郵件守門員服務

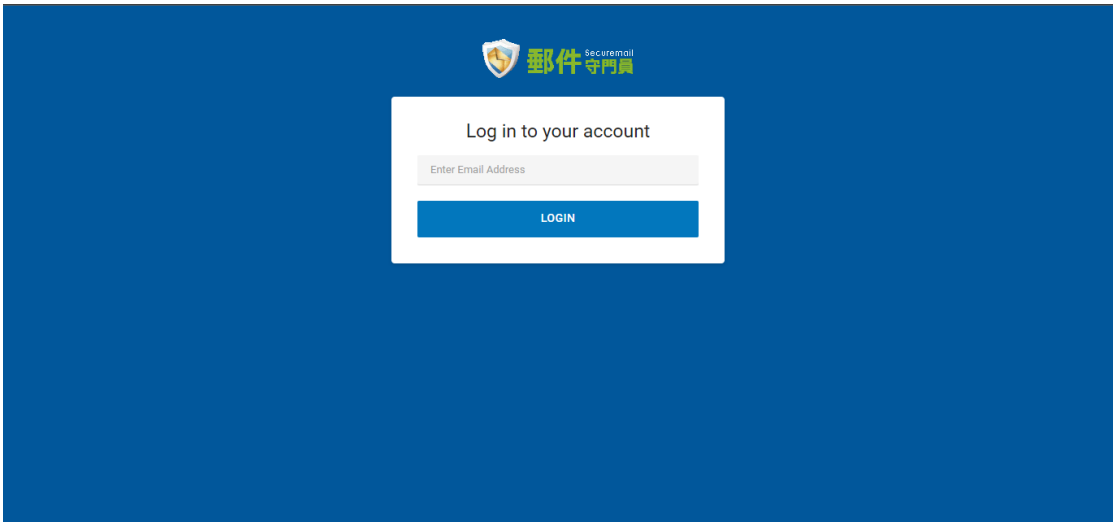
快速設定指南

登入使用者介面

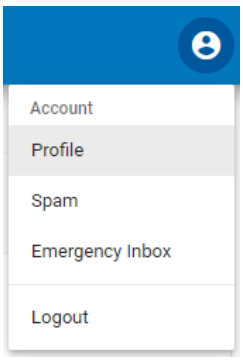
當公司所申請的郵件守門員服務啟用後，管理者便可依據服務啟用通知信內的管理者帳號與密碼來登入使用者介面。為了確保郵件守門員服務能順利運作，管理者須先行至使用者介面進行初步的設定，其相關設定項目如下：

- 使用者管理
- 垃圾郵件設定
- 垃圾郵件隔離摘要設定
- 內送電子郵件傳送目的地設定
- 外寄郵件轉寄設定（選項）

在郵件守門員服務使用者介面(https://securemail.cloud-protect.net/app/login.php)輸入服務啟用通知信內的管理者帳號，點選「LOGIN 按鈕」，再輸入密碼與點選「LOGIN 按鈕」後即可登入使用者介面。

