產品安全使用手冊

UM024004T_20241004

1. 安全指南

1.1 文件目的

為了使人機介面與其相關軟體在使用時能提供安全正確的安裝、操作、維護與汰除等行動，本文件將參考 IEC 62443-4-1 標準，列舉出使用人機介面時會遇到的配置與工程檔案的設計相關的安全強化機制，強烈建議使用者參考本文件的步驟操作，在應用實際運行之前即具備最大限度的安全防範，並在運行過程中持續地維護，以確保應用不會受到負面影響，直至產品被安全汰除為止。
注意: 文件中的 SG-X 代表對應 IEC62443-4-1 SG 對應的指引。

1.2 文件架構

本文件將依照使用產品時，從初始配置安排到軟硬體的設定，最後到產品生命結束時的處置，詳細地探討以下各主題領域與各自的安全方針。

- 初始配置：最大限度地減少與防止配置過程中的操作
- 編輯程式時：程式編輯軟體中的風險
- 產品運行時：管理者與操作員的權限管理
- 遠端維護時：通過適當的保護措施防止不必要的遠程訪問
- 硬體相關：外部儲存設備
- 產品生命終止：安全汰除守則

1.3 縱深防禦

縱深防禦的概念就是，不單單僅依靠單一的安全措施，在各個層級都賦予一定程度的安全機制保護，藉此大幅度的降低資訊外洩與駭客攻擊等潛在風險並提升產品在安裝、操作、維護與汰除時的安全保護。

1.3.1 外部環境 (SG-2/SG-3a)

根據圖片所示，針對產品安全的外部環境三大防線便是現場安全、其次是網路環境以及系統整合的安全。以下分別說明：

現場安全

通過系統盤查確保人員對人機介面的使用存在安全機制。

- 於校園或工廠設置帶有門禁控制的圍欄。
- 於實驗室或擺放伺服器空間設置生物識別訪問控制或者上鎖。
- 報警系統或視訊監控。

網路環境安全

為了確保網路通訊不被輕易滲透，請將網路環境單純化。

- 監控辦公室網路和工廠網路之間的通訊介面，例如防火牆。
- 將網路通訊架設於路由器底下，避免能直接透過公開 IP 就能訪問到產品。
- 若是產品上有兩個網路孔，建議將 LAN 1 連接對外網路，LAN 2 連接對內的設備。如此通訊資料便不會與對外網路有所連結。

系統整合安全

確保內部保護的功能在系統整合時能起到作用，例如防毒軟體、白名單等。

- 定期維護與更新。
- 工廠或人機操作員的用戶身份驗證。

1.3.2 產品操作 (SG-1/SG-3c)

人機介面的系統設定通常皆為製作檔案與系統整合的人員來操作，在使用者操作期間應避免參數被修改而造成無法正常使用的情況，因此一般建議採取以下措施。

- 隱藏系統設定。
- 修改登入預設密碼。
- 透過網頁設定頁面的路徑，請使用 HTTPS 加密通訊。

1.4 一般安全性維護 (SG-3h)

本節說明維護產品安全性的準則與建議，以利使用者規畫與進行日常的資訊安全維護工作。

- 定期更新產品版本，確保軟體和韌體都維持在最新的版本，包括應用程式、操作系統等。這樣能夠防止已知漏洞被利用，同時也能提供新的安全功能。
- 針對安全漏洞定期進行測試，包括漏洞掃描、滲透測試等，以確保產品的安全性。如此可發現並修復潛在的弱點。
- 利用產品提供的監控功能，監控產品的運作情況、檢測異常行為和安全事件。同時，儲存所有的安全事件記錄，以便日後分析和調查。
- 對於敏感資料和通訊，使用適當的加密機制，確保資料在傳輸和儲存過程中都能保持機密性和完整性。
- 建立應變計畫，以應對可能的安全事件，並迅速採取應對措施。同時，建立漏洞管理流程，定期評估、追蹤和修補漏洞。
- 若本產品提供委外服務供應商存取，確保他們也遵循相同的安全標準，並定期評估他們的安全性。可參考委外供應商的管理國際標準。(e.g. ISO 28000 / ISO 27001)

1.5 風險分析與回報機制 (SG-3g)

在使用產品的任何過程當中，若有安全相關的風險發生，請執行以下的流程並嘗試強化產品安全來達成風險管理的需求。

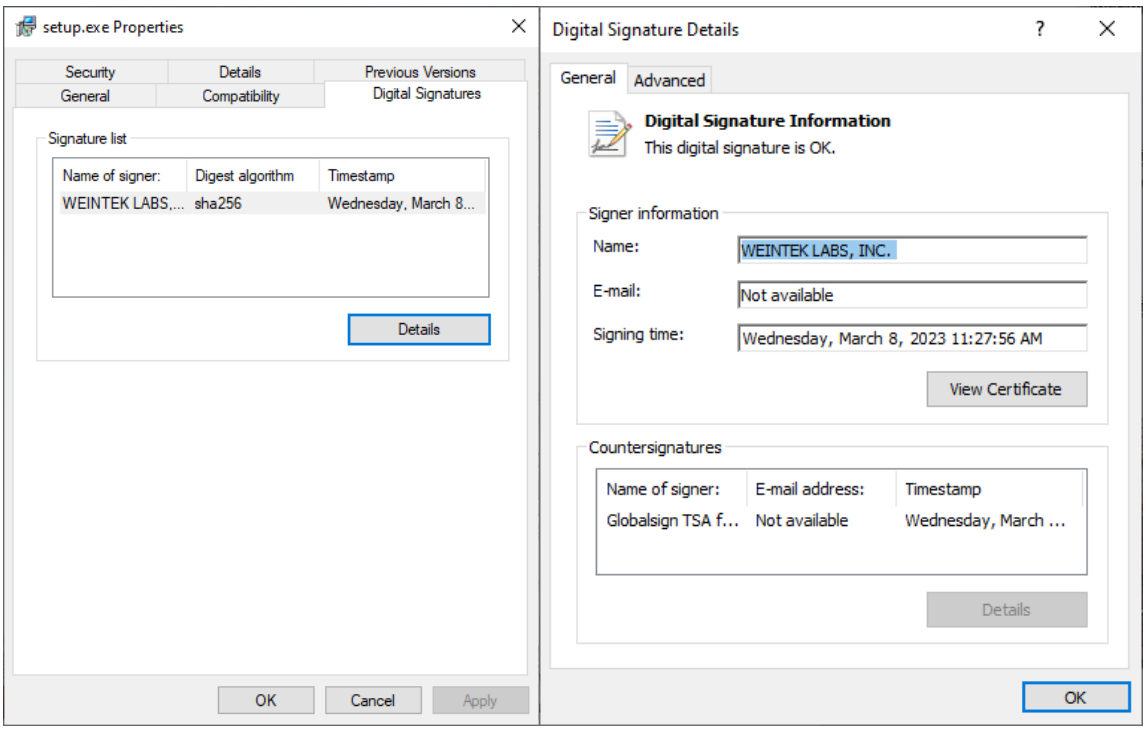
- 風險分析
- 產品安全使用手冊
- 評估風險是否消弭
- 若無法自行排除，請將問題回報於 this URL address

