Synology®

Synology MailPlus Server 管理手冊

根據 MailPlus Server 2.0

目錄

第 10 章：監控設定

第 11 章：災難備援

簡介

Synology MailPlus 套件組合提供進階、高安全性以及高可用性的郵件服務，該組合當中包含兩個套件：**MailPlus Server** 和 **MailPlus**。MailPlus Server 提供許多管理細節與設定，而 MailPlus 則是提供用戶端管理電子郵件的服務。

本管理手冊不僅能引導您完成 MailPlus Server 的架設與細部設定，更提供了 DNS 相關設定、舊有郵件服務移轉，以及其他安全性的調校。更多功能包含 MailPlus High-availability (HA) 幫助您提供服務不中斷的郵件服務，佇列提供延遲寄送的郵件管理，以及狀態監控幫助您全面掌控 MailPlus 的健康狀況。

開始使用 MailPlus Server

Synology MailPlus Server 套件讓您的 Synology NAS 可成為支援 SMTP、POP3、IMAP 的郵件系統。您可以在 Synology NAS 上集中管理使用者帳號及郵件訊息。此外，MailPlus 套件亦能為 DSM 使用者提供容易使用、網路介面的郵件用戶端，方便您檢視、管理及傳送訊息。

本章節將協助您完成特定準備工作，並引導您順利執行 Synology NAS 上的 MailPlus Server 及 MailPlus。

將 Synology NAS 連線至網際網路

Synology NAS 可透過三種方式連線至網際網路：直接連線、PPPoE 連線與路由器連線。如需了解透過網際網路存取 Synology NAS 的詳細資訊，請參考此處。

對郵件系統而言，擁有固定的外部 IP 位址是非常重要的。雖然使用動態 IP 亦可架設郵件系統，但固定 IP 可使伺服器更加穩定可靠。因此，建議您為郵件系統註冊固定的外部 IP 位址。如需更多資訊，請聯絡您的網際網路服務供應商 (ISP)。

設定固定 IP/PPPoE

在 Synology NAS 中，共有兩種方法可以設定固定外部 IP 位址：

- **PPPoE**：部份服務供應商 (ISP) 會提供免費的固定 IP，但用戶需要透過 PPPOE 連線以取得該固定 IP 的使用權。
  1. 登入 DSM。
  2. 前往控制台 > 網路。
  3. 在網路介面中選擇 PPPoE 然後按一下編輯按鈕。
  4. 設定您要連接到數據機的網路埠。
  5. 輸入 ISP 提供的使用者帳號與密碼。
- **固定 IP**：如果您已經擁有一組固定 IP，您可以直接將該組 IP 位址輸入至 Synology NAS。
  1. 登入 DSM。
  2. 前往控制台 > 網路。
  3. 在網路介面中選擇您想編輯的網路埠並按一下編輯按鈕。
  4. 輸入您的固定 IP 位址。

設定 DNS

為使用戶端能透過網際網路將郵件成功寄送到您的 MailPlus Server，您需要一個有效的網域名稱。此外，您必須在 DNS 伺服器上設定 MX 記錄與 A 記錄。

MX 記錄，或稱郵件交換記錄 (Mail Exchange record)，是一種位於網域名稱系統 (DNS) 上的記錄資源。它可標示出電子郵件應如何透過 SMTP 被引導至正確的目的地。每一筆 MX 記錄都包含一個主機名稱與一個優先順序的設定。主機名稱指出郵件應抵達的正確目的地。優先順序的設定則指出各伺服器間的優先順序。

例如：若要讓電子郵件地址 alex@example.com 成功收發郵件，您必須設定網域 example.com 的 MX 記錄。其方式為：將 MX 記錄指到您 Synology NAS 的 IP 位址或網域名稱。若您已註冊了網域名稱，您可以在管理主控台中修改該網域名稱的這些設定。

- **A 紀錄**：example.com > 111.222.112.223
- **MX 紀錄**：example.com > nas.example.com (優先順序為 0)

例如：若要讓 *alex@example.com* 可以正常收發信，您需要設定好 *example.com* 的相關 MX 紀錄，將該網域的 MX 紀錄指向到您的 Synology MailPlus Server。若該網域 *example.com* 僅用於 Synology MailPlus Server，則設定 MX 紀錄時，主機與指向可設定為相同。優先順序的設定則是當數字越低，優先順序越高。

設定反向 DNS

將 DNS 記錄指到網域名稱的步驟稱為**正向 DNS**。此舉可將網域名稱指到正確的伺服器位址。不過，除了正向 DNS 之外，還需要做反向的設定，稱為**反向 DNS**。

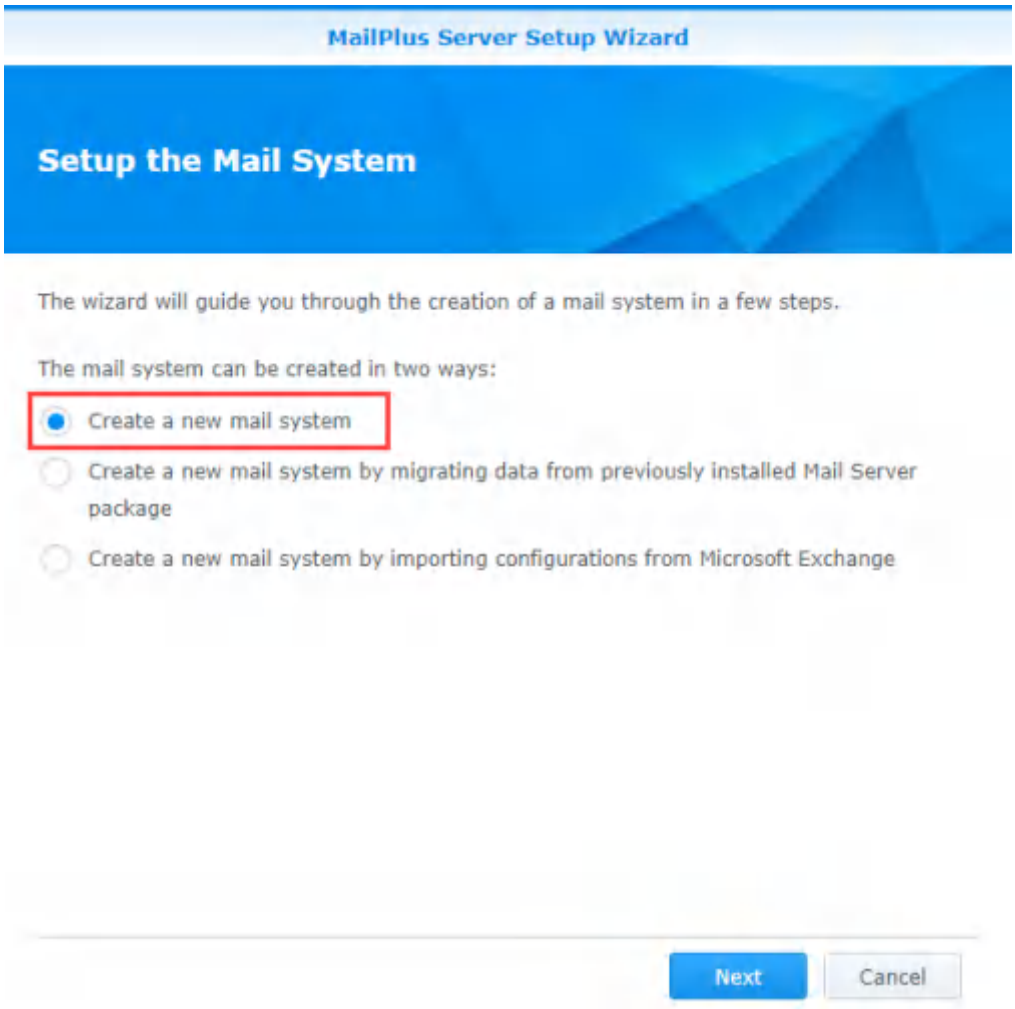
- **什麼是反向 DNS ？**反向 DNS 與正向 DNS 相反，正向 DNS 是將網域 / 主機名稱轉譯為 IP 位址的過程，而反向 DNS 則是將網站的數字位址 (亦即 IP 位址) 轉譯為網域 / 主機名稱的過程。反向 DNS 同時也可由 IP 位址定位出其對應的網域 / 主機名稱，因此也常被稱作**反向 DNS 查詢**。若網域名稱的反向 DNS 設定正確，即可使用 IP 位址直接連線。
- **反向 DNS 的作用是什麼？**郵件伺服器為什麼需要設定反向 DNS ？反向 DNS 是架設郵件系統的必要基礎設定之一，通常用於過濾垃圾郵件，可判斷郵件的來源 IP 位址是否為通過驗證的網域名稱；若其 IP 位址並非來自可靠的網域，便封鎖此封郵件。若您沒有為郵件伺服器設定反向 DNS，從您的郵件伺服器發送的信件將會被大部分電子郵件服務封鎖而無法投遞。若您無法自行設定反向 DNS，郵件投遞又持續發生問題，請新增另一個 SMTP 伺服器以正常投遞郵件。建議您使用更為知名的 SMTP 伺服器，以避免在寄送郵件時被視為垃圾郵件封鎖。
- **如何設定反向 DNS ？**請在自己的主機上設定反向 DNS，某些網路服務供應商可能會提供部分區塊，供您自行設定反向 DNS。您可修改 DNS 伺服器上的 PTR 記錄來設定反向 DNS，PTR 記錄是由發給您 IP 位址的單位負責管理。若您的主機可授權您修改反向 DNS，那麼負責管理 PTR 記錄的單位可能是您的主機，或是您自己。PTR 記錄通常代表反向輸入的 IP，結尾為 in-addr.arpa。請透過您的網路服務供應商設定反向 DNS，因為只有網路服務供應商或擁有您 IP 位址的單位可以增加正確的 PTR 紀錄，您可能需要與他們聯絡，以進行反向 DNS 設定。

設定 MailPlus Server

完成安裝後，即可開始設定 MailPlus Server。在以下段落中，我們將介紹如何啟動 SMTP (簡易郵件傳輸協定)。請注意，以下的螢幕截圖僅供參考，您的實際設定可能會有所不同。

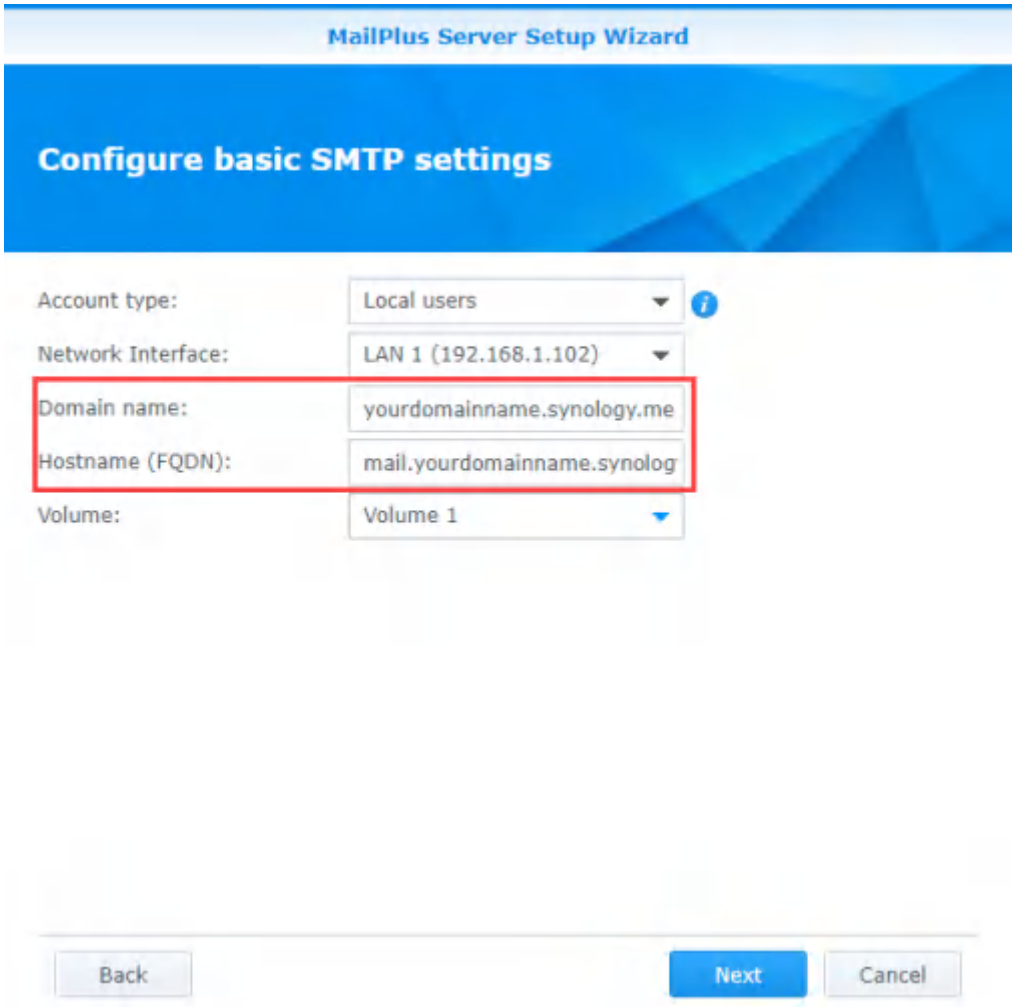
1 前往**套件中心**來尋找並安裝 **MailPlus Server**。

2 開啟 **MailPlus Server**，選擇**建立新的郵件系統**來建立一個全新的郵件系統，再按一下**下一步**以繼續設定。或者，您也可以選擇**從先前安裝的 Mail Server 套件轉移資料並建立新的郵件系統**。參閱**此處**來了解如何將 Mail Server 轉移至 MailPlus Server。

