UMail V5 增加 SPF/DKIM/DMARC 的 DNS 紀錄

[說明]

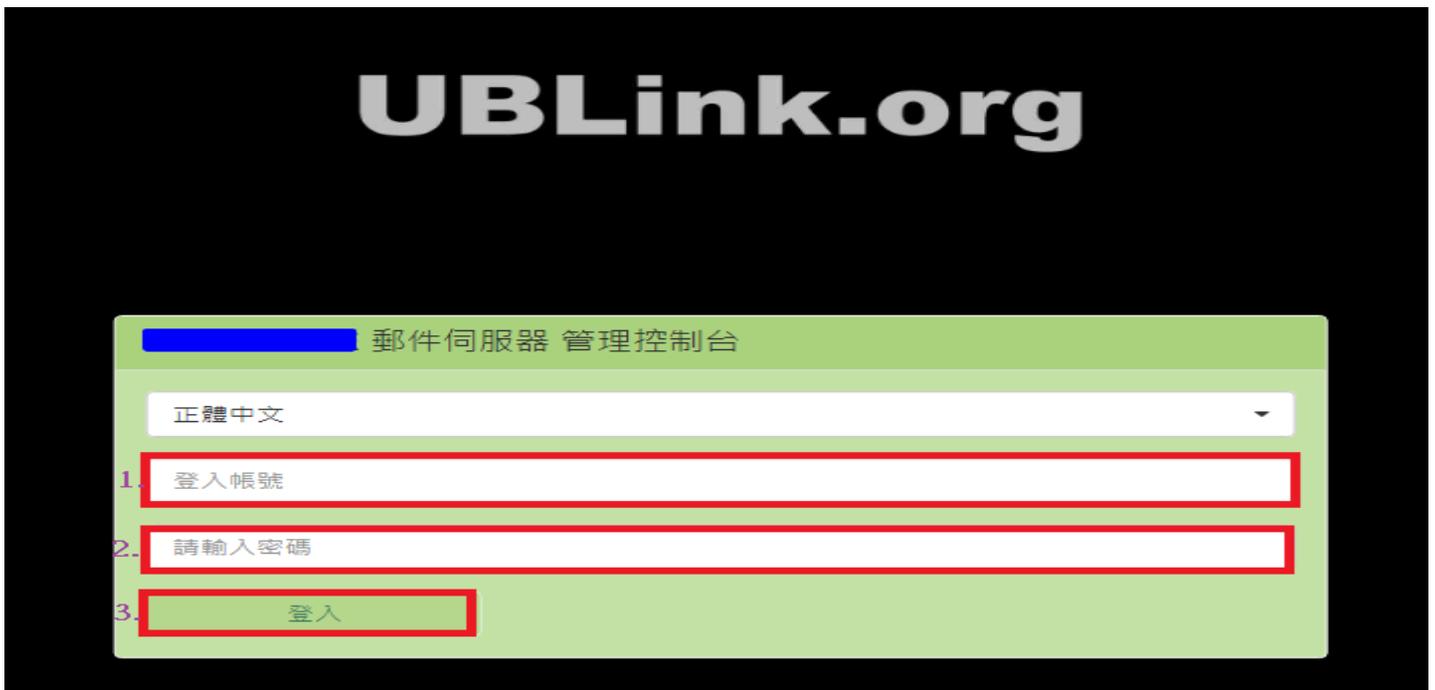使用 SPF/DKIM/DRARC 這 3 種電子郵件標準可以防範偽造郵件或詐騙郵件，有助於確保你發送的郵件不會被標記為垃圾郵件。

