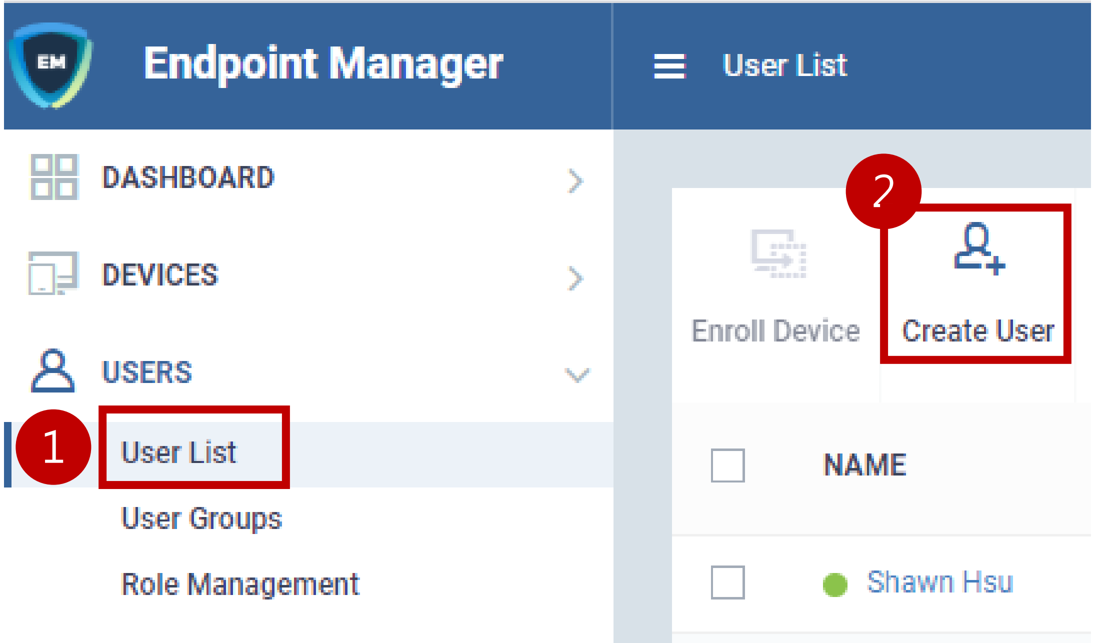
EM中央管理介面說明書

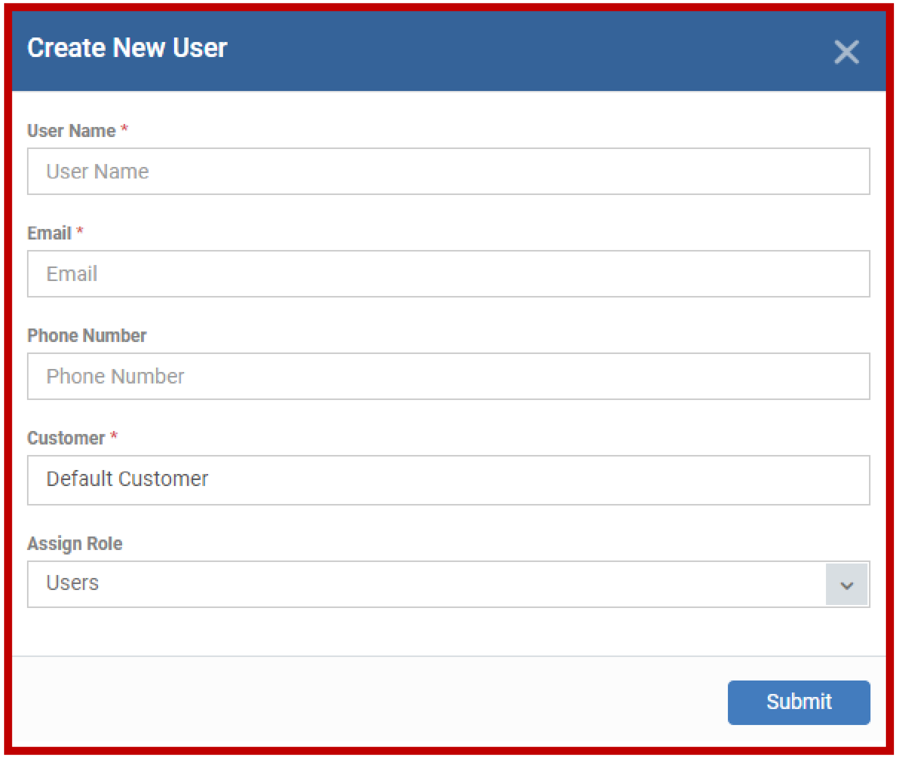
COMODO

Creating Trust Online™

創建新角色



3



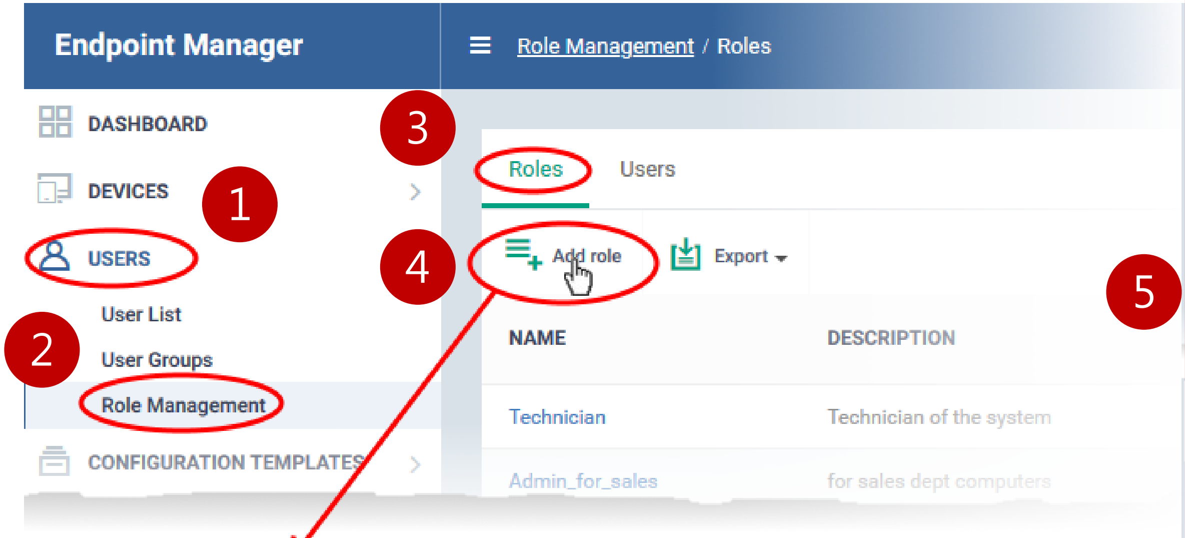
Create New User

User Name *	User Name
Email *	Email
Phone Number	Phone Number
Customer *	Default Customer
Assign Role	Users

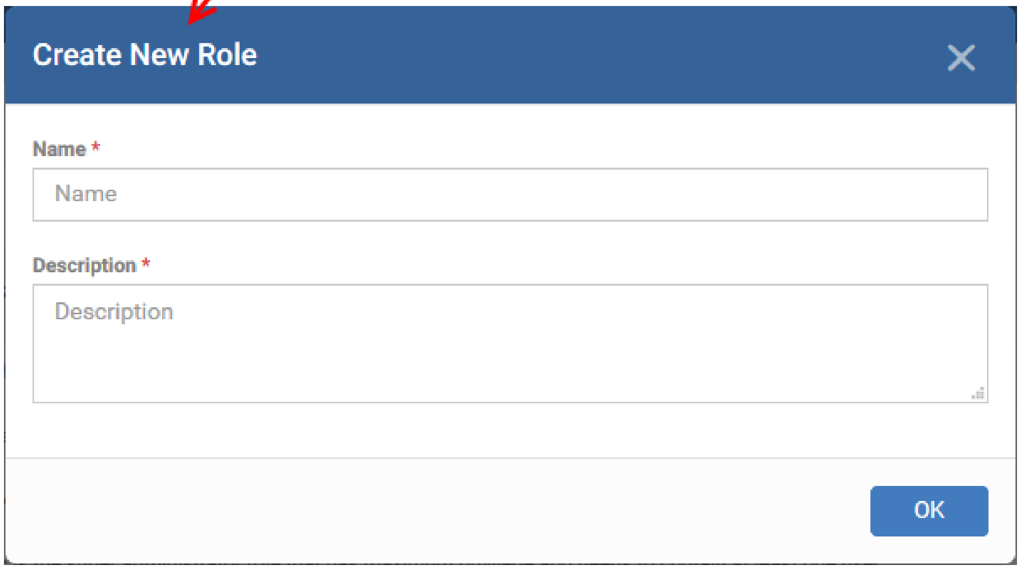
填寫註冊資料

更改角色權限

COMODO
Creating Trust Online™

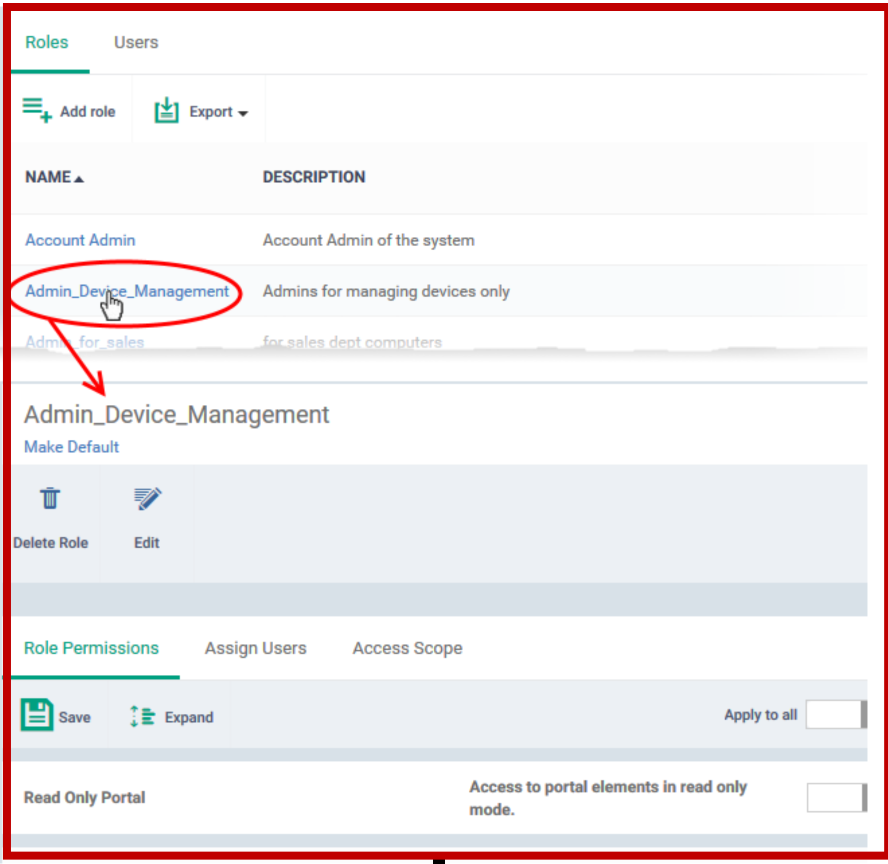


NAME	DESCRIPTION
Technician	Technician of the system
Admin_for_sales	for sales dept computers



Name *
Name

Description *
Description



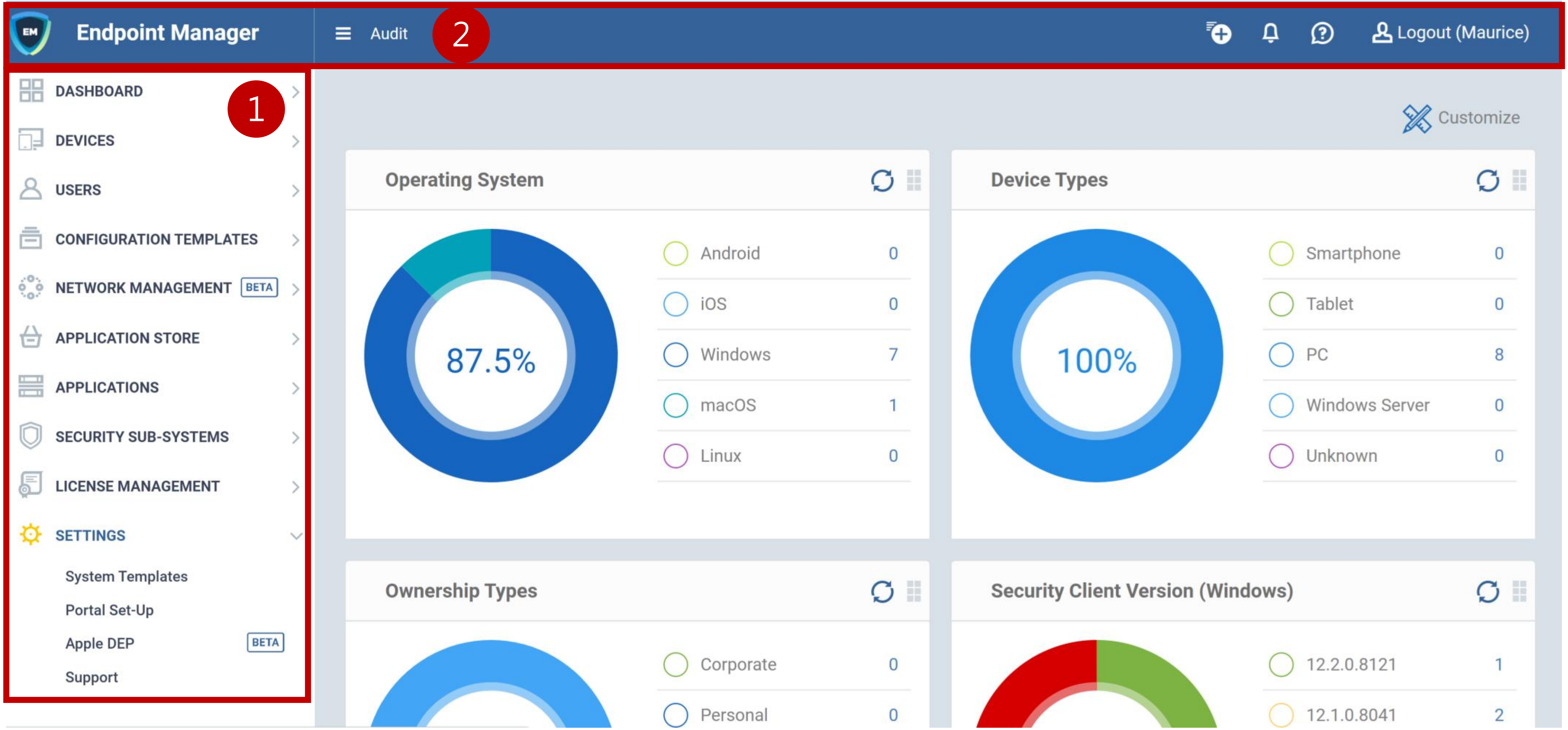
NAME ▲	DESCRIPTION
Account Admin	Account Admin of the system
Admin_Device_Management	Admins for managing devices only
Admin_for_sales	for sales dept computers

Admin_Device_Management
Make Default

Read Only Portal	Access to portal elements in read only mode.

單擊新角色以編輯其權限

中央管理界面主要功能選項



Operating System

87.5%

Android	0
iOS	0
Windows	7
macOS	1
Linux	0

Device Types

100%

Smartphone	0
Tablet	0
PC	8
Windows Server	0
Unknown	0

Ownership Types

Corporate	0
Personal	0

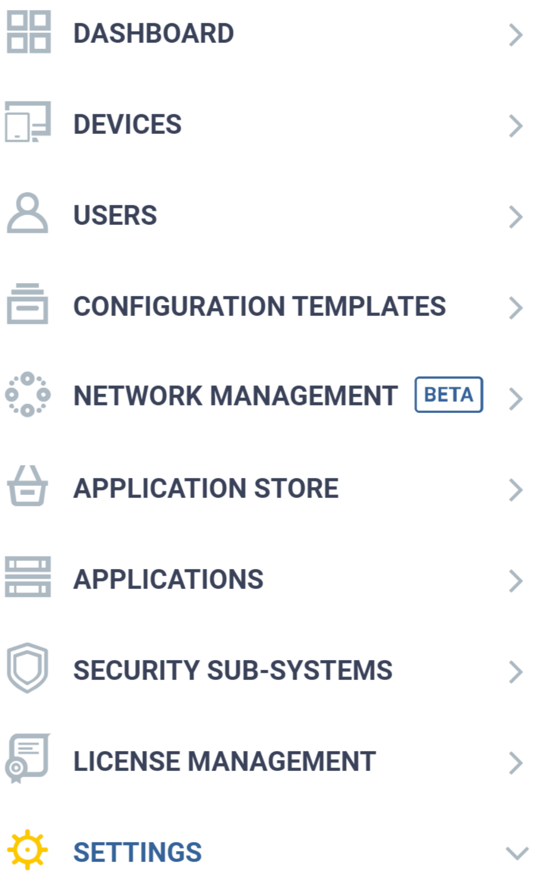
Security Client Version (Windows)

12.2.0.8121	1
12.1.0.8041	2

1 功能選單　2 EM通知選單

功能選單介紹

1 功能選單



儀表板 -包含圖表和圖形，顯示網絡中設備的結構和安全狀態。

設備 -管理和控制已註冊的設備

用戶 -創建和管理用戶和用戶組，註冊他們的設備並將配置配置文件分配給設備。

配置模板 -配置文件控制設備的網絡訪問權限，掃描計劃和其他系統設置。

網絡管理 -在您的網絡上運行設備發現掃描。

應用程序商店 -可以直接從EM推送到iOS / Android / Windows設備的應用程序庫。

應用程序 -查看和管理安裝在Android，iOS和Windows設備上的應用程序。

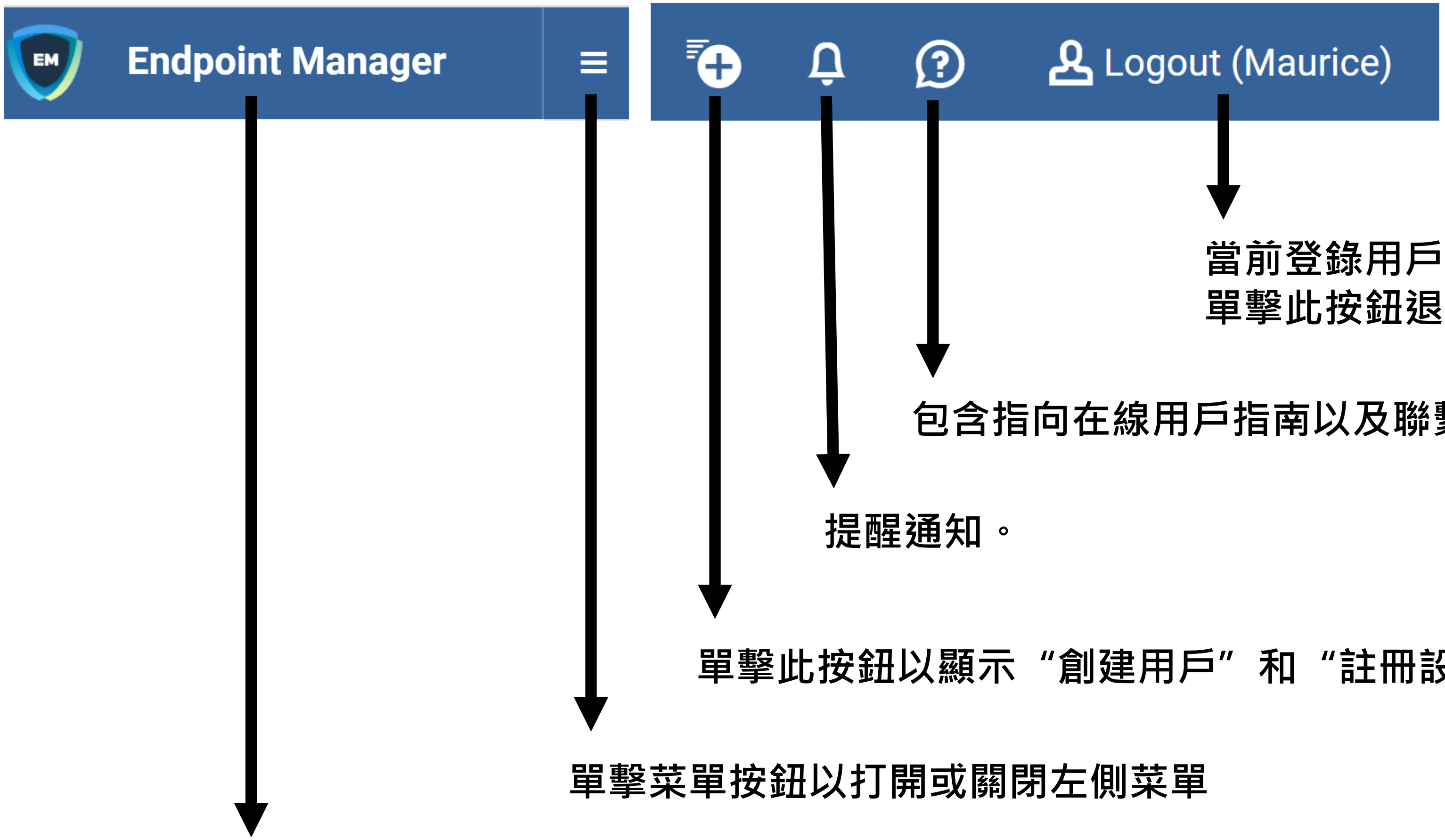
安全子系統 -運行AV掃描和數據庫更新。查看和管理惡意軟件，隔離項目和包含的應用程序

許可證管理 –管理您的訂閱。

設置 -配置電子郵件通知，活動目錄和Apple Push Notification（APN）證書等等。

EM通知選單介紹

2 EM通知



當前登錄用戶的用戶名。
單擊此按鈕退出EM控制台

包含指向在線用戶指南以及聯繫支持團隊的快捷方式。

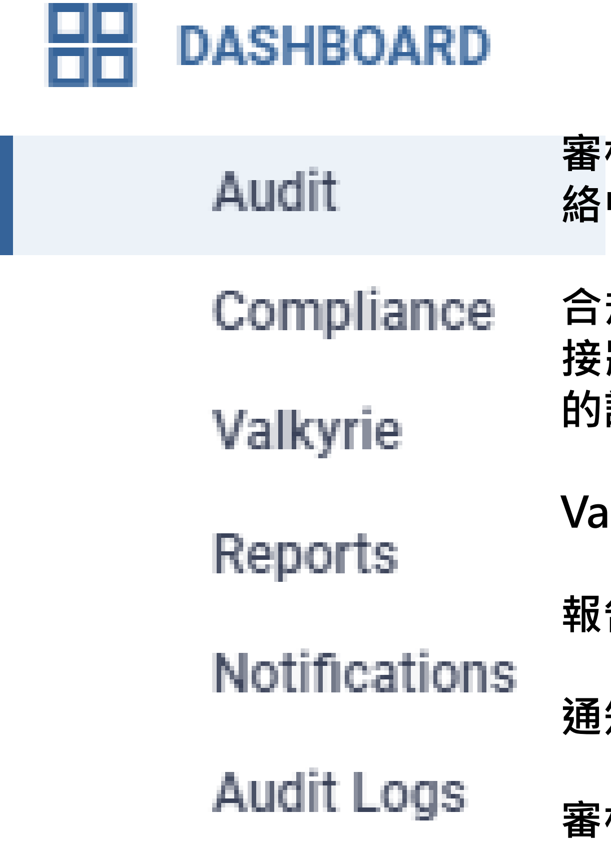
提醒通知。

單擊此按鈕以顯示“創建用戶”和“註冊設備”下拉菜單。

單擊菜單按鈕以打開或關閉左側菜單

單擊徽標以打開“歡迎”屏幕。

儀表板選單介紹



審核 -顯示您網絡上設備上安裝的操作系統和客戶端版本的圖表。還包含顯示網絡中設備類型以及設備是個人設備還是公司設備的圖表。

合規性 -統計信息，詳細說明您的設備與EM安全策略的合規性。例如，設備連接狀態，帶有病毒的設備，具有列入黑名單的應用程序的設備，已root和越獄的設備以及設備掃描狀態。

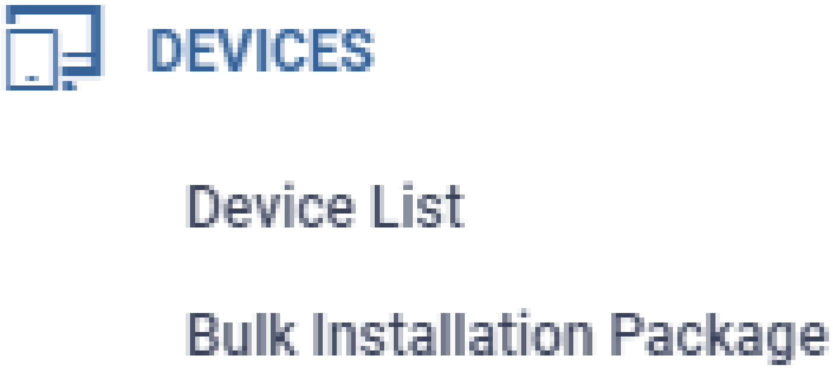
Valkyrie-對提交給Valkyrie文件分析系統的未知文件的判決摘要。

報告 -Endpoint Manager生成的所有報告的列表。

通知 -EM發送給管理員的通知列表。

審核日誌 -顯示管理員和工作人員在託管設備上執行的操作的列表。

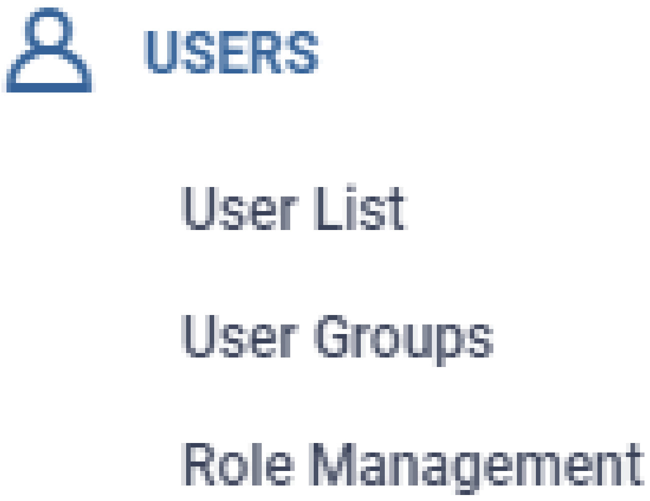
設備選單介紹



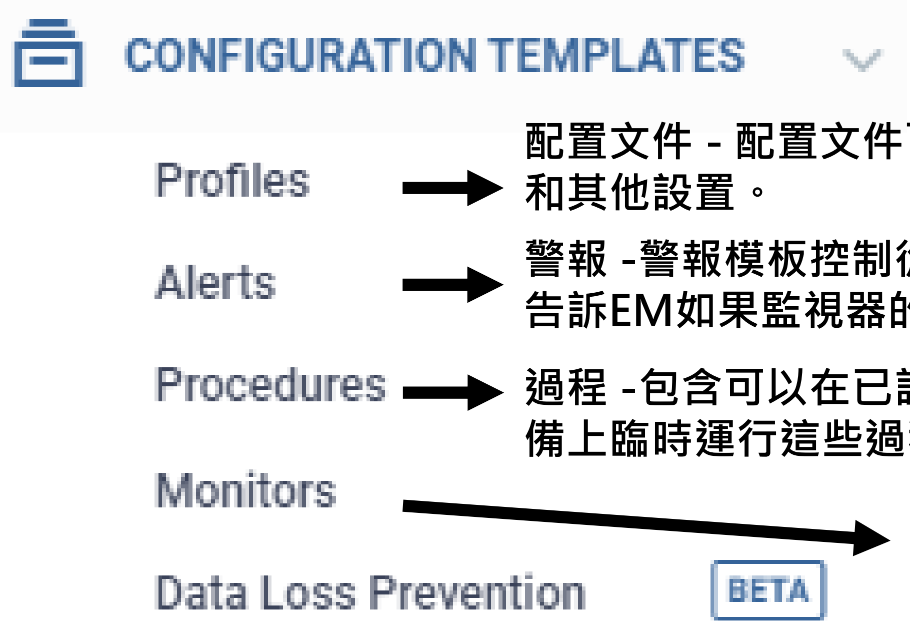
組管理 -創建新的設備組，查看和管理現有組的成員資格，將配置文件應用於組等等。您可以從中間列的列表中選擇要管理的組。

批量安裝軟件包 -下載從Active Directory手動註冊設備所需的通信客戶端軟件包。您還可以下載“遠程控制”工具，該工具可讓您與遠程Windows和Mac OS端點進行交互。

用戶選單介紹



配置模板選單介紹



CONFIGURATION TEMPLATES

- Profiles → 配置文件 - 配置文件可讓您定義設備的安全策略，網絡訪問權限，防病毒掃描計劃和其他設置。

- Alerts → 警報 -警報模板控制從過程/監視器收到警報時會發生什麼。例如，警報模板可以告訴EM如果監視器的條件得到滿足，則向您發送通知。

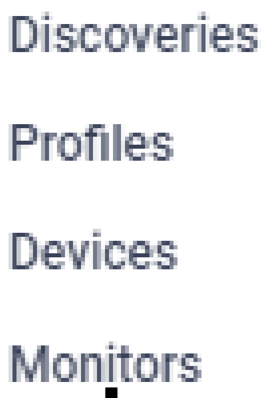
- Procedures → 過程 -包含可以在已註冊設備上執行的預定義和自定義過程的列表。可以在選定設備上臨時運行這些過程，也可以在配置文件中安排這些過程以設置的間隔運行。

