HERHSIANG

MArchive 系列歸檔伺服器

2023

DKIM & DMARC 驗證機制設定方式

技術文件製作: HERHSIANG FREEDY

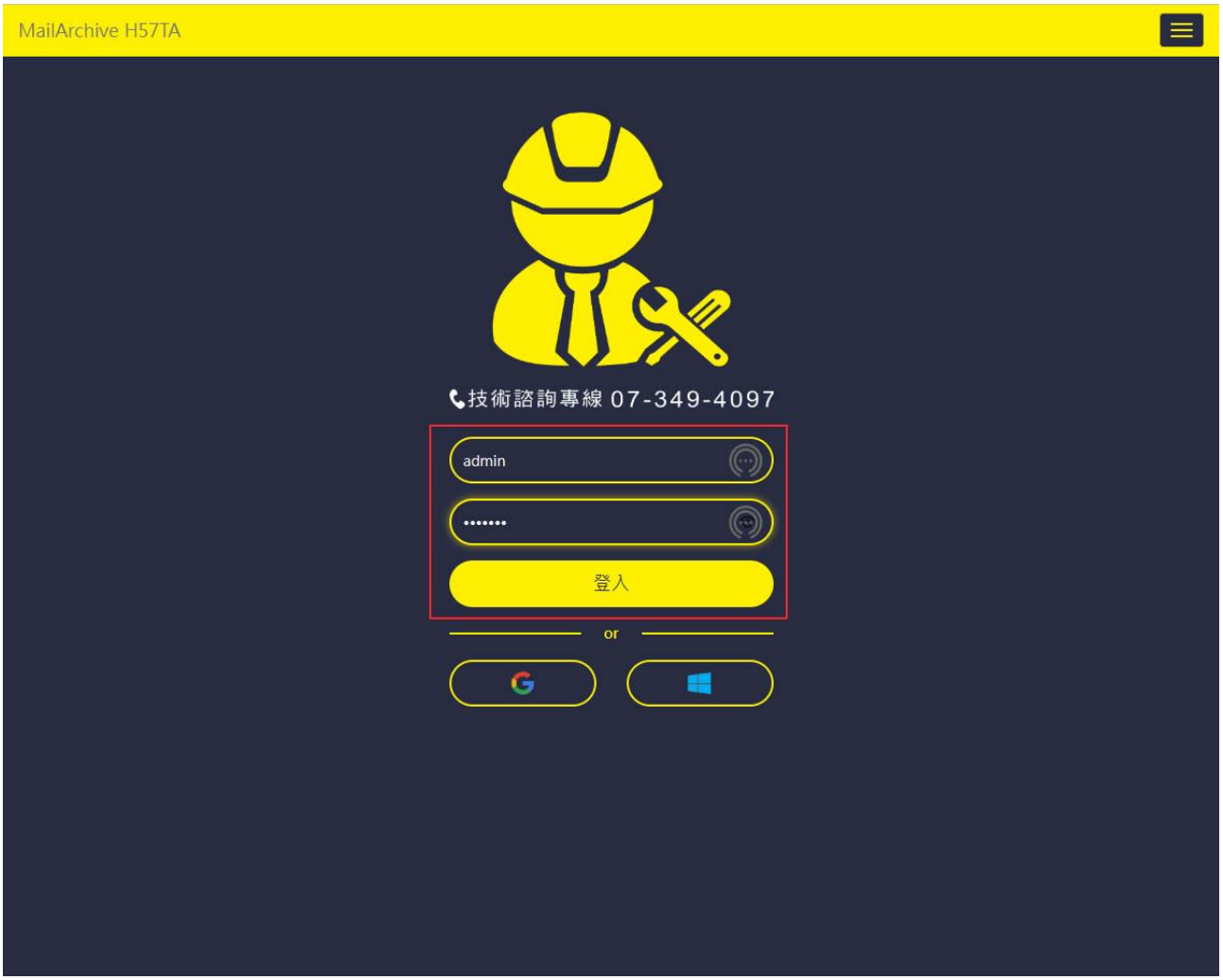
驗證機制說明:
DKIM (DomainKeys Identified Mail)，網域驗證郵件，用來防止郵件內容遭到竄改
跟隨 MArchive 郵件歸檔伺服器內建功能產生，設定於管理網域 DNS SERVER.