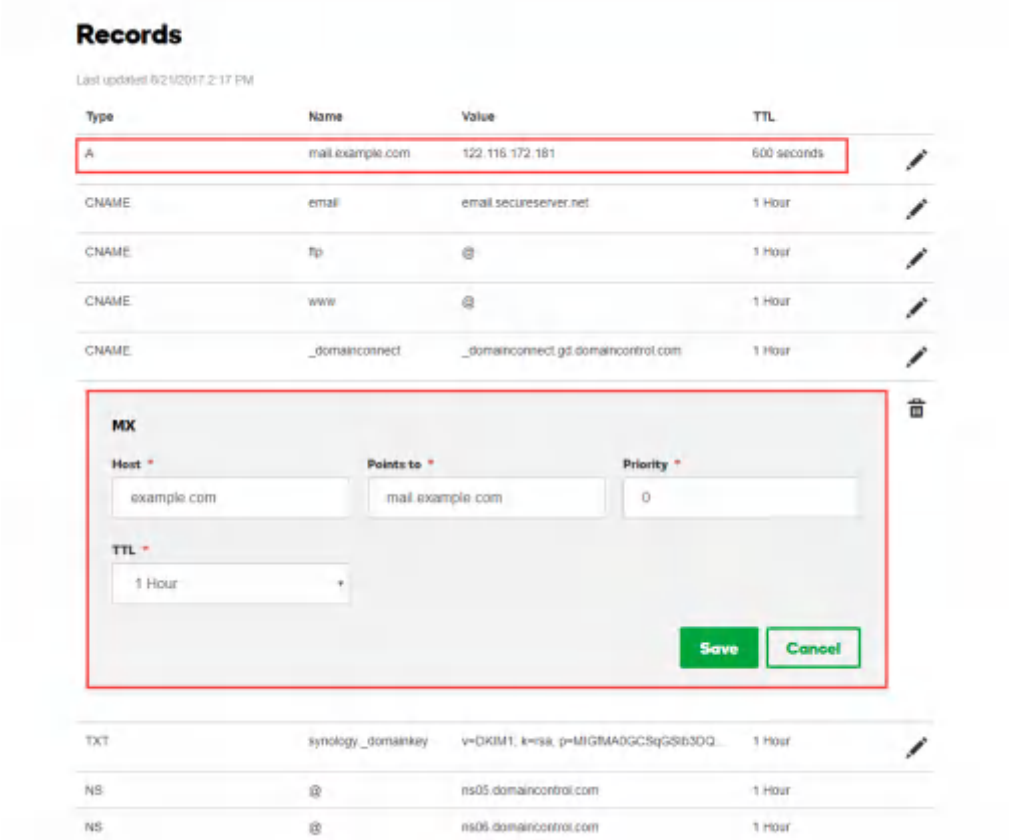


3 輸入網域名稱以及主機名稱 (FQDN)。

- **網域名稱**：網域名稱是您收發信使用的電子郵件地址，請確認您的網域名稱與 DNS 設定中的 MX 紀錄符合。
- **主機名稱 (FQDN)**：主機名稱是您的 MailPlus Server 位址。請確認您的主機名稱與 DNS 設定中的 A 紀錄符合。



- 例如：如果您的網域名稱是 *example.com*，您的 MailPlus Server 網址就是 *mail.example.com*，接著您可以參考以下說明完成相關設定。
  1. 設定 A 紀錄時，將「mail.example.com」指向 MailPlus Server 所使用的固定 IP 位址。
  2. 設定 MX 紀錄時，在主機欄位中輸入「example.com」、在指向欄位中輸入「mail.example.com」、在優先順序欄位中輸入「0」。
  3. 在 MailPlus Server 當中，將「example.com」設定為網域名稱，而「mail.example.com」設定為主機名稱 (FQDN)。

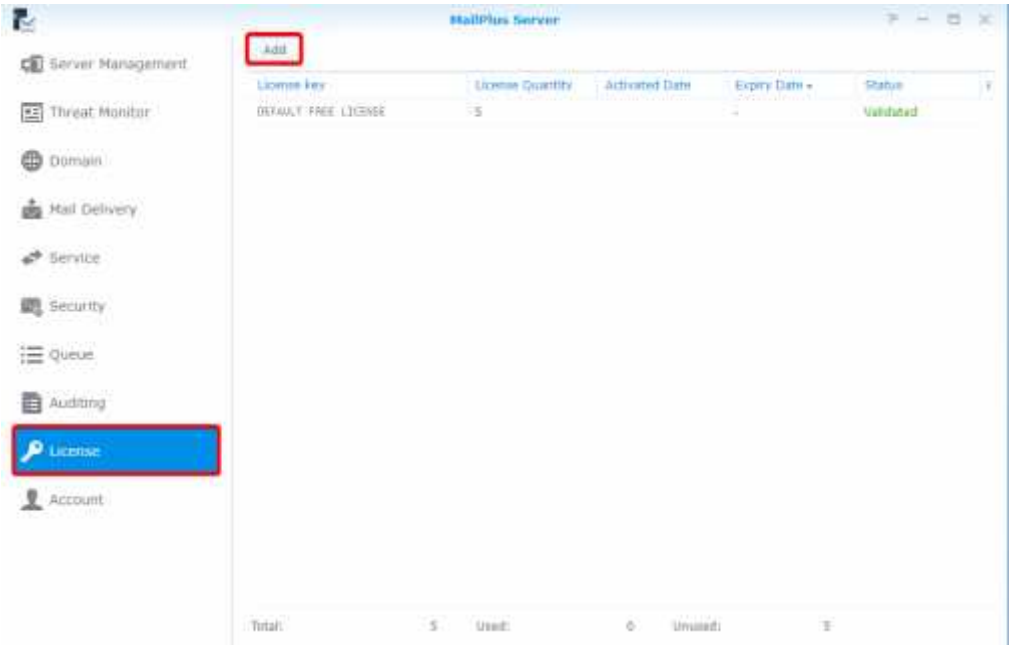


4 您可以依需求修改下列的額外設定：

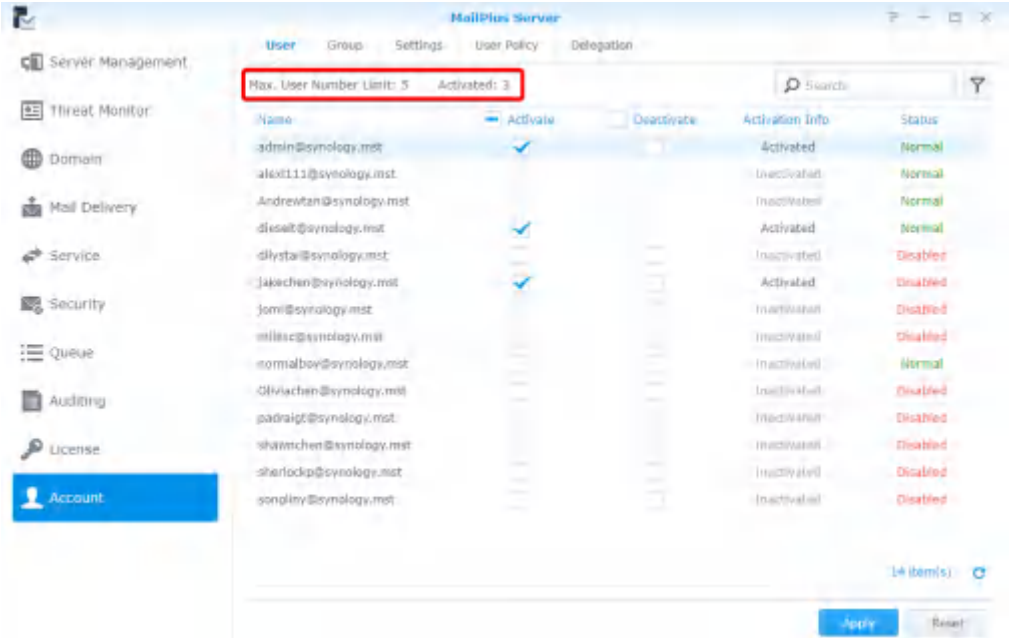
- **帳號類型**：選擇哪些類型的使用者帳號 (本地、LDAP 或網域使用者) 可以使用 MailPlus Server 提供的服務。
- **網路介面**：選擇 MailPlus Server 使用的網路埠。
- **儲存空間**：選擇 MailPlus Server 及其資料使用的儲存空間。

5 按一下**下一步**來檢查設定，然後按一下**套用**來完成設定。

6 MailPlus Server 安裝時預設提供 5 個免費的郵件帳號；若需啟動更多郵件帳號，您可以在**授權**頁面新增更多授權。如想了解更多 MailPlus 授權機制的資訊，請參考**此處**。



7 前往帳號頁面啟動電子郵件帳號，您可以依使用者或群組來啟動帳號，也能在左上角檢視可啟動的使用者數量上限。請參考啟動帳號來了解更多資訊。



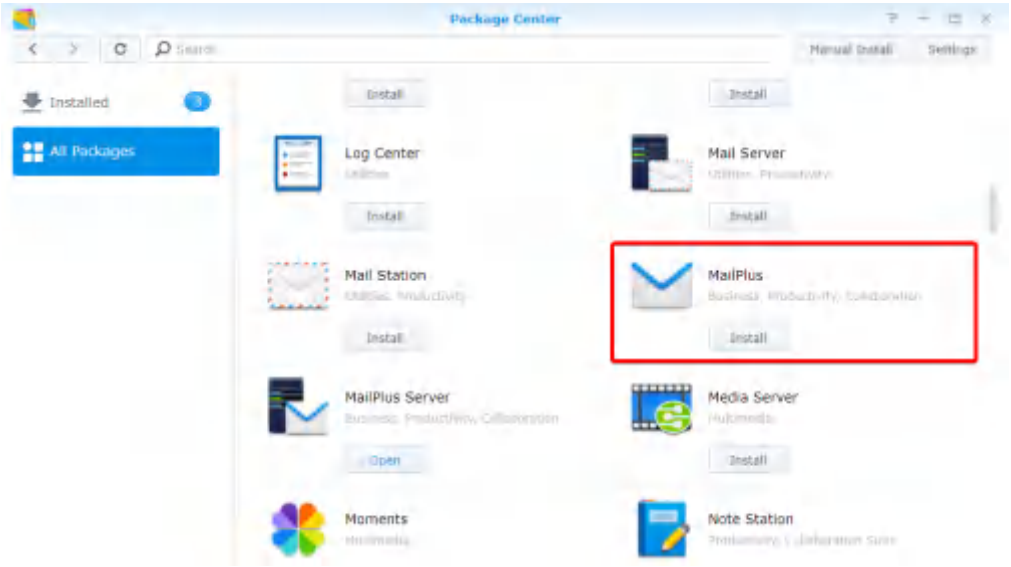
設定 MailPlus 電子郵件用戶端

使用 MailPlus 存取 Synology NAS 上的電子郵件

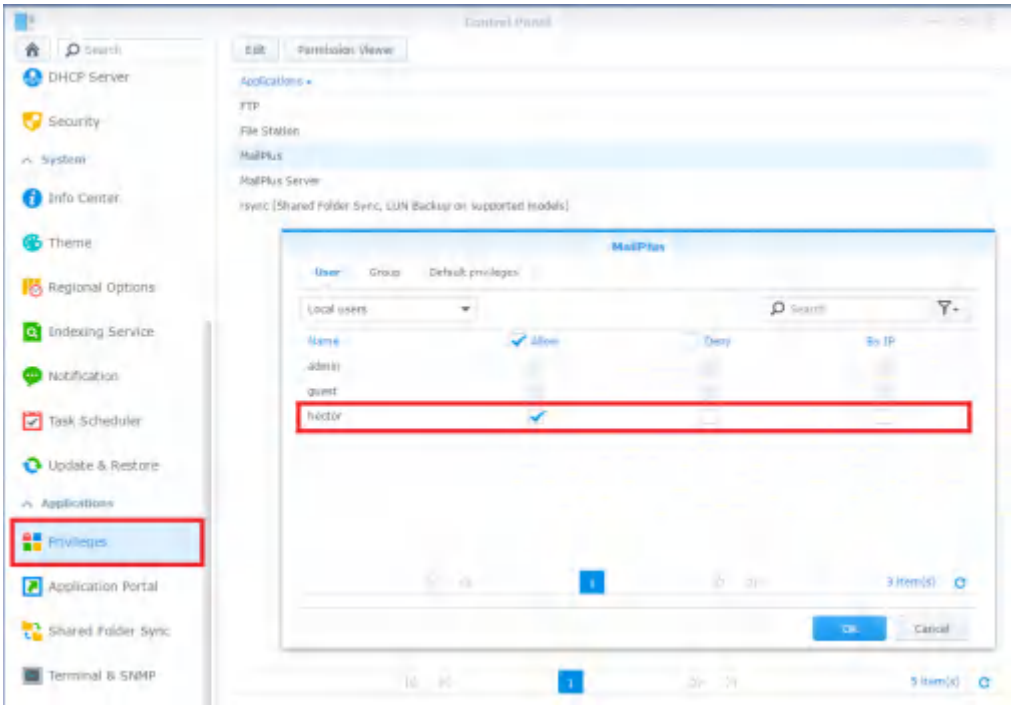
MailPlus 是一款附加套件，讓您可以透過網頁介面存取與管理 Synology NAS 上的電子郵件。此外，您可在 MailPlus 中建立多個 POP3 帳號，藉此接收、儲存其它電子郵件服務的信件 (例如：Gmail、O□ce 365)。

