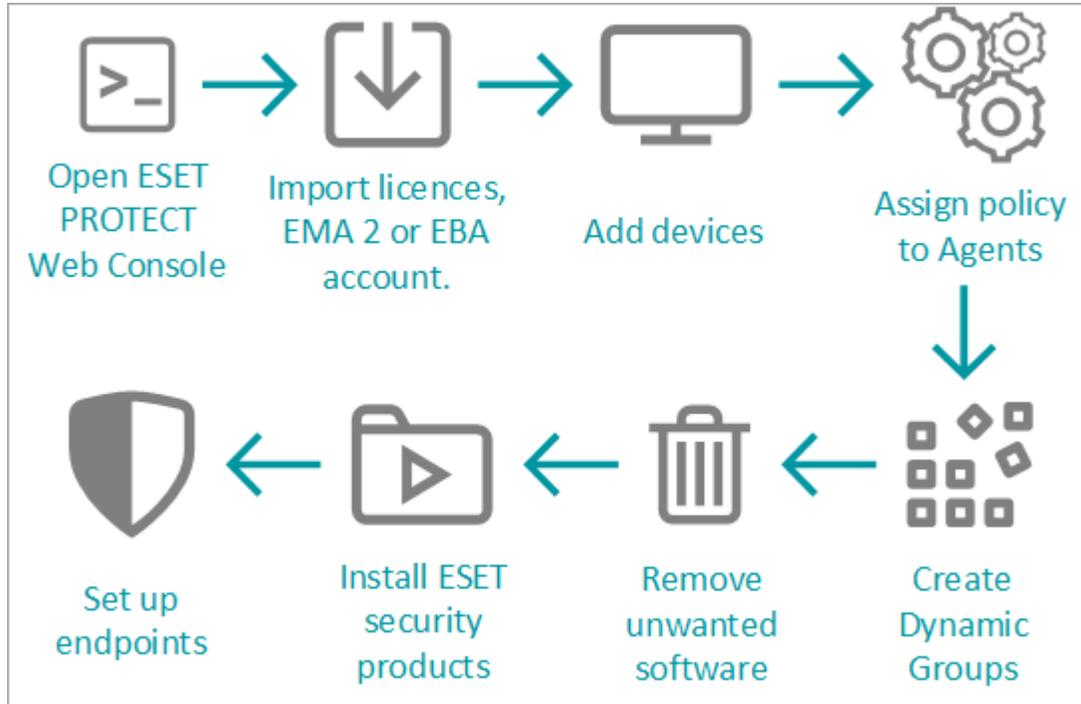


ESET PROTECT On-Prem 開始前注意事項

ESET Protect On-Prem/ ESET Protect Cloud管理介面 瀏覽器支援

Web 瀏覽器
Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera

開始前注意事項



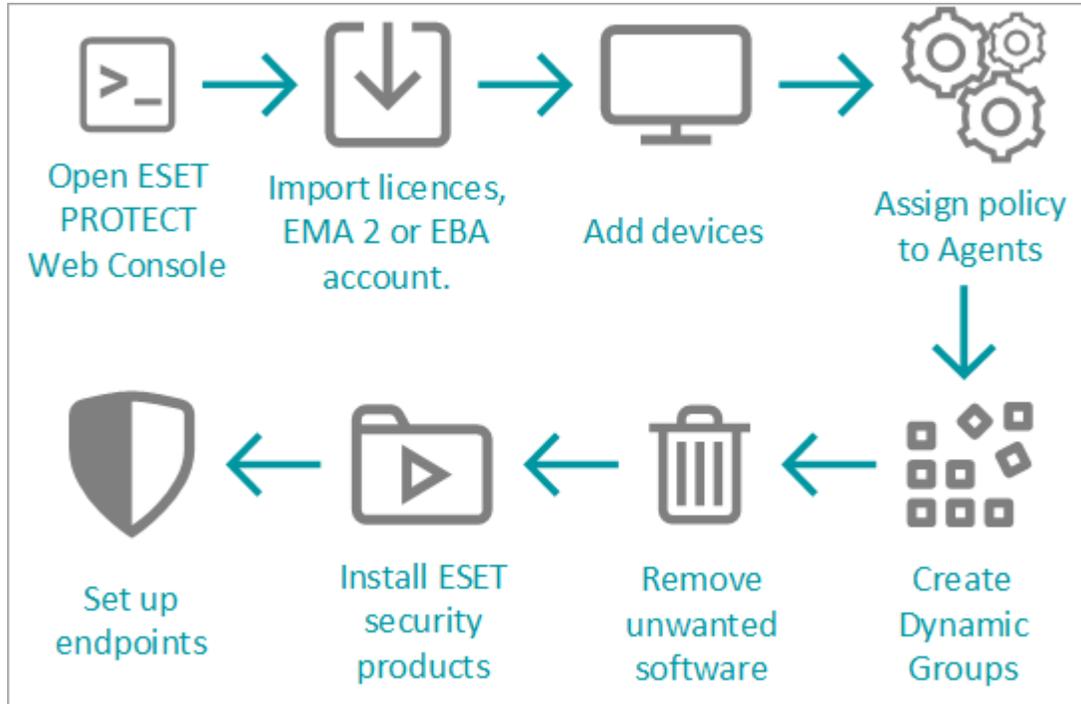
1. 在您的網頁瀏覽器中開啟 [ESET PROTECT Web Console](#) 並登入。

2. 將您的授權新增至 [ESET PROTECT On-Prem](#)。

3. [新增電腦](#) - 將網路上的用戶端電腦及伺服器新增到 ESET PROTECT On-Prem 結構。

4. [指派內建原則 \[應用程式報告 - 報告所有安裝的應用程式\]](#) 給所有電腦。

開始前注意事項(續)



5.為包含 ESET 產品的電腦建立動態群組。

6.使用 [軟體解除安裝] 工作移除第三方防毒應用程式。

7.使用 [軟體安裝] 工作安裝 ESET 安全性產品 (除非您已經使用全方位安裝程式安裝代理程式)。

8.將包含建議設定的原則指派給包含已安裝 ESET 安全性產品的每個機器。例如，對於包含 ESET Endpoint 的 Windows 機器，指派內建的原則 [防毒 - 最大安全性 - 建議]。另請參閱管理 ESET PROTECT On-Prem 的端點產品。



ESET PROTECT On-Prem版本更新資訊

更新與修復

Added

- Linux的網路隔離
- 改進許可證管理的企業帳戶連結
- ESET PROTECT 本地伺服器性能優化
- 任務中的審計功能
- 動態組範本的審核功能
- Microsoft Exchange Server 上的維護模式檢測
- 支援在Ubuntu 24.04 LTS、22.04 LTS、RHEL 9和Debian12上安裝ESET PROTECT本地伺服器
- 支援 MySQL ODBC 驅動程式版本 9.2 和 9.3
- 生命週期終止和服務更新警報中的更新選項

Improved

- 支援使用叢集 MS SQL 資料庫進行 ESET PROTECT 本地安裝
- MySQL 資料庫字元集更新為 utf8mb4
- 用於 Reports 和 Dashboards 的圖形可視化技術

Removed

- SysInspector 紀錄查看器
- 支援在 Microsoft Windows Server 2012 R2 上安裝 ESET PROTECT 本地伺服器
- 支援 Microsoft SQL Server 2014
- 支援 MySQL 5.7

更新與修復(續)

Fixed

Version 12.1.9.0

- 為託管客戶創建和編輯現有報告時出現問題
- 缺少永久組排序設置
- 使用 “is one of” 或 “is not one of” 對多個規則進行動態組評估時出現問題
- 無法正常工作的映射域用戶主組選擇器
- 側面板消失，沒有檢索選項
- 篩選器 “Network access protection is non-functional” (網絡訪問保護無法正常工作) 中缺少值

Fixed

Version 12.1.11.0

- 由於早期版本發現漏洞 **CVE-2025-48988**、**CVE-2025-48976**、**CVE-2025-52520** 和 **CVE-2025-52434**，Apache Tomcat 升級至 9.0.107
- 當未連接到資料庫時，從 12.0 版本升級到 12.1 版本時產品升級崩潰
- MSP 授權同步需要很長時間並降低產品速度
- 叢集環境中的報告產生導致請求逾時失敗
- 在簡化許可證管理下，配置 ESET LiveGrid 信譽和回饋系統的選項不起作用
- 其他各種小改進和修復



ESET PROTECT On-Prem 作業系統支援

Windows用戶端作業系統支援

作業系統	代理程式	RD Sensor
Windows 10 x86	10.1—12.1	✓
Windows 10 x64 (所有正式版本)	10.1—12.1、12.2—12.4	✓
ARM 上的Windows 10	10.1—12.1、12.2—12.4	
Windows 11 x64	10.1—12.1, 12.2—12.4 (21H2, 22H2) 10.1—12.1, 12.2—12.4 (23H2) 11.3—12.1, 12.2—12.4 (24H2)	✓
ARM 上的Windows 11	10.1—12.1、12.2—12.4	

Windows伺服器作業系統支援

作業系統	代理程式	RD Sensor
Windows Server 2012 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2012 核心 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2012 R2 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2012 R2 核心 x64	10.1—12.1、12.2—12.4	✓
Windows 儲存伺服器 2012 R2 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2016 x64	10.1—12.1、12.2—12.4	✓
Windows 儲存伺服器 2016 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2019 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2022 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2022 CORE x64	11.0—12.1、12.2—12.4	
Windows Server 2025 x64	12.0—12.1、12.2—12.4	

Linux作業系統支援

作業系統	代理程式	RD Sensor
Ubuntu 18.04.1 LTS x64 桌面	10.1—12.1、12.2—12.4	✓
Ubuntu 18.04.1 LTS x64 伺服器	10.1—12.1、12.2—12.4	✓
Ubuntu 20.04 LTS x64	10.1—12.1、12.2—12.4	✓
Ubuntu 22.04 LTS x64	10.1—12.1、12.2—12.4	✓
Ubuntu 24.04 LTS x64	11.0—12.1、12.2—12.4	
Linux Mint 20	10.1—12.1、12.2—12.4	✓
Linux Mint 21	10.1—12.1、12.2—12.4	✓
Linux Mint 22	11.3—12.1、12.2—12.4	✓
RHEL 伺服器 7 x64	10.1—12.1、12.2—12.4	✓
RHEL 伺服器 8 x64	10.1—12.1、12.2—12.4	
RHEL 伺服器 9 x64	10.1—12.1、12.2—12.4	✓
CentOS 7 x64	10.1—12.1、12.2—12.4	✓

Linux作業系統支援(續)

作業系統	代理程式	RD Sensor
SLED 15 x64	10.1—12.1、12.2—12.4	✓
SLES 12 x64	10.1—12.1、12.2—12.4	✓
SLES 15 x64	10.1—12.1、12.2—12.4	✓
Debian 9 x64	10.1—12.1、12.2—12.4	✓
Debian 10 x64	10.1—12.1、12.2—12.4	✓
Debian 11 x64	10.1—12.1、12.2—12.4	✓
Debian 12 x64	10.1—12.1、12.2—12.4	✓
Oracle Linux 8	10.1—12.1、12.2—12.4	✓
亞馬遜Linux 2	10.1—12.1、12.2—12.4	✓
亞馬遜Linux 2023	11.3—12.1、12.2—12.4	✓
Alma Linux 9	10.1—12.1、12.2—12.4	✓
Rocky Linux 8	10.1—12.1、12.2—12.4	
Rocky Linux 9	10.1—12.1、12.2—12.4	

Mac用戶端作業系統支援

作業系統	代理程式
macOS Catalina (10.15)	10.1—12.1、12.2—12.4
macOS Big Sur (11.0)	10.1—12.1、12.2—12.4
macOS Monterey (12.0)	10.1—12.1、12.2—12.4
macOS Ventura (13.0)	10.1—12.1、12.2—12.4
macOS Sonoma (14.0)	10.1—12.1、12.2—12.4
macOS Sequoia (15.0)	11.3—12.1、12.2—12.4



ESET PROTECT On-Prem EOL資訊

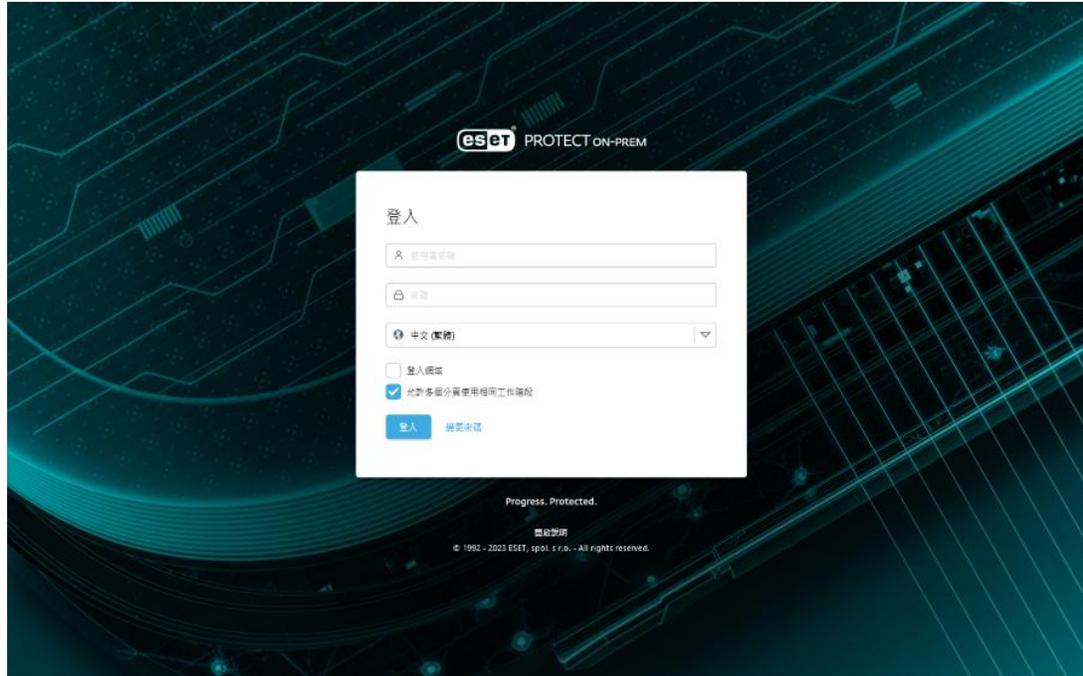
ESET防毒伺服器EOL資訊

版本	原始發布日期	最新版本	最新版本發布日期	目前狀態	全力支持	有限支持
12.0	2025年2月18日	12.0.12004.0	2025年4月22日	✓ 全力支持	直到下次功能更新 (最晚 2026 年 2 月 28 日)	截止至2028年2月29日
11.1	2024年10月15日	11.1.12013.0	2025年5月29日	✓ 全力支持	截至 2025 年 10 月 31 日	截至 2027 年 10 月 31 日
11.0	2024年2月29日	11.0.12012.0	2025年1月29日	! 有限支持	已結束 (2025 年 2 月 28 日)	截止至2027年2月28日
10.0	2023年3月14日	10.0.12017.0	2025年1月29日	! 有限支持	已結束 (2025 年 2 月 28 日)	截止至2027年2月28日
9.0	2022年5月4日	9.0.12019.0	2025年1月29日	! 有限支持	已結束 (2024 年 3 月 31 日)	截至 2026 年 3 月 31 日
8.0	2021年6月16日	8.0.12016.1	2024年1月25日	生命終點	已結束 (2023 年 5 月 4 日)	已結束 (2025 年 5 月 31 日)



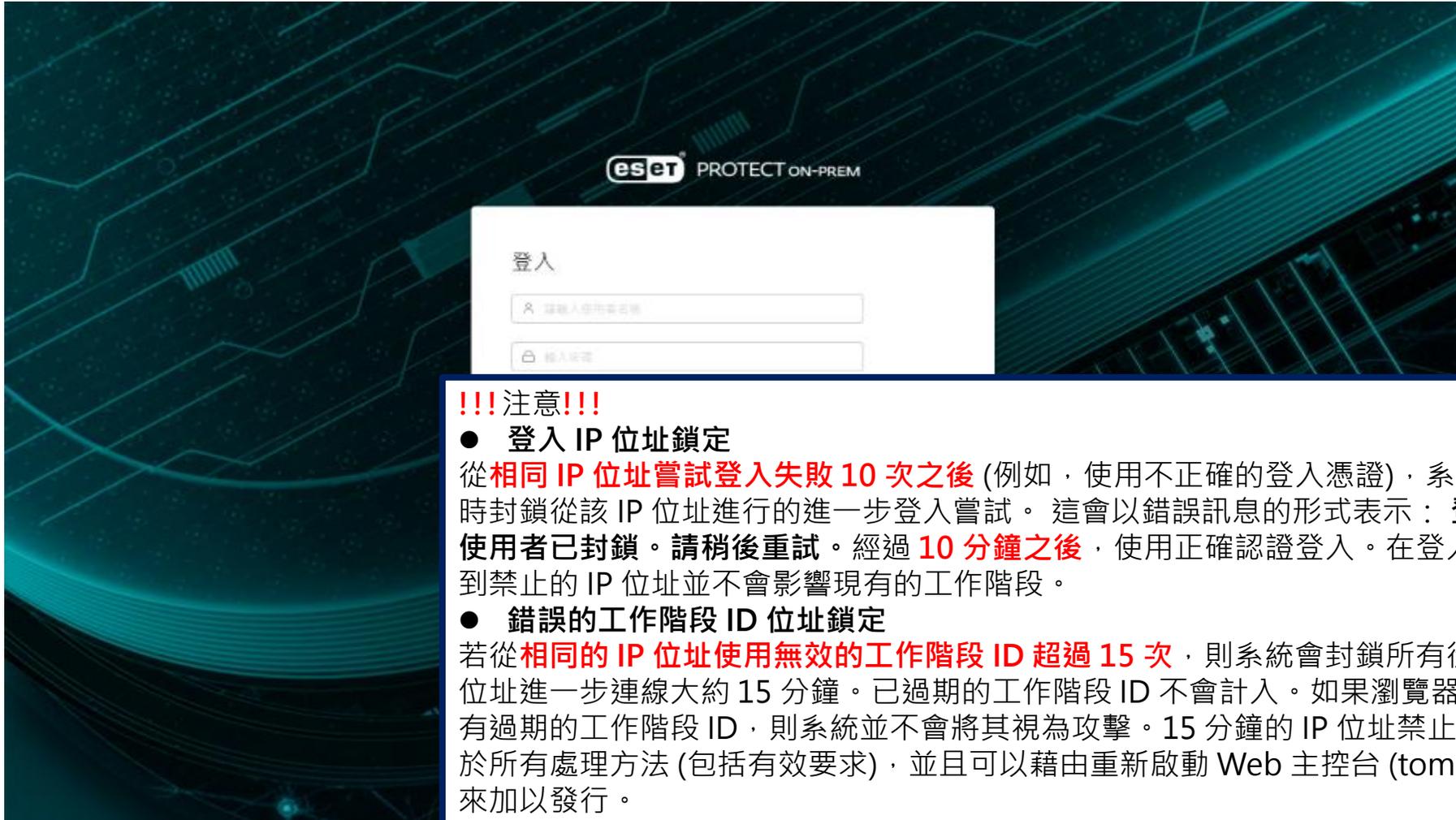
ESET PROTECT On-Prem WebConsole

WebConsole注意事項



- 在 [本機伺服器] (裝載 Web Console 的電腦) 的網頁瀏覽器中輸入此 URL：<https://localhost/era/>
- 在任何能經由網際網路存取 Web 伺服器之處，輸入下列格式的 URL：<https://yourservername/era/> 用您 Web 伺服器的真正名稱或 IP 位址取代 "yourservername"。
- 若要登入至 ESET PROTECT On-Prem 虛擬設備]，請使用下列 URL：[https://\[IP address\]/](https://[IP address]/) 用您 ESET PROTECT On-Prem VM 的 IP 位址取代「[IP 位址]」。
- 在您的本機伺服器 (裝載 Web Console 的電腦) 上，按一下 [開始] > [所有程式] > [ESET] > [ESET PROTECT On-Prem] > [ESET PROTECT] - 將會以預設的網頁瀏覽器開啟登入畫面。這**不適用於 ESET PROTECT 虛擬設備**。

WebConsole 登入畫面



WebConsole 導覽精靈

ESET PROTECT on-prem 瀏覽

儀表板

[儀表板] 區域提供您公司網路的概觀，並顯示所有已連線裝置的狀態。

預先定義的儀表板會顯示與您網路相關的不同報告，例如裝置狀態、安全性、偵測等等。您可以使用快捷動作立即更新安裝在受管理裝置上的 ESET 安全性產品，或探索所回報問題的詳細資訊。

您也可以建立最符合您需求的自訂儀表板。

[深入瞭解 ESET 說明中有關儀表板的資訊](#)

Dashboard

Status Overview Security Overview ESET LiveGuard Computers Server Performance Status

316
Total number of devices ⓘ

300
Ok

4
Attention required

8
Security risks

Connection status

5

- 1 day 5
- > 7 days 311
- Never 2

第 1 頁 (共 8 頁)

上一步 下一步

ESET LiveGrid® 聲譽及意見系統原則



ESET LiveGrid® 聲譽及意見系統

i 我們已新增一組新原則，以提高使用 ESET LiveGrid® 的威脅偵測功能，我們強大的意見系統可以分析來自全球數百萬使用者的即時資料，以更有效地識別和回應最新和正在出現的威脅。

這組原則將會自動套用您網路中目前透過 ESET PROTECT On-Prem (靜態群組「全部」) 管理的所有裝置，以及任何新新增的裝置。

啟用原則 拒絕原則 稍後提醒我

當滿足以下條件時，將出現 [ESET LiveGrid® 聲譽及意見系統] 視窗：

- 你有 ESET PROTECT On-Prem **11.1 及更新版本**。
- 您首先登入 Web 主控台，並且您是管理員。
- 您擁有作用中的 ESET PROTECT 防護階層，但沒有 ESET LiveGuard Advanced 授權。

WebConsole 主控台功能說明

The screenshot displays the ESET WebConsole interface. At the top, there is a navigation bar with the ESET logo, 'PROTECT ON-PREM', a search bar, and user information for 'ADMINISTRATOR'. Below the navigation bar is a menu with various options: 儀表板 (Dashboard), 電腦 (Computers), 偵測 (Detection), 報告 (Reports), 工作 (Jobs), 安裝程式 (Installers), 原則 (Policies), 通知 (Notifications), 狀態概觀 (Status Overview), and 其他 (Other). A red arrow points to the '儀表板' option.

The dashboard is divided into several sections:

- Summary Cards:**
 - 裝置的總數 (Total Devices): 5, 確定 (Confirmed): 3
 - 需要注意 (Needs Attention): 0, 安全風險 (Security Risk): 2
- Desktop (桌面):** Donut chart showing 3 items: 2 Safety Risks (red), 0 Needs Attention (yellow), 1 Confirmed (green).
- Server (伺服器):** Donut chart showing 2 items: 0 Safety Risks (red), 0 Needs Attention (yellow), 2 Confirmed (green).
- Connection Status (連線狀態):** Donut chart showing 5 items: 2 for 1 day (dark teal), 2 for 3 days (medium teal), 1 for > 7 days (light teal).
- Component Version Status (元件版本狀態):** Stacked bar chart showing the percentage of components that are latest (green), pending (blue), overdue (yellow), or old (red). Categories include 代理程式 (Proxy), Endpoint, 伺服器 (Server), 加密 (Encryption), EDR, and 其他 (Other).
- Management Status (管理狀態):** Horizontal bar chart showing 5 managed and protected devices (blue), 0 unmanaged devices (red), and 109 total devices (yellow).
- RSS Summary (RSS 摘要):** News item titled 'ESET Support News' dated 2025年6月3日, stating 'ESET PROTECT On-Prem version 12.1.9.0 has been released'.