2. 編輯程式時的風險

2.1 安裝檔案確認

2.1.1 數位簽章

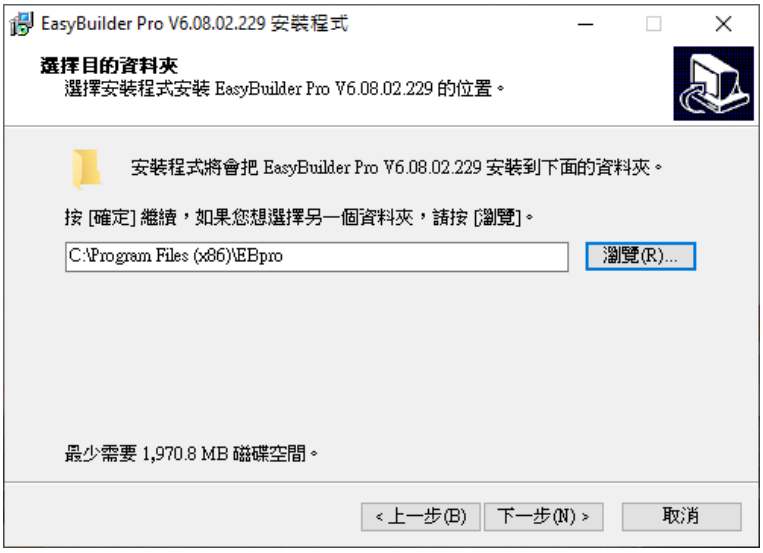
在安裝 EasyBuilder Pro 前，請確認安裝檔案(setup.exe)是否有數位簽章，且簽章沒有被破壞。在安裝檔案使用右鍵進入數位簽章的屬性，可按下細節確認是否為正常的數位簽章。



數位簽章

2.1.2 安裝路徑

安裝 EasyBuilder Pro 至受存取權限管控的資料夾 (e.g. C:\Program Files (x86)) 。

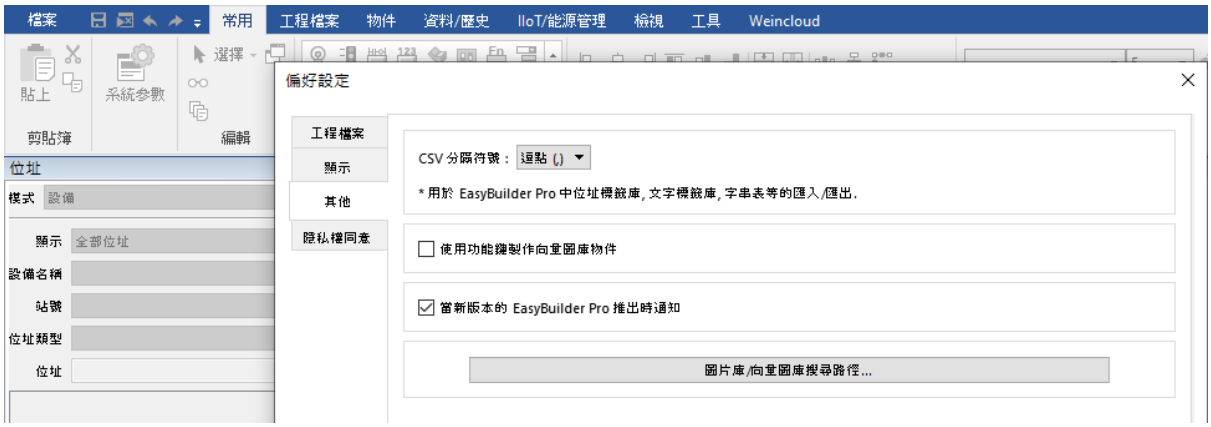


安裝路徑

2.1.3 啟用自動更新

開啟 EasyBuilder Pro 自動更新，確保可立即升級至解決安全問題的新版本。

進入 EasyBuilder Pro 之後，從上方 [檔案] 開啟 [偏好設定] 頁面，在 [其他] 頁籤中，啟用當新版本的 EasyBuilder Pro 推出時通知功能。



當新版本的 EasyBuilder Pro 推出時通知

2.2 軟體安全設定 (SG-3d)

2.2.1 啟用安全通訊

開啟安全加密通訊確保 HMI 與其他設備通訊時會使用加密的內容進行通訊。

進入 EasyBuilder Pro 之後，從上方 [常用] 開啟 [系統參數] 頁面，在 [設備] 頁籤中，點選 HMI 並進入 [設定/保護] 視窗即可啟用安全通訊，如下圖。

啟用安全通訊

2.2.2 使用進階安全模式 (SG-6)

在 HMI 的操作控制，建議使用進階安全模式。設計檔案人員可針對不同的使用者提供不同的類別權限，藉此來控制特定物件的存取權。

進入 EasyBuilder Pro 之後，從上方 [常用] 開啟 [系統參數] 頁面，在 [使用者密碼] 頁籤中，選擇進階安全模式，如下圖。詳細設定請參考使用手冊第 10 章。