DMARC 是用來輔助 SPF 與 DKIM 的不足跟隨 DKIM 功能內建於設備, DKIM 生效 DMARC 自動生效.

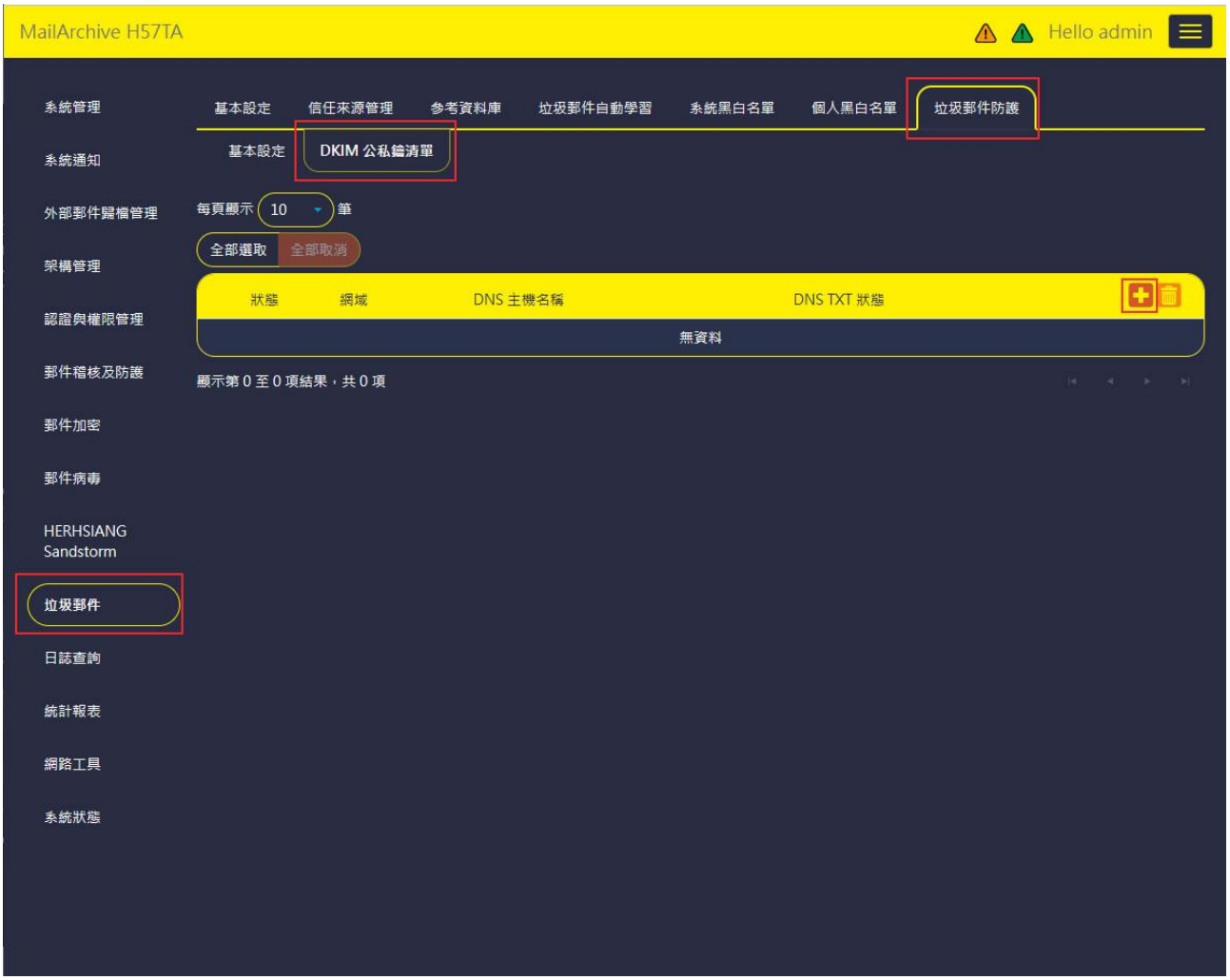
以下輸入 IP&帳號&密碼皆以出廠預設值及網域輸入以官網網域 herhsiang.com.tw 為範例，如已修改 IP&帳號&密碼請換成已修改 IP&帳號&密碼輸入