ESET PROTECT On-Prem WebConsole疑難 排解

疑難排解

錯誤訊息	可能原因
登入失敗：無效的使用者名稱或密碼	確定您已正確輸入使用者名稱和密碼。您可以 重設 ESET PROTECT Web 主控台密碼 。 ! 密碼必須至少包含 14 個字元，且包含下列其中三個類別：小寫字母、大寫字母、數字或特殊字元。我們建議使用不少於 17 個字元的密碼。
登入失敗：連線失敗，狀態為 [未連線]	查看 ESET PROTECT 伺服器服務及您的資料庫服務是否正在執行中，請參閱 知識庫文章 中的逐步指示。
登入失敗：使用者已封鎖。請稍後重試	從相同 IP 位址嘗試登入失敗 10 次之後 (例如，使用不正確的登入憑證)，系統將會暫時封鎖從該 IP 位址進行的進一步登入嘗試。經過 10 分鐘之後，使用正確認證登入。
登入失敗：通訊錯誤	確認 ESET PROTECT 伺服器服務執行中 Apache Tomcat 執行中且正常運作 。檢閱 Apache Tomcat 的 記錄檔 。如需此問題的詳細資訊，請參閱我們的 知識庫文章 。
登入失敗：連線逾時	檢查網路連線和防火牆設定，以確定 ESET PROTECT Web Console 可以連接 ESET PROTECT 伺服器。此外 ESET PROTECT 伺服器可能超載，請嘗試重新開機。使用不同的 ESET PROTECT Web Console 與 ESET PROTECT 伺服器版本可能導致此問題。
登入失敗：使用者沒有指派存取權	未對使用者指派任何存取權限。以管理員身分登入，並編輯使用者的帳戶，以便將至少一個 權限集 指派給使用者。
登入失敗：回應剖析錯誤	您的 Web 主控台與 ESET PROTECT 伺服器的版本不相容。這可能在發生元件升級之後發生。如果問題持續發生，請手動部署正確版本的 Web Console。
正在使用未加密的連線！請配置 webserver 以使用 HTTPS	基於安全性理由，建議您設定 ESET PROTECT Web Console 使用 HTTPS 。
JavaScript 已停用。請在瀏覽器中啟用 JavaScript	啟用 JavaScript 或更新 Web 瀏覽器 。
SEC_ERROR_INADEQUATE_KEY_USAGE (僅 Mozilla Firefox)	Mozilla Firefox 有 損壞的憑證存放區 。

疑難排解(續)

錯誤	可能原因
看不到登入畫面，或登入畫面似乎不斷載入中	<ul style="list-style-type: none">●重新啟動 ESET PROTECT On-Prem Server 服務 <p>在 ESET PROTECT On-Prem Server 服務重新啟動並執行後，請重新啟動 Apache Tomcat 服務。在此之後，將成功載入 ESET PROTECT Web Console 登入畫面。另請參閱我們的知識庫文章。</p> <ul style="list-style-type: none">●如果 Apache Tomcat 無法從 era.war 檔提取內容，並且 Web 主控台無法訪問，請按照我們的知識庫文章中的步驟進行操作
此文字在 ESET PROTECT Web Console 的內容功能表和 [快速連結] 功能表中會遺失。	這個問題可能是由廣告封鎖的瀏覽器延伸所造成。若要解決這個問題，請對 ESET PROTECT Web 主控台頁面停用廣告封鎖的瀏覽器延伸。
登入之後，Web Console 並未正確顯示 (缺少元素等)	確定您使用的是 支援的網頁瀏覽器
登入後，某些 Web 主控台畫面未載入	<p>如果某些 ESET PROTECT Web 主控台畫面 (例如電腦) 未載入，請開啟 Tomcat9w.exe 檔案 (位於 C:\Program Files\Apache Software Foundation [Tomcat 資料夾中])</p> <ul style="list-style-type: none">●在 [一般] 標籤中，按一下 [停止] 以停止 Apache Tomcat 服務。●選取 [Java] 標籤，然後在 Java Options 下的內容中添加以下代碼： -Duser.country=US -Duser.language=en●在一般標籤中，按一下 [開始] 以啟動 Apache Tomcat 服務。
Web 主控台載入需要很長時間(當載入大量物件時，主控台將崩潰)	Web 主控台在處理大型物件集時需要額外的記憶體。請參閱 Web 主控台中的 企業設定 。
Web 主控台某些畫面不能正確載入，且您會看到錯誤訊息。例如，在編輯原則時，您會看到錯誤：「ERROR WHILE INITIALIZING CONFIGURATION EDITOR.: (TYPEERROR): ((INTERMEDIATE VALUE)(INTERMEDIATE VALUE), K).INITCONFIGEDITOR IS NOT A FUNCTION」	<p>如果您正在使用的反向 Proxy 會禁止載入某些 Web 主控台模組，則會發生此問題。個別 Web 主控台模組 (在 Apache Tomcat 中載入) 的 URL 字串可能會動態變更 (例如，era/webconsole/configEngine/02645EFC6ABCDE2B449042FB8S63FD3/v0.0/css/001_ce.ltr.css) 中在 era/webconsole/configEngine/ 後的字串。若要解決此問題，請確保正確配置您的反向 Proxy。</p>
匯入較大 (超過 20 MB) 的檔案 (例如原則) 時，該處理程序將失敗	Web 主控台的檔案大小限制為 20 MB。您可以透過編輯位於 [Tomcat folder]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\ 資料夾中的 EraWebServerConfig.properties 檔案來加以變更。將 file_size_limit=20 變更為更高的值，最大值為 250。



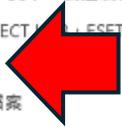
ESET PROTECT On-Prem 新增授權

新增授權金鑰

新增授權

您可以使用以下其中一個選項新增授權：

- ESET PROTECT / ESET Business Account 或 ESET MSP Administrator
- 授權金鑰
- 雲端授權金鑰



授權金鑰

[我有一組使用者名稱和密碼，我可以做什麼？](#)

新增授權

取消

- × 在 **[授權金鑰]** 欄位中，輸入或複製貼上您在購買 ESET 安全性解決方案時，所收到的 **[授權金鑰]**，然後按一下 **[新增授權]**。

！您可以為以下防護層新增授權金鑰：

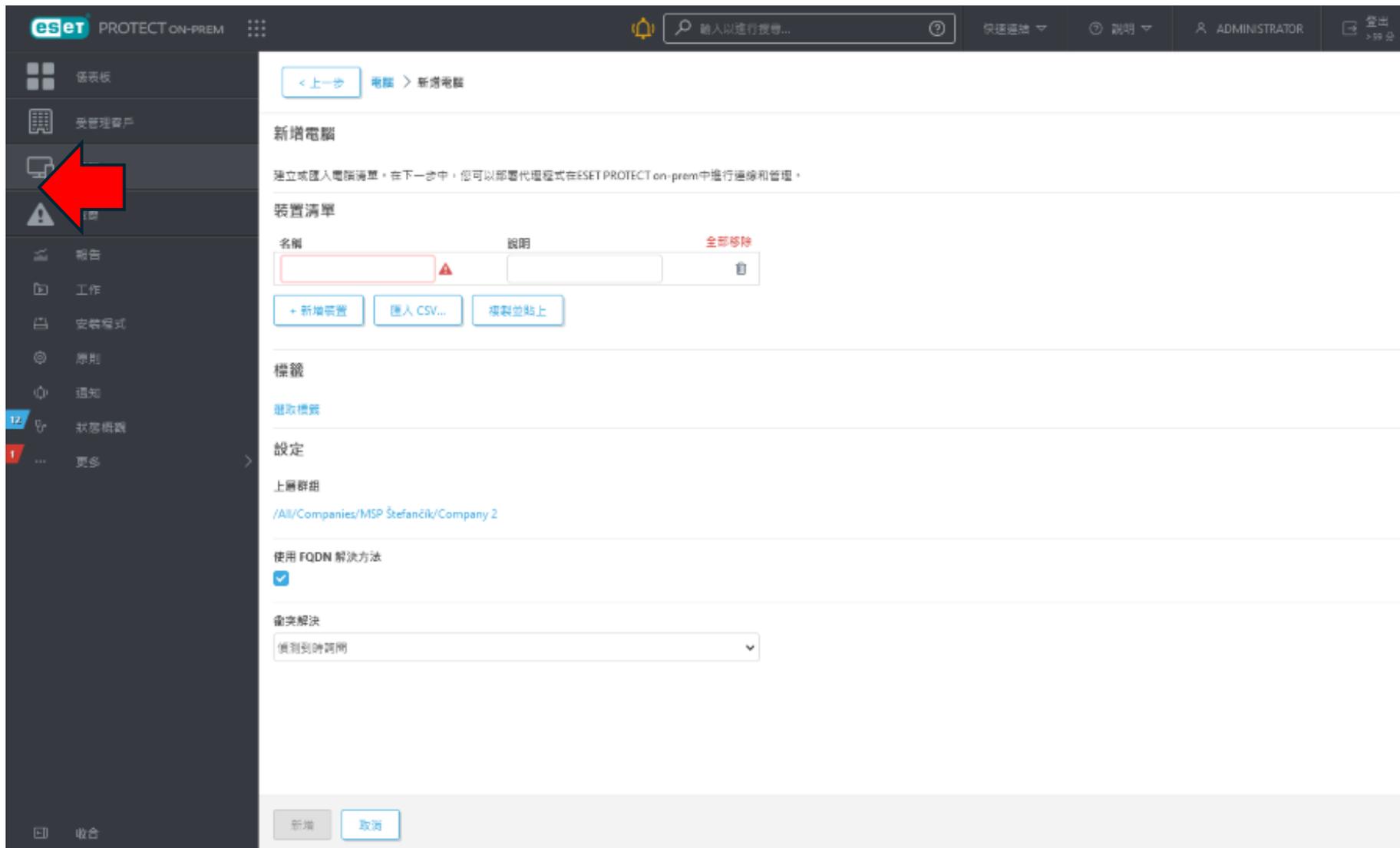
- ESET PROTECT Entry On-Prem
- ESET PROTECT Essentials On-Prem

若您新增更高防護層級的授權金鑰，將導致系統發生錯誤。您可以[同步](#) ESET PROTECT On-Prem 和 ESET PROTECT Hub、ESET Business Account 或 ESET MSP Administrator 以新增更高的防護層級。



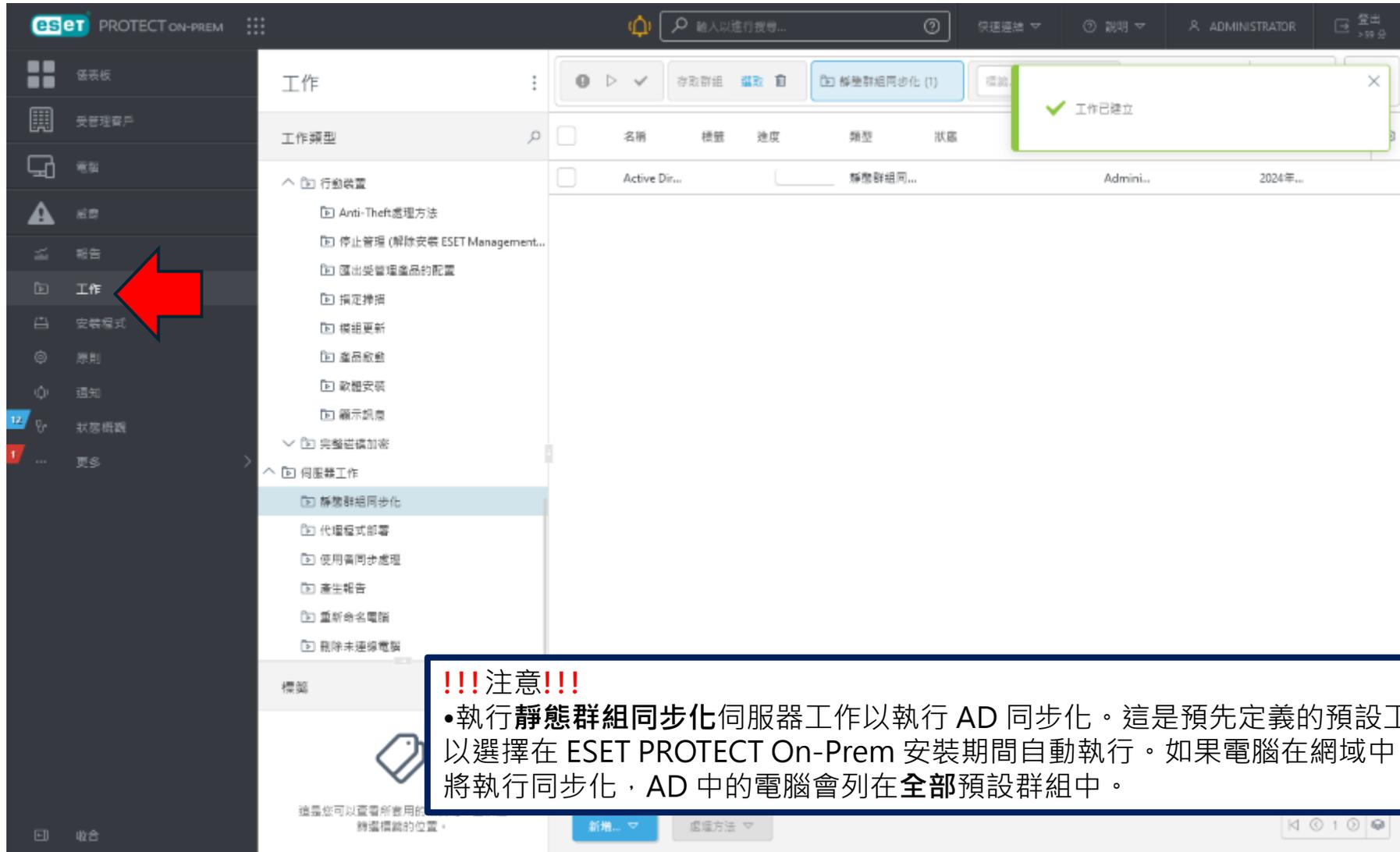
ESET PROTECT On-Prem 新增電腦

1.使用手動新增



The screenshot displays the ESET PROTECT ON-PREM web interface. The top navigation bar includes the ESET logo, a search bar, and user information (ADMINISTRATOR). The left sidebar contains various management options, with a red arrow pointing to the 'Add Computer' (新增電腦) icon. The main content area is titled '新增電腦' (Add Computer) and includes a breadcrumb trail: '< 上一步' (Previous Step) > 電腦 > 新增電腦 (Computers > Add Computer). Below the title, there is a descriptive paragraph and a '裝置清單' (Device List) section with a table for adding devices. The table has columns for '名稱' (Name) and '說明' (Description), and a '全部移除' (Remove All) button. Below the table are buttons for '+ 新增裝置' (Add Device), '匯入 CSV...' (Import CSV...), and '複製並貼上' (Copy and Paste). Further down, there are sections for '標籤' (Tags) with a '選取標籤' (Select Tags) button, '設定' (Settings) for '上層群組' (Parent Group) (set to '/All/Companies/MSP Štefančík/Company 2'), '使用 FQDN 解決方法' (Use FQDN Resolution Method) (checked), and '衝突解決' (Conflict Resolution) (set to '偵測到時關閉'). At the bottom, there are '新增' (Add) and '取消' (Cancel) buttons.

2.使用 Active Directory 同步



工作

工作類型

名稱	標籤	速度	類型	狀態
Active Dir...			靜態群組同...	Admini...

工作已建立

!!! 注意!!!

- 執行靜態群組同步化伺服器工作以執行 AD 同步化。這是預先定義的預設工作，您可以選擇在 ESET PROTECT On-Prem 安裝期間自動執行。如果電腦在網域中，則系統將執行同步化，AD 中的電腦會列在全部預設群組中。

3.使用RD Sensor

The screenshot displays the ESET PROTECT ON-PREM dashboard. The top navigation bar includes the ESET logo, 'PROTECT ON-PREM', a search bar, and user information for 'ADMINISTRATOR'. The main content area is titled '儀表板' (Dashboard) and features several widgets:

- 電腦狀態概要** (Computer Status Overview): A donut chart showing 5 total computers, with segments for '安全性風險' (Security Risk), '故障' (Failure), and '確定' (Confirmed).
- 首要電腦問題** (Primary Computer Issues): A donut chart showing 2 issues, both labeled '產品...' (Product...).
- 電腦上次連線時間** (Computer Last Connection Time): A donut chart showing 5 computers, with segments for '14天' (14 days), '1天' (1 day), and '> 3天' (> 3 days).
- 上次更新** (Last Update): A donut chart showing 5 computers, with segments for '1天' (1 day) and '> 3天' (> 3 days).
- 作業系統** (Operating System): A donut chart showing 5 computers, with segments for 'Ubuntu' and 'Microsoft Wi...'.
- 惡意電腦比例** (Malicious Computer Ratio): A donut chart showing 11 malicious computers, with a segment for '惡意' (Malicious).
- 有問題的電腦** (Problematic Computers): A table with columns for '電腦名稱' (Computer Name), '發生時間' (Occurrence Time), '嚴重性' (Severity), '來源' (Source), '功能' (Function), '狀態' (Status), and '問題' (Issue).

A red arrow points from the '電腦' (Computer) tab in the top navigation to the '惡意電腦比例' widget. A blue box highlights the table header for '有問題的電腦'.

!!!注意!!!

•RD Sensor **主動監聽 ARP 廣播**。當 RD Sensor 偵測到新的作用中網路元件時，RD Sensor 會傳送 ARP 單點傳播、執行主機指紋 (使用數個連接埠) 並將檢測的電腦相關資訊傳送到 ESET PROTECT 伺服器。然後 ESET PROTECT 伺服器會評估網路上所找到的 PC 是否屬於 ESET PROTECT 伺服器不知道的 PC，還是屬於已經受管理的 PC。

3.使用RD Sensor(續)

eset PROTECT ON-PREM

ADMINISTRATOR

報告: Rogue computers

伺服器名稱

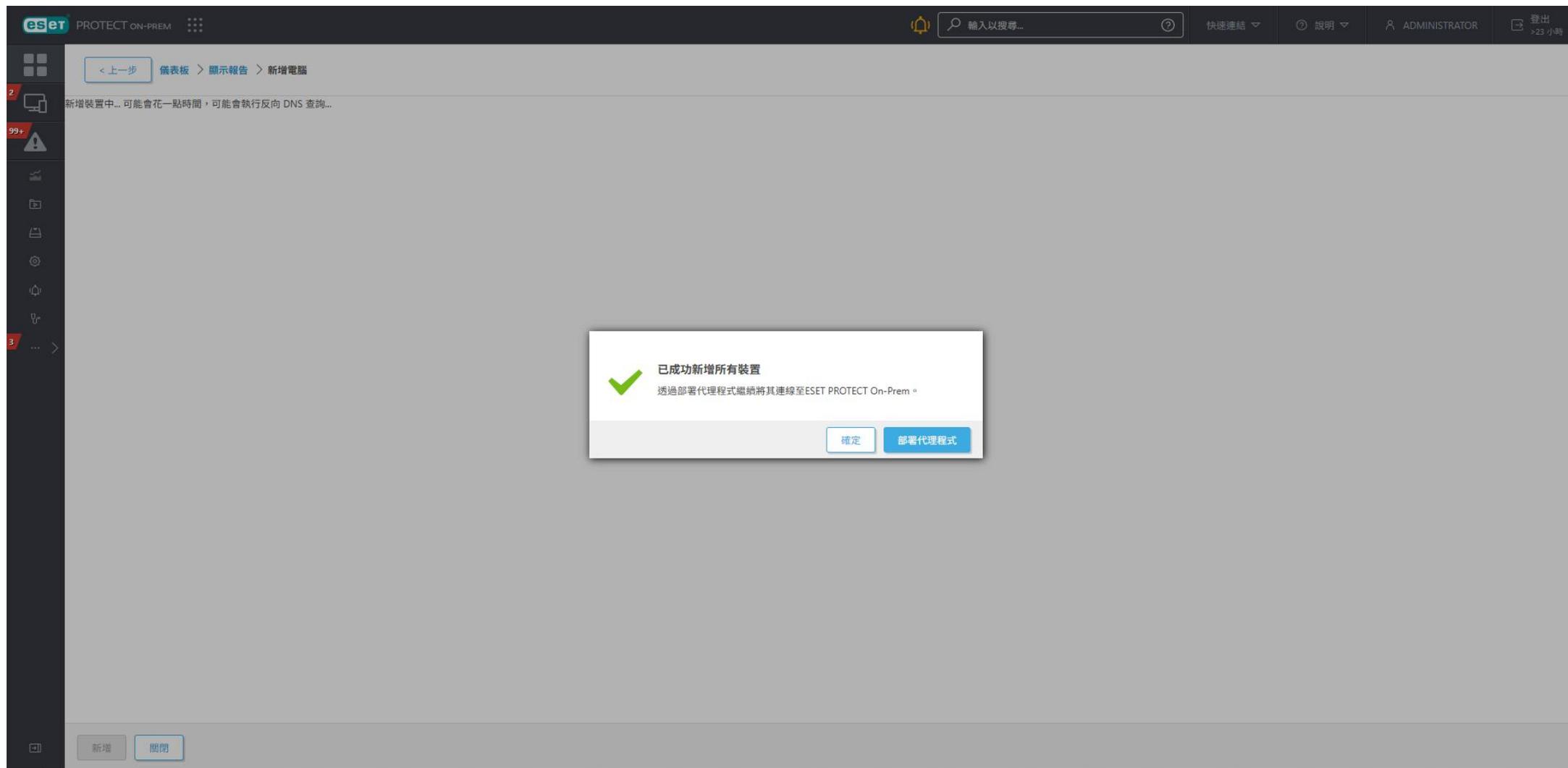
產生於: 2024年4月5日 12:47:21 (UTC+02:00)

記錄數: 340

MAC 位址	IPv4 位址	IPv6 位址	替代主機名稱	主機名稱	網路介面卡廠商	偵測到的 OS
未知的數據						

每頁顯示的項目: 500 1 / 1

3.使用RD Sensor(續)





ESET PROTECT On-Prem Agent佈署

1. 手動執行安裝包

The screenshot displays the ESET Protect On-Prem console interface. The main content area is titled '安裝程式' (Installers) and shows a table of installed agents. The table has columns for Name, Label, Type, Status, Product, Policy, Privilege, Language, Certificate, Parent Group, and Modified Time. Two entries are visible:

名稱	標籤	類型	狀態	產品	原則	授權	語言	憑證	上層群組	修改時間
ESET Management Agent		代理程式 Live Installer						CN=Agent at *,OU=aaa,O=aaa,L=a...	未分類	2025年6月13日 11:52:16
ESET Management Agent		全方位安裝程式						CN=Agent at *,OU=aaa,O=aaa,L=a...	未分類	2025年6月2日 13:46:55

At the bottom of the interface, there is a toolbar with buttons for '新增' (Add), '下載' (Download), and '處理方法' (Action). The '新增' button is highlighted with a red box, and a red arrow points to it from another red box highlighting the '新增過濾器' (Add Filter) button in the top right corner of the main content area.