進階安全模式

2.2.3 高強度的使用者密碼

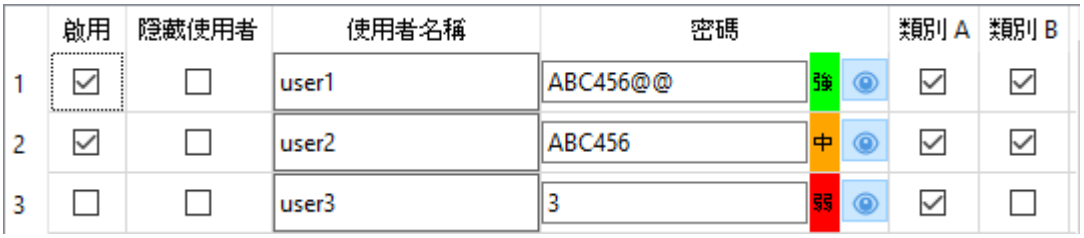
越複雜的使用者密碼越不容易被有心人士破解，在設定使用者密碼的時候，視窗中會以顏色以及強度來告知該使用者密碼的安全程度。

主要分成大寫英文字母、小寫英文字母、數字與符號四種類型。規格如下：

強：上述類型三種以上且長度大於 8 個字元。(請參考下方建議)

中：上述類型兩種以上且長度大於 6 個字元。

弱：其餘類型。



使用者密碼強度

(建議)如何選擇你的使用者密碼？

- 長度至少大於 8 個字元
- 請不要只使用一種類型，而是將大小寫英文字母、數字與符號混合使用
- 如果可以的話，請不要使用字典內會出現的詞彙 (例如: Mouse)
- 請不要使用鍵盤上連續文字的組合 (例如: 123456 或是 asdfgh)

- 請不要使用重複的字元 (例如: AAAA)

2.2.4 使用者密碼安全設定防護

啟用“唯讀”模式能在他人取得原始工程檔案時，防止未經授權的使用者進行安全設定。在唯讀模式中，安全設定不能被變更，且密碼會使用暗碼顯示，以防止密碼外流。必須使用原始設定的密碼才能重新取得管理權限。

在 [使用者密碼] 頁籤中，選擇 [編輯] 進入 [唯讀設定]，啟用唯讀後即可將使用者密碼資訊保護不讓有心人士查看。

唯讀模式

2.2.5 啟用自動登出

當 HMI 閒置(無人操作)的時候，為了避免前一位使用者離開後忘記登出，而讓接著使用的人可以存取到前一位的使用權限，建議啟用自動登出。

進入 EasyBuilder Pro 之後，從上方 [常用] 開啟 [系統參數] 頁面，在 [系統] 頁籤中，啟用自動登出，如下圖。

自動登出

2.2.6 啟用時間同步 (透過 NTP 伺服器)

為了確保時間的正確性，建議將 HMI 的時間定期與 NTP 伺服器同步。

進入 EasyBuilder Pro 之後，從上方 [常用] 開啟 [系統參數] 頁面，在 [時間同步/夏令時間] 頁籤中，啟用時間同步(透過 NTP 伺服器)，如下圖。

時間同步

2.2.7 物件安全

HMI 的基本操作元件即為物件，針對每一個可操作的物件，建議使用者啟用安全控制，在實際發出命令之前提供再度確認的功能，另外也可以搭配使用者密碼的權限功能實行物件的管控。

進入物件的屬性，在 [安全] 頁籤中，啟用安全控制以及使用者密碼的權限管控，如下圖。

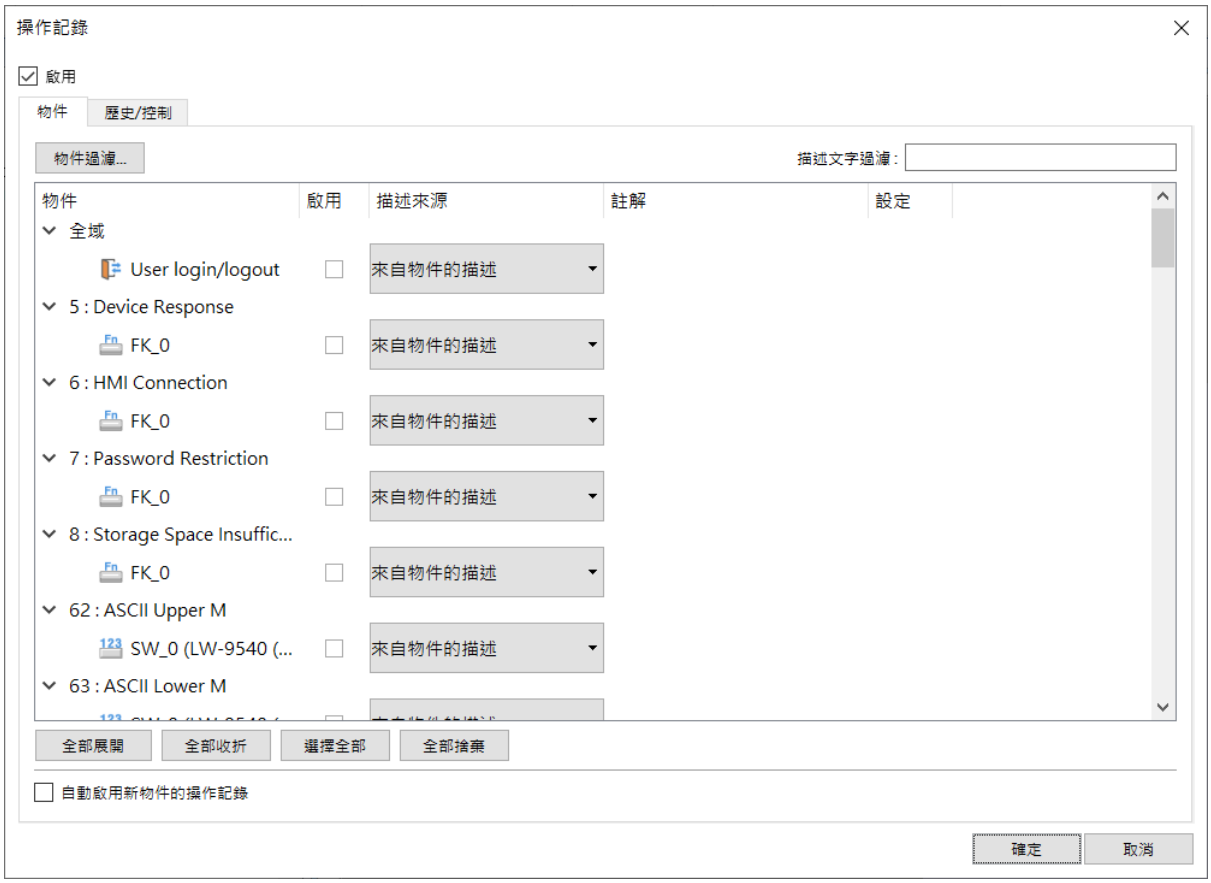
物件安全

2.2.8 操作記錄

當對各物件執行任何操作，操作記錄能記錄所有關於該動作操作的資訊，包括：日期/時間、使用者名稱、物件類別、視窗編號、物件名稱、使用者定義的描述、動作(物件種類)、位址、以及變更資訊。