安裝 MailPlus

1 前往套件中心來安裝 MailPlus。



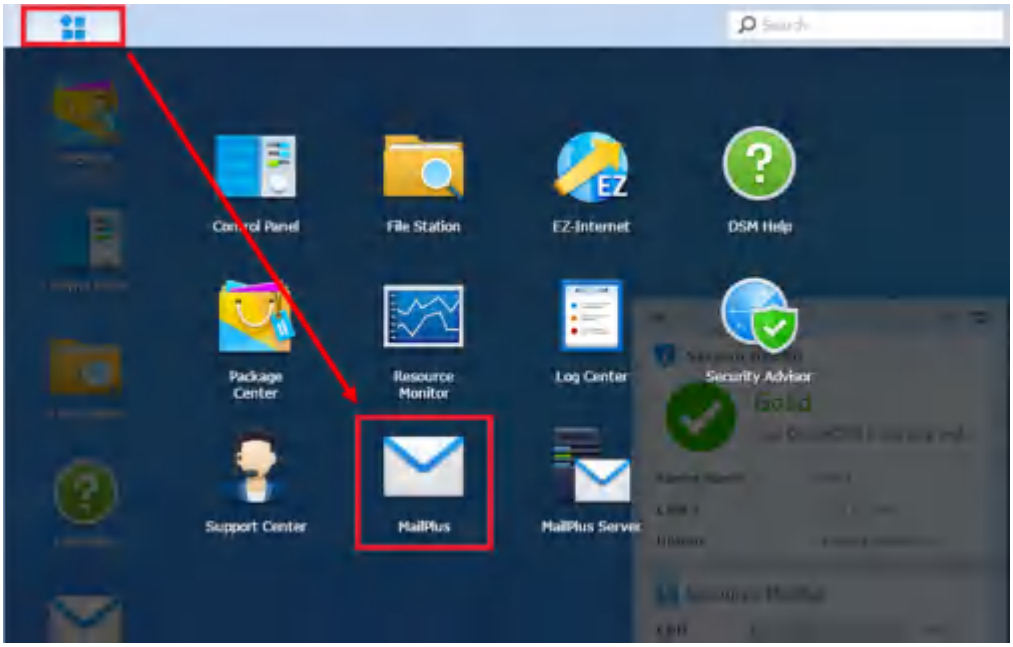
2 前往控制台 > 權限，來設定可以存取 MailPlus 的帳號。



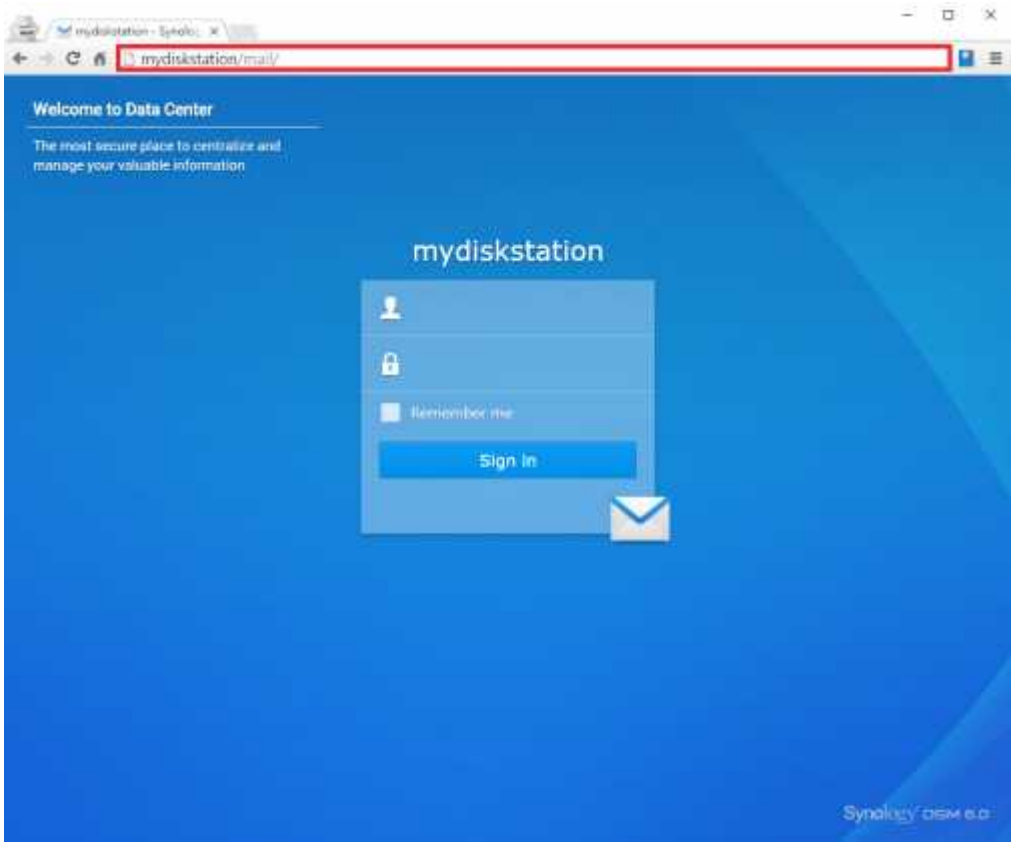
執行 MailPlus

1 您可透過兩種方式前往 MailPlus 登入頁面：

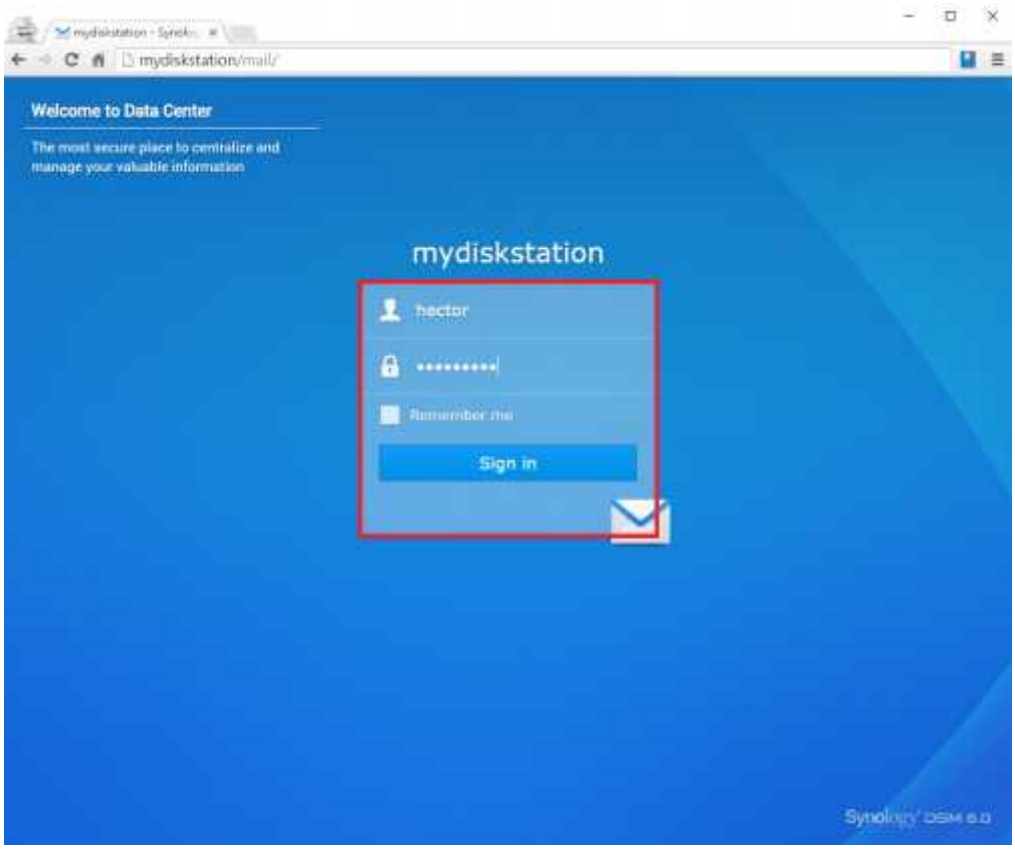
- 前往**主選單** > **MailPlus**。



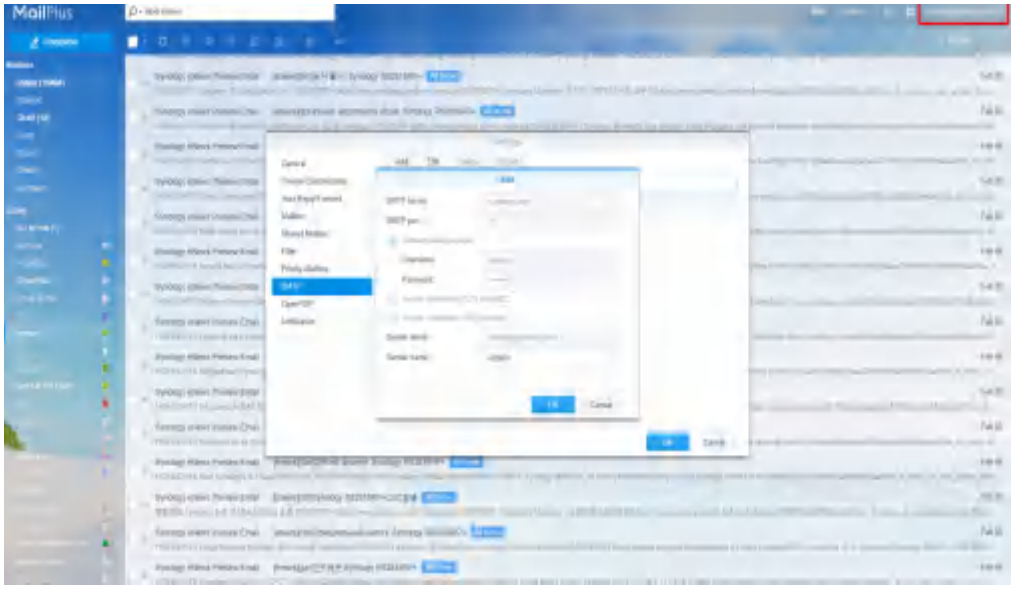
- 直接透過應用程式入口來存取 MailPlus。在網頁瀏覽器的網址列中輸入 Synology NAS 的名稱，後接「/mail」。例如：若您的 Synology NAS 名稱為 *mydiskstation*，則輸入 *mydiskstation/mail*。請參閱**此處**來了解如何啟動**應用程式入口**。



2 輸入您的 DSM 使用者帳號及密碼來登入。



3 若在安裝 MailPlus 之前已完成 MailPlus Server 的設定，**設定** > **SMTP** 中將自動帶入 MailPlus Server 的 SMTP 設定。

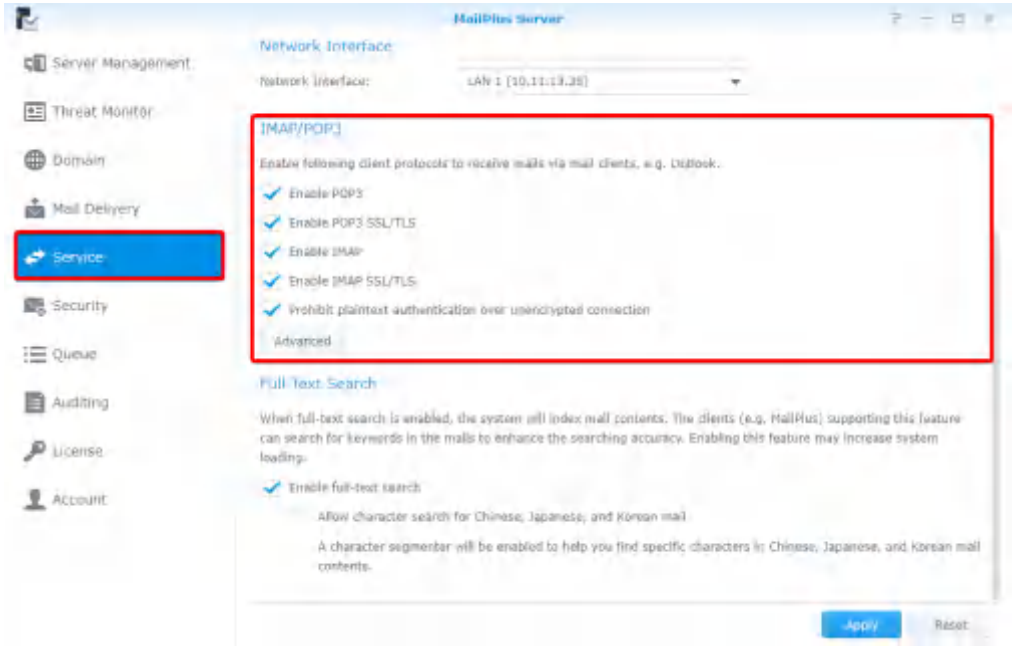


第三方電子郵件用戶端

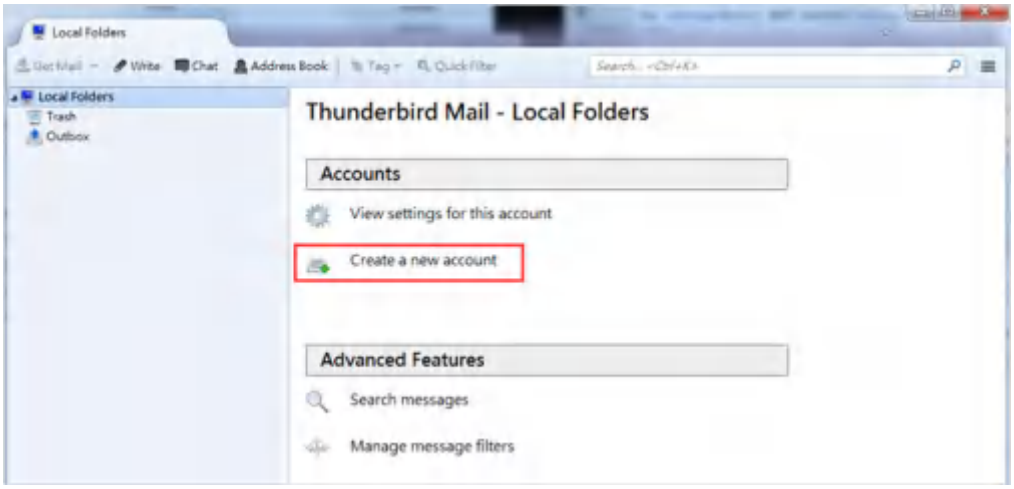
透過其它電子郵件用戶端存取 Synology NAS 上的電子郵件

Synology NAS 上的電子郵件帳戶可與各種不同的郵件用戶端連結，例如 Microsoft® Outlook® 或 Mozilla® Thunderbird™。在下面的例子中，我們將介紹如何使用 Thunderbird 來存取 Synology NAS 上的電子郵件帳號。

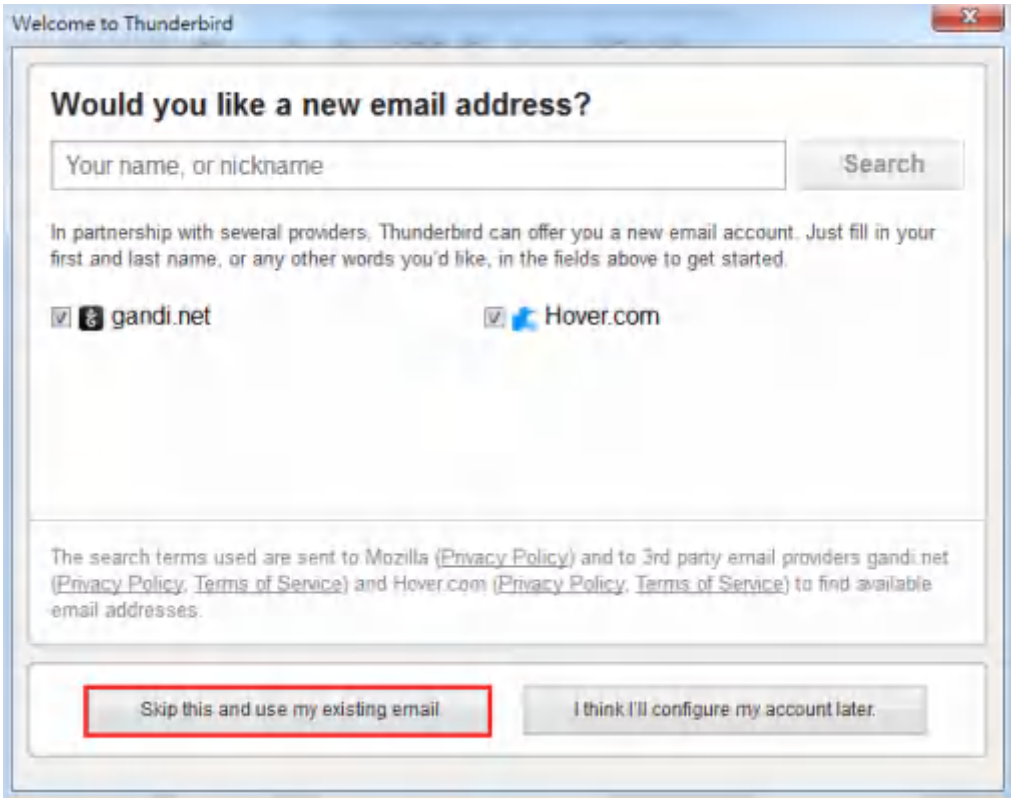
1 開啟 **MailPlus Server** 並前往**服務**頁面來啟動 IMAP 或 POP3 (視用戶端而定)。