1. 手動執行安裝包(續)

The screenshot shows the ESET Management Console interface for installing the ESET Management Agent. The 'Basic' step is selected in the left sidebar. The main content area displays three operating system options: Windows, macOS, and Linux. Below these are deployment methods: 'Download installation package or use ESET Remote Deployment Tool' (selected), 'First deployment agent (agent command-line installation)', and 'Use GPO or SCCM for deployment'. Under 'Components', 'Management Agent' is checked, while 'Security products', 'Full disk encryption', and 'ESET Inspect Connector' are unchecked. The 'Product improvement plan' section has 'Participate in product improvement plan' checked. The 'Super Group' field is highlighted with a red arrow and a red box containing the following notes:

!!! 注意!!!

- [伺服器主機名稱] 欄位不支援特殊字元 - 例如，帶有變音符號的字母。
- 憑證密碼不得包含下列字元：" \ 這些字元在代理程式初始化期間會造成嚴重錯誤。
- 密碼必須至少包含 14 個字元，且包含下列其中三個類別：小寫字母、大寫字母、數字或特殊字元。我們建議使用不少於 17 個字元的密碼。

2.使用GPO或SCCM

儀表板 安裝程式
安裝程式 > ESET Management Agent

基本
產品設定
發送

發送

下載安裝程式或使用 ESET Remote Deployment Tool
 首先部署代理程式 (代理程式指令)
 使用 GPO 或 SCCM 進行部署

元件

Management Agent
 安全性產品
 完整磁碟加密
 ESET Inspect Connector

產品改進計畫 **建議**
 參與產品改進計畫

上層群組
選取 或 建立
此欄位為必要。

伺服器主機名稱 (選用)
WIN-QK1V2D02HLS

上一步 繼續 完成 取消

!!! 注意!!!

- [伺服器主機名稱] 欄位不支援特殊字元 - 例如，帶有變音符號的字母。
- 憑證密碼不得包含下列字元：" \ 這些字元在代理程式初始化期間會造成嚴重錯誤。
- 密碼必須至少包含 14 個字元，且包含下列其中三個類別：小寫字母、大寫字母、數字或特殊字元。我們建議使用不少於 17 個字元的密碼。

2.使用GPO或SCCM (續)

eset PROTECT ON-PREM

輸入以搜尋...

快速連結

說明

ADMINISTRATOR

登出 > 23 小時

建立安裝程式

安裝程式 > ESET Management Agent

基本

發送

透過安裝程式下載 GPO/SCCM 指令碼

除了本機部署或遠端部署以外，您也可以使用例如群組原則物件 (GPO) 或 Software Center Configuration Manager (SCCM) 等管理工具。[深入瞭解...](#)

32 bit

64 bit

ARM 64

!!! 注意!!!

- 將代理安裝程式.msi 檔案和 install_config.ini檔案儲存在網域控制站上的共用資料夾中，以便所有用戶端電腦都可以使用讀取和執行權限存取它。

上一步 繼續 完成 取消

3.ESET Remote Deployment Tool

ESET 遠端部署工具先決條件

若要在 Windows 上使用 ESET Remote Deployment Tool，必須先符合下列先決條件：

- 必須安裝 ESET PROTECT 伺服器 and ESET PROTECT Web Console (在伺服器電腦上)。
- 必須開啟適當的連接埠。請參閱[用於在 Windows 作業系統的目標電腦上遠端部署 ESET Management 代理程式的連接埠](#)。
- 安裝套件的名稱必須包含字串 "x86" 或 "x64"。否則部署將無法運作。
- 必須建立搭售 (全方位) 安裝程式套件並將其下載到本機磁碟。
- 必須要具備建立全方位安裝程式的權限。



ESET PROTECT On-Prem Agent 佈署疑難排 解

疑難排解-代理程式部署

Windows

若要瞭解代理程式部署為何失敗，請瀏覽至 **[報告]** > **[自動]** > 按一下 **[過去 30 天代理程式部署工作資訊]**。

表格會顯示部署資訊。**[進度]** 欄會顯示關於代理程式部署失敗原因的錯誤訊息。

如果您需要更多詳情，請變更 ESET PROTECT 伺服器追蹤記錄的簡化設定。瀏覽至 **[其他]** > **[設定]** > **[進階設定]** > **[記錄]**，然後從下拉式功能表選取 **[錯誤]**。再次執行代理程式部署，若失敗，請在 ESET PROTECT 伺服器追蹤記錄檔中，查看位於檔案底端的最新記錄項目。報告將包括如何解決問題的建議。

ESET PROTECT 伺服器防護記錄	C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\tra
ESET Management 代理程式防護記錄	C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs

疑難排解-代理程式部署(續)

錯誤訊息	可能原因
無法連線	<ul style="list-style-type: none">•無法連線到網路上的用戶端，防火牆封鎖了通訊•用戶端防火牆或 Windows 防火牆上的外來連接埠 135、137、138、139 及 445 未開啟：允許外來檔案和印表機共用例外未使用。•無法解析用戶端的主機名稱，請使用有效的 FQDN 電腦名稱。
拒絕存取	<ul style="list-style-type: none">•在從加入網域的伺服器部署到加入網域的用戶端時，請以下列格式使用網域管理員群組成員之使用者的認證：Domain\DomainAdmin•在從加入網域的伺服器部署到加入網域的用戶端時，您可以從網路服務暫時提高 ESET PROTECT 伺服器服務的權限，以在網域管理員帳戶之下執行。•在從伺服器部署到非屬相同網域的用戶端時，請停用目標電腦上的遠端 UAC 過濾。•從伺服器部署到不同網域的用戶端時，請以下列格式使用系統管理員群組成員之本機使用者的認證：管理員。系統會自動在登入資訊前方加上目標電腦名稱。<ul style="list-style-type: none">•尚未設定管理員帳戶密碼•存取權限不足•ADMIN\$ 系統管理共用無法使用•IPC\$ 系統管理共用無法使用•簡易檔案共用已啟用
未找到存放庫中的套件	<ul style="list-style-type: none">•存放庫的連結不正確•存放庫無法使用•存放庫未包含所需套件
錯誤 1603	<ul style="list-style-type: none">•檢查 ra-agent-install.log 檔案。它位於下列位置：它位於下列位置：在目標電腦上的 C:\Users\%user%\AppData\Local\Temp\ra-agent-install.log。•如果仍會發生錯誤，請遵循我們的知識庫文章。

疑難排解-代理程式部署(續)

錯誤訊息	可能原因
無法連線到網路上的用戶端	從 ESET PROTECT 伺服器 伺服器 Ping 用戶端，若有得到回應，請嘗試遠端登入用戶端電腦 (例如透過遠端桌面)。
防火牆封鎖通訊	檢查伺服器與用戶端的防火牆設定，以及兩台電腦之間存在的任何其他防火牆 (如果適用的話)。 順利部署後，防火牆中連接埠 2222 和 2223 並未開放。確定已為兩台電腦 (用戶端與伺服器) 間的所有防火牆，開啟上述的連接埠。
無法解析用戶端的主機名稱	DNS 問題的可能解決方案包含 (但不限於)： •針對發生代理程式部署問題之伺服器和/或用戶端的 IP 位址和主機名稱使用 nslookup 命令。結果應符合該電腦的資訊。例如，對於針對主機名稱的 nslookup，其解析的 IP 位址應該要與發生問題之主機上 ipconfig 命令顯示的 IP 位址相同。nslookup 命令必須在用戶端與伺服器上執行。 •手動檢查 DNS 記錄是否有重複的項目。
尚未設定管理員帳戶密碼	為管理員帳戶設定適當的密碼 (不要使用空白密碼)。
存取權限不足	建立代理程式部署工作時嘗試使用網域管理員的憑證。如果用戶端電腦屬於工作群組，請使用該特定電腦上的本機管理員帳戶。 若要執行代理程式部署工作，則必須啟動管理員使用者帳戶。您可以建立屬於管理員群組的本機使用者，或藉由建立本機使用者來啟用內建的本機管理員帳戶。 若要啟動管理員使用者帳戶： 1.開啟系統管理命令提示字元 2.輸入下列命令： net user administrator /active:yes
ADMIN\$ 系統管理共用無法使用	用戶端電腦必須啟用共用資源 ADMIN\$。請確定在其他共用間也是啟用 ([開始] > [控制台] > [管理工具] > [電腦管理] > [共用資料夾] > [共用])。
IPC\$ 系統管理共用無法使用	請從伺服器的命令提示字元發出下列命令以確定伺服器可存取 IPC\$： net use \\clientname\IPC\$，其中 clientname 是目標電腦的名稱。
[使用簡易檔案共用] 已啟用	如收到「拒絕存取」錯誤訊息，且為混合式環境 (包含網域與工作群組)，則針對所有發生代理程式部署問題的電腦，停用 [使用簡易檔案共用] 或 [使用共用精靈]。例如，在 Windows 11 中執行下列步驟： •按一下 [開始]、在 [搜尋] 方塊中輸入檔案總管，然後按一下 [檔案總管選項]。按一下 [檢視] 索引標籤，並在 [進階設定] 方塊中向下捲動清單，接著取消選取 [使用共用精靈] 旁邊的核取方塊。

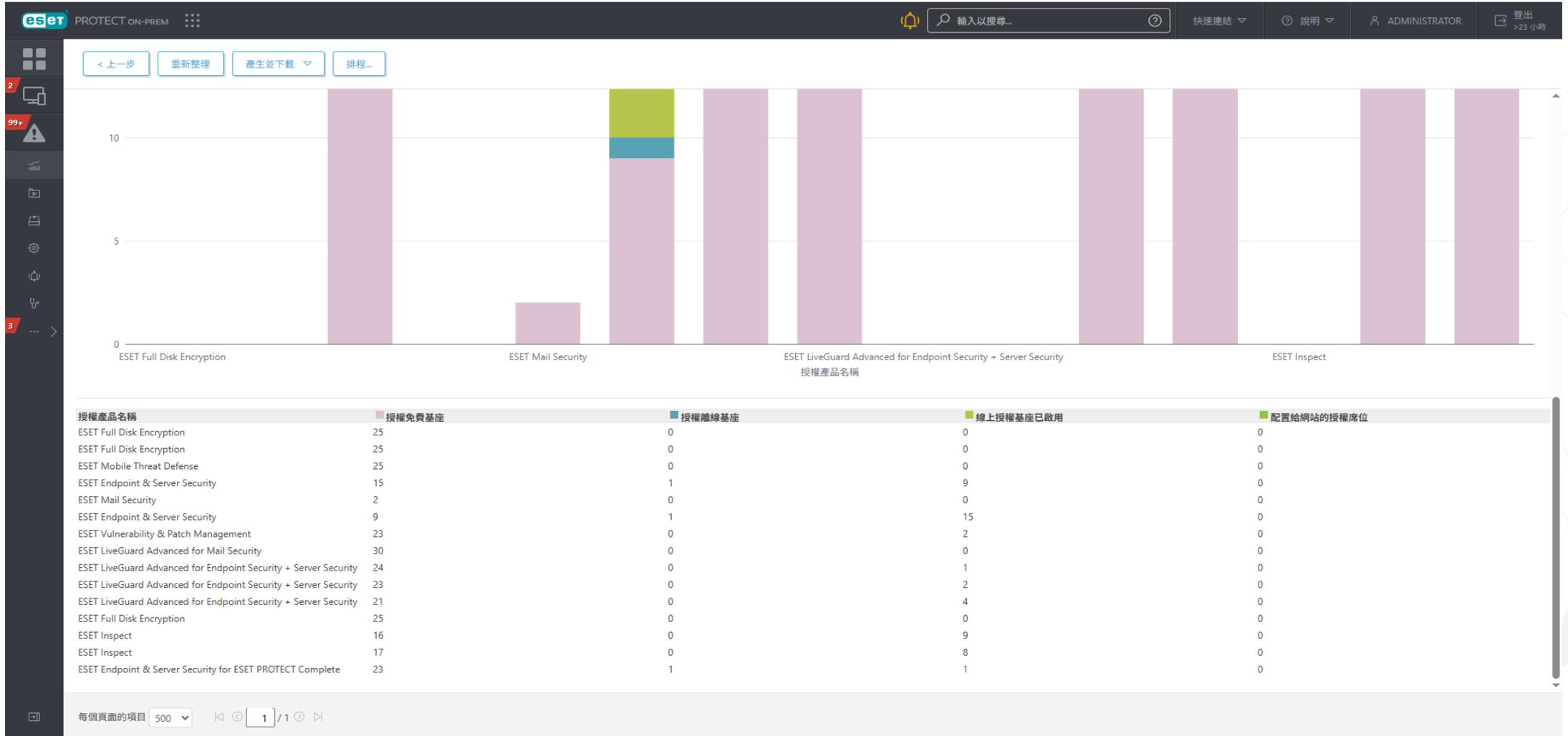


ESET PROTECT On-Prem 報告

1. 授權用途報告

The screenshot displays the ESET Protect On-Prem dashboard. The left sidebar contains a navigation menu with the following items: ESET Inspect, ESET LiveGuard, 伺服器效能 (Server Performance), 完整磁碟加密 (Full Disk Encryption), 審核和授權管理 (Audit and Authorization Management), 硬體存貨 (Hardware Inventory), 綜合報告 (Comprehensive Reports), 自動 (Automatic), 防毒偵測 (Antivirus Detection), 防火牆偵測 (Firewall Detection), 隔離區 (Isolation), 電子郵件伺服器 (Email Server), and 電腦 (Computer). A red arrow points to '審核和授權管理'. The main content area is divided into several sections: 伺服器效能 (Server Performance), 完整磁碟加密 (Full Disk Encryption), 審核和授權管理 (Audit and Authorization Management), and 硬體存貨 (Hardware Inventory). The '審核和授權管理' section contains three report cards: '新增報告範本' (New Report Template), '授權用途' (Authorization Usage), and '授權狀態總攬' (Authorization Status Overview). The '授權用途' card is highlighted with a red box and contains the text: '授權用途虛擬化，例如線上或離線啟動的可用單位數目' (Virtualization of authorization usage, such as the number of available units for online or offline activation). The top of the interface shows the ESET logo, 'PROTECT ON-PREM', a search bar, and user information for 'ADMINISTRATOR'.

1.授權用途報告(續)



2.電腦硬體概觀報告

The screenshot displays the ESET Protect On-Prem dashboard. The left sidebar contains a navigation menu with the following items: ESET Inspect, ESET LiveGuard, 伺服器效能, 完整磁碟加密, 審核和授權管理, **硬體存貨** (highlighted with a red arrow), 綜合報告, 自動, 防毒偵測, 防火牆偵測, 隔離區, 電子郵件伺服器, and 電腦. The main content area is titled '硬體存貨' and features several report cards. The '電腦硬體概觀' (Computer Hardware Overview) report card is highlighted with a red box. Below this, there are sections for '綜合報告' (Comprehensive Reports) and '自動' (Automatic) reports. At the bottom of the dashboard, there are buttons for '新增報告範本', '添加類別', and '匯入報告範本'. The top navigation bar includes the ESET logo, 'PROTECT ON-PREM', a search bar, and user information for 'ADMINISTRATOR'.

2.電腦硬體概觀報告(續)

ESet PROTECT ON-PREM

快速連結 說明 ADMINISTRATOR 登出 >23 小時

< 上一步 重新整理 產生並下載 排序...

報告: 電腦硬體概觀

伺服器名稱
WIN-QK1V2D02HLS

產生於:
2025年6月17日 09:28:46 (UTC+08:00)

記錄數
6

過濾
無過濾

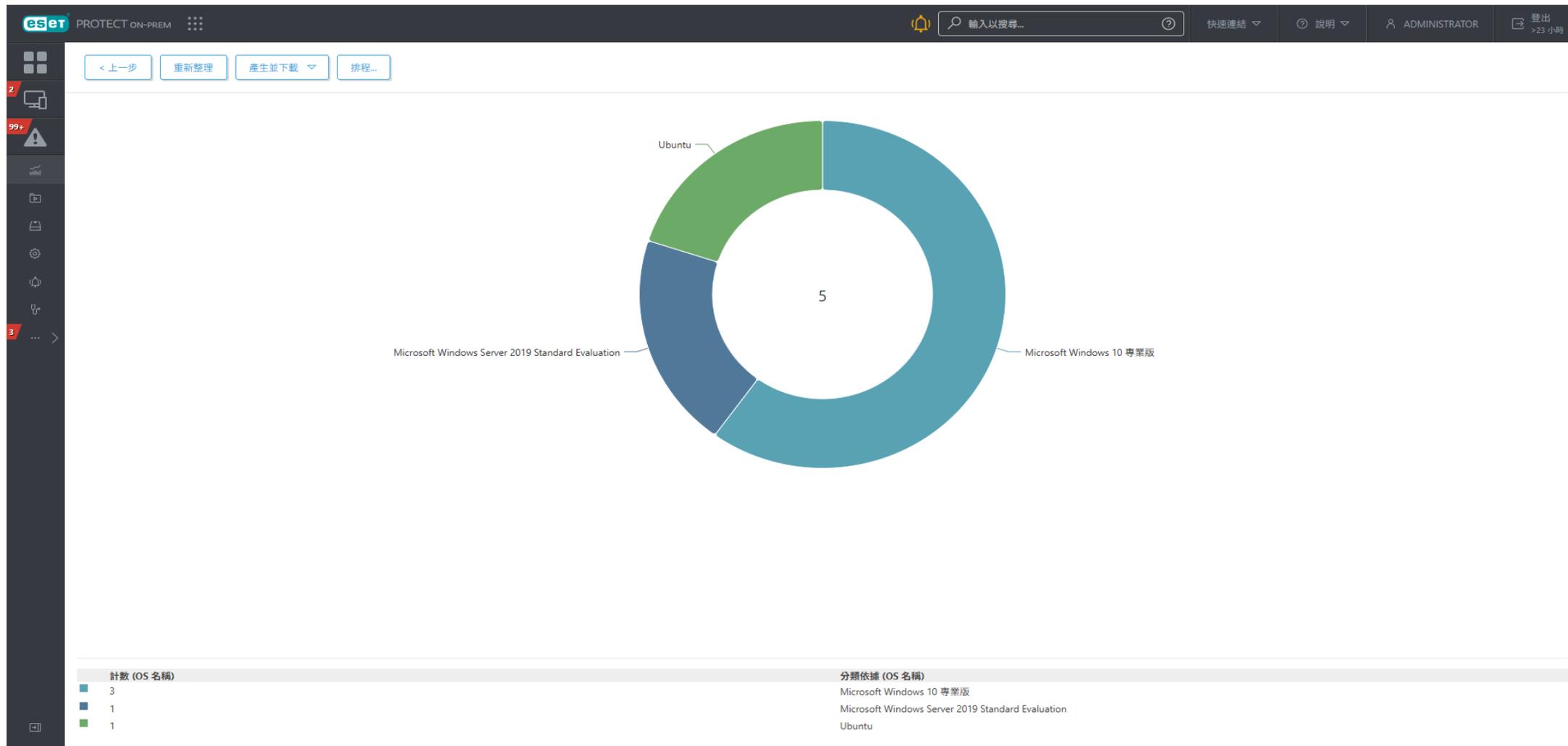
電腦名稱	CPU 製造商	CPU 架構類型	核心數量	RAM容量 [MB]	儲存容量 [MB]	裝置製造商	裝置型號	序號
win-qk1v2d02hls	GenuineIntel	x64	3		51199	innotek GmbH	VirtualBox	VirtualBox-d32ed3ce-3e1a-4876-a1ee-5962802b54f1
laptop-ao9its7e	GenuineIntel	x64	4	32768	976756	LENOVO	20S5S12X00	PF1SPDXF
desktop-dudrcp7	GenuineIntel	x64	1		51199	innotek GmbH	VirtualBox	VirtualBox-8dd8853c-f767-4b75-b705-deb3a9927971
desktop-armkk50	GenuineIntel	x64	2		51199	innotek GmbH	VirtualBox	VirtualBox-73040790-4f4c-47f9-aa82-15cad5aed569
ubuntu-srv								192.168.0.109

3. 作業系統報告

The screenshot displays the ESET Protect On-Prem dashboard. The top navigation bar includes the ESET logo, 'PROTECT ON-PREM', a search bar, and user information for 'ADMINISTRATOR'. The left sidebar lists various security features, with '電腦' (Computer) highlighted and a red arrow pointing to it. The main content area is titled '電腦' and contains a grid of 20 report cards. The '作業系統' (Operating System) report card is highlighted with a red border. Below the grid are buttons for '新增報告範本', '添加類別', and '匯入報告範本'.

報告類別	圖示	簡述
新增報告範本	📄	新增報告範本
上次更新	🕒	電腦依最新的偵測引擎更新分組
已安裝 ESET 應用程式	📄	安裝在電腦上的應用程式概要。僅回報 ESET 應用程式
已安裝 ESET 應用程式的細目	🕒	顯示已安裝 ESET 應用程式比例的環圖圖
已安裝的應用程式	📄	安裝在電腦上的應用程式概要。依預設，只會回報 ESET 應用程式
未連線電腦	📄	超過 14 天未連線的電腦概觀
未解決的複製問題	📄	所有目前未解決的複製問題清單。當代理程式 UUID 相同但硬體指紋 ID 不同的電腦連線至 ESET 安全管理中心時，會...
在過去 7 天內第一次連線的電腦	📄	過去 7 天內 ESET Management Agent 第一次連線至 ESET 安全管理中心 的電腦清單
在過去 7 天內復原身分的電腦清單	📄	在過去 7 天內復原身分的電腦清單。連線 ESET Management Agents 的電腦，會依據其電腦硬體指紋及來源電腦 (其...
有問題的電腦	📄	作業系統或受管理產品的已回報問題，其中包含詳細說明
作業系統	🕒	電腦作業系統概要
依據硬體偵測可靠性狀態分組的電腦	🕒	依據硬體偵測可靠性狀態分組的電腦。硬體可靠性狀態會表示機器是否適用於複製和重新成像
具有不可靠硬體偵測的電腦	📄	電腦清單 - 不會提供足夠資訊以進行可靠的硬體偵測。應停用硬體偵測，而且不應該用於複製及重新成像
具有未解決偵測的靜態群組	📄	回報顯示靜態群組，其中包含處於未解決狀態的偵測數量
首要電腦問題	🕒	由作業系統或受管理產品所回報的常見問題
偵測引擎更新狀態比例	🕒	由安全性產品所回報之已更新及未更新偵測引擎的比例
設定為複製原版的電腦	📄	設定為複製原版的電腦清單。從此類裝置複製和重新成像電腦應該不會造成問題
惡意電腦	📄	由 Rogue Detection Sensor 偵測到、但在 ESET 安全管理中心 Server 群組中沒有項目的電腦
惡意電腦比例	🕒	已知電腦和惡意電腦的比例
發生複製問題的電腦	📄	具有未解決複製問題的電腦清單。這可能表示正在從具有不同硬體指紋 ID 的機器回報相同的 Management UUID
過去 7 天內安裝的應用程式	📄	過去 7 天內安裝在電腦上的應用程式概要。依預設，只會回報 ESET 應用程式。
過期的應用程式	📄	電腦上逾期應用程式的概要
電腦上次連線時間	🕒	依上次連線時間而分類的電腦概觀
電腦狀態概要	🕒	依電腦狀態分類的電腦數

3.作業系統報告(續)





ESET PROTECT On-Prem 通知

SMTP伺服器設定

The screenshot displays the ESET Protect On-Prem administration console. The top navigation bar includes the ESET logo, 'PROTECT ON-PREM', a search bar, and user information for 'ADMINISTRATOR'. The left sidebar contains various management options, with '設定' (Settings) highlighted by a red arrow. The main content area shows the 'SMTP 伺服器' (SMTP Server) configuration page, which is enclosed in a red rectangular box. This page includes a search bar, a '設定' (Settings) header, and several configuration sections: 'SMTP 伺服器' (SMTP Server), 'ACTIVE DIRECTORY', and '系統日誌伺服器' (System Log Server). The 'SMTP 伺服器' section is the primary focus, containing a toggle for '使用 SMTP 伺服器' (Use SMTP Server), fields for '主機' (Host), '連接埠' (Port), '使用者名稱' (Username), and '密碼' (Password), and dropdown menus for '連線安全類型' (Connection Security Type) and '驗證類型' (Authentication Type). A '寄件者地址' (Sender Address) field is also present. Below these fields is a '測試 SMTP 伺服器' (Test SMTP Server) button and a note: '測試電子郵件將經由指定的 SMTP 伺服器傳送。' (Test email will be sent via the specified SMTP server). The 'ACTIVE DIRECTORY' section has a toggle for '使用 Active Directory 伺服器' (Use Active Directory Server) and fields for '主機' (Host), '使用者名稱' (Username), and '密碼' (Password). The '系統日誌伺服器' (System Log Server) section has a toggle for '使用系統日誌伺服器' (Use System Log Server). At the bottom of the settings page are '儲存' (Save) and '取消' (Cancel) buttons.