SPF：發送郵件的服務器和網域名稱。

DKIM：為每封外送郵件添加數字簽名，讓接收郵件的主機驗證郵件是否確實來自貴公司的網域。

DMARC：告知接收郵件的主機如何處理來自未通過 SPF 或 DKIM 檢查的郵件。

PS：偽造的郵件看上去像來自於某個網域，而實際上相對應單位的網域是攻擊者偽造的，DKIM 可檢測出郵件遭偽造的情況，以及郵件發信人地址是否來自於某網域。

[步驟 1] 登入 UMail V5 管理界面，請依照下面畫面操作。
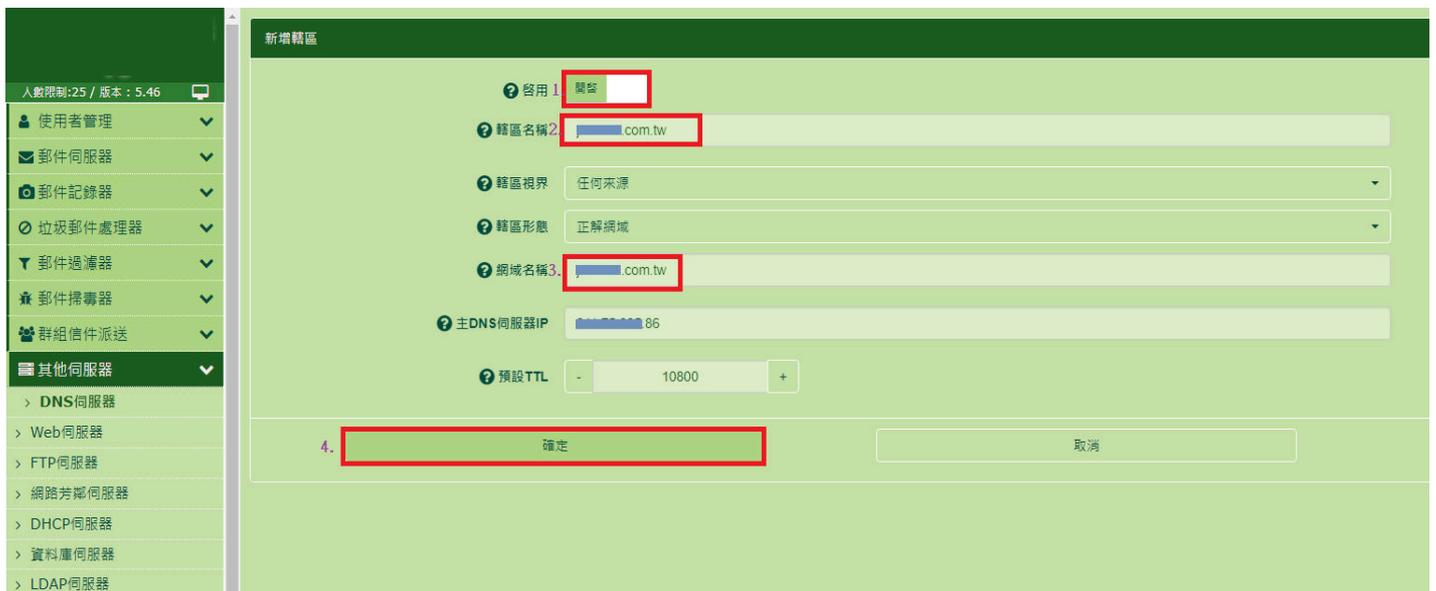

[步驟 2] 產生網域的 DKIM 資料，請依照下面畫面操作。

[步驟 3] 設定 DNS 伺服器，請依照下面畫面操作。

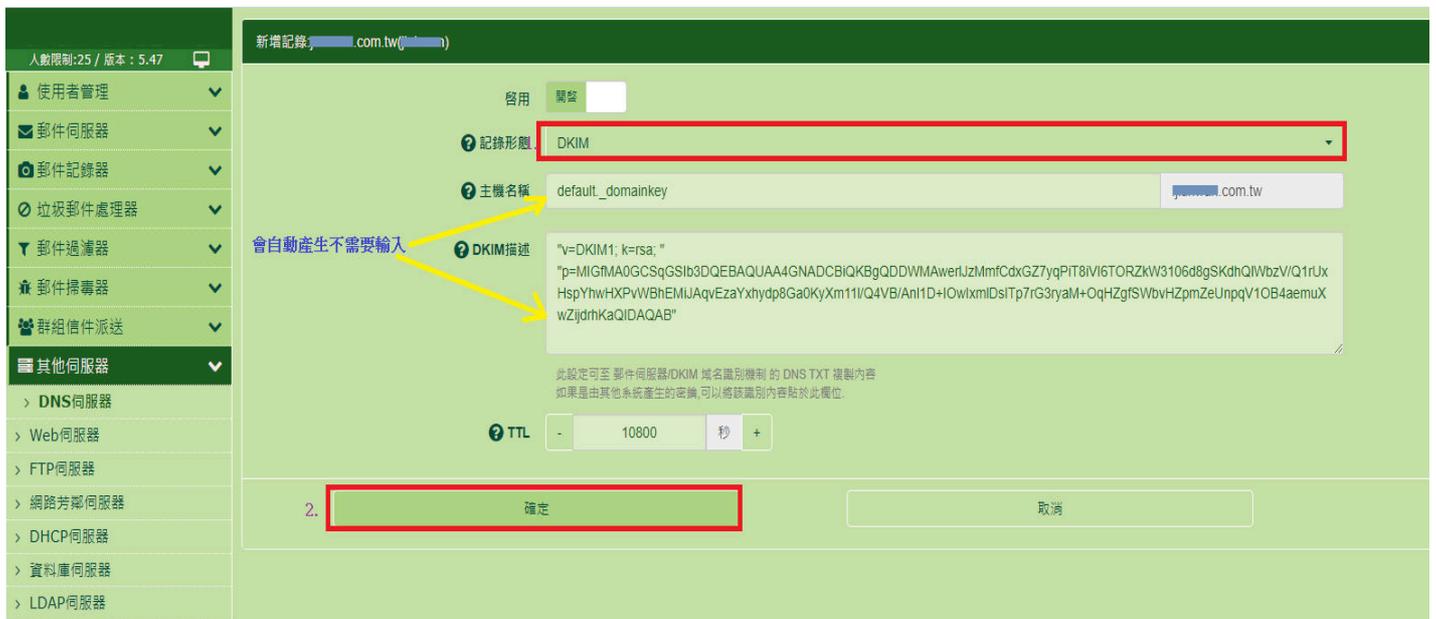**[步驟 4]** 新增網域資料，請依照下面畫面操作。

[步驟 5] 輸入網域名稱與 DNS 伺服器外部 IP，請依照下面畫面操作。

[步驟 6] UMail V5 建好的網域資料如下(NS/A/MX/SPF 等...)，請點選 **[新增]**。

基本設定　轉區zone管理

● ● j_____.com.tw
(j_____.com.tw)

⊕ 新增轉區　✎ 編輯轉區　🗑 刪除轉區　⬆ 匯出轉區　⬇ 匯入轉區

✚ 新增　🗑 刪除

顯示第 1 到第 9 項記錄，總共 9 項記錄

	啟..↕	主機名稱	TTL	形態	設定值	操作
☐	●	dns	10800	A	____.86	✎ 🗑