MArchive 歸檔伺服器如何設定產生 DKIM:

1. 瀏覽器輸入 https://192.168.2.1:88 登入郵件歸檔管理介面，輸入管理帳號 / 密碼:admin / adminpw



2. 進入畫面後選擇左邊欄位垃圾郵件選擇上面欄位垃圾郵件防護選擇 DKIM 公私鑰清單按+符號新增



3. 選擇自家網域，前置字串請自訂，金鑰大小請自選, 1024 一般 DNS Server 及代管都能接受, 2048 一般 DNS Server 及代管不一定能接受甚至需另外付費, 1024 及 2048 有些代管需另外付費, 2048 相對安全性高對方接受率也相對高，按新增及產生相對自家網域驗證數據.

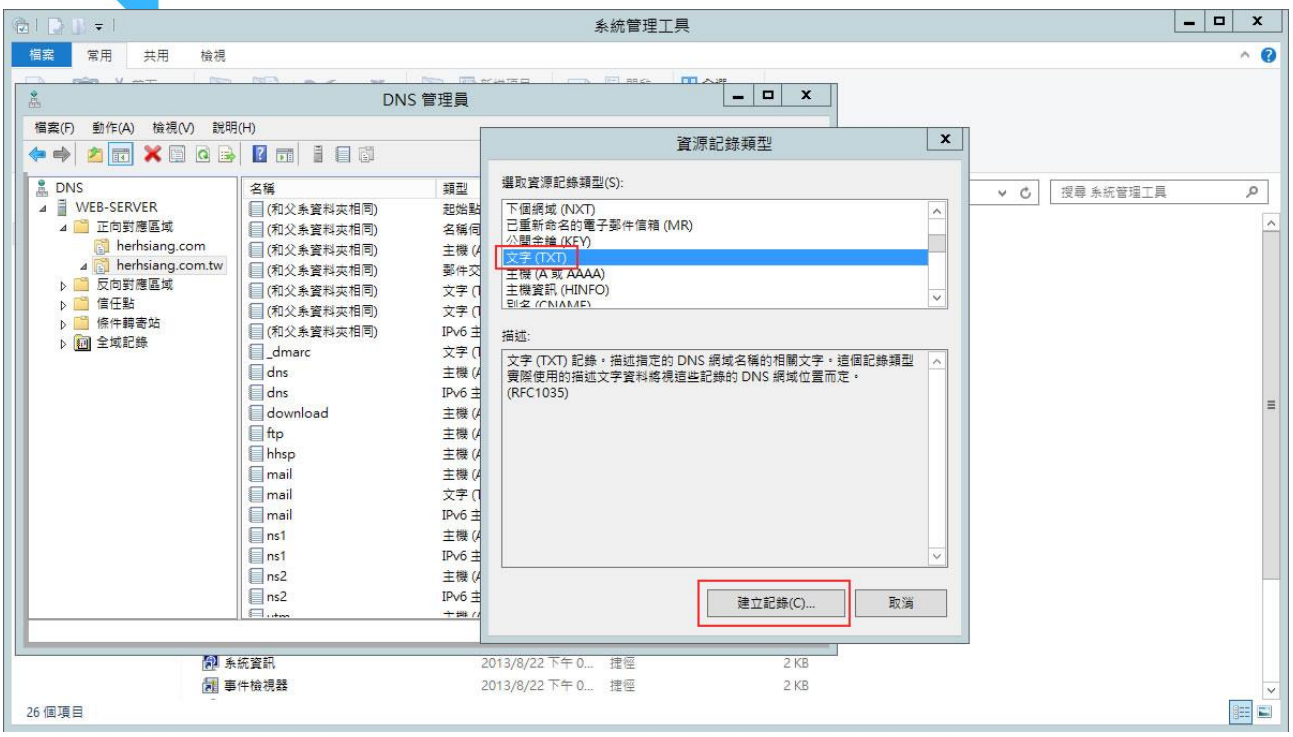