- Monitors → 監視器 -監視器是一種腳本，用於跟踪網絡上的事件並在滿足其條件時採取特定的措施。例如，“當將USB可移動磁盤連接到系統時提醒我”，或“如果CPU使用率在一定時間內超過75%，則創建日誌”。

- Data Loss Prevention BETA → 數據丟失防護 -數據丟失防護（DLP）發現規則使您可以在受管設備上掃描包含敏感信息的文件。例如，信用卡號，身分證等。

網絡管理選單介紹

NETWORK MANAGEMENT BETA



Discoveries → 發現 - 發現區域使您可以管理，創建和運行發現掃描

Profiles → 管理網絡SNMP設備的配置文件 - 網絡配置文件用於不運行受支持的操作系統（Windows，Linux，iOS等）的SNMP兼容設備。示例設備包括路由器，交換機和打印機。

Devices → 管理網絡設備 - 您可以查看所有發現掃描的結果。您還可以管理兼容簡單網絡管理協議（SNMP）的設備。

Monitors → 管理網絡監視器 - 監視器是一種腳本，用於跟踪SNMP設備上的事件，並在滿足其條件時採取特定的措施。例如，您可以設置監視器以在設備關閉一定時間後向您發出警報。

應用程序商店選單介紹

APPLICATION STORE

iOS Store → iOS商店區域包含已上載到Endpoint Manager的所有可用iOS應用程序。

Android Store → Android商店區域包含已上載到Endpoint Manager的所有可用Android應用程序。

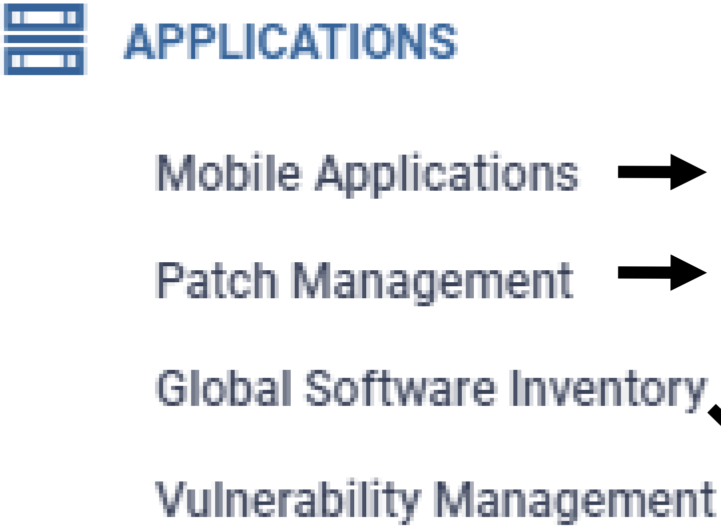
Windows Application Store

↓

Windows應用程序商店是可以部署到Windows設備的應用程序庫。您可以安裝的應用程序包括Adobe Acrobat，CCleaner，Firefox，Thunderbird等。

應用程序選單介紹

COMODO
Creating Trust Online™



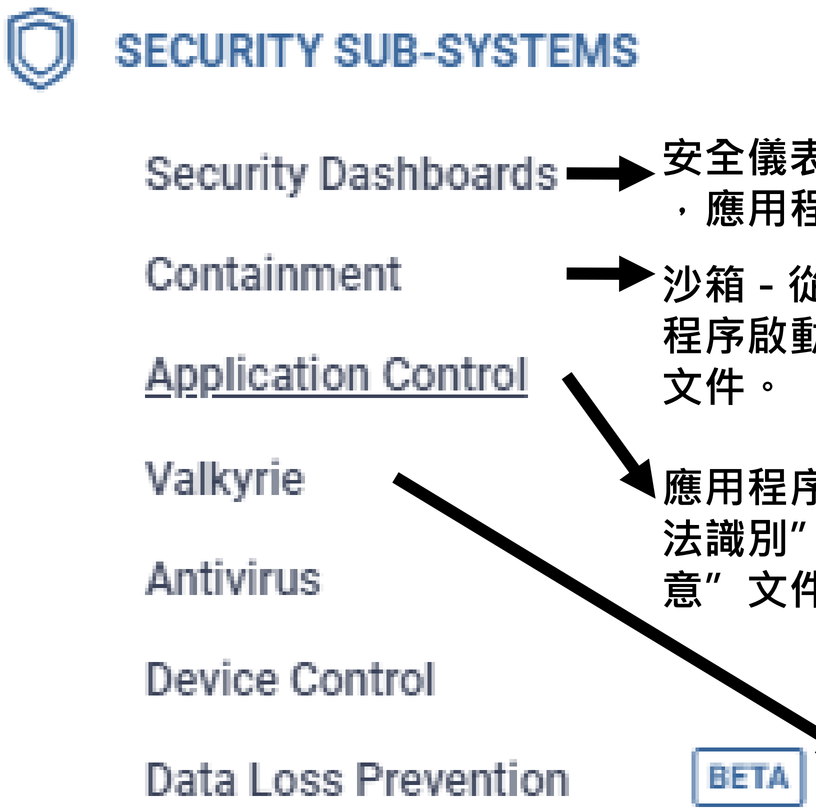
移動應用程序 -查看已註冊的Android和iOS設備上安裝的所有應用程序。阻止任何被識別為惡意的應用程序。一旦列入黑名單，該應用程序將不允許在其安裝的任何設備上運行。

修補程序管理 -查看可管理的Windows設備可用的操作系統和第三方應用程序修補程序的不斷更新的列表。該區域可讓您根據需要安裝或卸載補丁程序/更新。

全局軟件清單 -查看Windows設備上安裝的所有應用程序。您可以根據需要卸載不需要的應用程序。

漏洞管理 -顯示設備上的已知漏洞以及常見的漏洞和披露（CVE）列表。
您可以在受影響的設備上運行補丁。

安全子系統選單介紹



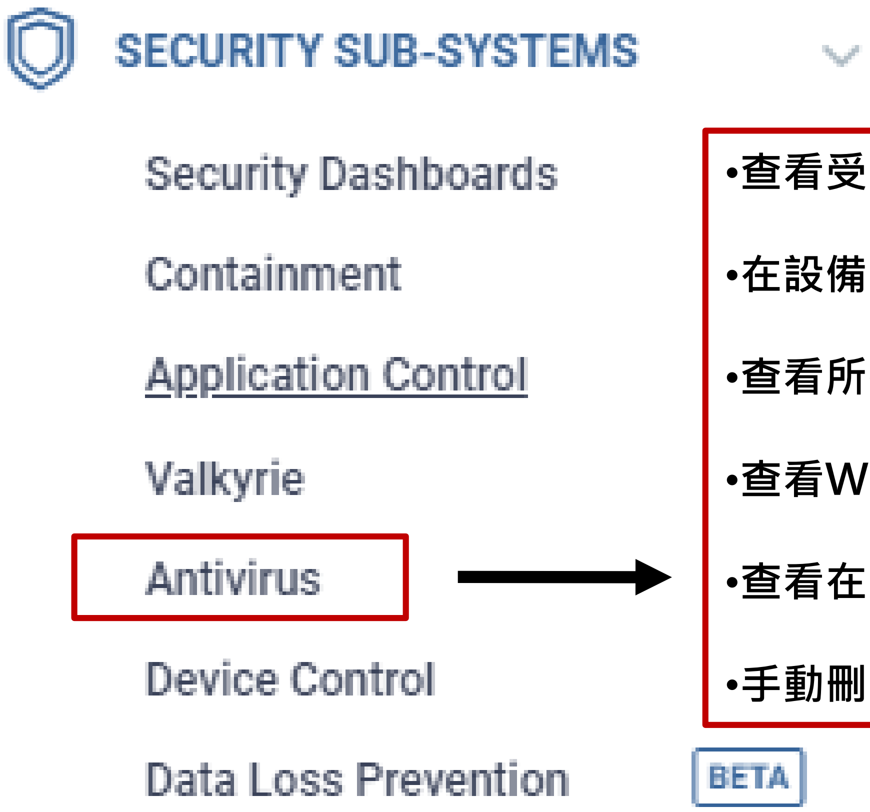
安全儀表板是受管端點上所有安全事件的列表。這包括來自防病毒，遏制，應用程序控制，自動運行控制和虛擬桌面組件的事件。

沙箱 - 從界面查看沙箱中運行的所有程序。管理員還可以查看沙箱的應用程序啟動的流程的活動。管理員可以選擇將沙箱的文件評為受信任或惡意文件。

應用程序控制 – 使您可以查看端點上文件的信任等級。可能的等級為“無法識別”，“受信任”或“惡意”，並向該界面報告“無法識別”和“惡意”文件。管理員可以自行決定手動設置等級。

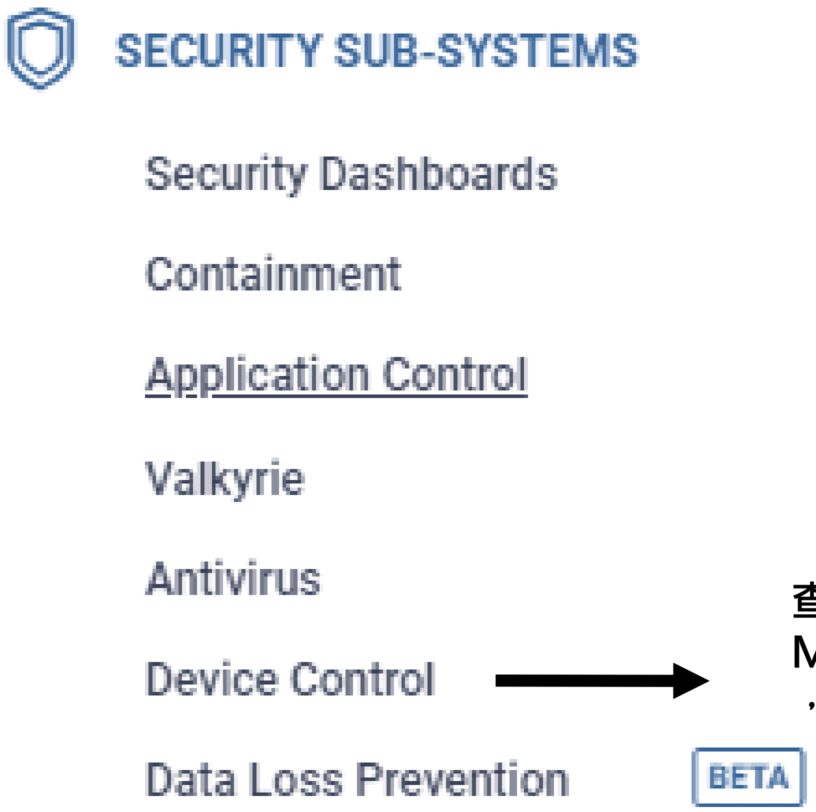
Valkyrie是基於雲的文件分析服務，可通過一系列靜態和行為檢查來測試未知文件。該服務可幫助ITarian確定未知文件是惡意文件還是安全文件

安全子系統選單介紹



- 查看受管Windows，Mas OS，Linux和Android設備的感染狀態。
- 在設備上運行防病毒和文件分級掃描
- 查看所有端點上所有惡意軟件的合併列表
- 查看Windows，Mac OS和Linux設備上的所有隔離文件
- 查看在所有端點上發現的威脅的歷史記錄
- 手動刪除，隔離或忽略惡意文件

安全子系統選單介紹



查看從外部設備到Windows端點的所有連接嘗試，，Endpoint Manager可以創建日誌條目。外部設備包括USB設備，DVD驅動器，印表機，藍牙設備等。

DLP掃描使您可以在託管端點中搜索敏感數據，例如卡號，社會保險號和銀行帳號。

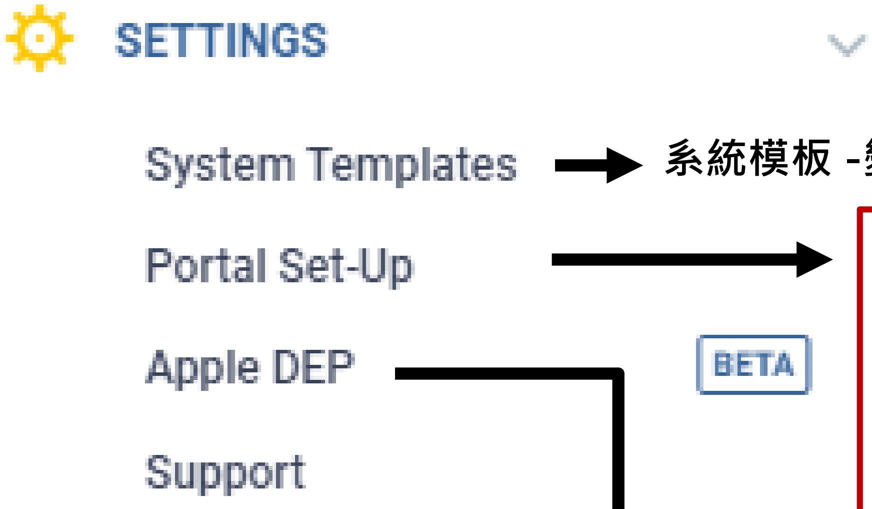
許可證管理選單介紹

LICENSE MANAGEMENT

License Management

- 查看許可證詳細信息
- 添加新許可證
- 刪除許可證
- 續訂許可證
- 使用單個許可證為多個客戶註冊設備（僅MSP）
- 向單個客戶分配多個許可證（僅適用於MSP）
- 配置許可證使用情況報告

設置選單介紹

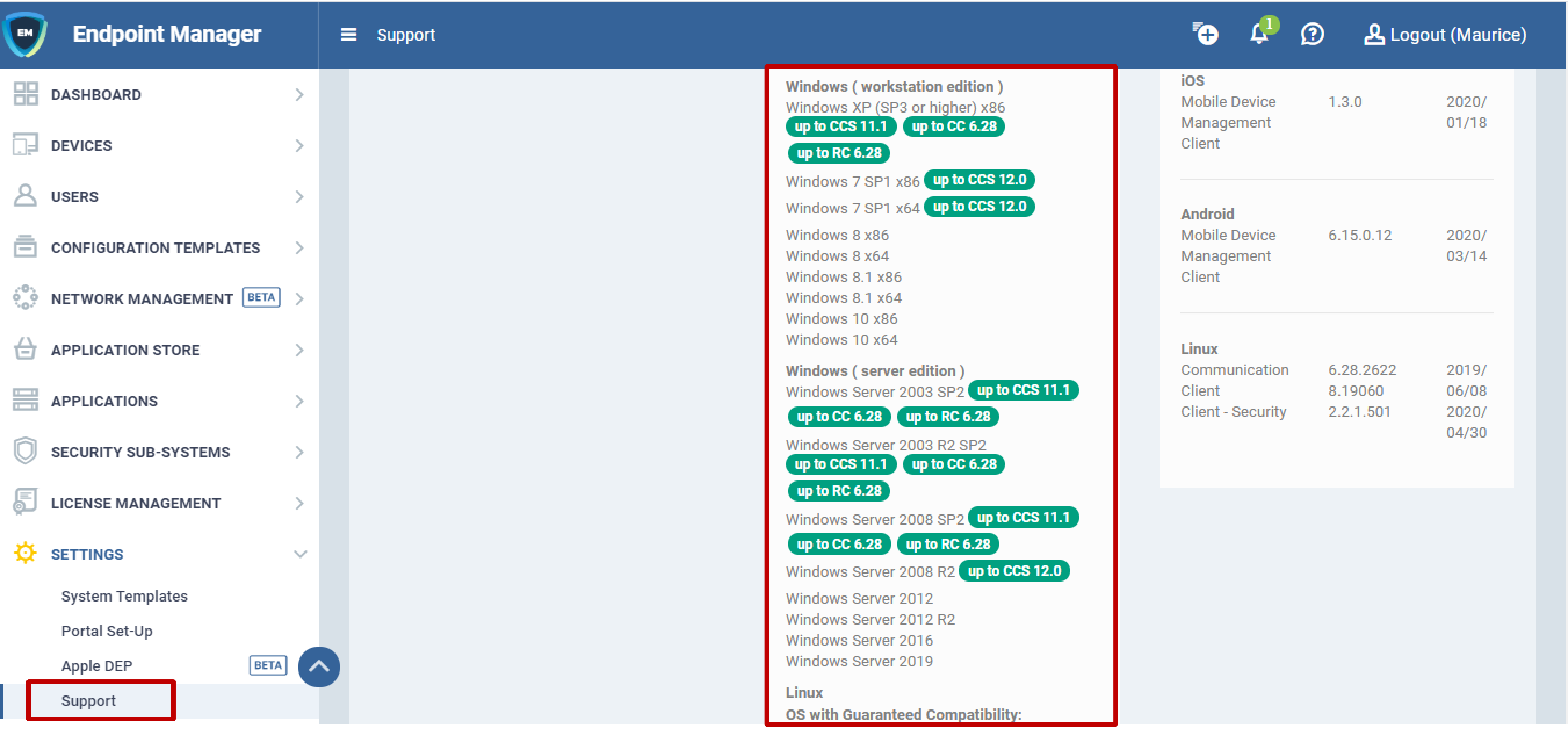


系統模板 -變量和文件組由各種Endpoint Manager模塊使用/引用。

- 集成Active Directory，以便您可以從域中導入用戶和設備
- 添加Apple和Google證書，以便Endpoint Manager可以與iOS和Android設備通信。
- 配置客戶端設置，報告，兩因素登錄，管理時區等。

蘋果的設備註冊計劃（DEP）簡化了企業網絡中iOS和Mac設備的激活和管理。儘管您將繼續使用Endpoint Manager進行日常設備管理，但DEP使管理員和用戶的初始設置過程變得更加容易。

支援作業系統



Windows (workstation edition)

Windows XP (SP3 or higher) x86 up to CCS 11.1 up to CC 6.28 up to RC 6.28
Windows 7 SP1 x86 up to CCS 12.0
Windows 7 SP1 x64 up to CCS 12.0
Windows 8 x86
Windows 8 x64
Windows 8.1 x86
Windows 8.1 x64
Windows 10 x86
Windows 10 x64

Windows (server edition)

Windows Server 2003 SP2 up to CCS 11.1 up to CC 6.28 up to RC 6.28
Windows Server 2003 R2 SP2 up to CCS 11.1 up to CC 6.28 up to RC 6.28
Windows Server 2008 SP2 up to CCS 11.1 up to CC 6.28 up to RC 6.28
Windows Server 2008 R2 up to CCS 12.0
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019

Linux

OS with Guaranteed Compatibility:

iOS

Mobile Device Management Client 1.3.0 2020/01/18

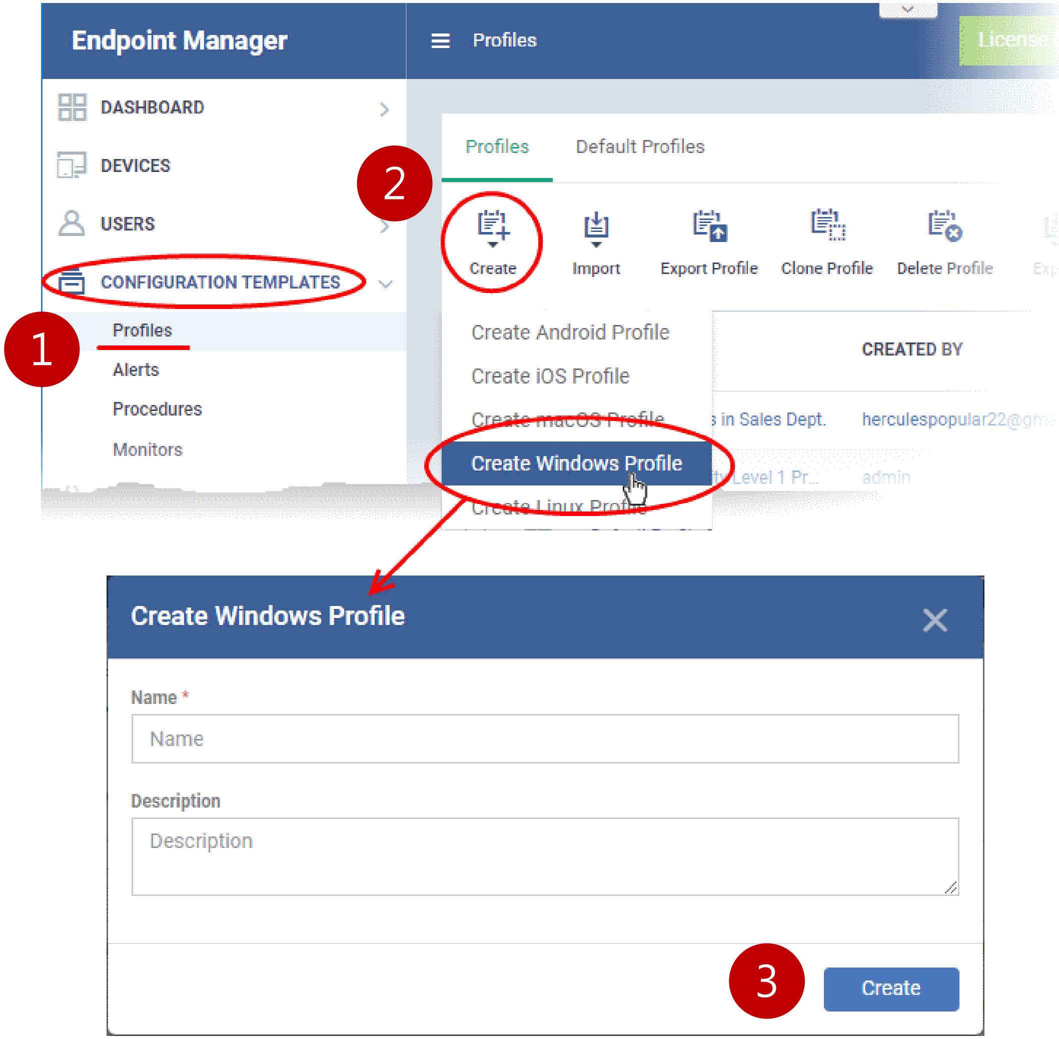
Android

Mobile Device Management Client 6.15.0.12 2020/03/14

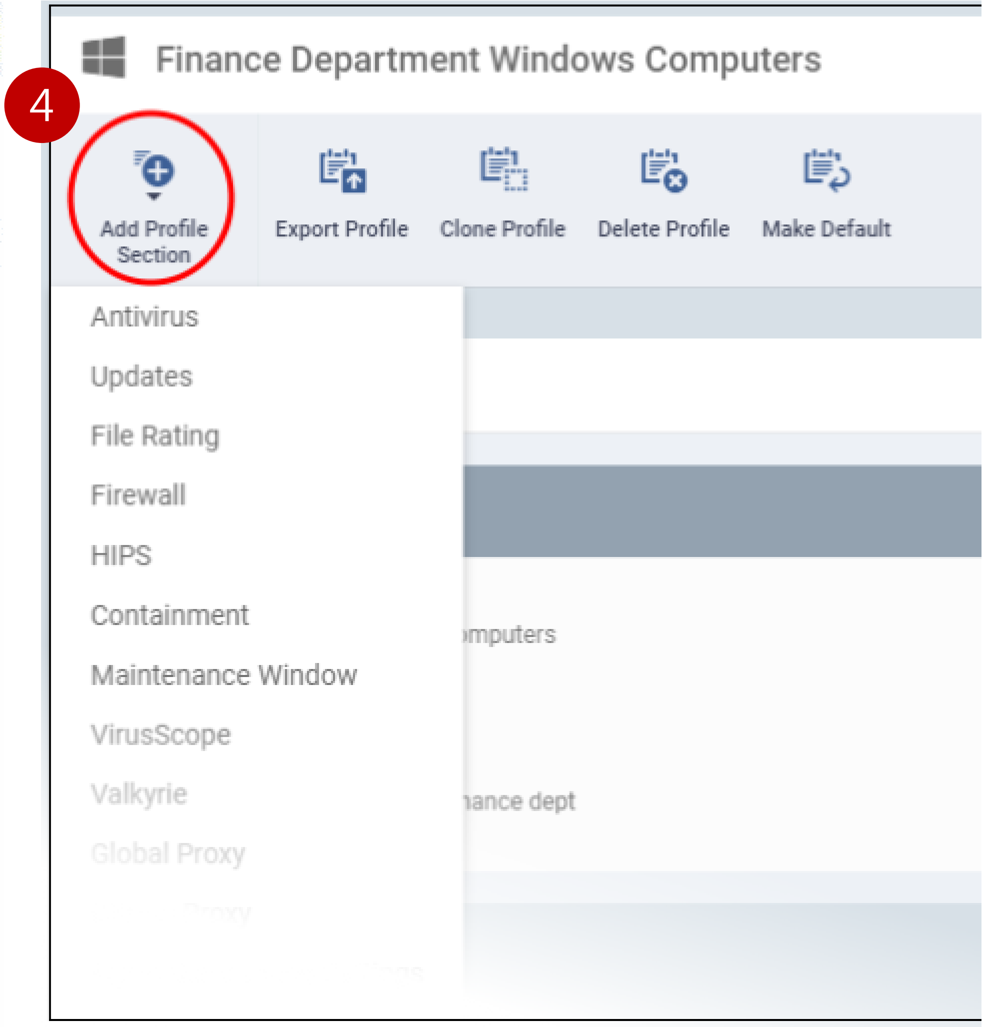
Linux

Communication Client 6.28.2622 2019/06/08
Client - Security 8.19060 2.2.1.501 2020/04/30

創建配置文件

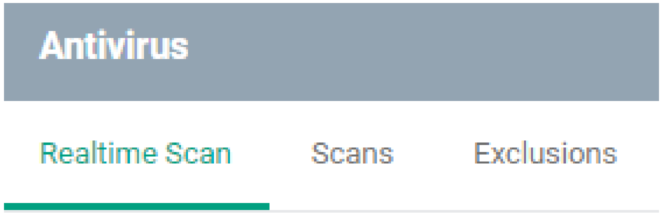


創建Windows配置文件



選擇要添加到配置文件中的組件

Antivirus 配置文件介紹

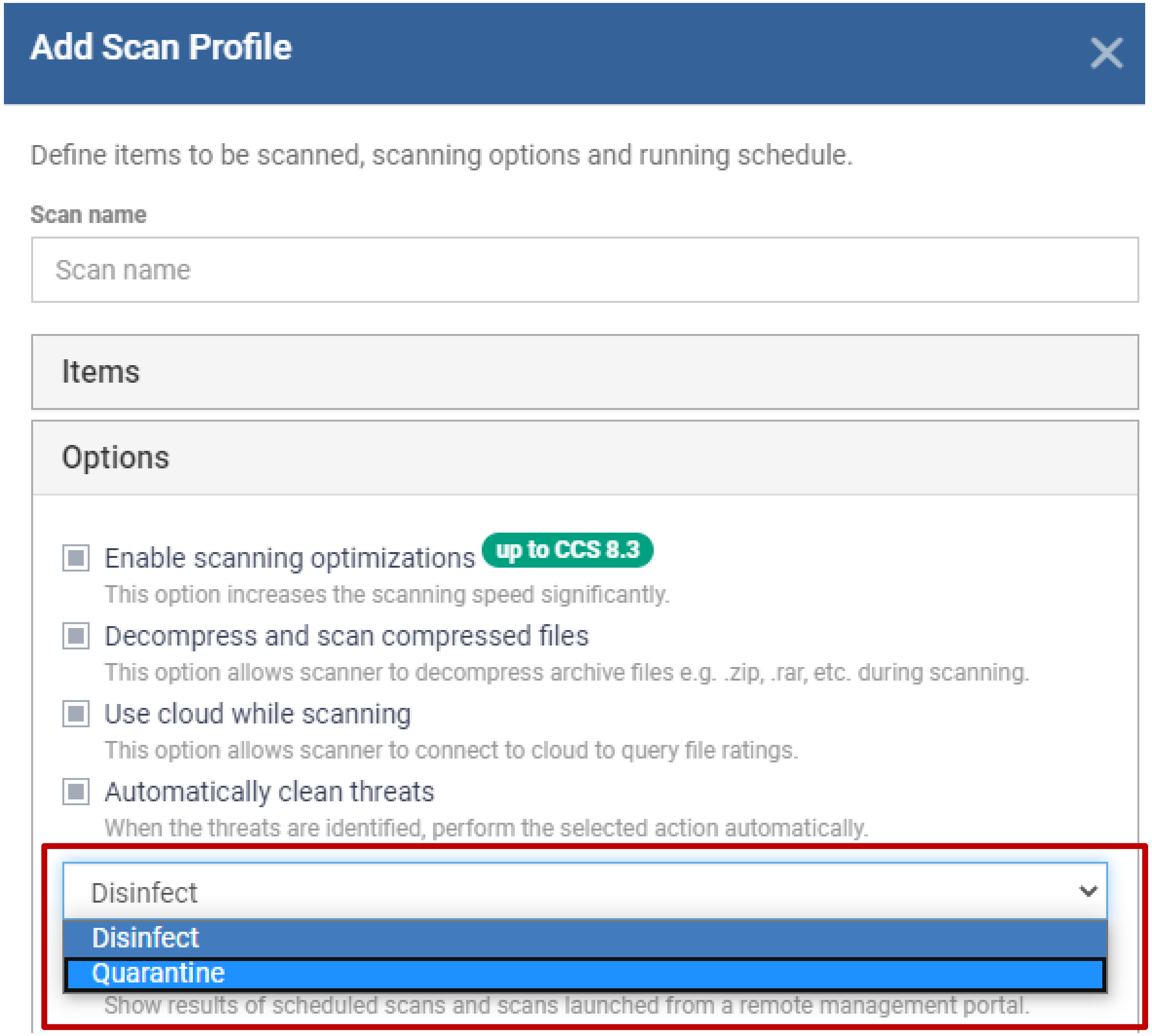


您在此處添加的項目在掃描和任
何自定義掃描配置文件將排除。

自定義掃描配置文件使您可以選擇要掃描的區域。

這是核心防病毒掃描程序，可不斷保
護您的端點免受惡意軟件的侵害。

Antivirus 配置文件介紹



Add Scan Profile

Define items to be scanned, scanning options and running schedule.