開始記錄後，操作記錄會預設以 sqlite 資料庫格式儲存 在 HMI 記憶體中，也能備份至連接的外部裝置中，例如 USB 碟。

在 [物件] » [操作記錄] » [操作記錄設定] 能啟用操作記錄功能。選擇所有需記錄操作過程的物件，並寫下關於該物件執行動作的描述。這些描述也會一併記錄在操作記錄中。



操作記錄設定

提示：點選物件過濾能指定欲檢視的物件

使用者需注意此頁的設定，若未詳細設定，資料可能遺失。在將外部記憶體的資料同步之前，請確認 HMI 記憶體之最大記錄筆數，以免超過。請同時將資料同步至外部裝置中，以便在 HMI 空間不足時，作為備用，以防資料流失。

操作記錄使用控制位址，以便在 HMI 運行時，對操作記錄下指令，或是確認與操作記錄相關的狀態報告。請謹慎使用控制位址，避免意外清除資料，或是關閉操作記錄，並且盡可能通報所有執行結果。

如欲檢視操作記錄，可在螢幕上放置一個操作記錄檢視物件。

3. 產品運行時的風險 (SG-5)

3.1 登入權限

開啟網路瀏覽器 (Windows Edge, Chrome, Firefox) 並輸入 cMT X 系列人機的 IP 位址，此時即可進入 cMT X 系列人機的網頁設定頁面。若輸入 IP 位址出現的是 Webview 介面，則需要輸入 https://HMI_IP/admin 才會是 Easyweb 2.0 系統參數登入頁面。
系統將權限分為三個等級，[Admin] 為最大權限，其登入後可更改系統內的所有設定。而登入 [Update] 時，可更改的設定項目則較少。基於安全考量，進入設定前須先進行密碼確認。另外進入 [History] 前，須登入密碼，登入後可備份歷史資料。請將管理者與操作者的密碼分別設定，避免操作者擁有管理者的權限。

登入權限

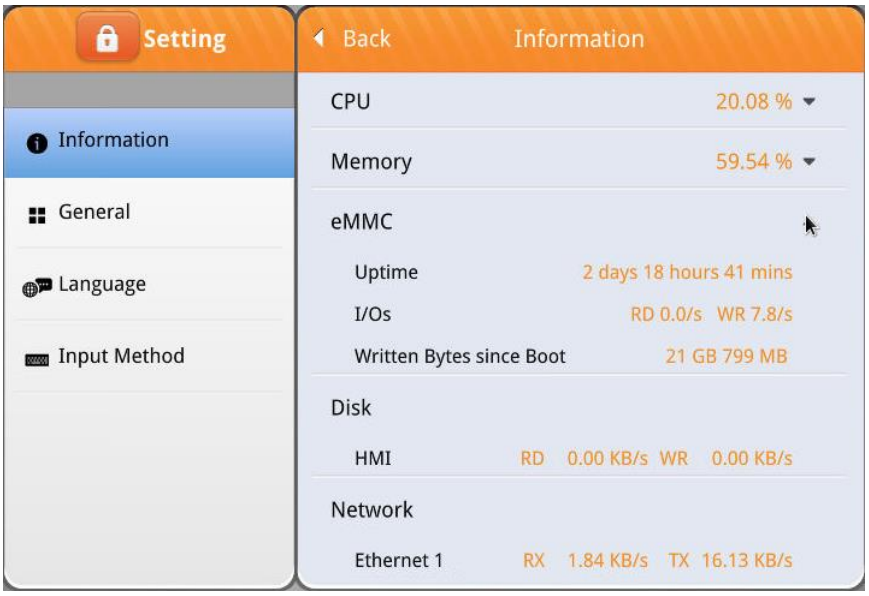
3.2 歷史檔案安全

歷史檔案包含資料取樣、事件記錄以及操作記錄物件所產生出的檔案，可藉由本節的內容來加強與歷史檔案相關的安全性。

3.2.1 延長快閃記憶體壽命

因為 HMI 內部的快閃記憶體有寫入次數的限制，若大量或頻繁的寫入歷史資料，將縮短快閃記憶體的壽命導致歷史資料無法讀取而最終 HMI 可能無法啟動。

因此建議快閃記憶體的每分鐘平均寫入速度應小於 1200 KB/min。(此資訊可以在 HMI 上的 System Setting 中取得)



平均寫入速度

降低快閃記憶體寫入速度的建議：

資料取樣

- 若未有歷史檔案的需求，僅需要檢視 HMI 開機後產生的資料，則不需要勾選儲存歷史資料。
- 設定較長的取樣時間。
- 減少在控制位址下達同步命令(2 或 3)的頻率。
- 若使用自訂檔案管理，請減少切換檔案的頻率。若啟用週期性自動同步，也可設定較長的同步時間。

事件記錄

- 若未有歷史檔案的需求，僅需要檢視 HMI 開機後產生的資料，則不需要勾選儲存歷史資料。
- 若非報警用途，只是希望在某些條件滿足時，執行特定動作，不要勾選 [儲存為歷史資料]，或改使用動作觸發物件。
- 減少在控制位址下達同步命令(2 或 3)的頻率。
- 啟用 Aggregate 模式。

