

WinMatrix IT 資源管理系統 3.8.38.x 版 組態稽核模組功能規格表

組態稽核模組 (此為選購功能)	
端 末 電 腦 組 態 稽 核	功能效益
	- 主動稽核電腦系統是否處於符合公司資訊安全規範的組態設定（如：防毒、DLP、SCCM 軟體是否正常運行），以利先期發現盡早改善。 - 公司內有電腦不符合資安設定規範時，主動通報給 IT 管理員，並令該等電腦無法存取內部重要的主機，能留下完整的稽核紀錄備查。
	編號 功能項目
	1-1 可設定管控原則稽核端末電腦狀態，並於違反原則時自動執行矯正措施。管控原則依照 WinMatrix Agent 原則套用模式，可適用於將原則套用至組織、電腦或使用者。
	1-2 端末電腦可設定的稽核項目包含： (1) 執行程序：檢查執行程序為執行中或是未執行。 (2) 服務：檢查服務狀態為已啟動或已停止。 (3) 機碼：檢查機碼是否存在 (4) 機碼值：比較機碼值是否符合特定的數值。比較條件可設定大於、小於、等於、大於等於、小於等於、包含、不包含。(可設定搜尋比對 N 階層的子機碼) (5) 目錄檔案：可設定稽核目錄/檔案是否存在、比對檔案名稱(支援 wildcard)、大小、日期等。(可設定搜尋比對 N 階層的子目錄)
	1-3 同一稽核設定中可設定至多 50 筆的稽核項目與下列條件： (1) 稽核時機：電腦開機後、使用者登入後。 (2) 稽核項目之間的比對邏輯（AND、OR）。例如：當執行程序 test.exe 不存在且特定機碼值小於 5 時，視為違反稽核原則。 (3) 須執行檢查的作業系統，例如：僅檢查 Win 7 與 Win 8.1，不須檢查 Win XP 的電腦。 (4) 須執行檢查的系統類型：32 位元(x86)或 64 位元(x64)作業系統環境。
	1-4 當檢查項目未符合預期狀態時，視為違反組態稽核，可執行矯正措施： (1) 產生違反組態稽核紀錄。 (2) 立即發送電子郵件通知管理者。 (3) 禁止連線指定的 IP 位址（個別或網段範圍。例如：無法連線檔案伺服器），或只能與指定的 IP 位址(個別或網段範圍。例如：僅能與 ActiveDirectory、防毒主機通訊)通訊連線。 (4) 顯示訊息告知使用者（可自訂訊息內容與顯示時間）。 (5) 執行特定遠端命令。
1-5 當電腦由違反組態稽核狀態恢復為符合管控原則時，可執行對應措施： (1) 產生違反狀態解除紀錄。 (2) 解除違反稽核原則時所禁止連線的 IP 位址（無須額外設定，系統將自動完成）。 (3) 顯示訊息告知使用者（可自訂訊息內容與顯示時間）。 (4) 執行特定遠端命令。	
1-6 報表與查詢： (1) 違反組態稽核紀錄。 (2) 可透過 WinMatrix 排程通知樣板，自動將違反紀錄報表依照分權分責模式寄送給各單位的管理人員。	

	1-7	稽核模式： 提供週期性與一次性稽核設定。 針對週期性稽核的校正命令，可以額外設定是否每次稽核都要執行。
--	-----	---

編修日期:2024.5.29.

*使用本模組的客戶，需要已經購買與建置 WinMatrix Server 與標準功能模組。

*若您需要了解更多，請洽電話：02-2732-9516，Email：support@simopro.com。

Notes: 隨著 Microsoft 宣布特定 Windows 作業系統版本的 EOS(End Of Service)，WinMatrix 陸續新增的功能有可能無法支援已經 EOS 的作業系統。

<產品範例畫面>

端末電腦組態稽核模組 應用案例

1. A 公司透過 WinMatrix 端末電腦組態稽核模組，確保 RD 在存取設計圖與程式碼時，已安裝並執行了 DLP 軟體，保護重要檔案的安全性，其設定的稽核條件與管控項目包含：
 - (1) 沒執行 DLP 軟體時，不允許存取 RD 檔案伺服器。
 - (2) 沒執行 DLP 軟體時，顯示提示訊息告知使用者。
 - (3) 產生違反組態稽核紀錄，並定期產生報表給 RD 主管檢視。
2. B 公司透過 WinMatrix 端末電腦組態稽核模組，電腦需執行安裝防毒軟體與公司內的安控軟體，才能存取資料分享區，避免中毒風險，其設定的稽核條件與管控項目包含：
 - (1) 電腦必須執行特定防毒軟體且版本應在 12.X 以上。
 - (2) 公司內的安控軟體服務須處於已啟動的狀態。
 - (3) 當電腦違反上述稽核設定時，會立即通知資訊部工程師，由資訊部工程師協助使用者完成防毒軟體與安控軟體的安裝設定。
 - (4) 當電腦違反上述稽核設定時，禁止存取網路上的資料分享區。
 - (5) 每週產生違反組態稽核紀錄給各部門主管，落實分權分責的管理模式。