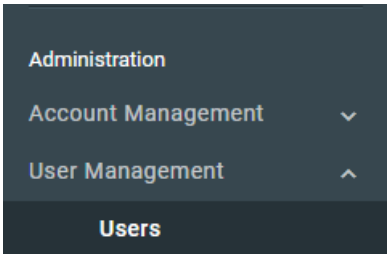


注意：使用服務啟用通知信內的管理者帳號與密碼登入後，建議您從右上角的使用者圖示，點選下拉選單中的「Profile 選項」變更密碼。

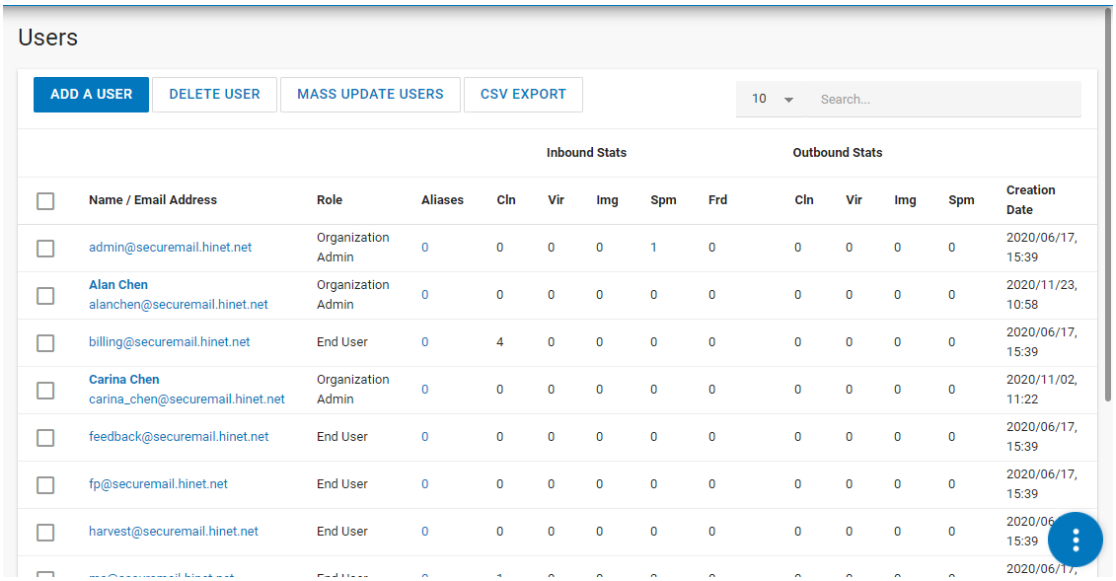


使用者管理

1. 點選「User Management > Users 選項」。



2. 在 Users 頁面會列出已建立的使用者。



注意：當郵件守門員服務啟用後，任何電子郵件傳送到未建立的使用者電子郵件地址將不會被接收，而且會引發 SMTP 550 的錯誤。

3. 確認所有對外收信的使用者電子郵件地址、別名地址與群組電子郵件地址是否都已建立與正確無誤。您可以透過手動或匯入的方式管理使用者。

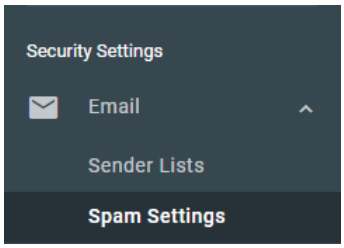
   注意：請在使用者設定使用者的**別名地址**。

   警告：在確認所有的電子郵件地址清單正確無誤之前，請勿將 MX 紀錄指到郵件守門員服務。否則寄到有效地址的電子郵件可能會遭拒。

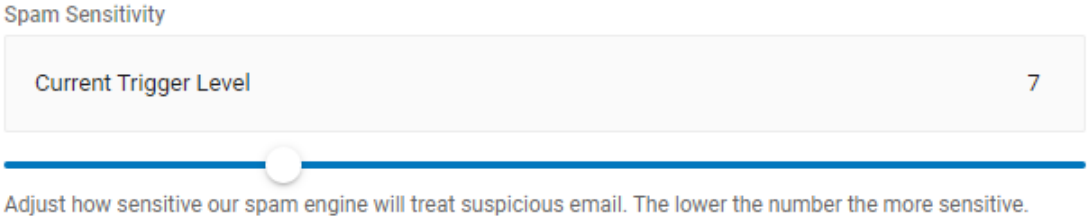
注意：*有關使用者管理的詳細資訊，請參閱《**郵件守門員服務管理者指南**》的使用者管理說明。*

垃圾郵件設定

1. 點選「Email > Spam Settings 選項」。

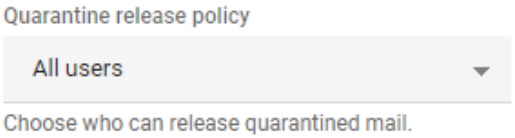


2. 垃圾郵件敏感度（Spam Sensitivity）



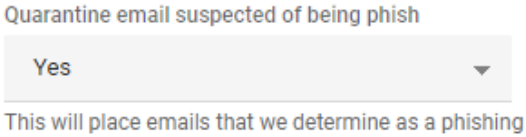
顯示垃圾郵件敏感度的目前觸發設定值(Current Trigger Level，預設值為 7)，以及調整垃圾郵件引擎敏感度。**數值越低，垃圾郵件過濾越嚴謹，數值越大，垃圾郵件過濾越寬鬆。**