Scan name

Scan name

Items

Options

□ Enable scanning optimizations up to CCS 8.3
This option increases the scanning speed significantly.

□ Decompress and scan compressed files
This option allows scanner to decompress archive files e.g. .zip, .rar, etc. during scanning.

□ Use cloud while scanning
This option allows scanner to connect to cloud to query file ratings.

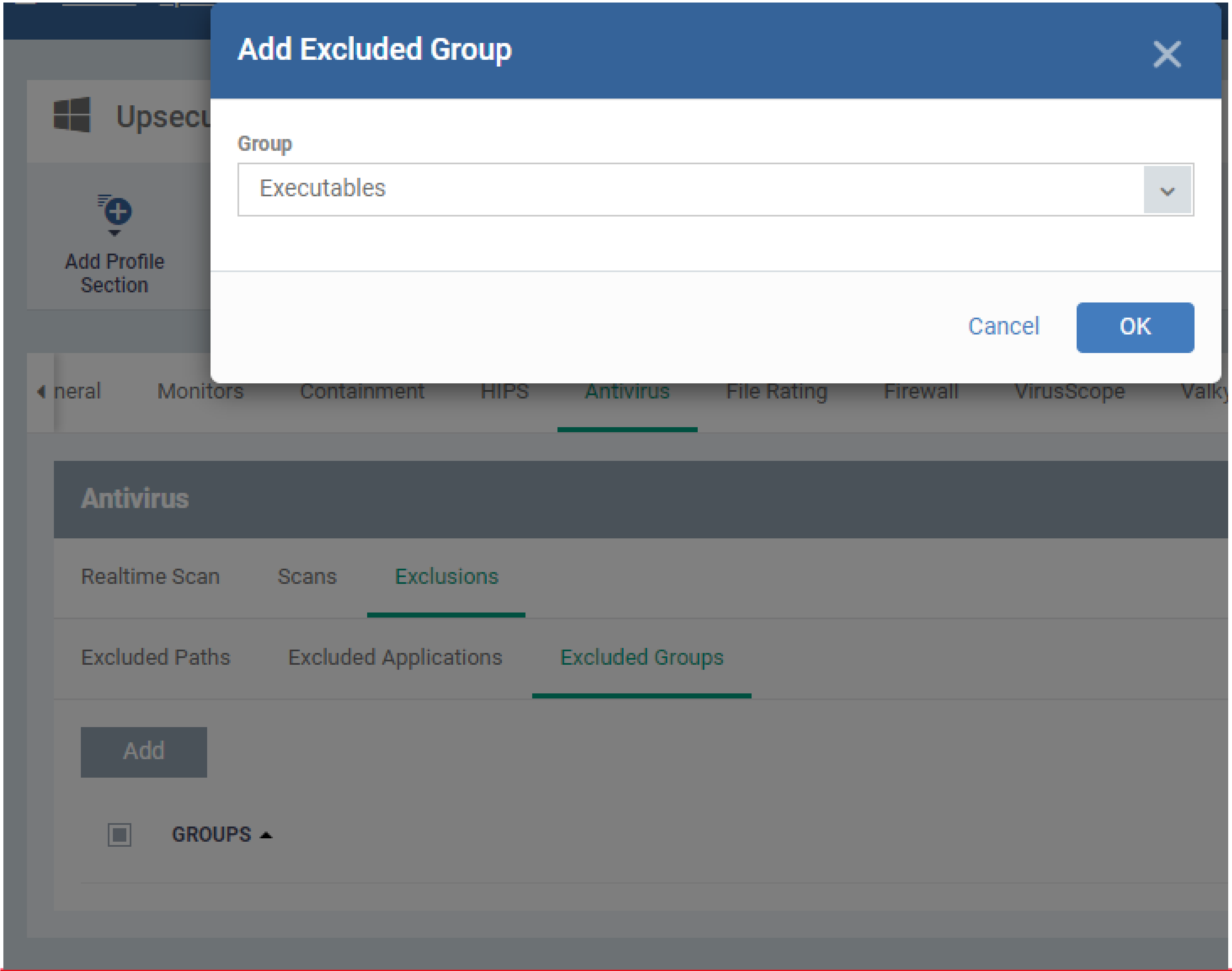
□ Automatically clean threats
When the threats are identified, perform the selected action automatically.

Disinfect

Show results of scheduled scans and scans launched from a remote management portal.

CCS將自動對檢測到的威脅採取措施，而不是顯示帶有威脅列表的結果屏幕。您可以從下拉菜單中選擇要採取的措施。可用的選項有：移除、隔離
選擇移除將無法在中控台上找到已刪除資料

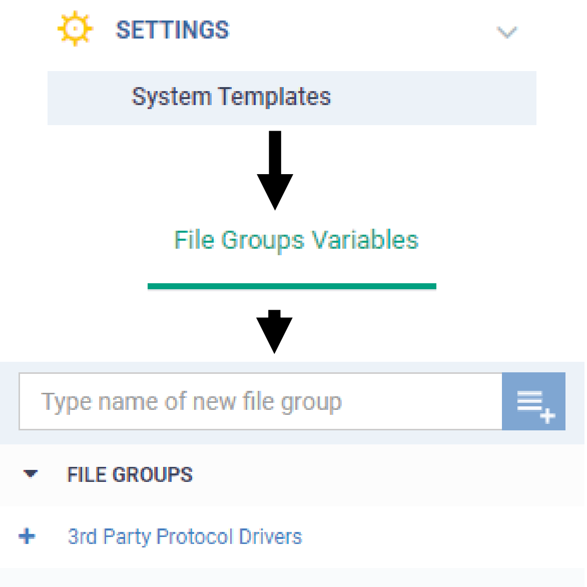
Antivirus 配置文件介紹



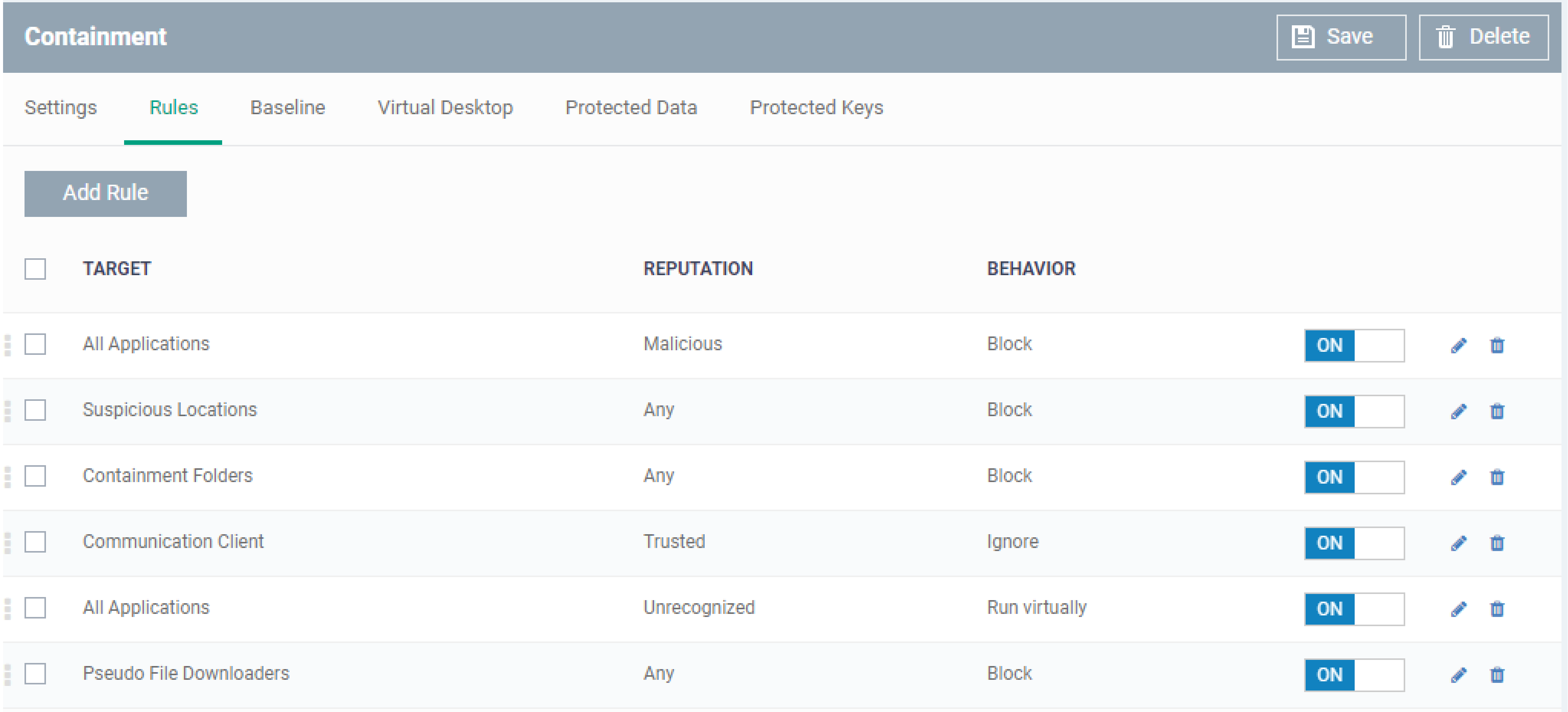
Add Excluded Group

Group: Executables

添加排除的組:
通過文件組，可以輕鬆排除整個文件類型。
單擊 “setting” > “system templates” > “file group variable” 以查看/編輯/創建文件組。



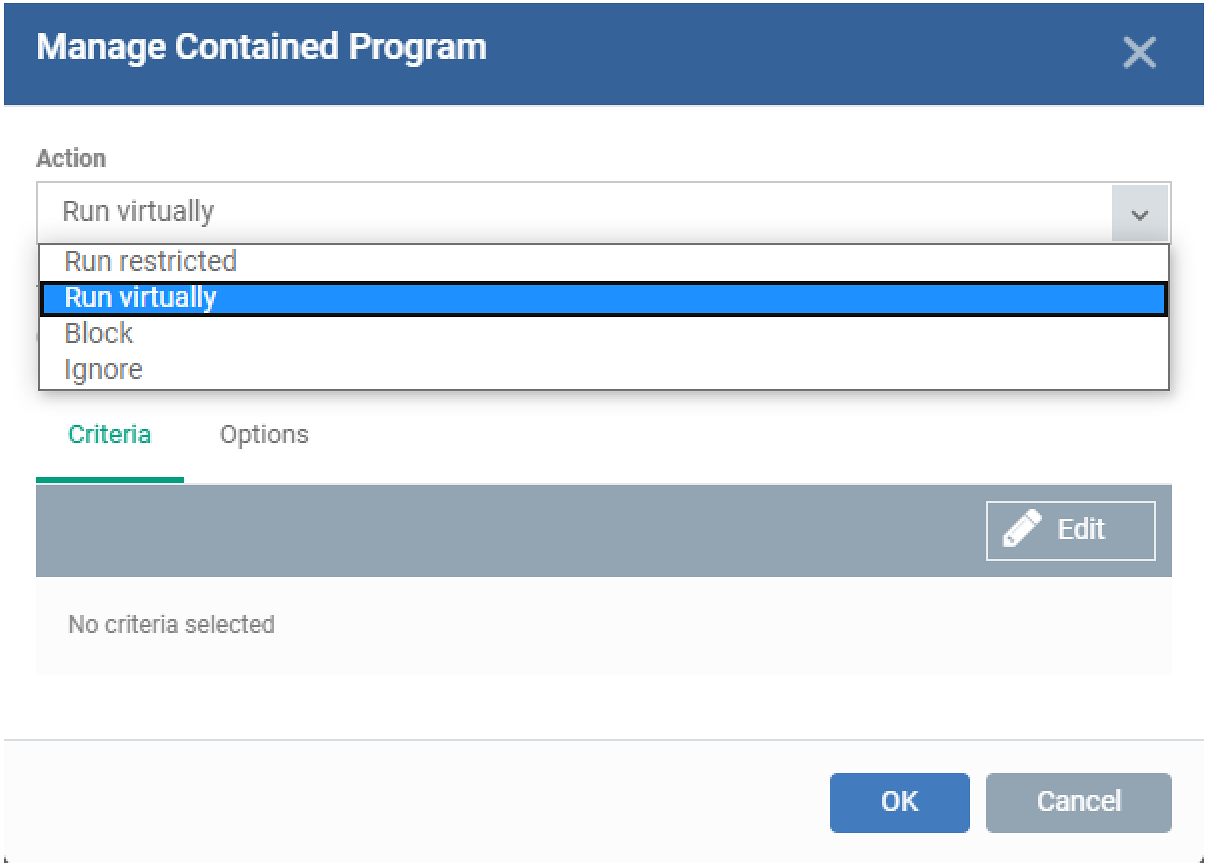
Containment配置文件介紹



□	TARGET	REPUTATION	BEHAVIOR		
□	All Applications	Malicious	Block	ON	✎ 🗑
□	Suspicious Locations	Any	Block	ON	✎ 🗑
□	Containment Folders	Any	Block	ON	✎ 🗑
□	Communication Client	Trusted	Ignore	ON	✎ 🗑
□	All Applications	Unrecognized	Run virtually	ON	✎ 🗑
□	Pseudo File Downloaders	Any	Block	ON	✎ 🗑

依使用者情境設計相關規則

Containment配置文件介紹



Manage Contained Program

Action

Run virtually

No criteria selected

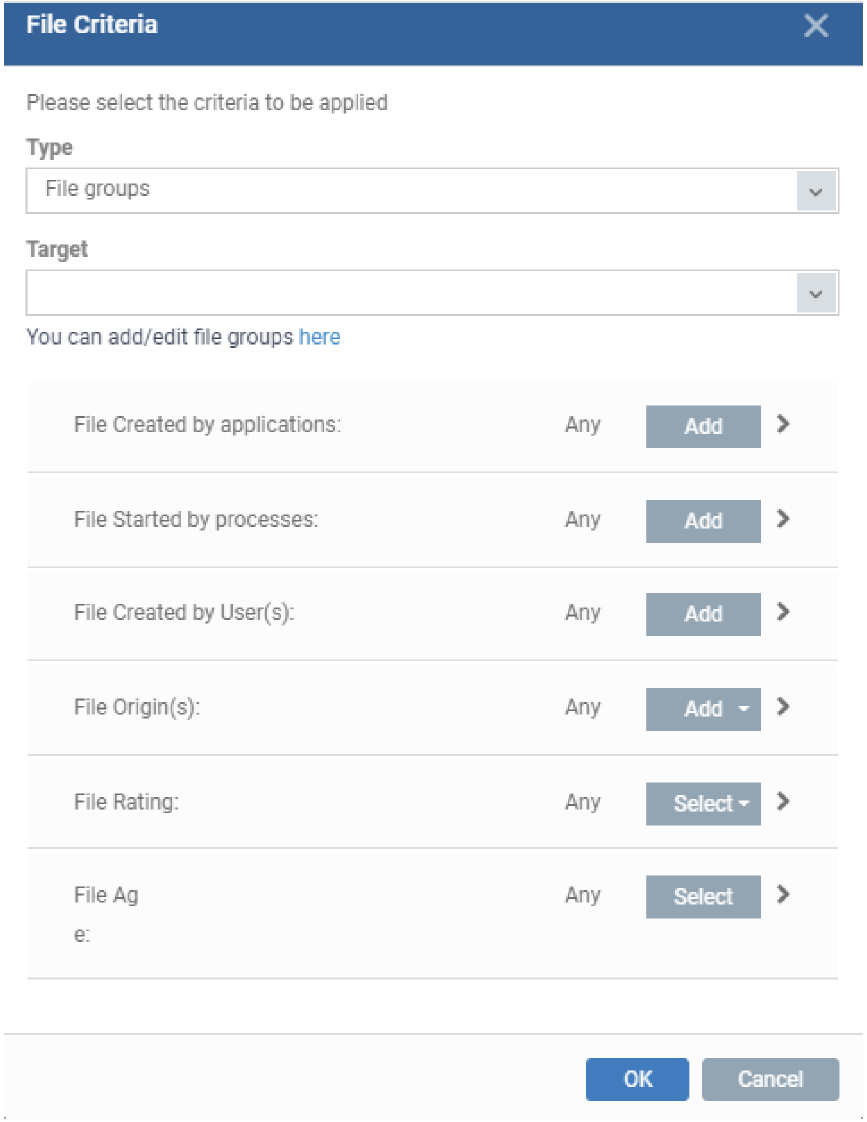
受限運行 -允許應用程序訪問很少的操作系統資源。該應用程序一次不能執行10個以上的進程，並且以非常有限的訪問權限運行。在此設置下，某些應用程序（例如計算機遊戲）可能無法正常運行

虛擬運行 -該應用程序將在與您的操作系統和計算機其餘部分完全隔離的虛擬環境中運行

阻擋 -完全不允許運行該應用程序

忽略 -將不包含該應用程序，並允許其以所有特權運行。

Containment配置文件介紹



File Criteria

Please select the criteria to be applied

Type: File groups

Target:

You can add/edit file groups here

File Created by applications: Any

File Started by processes: Any

File Created by User(s): Any

File Origin(s): Any

File Rating: Any

File Ag
e: Any

→ 指定應用程序。

→ 如果文件是由特定進程創建的，則自動包含該文件

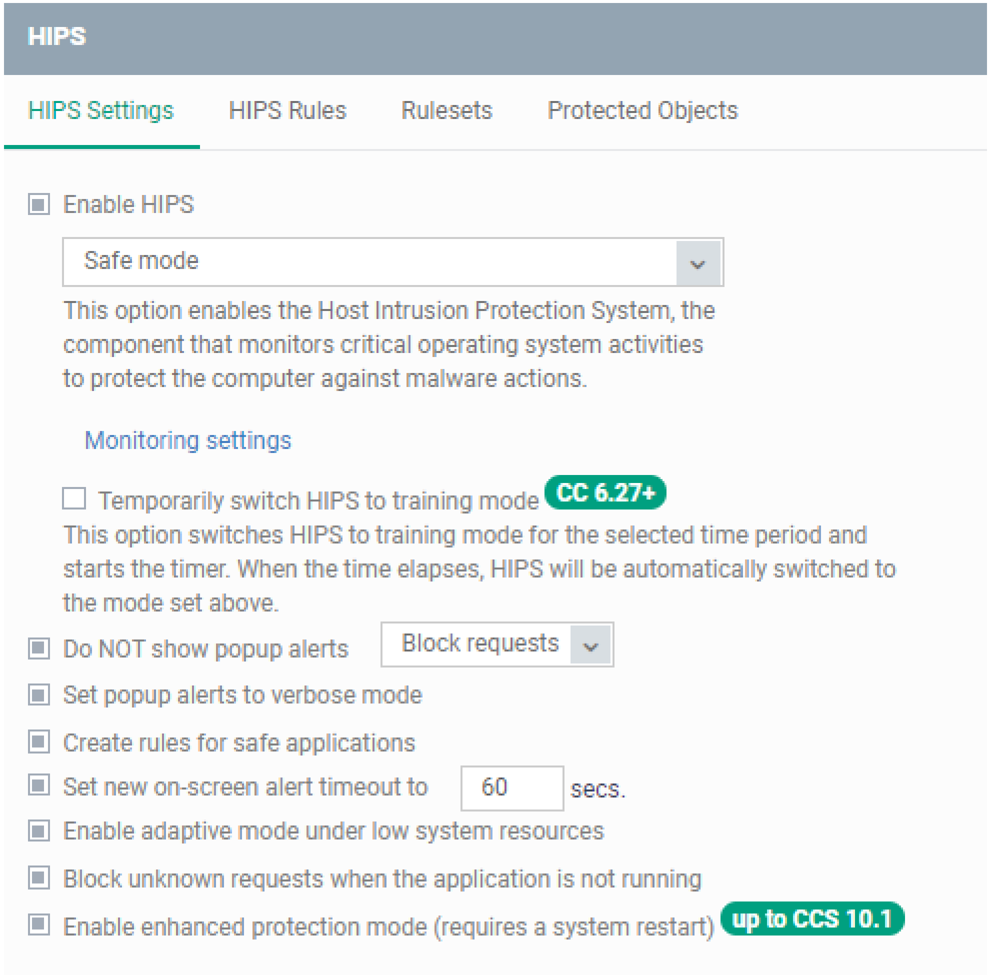
→ 指定特定用戶身分

→ 指定特定源下載文件

→ 指定檔案信任等級

→ 指定檔案時程

HIPS 配置文件介紹



HIPS

HIPS Settings | HIPS Rules | Rulesets | Protected Objects

▣ Enable HIPS

Safe mode

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

Monitoring settings

□ Temporarily switch HIPS to training mode CC 6.27+

This option switches HIPS to training mode for the selected time period and starts the timer. When the time elapses, HIPS will be automatically switched to the mode set above.

▣ Do NOT show popup alerts Block requests

▣ Set popup alerts to verbose mode

▣ Create rules for safe applications

▣ Set new on-screen alert timeout to 60 secs.

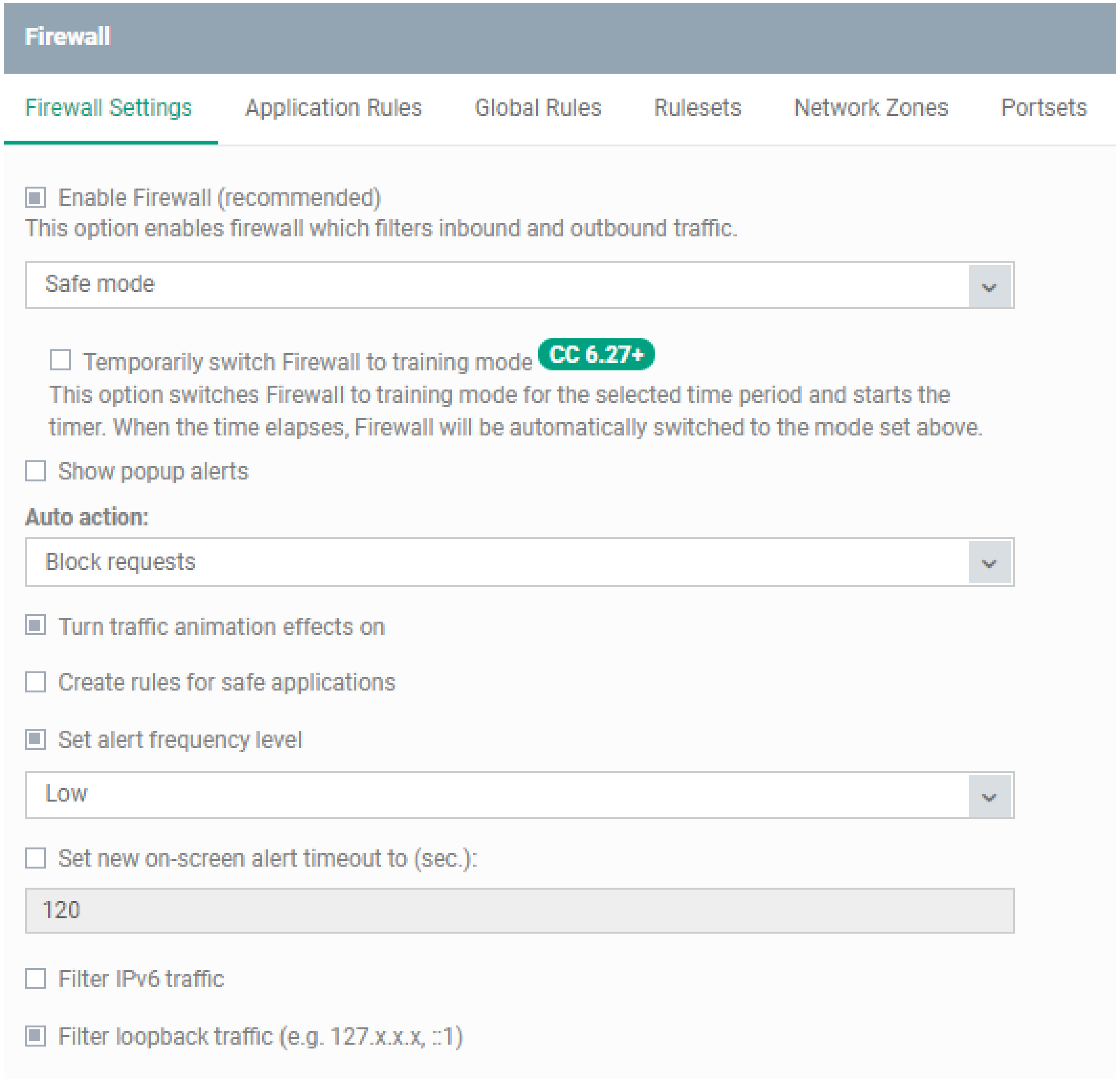
▣ Enable adaptive mode under low system resources

▣ Block unknown requests when the application is not running

▣ Enable enhanced protection mode (requires a system restart) up to CCS 10.1

主機入侵防禦系統（HIPS）不斷監視系統活動。僅當流程符合端點配置文件中的安全規則時，它才允許運行。HIPS保護系統關鍵文件和註冊表項免受惡意軟件的未經授權的修改。

Firewall 配置文件介紹



☑ Enable Firewall (recommended)
This option enables firewall which filters inbound and outbound traffic.

Safe mode

□ Temporarily switch Firewall to training mode CC 6.27+
This option switches Firewall to training mode for the selected time period and starts the timer. When the time elapses, Firewall will be automatically switched to the mode set above.