系統畫面

稽核設定-稽核項目：檢查執行程序是否執行與機碼值是否小於特定值（例：檢查版本），當任一項不符合規範時，即視為違反組態稽核。

The screenshot shows the '稽核設定' (Audit Settings) window. The '名稱*' (Name) field is set to '安控軟體應執行且為最新版本' (Security software should be executed and be the latest version). The '作業系統' (OS) and '系統類型' (System Type) fields are empty. The '稽核項目' (Audit Item) tab is selected, showing a list of items. The '稽核項目' (Audit Item) dropdown is set to '執行程序' (Executing Program). The '與下一個稽核項目比對邏輯' (Comparison Logic) is set to 'OR'. The '執行程序名稱*' (Program Name) is 'psdefender.exe'. The '狀態處於' (Status) is '未執行' (Not Running). The '設定' (Settings) button is visible. Below the settings, there is a table with the following content:

與下一個稽核項目比對邏輯	稽核項目	比對內容
OR	執行程序	執行程序名稱*: psdefender.exe, 狀態處於: 未執行
OR	機碼	機碼路徑*: HKEY_LOCAL_MACHINE\SOFTWARE

At the bottom, the '稽核時機' (Audit Timing) section shows '電腦開機後等待幾秒開始稽核' (Wait for several seconds after computer startup to start audit) set to 60, and '每隔幾分鐘再次稽核' (Audit again every several minutes) set to 1. The '確定' (OK) and '取消' (Cancel) buttons are at the bottom right.

稽核設定-矯正措施：可設定違反組態稽核與違反解除時，應執行的對應矯正措施。例如：顯示訊息告知使用者、禁止連線指定 IP 位址。

The dialog box is titled '稽核設定' (Audit Settings). It has a green header bar with a close button. Below the header, there are three input fields: '名稱*' (Name) with the value '安控軟體應執行且為最新版本' (Security software should be executed and is the latest version), '作業系統' (Operating System), and '系統類型' (System Type). Below these are two tabs: '稽核項目' (Audit Items) and '矯正措施' (Correction Measures). The '矯正措施' tab is selected. It contains two sections: '違反電腦組態稽核項目時' (When computer configuration audit item is violated) and '違反電腦組態稽核項目解除時' (When computer configuration audit item is resolved). The first section has checkboxes for '產生違反紀錄' (Generate violation record), '電子郵件通知管理者' (Email notification to administrator), '禁止連線指定 IP 位址' (Prohibit connection to specified IP address), '顯示訊息告知使用者' (Display message to user), and '執行遠端命令' (Execute remote command). The '產生違反紀錄' and '禁止連線指定 IP 位址' checkboxes are checked. Below '電子郵件通知管理者' is a table with columns '姓名' (Name) and 'E-mail', and buttons '加入' (Add) and '移除' (Remove). Below '禁止連線指定 IP 位址' is a table with columns 'IP 位址' (IP address) and a button '加入' (Add). The 'IP 位址' table has one row with the value '192.168.88.245' and buttons '修改' (Modify), '移除' (Remove), and '測試連線' (Test connection). Below '顯示訊息告知使用者' is a button '設定訊息內容' (Set message content). Below '執行遠端命令' is a button '設定遠端命令' (Set remote command). The second section, '違反電腦組態稽核項目解除時', has checkboxes for '產生違反狀態解除紀錄' (Generate violation status resolution record), '顯示訊息告知使用者' (Display message to user), and '執行遠端命令' (Execute remote command). The '產生違反狀態解除紀錄' and '顯示訊息告知使用者' checkboxes are checked. Below '顯示訊息告知使用者' is a button '設定訊息內容' (Set message content). Below '執行遠端命令' is a button '設定遠端命令' (Set remote command). At the bottom of the dialog are '確定' (OK) and '取消' (Cancel) buttons.

違反組態稽核紀錄：查詢違反組態稽核紀錄，可呈現稽核項目名稱，違反與違反解除的時間，並可將結果列印/匯出。

當有電腦違反組態稽核時，可立即 Email 通知管理員：Email 中顯示違反的稽核項目與電腦名稱、IP，管理人員可依照此資訊即時處理。



2015/10/6 (週二) 下午 02:41

winmatrix@simopro.com

[違反]端末組態稽核 - 研發部DLP執行檢查 : GARY-DELLNB (192.168.81.58)

收件者 朱懿中

檢查時間	2015/10/06 14:41:57
事件類型	違反
稽核項目名稱	研發部DLP執行檢查
組織名稱	產品管理部
電腦名稱	GARY-DELLNB
IP 位址	192.168.81.58
登入帳號	garychu

排程通知樣板：自動寄送前一日違反組態稽核紀錄報表給管理人員

組態稽核 通知樣板						
說明：查詢時間範圍：2015/10/05 15:14:54 ~ 2015/10/06 15:14:54, 樣板名稱：組態稽核 通知樣板, 樣板描述：, 樣板主類型：端末組態稽核, 樣本子匯出時間：2015/10/06 15:14						
共 5 筆						
檢查時間	事件類型	稽核項目名稱	組織名稱	電腦名稱	IP 位址	登入帳號
2015/10/06 14:59:53	解除	安控軟體應執行且為最新版本	產品管理部	GARY-WIN8	192.168.81.68	garychu@simopro.com
2015/10/06 14:57:53	違反	安控軟體應執行且為最新版本	產品管理部	GARY-WIN8	192.168.81.68	garychu@simopro.com
2015/10/06 12:26:31	違反	防毒軟體必須執行	技術支援部	RICK-PC	192.168.81.35	rick@simopro.com
2015/10/06 12:00:27	違反	防毒軟體必須執行	技術支援部	BIAIR-PC	192.168.81.36	blair@simopro.com
2015/10/06 11:56:02	違反	防毒軟體必須執行	產品管理部	GARY-WIN8	192.168.81.68	garychu@simopro.com