技術文件製作: HERHSIANG FREEDY

4. 選擇啟用，先點說明，說明說將相對應參數複製下來，將該參數新增到自管 DNS Server 或代管 DNS 做 TXT，將 DNS 主機名稱及 TXT 資料等參數先複製至記事本備用，按確定，如要重新產生新金鑰請按重新產生金鑰.

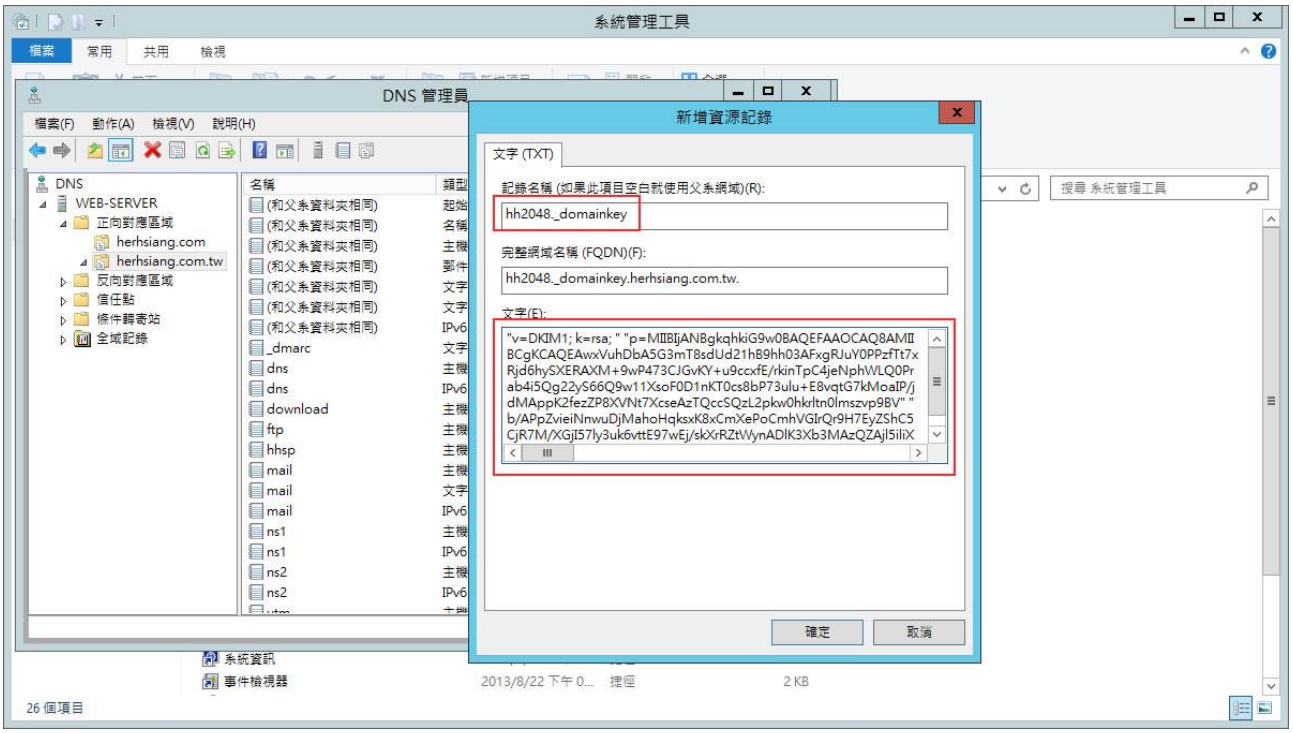
5. 步驟 4 案確定後會產下圖片顯示已新增成功，但因 DKIM 金鑰參數還未加入 DNS Server 及代管 DNS，所以設備檢測顯示沒有 TXT 資料.
P.S. 有些 DNS Server 及代管不接受金鑰所產生特殊字元，但並不一定無效，請利用 Google gmail.com 郵件帳號檢測，檢測方式請 Google 搜尋相關測試方式，這裡不再說明.