3. 隔離郵件釋放政策（Quarantine Release Policy）



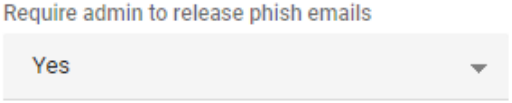
設定被隔離的垃圾郵件可由**使用者（All users）自行釋放**或**只能由管理者（Admin users only）釋放**。

4. 隔離網路釣魚郵件（Quarantine email suspected of being phish）



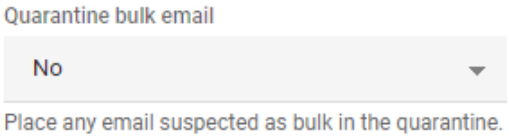
設定是否將判定為網絡釣魚郵件放置在隔離區。

5. 需由管理者釋放網路釣魚郵件（Required admin to release phishing emails）



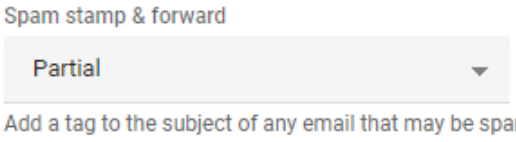
設定被隔離的網路釣魚郵件**需由管理者釋放，使用者無法自行釋放**。

6. 隔離大量發送的電子郵件（Quarantine bulk email）



設定是否將判定為大量發送的電子郵件放置在隔離區。

7. 垃圾郵件註記與轉寄（Spam stamp & forward）

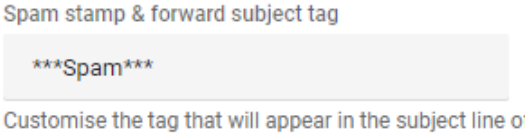


設定是否將垃圾郵件註記與轉寄的主旨標籤內容(預設值:“ ***Spam***”)附加在垃圾郵件主旨前，再轉寄給收件者。可在組織或使用者垃圾郵件設定啟用此選項。

此選項有以下設定值：

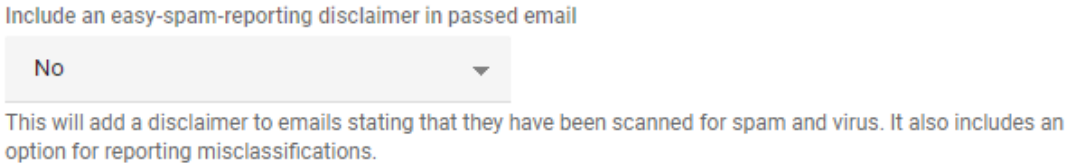
- **No**：停用此選項。
- **Partial**:**垃圾郵件分數介於 9 分與 19 分之間的垃圾郵件將套用此選項**。
- **All**：所有垃圾郵件套用此設定。

8. 垃圾郵件註記與轉寄的主旨標籤（Spam stamp & forward subject tag）



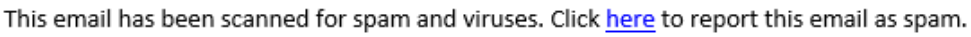
設定在啟用垃圾郵件註記與轉寄選項時，會套用在垃圾郵件主旨行前的標籤內容。

9. 在通過的電子郵件中附加垃圾郵件回報的免責聲明（Include an easy-spam-reporting disclaimer in passed email）

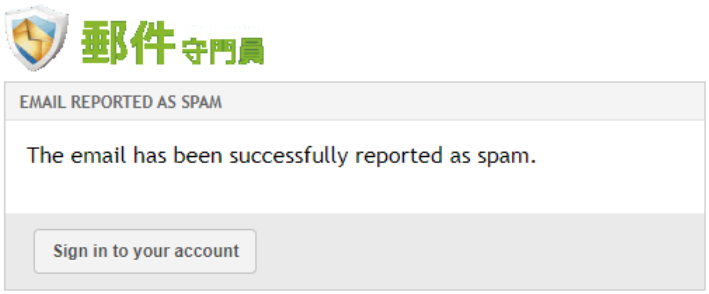


設定是否在通過郵件守門員服務所處理的每封內寄郵件中附加垃圾郵件回報免責聲明。該免責聲明會附加在每封 HTML 格式或文字格式郵件的底部，並提供連結連到垃圾郵件隔離區。這使郵件的收件者可從電子郵件本身直接回報該郵件給郵件守門員服務，從而使垃圾郵件引擎得知回報的電子郵件是收件者不要的郵件，並更新引擎的學習。