ESet PROTECT ON-PREM

設定 輸入以進行搜尋...

SMTP 伺服器

使用 SMTP 伺服器

主機

連接埠 25

使用者名稱

密碼 [顯示密碼](#)

連線安全類型 不安全

驗證類型 無認證

寄件者地址 ita 8

測試 SMTP 伺服器 [傳送測試電子郵件](#)

測試電子郵件將經由指定的 SMTP 伺服器傳送。

ACTIVE DIRECTORY

使用 Active Directory 伺服器

主機

使用者名稱

密碼 [顯示密碼](#)

根容器

系統日誌伺服器

使用系統日誌伺服器

儲存 取消

系統管理員 設定

通知啟用

The screenshot displays the ESET Protect On-Prem notification management interface. The interface includes a top navigation bar with the ESET logo, a search bar, and user information. The main content area shows a list of notifications with the following columns: Name, Status, and Description. Several notifications are highlighted with red boxes, indicating they are enabled and have a green status icon.

名稱	標籤	已啟用	狀態	通知說明	上次修改人員:
過期模組警告		○ 已停用	⚠ 電子郵件收件者遺失	至少 5% 的受管理電腦有過期模組 (...)	Administrator
受管理用戶端未連線警告		○ 已停用	⚠ 電子郵件收件者遺失	至少有 5% 的受管理用戶端超過 2 ...	Administrator
ESET 軟體過期警告		○ 已停用	⚠ 電子郵件收件者遺失	在至少一台受管理電腦上偵測到過...	Administrator
已偵測到惡意檔案 (木馬 / 蠕蟲 / 病毒 / 應用程式)		● 已啟用	✓	偵測到惡意檔案 (木馬 / 蠕蟲 / 病毒...	Administrator
通知具有無效的配置，因此不會進行觸發		○ 已停用	⚠ 電子郵件收件者遺失	因為不正確的配置、不適當的存取...	Administrator
已偵測到過期的 ESET Endpoint Antivirus 版本		○ 已停用	⚠ 電子郵件收件者遺失	在網路中偵測到至少一個過期的 ES...	Administrator
至少一部電腦已超過 14 天沒有連線		○ 已停用	⚠ 電子郵件收件者遺失	至少一部電腦已超過 14 天沒有連...	Administrator
已偵測到潛在不安的應用程式		● 已啟用	✓	在您網路中偵測到潛在不安全應用...	Administrator
電腦掃描期間已偵測到至少一個受感染的檔案並未自動清除		○ 已停用	⚠ 電子郵件收件者遺失	執行的電腦掃描已偵測到一個掃描...	Administrator
記憶體中發生的偵測		● 已啟用	✓	當進階記憶體掃描器偵測到偵測事...	Administrator
已偵測到潛在不需要的應用程式 (PUA)		● 已啟用	✓	當在您網路上偵測到 PUA (潛在不...	Administrator
已發生由 HIPS 偵測到的高嚴重性警示		● 已啟用	✓	當由 HIPS 觸發的高嚴重性偵測已報...	Administrator
已偵測到可疑的應用程式		● 已啟用	✓	在您網路中偵測到可疑的應用程式 (...)	Administrator
用戶端工作具有無效的配置，因此將會失敗		○ 已停用	⚠ 電子郵件收件者遺失	至少一個已建立的用戶端工作具有...	Administrator
第一次連線的新電腦		○ 已停用	⚠ 電子郵件收件者遺失	ESET Management Agent (7.x 及更...	Administrator
已復原電腦身分		○ 已停用	⚠ 電子郵件收件者遺失	已連線的電腦經重新成像 (將原版影...	Administrator
偵測到可能的電腦複製或硬體變更		○ 已停用	⚠ 電子郵件收件者遺失	在 ESET PROTECT On-Prem 中已連...	Administrator
授權即將到期警告		○ 已停用	⚠ 電子郵件收件者遺失	至少有一個受管理授權於不到 30 ...	Administrator
過度使用授權警告		○ 已停用	⚠ 電子郵件收件者遺失	至少有一個受管理授權過度使用時...	Administrator
授權限制警告		○ 已停用	⚠ 電子郵件收件者遺失	至少有一個受管理授權使用率超過 ...	Administrator

通知演示

The screenshot displays an email client interface with a list of messages on the left and a detailed view of a selected message on the right. The selected message is a security alert from ESET PROTECT.

Message List:

- 3/14/2025, 3:31 PM : this is test-2
- 3/14/2025, 5:37 PM : thisi u
- 3/27/2025, 4:53 PM : ita 已在電腦 laptop-ao9its7e 上偵測到惡意檔案 Python/Riskware.HackTool.Agent.A
- 3/28/2025, 11:44 AM : ita 已在電腦 desktop-armkk50 上偵測到惡意檔案 Win64/Havoc.L
- 3/31/2025, 11:53 AM : ita 已在電腦 desktop-armkk50 上偵測到惡意檔案 MSIL/Agent.DWN
- 4/1/2025, 11:12 AM : itz 已在電腦 laptop-ao9its7e 上偵測到惡意檔案 PowerShell/RiskWare.RemoteShell.E
- 4/24/2025, 11:18 AM : itac 已在電腦 laptop-ao9its7e 上偵測到惡意檔案 Win64/HackTool.GameHack.Q
- 4/29/2025, 11:23 AM : itz 已在電腦 laptop-ao9its7e 上偵測到惡意檔案 ASP/Webshell.K
- 5/6/2025, 9:29 AM : itz [ESET ALERT] 偵測到威脅:
- 5/6/2025, 9:30 AM : itad [ESET ALERT] 偵測到威脅:
- 5/6/2025, 9:32 AM : itad [ESET ALERT] 偵測到威脅:
- 5/6/2025, 9:35 AM : it [ESET ALERT] 偵測到威脅:

Selected Message Details:

Subject: 已在電腦 laptop-ao9its7e 上偵測到惡意檔案 Python/Riskware.HackTool.Agent.A

Sender: ESET PROTECT

Body:

新通知
已在電腦 laptop-ao9its7e 上偵測到惡意檔案 Python/Riskware.HackTool.Agent.A

偵測類型: 應用程式
偵測名稱: Python/Riskware.HackTool.Agent.A
電腦名稱: laptop-ao9its7e
電腦靜態群組階層: /全部/test_groups
登入的使用者: LA 德
發生時間: 2025/3/27 下午4:52:34 [UTC+8]
掃描器: 文件防護
已執行處理方法: 已保留

此訊息是由 ESET PROTECT On-Prem 傳送
ESET PROTECT On-Prem
© 1992-2025 ESET, spol. s r.o. All Rights Reserved.



ESET PROTECT On-Prem 威脅

威脅總覽

威脅

狀態	威脅類別	偵測類型	原因	物件	IP 位址	處理方法	電腦名稱
▲	防毒軟體			file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	潛在不安全應用程式	Linux/HackTool.AirCrack.A	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	潛在不安全應用程式	Linux/HackTool.AirCrack.A	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	潛在不安全應用程式	Linux/HackTool.AirCrack.A	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	潛在不安全應用程式	Linux/HackTool.AirCrack.A	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	潛在不安全應用程式	Linux/HackTool.AirCrack.A	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	應用程式	Python/Riskware.HackTool.Agent.A	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	特洛伊木馬程式	PowerShell/Agent.AVZ	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體			file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體			file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體			file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	特洛伊木馬程式	ASP/Webshell.LNE	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	特洛伊木馬程式	ASP/Webshell.FP	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	特洛伊木馬程式	CFM/Webshell.A	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	特洛伊木馬程式	Perl/Webshell.C	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	特洛伊木馬程式	Java/Webshell.DB	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	特洛伊木馬程式	ASP/Webshell.LAE	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e
▲	防毒軟體	特洛伊木馬程式		file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-inst...	192.168.0.143	已保留	laptop-ao9its7e

!!! 注意!!!
• 欄位設定記得新增物件這個設定，幫助標示出URI資訊。

威脅詳細資訊

The screenshot displays the ESET Protect On-Prem interface for a threat analysis. The main content area is divided into four sections, each highlighted with a green circle and a number:

- 1. 防毒軟體 (Antivirus Software):** A summary card showing the application type, occurrence date (3 months ago), and status (Total 1, Solved 0, Product handled 0). It includes a '調查 (INSPECT)' button.
- 2. 選擇標籤 (Select Tags):** A card showing system information for 'laptop-ao9its7e', including FQDN, last connection time, and a warning count of 54792. It includes a '顯示詳細資料' button.
- 3. 檔案 (File):** A table listing file details:

雜湊 (Hash)	064EEA07D840706B3ED3DE5A8A794A4C25C51FF3
名稱 (Name)	Python/Riskware.HackTool.Agent.A
偵測類型 (Detection Type)	應用程式 (Application)
物件類型 (Object Type)	檔案 (File)
統一資源識別碼 (URI)	file:///https://mirror.twds.com.tw/kali-images/kali-2025.1a/kali-linux-2025.1a-installer-amd64.iso/pool/main/c/commix/commix_4.0-0kali1_all.deb/data.tar.xz/data.tar/./usr/share/commix/src/core/shells/bind_tcp.py
程序名稱 (Process Name)	C:\Program Files\Google\Chrome\Application\chrome.exe
使用者 (User)	LA : 德 (German)
偵測旗標 (Detection Flag)	
- 4. 掃描 (Scan):** A bottom action bar with buttons for '偵測' (Detect), '標記為已解決' (Mark as Solved), '建立排除' (Create Exclusion), '電腦' (Computer), and '標籤' (Tag).

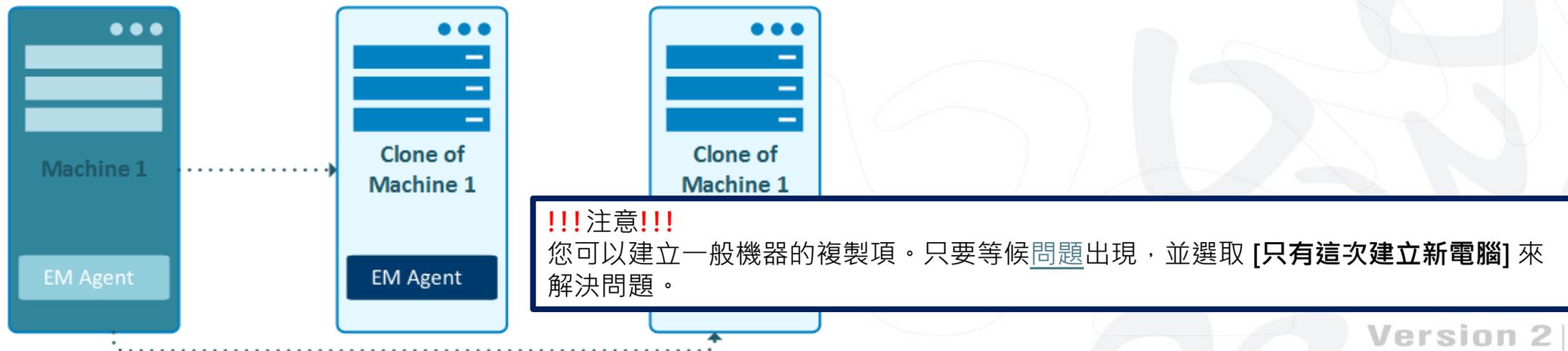


ESET PROTECT On-Prem VDI、克隆

VDI環境



在 Hypervisor 上克隆機器



VDI環境



1. 建立新電腦

每次映像部署之後於 ESET PROTECT On-Prem 中建立新機器。偵測到複製時，系統可以透過兩種方式做出反應：

- 手動 – 在 [問題] 中手動解決每部新電腦，然後選取 [每次建立新電腦]。
- 自動 – 在複製之前標記主機，並選取 [標記為主機以供複製] > [建立新電腦]。

2. 與現有電腦比對

如果在先前具有 ESET PROTECT On-Prem 歷程的電腦上重新部署映像 (已經部署 ESET Management 代理程式)，這部機器就會連線至其在 ESET PROTECT On-Prem 中的先前身分。如果先前沒有相符的身分，則系統會在新電腦上部署映像之後於 ESET PROTECT On-Prem 中建立新機器。偵測到複製時，系統可以透過兩種方式做出反應：

- 自動 – 在 [問題] 中手動解決每部新電腦，然後選取 [每次與現有電腦比對]。
- 自動 – 在複製之前標記主要機器，然後選取 [標記為主機以供複製] > [與現有電腦比對]

3. 平行複寫

ESET PROTECT 伺服器可辨識並解決將多部電腦平行複寫到 ESET PROTECT On-Prem 中的單一身分。系統會向電腦詳細資料 > [警示]回報這類事件 ('多個連線具有相同的代理程式 ID')。解決此問題的方式有兩種：

- 使用警示上可用的單擊動作 - 電腦已分割，其硬體偵測會永久關閉
- 在極少數情況下，即使已關閉硬體偵測的電腦也可能發生衝突 - 如果發生這種情況，重設複製代理程式工作是唯一的選項
- 在機器上執行重設複製代理程式工作，這將使您不必停用硬體偵測



ESET PROTECT Cloud管理



ESET PROTECT Cloud版本更新資訊

新功能

- 事件調查的新畫面

[事件] 區段現在包括新的畫面，顯示偵測、可執行檔案、處理程序和其他相關類別的資料，進而減少在事件調查期間切換到 ESET Inspect 的需要。[深入瞭解](#)

- 事件區段中 BETA 的處理程序樹狀結構

我們已在 [事件] 區段引入處理程序樹狀結構的 BETA 版本，以提高清晰度並簡化事件調查期間的瀏覽。目前，樹狀結構僅顯示一個偵測，但此限制將在下一個版本中解決。[深入瞭解](#)

- 修補程式管理擴展到 Linux

我們已將修補程式管理擴展到所有受支援的 Linux 發行版，確保其保持在最新和安全的狀態—就像 Windows 和 macOS 裝置一樣。[深入瞭解](#)

- Linux 上可用的網路隔離

我們將此功能擴展到 Windows 和 macOS 安全性產品之外，因此網路隔離現在可用於 Linux。安全性事件發生期間，Linux 端點可以快速進行隔離，防止威脅蔓延並增強跨多平台環境的防護。[深入瞭解](#)

- ESET Endpoint Antivirus for Linux 的新安裝程式

利用包含所有必要元件 (例如 Management Agent、EI 連接器、授權和自訂選項) 的綜合安裝程式，現在可以更輕鬆地上線 Linux 桌面裝置。[深入瞭解](#)

- 基本設定已擴展弱點與修補程式管理

基本設定可以輕鬆的配置整個網路的安全性設定，而無需使用原則或動態群組，現在還包括弱點與修補程式管理。[深入瞭解](#)

- 以 PDF 和 CSV 格式匯出弱點與修補程式管理報告

弱點與修補程式管理報告現在可以以 PDF 和 CSV 格式匯出，進而更容易的在主控制台之外共用資料和見解。[深入瞭解](#)

- 其他改進和錯誤修正

了解已在[變更日誌](#)上改進的其他內容。

更新與修復(續)

Added

- 新增：[Linux](#) 修補程式管理。
- 新增：[Linux](#) 的網路隔離。
- 新增：基本設定標籤中的漏洞和修補程式管理配置。
- 新增：適用於 Linux 的 ESET Endpoint Antivirus 的即時安裝程式。
- 新增：事件部分中的偵測、進程和執行檔的詳細畫面（適用於 ESET PROTECT 6.4 版本更新後所建立的事件）。
- 新增：事件部分中的偵測和進程的進程樹（適用於 ESET PROTECT 6.4 版本更新後建立的事件）。

Improved

- 改進：以 PDF 和 CSV 格式匯出漏洞和修補程式管理報告。
- 改進：審核導入的配置和透過 API 建立的配置。

REMOVED

- SysInspector 日誌檢視器。

FIXED

- 在電腦螢幕和用戶端詳細資訊中，應用的策略計數不同。
- 在稽核日誌中，匯入的策略中未顯示顯示變更的選項。
- 在 Rogue Computers 報告中，「新增全部」選項導致錯誤。
- 在電腦詳細資料中的策略應用程式訂單頁面上重新排序項目時的行為不正確。
- 安全產品的 CPU 使用率過高。
- 在極少數情況下，管理員無法對應新使用者。
- 其他小改進和錯誤修復。



ESET PROTECT Cloud作業系統支援

Windows用戶端作業系統支援

作業系統	代理程式	RD Sensor
Windows 10 x86	10.1—12.1	✓
Windows 10 x64 (所有正式版本)	10.1—12.1、12.2—12.4	✓
ARM 上的Windows 10	10.1—12.1、12.2—12.4	
Windows 11 x64	10.1—12.1, 12.2—12.4 (21H2, 22H2) 10.1—12.1, 12.2—12.4 (23H2) 11.3—12.1, 12.2—12.4 (24H2)	✓
ARM 上的Windows 11	10.1—12.1、12.2—12.4	

Windows伺服器作業系統支援

作業系統	代理程式	RD Sensor
Windows Server 2012 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2012 核心 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2012 R2 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2012 R2 核心 x64	10.1—12.1、12.2—12.4	✓
Windows 儲存伺服器 2012 R2 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2016 x64	10.1—12.1、12.2—12.4	✓
Windows 儲存伺服器 2016 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2019 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2022 x64	10.1—12.1、12.2—12.4	✓
Windows Server 2022 CORE x64	11.0—12.1、12.2—12.4	
Windows Server 2025 x64	12.0—12.1、12.2—12.4	

Linux作業系統支援

作業系統	代理程式	RD Sensor
Ubuntu 18.04.1 LTS x64 桌面	10.1—12.1、12.2—12.4	✓
Ubuntu 18.04.1 LTS x64 伺服器	10.1—12.1、12.2—12.4	✓
Ubuntu 20.04 LTS x64	10.1—12.1、12.2—12.4	✓
Ubuntu 22.04 LTS x64	10.1—12.1、12.2—12.4	✓
Ubuntu 24.04 LTS x64	11.0—12.1、12.2—12.4	
Linux Mint 20	10.1—12.1、12.2—12.4	✓
Linux Mint 21	10.1—12.1、12.2—12.4	✓
Linux Mint 22	11.3—12.1、12.2—12.4	✓
RHEL 伺服器 7 x64	10.1—12.1、12.2—12.4	✓
RHEL 伺服器 8 x64	10.1—12.1、12.2—12.4	
RHEL 伺服器 9 x64	10.1—12.1、12.2—12.4	✓
CentOS 7 x64	10.1—12.1、12.2—12.4	✓

Linux作業系統支援(續)

作業系統	代理程式	RD Sensor
SLED 15 x64	10.1—12.1、12.2—12.4	✓
SLES 12 x64	10.1—12.1、12.2—12.4	✓
SLES 15 x64	10.1—12.1、12.2—12.4	✓
Debian 9 x64	10.1—12.1、12.2—12.4	✓
Debian 10 x64	10.1—12.1、12.2—12.4	✓
Debian 11 x64	10.1—12.1、12.2—12.4	✓
Debian 12 x64	10.1—12.1、12.2—12.4	✓
Oracle Linux 8	10.1—12.1、12.2—12.4	✓
亞馬遜Linux 2	10.1—12.1、12.2—12.4	✓
亞馬遜Linux 2023	11.3—12.1、12.2—12.4	✓
Alma Linux 9	10.1—12.1、12.2—12.4	✓
Rocky Linux 8	10.1—12.1、12.2—12.4	
Rocky Linux 9	10.1—12.1、12.2—12.4	

Mac用戶端作業系統支援

作業系統	代理程式
macOS Catalina (10.15)	10.1—12.1、12.2—12.4
macOS Big Sur (11.0)	10.1—12.1、12.2—12.4
macOS Monterey (12.0)	10.1—12.1、12.2—12.4
macOS Ventura (13.0)	10.1—12.1、12.2—12.4
macOS Sonoma (14.0)	10.1—12.1、12.2—12.4
macOS Sequoia (15.0)	11.3—12.1、12.2—12.4

Android作業系統支援

作業系統	EESA	EESA 受限的輸入註冊	EESA 裝置擁有者	MDM iOS	MDM iOS ABM
Android 6.x 以上版本	✓	✓			
Android 7.x 以上版本	✓	✓	✓		
Android 8.x+	✓	✓	✓		
Android 9.0	✓	✓	✓		
Android 10.0	✓	✓	✓		
Android 11	✓	✓	✓		
Android 12	✓	✓	✓		
Android 13	✓	✓	✓		
Android 14	✓	✓	✓		
安卓 15	✓	✓	✓		
安卓 16	✓	✓	✓		

iOS作業系統支援

作業系統	EESA	EESA 受限的輸入註冊	EESA 裝置擁有者	MDM iOS	MDM iOS ABM
iOS 9.x 以上版本				✓	✓*
iOS 10.x 以上版本				✓	✓*
iOS 11.x 以上版本				✓	✓*
iOS 12.x 以上版本				✓	✓*
iOS 13.x+				✓	✓
iOS 14.x 以上版本				✓	✓
iOS 15				✓	✓
iOS 16				✓	✓
iOS 17				✓	✓
iOS 18				✓	✓
iPadOS 13				✓	✓
iPadOS 14				✓	✓
iPadOS 15				✓	✓
iPadOS 16				✓	✓
iPadOS 17				✓	✓
iPadOS 18				✓	✓

!!! 注意!!!
• iOS ABM 僅在選定的國家/地區可供使用。



ESET PROTECT 地端和雲端管理主控台之間的區別

主要差異的說明

一般差異	ESET 保護	ESET PROTECT 本機版
主機	在 ESET 維護的雲端環境中執行。	在實體或虛擬化環境上執行。
可管理的裝置限制	50,000 部用戶端裝置。	限制視伺服器硬體限制而定。
支援的產品版本	•商業產品第 6 版及更新版本	•商業產品第 4 版及更新版本
元件	<ul style="list-style-type: none"> •ESET Management 代理程式 •RD感測器 •部署工具 •CloudMDM 	<ul style="list-style-type: none"> •ESET Management 代理程式 •RD感測器 •部署工具
活動目錄	Active Directory 可使用 ESET Active Directory 掃描器 進行同步化。	Active Directory 同步化可用。
行動裝置管理	<div style="border: 2px solid blue; padding: 5px;"> <p>!!!注意!!!</p> <ul style="list-style-type: none"> •ESET PROTECT 行動裝置管理/連接器 (MDM/MDC) 元件 (僅限內部部署) 已於 2024 年 1 月終止支援。ESET PROTECT On-Prem 版本 11.1 及更新版本不支援行動裝置管理。 </div>	

主要差異的說明(續)

一般差異	ESET 保護	ESET PROTECT 本機版
憑證	由 ESET 處理憑證管理。	使用者可以建立、編輯或匯入/匯出憑證及憑證授權單位。
存取權限	存取權限管理已移動到 ESET Business Account，但您可以指定具有自訂權限的使用者對特定 ESET PROTECT 功能的存取權限。	進階多租戶存取權限安全性模型，可透過 ESET PROTECT On-Prem 介面加以管理
授權管理	授權管理已完全移動到 ESET Business Account。	授權管理有部分在 ESET PROTECT On-Prem，有部分在 ESET Business Account。
如何新增電腦	可以透過 Active Directory 同步化 同步化、從 RD Sensor 報告和使用 GPO 與 SCCM 安裝程式指令碼或透過 本機 安裝代理程式來新增電腦。	可透過 Active Directory 同步化 、從 RD Sensor 報告、使用 GPO 及 SCCM 安裝程式指令碼、新增「代理程式部署工作以手動新增裝置、或是在本機安裝代理程式來增加電腦。
額外防護階層	<ul style="list-style-type: none"> • ESET 弱點與修補程式管理 	<ul style="list-style-type: none"> • ESET LiveGuard

!!! 注意 !!!