6. 參數格式說明
hh2048._domainkey.herhsiang.com.tw (前置字串+自家網域即為 DKIM 設定於 DNS Server 或代管 DNS TXT 說明網域，而非設定主網域 herhsiang.com.tw)

7. 範例為 WINDOWS SERVER DNS SERVER，新增文字 TXT，按建立記錄

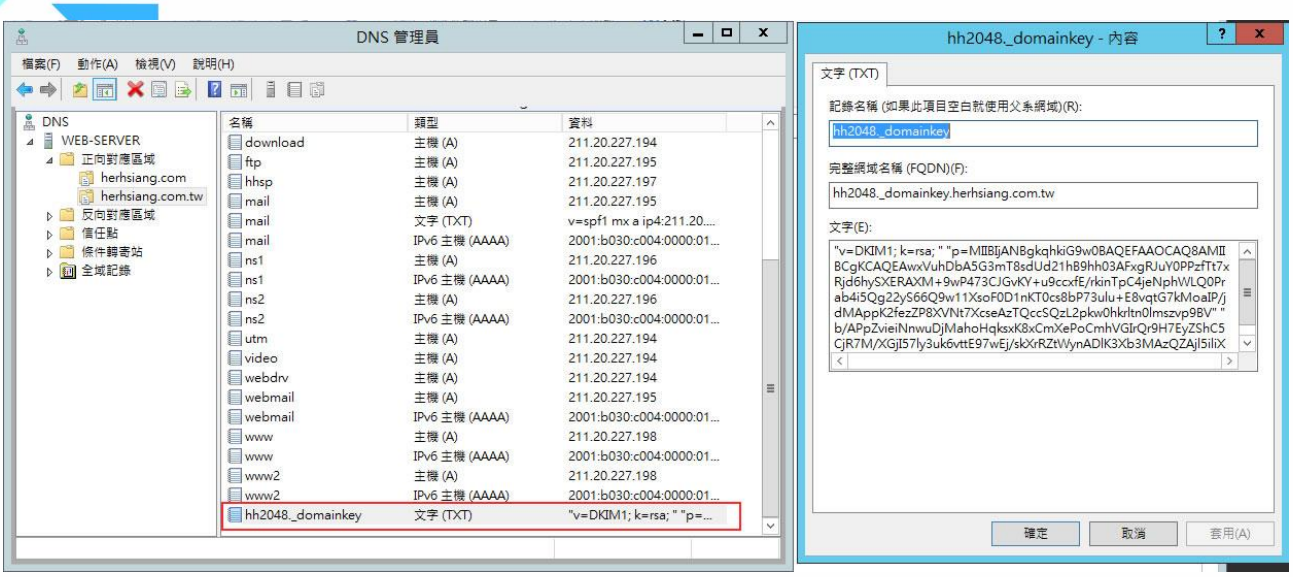


8. 將複製到記事本 DKIMR 金鑰參數複製到 TXT 設定欄位內，按確定即新增 TXT 參數成功.