免責聲明內容如下：



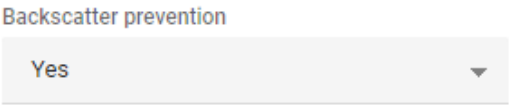
點擊免責聲明中的連結，收件者將被重導至垃圾郵件隔離區，並將該郵件回報為垃圾郵件。此外，收件者也可以將寄件者的電子郵件地址或網域加入使用者的封鎖寄件者清單來阻擋。



10. 內寄電子郵件網域詐騙保護（Inbound domain spoofing protection）

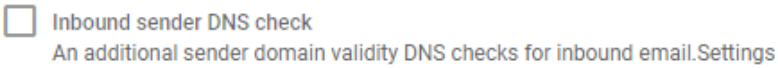
設定是否啟用防止詐騙的電子郵件威脅，如、商業詐騙郵件（BEC）或 CEO 偽冒郵件。

11. 電子郵件退信防護（Backscatter prevention）



設定是否啟用防止電子郵件退信攻擊的威脅。

12. 內寄電子郵件寄件者 DNS 檢查（Inbound sender DNS check）



設定是否啟用內寄郵件寄件者 DNS 檢查以提供另一層防垃圾郵件的保護，有助於確保不接收沒有目的地的退信。

此選項將執行兩個額外的 DNS 檢查：

1. 寄件者網域是否有 MX 記錄。
   - 檢查郵件是否可以退回，並稍後有需要時可以退還給寄件者。
   - 如果 MAIL FROM 網域具有以下條件，則該請求將被拒絕：
     - 沒有 DNS A 紀錄或 MX 記錄。
     - 格式錯誤的 MX 記錄，例如、MX 記錄的主機名稱長度為零。
2. 寄件者網域是否包含指向私有或保留 IP 範圍的 MX 記錄（例如，

10.0.0.0/8、127.0.0.0/8 等）。

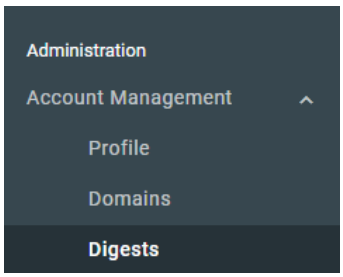
- 如果寄件者網域的 MX 指向內部 IP 地址，則請求將被拒絕。

建議啟用此選項，但是關閉此選項不會帶來重大風險。

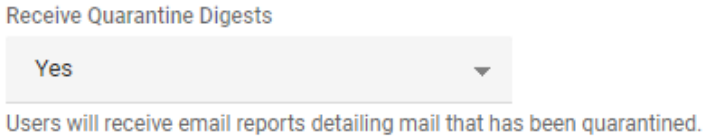
注意：*有關於垃圾郵件設定詳細資訊，請參閱《**郵件守門員服務管理者指南**》的垃圾郵件設定說明。*

垃圾郵件隔離摘要設定

1. 點選「Account Management > Digests 選項」。

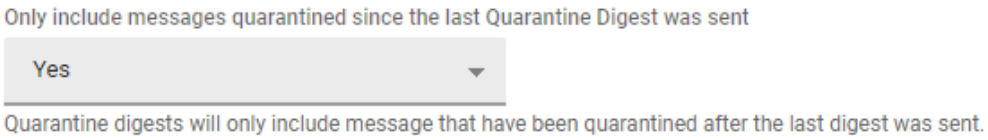


2. 收到垃圾郵件隔離摘要（Receive Quarantine Digests）



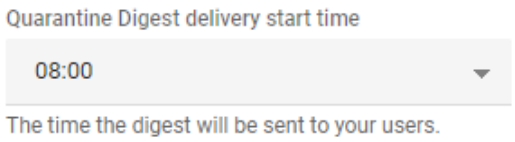
設定使用者是否收到垃圾郵件隔離摘要。

3. 僅包含自上次垃圾郵件隔離摘要發送以後被隔離的郵件（Only include messages quarantined since the last Quarantine Digest was sent）



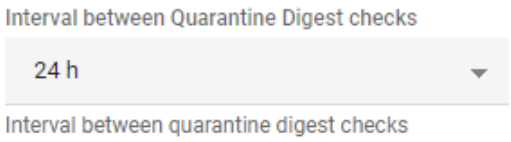
設定是否自上次垃圾郵件隔離摘要發送後有新隔離垃圾郵件時，才發送垃圾郵件隔離摘要。