☐	●	ns	10800	A	____.86	✎ 🗑
☐	●	@	10800	A	____.86	✎ 🗑
☐	●	mail	10800	A	____.86	✎ 🗑
☐	●	@	10800	MX	10 : j____.com.tw	✎ 🗑
☐	●	@	10800	MX	10 : mail.j____.com.tw	✎ 🗑
☐	●	@	10800	NS	dns	✎ 🗑
☐	●	@	10800	NS	ns	✎ 🗑
☐	●	@	10800	SPF	v=spf1 a mx -all	✎ 🗑

顯示第 1 到第 9 項記錄，總共 9 項記錄

[步驟 7] 記錄型態選擇 **[DKIM]**，請依照下面畫面操作。

新增記錄:j____.com.tw(j____)

啟用　開啟

記錄形態　DKIM

主機名稱　default._domainkey　　j____.com.tw

會自動產生不需要輸入

DKIM描述　"v=DKIM1; k=rsa; "
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDWMAwerIJzMmfCdxGZ7yqPiT8iVI6TORZkW3106d8gSKdhQlWbzV/Q1rUxHspYhwHXPvWBhEMiJAqvEzaYxhydp8Ga0KyXm11I/Q4VB/AnI1D+IOwIxmIDslTp7rG3ryaM+OqHZgfSWbvHZpmZeUnpqV1OB4aemuXwZijdrhKaQIDAQAB"