- ESET PROTECT 不支援 ESET Inspect On-Prem，但支援 ESET Inspect。如果從 ESET PROTECT On-Prem 遷移到 ESET PROTECT，您將無法從 ESET PROTECT 管理 ESET Inspect On-Prem，但您可以從 ESET PROTECT 管理 ESET Inspect。



ESET PROTECT Hub 重點提示

語系選擇

The image shows a two-part interface. On the left is a promotional banner for ESET PROTECT HUB, and on the right is a '2. out of 2 steps' account activation form. The form includes fields for user country, language, phone number, and time zone, along with a checkbox for terms of use and two buttons: 'BACK' and 'ACTIVATE YOUR ACCOUNT'. The 'Language' dropdown menu is highlighted with a red border and shows '中文 (繁體)' selected.

Former ESET Business Account / ESET MSP Administrator

ESET PROTECT Hub is the central gateway to the ESET PROTECT unified security platform. It provides centralized identity, subscription and user management for all ESET platforms and all platform users.

- ✓ Get an overview of security subscriptions
- ✓ Check usage and status of subscribed services
- ✓ Allocate and control granular access to individual ESET platforms
- ✓ Single sign-in for all linked and accessible ESET platforms

Progress. Protected.

2. out of 2 steps

Activate your account

- **User country**
Taiwan, Province of China
- **Language**
中文 (繁體)
- **Phone number**
Phone number
- **Automatic time zone**
 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
- **Time zone**
(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

I agree to the ESET [Terms of Use](#)

[Help](#) [English](#)

© 1992 - 2025 ESET, spol. s r.o. - All rights reserved

資料中心位置與語言

eset PROTECT HUB

儀表板

授權

網站

使用者

警示

作用中單位

要求

我的公司

管理員設定

審查防護記錄

提交意見

收合

啟動雲端解決方案

啟動 ESET PROTECT

● 必須欄位

資料中心位置

EU

USA

CANADA

GERMANY

選擇不推薦的遠端資料中心將會影響服務品質。啟動 ESET PROTECT 後，您將無法變更資料中心的位置。

語言

中文 (繁體)

上一步 啟動 取消

啟用ESET PROTECT

The screenshot displays the ESET PROTECT HUB dashboard. At the top, the ESET logo and 'PROTECT HUB' are visible. The user is logged in as 'RENDE WANG' with a '登出 > 5 分鐘' (Logout > 5 minutes) option. A notification bell icon shows '1' new notification. The main navigation menu on the left includes: 儀表板 (Dashboard), 授權 (Licenses), 網站 (Sites), 使用者 (Users), 警示 (Alerts), 作用中單位 (Active Units), 要求 (Requests), 我的公司 (My Company), 管理員設定 (Admin Settings), and 審查防護記錄 (Review Protection Records). The main content area is titled 'Dashboard' and features a large dark green panel with the text 'N/A, 歡迎您' (N/A, Welcome) and '請按照以下步驟設定您的環境, 並充分利用 ESET 解決方案。' (Please follow the following steps to set up your environment and fully utilize ESET solutions). The steps are: 1. 新增您購買的授權或產生 ESET PROTECT Advanced 免費試用授權 (Add your purchased license or generate ESET PROTECT Advanced free trial license) - marked with a green checkmark. 2. 啟動雲端解決方案以部署保護 (Activate cloud solutions for deployment protection). 3. 邀請使用者管理您的安全性 (Invite users to manage your security). 4. 自訂管理員設定 (Customize admin settings). Below this, the '警告' (Alerts) section shows 0 alerts, 0 warnings, and 0 information messages. A message box states '目前沒有警告。一切都安全無虞。' (There are no alerts. Everything is safe and sound). The 'ESET PROTECT 平台' (ESET PROTECT Platform) section lists: ESET PROTECT (正在進行啟動 - Starting), ESET Inspect (取得解決方案, 深入瞭解), ESET Cloud Office Security (取得解決方案, 深入瞭解), and ESET Secure Authentication (取得解決方案, 深入瞭解).

ESET PROTECT快速連結

The screenshot displays the ESET PROTECT HUB interface. The top navigation bar includes the ESET logo, 'PROTECT HUB', a notification bell with a '3' badge, a '說明' (Help) dropdown, the user name 'RENDE WANG', and a '登出 > 5 分鐘' (Logout > 5 minutes) button. The left sidebar contains menu items: 儀表板 (Dashboard), 授權 (Licenses), 網站 (Sites), 使用者 (Users), 警示 (Alerts), 作用中單位 (Active Units), 要求 (Requests), 我的公司 (My Company), 管理員設定 (Admin Settings), and 審查防護記錄 (Review Protection Records). The main 'Dashboard' area features a 'N/A, 歡迎您' (Welcome) message and a progress bar with three steps: '新增您購買的授權或產生 ESET PROTECT Advanced 免費試用授權' (Add licenses or generate trial licenses), '啟動雲端解決方案以部署保護' (Activate cloud solutions for deployment), and '邀請' (Invite). Below this is an '警告 0' (Alerts 0) section with three categories: '警告' (Warnings) with 0, '警告' (Warnings) with 0, and '資訊' (Info) with 0. A message at the bottom states '目前沒有警告。一切都安全無虞。' (No alerts at the moment. Everything is safe). The right-hand pane shows 'ESET PROTECT' status cards, with a red arrow pointing to the 'ESET PROTECT' card which is marked as '已啟動' (Activated). Below this are cards for 'ESET Inspect', 'ESET Cloud Office Security', and 'ESET Secure Authentication', each with '取得解決方案' (Get solution) and '深入瞭解' (Learn more) buttons.



ESET PROTECT Cloud WebConsole初次設定

WebConsole登入資訊說明



ESET PROTECT 是您用於管理整個組織之安全性的主要儀表板。

- ✓ 即時查看網路安全性
- ✓ 自動解決安全性事件
- ✓ 管理端點、伺服器及行動裝置
- ✓ 完整磁碟加密和雲端沙箱管理
- ✓ 使用預設原則範本，靈活地進行報告和配置

Progress. Protected.

登入

電子郵件

密碼

登入

[忘記密碼](#)

或

 使用 Microsoft 登入

BETA

!!!注意!!!

• 登入網址會跟資料中心位址有關, 下列網址選擇是EU範例
<https://eu02.protect.eset.com>,

WebConsole 首次登入設定精靈

步驟 2 之 1
設定防護

ESET 安全性產品 **建議**

檢閱並調整一律套用到與 ESET PROTECT 連線之所有裝置的安全性設定。[深入瞭解 ESET 說明。](#)

使用密碼鎖定安全性設定 ≥ 7.0 ⓘ

- 密碼

自動解決問題 ≥ 9.1 ⓘ

1 天之後 ▾

始終在現有和新裝置上安裝 ESET 安全性產品 ⓘ

始終在現有裝置上啟動 ESET 安全性產品 ⓘ

上一步 下一步 稍後詢問

提交意見 收合

!!! 注意!!!

• 把**始終在現有和新裝置上安裝 ESET 安全性產品**與**始終在現有裝置上啟動 ESET 安全性產品**關閉。

WebConsole首次登入設定精靈(續)

步驟 2 之 1
設定防護

ESET 安全性產品	ESET LiveGuard
	<p>ESET LiveGuard</p> <p>雲端沙箱提供一個功能強大的隔離測試環境，其中會執行可疑程式，而且會以自動方式觀察、分析和報告可疑程式的行為。這對於零時差威脅 (包含勒索軟體) 特別實用。深入瞭解 ESET LiveGuard。</p> <p>檢閱並調整一律套用到與 ESET PROTECT 連線之所有裝置的安全性設定。深入瞭解 ESET 說明。</p> <p><input checked="" type="checkbox"/> 一律啟用現有和新裝置上的 ESET LiveGuard ?</p> <p><input checked="" type="radio"/> 最佳防護 建議 風險檔 (包括支援巨集的文件類型) 將被傳送到安全的 ESET 伺服器，以用於自動掃描和行為分析。在檔案評估為安全之前，對檔案的存取將受到限制。將啟用 ESET LiveGrid[®] 意見系統。</p> <p><input type="radio"/> 基本防護 這提供基本的安全性層級，其中僅掃描有限的一組檔案。與建議的設定相比，防護受到限制。將啟用 ESET LiveGrid[®] 意見系統。</p> <p>上一步 套用 稍後詢問</p>



ESET PROTECT Cloud 新增管理者

建立新ESET PROTECT 使用者(續)

一.一般-提供有關使用者的基本資訊

二.存取權限:

a)公司存取 - 選取使用者在公司的存取層級：**寫入、讀取、僅能存取選取的網站**。

b)使用者管理存取 - 選取核取方塊以允許使用者管理 ESET Business Account 中的其他使用者。

c)ESET PROTECT 與 ESET Inspect 存取：

- 寫入 - 使用者可以完全存取 ESET PROTECT 和 ESET Inspect 。
- 讀取 - 使用者僅能檢視 ESET PROTECT 和 ESET Inspect 中的資料。
- 自訂 - 您可以稍後在 ESET PROTECT 的 [權限集] 中定義使用者存取。
- 無存取 - 使用者無權存取 ESET PROTECT 和 ESET Inspect 。

三.喜好設定-為 ESET Business Account 和 ESET PROTECT 設定使用者的語言，以及設定時區。

四.安全-調整使用者的安全設定 (密碼到期、閒置工作階段逾時、雙因素驗證)。

建立新ESET PROTECT 使用者(續)

新增使用者

一般

名字: John

姓氏: Smith

說明 (選用):

電子郵件地址: email@address.com

電話號碼 (選用):

國家: 美國

存取權限

公司存取權

- 高入
使用者具有完整存取權。
- 已讀取
使用者只能檢閱已收集的資料。
- 高入
使用者具有完整存取權，能夠建立和執行動作。
- 已讀取
使用者只能檢閱 ESET PROTECT 產品數據庫中已收集的資料。

建立 取消

	USER	STATUS
<input type="checkbox"/>		Active
<input type="checkbox"/>		Active
<input type="checkbox"/>	John Smith	Waiting for activation

新使用者會出現在具有等待啟動標籤的使用者管理中。

按一下 [建立] 以建立使用者。

建立新ESET PROTECT 使用者(續)

The image shows two parts of the ESET Business Account activation process. On the left is an email template addressed to 'John Smith'. The email text includes: 'Dear John Smith, You have been invited to access ESET Business Account of ESET by administrator [redacted]. [Activate your account](#) With this single user account, you can access all the ESET business cloud solutions for which you have permission. The activation link can be used for the next 48 hours. Sincerely, The ESET Team'. At the bottom of the email is the copyright notice '© 1992 - 2023 ESET | Progress. Protected.'. On the right is the 'ACTIVATE THE ACCOUNT' web page. It features the ESET logo and the text: 'ESET Business Account is a license management platform for all ESET business solutions as well as an entry point to ESET cloud services.' Below this is a list of benefits: '✓ Create a fully functional free trial (no commitment)', '✓ Get an overview of all your security licenses', '✓ Check the real-time status on used up seats', and '✓ Deactivate and recoup immediately'. At the bottom of the page is the slogan 'Progress. Protected.'. On the far right is a registration form with fields for Name (John Smith), E-mail, Phone number, Language (English), EPC Language (English), Create password, and Confirm password. The password requirements are: 'Minimum number of characters: 10', 'One lowercase character', 'One uppercase character', 'One number', and 'One special character'. There is a checked checkbox for 'I agree to the ESET Terms of Use' and a blue 'ACTIVATE THE ACCOUNT' button.

使用者將收到一封啟動電子郵件 (寄給在建立該使用者時您指定的電子郵件地址)。使用者必須按一下 [啟動您的帳戶]。

使用者需要調整使用者設定並輸入密碼兩次 ([建立密碼] 和 [確認密碼])，選取 [我同意 ESET 使用條款] 的核取方塊，然後按一下 [啟動該帳戶]。



ESET PROTECT Cloud Agent 佈署

保護裝置

The screenshot displays the ESET PROTECT web dashboard. The top navigation bar includes the ESET logo, a search bar with the placeholder text "輸入以搜尋...", and user information for "RENDE WANG" with a "登出" (Logout) button. The left sidebar contains a menu with items: 儀表板 (Dashboard), 電腦 (Computers), 事件 (Events), 威脅 (Threats), 報告 (Reports), 工作 (Jobs), 安裝程式 (Installers), 配置 (Configurations), 通知 (Notifications), 狀態概觀 (Status Overview), 平台模組 (Platform Modules), and 更多 (More). The main content area features a central message with a crossed-out computer icon, stating: "在公司網路上分發安全性產品。" (Distribute security products on the corporate network.) Below this, it says: "有不同方法可以啟用 ESET 安全性產品，並根據作業系統將裝置連線到 ESET PROTECT。" (There are different ways to enable ESET security products and connect the device to ESET PROTECT according to the operating system.) Two buttons are present: "保護裝置" (Protect Device) and "瀏覽 ESET PROTECT" (View ESET PROTECT). A large red arrow points to the "保護裝置" button. At the bottom left of the sidebar, there is a "提交意見" (Feedback) button and a "收合" (Collapse) button.

Agent佈署

eset PROTECT

儀表板
電腦
事件
威脅
報告
工作
安裝程式
1 配置
通知
狀態概觀
平台模組
更多

輸入以搜尋... 快速連結 說明 RENDE WANG 登出

正在套用設定

步驟 2 之 2
安裝 ESET 安全性產品以管理和保護您的裝置

在公司網路上散佈安全性產品。有多種方法可以根據作業系統啟用 ESET 安全性產品並將裝置連線到 ESET PROTECT。 [深入了解 ESET 說明。](#)

Windows macOS Linux Android或iOS

防護和安裝設定 **建議**

- 啟用 ESET LiveGrid® 意見系統 (建議) [?]
- 啟用潛在不需要的應用程式偵測 [?]
- 參與產品改進計畫 [?]

• 使用者授權合約

我接受 [使用者授權合約](#) 條款，並瞭解 [隱私權政策](#)。
此欄位為必要。

下載 自訂安裝程式 上一步 關閉

提交意見
收合

Agent佈署(續)

The screenshot shows the ESET Management Agent console interface. The top navigation bar includes the ESET logo, a search bar, and user information. The left sidebar contains various navigation options. The main content area is titled '建立安裝程式' (Create Installation) and '儀表板 > ESET Management Agent'. The '發送' (Send) step is selected in the left sidebar. The '分發安裝程式' (Distribute Installation) section shows a URL, a '下載' (Download) button, and a SHA256 hash. Below this is the '遠端部署' (Remote Deployment) section with a '深入瞭解' (Learn More) button. A red box highlights the '透過電子郵件傳送' (Send via email) section, which contains a table with columns for '電子郵件地址' (Email Address) and '名稱' (Name). The table is currently empty, and a message states '尚未新增任何電子郵件地址' (No email addresses added yet). A blue box at the bottom contains the following text:

!!! 注意!!!
• **更多**裡可以選擇以CSV檔案匯入更多成員。

Agent佈署(續)



!!!!注意!!!!

•收到電子郵件的使用者會看到這封郵件，點擊下載後進行套件安裝。



ESET PROTECT Cloud WebConsole與On-Prem差異的部分

儀錶板資訊

The screenshot displays the ESET PROTECT dashboard. The top navigation bar includes the ESET logo, a search bar, and user information (RENDE WANG). The left sidebar contains navigation options like '儀錶板', '電腦', '事件', '威脅', '報告', '工作', '安裝程式', '配置', '通知', '狀態概觀', '平台模組', and '更多'. The main content area is titled '儀錶板' and features several status cards:

- 電腦狀態 1:** 在電腦上未發現問題。網路目前沒有警示。如果出現任何問題，您將在此處看到顯示的受影響電腦數量及其狀態。 [重新整理]
- 事件狀態:** 沒有要顯示的事件。建立事件之後，其將出現在此處。 [重新整理]
- 主要功能問題:** 無功能問題。網路目前沒有任何功能問題。如果出現任何問題，您將在此處看到顯示的問題數量和嚴重性。 [重新整理]
- 最具影響力的作用中事件:** 沒有要顯示的事件。建立事件之後，其將出現在此處。 [重新整理]
- 電腦連線狀態:** 顯示連線狀態的圓形圖表。
 - 線上: 1
 - 1天: 0
 - 1-7天: 0
 - > 7天: 0
 - 絕不: 0
- 電腦管理狀態:** 顯示管理狀態的圓形圖表。
 - 受保護: 0
 - 未受保護: 1
 - 未受管理的: 0
- 平台模組:** 顯示各產品安裝進度的柱狀圖。
 - ESET 安全性產品: 100%
 - ESET LiveGuard: 100%
 - ESET Full Disk Encryption: 100%
 - ESET 弱點與修補程式管理: 100%
 - ESET Inspect: 100%
- 版本狀態:** 顯示版本更新進度的柱狀圖。
 - 100%
 - 80%
 - 60%
- 廣告:** WeLiveSecurity BladedFeline: Whispering in the dark, 2025年6月5日。

At the bottom left, there is a '提交意見' button and a '收合' button. A red box highlights a warning message:

!!! 注意!!!

- 最少要有一台端點有安裝Agent並正常連線回主控台後，儀錶板才會開始顯示資訊。
- 服務狀態網頁讓管理者知道目前雲端服務狀況，網址：<https://status.eset.com/>。

配置調整

The screenshot displays the ESET PROTECT web interface. The top navigation bar includes the ESET PROTECT logo, a search bar with the text "輸入以搜尋...", and user information for "RENDE WANG". The left sidebar contains a menu with items: 儀表板, 電腦, 事件, 威脅, 報告, 工作, 安裝程式, **配置** (highlighted with a red arrow), 通知, 狀態概觀, 平台模組, and 更多. The main content area is titled "配置" and has two tabs: "基本設定" (selected) and "進階設定". Under "基本設定", there is a sub-section for "ESET 安全性產品" and "ESET LiveGuard". The "ESET 安全性產品" section includes a sub-header "ESET 安全性產品" and a description: "檢閱並調整一律套用到與 ESET PROTECT 連線之所有裝置的安全性設定。" followed by a link "深入瞭解 ESET 說明。". Below this are five settings: 1. "使用密碼鎖定安全性設定" (version ≥ 7.0) is turned off. 2. "自動解決問題" (version ≥ 9.1) is turned on, with a dropdown menu set to "1 天之後". 3. "始終在現有和新裝置上安裝 ESET 安全性產品" is turned on. 4. "始終在現有裝置上啟動 ESET 安全性產品" is turned on. At the bottom of the settings area are three buttons: "上一步", "下一步", and "套用".

平台模組

平台模組

ESET LiveGuard Advanced 零時差防護

雲端沙箱提供一個功能強大的隔離測試環境，其中會執行可疑程式，而且會以自動方式觀察、分析和報告可疑程式的行為。這對於零時差威脅 (包含勒索軟體) 特別實用。

✓ 自動啟用目前處於作用中狀態，為所有符合資格的電腦提供最佳防護。

ESET Full Disk Encryption

由 ESET 遠端管理主控台原生管理的強大加密。您可增加您組織的資料安全性，以滿足合規性法規。

ESET 弱點與修補程式管理

透過修補過時的應用程式和作業系統，主動識別並修復公司裝置上的弱點。這改善了整體網路安全性並減輕網路攻擊者利用弱點的高危。

ⓘ 您目前的授權不包含 ESET 弱點與修補程式管理。若要存取此功能，請升級到更高階層的授權。 [了解哪些授權包含 ESET 弱點與修補程式管理](#)

ESET Inspect 和 MDR 全面的 XDR 和增強的威脅防護

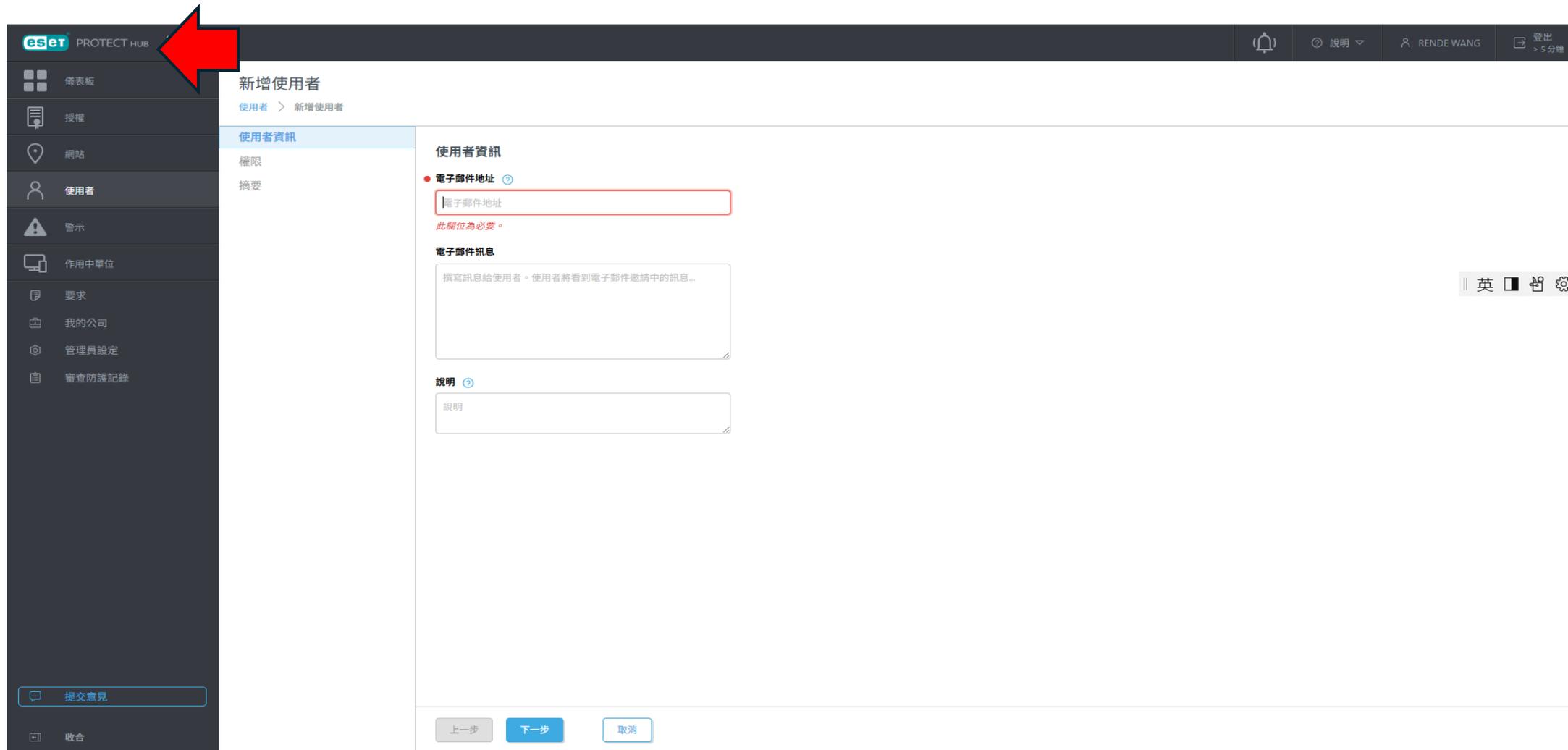
ESET Inspect 支援擴展的偵測和回應 (XDR)，可讓您快速有效地識別異常行為和洩露，並提供進階威脅偵測、風險評估、事件回應、調查和修復功能。這項保護的另一層是我們的受管偵測和回應 (MDR) 服務，可增強 XDR。它透過全天候受管偵測和回應，利用 AI 和人類專業知識，透過持續的威脅偵測和監視提供卓越的防護。

ⓘ 您目前的授權不包含 ESET Inspect (XDR) 和受管偵測和回應 (MDR)。若要存取這些功能，請升級到更高階層的授權。 [了解哪些授權包含 ESET Inspect \(XDR\) 和受管偵測和回應 \(MDR\)](#)

!!! 注意!!!