□ Show popup alerts

Auto action:

Block requests

☑ Turn traffic animation effects on

□ Create rules for safe applications

☑ Set alert frequency level

Low

□ Set new on-screen alert timeout to (sec.):

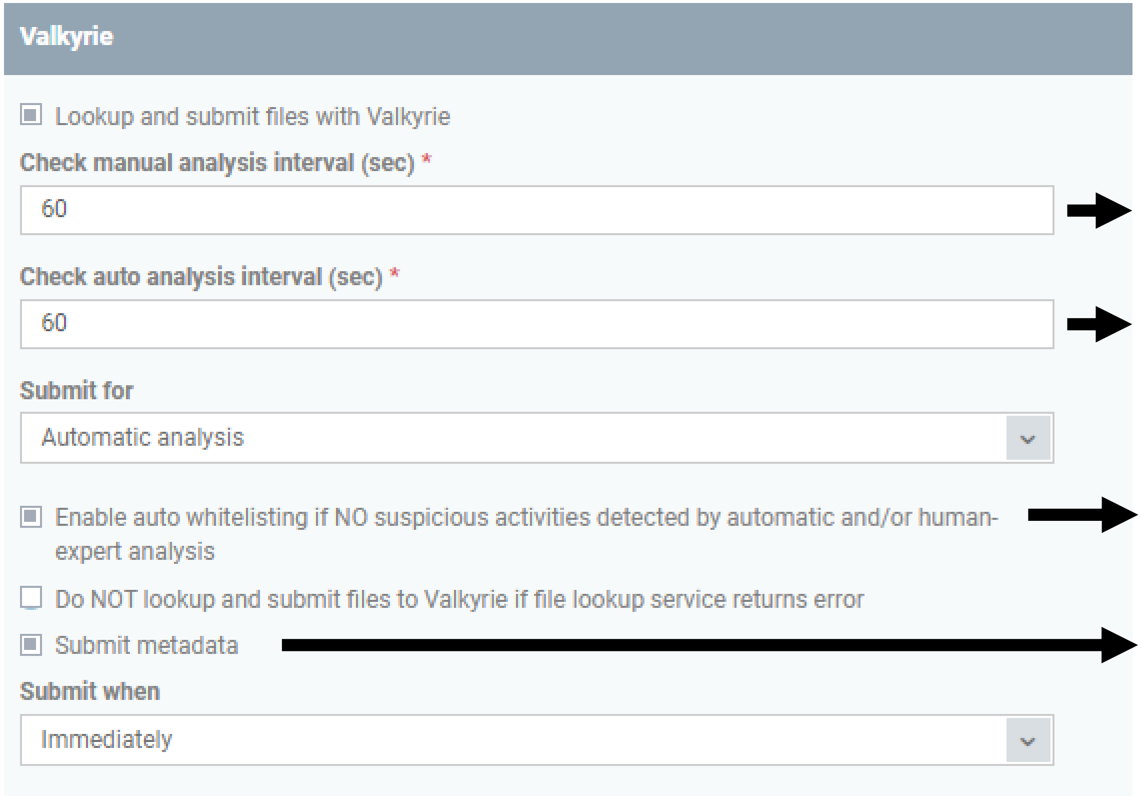
120

□ Filter IPv6 traffic

☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

配置網絡區域，端口集和流量過濾規則。

Valkyrie 配置文件介紹



Valkyrie

☑ Lookup and submit files with Valkyrie

Check manual analysis interval (sec) *

60

Check auto analysis interval (sec) *

60

Submit for

Automatic analysis

☑ Enable auto whitelisting if NO suspicious activities detected by automatic and/or human-expert analysis

□ Do NOT lookup and submit files to Valkyrie if file lookup service returns error

☑ Submit metadata

Submit when

Immediately

手動分析

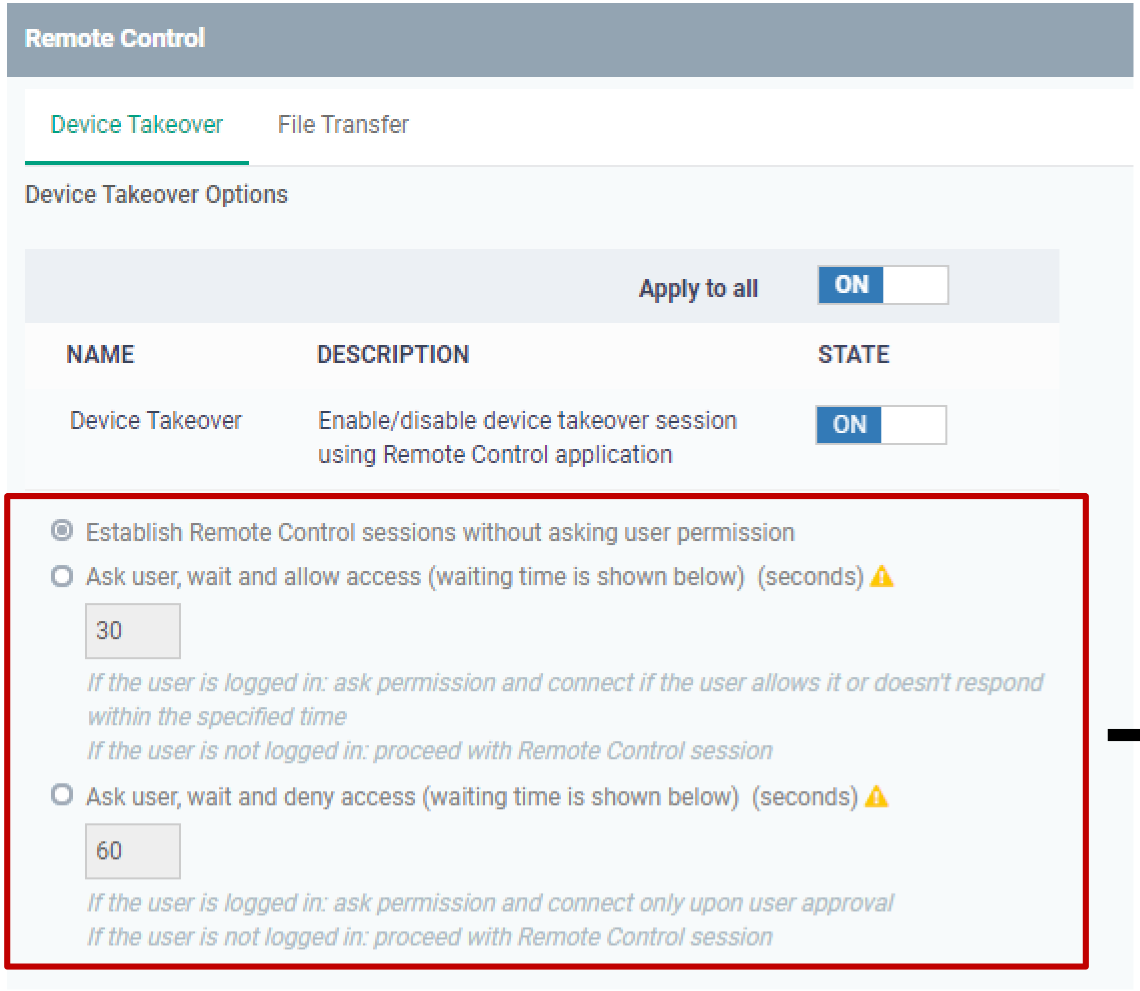
自動分析

將Valkyrie標識為無害的文件添加到本地白名單

提交元數據

Valkyrie是基於雲的文件判決服務，可對未知文件進行一系列測試，以識別惡意文件。

遠端控制 配置文件介紹



Remote Control

Device Takeover | File Transfer

Device Takeover Options

Apply to all ON

NAME	DESCRIPTION	STATE
Device Takeover	Enable/disable device takeover session using Remote Control application	ON

● Establish Remote Control sessions without asking user permission

○ Ask user, wait and allow access (waiting time is shown below) (seconds) ⚠

30

If the user is logged in: ask permission and connect if the user allows it or doesn't respond within the specified time
If the user is not logged in: proceed with Remote Control session

○ Ask user, wait and deny access (waiting time is shown below) (seconds) ⚠

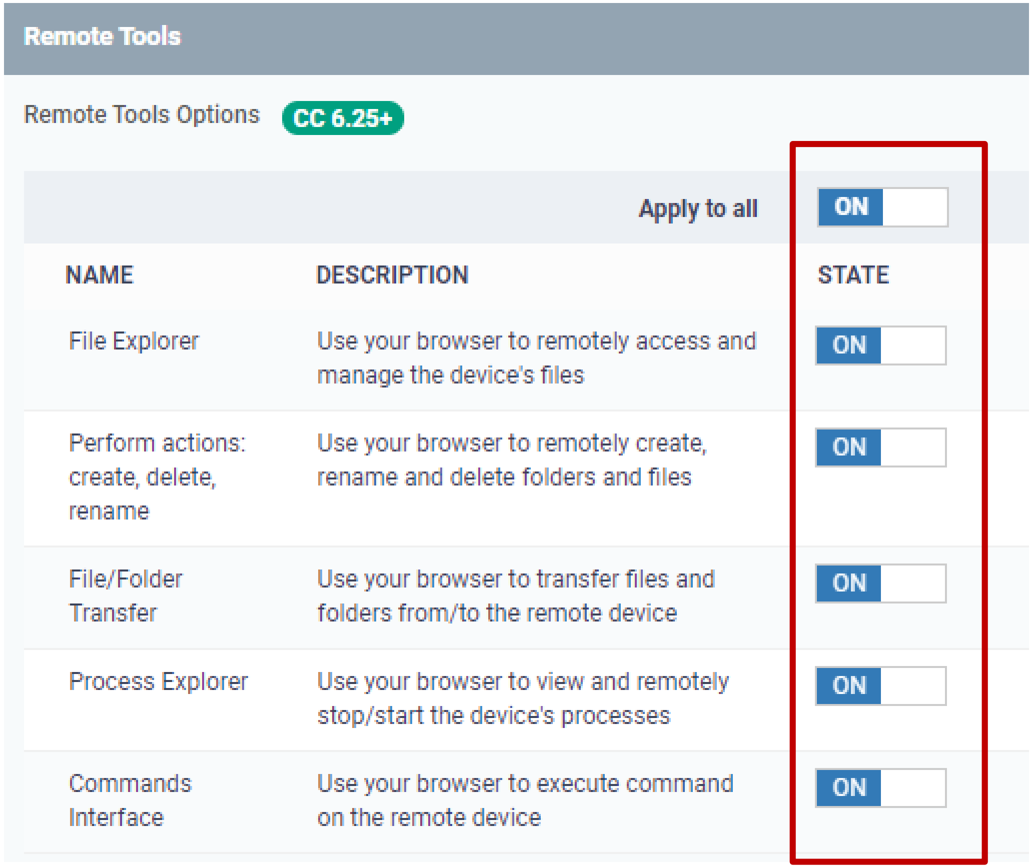
60

If the user is logged in: ask permission and connect only upon user approval
If the user is not logged in: proceed with Remote Control session

→ 連接後狀態設置

遠端工具 配置文件介紹

COMODO
Creating Trust Online™



Remote Tools

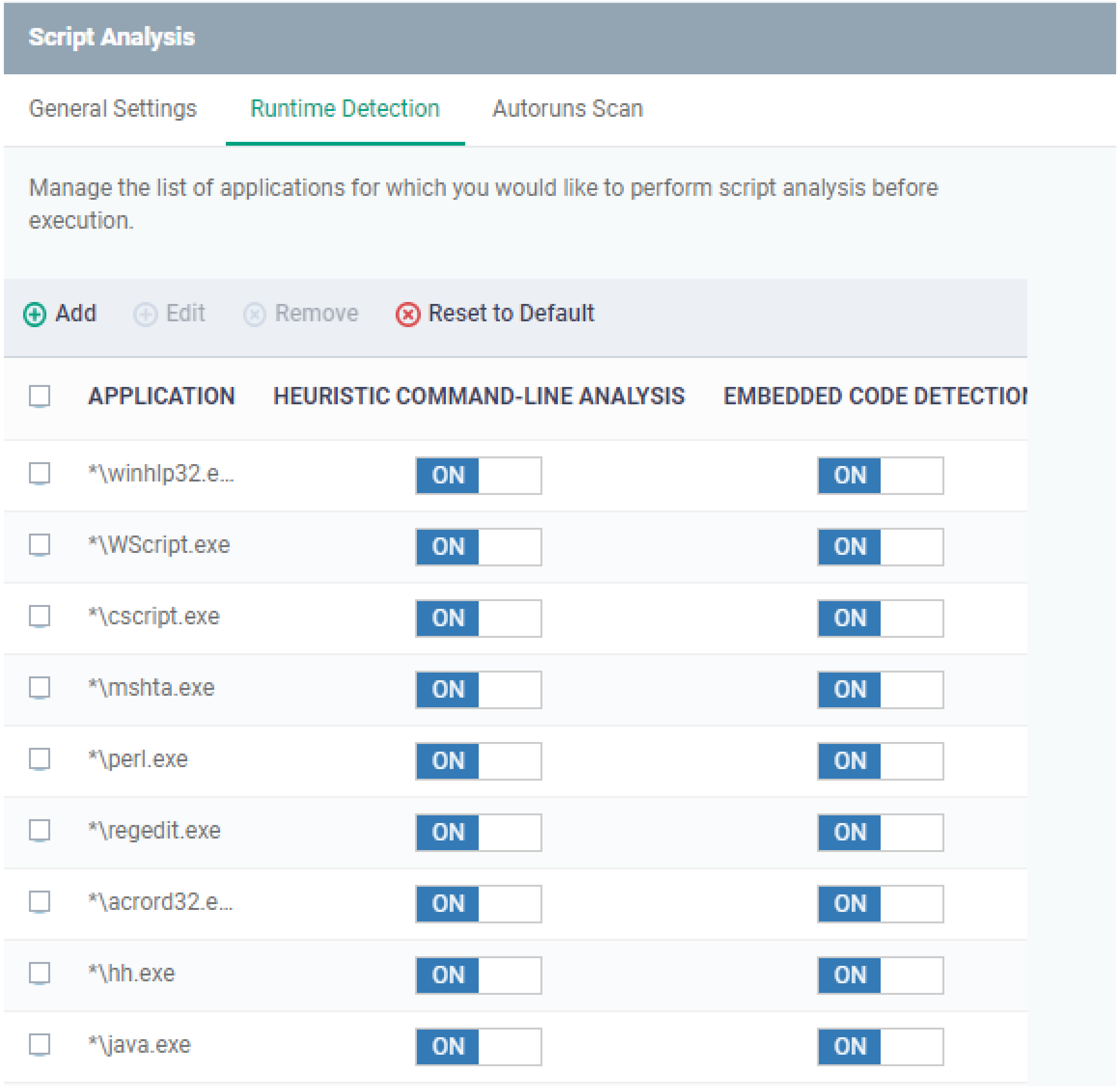
Remote Tools Options CC 6.25+

Apply to all ON

NAME	DESCRIPTION	STATE
File Explorer	Use your browser to remotely access and manage the device's files	ON
Perform actions: create, delete, rename	Use your browser to remotely create, rename and delete folders and files	ON
File/Folder Transfer	Use your browser to transfer files and folders from/to the remote device	ON
Process Explorer	Use your browser to view and remotely stop/start the device's processes	ON
Commands Interface	Use your browser to execute command on the remote device	ON

→ 開通與關閉透用政策者之功能

腳本分析 配置文件介紹



Script Analysis

General Settings | Runtime Detection | Autoruns Scan

Manage the list of applications for which you would like to perform script analysis before execution.

□	APPLICATION	HEURISTIC COMMAND-LINE ANALYSIS	EMBEDDED CODE DETECTIOI
□	*\winhlp32.e...	ON	ON
□	*\WScript.exe	ON	ON
□	*\cscript.exe	ON	ON
□	*\mshta.exe	ON	ON
□	*\perl.exe	ON	ON
□	*\regedit.exe	ON	ON
□	*\acrord32.e...	ON	ON
□	*\hh.exe	ON	ON
□	*\java.exe	ON	ON

啟發式命令行分析：

•啟發式技術可識別以前未知的病毒和木馬。

•對文件進行分析，以確定它們是否包含病毒的典型代碼。

•換句話說，試探法會識別具有類病毒屬性的文件，而不是尋找與黑名單上的簽名匹配的簽名。

•這使引擎可以預測新病毒的存在-即使它們不在當前病毒數據庫中。

嵌入式代碼檢測：

•嵌入式代碼檢測可保護您免受無文件惡意軟件攻擊。

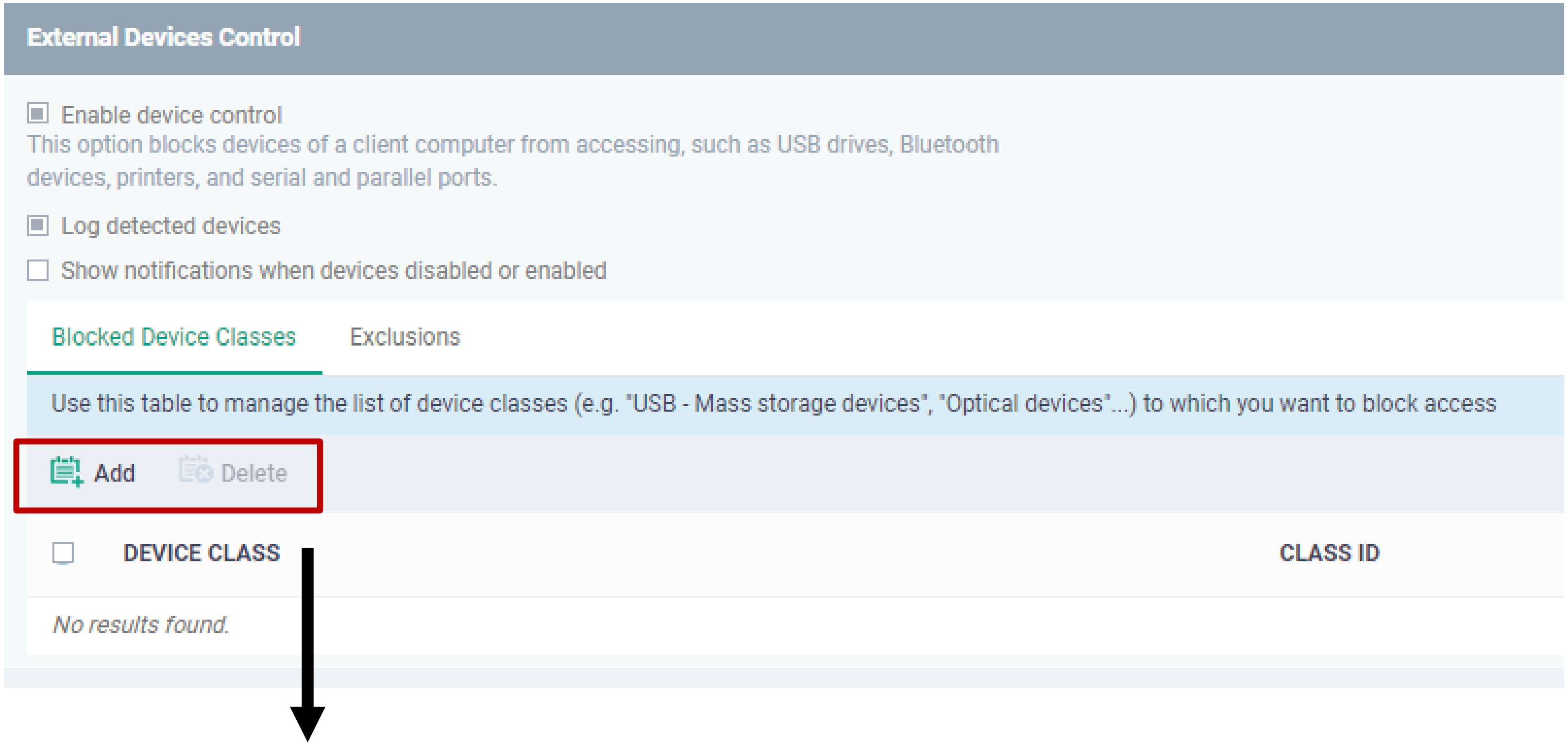
•無文件惡意軟件攻擊使惡意參與者可以直接在系統上執行Powershell命令。

•這些命令可用於控制端點，安裝勒索軟件，竊取機密數據等等。

•無文件腳本駐留在內存中，因此在重新啟動計算機後便不會留下任何痕跡。

•受此選項影響的示例程序是wscript.exe，cmd.exe，java.exe和javaw.exe。

外接設備控制 配置文件介紹



External Devices Control

☑ Enable device control
This option blocks devices of a client computer from accessing, such as USB drives, Bluetooth devices, printers, and serial and parallel ports.

☑ Log detected devices

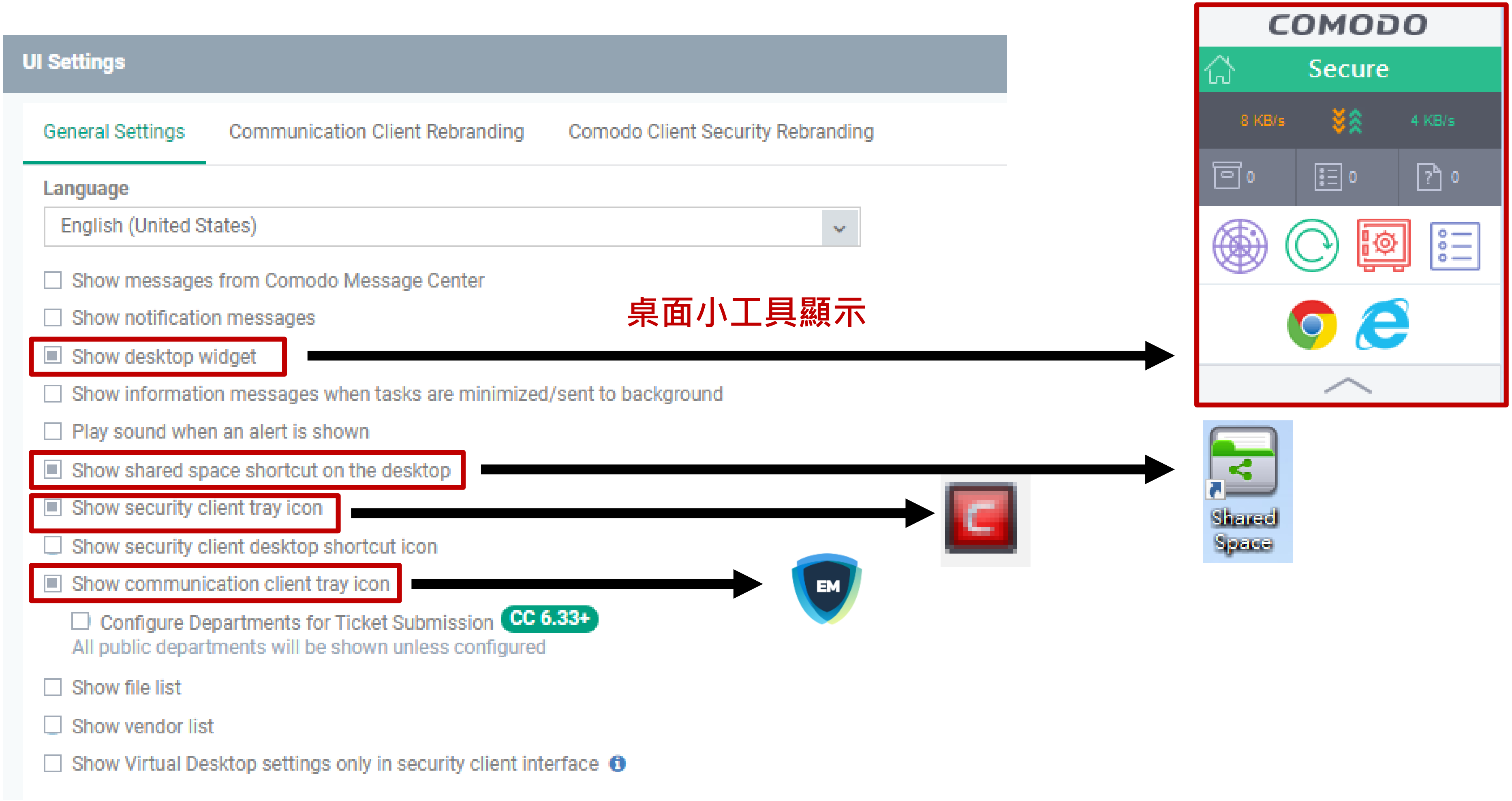
□ Show notifications when devices disabled or enabled

Use this table to manage the list of device classes (e.g. "USB - Mass storage devices", "Optical devices"...) to which you want to block access

□	DEVICE CLASS	CLASS ID
	No results found.	

設定指定之外接設備之連接狀況

UI Settings 配置文件介紹



UI Settings

General Settings | Communication Client Rebranding | Comodo Client Security Rebranding

Language

English (United States)

☐ Show messages from Comodo Message Center

☐ Show notification messages

☑ Show desktop widget

☐ Show information messages when tasks are minimized/sent to background

☐ Play sound when an alert is shown

☑ Show shared space shortcut on the desktop

☑ Show security client tray icon

☐ Show security client desktop shortcut icon

☑ Show communication client tray icon

☐ Configure Departments for Ticket Submission CC 6.33+
All public departments will be shown unless configured

☐ Show file list

☐ Show vendor list

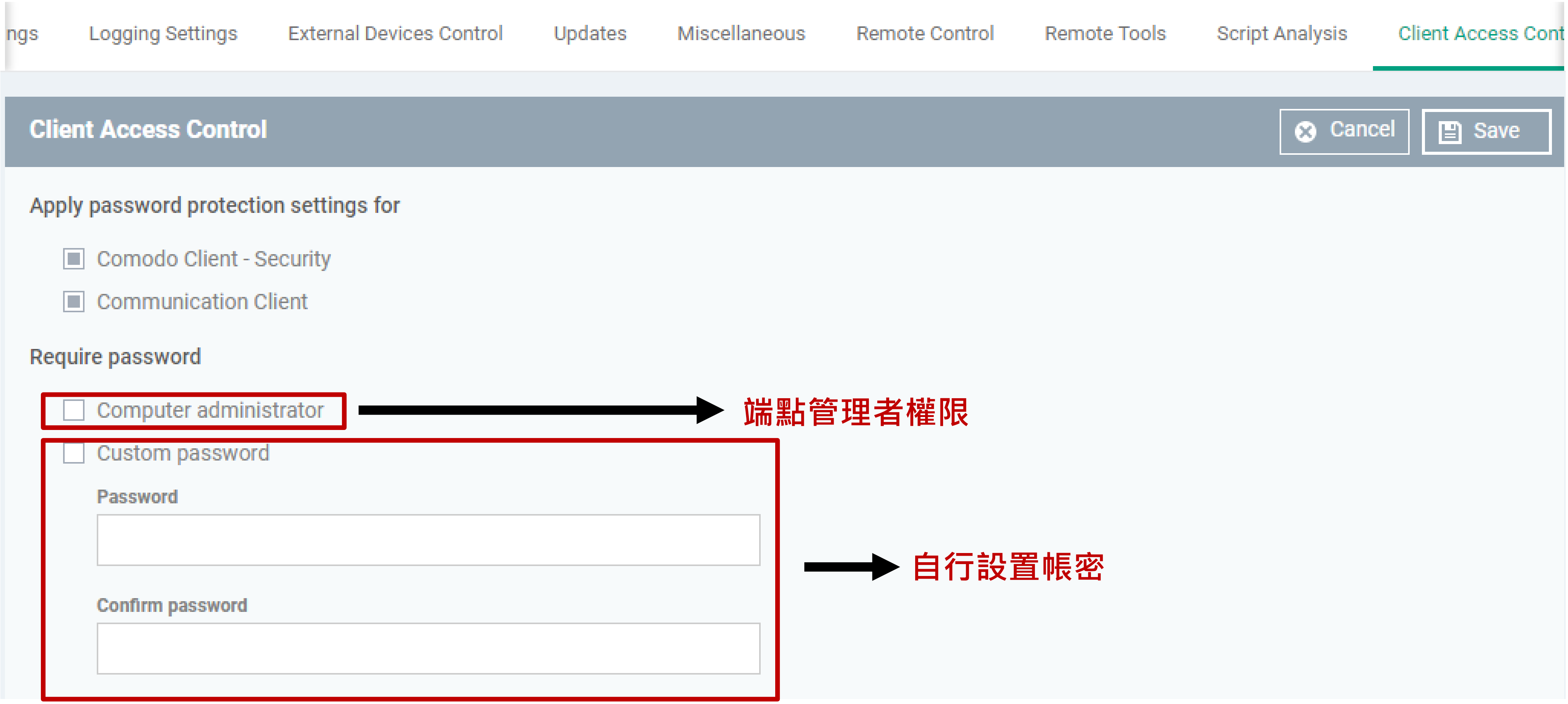
☐ Show Virtual Desktop settings only in security client interface

桌面小工具顯示

設定使用者介面

Client Access Control配置文件介紹

COMODO
Creating Trust Online™



Client Access Control

Apply password protection settings for

☑ Comodo Client - Security

☑ Communication Client

Require password

□ Computer administrator → 端點管理者權限

□ Custom password

Password

Confirm password

→ 自行設置帳密

設定使用者介面

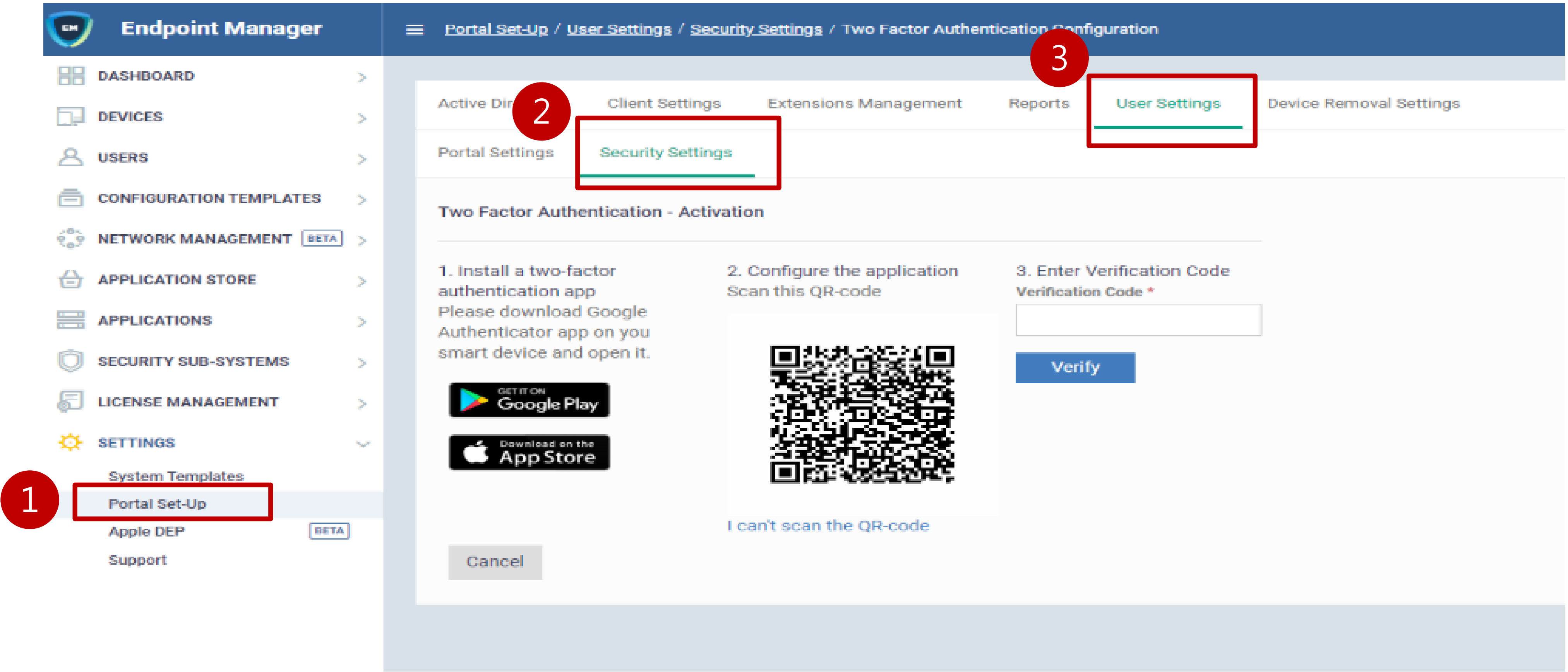
EM中央管理介面說明書

資產管理

COMODO

Creating Trust Online™

雙因子認證提升管理安全



Portal Set-Up / User Settings / Security Settings / Two Factor Authentication Configuration