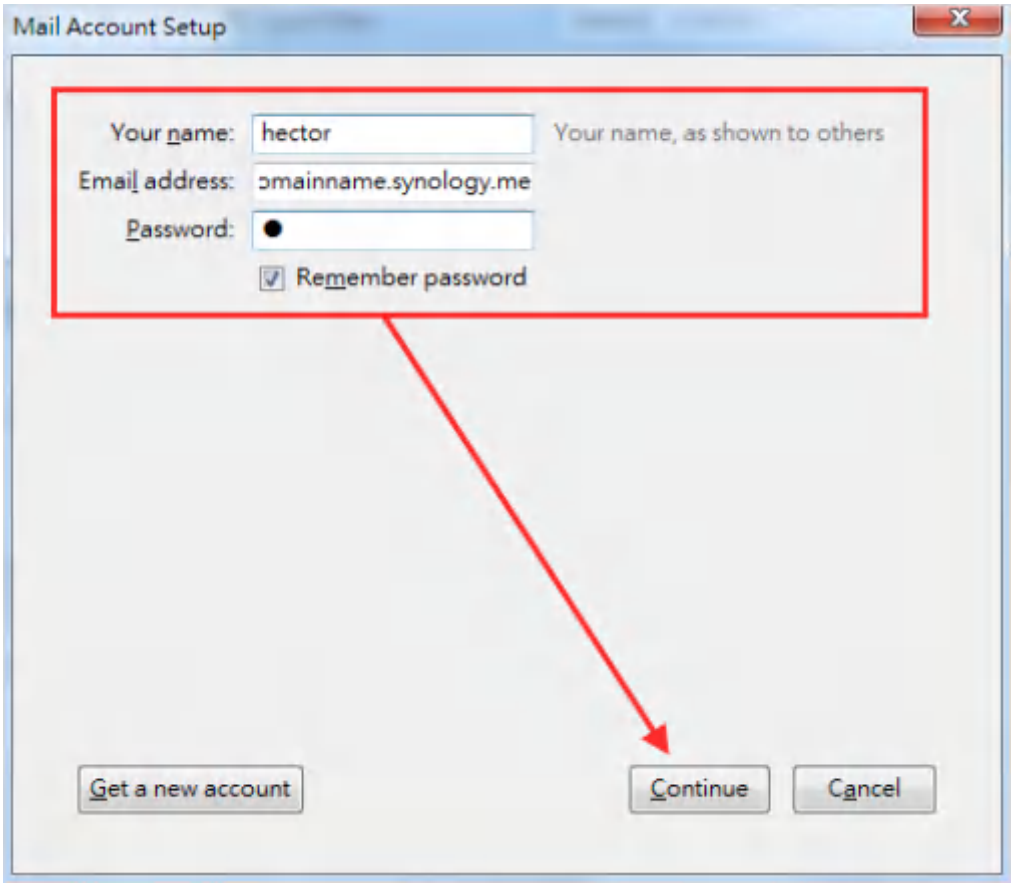
2 在電腦上開啟 Thunderbird，按一下**新增帳號**。



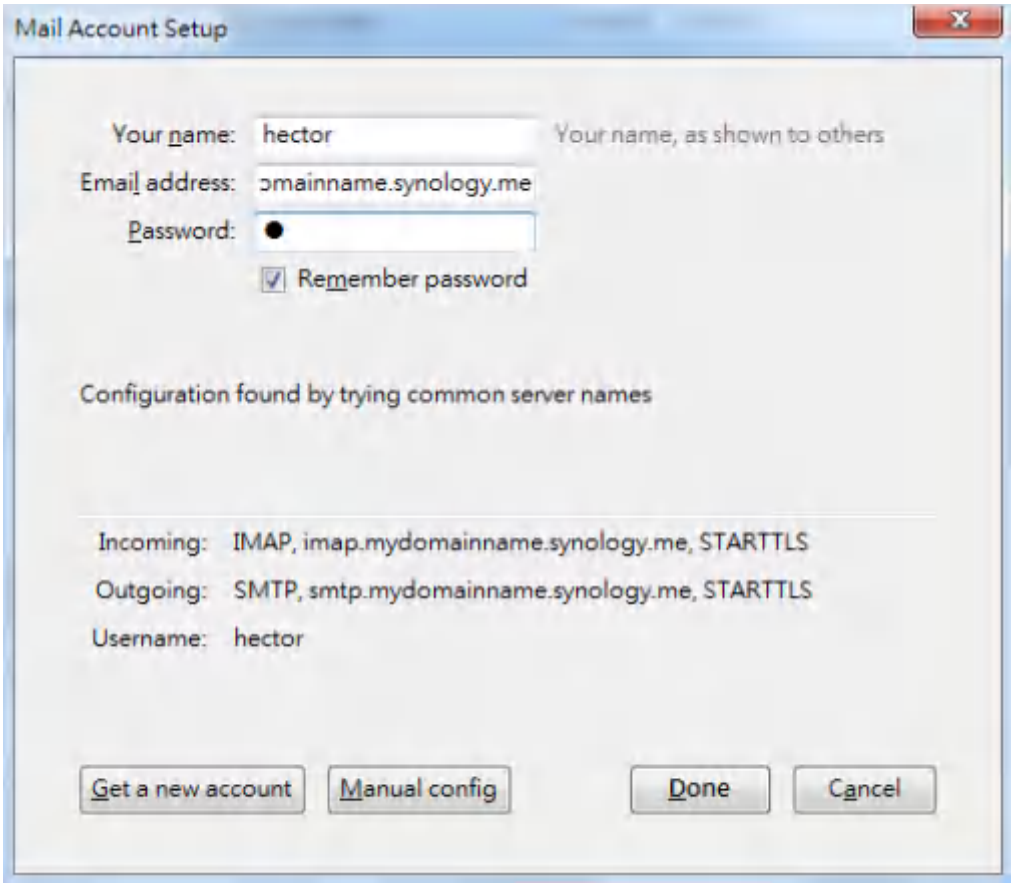
3 按一下**使用我現有的帳號**。



4 輸入您的 DSM 使用者帳號名稱、電子郵件地址及密碼。(例如：*hector@mydomainname.synology.me*) 按一下**繼續**。



5 Thunderbird 會搜尋您的信箱地址。若您的設定正確，您會看到以下畫面。



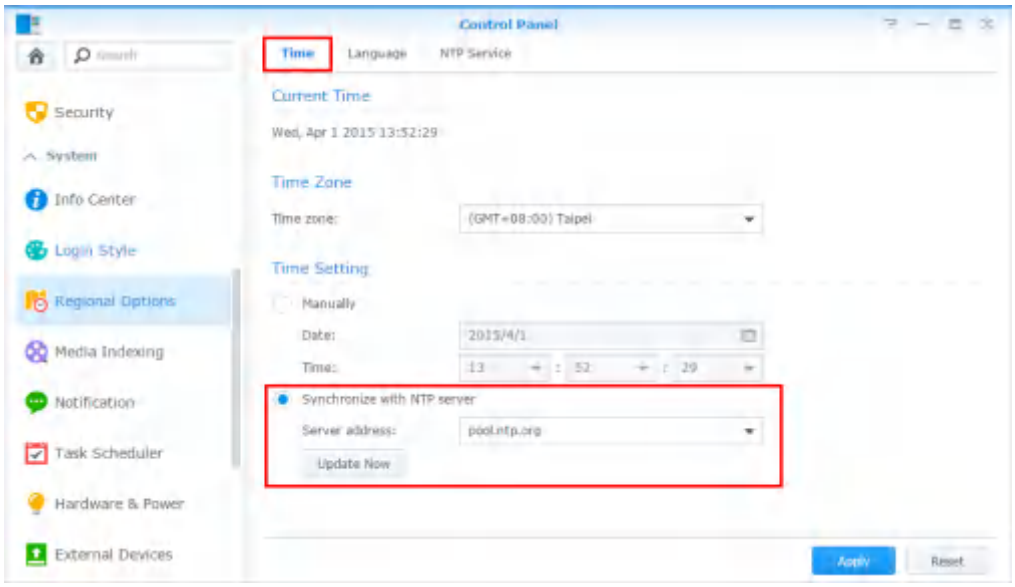
6 現在，Thunderbird 中將會顯示所選帳號的電子郵件！

疑難排除

為什麼我無法用 MailPlus 的網頁介面收發電子郵件？

1 請檢查您 MailPlus 的 SMTP、DNS、與 MX 記錄等設定是否正確。

2 請檢查 Synology NAS 的網際網路設定是否正確。前往**控制台** > **區域選項**。在**時間**頁籤下，勾選**與 NTP 伺服器同步**，然後按一下**立即更新**按鈕，以檢查網際網路設定是否正確。若同步成功，表示設定正確。



3 請檢查路由器的連接埠設定是否正確。

4 前往此**網站**查看您的 IP 位址是否遭舉報為垃圾信件發送者。若是，請將您的 IP 自該網站的封鎖名單中移除。

為什麼我無法用我的電子郵件用戶端收發電子郵件？

1 請檢查您是否已啟動 IMAP 與 POP3 協定。

2 請檢查您的使用者帳號與密碼是否正確。

3 請檢查您 MailPlus 的 SMTP、DNS、與 MX 記錄等設定是否正確。

4 請檢查 Synology NAS 的網際網路設定是否正確。前往**控制台** > **區域選項**。在**時間**頁籤下，勾選**與 NTP 伺服器同步**，然後按一下**立即更新**按鈕，以檢查網際網路設定是否正確。若同步成功，表示設定正確。

5 請檢查路由器的連接埠設定是否正確。

6 請檢查您的 IP 位址是否遭舉報為垃圾信件發送者。前往 **http://www.spamhaus.org/sbl/** 來查看。若是，請將您的 IP 自該網站的封鎖名單中移除。

為什麼我無法收取來自其它郵件伺服器 (如 Gmail) 的電子郵件？

1 請確認 DNS 的設定正確。您需將 MX 記錄與 A 記錄皆指向 Synology NAS，如此一來，其它的郵件伺服器才能找到 Synology NAS。

2 請確認 Synology NAS 使用固定 IP 位址，並已連線至網際網路，或者確認您的網域名稱可正確指向您的動態 IP。

3 如果 Synology NAS 是透過 NAT 防火牆或路由器連線至網際網路，請確定連接埠轉送設定是否正確。您可至 **http://canyouseeme.org/** 並輸入連接埠 25，以確認連接埠轉送的設定正確。

4 請查看被退回的信件內容 (如果有的話)，即可確知錯誤發生的詳細原因。

為什麼我寄信到某些網路郵件帳號，如 Gmail 和 Hotmail，電子郵件總是被退回？

許多免費的電子郵件供應商都會設定 DNS 反向位址查詢，以確保郵件可正確寄送。若您的 DNS 反向查詢結果與寄件的網域名稱不符，您的郵件就會被退回。請與您的網路供應商 (ISP) 聯絡。也有可能您的 IP 位址已被列入垃圾郵件封鎖清單中，請前往此**網站**查看您的 IP 位址是否遭到封鎖。

郵件移轉

MailPlus Server 內建郵件移轉器，毋需複雜設定，即可協助您從非 MailPlus 的電子郵件伺服器 (例如：Microsoft Exchange 及 IMAP 郵件伺服器) 及第三方服務 (例如：Gmail 及 Yahoo Mail) 移轉電子郵件。本文將引導您從 Microsoft Exchange 轉移電子郵件到 MailPlus Server 。在開始之前，請先確認您已完成以下準備工作：

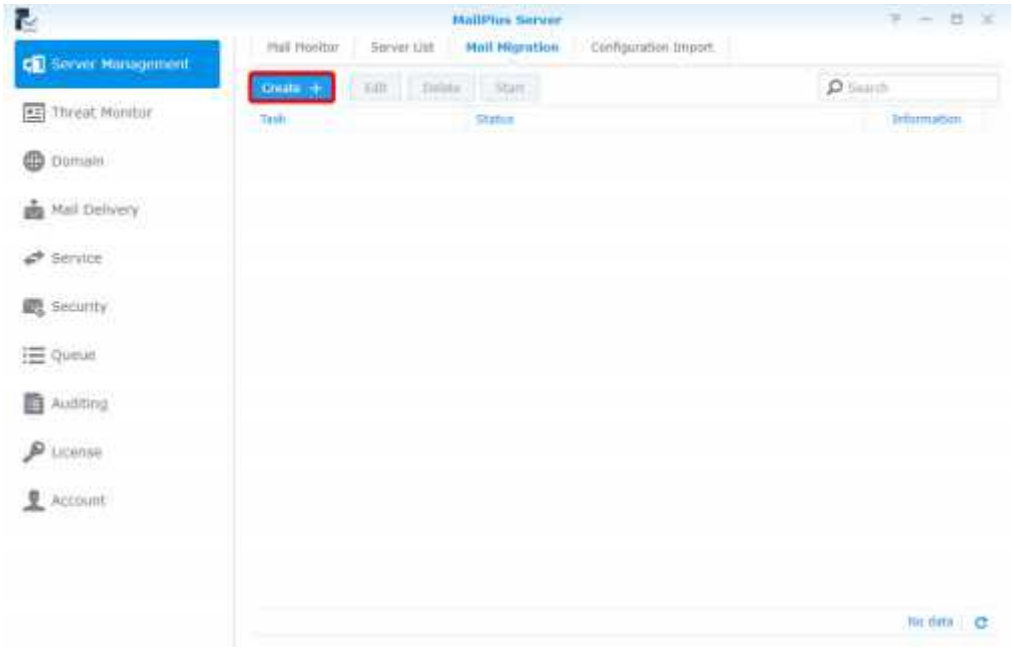
- 確認您的 Synology NAS 目前執行 DSM 6.0 或更新版本，並支援 MailPlus Server (可用機種請見此處)。
- Synology NAS 上已完成 MailPlus Server 設定，可作為目的地郵件伺服器。
- 匯整來源帳號與對應 MailPlus Server 帳號的使用者名稱及密碼。

在 MailPlus Server 新增郵件移轉任務

登入 MailPlus Server，前往**伺服器管理** > **郵件移轉** > **新增**來建立郵件移轉任務。然後，依照指示在下列頁籤完成任務設定。本章節將以 Microsoft Exchange 為例。