操作記錄

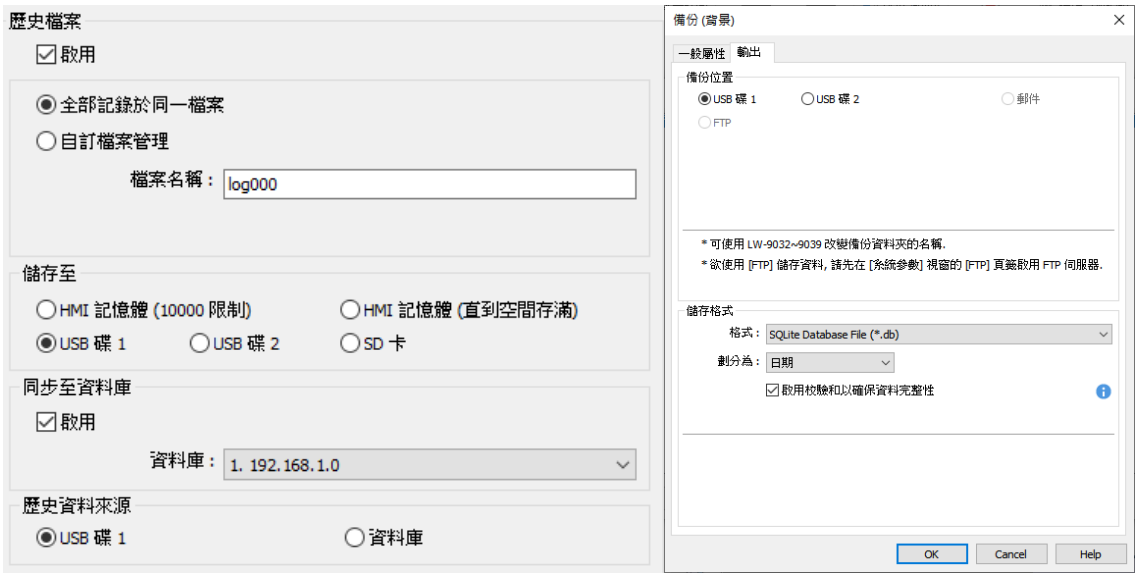
- 減少在控制位址下達同步命令的頻率。
- 啟用 Aggregate 模式。

Note

- 在 HMI 關機前，應將系統暫存器 LB-9034 設為 ON，以確保歷史資料完整寫入快閃記憶體。

3.2.2 儲存/備份歷史檔案到外部裝置

建議將歷史檔案儲存或備份到外部裝置，例如：USB 碟、SD 卡或是同步至資料庫伺服器，以便在 HMI 空間不足時，作為備用，以防止資料流失。



儲存/備份歷史檔案到外部裝置(以資料取樣為例)

外部裝置選用 USB 碟與 SD 卡的建議：
額外購置的 USB 碟與 SD 卡也有寫入次數的限制，依照記憶體種類不同，有不同的寫入次數上限。若歷史資料寫入較為頻繁，或希望歷史檔案能長久保存，建議儘量使用容量較大的 USB 碟與 SD 卡 (e.g. 32GB) ，且定期 (e.g. 每年) 執行一次異地備份。

外部裝置選用資料庫伺服器的建議：
啟用 RAID，且定期 (e.g. 每年) 執行一次異地備份。

3.2.3 備份檔案完整性

威綸提供的 EasyConverter 工具能在電腦上開啟 sqlite 檔案，以顯示備份檔案資料，並支援將檔案輸出為 Excel/CSV 格式。若備份檔案含有校驗和(checksum)，EasyConverter 將驗證校驗和，確認資料的一致性。在產生備份檔案時勾選 [啟用校驗和以確保資料完整性]，即可啟用此功能。此功能只支援於 cMT/cMT X 系列。

備份物件校驗和設定

EasyConverter 可用於檢驗備份檔案內容的完整性。若檢驗時發現檔案可能已被竄改，EasyConverter 將發出警示。

4. 遠端維護時的風險

4.1 通訊安全

4.1.1 關閉不必要的功能 (SG-3b)

在使用 HMI 時，若未使用的情況下，盡量關閉不必要的功能，或是至少使用密碼防護：

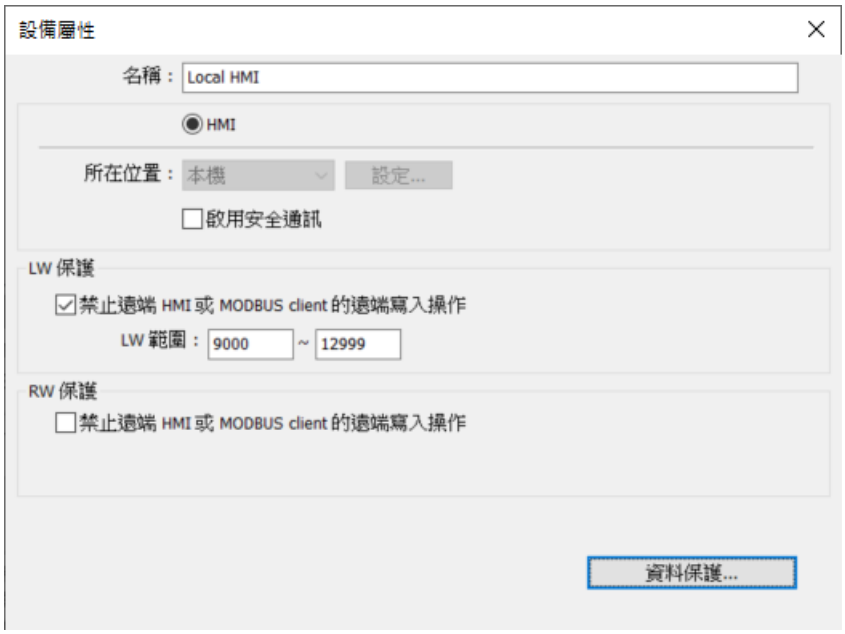
1. 遠端 HMI
2. PLC 控制 (換頁)
3. Modbus 伺服器
4. VNC 伺服器
5. cMT Diagnoser (cMT/cMT X 系列)
6. OPC UA 伺服器 (部分 cMT/cMT X 系列)

此列表不應視為詳盡無遺。

4.1.2 Modbus 伺服器

HMI 程式若有使用 Modbus 伺服器，請在 [系統參數] 的 [設備] 頁籤中，選擇 [設定/保護]，並勾選 [LW 保護]，以避免 HMI 與 Modbus client 端通訊時，系統暫存器的相關功能被任意調整，如下圖。