Two Factor Authentication - Activation

1. Install a two-factor authentication app
Please download Google Authenticator app on you smart device and open it.

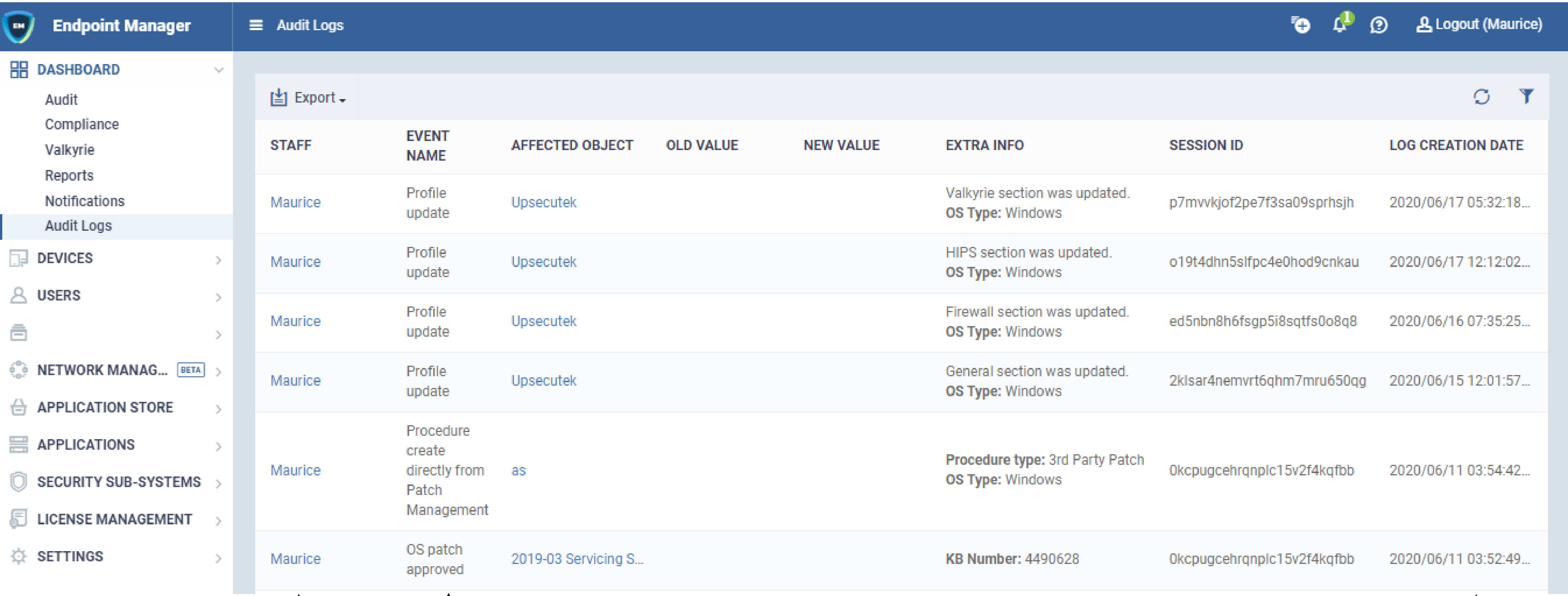
2. Configure the application
Scan this QR-code

I can't scan the QR-code

3. Enter Verification Code
Verification Code *

管理系統操作稽核紀錄

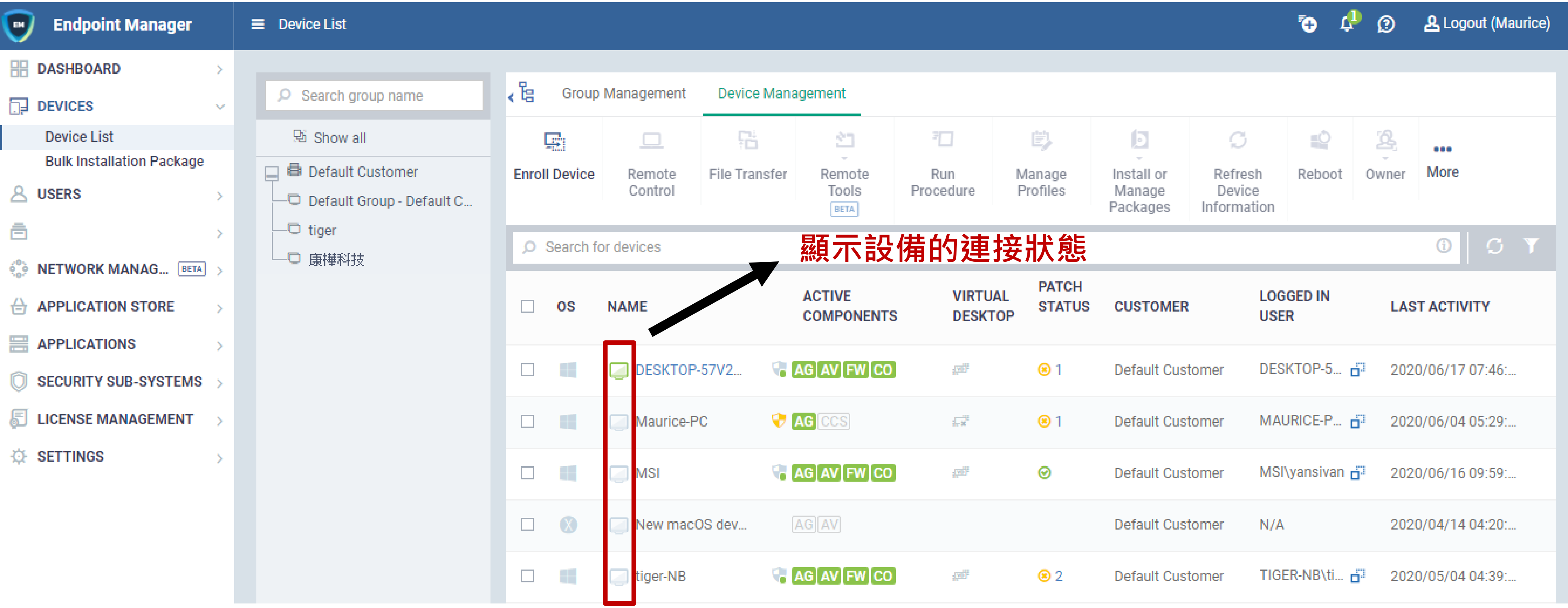
COMODO
Creating Trust Online™



STAFF	EVENT NAME	AFFECTED OBJECT	OLD VALUE	NEW VALUE	EXTRA INFO	SESSION ID	LOG CREATION DATE
Maurice	Profile update	Upsecutek			Valkyrie section was updated. **OS Type:** Windows	p7mvvkjof2pe7f3sa09sprhsjh	2020/06/17 05:32:18...
Maurice	Profile update	Upsecutek			HIPS section was updated. **OS Type:** Windows	o19t4dhn5slfpc4e0hod9cnkau	2020/06/17 12:12:02...
Maurice	Profile update	Upsecutek			Firewall section was updated. **OS Type:** Windows	ed5nbn8h6fsgp5i8sqtfs0o8q8	2020/06/16 07:35:25...
Maurice	Profile update	Upsecutek			General section was updated. **OS Type:** Windows	2klsar4nemvrt6qhm7mru650qg	2020/06/15 12:01:57...
Maurice	Procedure create directly from Patch Management	as			**Procedure type:** 3rd Party Patch **OS Type:** Windows	0kcpugcehrqnplc15v2f4kqfbb	2020/06/11 03:54:42...
Maurice	OS patch approved	2019-03 Servicing S...			**KB Number:** 4490628	0kcpugcehrqnplc15v2f4kqfbb	2020/06/11 03:52:49...

管理帳號 執行動作 時間

設備連接狀態



顯示設備的連接狀態

□	OS	NAME	ACTIVE COMPONENTS	VIRTUAL DESKTOP	PATCH STATUS	CUSTOMER	LOGGED IN USER	LAST ACTIVITY
□		DESKTOP-57V2...	AG AV FW CO		1	Default Customer	DESKTOP-5...	2020/06/17 07:46:...
□		Maurice-PC	AG CCS		1	Default Customer	MAURICE-P...	2020/06/04 05:29:...
□		MSI	AG AV FW CO		✓	Default Customer	MSI\yansivan	2020/06/16 09:59:...
□	X	New macOS dev...	AG AV			Default Customer	N/A	2020/04/14 04:20:...
□		tiger-NB	AG AV FW CO		2	Default Customer	TIGER-NB\ti...	2020/05/04 04:39:...

設備無法訪問。連接可能已斷開或端點已關閉。

連接緩慢。設備已連接，但是由於端點繁忙，命令和消息可能要花一些時間才能執行。

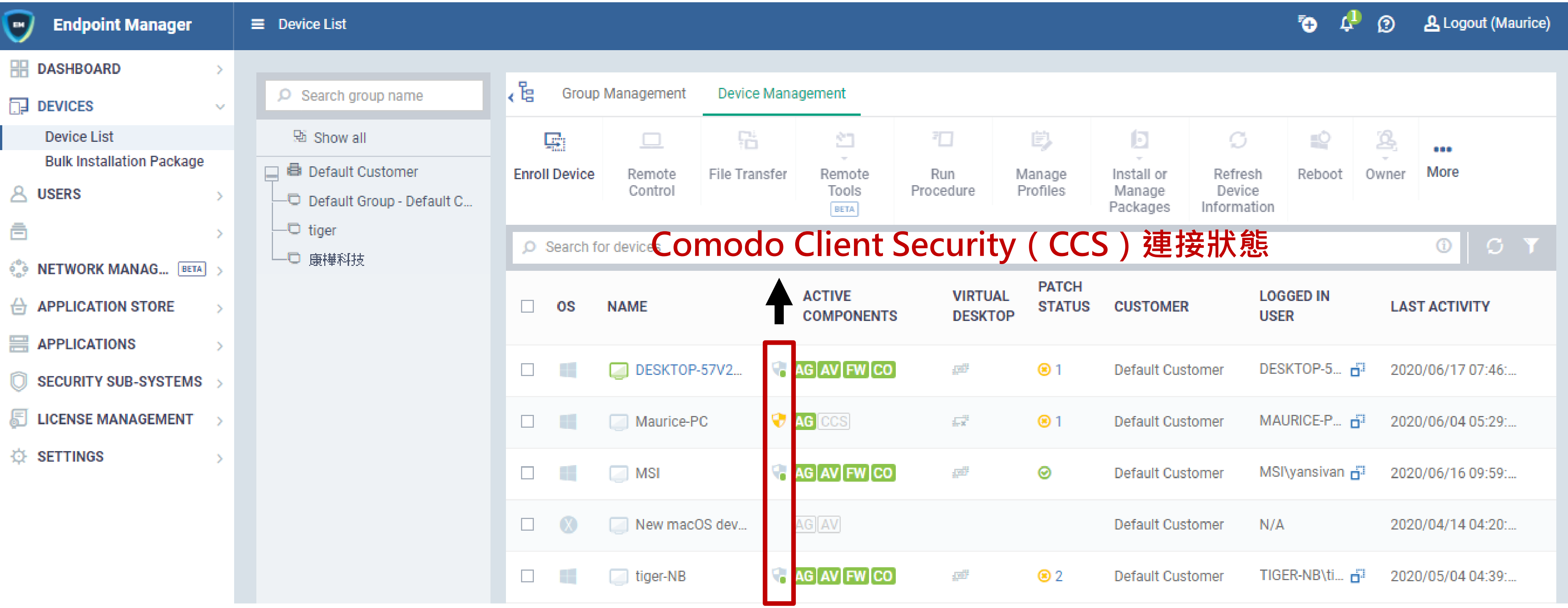
良好的聯繫。命令應實時執行。

如果設備在一定天數內未連接到EM，則將其標記為“old”。

該設備是重複的。僅適用於Windows設備。

Comodo Client Security連線狀態

COMODO
Creating Trust Online™



Comodo Client Security（CCS）連接狀態

□	OS	NAME		ACTIVE COMPONENTS	VIRTUAL DESKTOP	PATCH STATUS	CUSTOMER	LOGGED IN USER	LAST ACTIVITY
□		DESKTOP-57V2...		AG AV FW CO		1	Default Customer	DESKTOP-5...	2020/06/17 07:46:...
□		Maurice-PC		AG CCS		1	Default Customer	MAURICE-P...	2020/06/04 05:29:...
□		MSI		AG AV FW CO		✓	Default Customer	MSI\yansivan	2020/06/16 09:59:...
□		New macOS dev...		AG AV			Default Customer	N/A	2020/04/14 04:20:...
□		tiger-NB		AG AV FW CO		2	Default Customer	TIGER-NB\ti...	2020/05/04 04:39:...

黃色--端點上未安裝CCS。

灰色 -- 過時的客戶。端點上的Communication Client和/或Comodo Client Security需要更新。

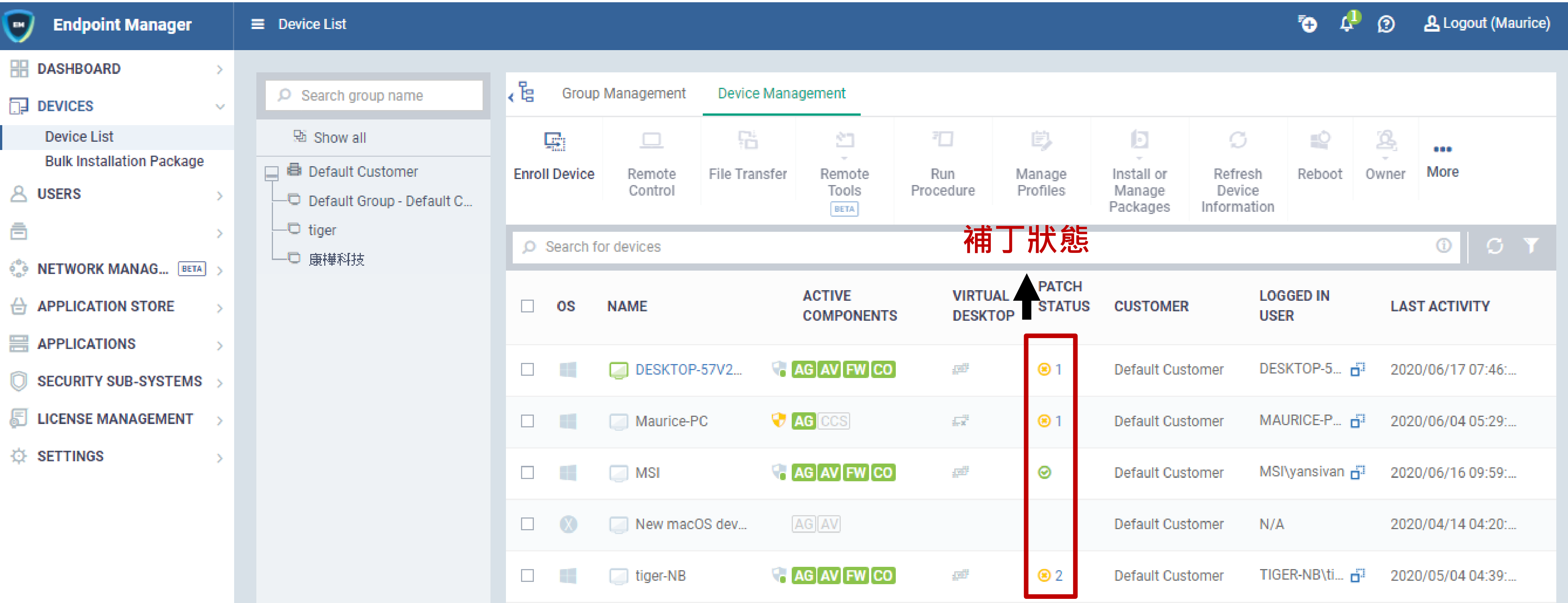
紅色--端點有風險。用戶可能已禁用了一個或多個安全組件（AV，FW)。

琥珀色--端點需要注意。安裝CCS後，病毒庫可能已過時，或者需要重新啟動端點。

綠色--端點是安全的。所有已安裝的組件均已啟動並正在運行。

藍色--CCS處於“靜音模式”。

補丁狀態



補丁狀態

☐	OS	NAME	ACTIVE COMPONENTS	VIRTUAL DESKTOP	PATCH STATUS	CUSTOMER	LOGGED IN USER	LAST ACTIVITY
☐		DESKTOP-57V2...	AG AV FW CO		⊗ 1	Default Customer	DESKTOP-5...	2020/06/17 07:46:...
☐		Maurice-PC	AG CCS		⊗ 1	Default Customer	MAURICE-P...	2020/06/04 05:29:...
☐		MSI	AG AV FW CO		✓	Default Customer	MSI\yansivan	2020/06/16 09:59:...
☐	X	New macOS dev...	AG AV			Default Customer	N/A	2020/04/14 04:20:...
☐		tiger-NB	AG AV FW CO		⊗ 2	Default Customer	TIGER-NB\ti...	2020/05/04 04:39:...

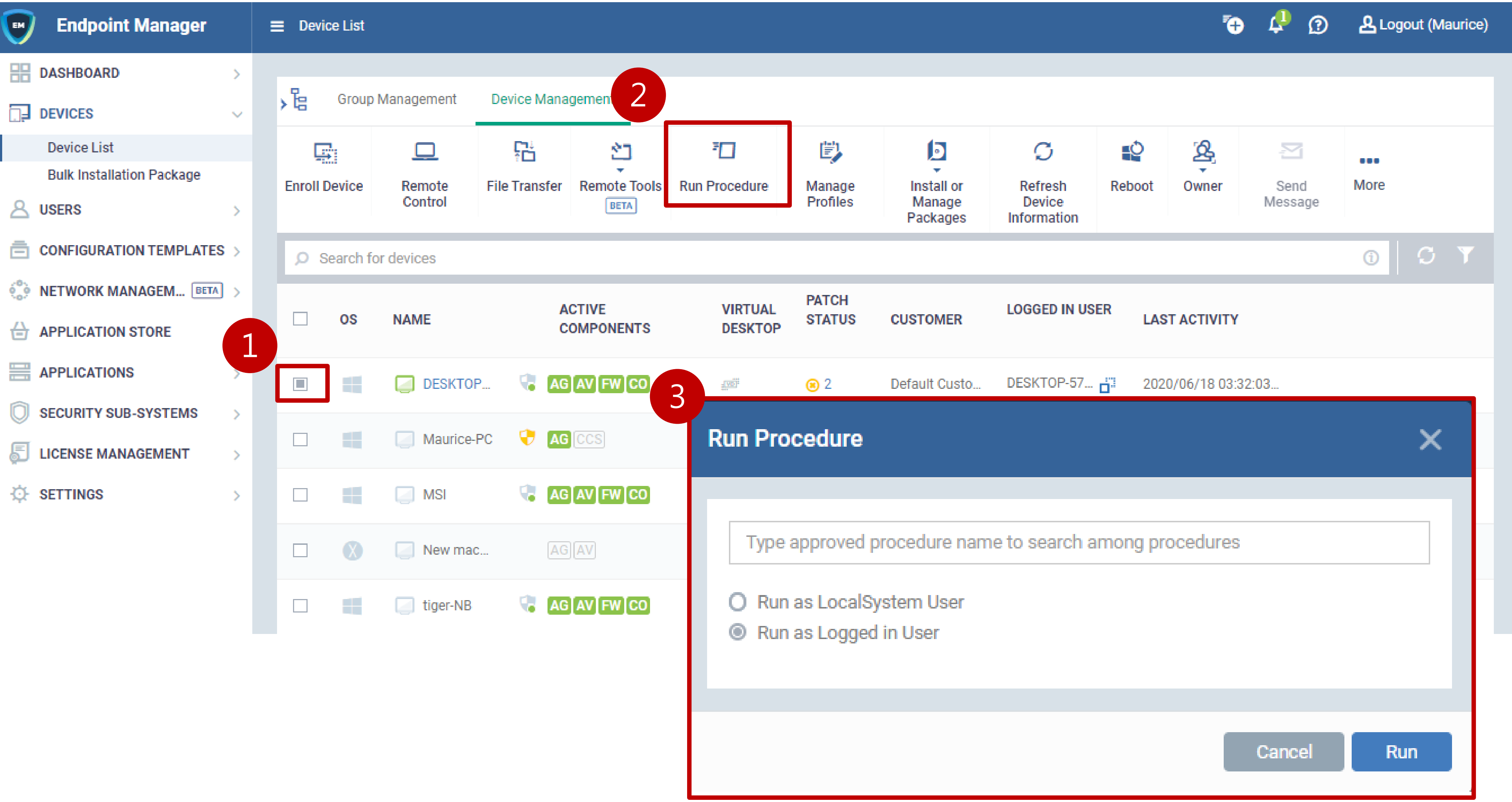
✓ 無需補丁。所有補丁都是最新的。

⚠ 可選補丁可用。單擊右側的數字以查看和管理補丁。

⊗ 重要補丁可用。

軟體派送

COMODO
Creating Trust Online™



□	OS	NAME	ACTIVE COMPONENTS	VIRTUAL DESKTOP	PATCH STATUS	CUSTOMER	LOGGED IN USER	LAST ACTIVITY
☒		DESKTOP...	AG AV FW CO		2	Default Custo...	DESKTOP-57...	2020/06/18 03:32:03...
□		Maurice-PC	AG CCS					
□		MSI	AG AV FW CO					
□		New mac...	AG AV					
□		tiger-NB	AG AV FW CO					

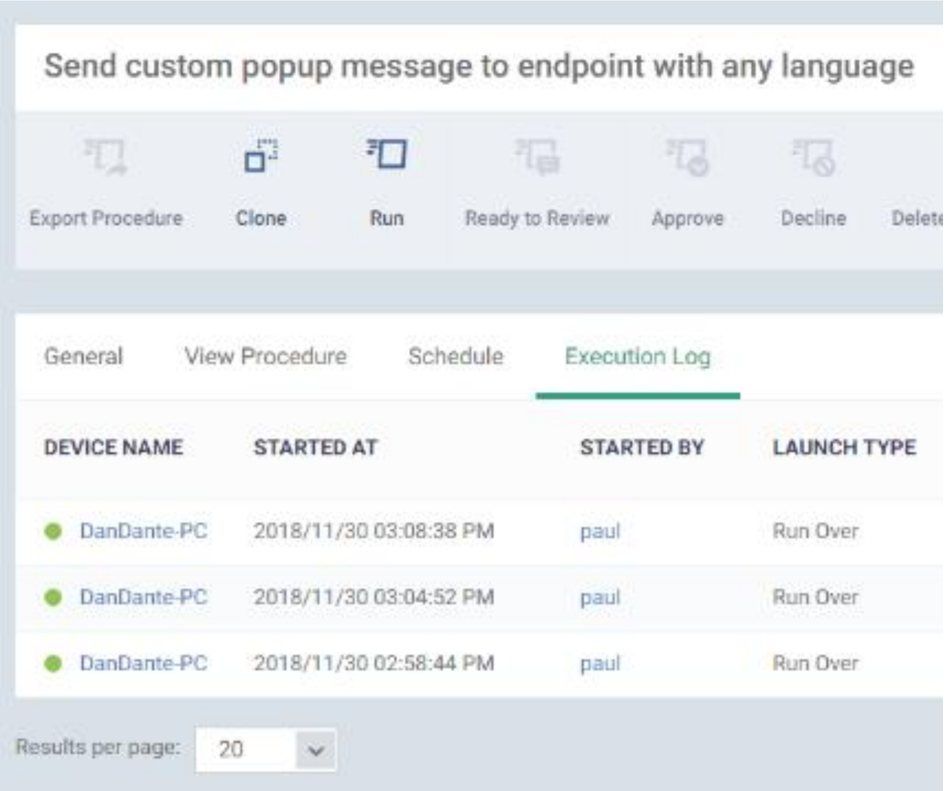
Run Procedure

Type approved procedure name to search among procedures

○ Run as LocalSystem User

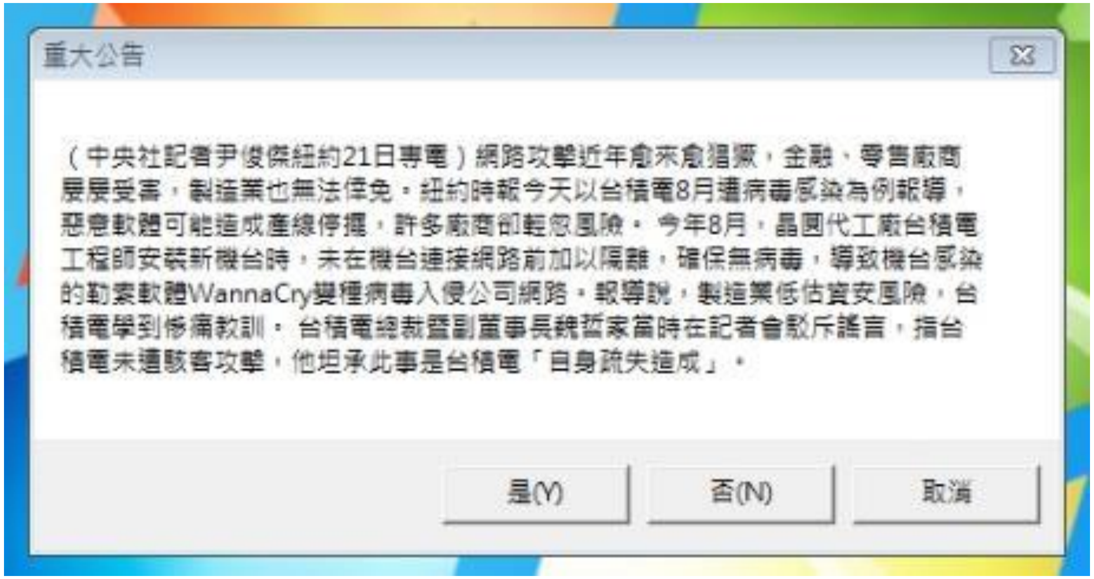
● Run as Logged in User

公司訊息POP-UP通知



Send custom popup message to endpoint with any language

DEVICE NAME	STARTED AT	STARTED BY	LAUNCH TYPE
● DanDante-PC	2018/11/30 03:08:38 PM	paul	Run Over
● DanDante-PC	2018/11/30 03:04:52 PM	paul	Run Over
● DanDante-PC	2018/11/30 02:58:44 PM	paul	Run Over

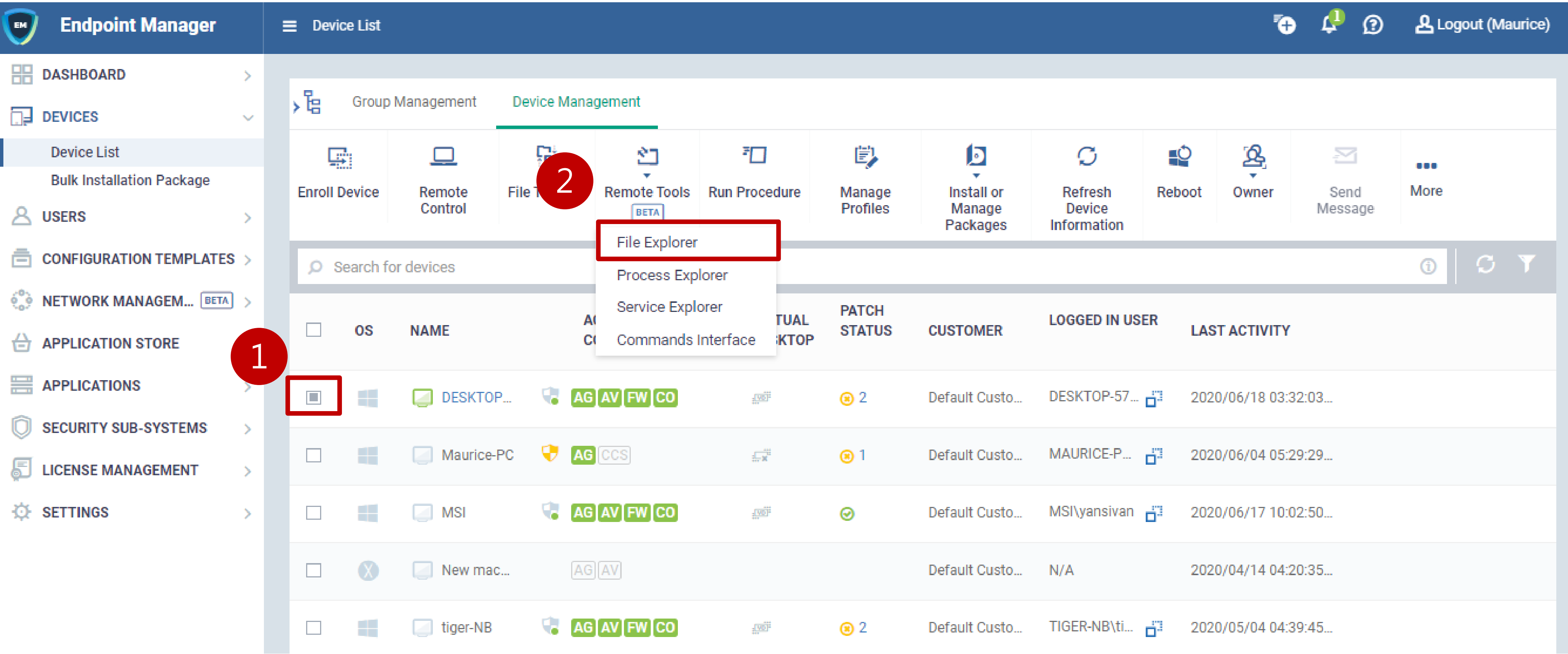


重大公告

（中央社記者尹俊傑紐約21日專電）網路攻擊近年愈來愈猖獗，金融、零售廠商屢屢受害，製造業也無法倖免。紐約時報今天以台積電8月遭病毒感染為例報導，惡意軟體可能造成產線停擺，許多廠商卻輕忽風險。 今年8月，晶圓代工廠台積電工程師安裝新機台時，未在機台連接網路前加以隔離，確保無病毒，導致機台感染的勒索軟體WannaCry變種病毒入侵公司網路。報導說，製造業低估資安風險，台積電學到慘痛教訓。 台積電總裁暨副董事長魏哲家當時在記者會駁斥謠言，指台積電未遭駭客攻擊，他坦承此事是台積電「自身疏失造成」。

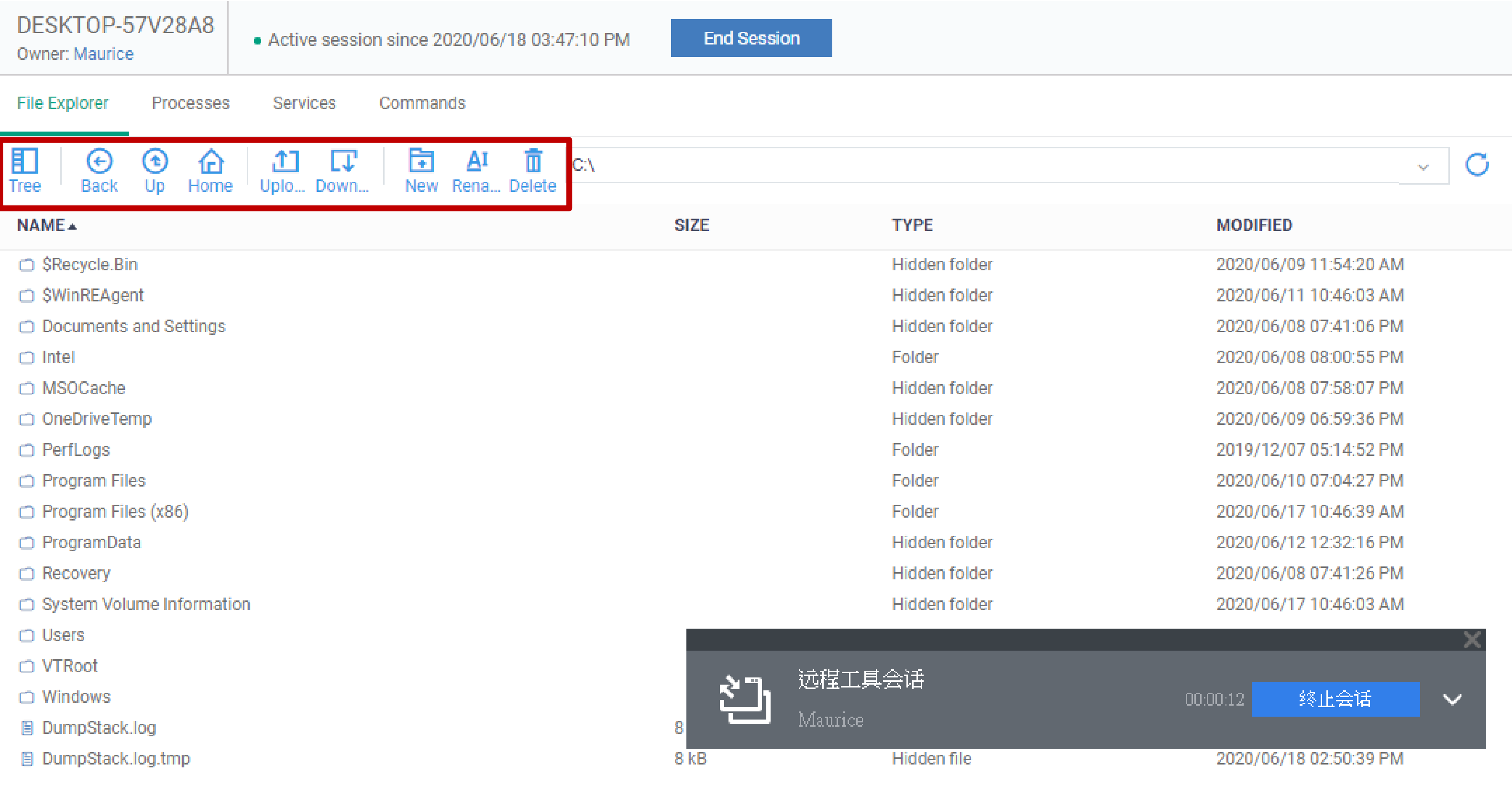
透過Procedures派送通知
標題與訊息內容可自定

遠端管理設備上文件夾和文件



□	OS	NAME	A C	TUAL KTOP	PATCH STATUS	CUSTOMER	LOGGED IN USER	LAST ACTIVITY
▣		DESKTOP...	AG AV FW CO		2	Default Custo...	DESKTOP-57...	2020/06/18 03:32:03...
□		Maurice-PC	AG CCS		1	Default Custo...	MAURICE-P...	2020/06/04 05:29:29...
□		MSI	AG AV FW CO		✓	Default Custo...	MSI\yansivan	2020/06/17 10:02:50...
□		New mac...	AG AV			Default Custo...	N/A	2020/04/14 04:20:35...
□		tiger-NB	AG AV FW CO		2	Default Custo...	TIGER-NB\ti...	2020/05/04 04:39:45...