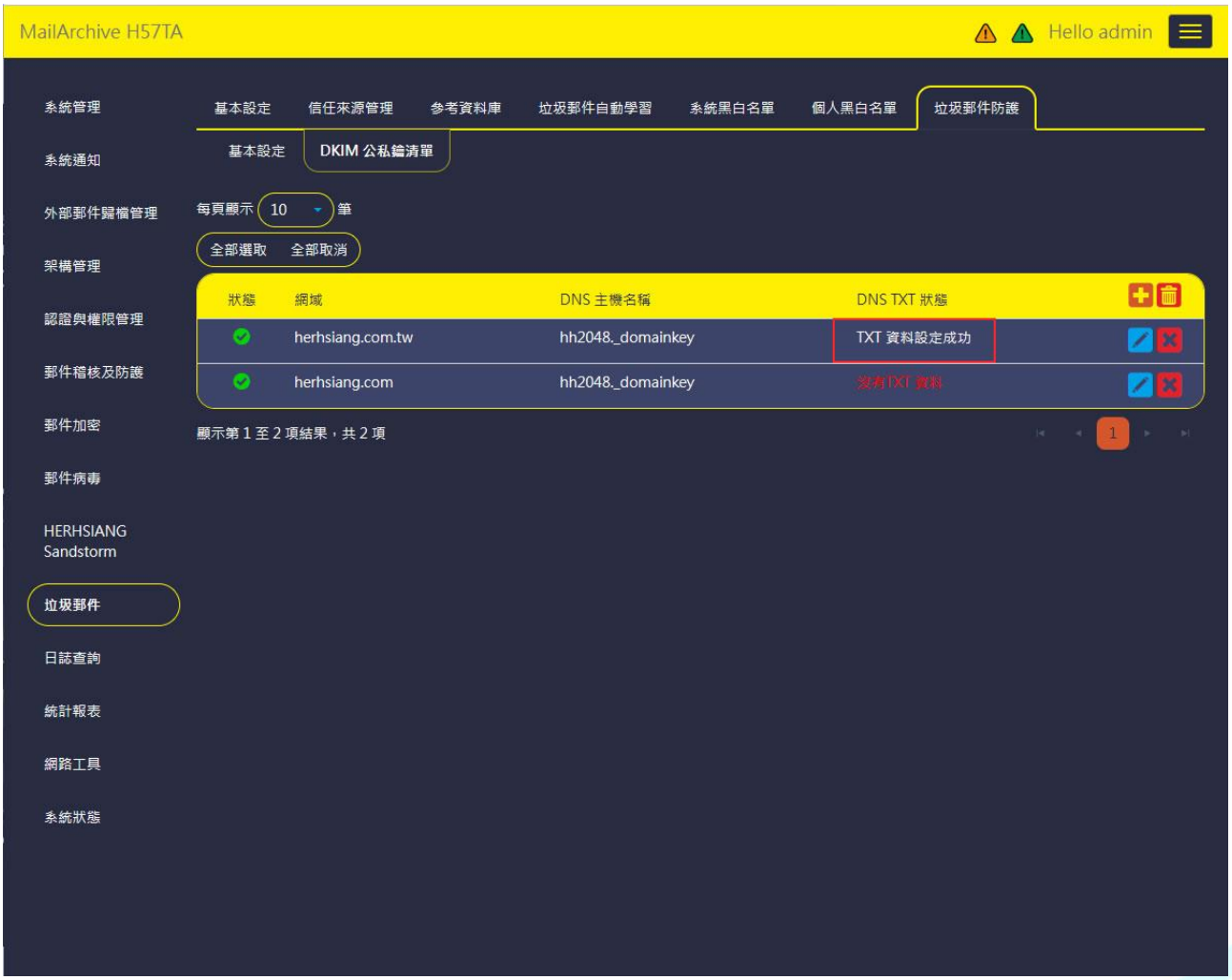


9. 再次核對設定資料

技術文件製作: HERHSIANG FREEDY



10. 待生效後，再次檢測顯示, TXT 資料設定成功，即完成 DKIM 驗證機制設定完成，請確定 SPF 驗證機制已生效, SPF+DKIM 兩者都生效 DMARC 驗證機制也會自動生效,.



技術文件製作: HERHSIANG FREEDY

11. 啟動 DKIM 驗證功能，即完成 DKIM 及 DMARC 我方網域驗證機制.