- 模組功能的啟用是灰色表示需要額外授權才能啟用模組功能。

新增管理人員



The screenshot shows the ESET Protect Hub interface for adding a new user. The left sidebar contains a navigation menu with the following items: 儀表板 (Dashboard), 授權 (Licenses), 網站 (Sites), 使用者 (Users), 警示 (Alerts), 作用中單位 (Active Units), 要求 (Requests), 我的公司 (My Company), 管理員設定 (Admin Settings), and 審查防護記錄 (Review Protection Logs). A red arrow points to the '使用者' (Users) item. The main content area is titled '新增使用者' (Add User) and includes a breadcrumb '使用者 > 新增使用者'. The '使用者資訊' (User Information) section is active, showing a form with the following fields: '電子郵件地址' (Email Address) with a red border and a note '此欄位為必要。' (This field is required.); '電子郵件訊息' (Email Message) with a placeholder '撰寫訊息給使用者。使用者將看到電子郵件邀請中的訊息...' (Compose a message for the user. The user will see the message in the email invitation.); and '說明' (Description) with a placeholder '說明' (Description). At the bottom of the form are buttons for '上一步' (Previous Step), '下一步' (Next Step), and '取消' (Cancel). The top right of the interface shows a notification bell, a help icon, the user name 'RENDE WANG', and a '登出' (Logout) button with a timer '> 5 分鐘'. A language selector '|| 英 | 中' and a settings gear icon are also visible.

新增管理人員(續)

歡迎使用 ESET PROTECT

Hub 收件匣



ESET PROTE... 17:11



寄給我 ▾



一律顯示這位寄件者的圖片

eset PROTECT HUB

您好，

使用者 **RENDE WANG** 邀請您加入公司
N/A 的 ESET PROTECT Hub。

啟動您的帳戶

!!!注意!!!

- 輸入必要資訊後，完成新的管理人員註冊資訊。

新增管理人員(續)

群組

原生使用者

RR Microsoft Entra ID 群組

名稱	電子郵件地址	狀態	我的公司	ESET PROTECT 存取權	雙因素驗證已啟用	說明
RENDE WANG	potatoesugi@gmail.com	✔ 啟動	現存取	存取	● 已停用	
	wrdu6422@gmail.com	🕒 擱置中	存取	存取	● 已停用	

!!!注意!!!

- 新的管理人員完成註冊後狀態資訊會變啟動。

新增使用者



ESET PROTECT Cloud 弱點與修補程式管理 常見問題

常見問題

弱點涵蓋的應用程式清單多久更新一次？

- V&PM 可根據**每週更新數次的資料庫**偵測新增的軟體。
- 該清單每天都會根據提供者的資料進行更新。

弱點功能中是否會掃描不在受支援應用清單內的應用程式？

仍會偵測到弱點清單中未涵蓋的應用程式。僅未偵測和列出特定版本的弱點。修補程式管理提供最新版本的升級。

V&PM 是否僅會顯示和修補先前易受攻擊的應用程式版本，還是也會修補過時且不易受攻擊的應用程式版本？

V&PM **可以修補非 CVE 型的應用程式**。修補程式管理可以升級弱點清單中未涵蓋的應用程式版本。

弱點解決後，弱點清單是否會移除？

是的，**弱點解決後，弱點清單就會移除或更新**。

V&PM 掃描具體的觸發方式為何？

根據管理員在原則中進行的設定，V&PM 排程器會觸發 V&PM 掃描。

在選定的時段內會發生什麼事？

掃描每天會在指定的時間範圍內執行一次。當電腦在此時間範圍內啟動時，系統將啟動掃描。

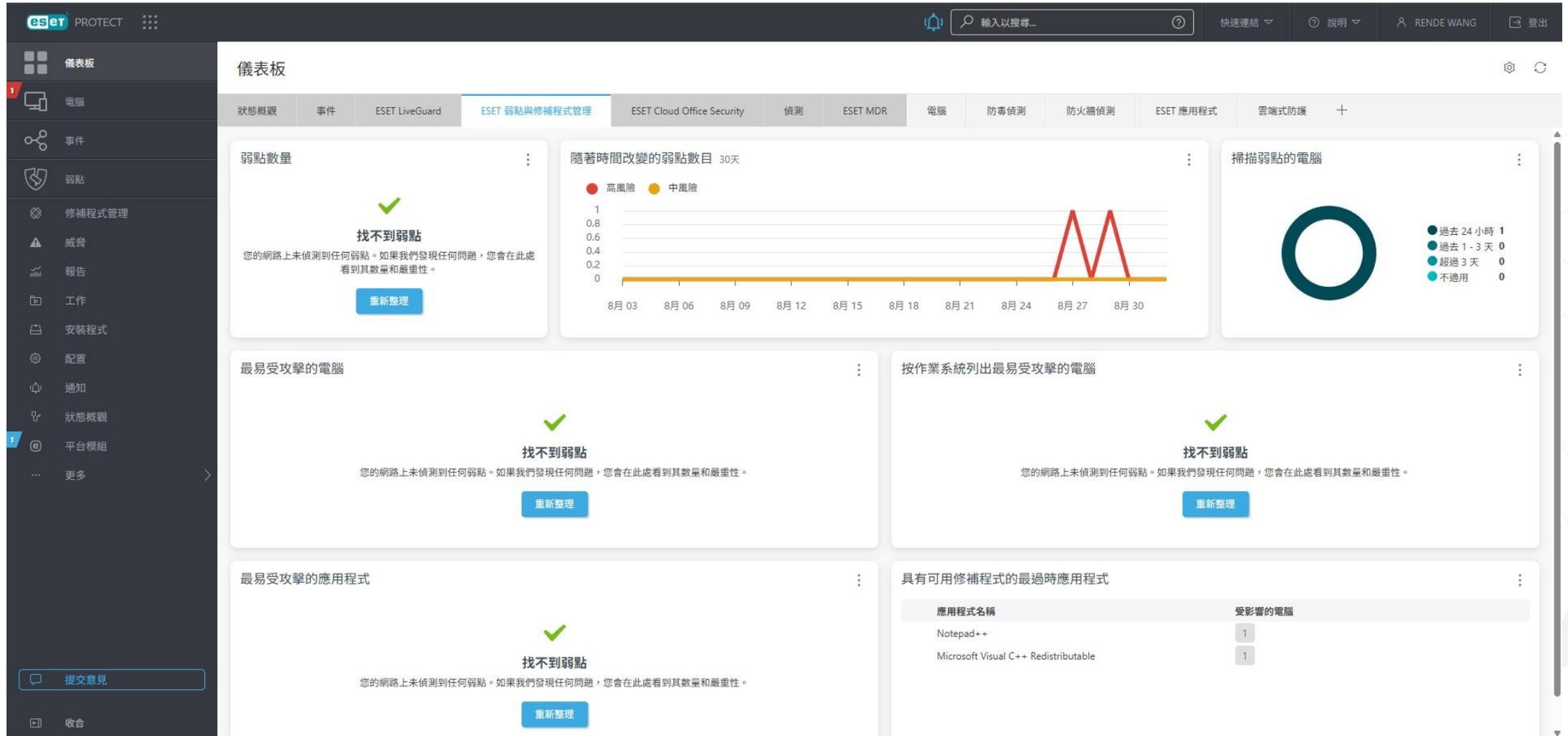
我是否應該在弱點頁面中看到作業系統弱點？

V&PM **可以偵測應用程式弱點和作業系統弱點**。

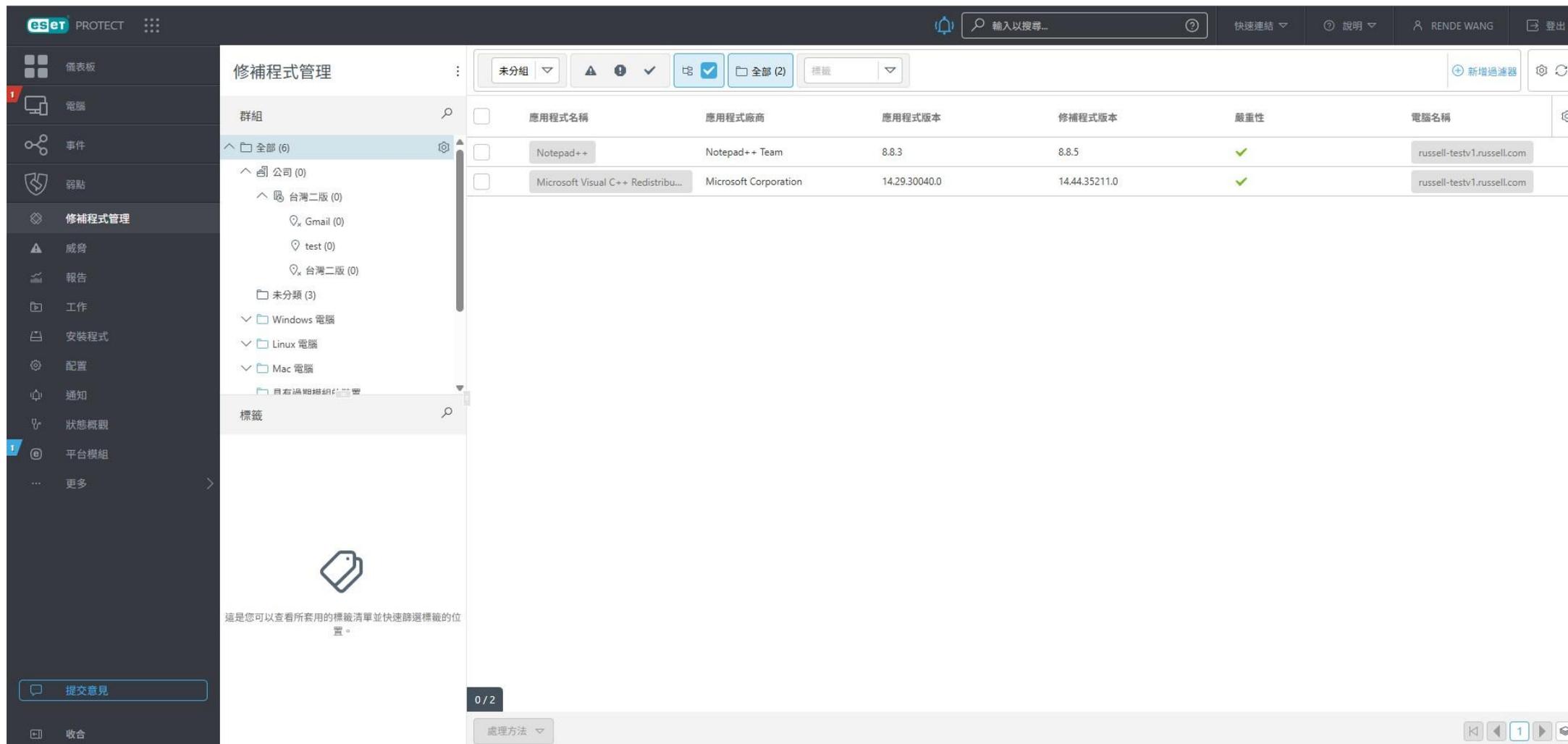
掃描是如何執行？

系統不會主動執行可利用性檢查。**已安裝軟體的版本將會與資料庫中列為易受攻擊的版本進行比較**。

儀錶板



修補程式管理



ESet PROTECT

儀表板
電腦
事件
弱點
修補程式管理
威脅
報告
工作
安裝程式
配置
通知
狀態概觀
平台模組
更多

提交意見
收合

修補程式管理

未分組 [警告] [信息] [勾] [比] [全部 (2)] 標籤

新增過濾器

群組	應用程式名稱	應用程式廠商	應用程式版本	修補程式版本	嚴重性	電腦名稱
全部 (6)	Notepad++	Notepad++ Team	8.8.3	8.8.5	✓	russell-testv1.russell.com
公司 (0)						
台灣二版 (0)						
Gmail (0)						
test (0)						
台灣二版 (0)						
未分類 (3)						
Windows 電腦						
Linux 電腦						
Mac 電腦						
具有過期標記的裝置						
標籤						
	Microsoft Visual C++ Redistribu...	Microsoft Corporation	14.29.30040.0	14.44.35211.0	✓	russell-testv1.russell.com

這是可以查看所套用的標籤清單並快速篩選標籤的位置。

0/2

處理方法

結論

產品背景

秉持著ESET超過30年來的專精技術，成功的為企業打造安全防護網，更同時讓企業兼顧管理成本與系統運作效能。

端點安全的重要性

ESET企業安全解決方案 (ESET Business Security Solutions) 是針對企業複雜網路環境提供最高等級的全面防護規劃。

產品特色

端點偵測與反應系統 (EDR)
端點設備防護
雲端沙箱

ESET PROTECT PROTECT ON-PREM/Cloud Demo



V2



&

A

ESET PROTECT PROTECT ON-PREM/Cloud 相關連結

- ESET PROTECT On-Prem 管理 https://help.eset.com/protect_admin/12.1/zh-TW/changelog.html?index.html
- ESET PROTECT Cloud 管理 https://help.eset.com/protect_cloud/zh-TW/
- ESET Operating systems support charts https://support-eol.eset.com/en/policy_business/os_support_charts.html
- ESET On-premises Consoles https://support-eol.eset.com/en/policy_business/product_tables.html#server
- [KB6864] Deploy the ESET Management Agent using a Group Policy Object (Windows) <https://support.eset.com/en/kb6864-deploy-the-eset-management-agent-using-a-group-policy-object-windows-8x9x>
- ESET Network Status <https://status.eset.com/>
- Windows EOL <https://learn.microsoft.com/zh-tw/lifecycle/products/>
- [KB6864] Deploy the ESET Management Agent using a Group Policy Object (Windows) <https://support.eset.com/en/kb6864-deploy-the-eset-management-agent-using-a-group-policy-object-windows-8x9x>

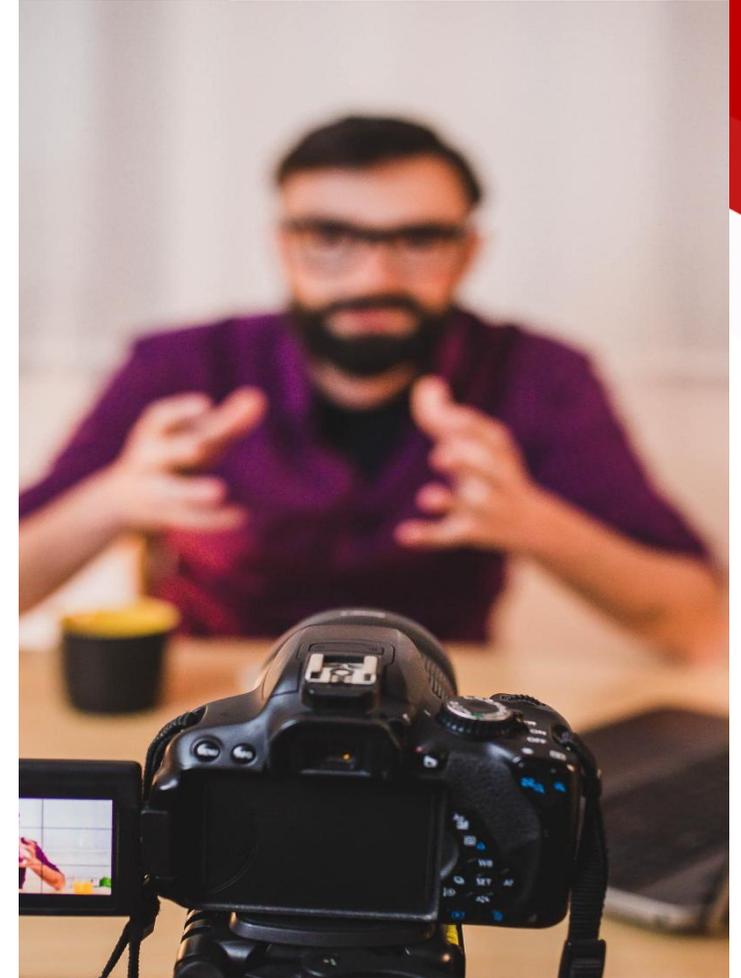


PANDORA**FMS**

PandoraFMS產品介紹

議程內容

- PandoraFMS產品背景
- PandoraFMS主要功能說明



PandoraFMS產品背景

關於PandoraFMS



PandoraFMS ?

我們於2004年以Artica的名義在一間與加州車庫差不多大小的小辦公室創立了公司。最初的專案基於GPL2開源許可證發布，是其執行長兼創始人Sancho Lerena的個人專案。從那時起，它不斷發展，成為一套針對企業的監控套件，超越了國界和語言的界限，提供了市場上最完整的解決方案之一。



Pandora產品

產品簡介

PANDORA FMS

- 一個靈活且適合任何類型組織的監控平台。

PANDORA SIEM

- 將來自不同系統、應用程式和裝置的日誌和事件資料收集、集中並整合到單一平台。資料與 Pandora FMS 代理原生集成，無需額外工具即可擷取關鍵資訊。

PANDORA RMM

- 遠端監控和管理解決方案，用於主動監管設備、網路和應用程式。非常適合尋求自動化、可擴展性和即時控制的託管服務提供者 (MSP) 和 IT 團隊。

PANDORA ITSM

- 為支援和客戶服務團隊提供強大且靈活的幫助台，與資訊技術基礎架構庫 (ITIL) 流程保持一致。

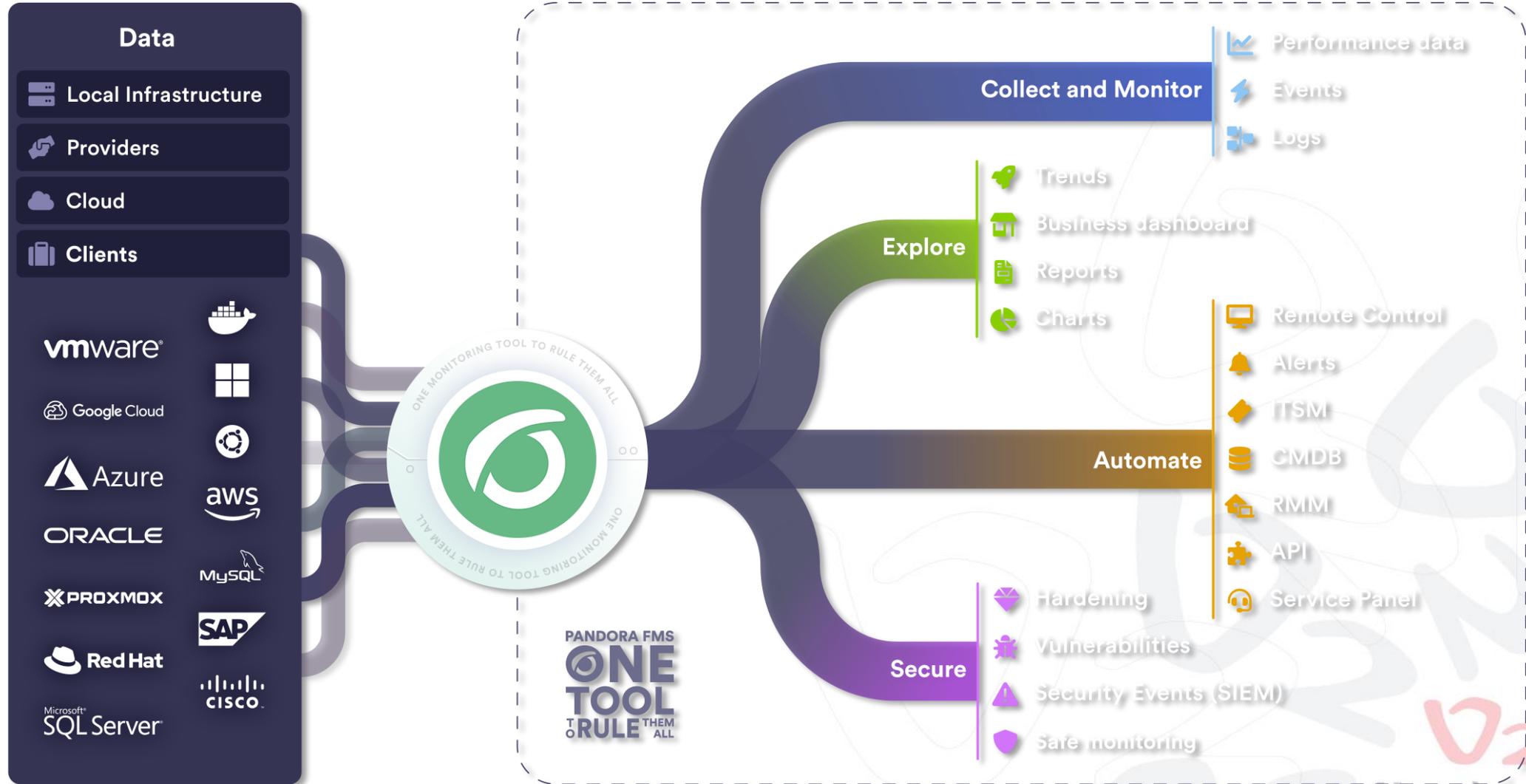
PANDORA RC

- 適用於伺服器以及 Windows、Linux 和 Mac 的遠端控制軟體，適用於系統技術人員和主機服務公司 (MSP)。快速、簡單，無需記憶或安裝任何內容。

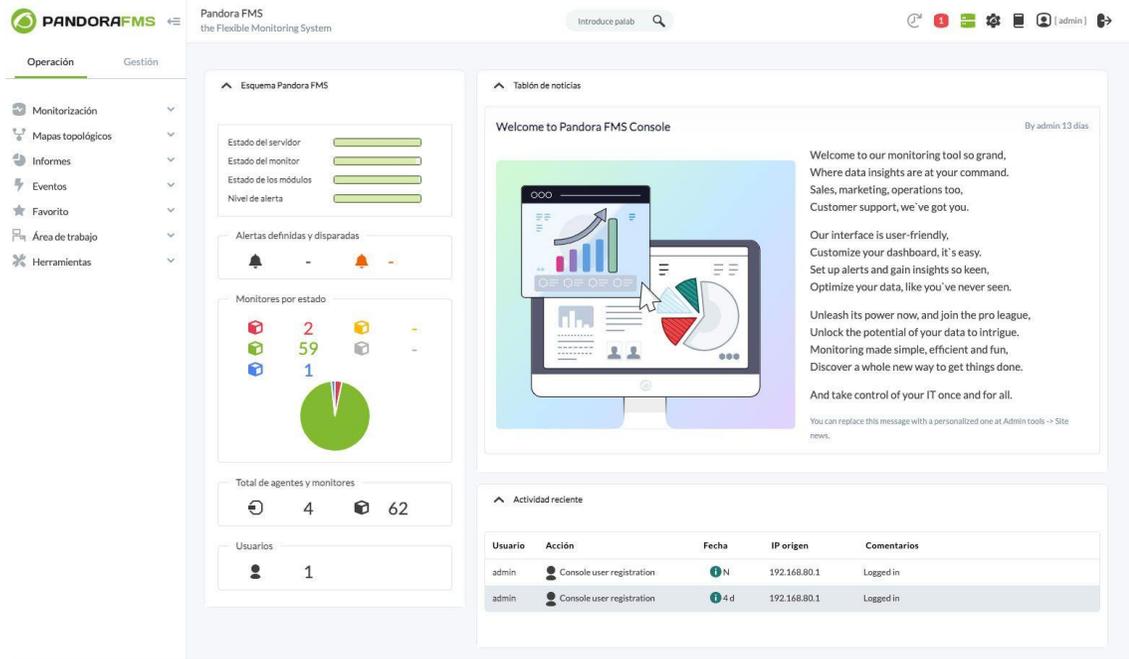
PANDORA MINI

- Pandora MINI 是一個簡化、直接且易於存取的版本，在基本監控任務中具有高效和敏捷性。

功能特色



產品摘要



全面可觀察的監控解決方案

你無法控制你不知道的事。知識涉及識別每個元素、每個部件以及組件之間的每種關係，這通常涉及來自不同部門的數百種技術。

單一工具能否提供完整可見度？

Pandora FMS 用途？

- Pandora FMS 即時顯示您組織的技術進展。產生警報，分析多年趨勢，並與客戶或供應商分享資訊。我們的客戶利用這些資訊節省時間和金錢，更重要的是，幫助他們的IT團隊優化工作。