File Explorer 工具列介紹



DESKTOP-57V28A8
Owner: Maurice

● Active session since 2020/06/18 03:47:10 PM

End Session

NAME ▲	SIZE	TYPE	MODIFIED
$Recycle.Bin		Hidden folder	2020/06/09 11:54:20 AM
$WinREAgent		Hidden folder	2020/06/11 10:46:03 AM
Documents and Settings		Hidden folder	2020/06/08 07:41:06 PM
Intel		Folder	2020/06/08 08:00:55 PM
MSOCache		Hidden folder	2020/06/08 07:58:07 PM
OneDriveTemp		Hidden folder	2020/06/09 06:59:36 PM
PerfLogs		Folder	2019/12/07 05:14:52 PM
Program Files		Folder	2020/06/10 07:04:27 PM
Program Files (x86)		Folder	2020/06/17 10:46:39 AM
ProgramData		Hidden folder	2020/06/12 12:32:16 PM
Recovery		Hidden folder	2020/06/08 07:41:26 PM
System Volume Information		Hidden folder	2020/06/17 10:46:03 AM
Users			
VTRoot			
Windows			
DumpStack.log	8		
DumpStack.log.tmp	8 kB	Hidden file	2020/06/18 02:50:39 PM

远程工具会话
Maurice
00:00:12
終止会话

Tree 在樹形視圖和列表視圖之間切換

Back 返回上一個位置

Up 向上一級文件夾樹

Home 轉到所選驅動器/分區的根文件夾

Upload 將文件/文件夾從您的電腦傳輸到遠程設備

Download 從遠程設備將選定的文件/文件夾複製到您的電腦

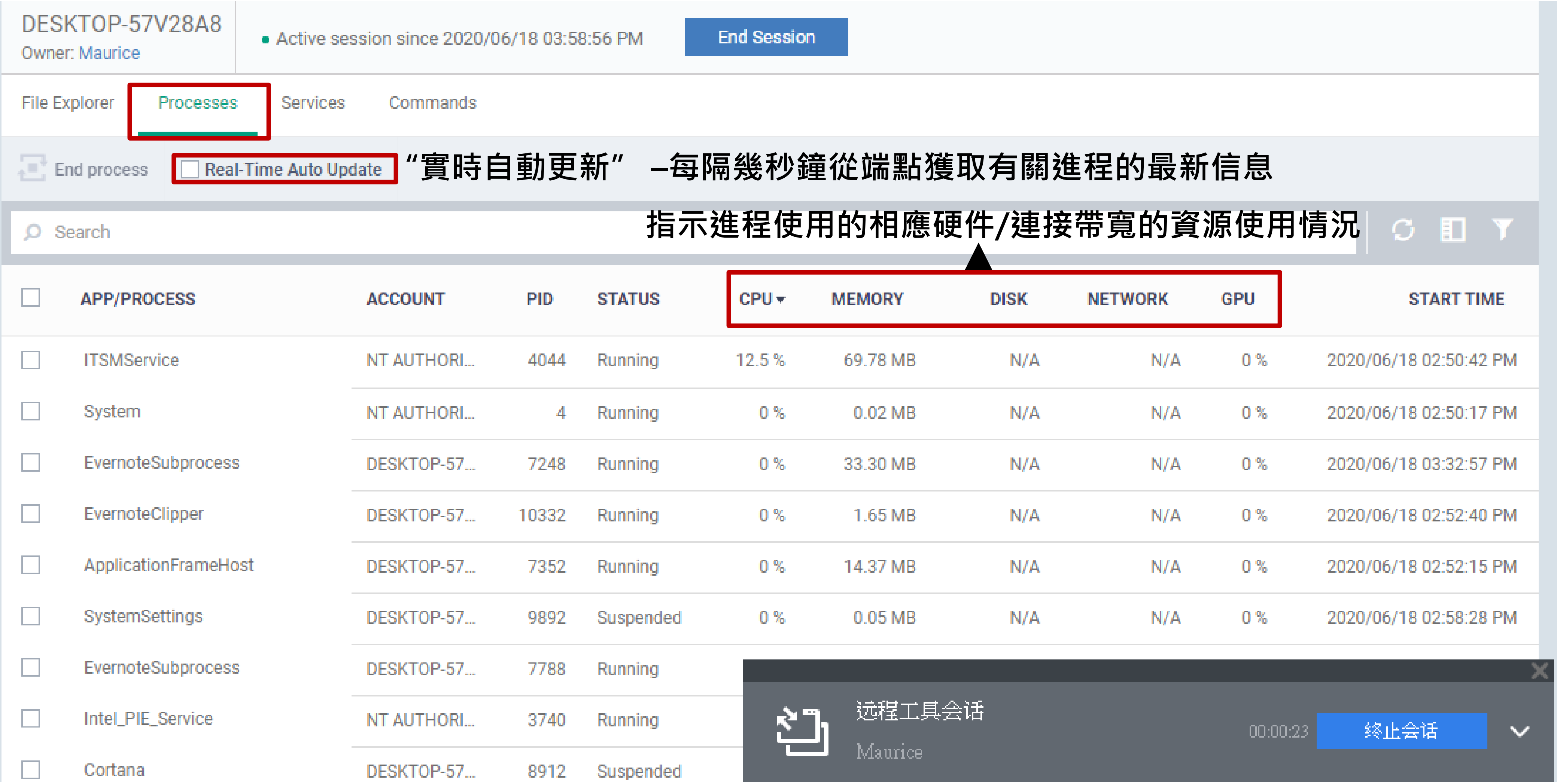
New 在遠程設備上創建一個新文件夾

Rename 為遠程設備上的文件/文件夾設置新名稱

刷新當前文件夾的內容

Delete 從遠程設備中刪除不需要的項目

Processes Explorer工具列介紹



DESKTOP-57V28A8
Owner: Maurice

● Active session since 2020/06/18 03:58:56 PM

□ Real-Time Auto Update

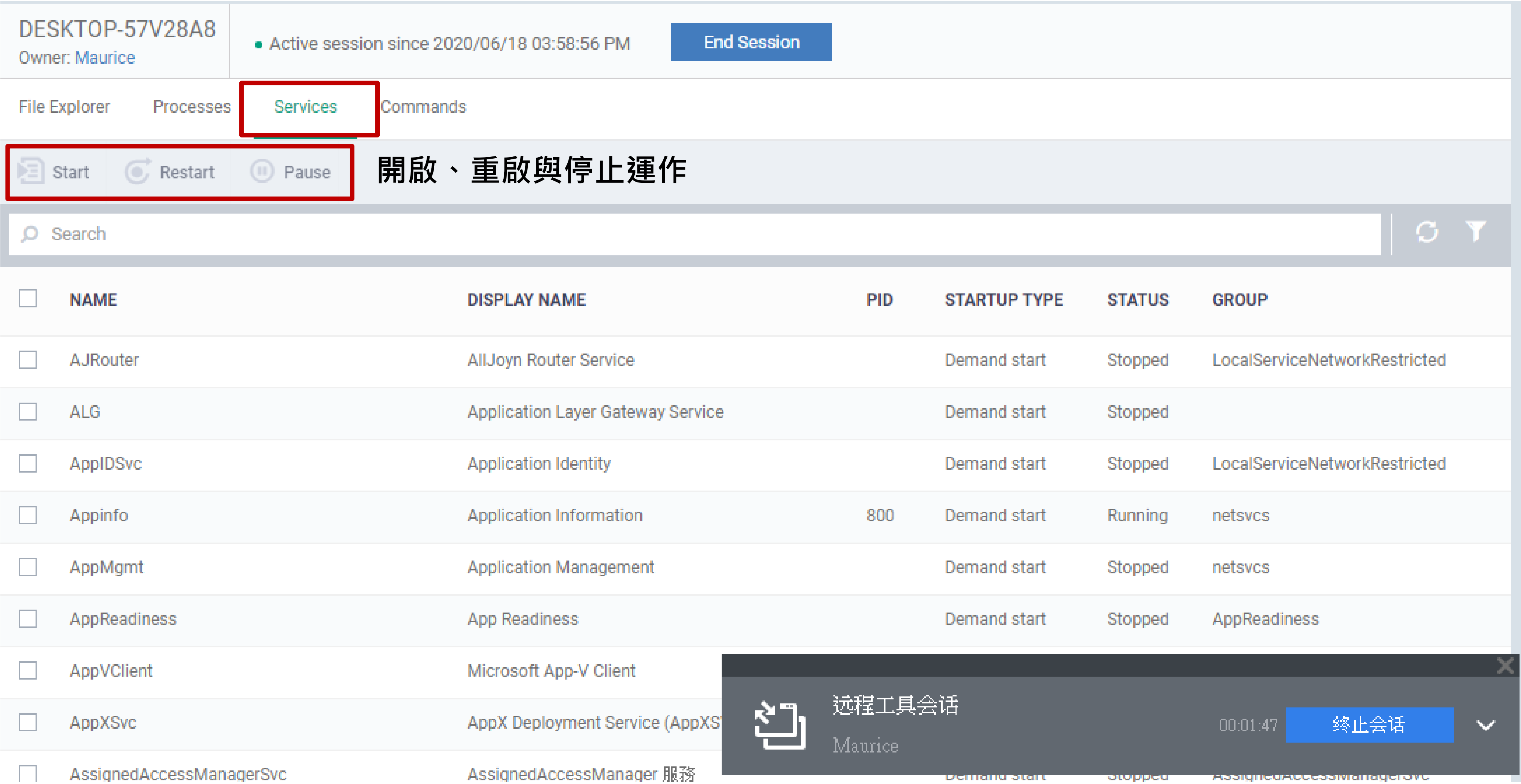
"實時自動更新" –每隔幾秒鐘從端點獲取有關進程的最新信息

指示進程使用的相應硬件/連接帶寬的資源使用情況

□	APP/PROCESS	ACCOUNT	PID	STATUS	CPU ▾	MEMORY	DISK	NETWORK	GPU	START TIME
□	ITSMService	NT AUTHORI...	4044	Running	12.5 %	69.78 MB	N/A	N/A	0 %	2020/06/18 02:50:42 PM
□	System	NT AUTHORI...	4	Running	0 %	0.02 MB	N/A	N/A	0 %	2020/06/18 02:50:17 PM
□	EvernoteSubprocess	DESKTOP-57...	7248	Running	0 %	33.30 MB	N/A	N/A	0 %	2020/06/18 03:32:57 PM
□	EvernoteClipper	DESKTOP-57...	10332	Running	0 %	1.65 MB	N/A	N/A	0 %	2020/06/18 02:52:40 PM
□	ApplicationFrameHost	DESKTOP-57...	7352	Running	0 %	14.37 MB	N/A	N/A	0 %	2020/06/18 02:52:15 PM
□	SystemSettings	DESKTOP-57...	9892	Suspended	0 %	0.05 MB	N/A	N/A	0 %	2020/06/18 02:58:28 PM
□	EvernoteSubprocess	DESKTOP-57...	7788	Running						
□	Intel_PIE_Service	NT AUTHORI...	3740	Running						
□	Cortana	DESKTOP-57...	8912	Suspended						

远程工具会话
Maurice
00:00:23

Service Explorer工具列介紹



DESKTOP-57V28A8
Owner: Maurice

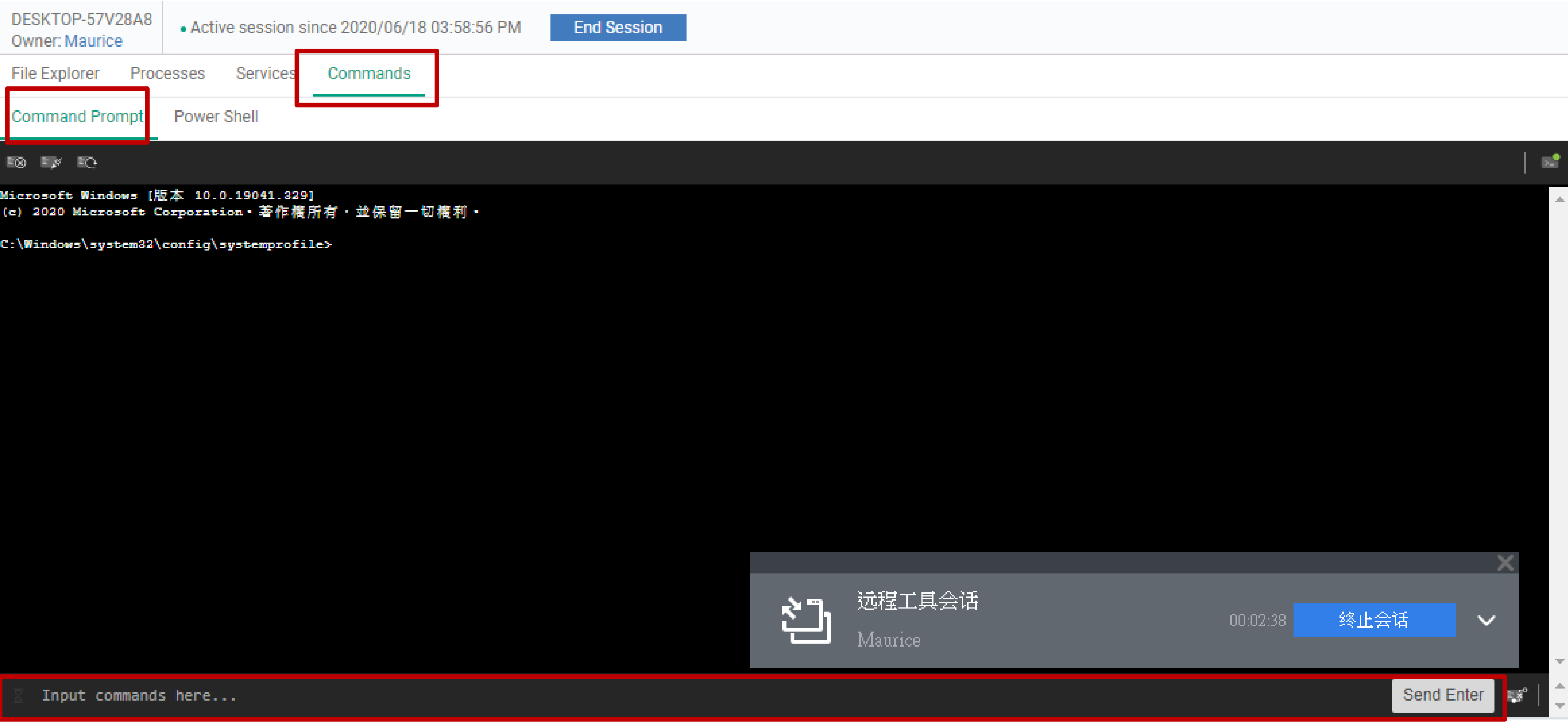
● Active session since 2020/06/18 03:58:56 PM

開啟、重啟與停止運作

□	NAME	DISPLAY NAME	PID	STARTUP TYPE	STATUS	GROUP
□	AJRouter	AllJoyn Router Service		Demand start	Stopped	LocalServiceNetworkRestricted
□	ALG	Application Layer Gateway Service		Demand start	Stopped	
□	AppIDSvc	Application Identity		Demand start	Stopped	LocalServiceNetworkRestricted
□	Appinfo	Application Information	800	Demand start	Running	netsvcs
□	AppMgmt	Application Management		Demand start	Stopped	netsvcs
□	AppReadiness	App Readiness		Demand start	Stopped	AppReadiness
□	AppVClient	Microsoft App-V Client				
□	AppXSvc	AppX Deployment Service (AppXS				
□	AssignedAccessManagerSvc	AssignedAccessManager 服務		Demand start	Stopped	AssignedAccessManagerSvc

远程工具会话
Maurice
00:01:47

Command Prompt工具列介紹



DESKTOP-57V28A8
Owner: Maurice

• Active session since 2020/06/18 03:58:56 PM

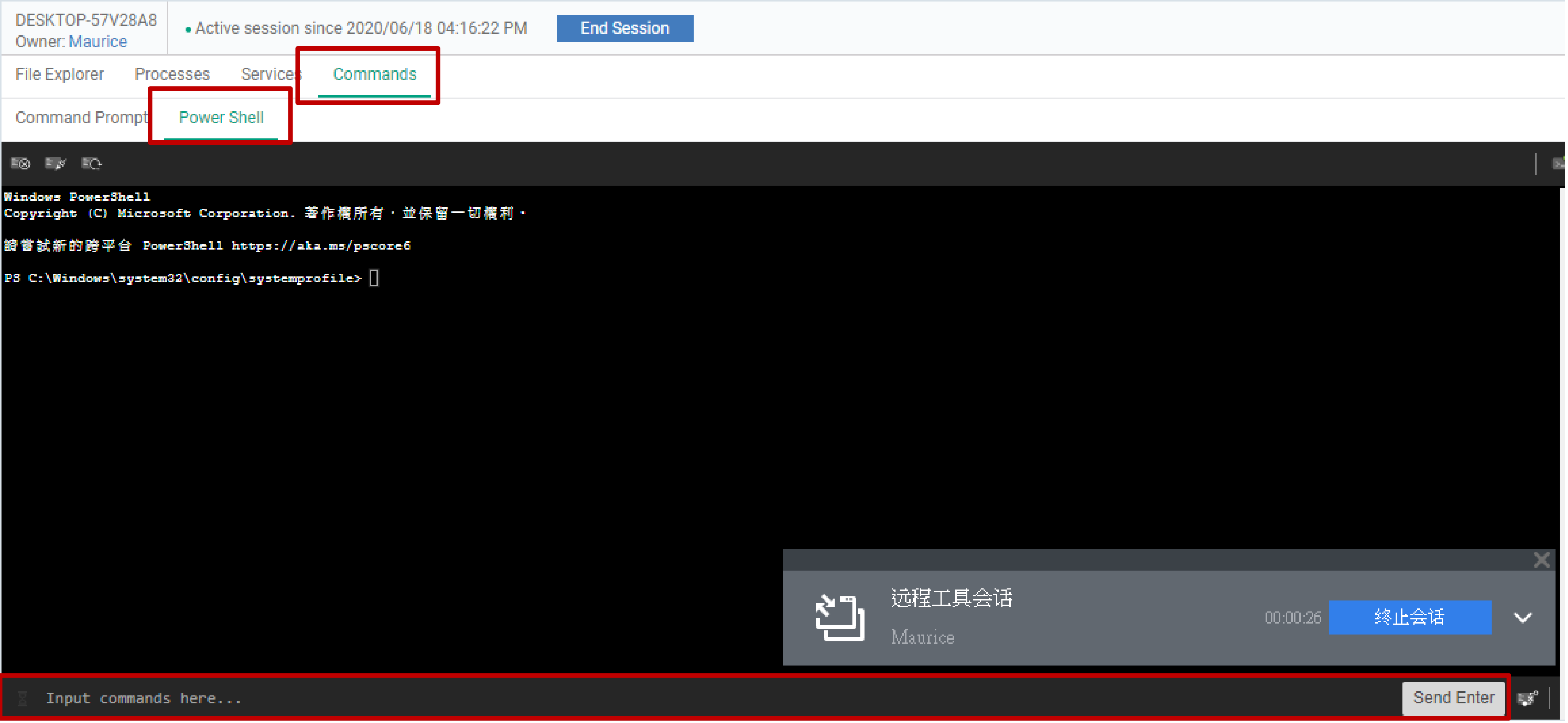
```
Microsoft Windows [版本 10.0.19041.329]
(c) 2020 Microsoft Corporation・著作權所有・並保留一切權利・

C:\Windows\system32\config\systemprofile>
```

远程工具会话
Maurice
00:02:38

根據需要在遠程計算機上運行命令行

Power Shell工具列介紹



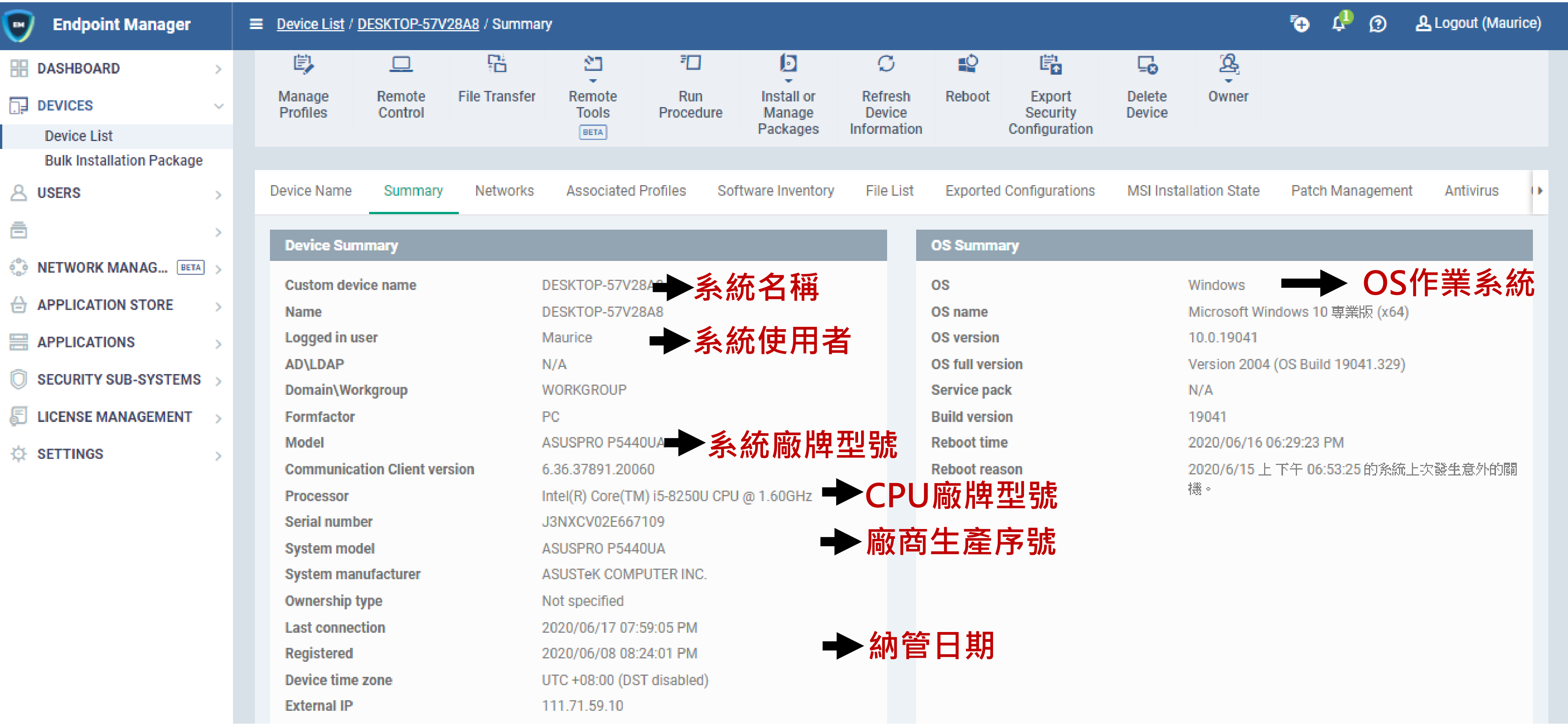
```
Windows PowerShell
Copyright (C) Microsoft Corporation. 著作權所有，並保留一切權利。

請嘗試新的跨平台 PowerShell https://aka.ms/pscore6

PS C:\Windows\system32\config\systemprofile> 
```

根據需要在遠程計算機上運行Power Shell命令行

系統環境資訊



Device Summary

Custom device name	DESKTOP-57V28A8
Name	DESKTOP-57V28A8
Logged in user	Maurice
AD\LDAP	N/A
Domain\Workgroup	WORKGROUP
Formfactor	PC
Model	ASUSPRO P5440UA
Communication Client version	6.36.37891.20060
Processor	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz
Serial number	J3NXCV02E667109
System model	ASUSPRO P5440UA
System manufacturer	ASUSTeK COMPUTER INC.
Ownership type	Not specified
Last connection	2020/06/17 07:59:05 PM
Registered	2020/06/08 08:24:01 PM
Device time zone	UTC +08:00 (DST disabled)
External IP	111.71.59.10

OS Summary

OS	Windows
OS name	Microsoft Windows 10 專業版 (x64)
OS version	10.0.19041
OS full version	Version 2004 (OS Build 19041.329)
Service pack	N/A
Build version	19041
Reboot time	2020/06/16 06:29:23 PM
Reboot reason	2020/6/15 上 下午 06:53:25 的系統上次發生意外的關機。