進行一般任務設定

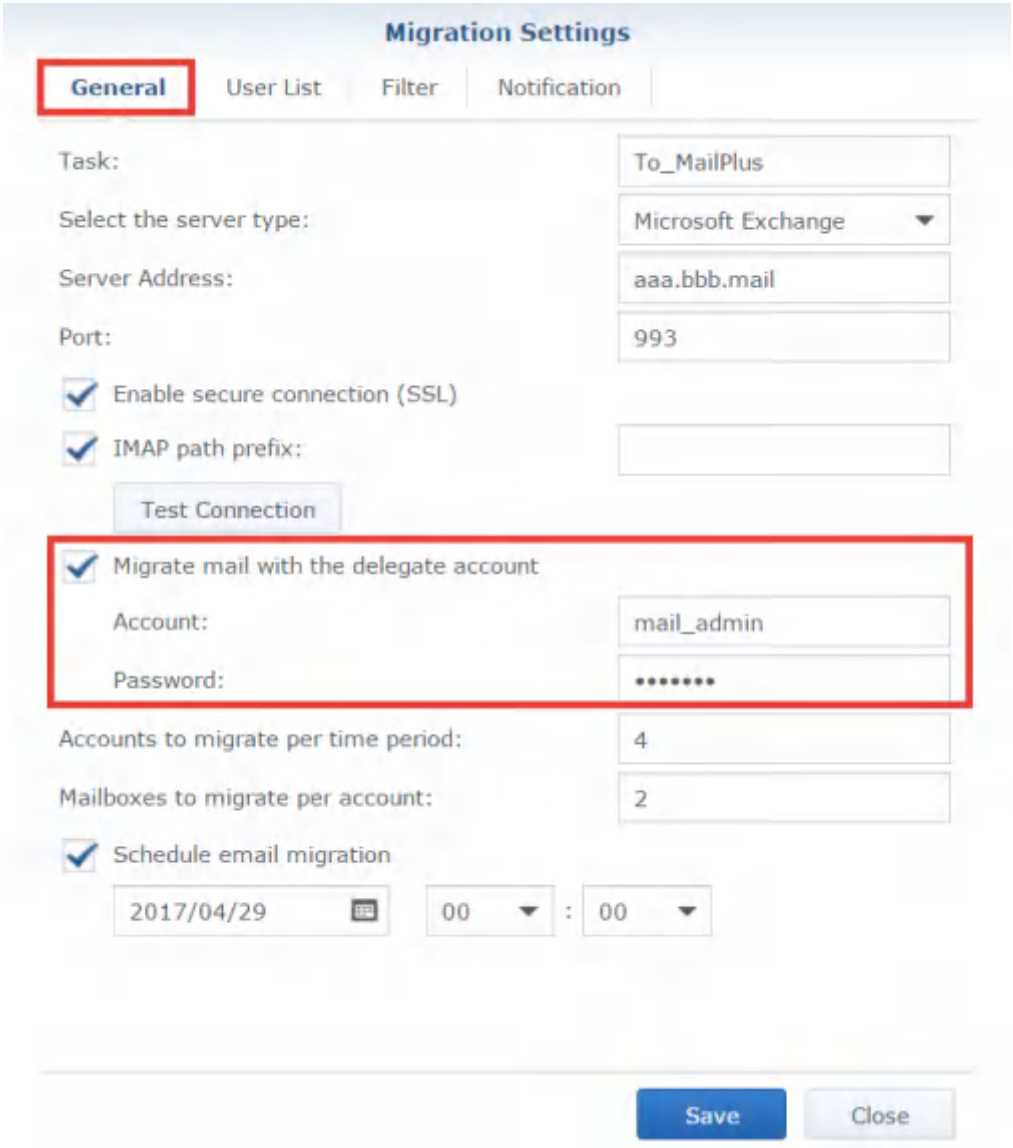
1 前往**伺服器管理** > **郵件移轉**，然後按一下 **新增**按鈕。



2 在**轉移設定**視窗的**一般**頁籤中，將**選擇伺服器類型**設定為 **Microsoft Exchange**，並填入來源 Microsoft Exchange 伺服器的必要資訊。

3 您可以在來源 Microsoft Exchange 伺服器的設定中找到 **IMAP 路徑前置碼**。

4 如果來源伺服器上已有代理帳號，且該帳號具備所有其他來源帳戶的完整存取權限，選擇**透過代理帳號移轉郵件**並填入對應的帳號密碼，即可透過該帳號來移轉郵件，不須取得各個來源帳戶的存取權限。



5 依據來源伺服器能力，設定**各時段移轉的帳號數**及**各帳號移轉的信件匣數**。例如：Microsoft Exchange Server 2013 最多可為各個帳戶移轉 16 個信件匣。

注意：若要了解如何從其他來源 (例如：Gmail 或 Yahoo Mail) 移轉電子郵件，請見此篇**說明文章**。

匯入使用者清單

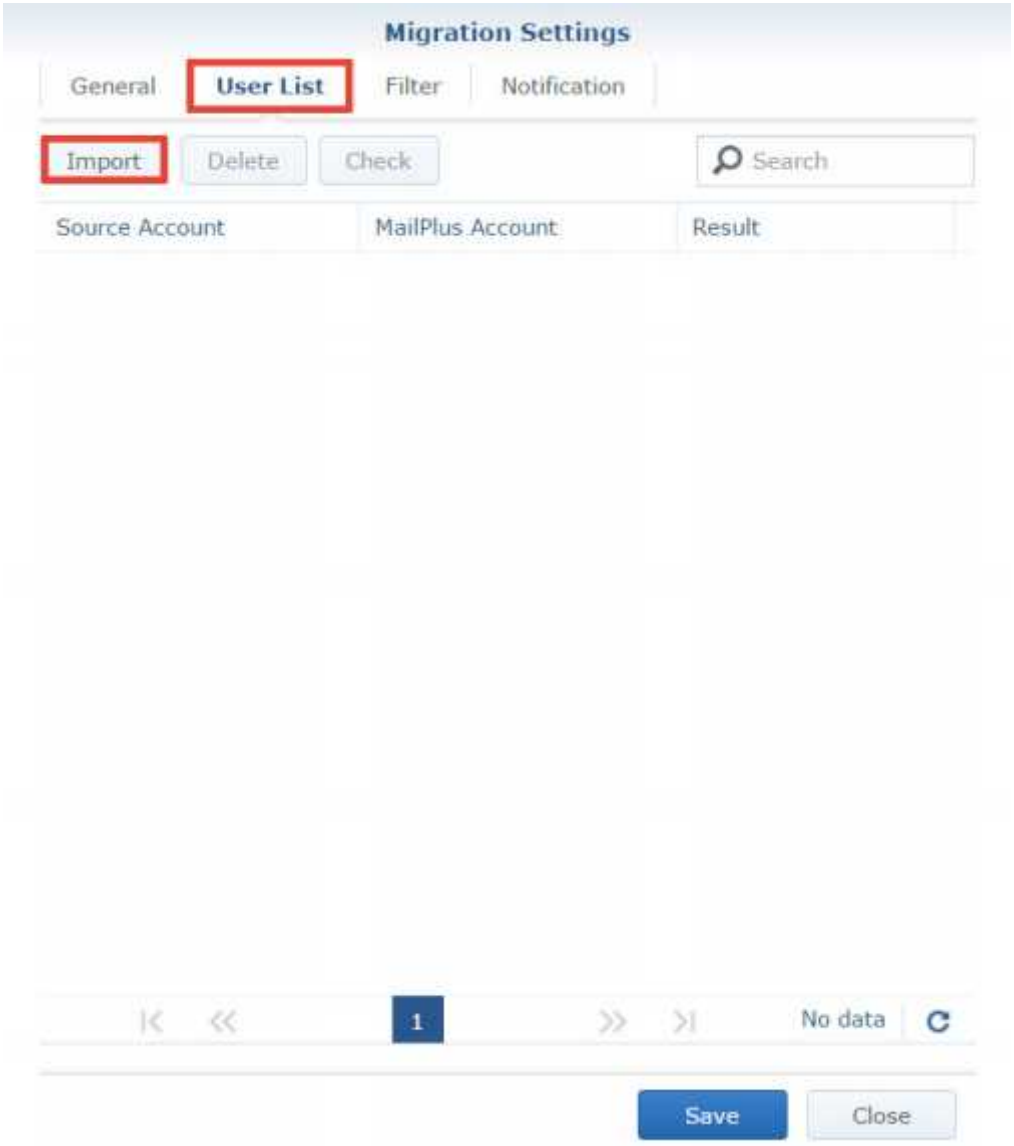
1 依據下列規範，準備一份使用者清單：

- 使用者清單應為 CSV 檔案。可透過 Microsoft Excel 或 Google 試算表產生。
- 一列只列出一個使用者帳號資訊。
- 從左至右，為各個使用者列出下列資訊：來源帳號、來源帳號的密碼、對應的 MailPlus Server 帳號。
- 使用逗號 (,) 分隔各個類型的資訊。
- 當來源伺服器類型設定為 **Microsoft Exchange** 並啟動**透過代理帳號移轉郵件**，可省略來源帳號的密碼 (例如：來源 _ 帳號 _X,,MailPlus_Server_ 帳號 _X)。

2 有效的使用者清單樣式如下：

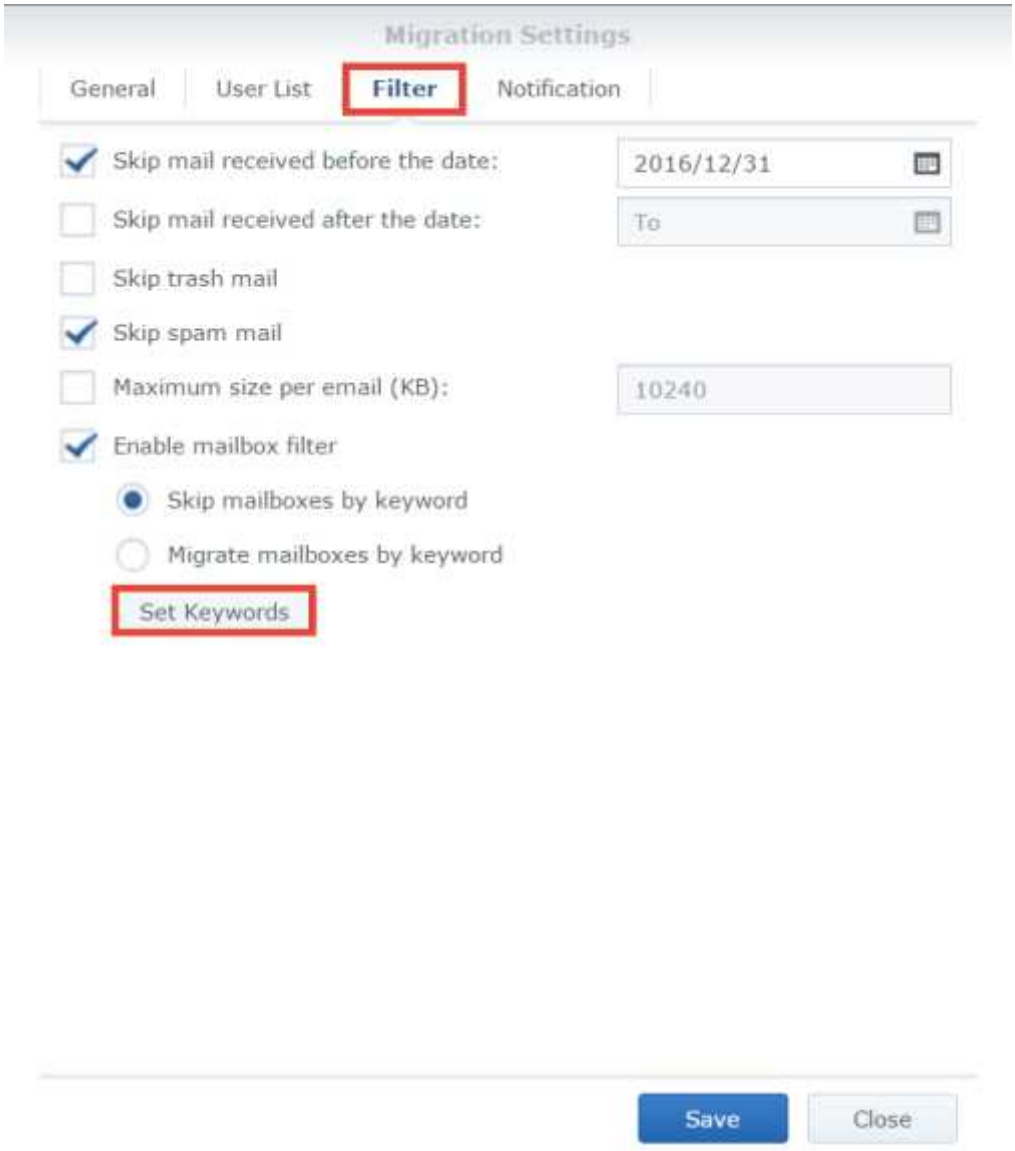
來源 _ 帳號 _1, 來源 _ 帳號 _1_ 密碼 ,MailPlus_Server_ 帳號 _1
來源 _ 帳號 _2, 來源 _ 帳號 _2_ 密碼 ,MailPlus_Server_ 帳號 _2
來源 _ 帳號 _3, 來源 _ 帳號 _3_ 密碼 ,MailPlus_Server_ 帳號 _3
...
來源 _ 帳號 _N, 來源 _ 帳號 _N_ 密碼 ,MailPlus_Server_ 帳號 _N