注意: 需設定保護的 LW 範圍請查閱系統暫存器支援範圍。

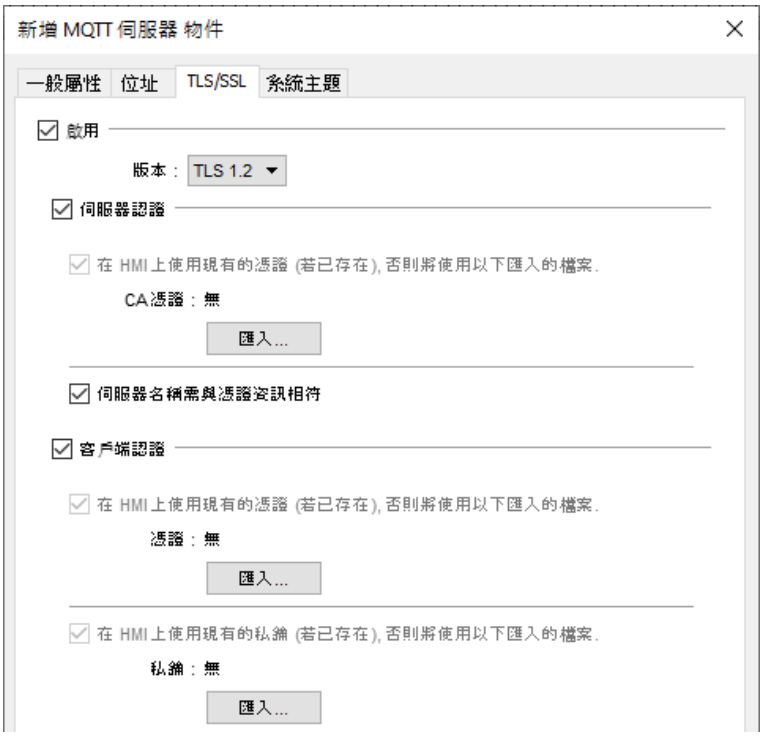


LW 保護

4.1.3 MQTT

HMI 程式若有使用 MQTT 功能，請使用 TLS 1.2 安全加密通訊，並匯入伺服器 CA 憑證、客戶端憑證以及私鑰檔案。

選擇 MQTT 伺服器物件之後，在 [TLS/SSL] 頁籤中，啟用加密以及認證功能，如下圖。



MQTT TLS/SSL 加密

4.1.4 OPC UA 伺服器

HMI 程式若有使用 OPC UA 伺服器功能，請取消勾選明文通訊，改使用安全加密通訊。選擇 OPC UA 伺服器物件之後，在 [一般] 頁籤中，取消勾選 [無] 的安全策略，強制客戶端必須以加密的內容通訊，如下圖。

OPC UA 伺服器安全策略

4.1.5 資料庫伺服器

HMI 程式若有使用資料庫伺服器功能，請使用 TLS 1.2 安全加密通訊，並匯入伺服器

CA 憑證。

選擇資料庫伺服器物件之後，在 [TLS/SSL] 頁籤中，啟用加密以及認證功能，如下圖。

資料庫伺服器 TLS/SSL 加密

4.1.6 郵件功能

HMI 程式若有使用郵件功能，請使用需要認證的 SMTP 伺服器並啟用 TLS/SSL 安全加密類型連結。

在 [系統參數設定] 啟用郵件功能之後，勾選 [SMTP 伺服器需要認證] 與 [使用下列加密類型連結]，如下圖。

郵件功能加密

4.1.7 cMT Viewer 遠端監控

若 cMT/cMT X 系列 HMI 有遠端監控的需求，使用者可以透過 cMT Viewer 來監控畫面。建議在 HMI 的系統設定修改各個權限的密碼，於 cMT Viewer 中使用各個權限的密碼皆可登入監控畫面，系統密碼設定頁面如下圖。


設定
系統設定
系統密碼
進階安全模式
VNC 設定
EasyAccess 2.0
語言
輸入法
系統密碼
系統設定
更新工程檔案
歷史
使用者

系統密碼

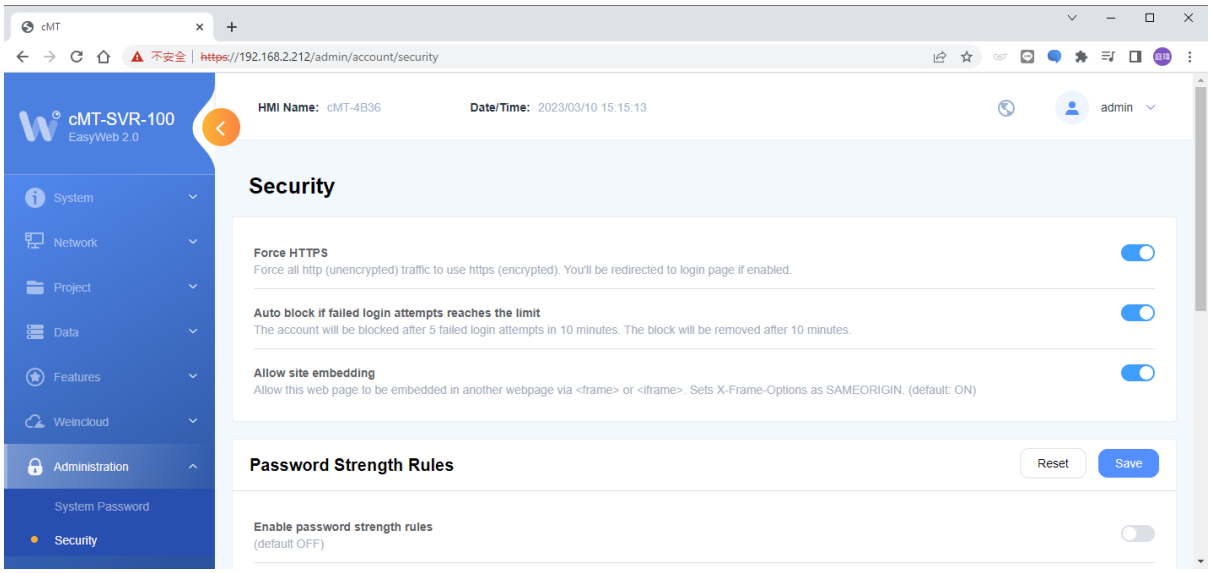
4.2 網頁安全

cMT/cMT X 系列 HMI 可透過網頁登入設定頁面 EasyWeb 2.0 並具備各種功能，包含設定網路 IP、上傳下載工程檔案、備份資料等至關重要的內容，所以網頁的安全也是必須按照建議設定來進行保護。