系統名稱

系統使用者

系統廠牌型號

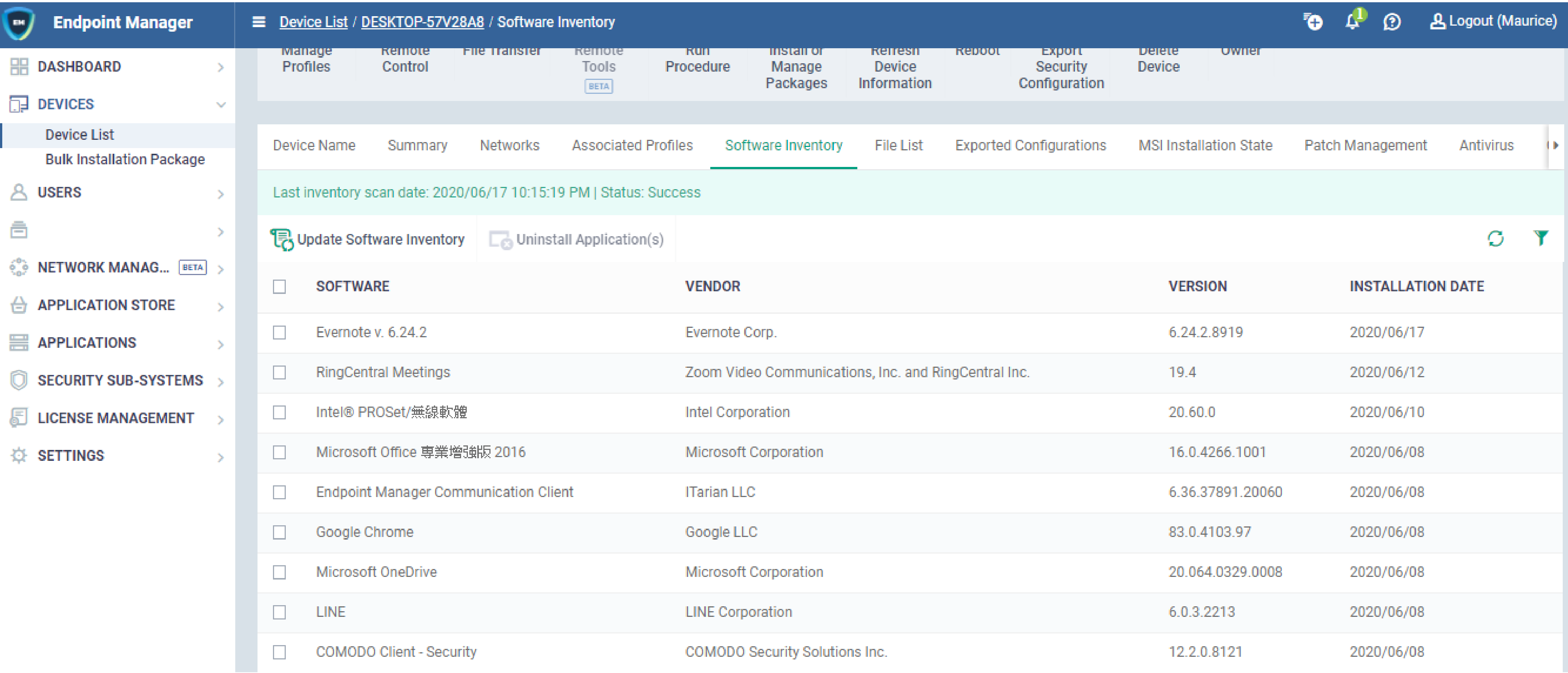
CPU廠牌型號

廠商生產序號

納管日期

OS作業系統

系統軟體安裝資訊

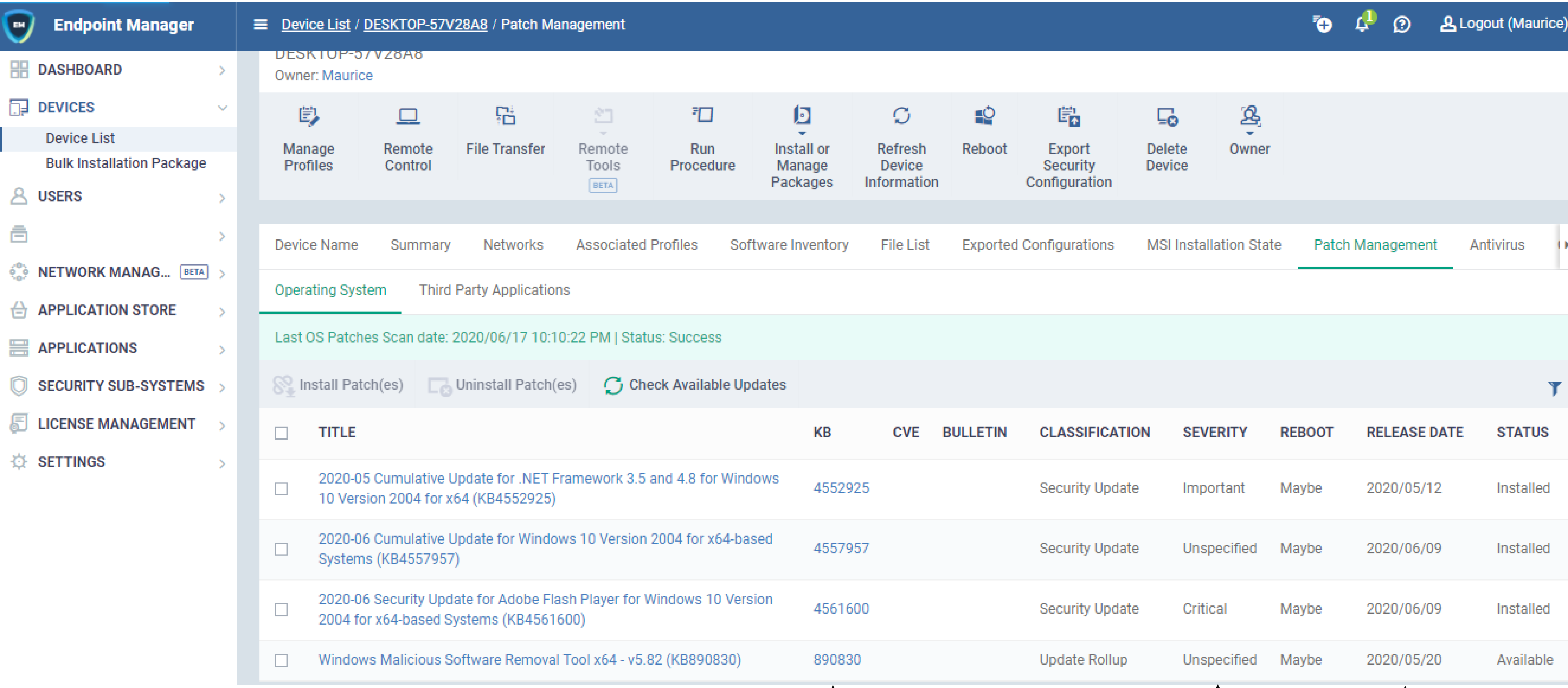


Last inventory scan date: 2020/06/17 10:15:19 PM | Status: Success

□	SOFTWARE	VENDOR	VERSION	INSTALLATION DATE
□	Evernote v. 6.24.2	Evernote Corp.	6.24.2.8919	2020/06/17
□	RingCentral Meetings	Zoom Video Communications, Inc. and RingCentral Inc.	19.4	2020/06/12
□	Intel® PROSet/無線軟體	Intel Corporation	20.60.0	2020/06/10
□	Microsoft Office 專業增強版 2016	Microsoft Corporation	16.0.4266.1001	2020/06/08
□	Endpoint Manager Communication Client	ITarian LLC	6.36.37891.20060	2020/06/08
□	Google Chrome	Google LLC	83.0.4103.97	2020/06/08
□	Microsoft OneDrive	Microsoft Corporation	20.064.0329.0008	2020/06/08
□	LINE	LINE Corporation	6.0.3.2213	2020/06/08
□	COMODO Client - Security	COMODO Security Solutions Inc.	12.2.0.8121	2020/06/08

軟體名稱　　軟體發行商　　軟體版本　　軟體安裝日期

Windows Update 系統補丁管理



Device List / DESKTOP-57V28A8 / Patch Management

DESKTOP-57V28A8
Owner: Maurice

Last OS Patches Scan date: 2020/06/17 10:10:22 PM | Status: Success

□	TITLE	KB	CVE	BULLETIN	CLASSIFICATION	SEVERITY	REBOOT	RELEASE DATE	STATUS
□	2020-05 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 2004 for x64 (KB4552925)	4552925			Security Update	Important	Maybe	2020/05/12	Installed
□	2020-06 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB4557957)	4557957			Security Update	Unspecified	Maybe	2020/06/09	Installed
□	2020-06 Security Update for Adobe Flash Player for Windows 10 Version 2004 for x64-based Systems (KB4561600)	4561600			Security Update	Critical	Maybe	2020/06/09	Installed
□	Windows Malicious Software Removal Tool x64 - v5.82 (KB890830)	890830			Update Rollup	Unspecified	Maybe	2020/05/20	Available

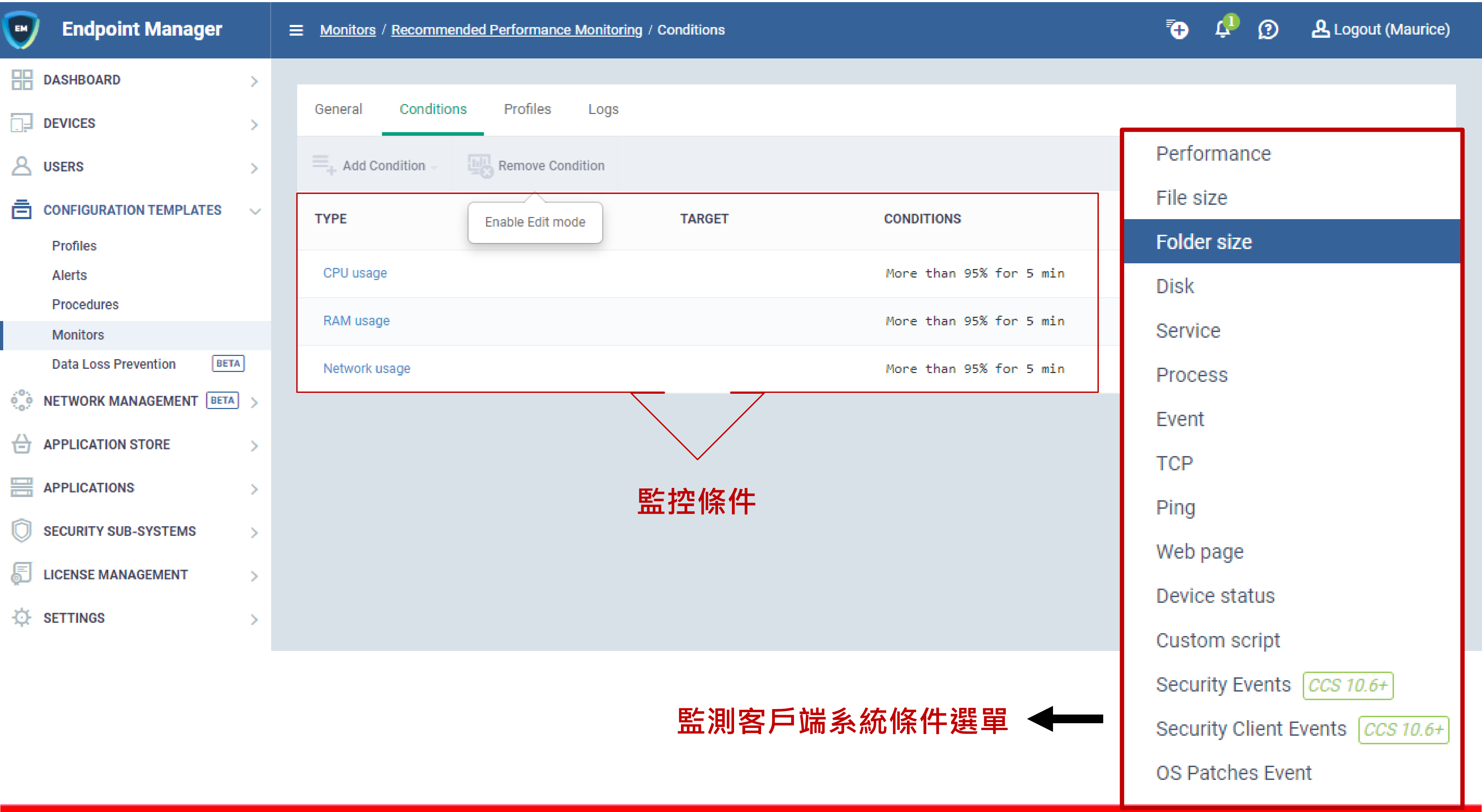
系統補丁KB

安全等級

釋出日期

系統效能監控

COMODO
Creating Trust Online™



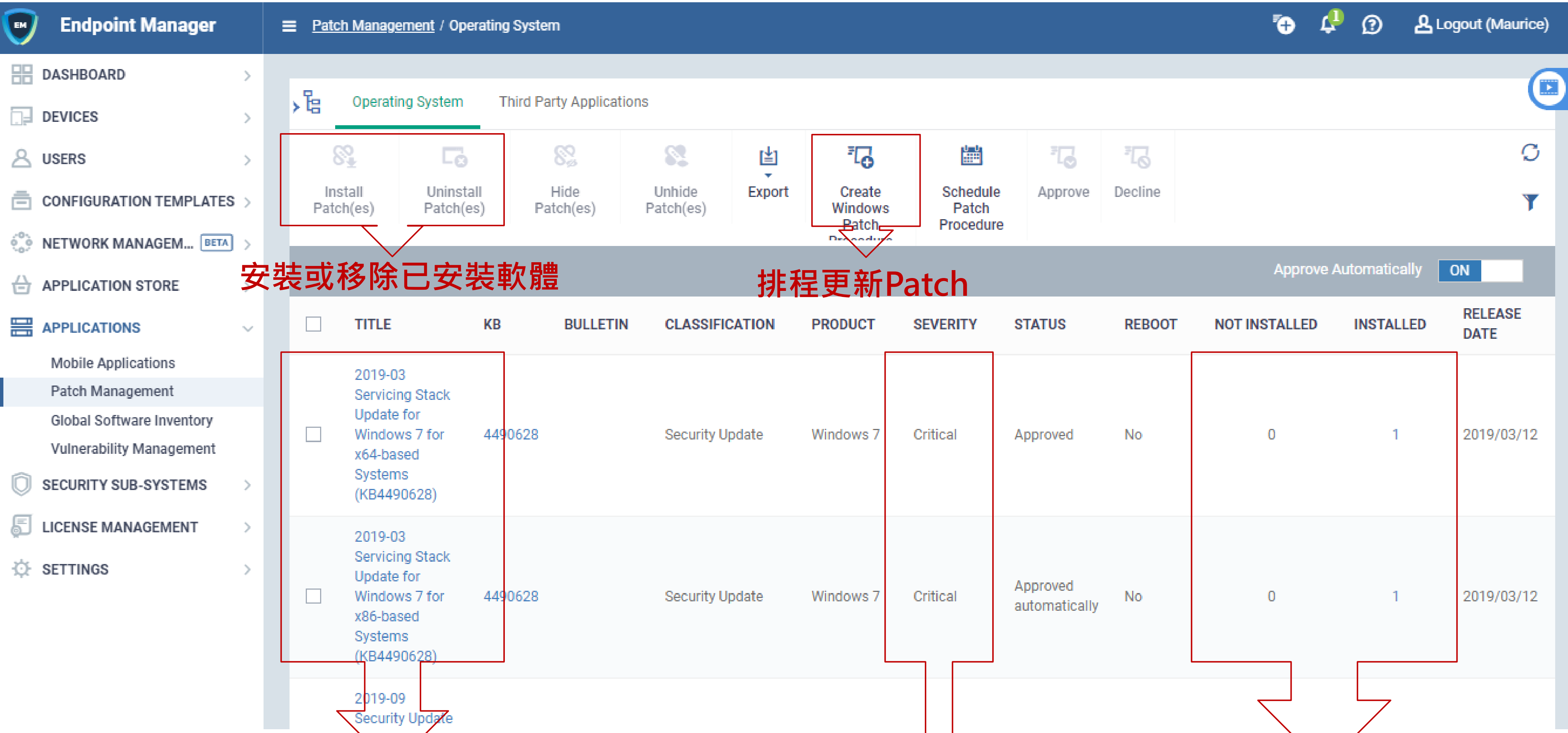
TYPE	TARGET	CONDITIONS
CPU usage		More than 95% for 5 min
RAM usage		More than 95% for 5 min
Network usage		More than 95% for 5 min

監控條件

監測客戶端系統條件選單

公司端點系統Patch安裝狀態統計

COMODO
Creating Trust Online™



安裝或移除已安裝軟體

排程更新Patch

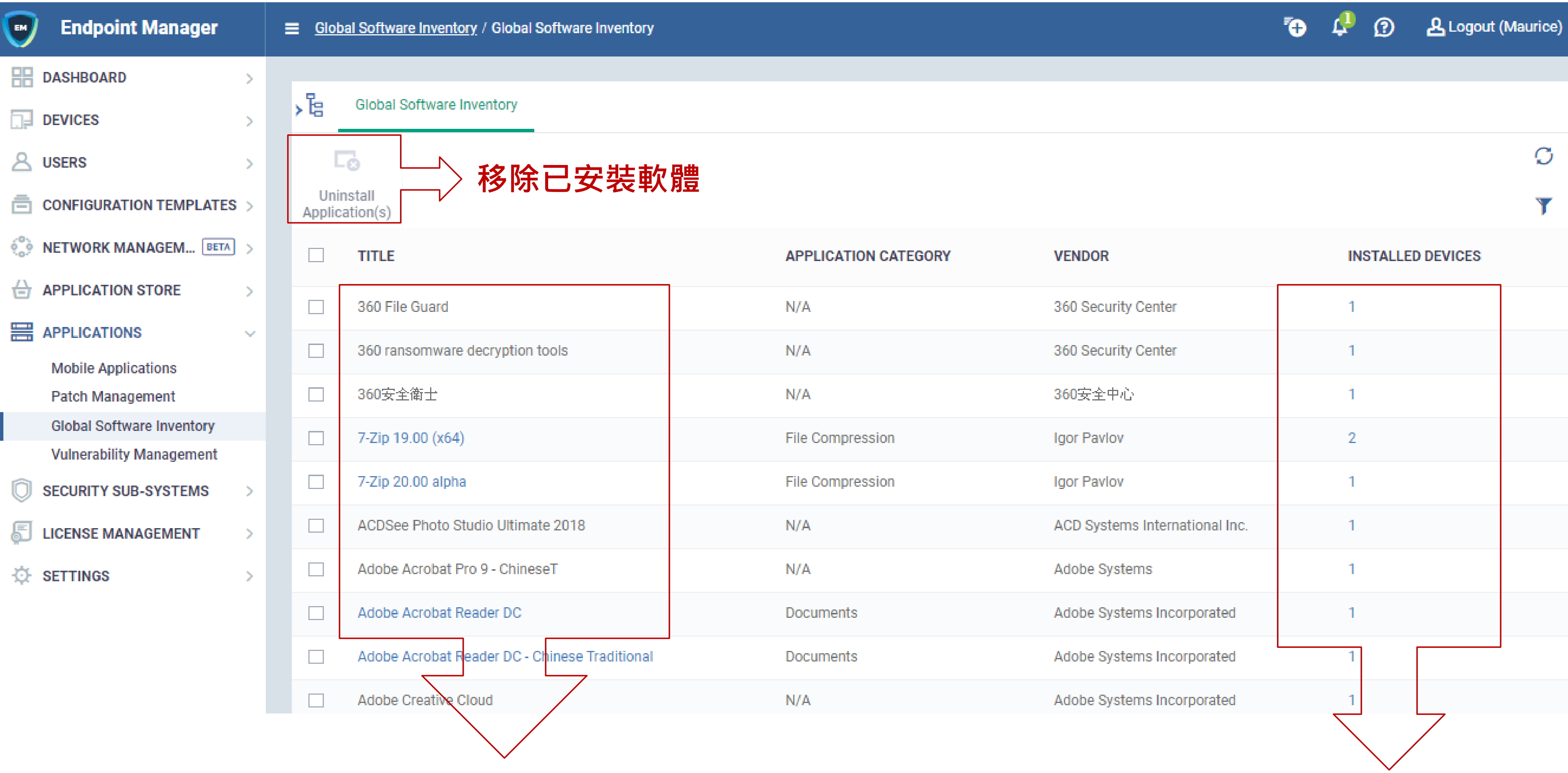
□	TITLE	KB	BULLETIN	CLASSIFICATION	PRODUCT	SEVERITY	STATUS	REBOOT	NOT INSTALLED	INSTALLED	RELEASE DATE
□	2019-03 Servicing Stack Update for Windows 7 for x64-based Systems (KB4490628)	4490628		Security Update	Windows 7	Critical	Approved	No	0	1	2019/03/12
□	2019-03 Servicing Stack Update for Windows 7 for x86-based Systems (KB4490628)	4490628		Security Update	Windows 7	Critical	Approved automatically	No	0	1	2019/03/12
	2019-09 Security Update										

Patch名稱

等級

安裝統計狀態

公司軟體使用統計



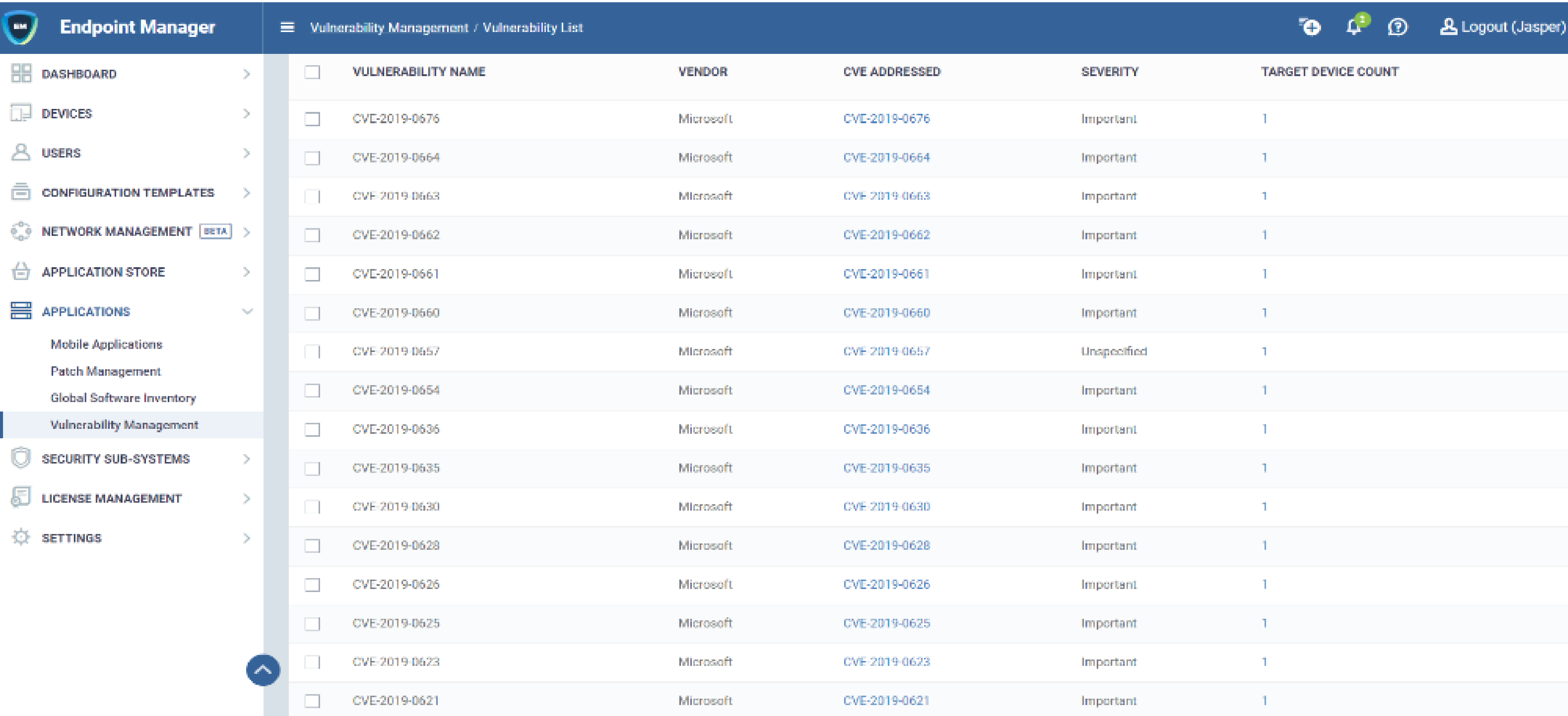
移除已安裝軟體

□	TITLE	APPLICATION CATEGORY	VENDOR	INSTALLED DEVICES
□	360 File Guard	N/A	360 Security Center	1
□	360 ransomware decryption tools	N/A	360 Security Center	1
□	360安全衛士	N/A	360安全中心	1
□	7-Zip 19.00 (x64)	File Compression	Igor Pavlov	2
□	7-Zip 20.00 alpha	File Compression	Igor Pavlov	1
□	ACDSee Photo Studio Ultimate 2018	N/A	ACD Systems International Inc.	1
□	Adobe Acrobat Pro 9 - ChineseT	N/A	Adobe Systems	1
□	Adobe Acrobat Reader DC	Documents	Adobe Systems Incorporated	1
□	Adobe Acrobat Reader DC - Chinese Traditional	Documents	Adobe Systems Incorporated	1
□	Adobe Creative Cloud	N/A	Adobe Systems Incorporated	1

已安裝軟體

已安裝數量

系統弱點風險管理



□	VULNERABILITY NAME	VENDOR	CVE ADDRESSED	SEVERITY	TARGET DEVICE COUNT
□	CVE-2019-0676	Microsoft	CVE-2019-0676	Important	1
□	CVE-2019-0664	Microsoft	CVE-2019-0664	Important	1
□	CVE-2019-0663	Microsoft	CVE-2019-0663	Important	1
□	CVE-2019-0662	Microsoft	CVE-2019-0662	Important	1
□	CVE-2019-0661	Microsoft	CVE-2019-0661	Important	1
□	CVE-2019-0660	Microsoft	CVE-2019-0660	Important	1
□	CVE-2019-0657	Microsoft	CVE-2019-0657	Unspecified	1
□	CVE-2019-0654	Microsoft	CVE-2019-0654	Important	1
□	CVE-2019-0636	Microsoft	CVE-2019-0636	Important	1
□	CVE-2019-0635	Microsoft	CVE-2019-0635	Important	1
□	CVE-2019-0630	Microsoft	CVE-2019-0630	Important	1
□	CVE-2019-0628	Microsoft	CVE-2019-0628	Important	1
□	CVE-2019-0626	Microsoft	CVE-2019-0626	Important	1
□	CVE-2019-0625	Microsoft	CVE-2019-0625	Important	1
□	CVE-2019-0623	Microsoft	CVE-2019-0623	Important	1
□	CVE-2019-0621	Microsoft	CVE-2019-0621	Important	1

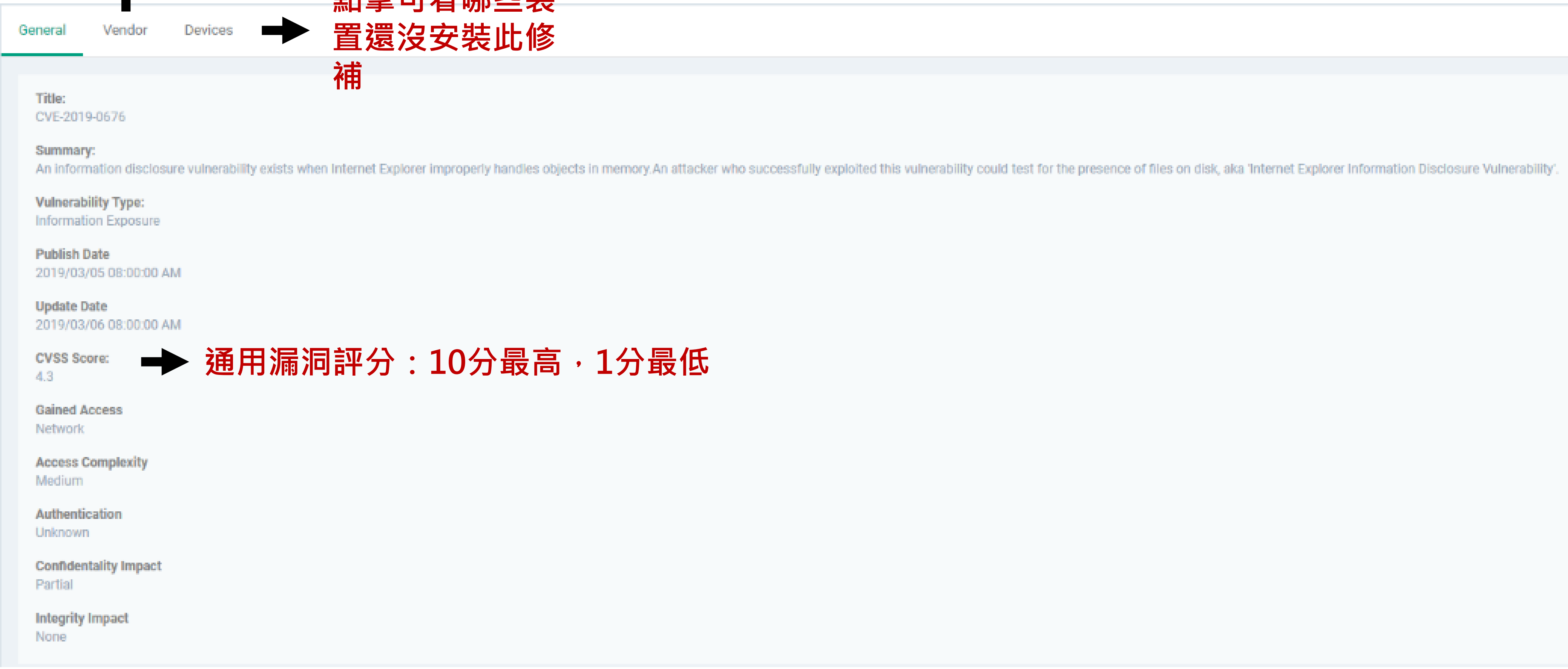
漏洞編號

存在漏洞系統數量

系統弱點風險管理

點擊可看提供修補的供應商與官方出處

點擊可看哪些裝置還沒安裝此修補



Title:
CVE-2019-0676

Summary:
An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory.An attacker who successfully exploited this vulnerability could test for the presence of files on disk, aka 'Internet Explorer Information Disclosure Vulnerability'.