3 前往**使用者帳號列表**，即可匯入清單並確認所有帳戶資料是否皆正確。



設定電子郵件及信件匣篩選器

1 在**篩選**頁籤，指定條件來移轉或略過來源伺服器上的某些電子郵件或信件匣。



2 若要透過關鍵字篩選信件匣，選擇**啟動信件匣篩選器**及篩選方式 (**依據關鍵字略過信件匣**或**依據關鍵字移轉信件匣**)。

3 按一下**設定關鍵字**，在兩個區域中輸入文字：

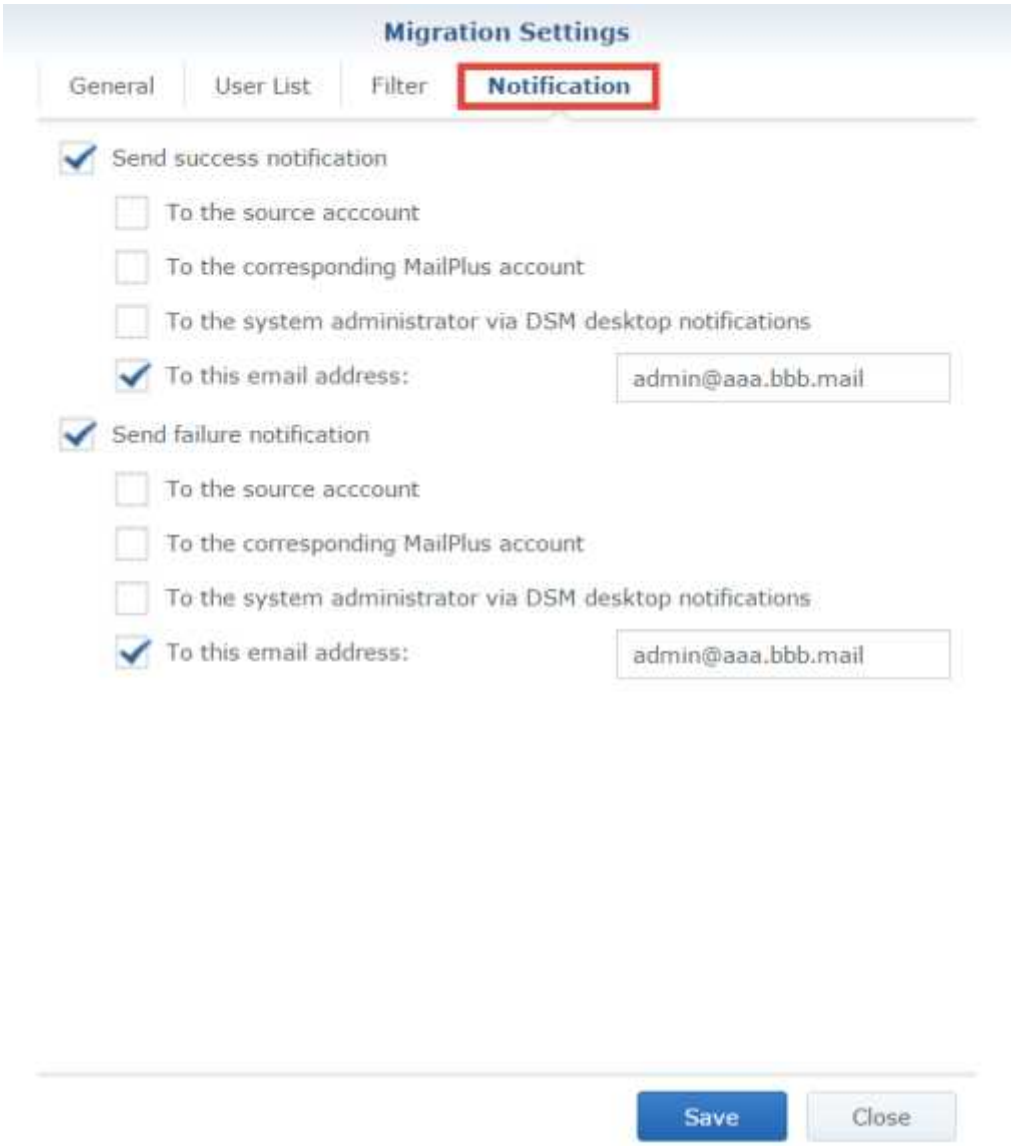
- **關鍵字：**輸入文字來依據篩選方式處理符合的信件匣。
- **例外情況：**輸入文字後，將不會依據篩選方式來處理符合的信件匣。

4 您可以在此二個區域中輸入正規表示式，兩旁皆須加上斜線 (例如：/ 正規 _ 表示式 /)。

設定移轉通知

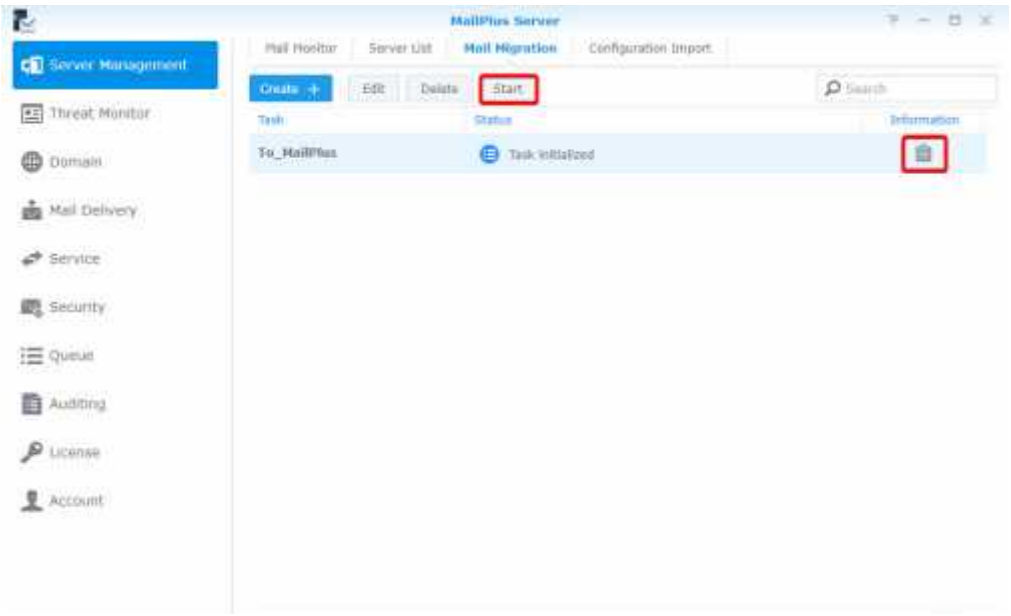
1 確認 MailPlus Server 上已選擇**啟動 SMTP** (位於**通訊協定** > **SMTP**)，便能傳送通知訊息。

2 在**通知設定**頁籤中決定 MailPlus Server 是否應寄送各帳戶的移轉結果以及管理者可在何處接收訊息。

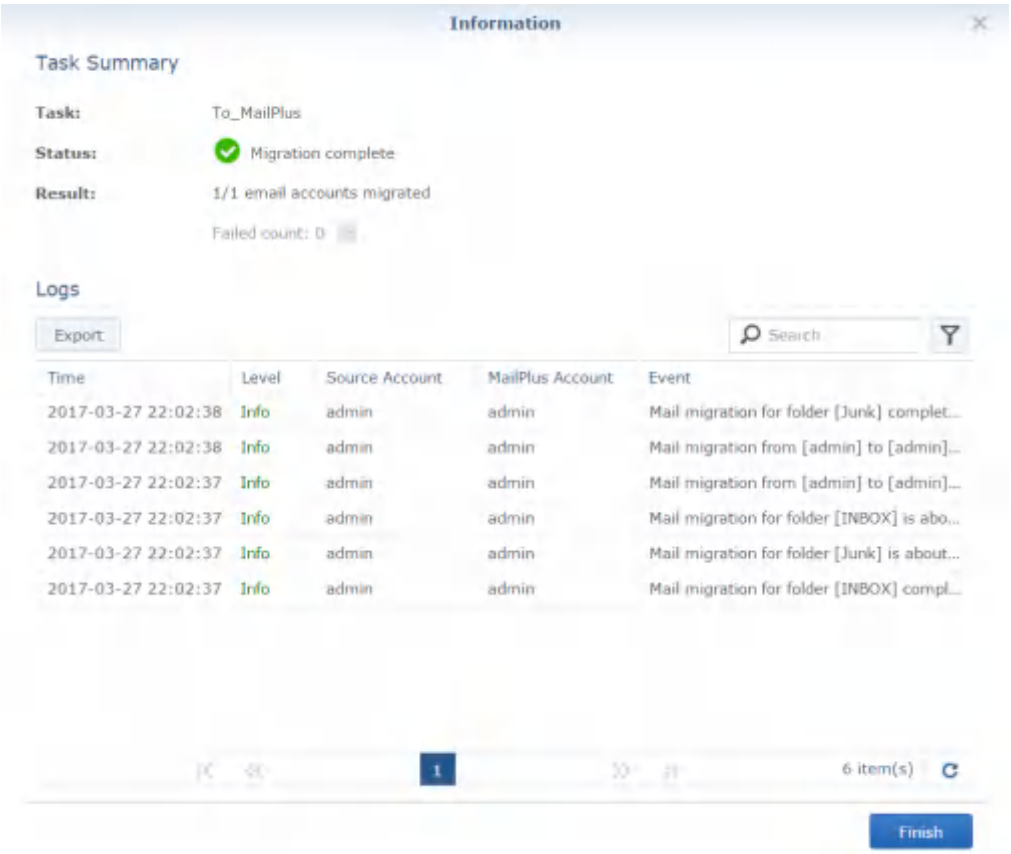


執行郵件移轉任務

1 在**伺服器管理** > **郵件移轉**選擇移轉任務，然後按一下**開始**來執行。若要避免移轉時發生錯誤，請勿更改 MailPlus Server 上的 IMAP/POP3 設定，或在來源郵件伺服器上移動 / 刪除郵件。



2 若要查看移轉統計資料及日誌，按一下**詳細資訊** (文件圖示)。



將 Microsoft Exchange 系統設定匯入 MailPlus Server

您可以將 Microsoft Exchange 的系統設定及別名匯出，再匯入到 MailPlus Server 繼續使用。

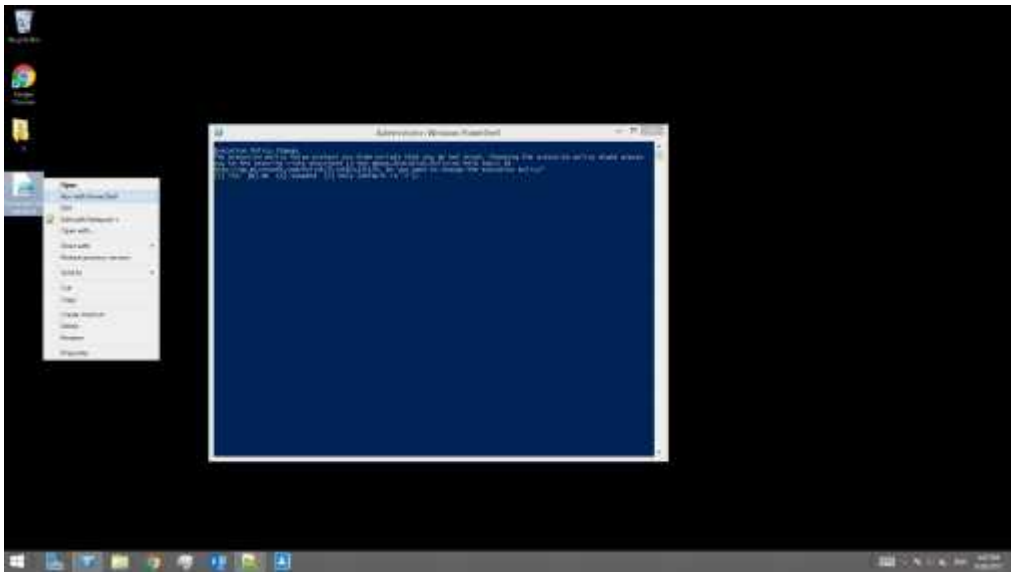
從 Microsoft Exchange 匯出系統設定及別名

1 從此處下載指令檔 (**ExchangeConfigExport.ps1**)。

2 在執行 Microsoft Exchange 伺服器的 Windows 電腦上，以系統管理員身份登入。

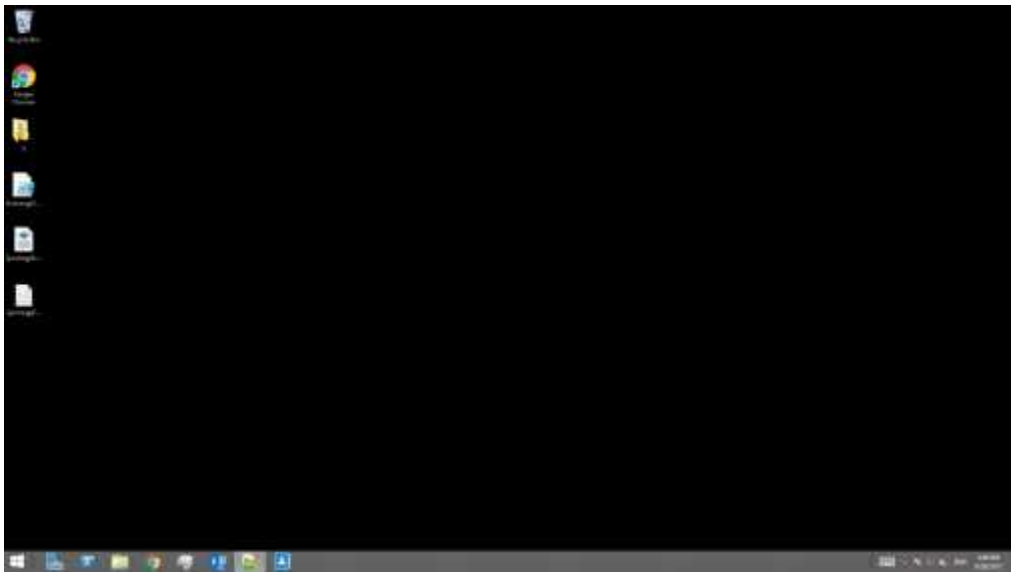
3 將指令檔移動到該臺 Windows 電腦。

4 在 Microsoft Exchange 伺服器上，使用 Windows PowerShell 執行指令檔。



5 當系統提示您變更執行方式時，選擇 Yes 來執行指令。

6 執行完成後，Microsoft Exchange 伺服器會將系統設定匯出為 **SynologyExportedExchangeConf.xml** 檔案，同時將別名匯出為 **SynologyExportedAlias.txt** 檔案。