4. 垃圾郵件隔離摘要發送起始時間（Quarantine Digest delivery start time）



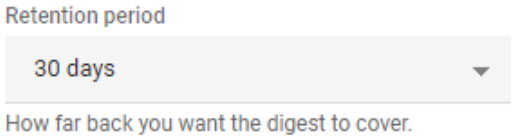
設定垃圾郵件隔離摘要發送排程的起始時間。例如，如果您選擇 08:00，則發送時間將為 8:00 AM，而發送間隔（請參見下文）將以起始時間為基準。時間的表示取決於帳戶資訊（Account Management > Profile）中的時區設定。

5. 垃圾郵件隔離區摘要發送的時間間隔（Interval between Quarantine Digest checks）



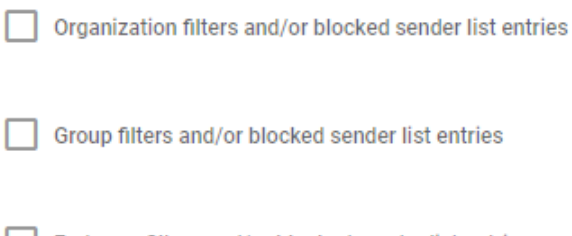
設定垃圾郵件隔離摘要發送的頻率。預設值為 24 小時，可以選擇 12 小時、8 小時、6 小時或 4 小時。例如、垃圾郵件隔離摘要在本地時間 3:00 AM 送出（取決於帳戶資訊的時區設定），而一天中的其他送出時間取決於選擇的時間間隔。

6. 保留期間（Retention period）



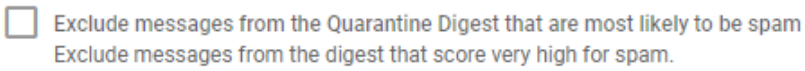
設定將郵件保留在垃圾郵件隔離區中的天數。

7. 垃圾郵件隔離摘要包含全域、群組或使用者封鎖寄件者清單隔離的電子郵件（Include messages that have been quarantined by）



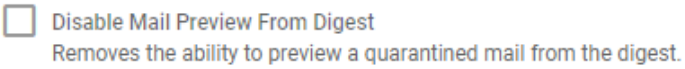
選擇垃圾郵件隔離摘要是否包含被全域、群組或使用者封鎖寄件者清單隔離的電子郵件。

8. 在垃圾郵件隔離摘要中排除最有可能的垃圾郵件（Exclude messages from the Quarantine Digest that are most likely to be spam）



啟用此選項，任何垃圾郵件分數得分最高的電子郵件將不包含在垃圾郵件隔離摘要中。但這些垃圾郵件仍可在垃圾郵件隔離網站中檢視。

9. 關閉垃圾郵件隔離摘要郵件預覽（Disable Mail Preview From Digest）



關閉垃圾郵件隔離摘要中預覽隔離郵件的功能。

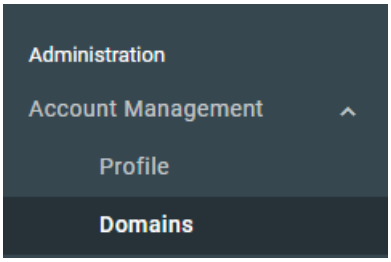
10. 將垃圾郵件隔離摘要設定更新到所有現有的使用者帳戶（Update Quarantine Digest settings for all existing user accounts）

啟用此選項，全域的垃圾郵件隔離摘要設定將取代使用者的垃圾郵件隔離摘要設定。

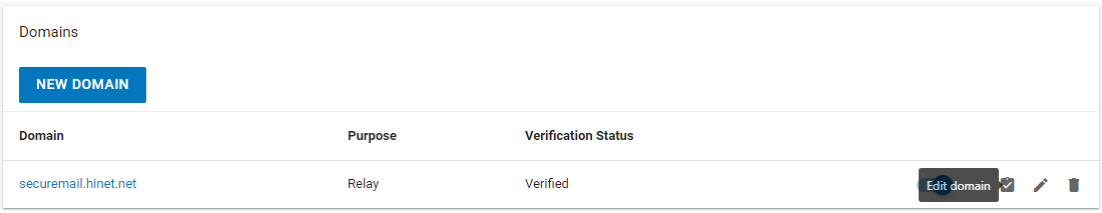
注意：*有關於垃圾郵件隔離摘要設定詳細資訊，請參閱《**郵件守門員服務管理者指南**》的垃圾郵件隔離摘要設定說明。*