4.2.1 啟用 HTTPS 安全加密通訊

建議啟用 HTTPS 加密通訊。

進入 EasyWeb 2.0 之後，從左方 [Administration] 開啟 [Security] 頁面，啟用 [Force HTTPS] 選項，如下圖。

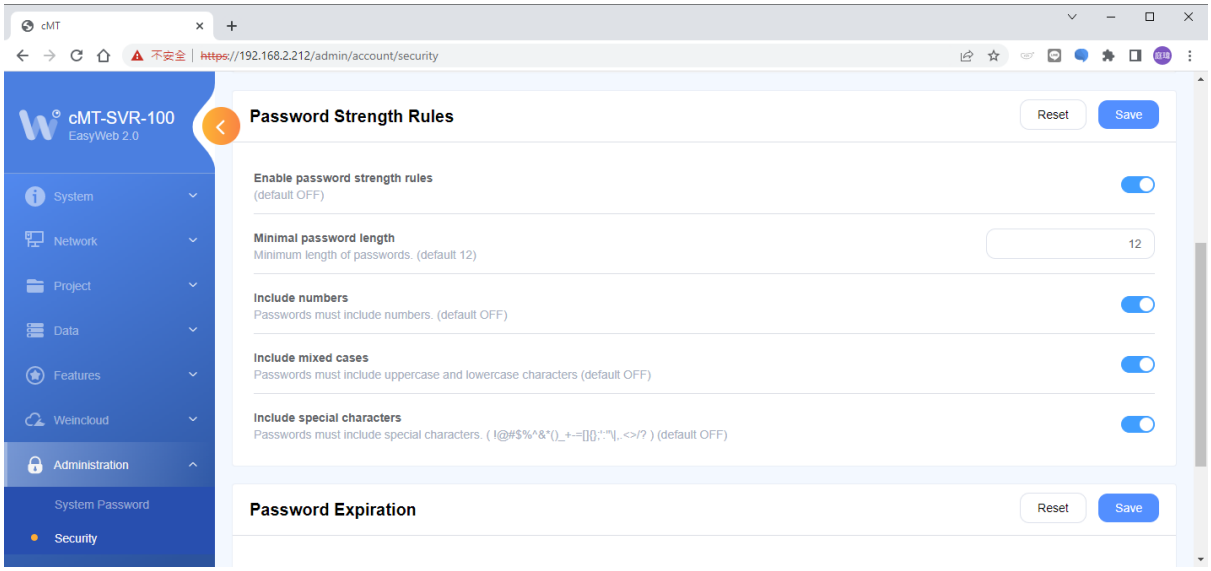


Force HTTPS

4.2.2 啟用系統密碼強度規則

建議啟用系統密碼強度規則。針對登入網頁密碼的長度、大小寫、特殊字元進行強制使用的限制，可強化網頁整體的安全性。

進入 EasyWeb 2.0 之後，從左方 [Administration] 開啟 [Security] 頁面，在 [Password Strength Rules] 的範圍進行設定，設定完畢請使用 Save 儲存，如下圖。

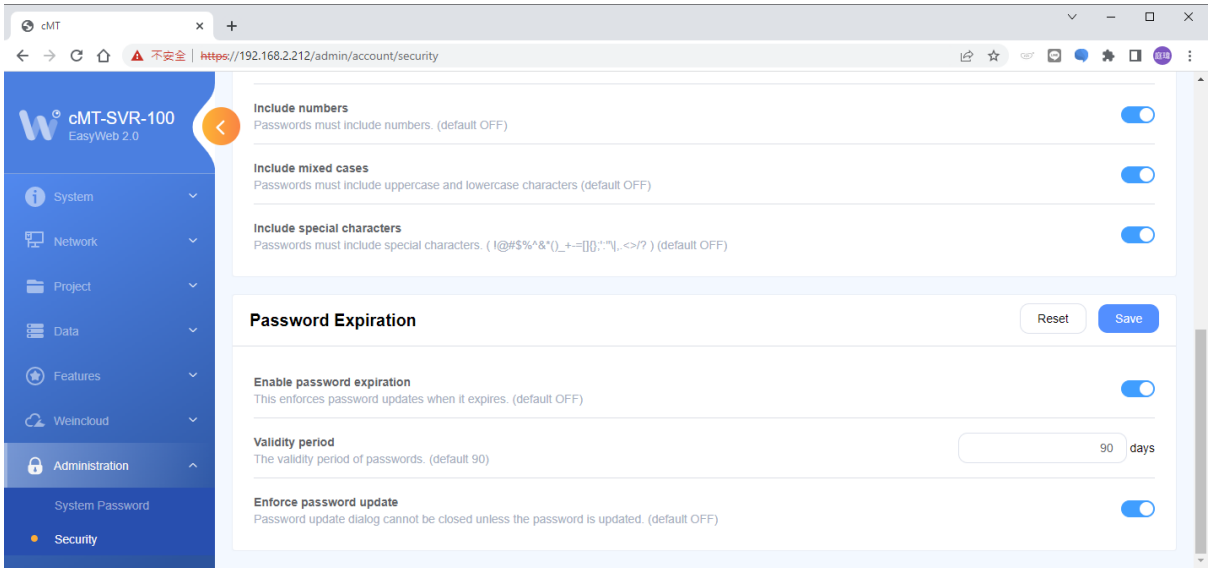


Password Strength Rules

4.2.3 啟用系統密碼有效期限

建議啟用系統密碼有效期限。在此可設定天數，若系統密碼使用期限到期後建議強制更換新的系統密碼。

進入 EasyWeb 2.0 之後，從左方 [Administration] 開啟 [Security] 頁面，在 [Password Expiration] 的範圍進行設定，設定完畢請使用 Save 儲存，如下圖。