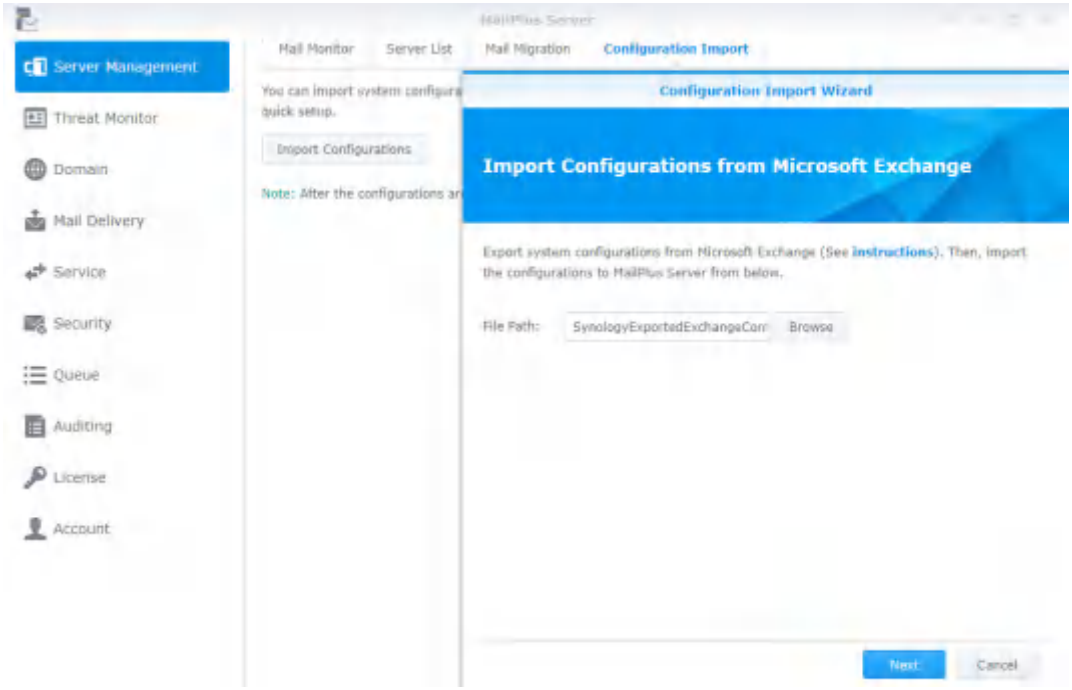
7 將產生的 .xml 檔案及 .txt 檔案移動到您的本機電腦。

匯入系統設定至 MailPlus Server

1 透過任一方式匯入：

- 當 MailPlus Server 進行初始化時：開啟 MailPlus Server，選擇從 **Microsoft Exchange 匯入設定來建立新的郵件系統**。
- 當 MailPlus Server 已完成初始化時：開啟 MailPlus Server，前往伺服器管理 > 匯入設定 > 匯入設定。

2 按一下瀏覽來從本機電腦匯入 **SynologyExportedExchangeConf.xml** 檔案。



3 按一下下一步，檢查一般設定 (例如：SMTP 及安全性設定) 與條件 (例如：黑白名單) 的設定細節。按一下匯入來完成匯入。

使用者授權

MailPlus Server 需要有足夠的授權數量，才能正常運作。授權數量是以啟動的帳號數量來計算。MailPlus Server 預設提供五組免費電子郵件帳號，若要增加更多使用者，需要購買額外授權。請參考**購買授權**來購買授權。啟動的帳號數量不計算以下項目：

- 停用的帳號
- 郵件別名
- 網域數量 (包含其他網域)
- 指定帳號類型以外的 DSM 使用者 (例如：指定帳號類型為 LDAP 使用者，則所有本地使用者均不計算在使用授權數量中)

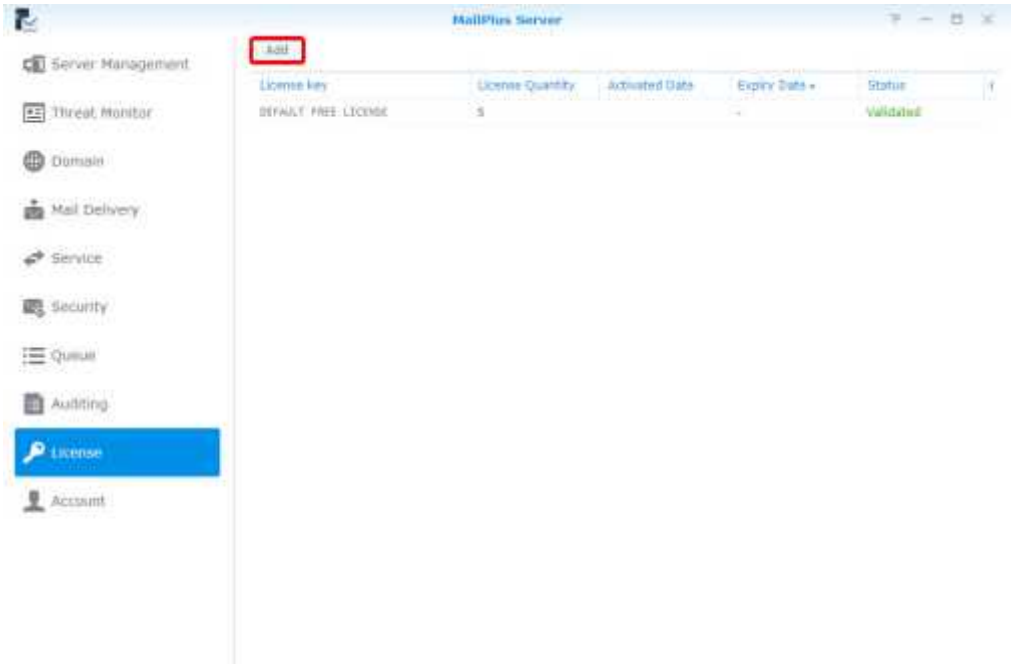
購買授權

MailPlus 授權分為五組或二十組帳號，可經由 Synology 的授權**經銷商**購買，請參考 **MailPlus 授權**來了解詳細資訊。

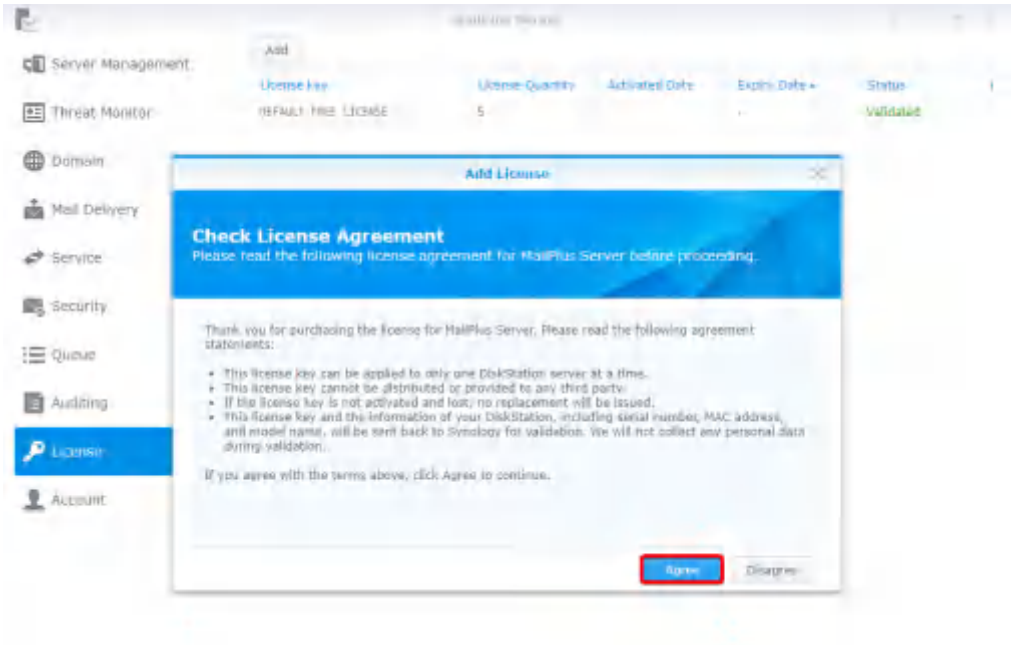
安裝授權

需要安裝購買之授權後，才能啟動電子郵件帳號。請參考下列步驟：

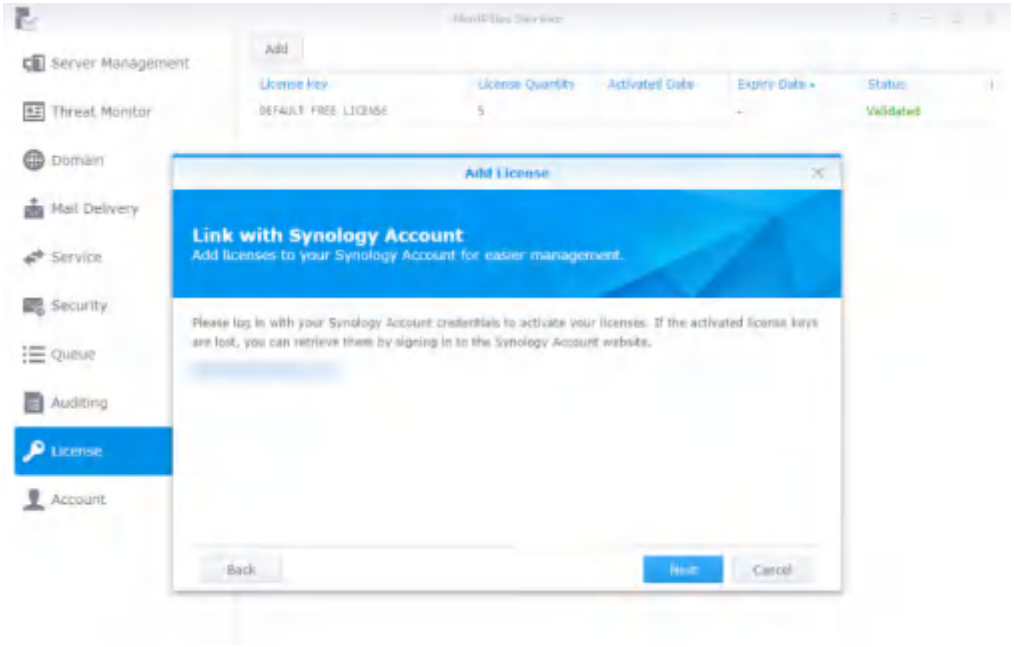
1 前往**授權**，按一下**新增**按鈕來新增授權。



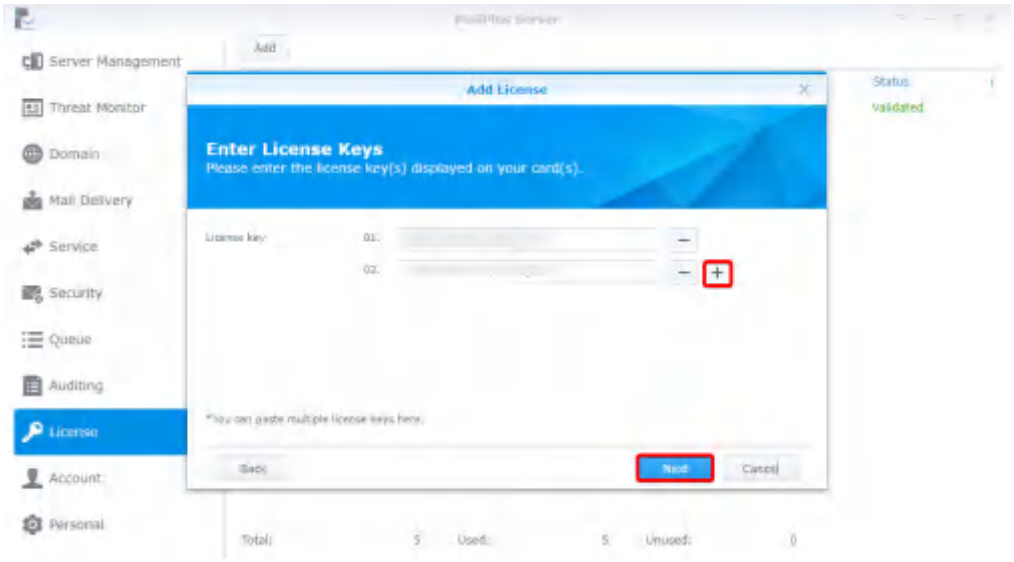
2 在**新增授權**的視窗中，請先詳細閱讀 MailPlus Server 的授權合約，確認並同意內容後，再按一下**同意**。



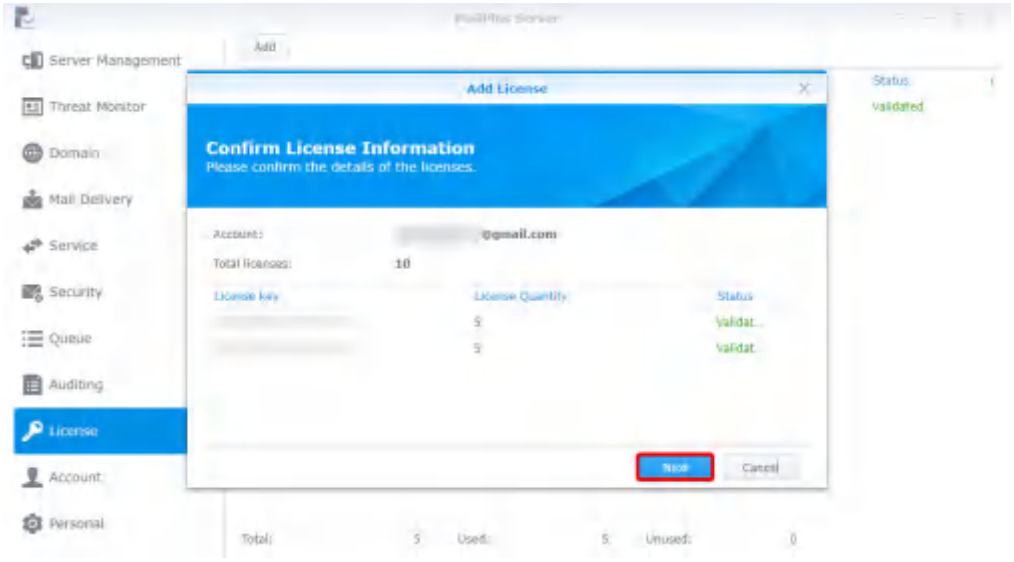
3 請登入 Synology 帳戶，讓新增的授權註冊在該 Synology 帳戶底下。如果發生已啟動的授權碼遺失的情況，只要登入 Synology 帳戶網站即可確認所有註冊在該帳戶底下的授權碼。登入 Synology 帳號後，按一下下一步。



4 如下圖所示，將欲新增的授權碼輸入至授權碼欄位中。若需一次新增多組授權，您可以按一下 + 按鈕來新增更多授權碼欄位。



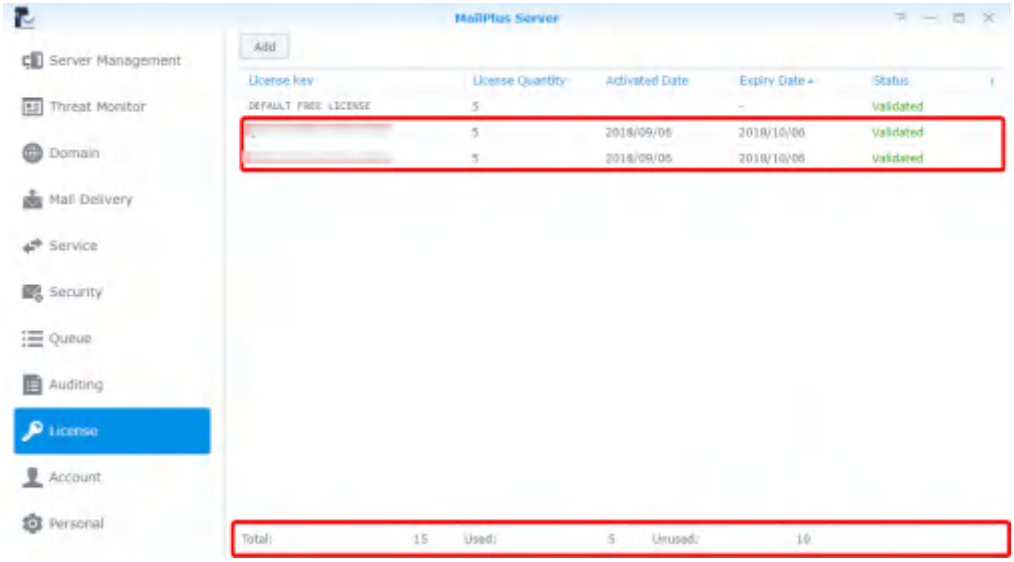
5 請確認欲新增的授權數量及授權碼是否正確，因為授權一經註冊，即無法移轉至另外一台 MailPlus Server。確認無誤後，按一下下一步來完成新增授權。