內送電子郵件傳送目的地設定

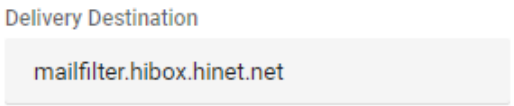
1. 點選「Account Management > Domains 選項」。



2. 在 Domains 頁面的 Domains 區域尋找要設定或確認內送電子郵件傳送目的地的網域，點選 Domain 欄位的「網域名稱」或右邊的「✎ 圖示」。



3. 在 Edit Domain 頁面的「Delivery Destination 欄位」設定或確認內送電子郵件傳送目的地郵件伺服器的主機名稱或 IP 位址。



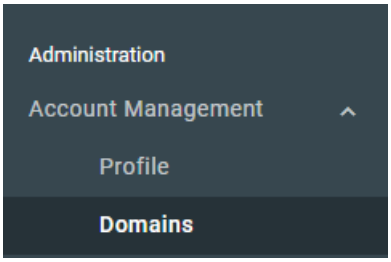
4. 在 Edit Domain 頁面的「SMTP Failover 1、SMTP Failover 2、SMTP Failover 3 與 SMTP Failover 4 欄位」設定備援郵件伺服器的的主機名稱或 IP 位址（選項）。

5. 點選「SAVE 按鈕」儲存。

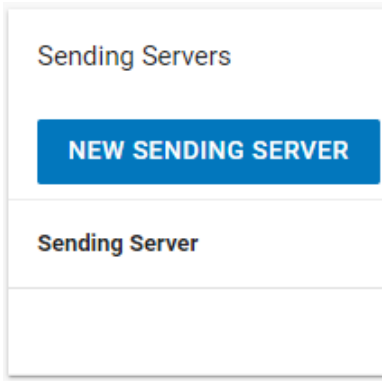
注意：*有關於內送電子郵件傳送目的地設定詳細資訊，請參閱《**郵件守門員服務管理者指南**》的設定內送電子郵件傳送目的地說明*。

外寄郵件轉寄設定（選項）

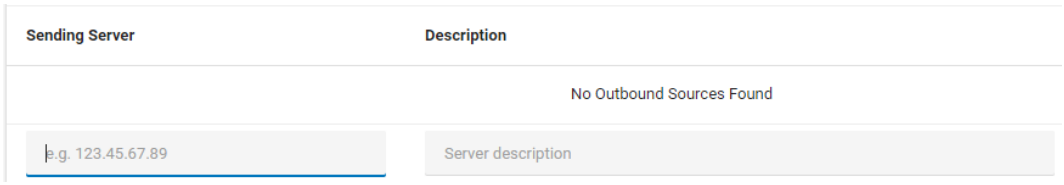
1. 點選「Account Management > Domains 選項」。



2. 在 Domains 頁面的 Sending Servers 區域點選「NEW SENDING SERVER 按鈕」。



3. 在 Domains 頁面的 Sending Servers 區域的「Sending Server 欄位」輸入外寄郵件伺服器 IP 位址，在「Description 欄位」輸入說明（選項）。



4. 點選「SAVE 按鈕」儲存。

5. 如有要新增多筆外寄郵件伺服器 IP 位址，請重複執行步驟 2 至 4。

   外寄郵件伺服器除了可用標準 IP 位址新增外，也**支援 CIDR 表示法（A.B.C.D / n）**。 只需在「Sending Server 欄位」中輸入 CIDR 值。

6. 設定 DNS SPF 紀錄，紀錄內容為**"v=spf1 a:ppe-spf.securemail.hinet.net ~all"**。

7. 待 1 小時設定生效後，於郵件伺服器設定將外寄郵件轉寄至 **ppe-out.securemail.hinet.net** 主機。

注意：*有關於內送電子郵件傳送目的地設定詳細資訊，請參閱《**郵件守門員服務管理者指南**》的設定內送電子郵件傳送目的地說明*。