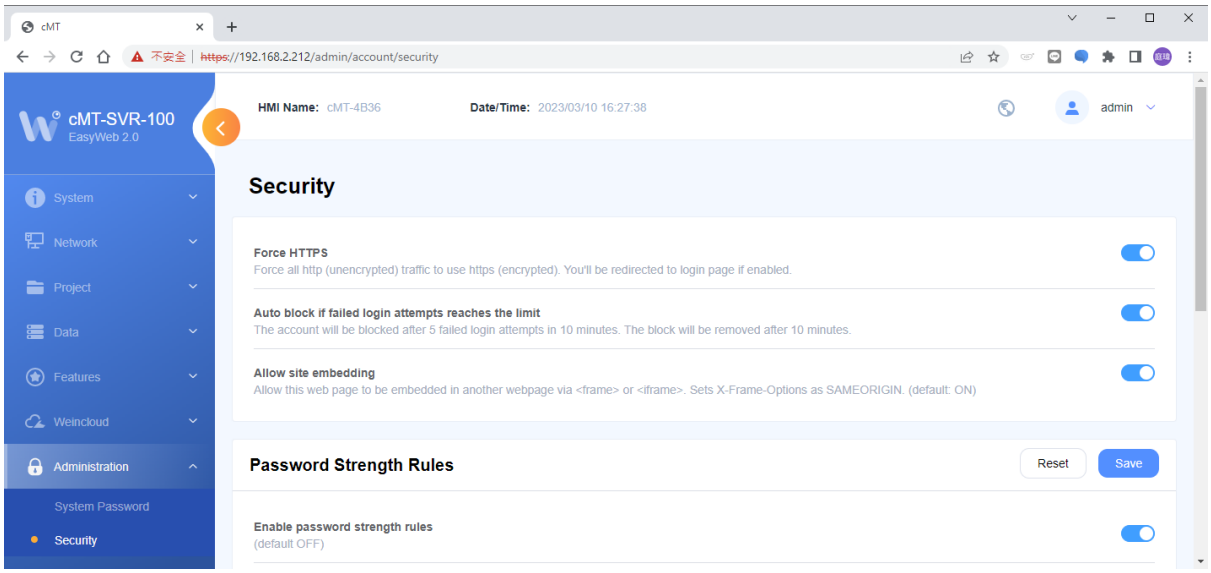


Password Expiration

4.2.4 啟用登入失敗鎖定功能

建議啟用登入失敗鎖定功能。使用者在登入其網頁時，若嘗試5次密碼都登入失敗的話，該系統將會停止 10 分鐘。

進入 EasyWeb 2.0 之後，從左方 [Administration] 開啟 [Security] 頁面，啟用 [Auto block if failed login attempts reaches the limit] 選項，如下圖。

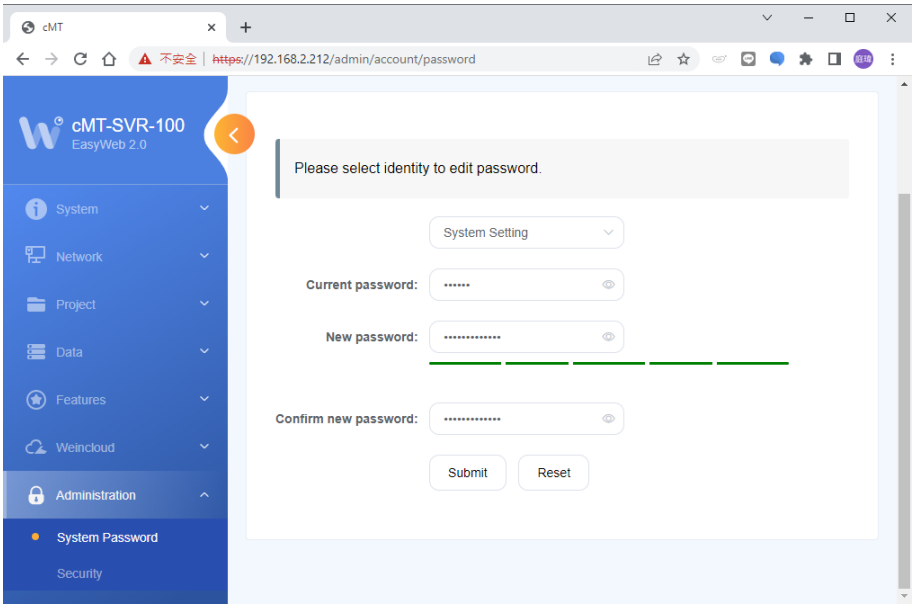


Auto block if failed login attempts reaches the limit

4.2.5 修改出廠預設系統密碼

經過上述網頁設定的修改之後，請修改出廠預設系統密碼，並變更至高強度密碼。

進入 EasyWeb 2.0 之後，從左方 [Administration] 開啟 [System Password] 頁面，可在此重新設定系統登入密碼，如下圖。



修改系統密碼

4.3 定期安全維護活動 (SG-3f)

定期的資訊安全維護活動是確保您的系統和數據持續安全的關鍵部分。以下是一些建議的定期資訊安全維護活動：

- 定期更新軟體：確保您的作業系統、應用程式和所有相關的軟體都保持最新的安全更新和修補程序。這可以防止已知漏洞被利用。
- 定期更換密碼：建議定期更換用戶帳戶的密碼，並要求使用強大的密碼，包括大小寫字母、數字和特殊符號。
- 定期備份數據：執行定期的數據備份，並確保備份存儲在安全的位置。這可以保護您的數據免受潛在的故障風險或攻擊。
- 定期強化防火牆和入侵防護系統：確保防火牆和入侵防護系統保持最新且有效。這些工具可以幫助阻止不明來源的網路流量進入您的系統。
- 定期漏洞掃描和測試：定期執行系統漏洞掃描和安全測試，以發現可能的安全漏洞並及時加以修復。
- 定期審查權限和訪問控制：定期審查用戶的權限和訪問控制，確保只有授權的用戶可以訪問敏感資源。
- 定期監控日誌：定期檢查系統和應用程式的日誌，以檢測潛在的安全事件或異常活動。
- 定期進行安全稽核：定期進行內部或外部的安全稽核，以確保您的資訊安全措施符合標準和最佳實踐。

5. 產品安全汰除指南 (SG-4)

本節闡述產品需安全除役是為確保設備除役或下線時，不會因其退役而造成資訊安全問題。(e.g.機敏資訊外洩等等)

5.1 安全除役的建議

- 將產品從設備配置中移出且不造成任何物理損壞。
- 透過重置 HMI 的方式來完整刪除產品中的程式和配置數據。
- 安全刪除產品與外部儲存裝置中留存的歷史檔案。
- 安全處置產品（物理銷毀），以防止產品中包含的無法刪除的數據可能被洩露。