Vulnerability Type:
Information Exposure

Publish Date
2019/03/05 08:00:00 AM

Update Date
2019/03/06 08:00:00 AM

CVSS Score:
4.3

通用漏洞評分：10分最高，1分最低

Gained Access
Network

Access Complexity
Medium

Authentication
Unknown

Confidentality Impact
Partial

Integrity Impact
None

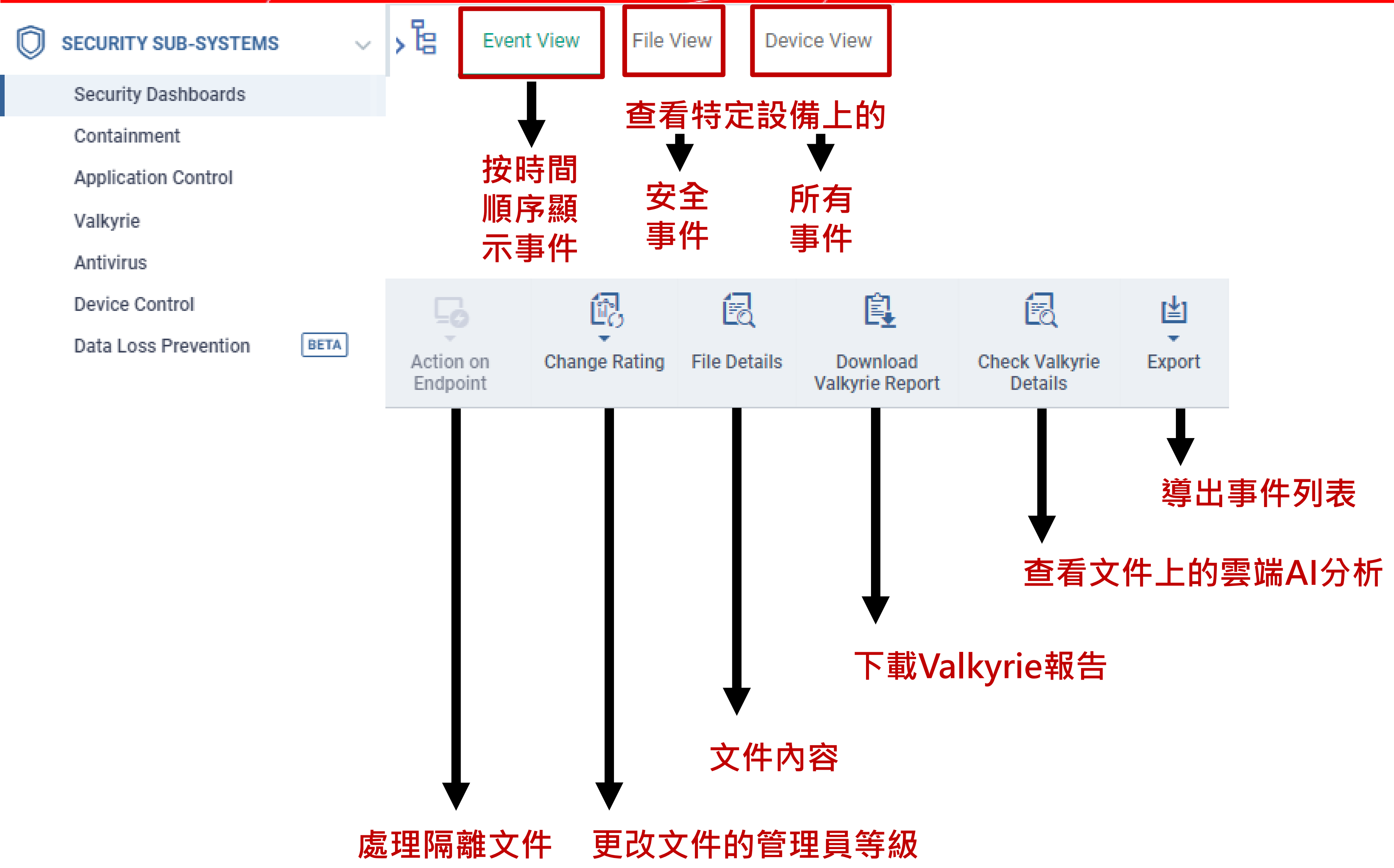
EM中央管理介面說明書

端點安全防護

COMODO

Creating Trust Online™

安全儀表板 介紹



按時間順序顯示事件

查看特定設備上的

安全事件

所有事件

處理隔離文件

更改文件的管理員等級

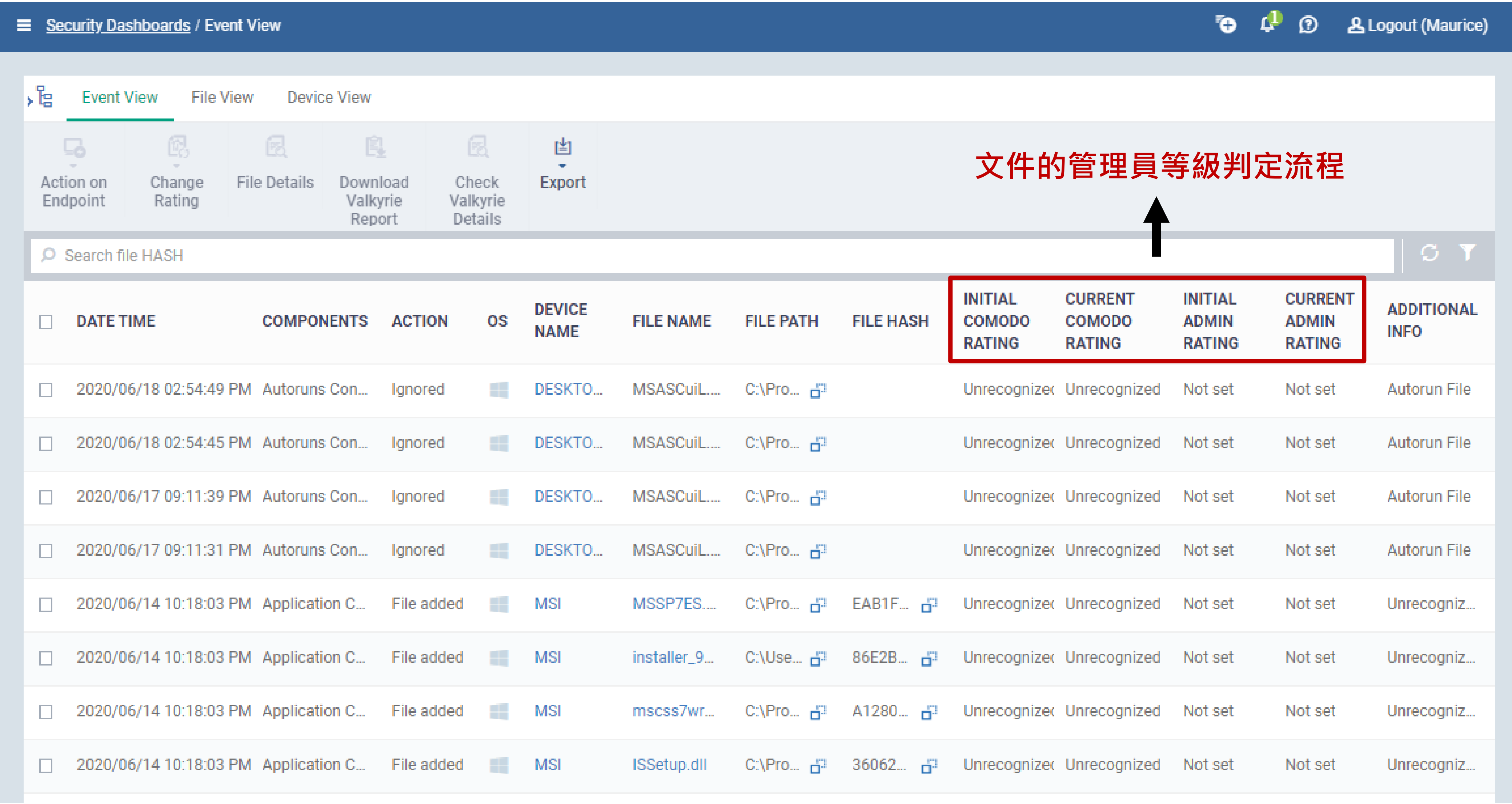
文件內容

下載Valkyrie報告

查看文件上的雲端AI分析

導出事件列表

安全儀表板 介紹



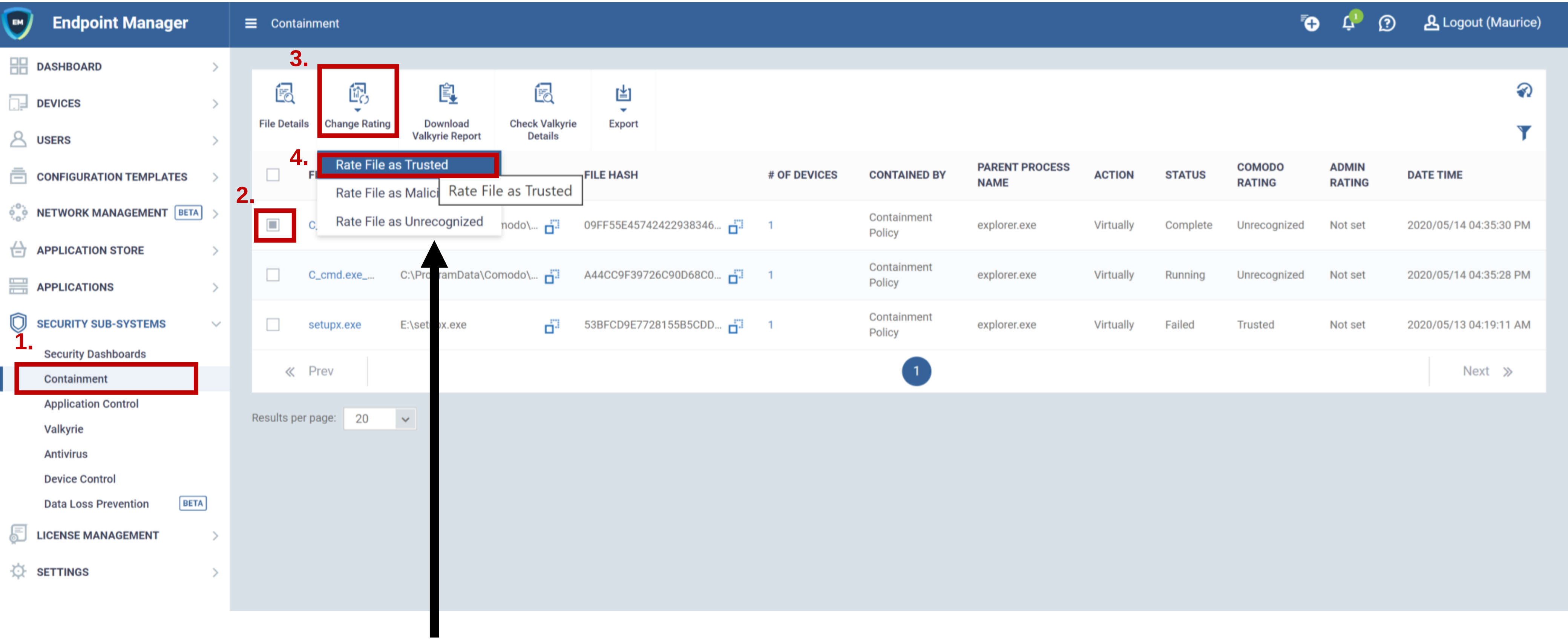
≡ Security Dashboards / Event View

文件的管理員等級判定流程

☐	DATE TIME	COMPONENTS	ACTION	OS	DEVICE NAME	FILE NAME	FILE PATH	FILE HASH	INITIAL COMODO RATING	CURRENT COMODO RATING	INITIAL ADMIN RATING	CURRENT ADMIN RATING	ADDITIONAL INFO
☐	2020/06/18 02:54:49 PM	Autoruns Con...	Ignored	⊞	DESKTO...	MSASCuiL....	C:\Pro...		Unrecognizec	Unrecognized	Not set	Not set	Autorun File
☐	2020/06/18 02:54:45 PM	Autoruns Con...	Ignored	⊞	DESKTO...	MSASCuiL....	C:\Pro...		Unrecognizec	Unrecognized	Not set	Not set	Autorun File
☐	2020/06/17 09:11:39 PM	Autoruns Con...	Ignored	⊞	DESKTO...	MSASCuiL....	C:\Pro...		Unrecognizec	Unrecognized	Not set	Not set	Autorun File
☐	2020/06/17 09:11:31 PM	Autoruns Con...	Ignored	⊞	DESKTO...	MSASCuiL....	C:\Pro...		Unrecognizec	Unrecognized	Not set	Not set	Autorun File
☐	2020/06/14 10:18:03 PM	Application C...	File added	⊞	MSI	MSSP7ES....	C:\Pro...	EAB1F...	Unrecognizec	Unrecognized	Not set	Not set	Unrecogniz...
☐	2020/06/14 10:18:03 PM	Application C...	File added	⊞	MSI	installer_9...	C:\Use...	86E2B...	Unrecognizec	Unrecognized	Not set	Not set	Unrecogniz...
☐	2020/06/14 10:18:03 PM	Application C...	File added	⊞	MSI	mscss7wr...	C:\Pro...	A1280...	Unrecognizec	Unrecognized	Not set	Not set	Unrecogniz...
☐	2020/06/14 10:18:03 PM	Application C...	File added	⊞	MSI	ISSetup.dll	C:\Pro...	36062...	Unrecognizec	Unrecognized	Not set	Not set	Unrecogniz...

Containment 介紹

COMODO
Creating Trust Online™

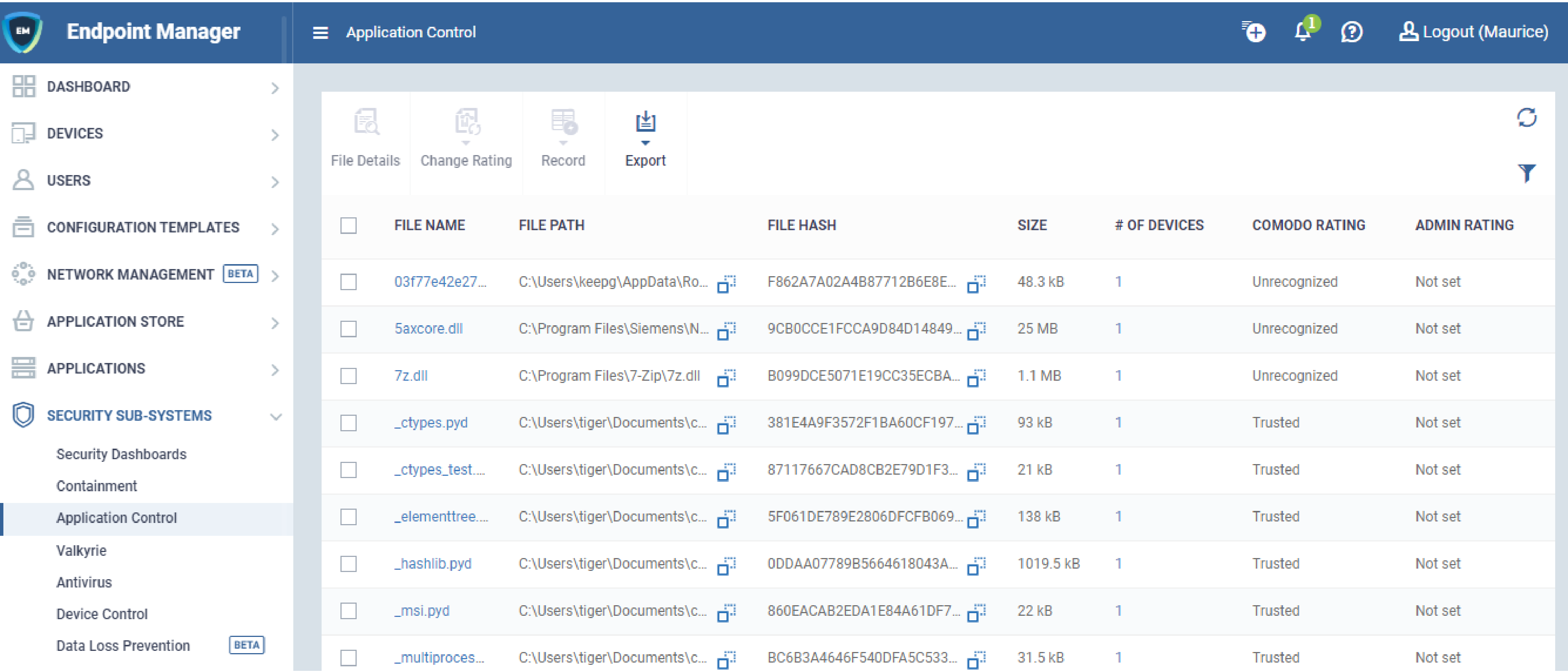


□	FI		FILE HASH	# OF DEVICES	CONTAINED BY	PARENT PROCESS NAME	ACTION	STATUS	COMODO RATING	ADMIN RATING	DATE TIME
■	C	nodo\...	09FF55E45742422938346...	1	Containment Policy	explorer.exe	Virtually	Complete	Unrecognized	Not set	2020/05/14 04:35:30 PM
□	C_cmd.exe_...	C:\Pro amData\Comodo\...	A44CC9F39726C90D68C0...	1	Containment Policy	explorer.exe	Virtually	Running	Unrecognized	Not set	2020/05/14 04:35:28 PM
□	setupx.exe	E:\set x.exe	53BFCD9E7728155B5CDD...	1	Containment Policy	explorer.exe	Virtually	Failed	Trusted	Not set	2020/05/13 04:19:11 AM

文件的管理員等級

Application Control 介紹

COMODO
Creating Trust Online™

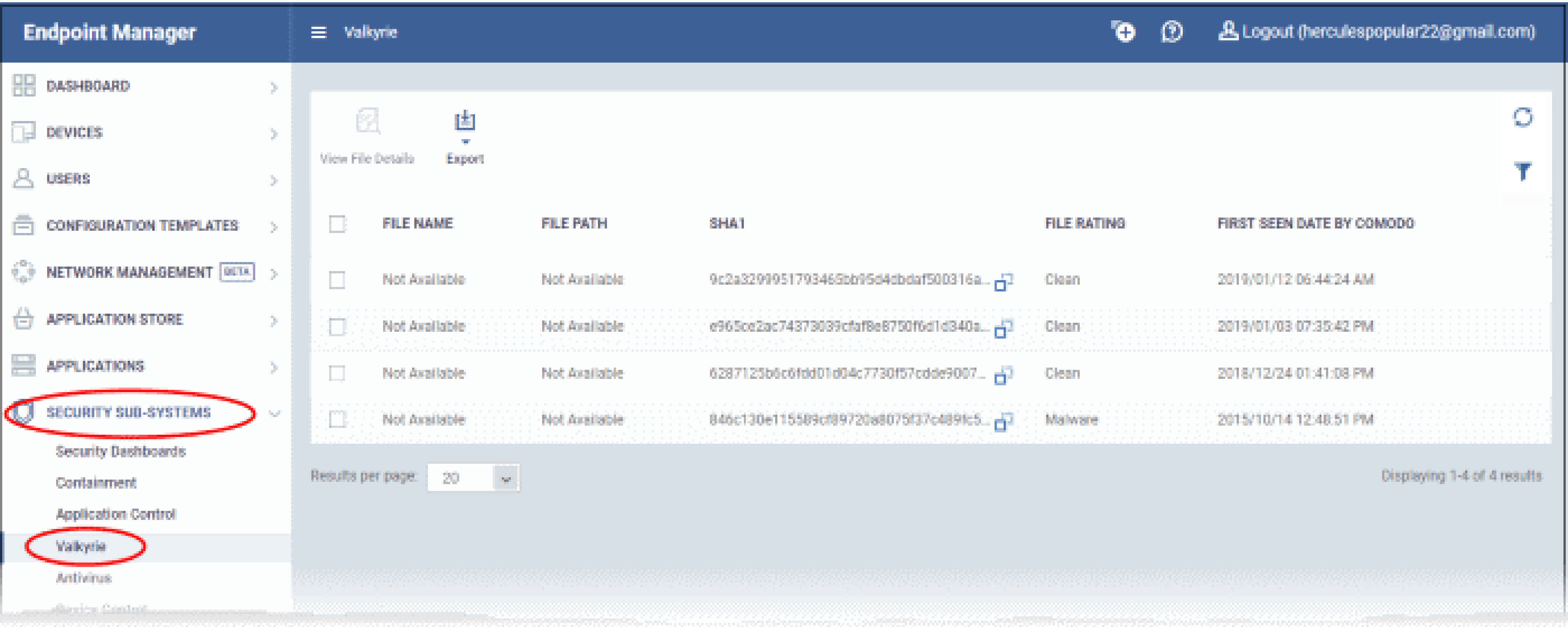


□	FILE NAME	FILE PATH	FILE HASH	SIZE	# OF DEVICES	COMODO RATING	ADMIN RATING
□	03f77e42e27...	C:\Users\keepg\AppData\Ro...	F862A7A02A4B87712B6E8E...	48.3 kB	1	Unrecognized	Not set
□	5axcore.dll	C:\Program Files\Siemens\N...	9CB0CCE1FCCA9D84D14849...	25 MB	1	Unrecognized	Not set
□	7z.dll	C:\Program Files\7-Zip\7z.dll	B099DCE5071E19CC35ECBA...	1.1 MB	1	Unrecognized	Not set
□	_ctypes.pyd	C:\Users\tiger\Documents\c...	381E4A9F3572F1BA60CF197...	93 kB	1	Trusted	Not set
□	_ctypes_test....	C:\Users\tiger\Documents\c...	87117667CAD8CB2E79D1F3...	21 kB	1	Trusted	Not set
□	_elementtree....	C:\Users\tiger\Documents\c...	5F061DE789E2806DFCFB069...	138 kB	1	Trusted	Not set
□	_hashlib.pyd	C:\Users\tiger\Documents\c...	0DDAA07789B5664618043A...	1019.5 kB	1	Trusted	Not set
□	_msi.pyd	C:\Users\tiger\Documents\c...	860EACAB2EDA1E84A61DF7...	22 kB	1	Trusted	Not set
□	_multiproces...	C:\Users\tiger\Documents\c...	BC6B3A4646F540DFA5C533...	31.5 kB	1	Trusted	Not set

評級為“無法識別”或“惡意”的文件將報告到“應用程序控制”界面。
管理員可以根據需要更改文件的等級。

Valkyrie 介紹

COMODO
Creating Trust Online™



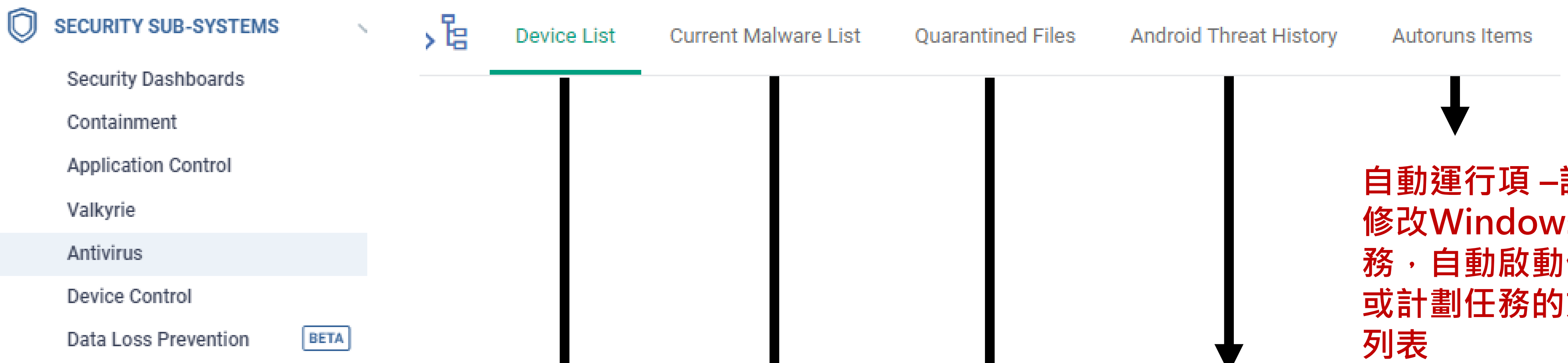
□	FILE NAME	FILE PATH	SHA1	FILE RATING	FIRST SEEN DATE BY COMODO
□	Not Available	Not Available	9c2a3299951793465bb95d4dbdaf500316a...	Clean	2019/01/12 06:44:24 AM
□	Not Available	Not Available	e965ce2ac74373039cfaf8e8750f6d1d340a...	Clean	2019/01/03 07:35:42 PM
□	Not Available	Not Available	6287125b6c6fdd01d04c7730f57cdde9007...	Clean	2018/12/24 01:41:08 PM
□	Not Available	Not Available	846c130e115589cf89720a8075f37c489fc5...	Malware	2015/10/14 12:48:51 PM

Results per page 20

Displaying 1-4 of 4 results

Valkyrie是基於雲的文件分析服務，可通過一系列靜態和行為檢查來測試未知文件。
該服務可幫助ITarian確定未知文件是惡意文件還是安全文件

Antivirus 介紹



設備列表 -顯示有關防病毒運行狀況的所有受管設備的狀態

當前惡意軟件列表 –列出託管設備上所有未處理的惡意軟件。

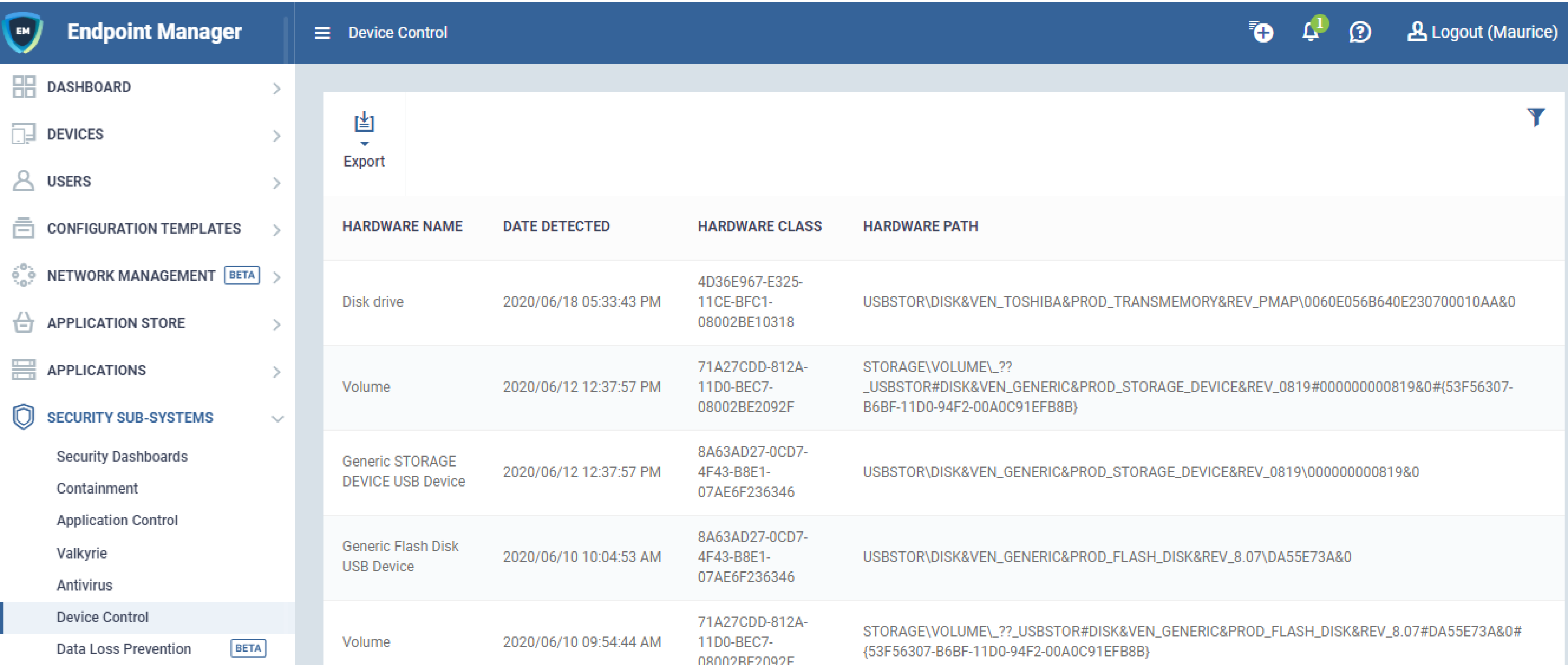
Windows隔離區 -惡意軟件已由Comodo Client Security在Windows，Mac和Linux設備上隔離。您可以刪除或還原隔離的項目，或為項目分配信任等級。

Android威脅歷史記錄 -一段時間內在Android設備上發現的所有惡意項目的日誌。

自動運行項 –試圖修改Windows服務，自動啟動條目或計劃任務的文件列表

外部設備連接紀錄

COMODO
Creating Trust Online™



HARDWARE NAME	DATE DETECTED	HARDWARE CLASS	HARDWARE PATH
Disk drive	2020/06/18 05:33:43 PM	4D36E967-E325-11CE-BFC1-08002BE10318	USBSTOR\DISK&VEN_TOSHIBA&PROD_TRANSMEMORY&REV_PMAP\0060E056B640E230700010AA&0
Volume	2020/06/12 12:37:57 PM	71A27CDD-812A-11D0-BEC7-08002BE2092F	STORAGE\VOLUME_??_USBSTOR#DISK&VEN_GENERIC&PROD_STORAGE_DEVICE&REV_0819#000000000819&0#{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}
Generic STORAGE DEVICE USB Device	2020/06/12 12:37:57 PM	8A63AD27-0CD7-4F43-B8E1-07AE6F236346	USBSTOR\DISK&VEN_GENERIC&PROD_STORAGE_DEVICE&REV_0819\000000000819&0
Generic Flash Disk USB Device	2020/06/10 10:04:53 AM	8A63AD27-0CD7-4F43-B8E1-07AE6F236346	USBSTOR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07\DA55E73A&0
Volume	2020/06/10 09:54:44 AM	71A27CDD-812A-11D0-BEC7-08002BE2092F	STORAGE\VOLUME_??_USBSTOR#DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07#DA55E73A&0#{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}

部設備包括USB設備，DVD驅動器，列印機，藍牙設備等。