CPS Systems Ultimate Auditor *Plus*

新一代維運稽核與風險控制系統

CPS Ultimate Auditor *PLUS*是CPS Systems基於多年的市場經驗與客戶需求，投入大量的技術研發所開發出的新一代維運稽核與風險控制系統，是一種符合5A的統一安全管理方案，可作為進入內部網路的一個連線與檢查設備，透過細緻的政策設定與工單系統，防止未經授權的連線行為，對不合法的指令進行告警或阻斷，是針對系統特權帳號及系統使用者的操作行為，進行控制和稽核的合規性管控系統。

CPS UAP具備強大的輸入輸出稽核功能，為企業內部提供完全的稽核資訊，通過帳號管理、身份認證、資源授權、即時監控、操作還原、自訂策略、工單系統、定期與彈性化報表等系統功能，增強維運操作與稽核管理的安全性，廣泛適用於需要維運稽核與安全管理的各個機關與行業。

新一代維運稽核與風險控制系統組成

不同於第一代CPS系統使用軟硬體一體化設計，新一代維運稽核與風險控制系統CPS UAP系統可架構在虛擬化平台內(VMware)，新一代系統架構由WEB模組、協議代理模組、行為稽核模組和應用發佈模組所組成。

➢ WEB模組

新一代系統為維運使用者提供WEB方式的訪問介面，維運使用者在Web介面中進行單一登錄認證與操作行為。CPS管理員也使用WEB介面中進行維運使用者管理、設備及帳號管理、用戶授權管理和維運稽核管理等配置管理功能。

➢ 協議代理模組

實現對標的物設備在維運過程中的協議資料，進行代理操作、行為還原及記錄、將危險與違規行為阻斷等功能。

➢ 行為稽核模組

實現對操作行為的稽核功能，包括危險與違規行為即時的告警、即時監控、歷史資料檢索及報表統計等功能。

➢ 應用發佈模組

安裝在Windows伺服器上，用於發佈非標準協定或應用用戶端的工具，例如IE、PLSQL、SQLplus、PCanywhere、Toad、Teamviewer、vCenter..等。可實現對應用用戶端工具的自動調出、密碼代填和操作側錄功能。

系統功能

➢ 使用者認證與單一登入 Single sign-on (SSO)

系統使用者介面採用WEB2.0風格，支援單一登錄 Single sign-on (SSO)功能，維運人員一次登入，即可訪問所有目標資源，無需二次輸入用戶名及密碼資訊。

使用者登錄認證則提供單因素認證和雙因素二級加強認證模式，單因素認證包括靜態帳號密碼認證、LDAP認證、AD認證和Radius認證；雙因素加強二級認證包括硬體式動態Token、硬體式USB Token。可有效解決維護人員使用共用系統帳號，進行操作所產生的稽核問題。

➢ 維運工單流程管理功能

系統提供維運工單流程管理功能，讓不具有權限但臨時需要進行維運的使用者，可透過申請後由管理員設定並下發工單，讓授權維運人員有許可權在指定時間內訪問指定的資源。工單功能包含，維運者可以進入系統後進行臨時授權申請、並可提供其他管理者二次審核、維運者在系統內接受工作任務與進行連線操作，工單訊息可透過E-mail通知相關管理者，也能使用日誌查詢相關工單操作資訊。

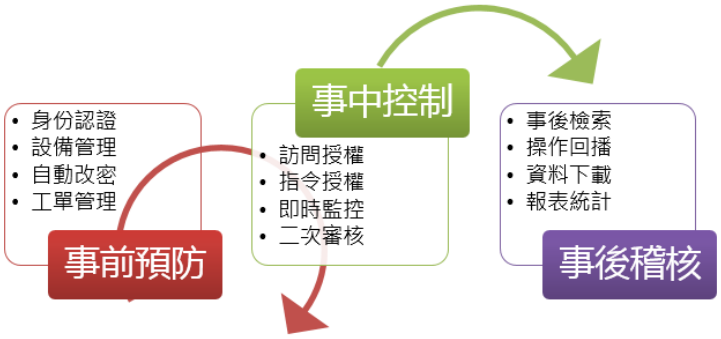
➢ 密碼策略與自動改密

密碼策略可設定登錄的帳號密碼原則，包含最小長度、大小寫、數字、特殊符號之密碼複雜度、也具有可用週期與到期提醒與舊密碼歷史比對次數之功能。

自動改密是支援有託管之作業系統，例如Windows、Linux、Unix能自動定期修改帳號密碼。

CPS Systems Ultimate Auditor Plus

新一代維運稽核與風險控制系統



➢ 策略管理

策略管理分為訪問策略與指令策略，可限制連線IP、時間、RDP剪貼與硬碟映射，並透過巨集功能來限制多組IP與多組時間區間。利用黑白名單功能與多種告警級別和告警方式，能同時限制多項指令並可將操作指令和對象配對為進階政策，在政策設定內綁定使用者、群組與設備形成細緻的管理規則。

➢ 二次審核

內建二次審核功能，對特殊性的訪問與操作進行二次審核，加強維運者行為管控，確保所有訪問操作都在即時監控過程中進行。

➢ 告警與阻斷

系統根據已設定的策略規則，自動檢測維運過程中的越權與違規的操作行為，系統能根據所設定的事件類型、等級條件進行自動的告警和阻斷處理。阻斷功能分為阻斷連線與忽略指令兩種行為，告警功能具有Syslog、郵件、SNMP三種方式。

➢ 歷史操作回放

所有使用CPS UAP系統連線的操作連線都將被記錄下來，管理員可透過查詢功能對歷史操作進行指令與畫面回播，系統對不同協定與工具能自動提供不同回播選項，回播內容也提供管理員進行下載做為稽核附件。

回播畫面支援快速播放、游標拖動、暫停與重播，對關鍵字與特定操作進行定位回播。

➢ 系統管理者三權分立

各自獨立的管理權限：系統帳號管理員、系統稽核員、系統管理員。以達到不同業務性質的管理員許可權可以完全隔離。

➢ 即時監控操作連線

維運操作連線監控，管理員可以即時手動中斷操作，搭配二次審核功能，確保高危險指令或關鍵設備的操作能完全掌控。

➢ 日誌查詢與稽核報表

系統具有多樣化的日誌與報表，有維運日誌、工單日誌、登入日誌、管理日誌多種系統日誌，可透過關鍵字、IP、時間、使用者、服務、審核動作、狀態、工單編號....等查詢條件進行查詢。

管理者能使用系統預設的連線操作與異常報表樣本，設定手動報表產出與週期性報表產出 ，並可以透過新增樣版功能去自訂報表範本，彈性調整報表內容。

➢ 支援資料庫協定

支援多種資料庫協定：Oracle（RAC）、MS SQL、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL

➢ 本地工具

支援多種工具：MS SQL(SSMS)、SecureCRT、Mysql 、WinSCP、SQLPlus、PLSQLDev、Toad4Oracle、 Xshell 、Db2cmd、TightVNC、pgAdmin3、SqlAdvantage、Sqleditor、SSH Secure Shell Client 、Navicat QuestCentral

➢ 管控多種系統與協定

管控系統Windows、Linux、AIX、HP-UX、Cisco

字元協定：SSHv1、SSHv2、TELNET、RLOGIN

圖形協定：RDP、VNC

檔案傳輸通訊協定：FTP、SFTP

➢ 高可用性(HA)與負載平衡

可選購高可用性(High Availability)模組與負載平衡模組，強化系統營運的可靠性。

CPS Systems Ultimate Auditor Plus
維運稽核與風險控制系統
事前導入政策管理‧事中及時發現並處理‧事後分析追查