對於任何類型的組織

- SAP 可以以多種方式使用，就像 Oracle 資料庫或 Amazon 或 Azure 雲端「事物」執行個體一樣。不同之處在於，市場上很少有軟體可以在同一螢幕上向您顯示公司 IT 難題的每個部分的狀態。

如何幫助你？

- 它可以幫助您進行優化。這可以理解為：透過提供可靠的即時訊息，節省技術人員在管理任務上的時間；透過使用相同的軟體完成所有操作，節省許可證成本；透過簡化監督和管理，節省硬體或服務成本；或提升客戶或供應商對您服務品質的認知。但這些還不夠，最重要的是 Pandora FMS 在之前一片混亂和陰影的地方提供了光明、秩序和目的。



授權

軟體即服務

雲端監控即服務的設計目的是讓您不必花時間安裝軟體、維護硬體、作業系統或管理安全性修補程式或更新。您可以享受由我們維護但全天候供您使用的 Pandora FMS 雲端實例。

開源

我們有一個完全免費的版本，遵循開源授權 (GPL2)。您可以無限制地使用它。如果您將來決定使用企業版，您可以自動遷移到開源系統。

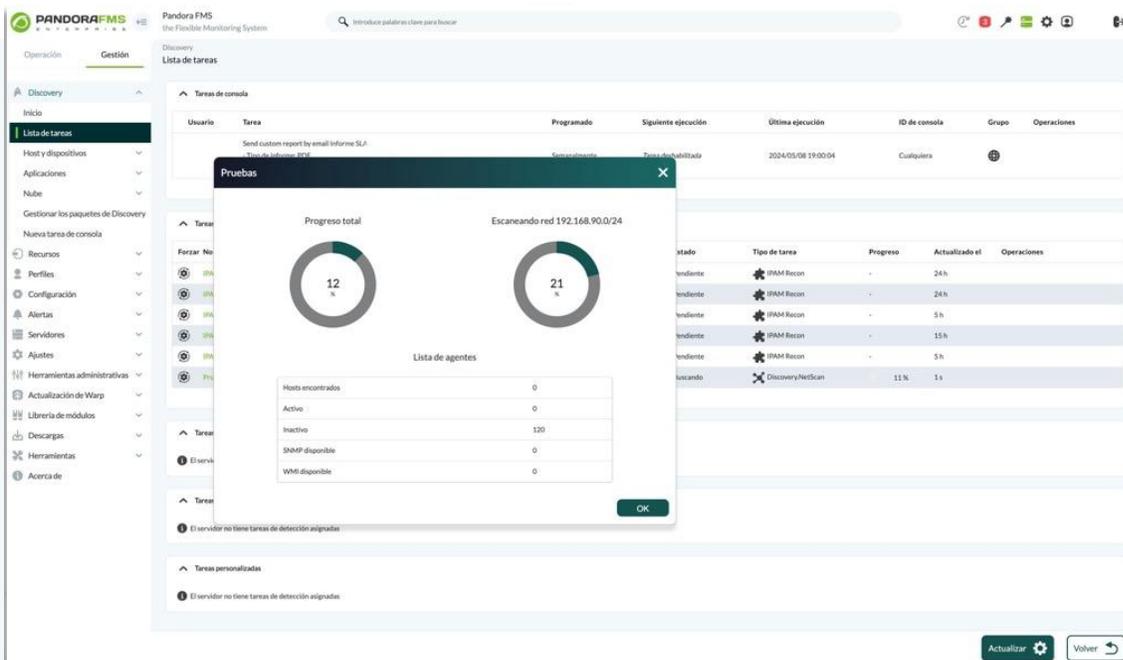
本地部署

傳統軟體許可證，用於在您的電腦上永久（終身）安裝 Pandora FMS。您只需支付一次許可證費用，支援服務為可選，並且每年都需要付費。支援費用為許可證費用的 30%，且不限次數。也就是說，您可以進行所有必要的諮詢，存取所有更新和產品改進，並無限制地存取插件和整合庫。此外，您還可以透過我們的線上學習系統免費獲得培訓。

監控

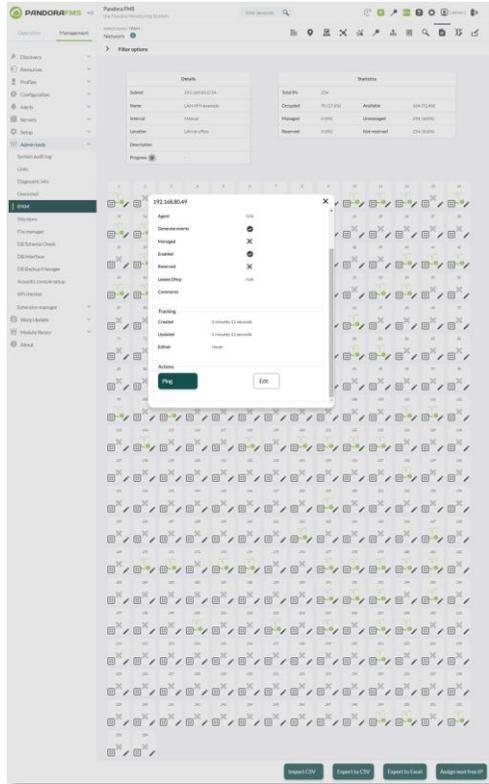


- Pandora FMS 讓您發現所有網路設備，並透過連接介面的地圖呈現其拓撲結構，詳細顯示網路結構。更進一步，統一設備管理，實現全面的網路可觀察性。

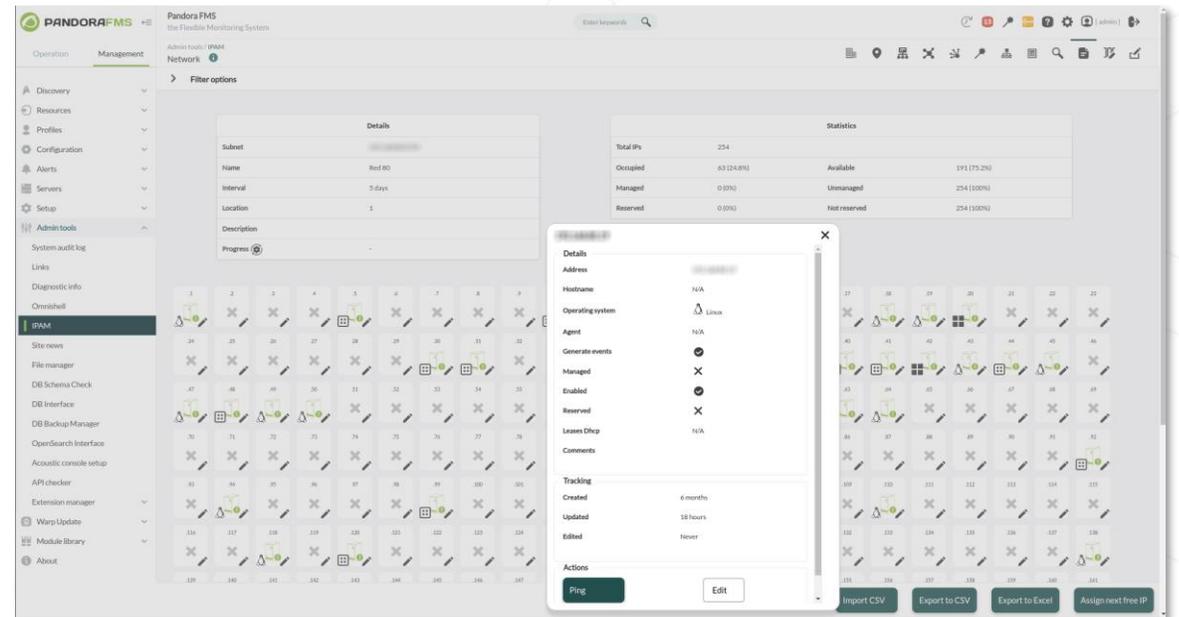


- 具有鏈路級動態拓撲的網路地圖。SNMP v1、v2 和 v3。動態網路介面偵測、陷阱管理和分散式自動發現。

監控(續)

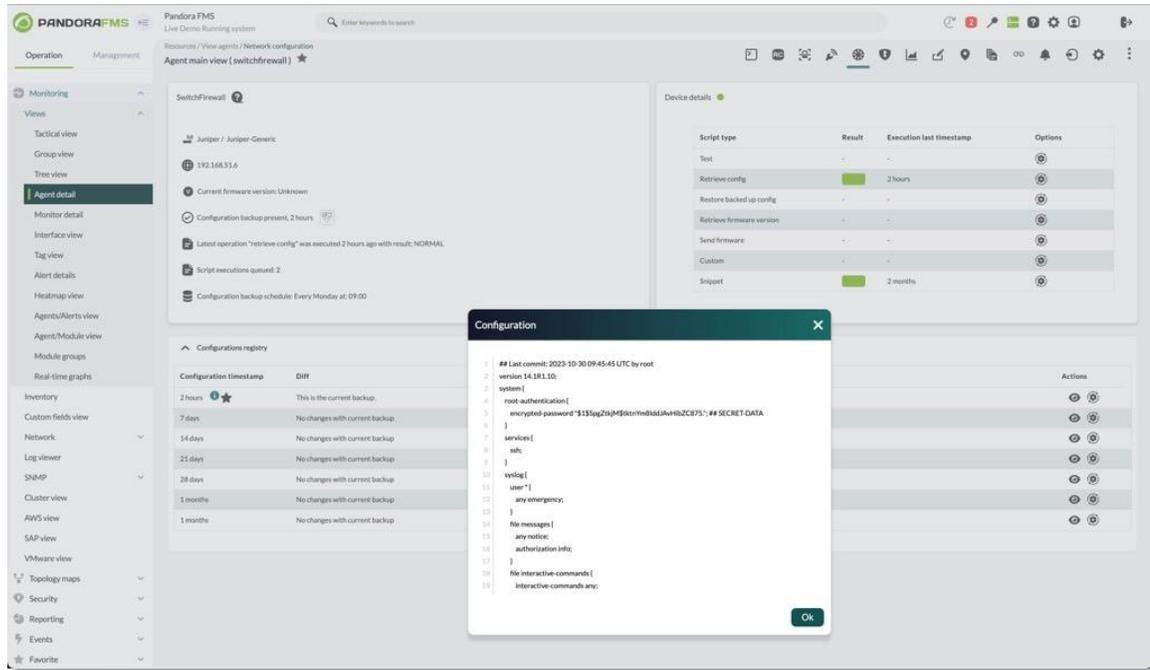


- 管理網路和超級網路。實體位置、IP預留和各種使用地圖。可用IP位址耗盡時發出警報。可與外部DHCP伺服器整合。



- 取得網路設備 (路由器、交換器、防火牆) 的即時統計資料並提供使用情況報告、瓶頸或診斷問題。

監控(續)



- 大規模更新韌體，一鍵分發配置變更並進行配置備份。檢測設備中的配置變更並恢復上次已知配置。

企業版專屬

PANDORA FMS 功能

我們的一體化軟體可以幫助您在任何 IT 環境中快速解決問題！

伺服器監控

Pandora FMS 涵蓋硬體和用戶應用程式。我們的多租戶指揮中心可以同時整合部門、IT 系統和位置。

[閱讀更多 →](#)

日誌監控

使用相同的許可證，輕鬆收集您已監控的任何電腦中的 Windows 日誌和事件。無需任何其他程序。

[閱讀更多 →](#)

使用者體驗監控

您將能夠以非常簡單且用戶友好的方式在客戶的應用程式上執行與任何其他用戶相同的操作，並檢查它是否按預期工作。

[閱讀更多 →](#)

網路監控

發現所有網路設備並透過連接介面的地圖表示其拓撲並詳細顯示網路結構。

[閱讀更多 →](#)

安全監控

透過細緻的稽核和安全措施以及超過 1,500 種不同的安全關鍵檢查，確保為您的系統提供最大程度的保護。

[閱讀更多 →](#)

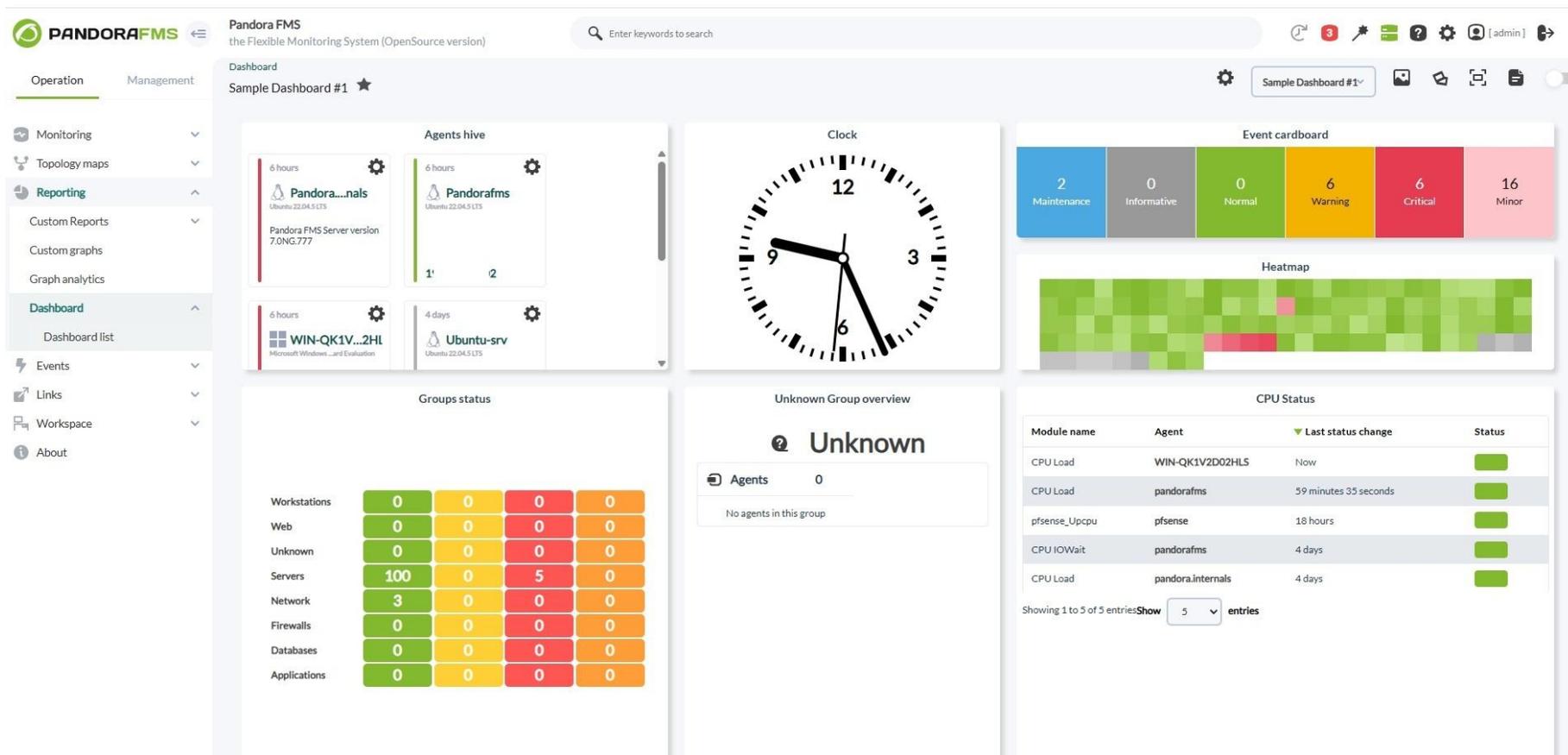
雲端監控

密切注意您的基礎架構，無論是本地部署、虛擬化、混合部署或雲端部署。降低風險，確保無縫營運。

[閱讀更多 →](#)

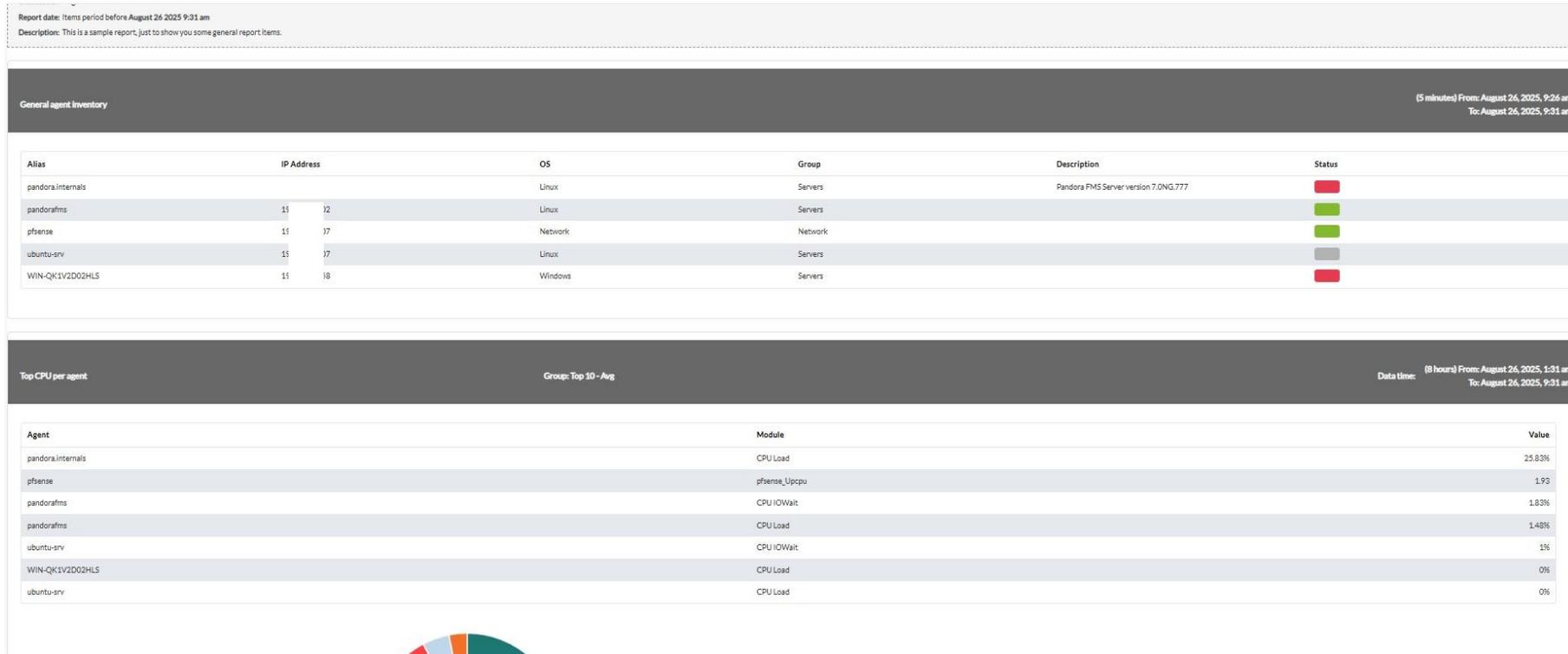
- 雲端和虛擬監控
- 日誌監督
- 使用者體驗監控
- 硬體和軟體監控
- 應用程式監控
- 系統清單
- 業務流程監控

儀錶板



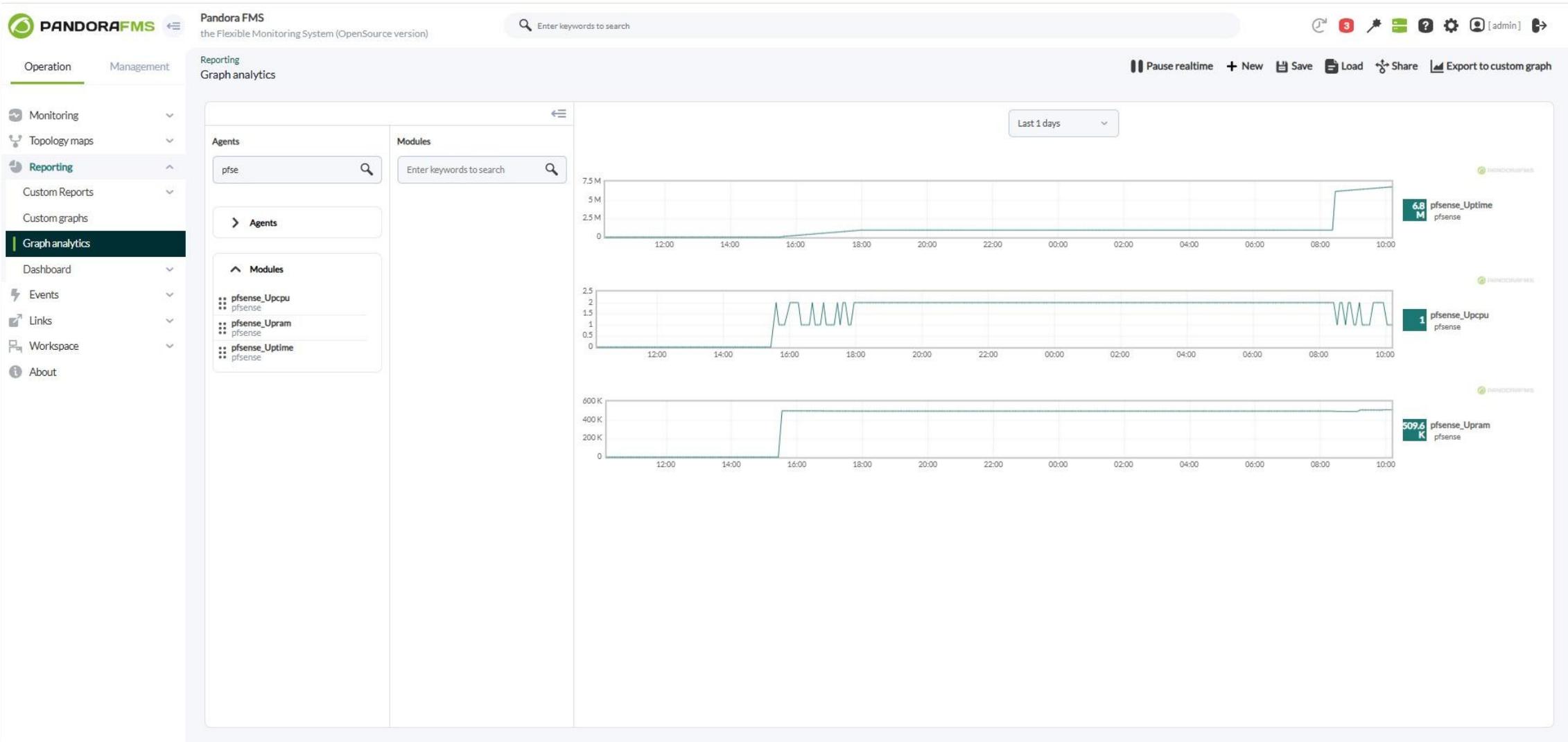
- 每個用戶都可以建立自己的儀錶板，突出顯示與其團隊及其營運最相關的關鍵指標。讓所有成員都能了解系統的性能等級。