此設定可至 郵件伺服器/DKIM 域名識別機制 的 DNS TXT 複製內容
如果是由其他系統產生的密鑰，可以將該識別內容貼於此欄位

TTL　-　10800　秒　+

2.　確定　　　　取消

[步驟 8] 接下來在新增一筆 DMARC，請在記錄型態選擇 **[DMARC]**，請依照下面畫面操作。
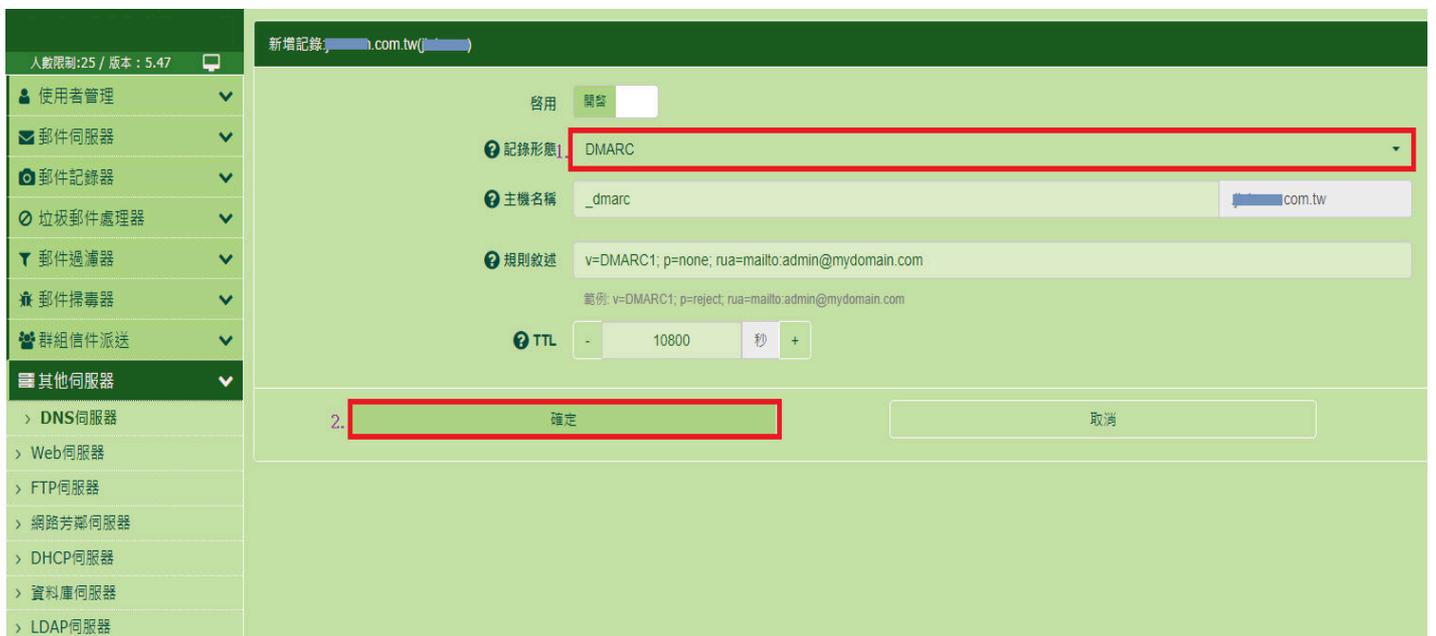
新增記錄:j____.com.tw(j____)

啟用　開啟

記錄形態　DMARC

主機名稱　_dmarc　　j____.com.tw

規則敘述　v=DMARC1; p=none; rua=mailto:admin@mydomain.com

範例: v=DMARC1; p=reject; rua=mailto:admin@mydomain.com

TTL　-　10800　秒　+

2.　確定　　　　取消

[步驟 9] DKIM 與 DMARC 新增完成後，會看到如下的畫面。

以上步驟就完成了在 UMail V5 增加 SPF/DKIM/DRARC 的 DNS 紀錄了，接下來要驗證
SPF/DKIM/DMARC 的紀錄是否有效。

[步驟 10] 打開瀏覽器，在網址輸入-> https://easydmarc.com/tools/spf-lookup，請依照下面畫面操作。

[步驟 11] SPF 紀錄的檢查結果如下(SPF 是有效的，並且查到了 2 筆 SPF 的紀錄)。

[步驟 12] 打開瀏覽器，在網址輸入-> https://easydmarc.com/tools/dkim-lookup，請依照下面畫面操作。

[步驟 13] DKIM 紀錄的檢查結果如下(DKIM 是有效的，並且看到了 DKIM Key 的資料)。

[步驟 14] 打開瀏覽器，在網址輸入-> https://easydmarc.com/tools/dmarc-lookup，請依照下面畫面操作。。

[步驟 15] DMARC 紀錄的檢查結果如下(DMARC 是有效的，並且看到了 DMARC 的資料)。

經過步驟 10~步驟 15 的 SPF/DKIM/DMARC 檢查，確認了我們在 UMail V5 上面增加的 SPF/DKIM/DMARC 的 DNS 紀錄是正確無誤的。