報表

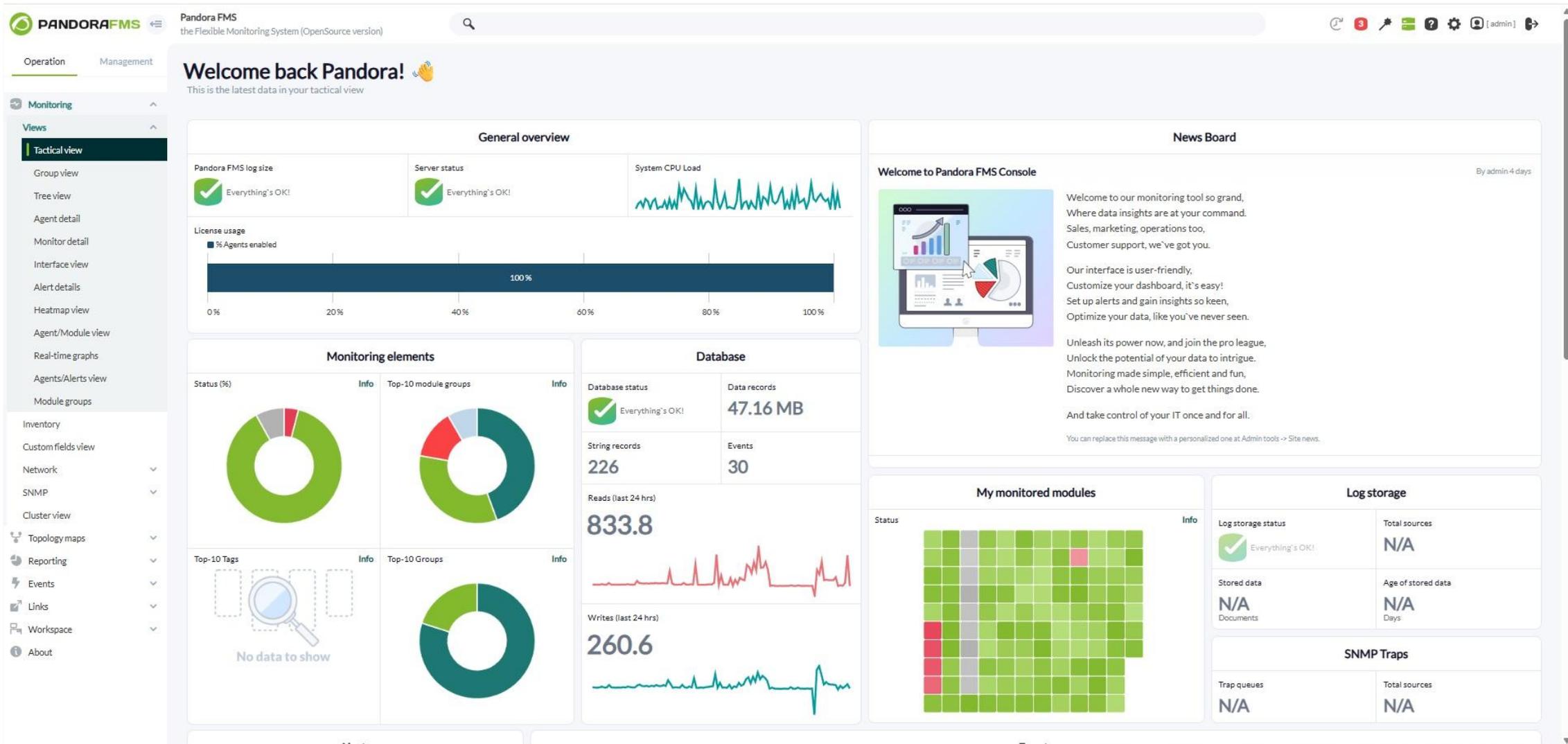


- 報告產生器可讓您設計自己的報告，並自訂封面、標題和不同的內容。自訂佈局類似於儀表板，可以定義即時數據和多年歷史數據。系統提供預先定義的報告，包括可用性計算、Top-N、SLA（每月、每週或每日）、直方圖、圖形、容量規劃報告、報告事件、庫存、配置等。

報表



監控-戰術



監控-群組

PANDORA FMS the Flexible Monitoring System (OpenSource version) [admin]

Operation Management Monitoring / Views Group view

Monitoring Views Tactical view Group view Tree view Agent detail Monitor detail Interface view Alert details Heatmap view Agent/Module view Real-time graphs Agents/Alerts view Module groups Inventory Custom fields view Network SNMP Cluster view Topology maps Reporting Events Links Workspace About

Summary of the status groups

Agents: 40% 0% 40% 20% 0%

Modules: 4.27% 0% 88.03% 7.69% 0%

Total items: 2

Force Group/Tags	Agents					Modules						
	Total	Unknown	Not initialised	Normal	Warning	Critical	Unknown	Not initialised	Normal	Warning	Critical	Alert triggered
All	5	1		2		2	9		103		5	
Network	1			1					3			
Servers	4	1		1		2	9		100		5	

監控-樹狀

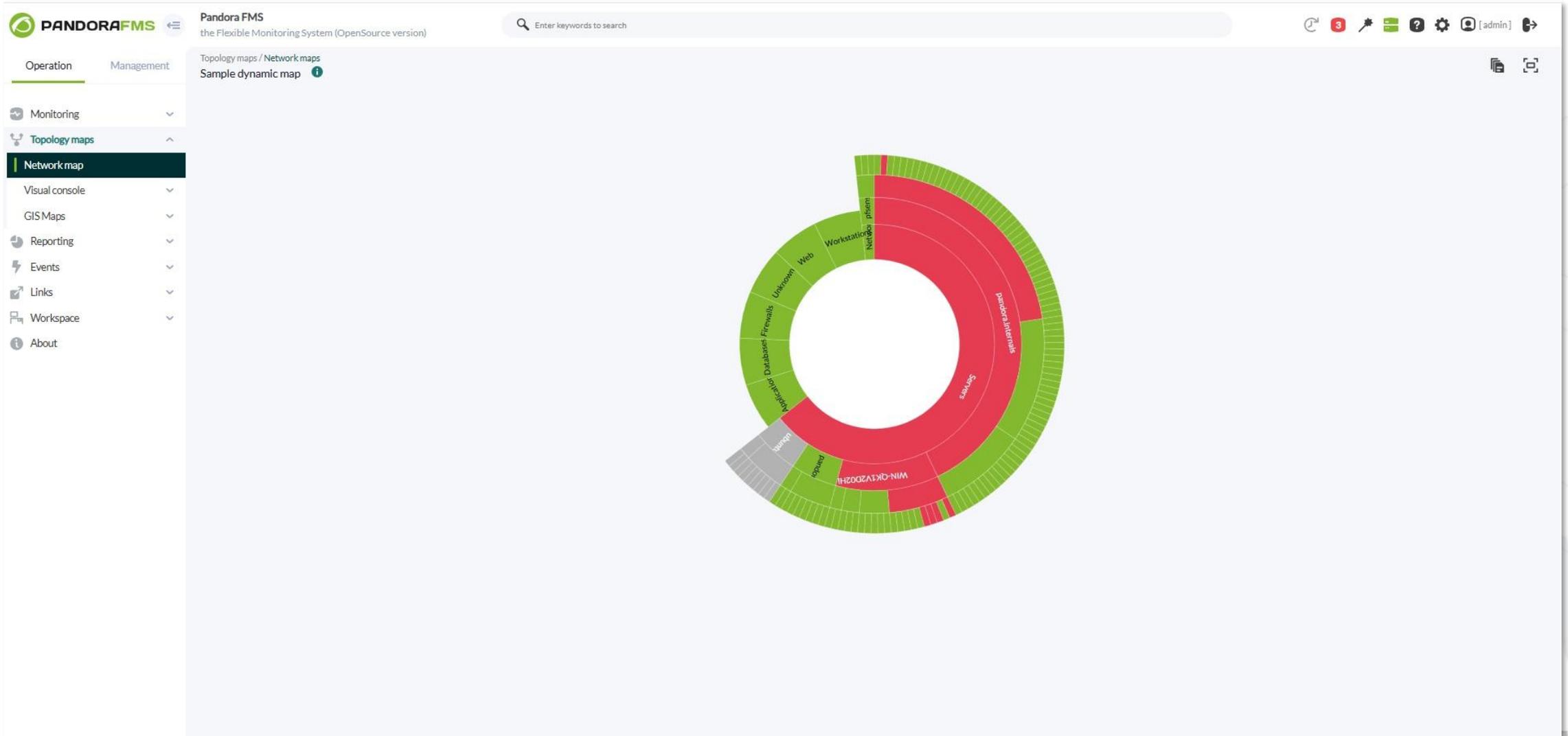
The screenshot displays the Pandora FMS web interface. The top navigation bar includes the Pandora FMS logo, the text "Pandora FMS the Flexible Monitoring System (OpenSource version)", a search bar, and user information "[admin]". The left sidebar contains navigation menus for "Monitoring" and "Views". The main content area shows a "Tree view" of agents, with a search bar at the top. The tree is expanded to show two main groups: "Network" and "Servers".

Tree search

Groups found: 2

- Network** [1:1]
 - pfsense** [3:3]
 - pfsense_Upcpu 2 123
 - pfsense_Upram 507,252 123
 - pfsense_Uptime 6,610,517 123
 - Servers** [4:2:1:1]
 - pandora.internals [76:1:75]
 - pandorafms [9:9]
 - ubuntu-srv [9:9]
 - WIN-QK1V2D02HLS** [20:4:16]
 - All users enforced password 0 123
 - Check logon event audited 1 123
 - CPU Load 6 % 123
 - DiskUsed_C: 85.1 % 123
 - Firewall profile: Domain status 0 123
 - Firewall profile: Private status 0 123
 - Firewall profile: Public status 0 123
 - Hardening - Failed checks 38 123
 - Hardening - Not applied checks 431 123
 - Hardening - Passed checks 38 123
 - Hardening - Score 50 123
 - Lockscreen status 1 123
 - Memory_Used 55 % 123

MAP-網路



MAP-地理



Pandora FMS
the Flexible Monitoring System (OpenSource version)

Enter keywords to search

[admin]

Operation Management

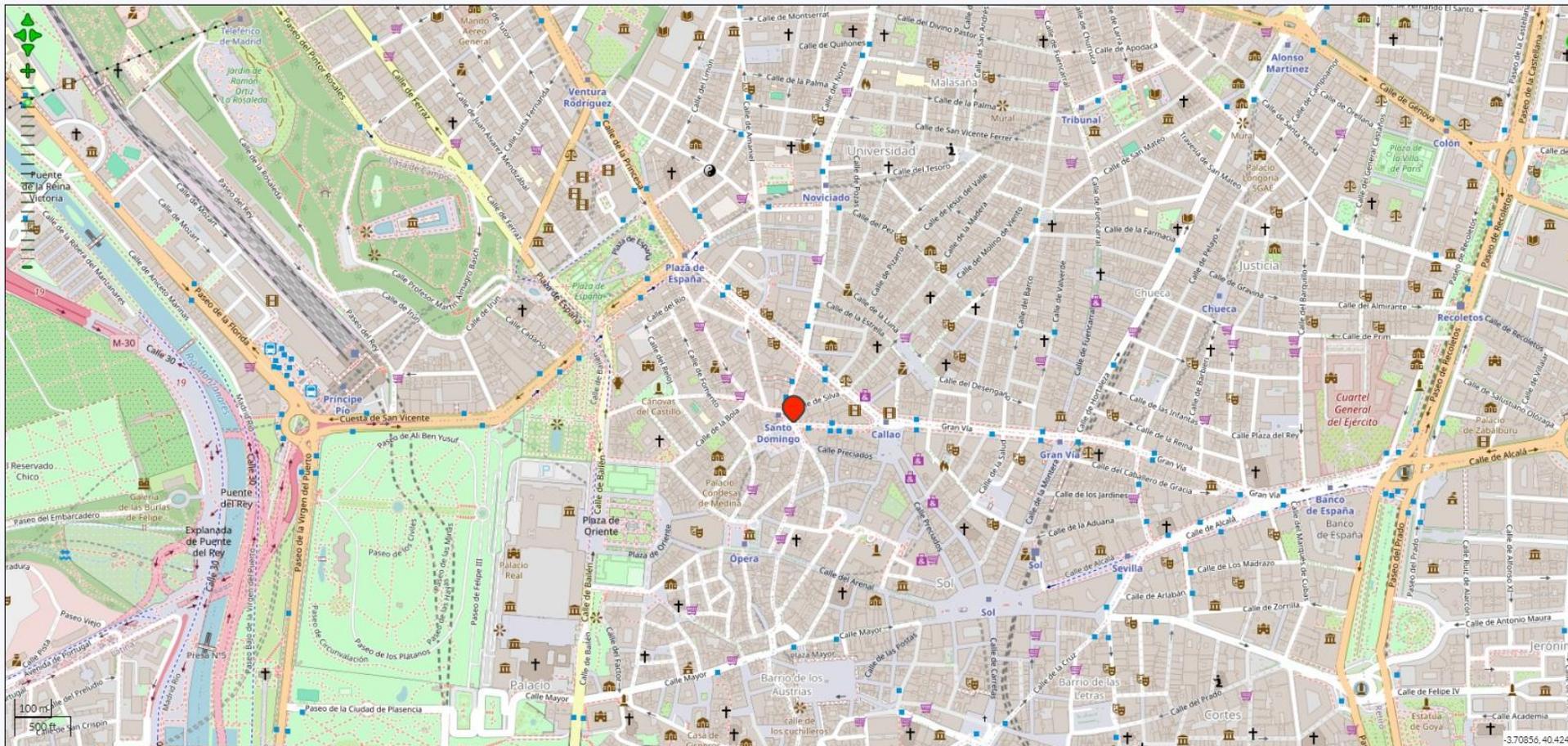
Topology maps / GIS Maps

Filter by status: None

Refresh: 1 minute

Map: Sample

- Monitoring
- Topology maps
- Network map
- Visual console
- GIS Maps
 - List of GIS maps
 - Sample
- Reporting
- Events
- Links
- Workspace
- About



事件



Pandora FMS
the Flexible Monitoring System (OpenSource version)

Enter keywords to search

[admin]

Operation Management

- Monitoring
- Topology maps
- Reporting
- Events
- View events**
- Acoustic console
- Links
- Workspace
- About

Events
Events list

Filters

Show graph



Current filter

Not set.

Event status

Not validated.

Max. hours old

Last 8 hours.

Duplicated

Group events



Event name	Status	Agent name	Timestamp	Options
Module 'Service W3SVC - Status' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'Lockscreen status' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'Firewall profile: Privat...status' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'Firewall profile: Public status' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'All users enforced password' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'Check logon event audited' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'CPU Load' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'TCP_Connections' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'DiskUsed_C:' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'Memory_Used' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'Network_Usage_Bytes' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'Service Dnscache - Status' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'Service IISADMIN - Status' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'Service MSSQL\$ERASQL - Status' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'Service MySQL80 - Status' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Module 'Firewall profile: Domain status' is going to UNKNOWN	★	WIN-QK1V2D02HLS	1 hours	<input type="checkbox"/>
Warmup mode for unknown modules ended.	★		1 hours	<input type="checkbox"/>
pandorafms inventoryserver going UP	★		2 hours	<input type="checkbox"/>

Previous 1 2 Next Show 20 entries

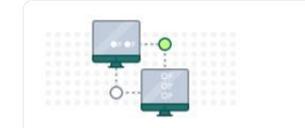
Sound events

In progress selected

Execute event response

模組庫

按類別發現

 <p>雜項 其他類型的模組，如網站監控、桌面應用程式等。</p>	 <p>應用程式監控 用於監控應用程式的模組。</p>	 <p>網路監控 網路監控模組。</p>
 <p>作業系統 適用於所有類型作業系統的監控模組。</p>	 <p>藝術品 控制台背景和圖示、狀態和其他圖形的新圖示。</p>	 <p>安全監控 保護您與 Pandora FMS 的連線。</p>
 <p>工具 Pandora FMS 的工具，未歸入其他類別。</p>	 <p>存貨 清點模組，無論本地或遠端。</p>	 <p>系統整合 將 Pandora FMS 與其他系統和服務整合。</p>

這是一個為 Pandora FMS 使用者（包括公共開源使用者和企業使用者）提供的包含 **700** 多個模組、文件和工具的函式庫。

Search any technology

AIX tag	apc	aws	Azure	Cisco tag	cloud	color	database
Databases tag	discovery	enterprise	hp	hp ux	ibm	Inventory	juniper
laserjet	Linux tag	memory	modules	MSSQL	mysql	network	
Oracle tag	plugin	policy	politica	postgreSQL	printer	procesos	
remote	resources	router	samsung	server	SNMP tag	Solaris tag	SQL
storage	switch	unix	unix resources	UPS tag	vmware	windows	

模組庫(續)

The screenshot displays the Pandora Module Library website. At the top, the Pandora logo and navigation menu are visible. The main content area lists several modules, each with a title, date, category, and description. A red callout box highlights the 'Enterprise' (E) icon next to the 'Azure Discovery' module, with the text 'Only enterprise users can view the download links.' The right sidebar contains a search bar, a 'Discover by category' dropdown, a 'Tags' section with various filter buttons, and a 'Most downloaded' section.

PANDORA
Module library

Product Solutions Resources Support Prices Community My plugins Register Login

Azure Discovery E
Nov 30, 2023 | Application monitoring, Cloud, Enterprise
AZURE With this Plug-in you can monitor instances and zones of an Azure environment, through the PandoraFMS "Discovery" functionality. AZURE CLOUD Ver. 5-10-2023 With this Plug-in you can monitor instances and zones of an Azure environment, through the PandoraFMS...

Pandora Azure Event Hubs E
Sep 30, 2022 | Application monitoring, Enterprise
Ver. 23-08-2022 Plugin to monitor an azure Event Hubs namespace. Type: Server plug-in Modules created by the plugin SuccessfulRequests ServerErrors UserErrors QuotaExceededErrors ThrottledRequests IncomingRequests IncomingMessages IncomingBytes OutgoingBytes...

Pandora Azure PostgreSQL E
Sep 30, 2022 | Databases category, Enterprise
Ver. 23-08-2022 Plugin with which to monitor an azure postgresql data server. Type: Server plug-in Modules generated by the plugin cpu_percent memory_percent io_consumption_percent storage_percent storage_used storage_limit serverlog_storage_percent...

Pandora Azure SQL E
Jun 23, 2022 | Databases category, Enterprise
Ver. 11-05-2022 With this plugin you can get performance and connectivity data from an Azure SQL database such as cpu used, failed or successful connections or firewall blockages. Type: Server plug-in Modules created by the plugin allocated_data_storage app_cpu_billed...

Search

Discover by category
Select Category

Tags
AIX tag apc aws Azure
Cisco tag cloud color
database Databases tag
discovery enterprise hp
hp ux ibm Inventory juniper
laserjet Linux tag memory
modules MSSQL mysql
network Oracle tag plugin
policy politica postgresSQL
printer procesos remote
resources router samsung
server SNMP tag Solaris tag
SQL storage switch unix
unix resources UPS tag
vmware windows

Most downloaded
ARP Table (Windows, Local)
(6,550)



模組庫(續)

PANDORAFMS the Flexible Monitoring System (OpenSource version)

Resources / View agents / Main
Agent main view (win-qk1v2d02hls)

WIN-QK1V2D02HLS

Microsoft Windows Server
OS Version 2019 Standard Evaluation
IP address 1 8
Agent version 7.0NG.777.11 Build 250804
Description N/A

Events (Last 24h)

Agent contact

Interval 5 minutes
Last contact / Remote 22 hours / August 26, 2025, 5:40 pm
Next contact Out of bounds
Group Servers
Last status change 1 hours
Remote configuration Enabled

List of modules 4 16

Status: All Free text for search (*) Module group: All Show in hierarchy mode:

T	Module name	Description	Status	Thresholds	Data	Last contact	Graphs	Actions
	Service Dnscache - Status			N/A - N/A	1	16 hours		
	Service IISADMIN - Status			N/A - N/A	1	16 hours		
	Service MSSQLSERVERSQL - Status			N/A - N/A	1	16 hours		
	Service MySQL80 - Status			N/A - N/A	1	16 hours		
	Service WSSVC - Status			N/A - N/A	1	16 hours		
Networking								
	Network_Usage_Bytes	Total bytes/sec transferred in this system		N/A - N/A	1,781.9 bytes/sec	16 hours		
	TCP_Connections	Total number of TCP connections active		N/A - N/A	220	16 hours		
Security								
	All users enforced password	Check if all users has enforced password, not secure users ...		N/A - N/A	0	16 hours		
	Check logon event audited	Check if the logon events audit log is enabled, status: Logo...		N/A - N/A	1	16 hours		
	Firewall profile: Domain status	Check if firewall profile Domain is enabled		N/A - N/A	0	16 hours		
	Firewall profile: Private status	Check if firewall profile Private is enabled		N/A - N/A	0	16 hours		
	Firewall profile: Public status	Check if firewall profile Public is enabled		N/A - N/A	0	16 hours		
	Hardening - Failed checks	Number of failed checks across policies.		N/A - N/A	38	5 days		

案例

主要需求

Toshiba在西班牙為餐飲客戶提供IT支援，而自助服務機器分散不同地點，無法持續有人監控。所以發生故障，則無法立即修復。因此，Toshiba需要一套隨時掌握多家門市設備狀態的監控系統。

為什麼選擇PandoraFMS?

- ✓ 靈活性和高度可擴展性
- ✓ 售後服務
- ✓ 整合優勢



270 + 16.800 + 750 + 10

PREMISES MONITORED

MODULES

MONITORED ELEMENTS

CUSTOM PLUGINS

PandoraFMS

Pandora FMS (Flexible Monitoring System) 是一款功能強大的 IT 監控解決方案，能夠，

- 監控伺服器
- 網路設備
- 應用程式
- 雲端服務

確保系統穩定運行。透過可視化儀表板，使用者可監測，

- CPU 負載
- 記憶體使用率
- 磁碟空間等指標

並透過即時告警機制迅速應對問題。

它支援 API 與腳本自動化管理，並能與 Elasticsearch、Grafana 等工具整合。Pandora FMS 提供免費的社群版與具備進階功能的企業版，適用於不同規模的企業，幫助 IT 團隊提升運維效率並降低風險。



&

A