6 新增完授權後，您可以至授權頁面檢視各個授權的詳細資訊及狀態，包含：

- 授權碼序號
- 授權碼所提供的電子郵件帳號數量
- 授權啟動日期
- 授權到期日期
- 授權有效狀態

7 另外，授權頁面最下方則會顯示該台 MailPlus Server 目前所有能使用的授權數量，以及已使用和尚未使用的授權數量。



使用授權

新增完授權後，您可以前往帳號 > 使用者來選擇欲啟動的帳號。詳細資訊請參考啟動帳號。

帳號設定

帳號系統

MailPlus Server 和 DSM 的帳號系統是連動的，因此您可以在 MailPlus Server 上從 DSM 現有的帳號中選擇您要啟動的使用者帳號。

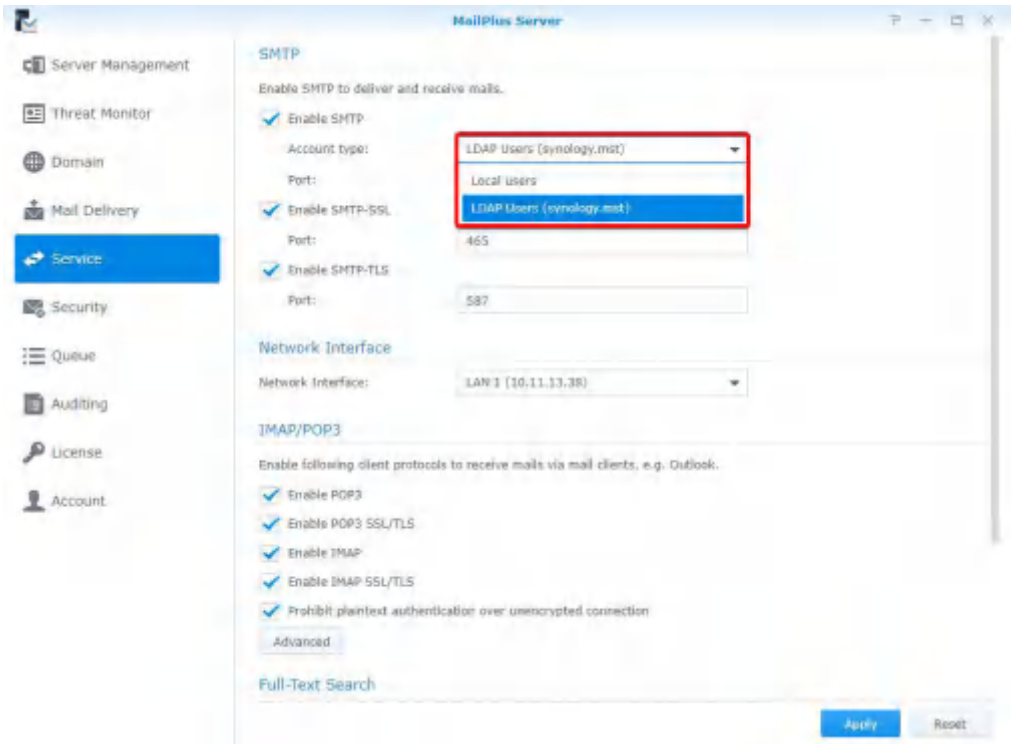
除了使用 DSM 上現有的本地使用者之外，您也可以啟動網域 /LDAP 帳號系統上的使用者帳號。(前往 **DSM** > **控制台** > **網域 /LDAP** 來綁定 **LDAP** 與**網域**上的帳號。) 然而，因為 DSM 一次只能與一台目錄服務同步，因此 MailPlus Server 無法同時同步多台目錄服務的帳號。

注意：MailPlus Server 只能從以下帳號類型中，選擇一種作為使用者帳號來源：本地、LDAP 或網域。

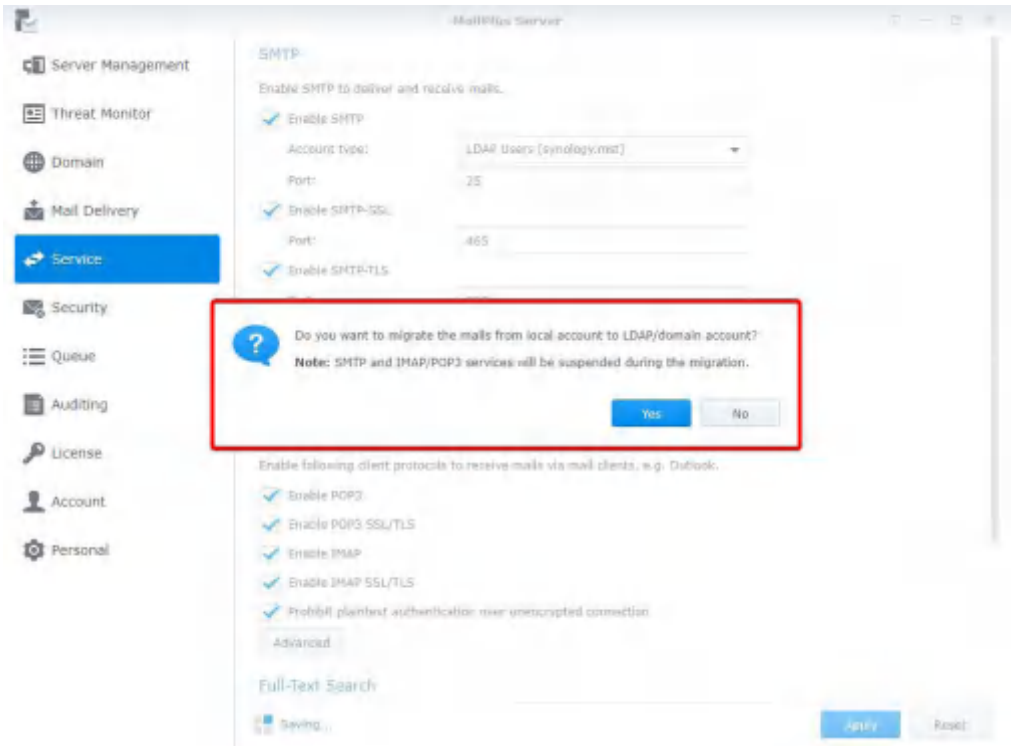
修改帳號類型

請參考以下步驟來修改帳號類型：

1 登入 **DSM**。
2 前往**控制台** > **網域 /LDAP** 與指定的目錄服務綁定。若您使用**本地使用者**作為帳號類型，請跳過此步驟。
3 開啟 **MailPlus Server**。
4 前往**服務**，然後從**帳號類型**下拉式選單選擇您要使用的帳號類型。(僅顯示 DSM 上已設定的目錄服務)



5 按一下套用將目錄服務中的使用者帳號匯入。如下圖所示，如果您從本地使用者切換至 LDAP 使用者或網域使用者，然後按一下套用，會出現提示視窗。



注意：因為不同的帳號類型有不同的郵件地址，因此每個帳號類型下的使用者信件並不互通。若要將本地使用者的信件轉移至 LDAP 使用者或網域使用者，按一下是。系統會將本地與目錄服務上同名的使用者帳號的信件轉移過去。若沒有同名的使用者，系統會自動忽略。

啟動帳號

您必須先在 MailPlus Server 裡啟動使用者帳號，才能開始使用收寄信等郵件服務。

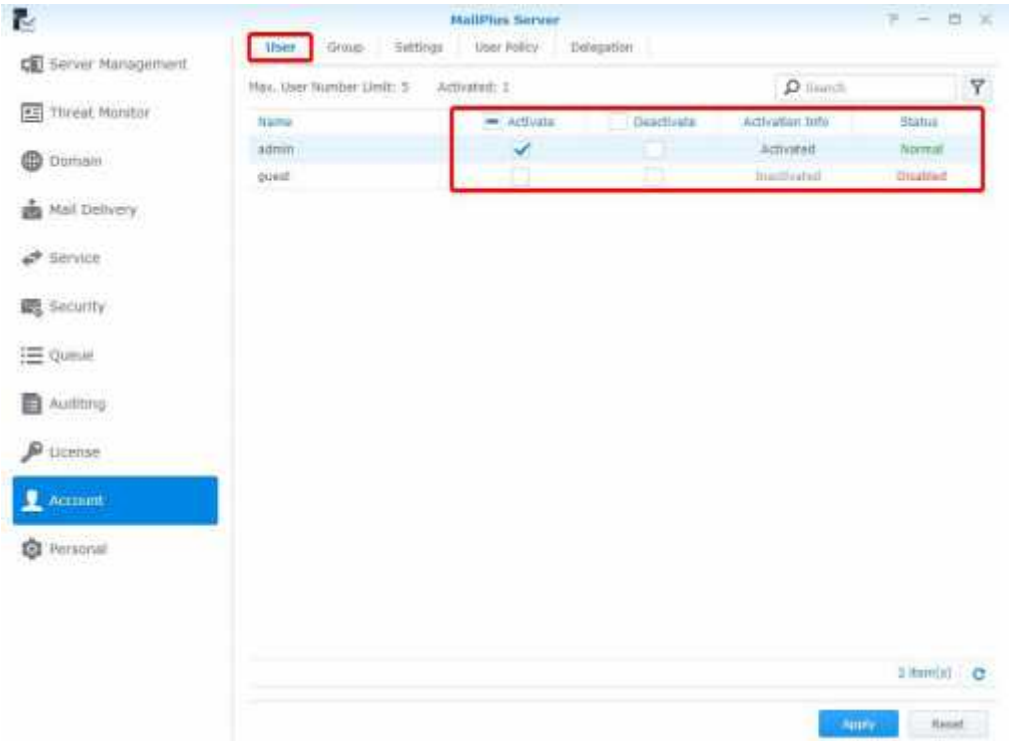
在開始正式使用 MailPlus Server 前，您必須啟動那些可以使用郵件服務的使用者。啟動帳號需要有足夠的授權，詳細的說明請參考使用者授權章節。

如果您已經啟動了若干使用者，但是使用者無法登入 DSM 或開啟 MailPlus/MailPlus Server，請確認您是否已停用使用者或是使用者沒有使用這些應用程式的權限。請參考 DSM 說明來取得更多資訊。

啟動使用者帳號

啟動使用者帳號需要有足夠的授權，相關說明請參考使用者授權。如果您需要啟動大量使用者，可以先參考啟動群組以及預設狀態。請參考下列步驟：

1 前往帳號 > 使用者帳號。
2 選擇您要啟動的使用者。若使用者的啟動與停用欄位下的核取方塊皆未勾選，則該使用者將被設定為預設狀態。請參考預設狀態。勾選啟動核取方塊時，授權數量將會減少。



3 **啟動資訊**顯示該使用者帳號是否套用授權。

4 **狀態**分為**正常**、**停用**，及**使用者名稱不受支援**。

注意：只有當**啟動資訊**為**已啟動**，且**狀態**為**正常**時，該使用者才能順利使用郵件服務。

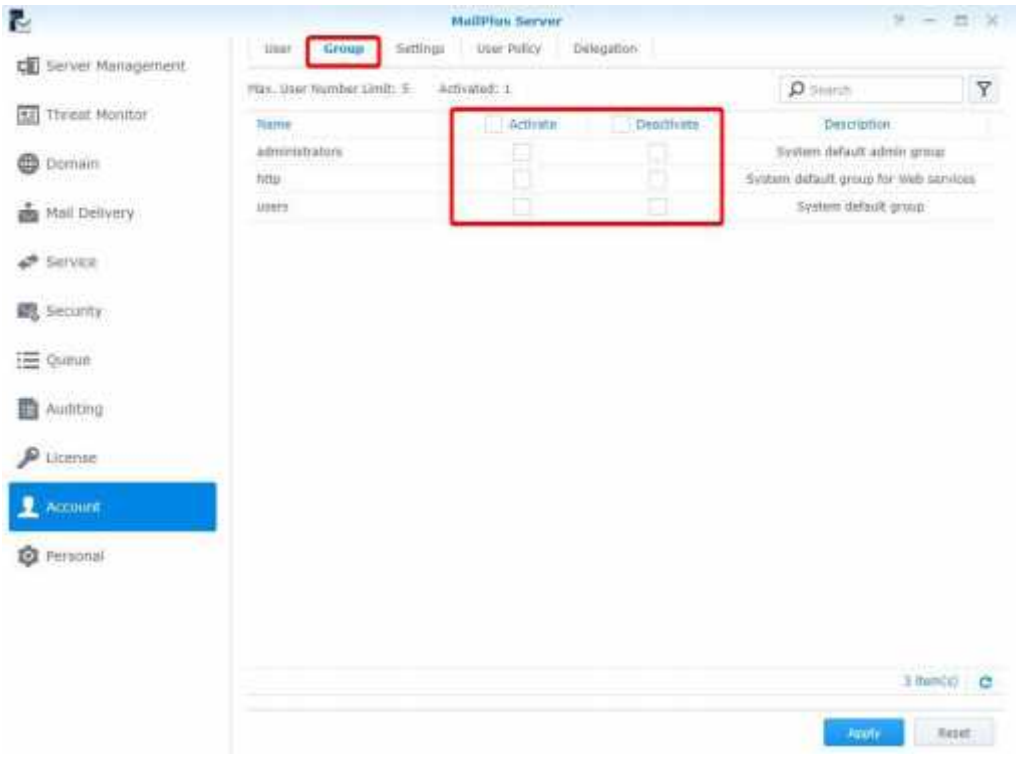
5 按一下**套用**來啟動使用者帳號。

啟動群組

您可以在此處快速針對使用者群組做啟動、停用的操作，且操作設定將會套用到群組下的每一位成員。請參考下列步驟：

1 前往**帳號** > **使用者群組**來啟動或停用該組群。

注意：最後使用者帳號是否啟動的判斷順序由高到低為：**使用者帳號**設定、**使用者群組**設定、**預設**設定。



2 按一下套用來啟動群組內的使用者。

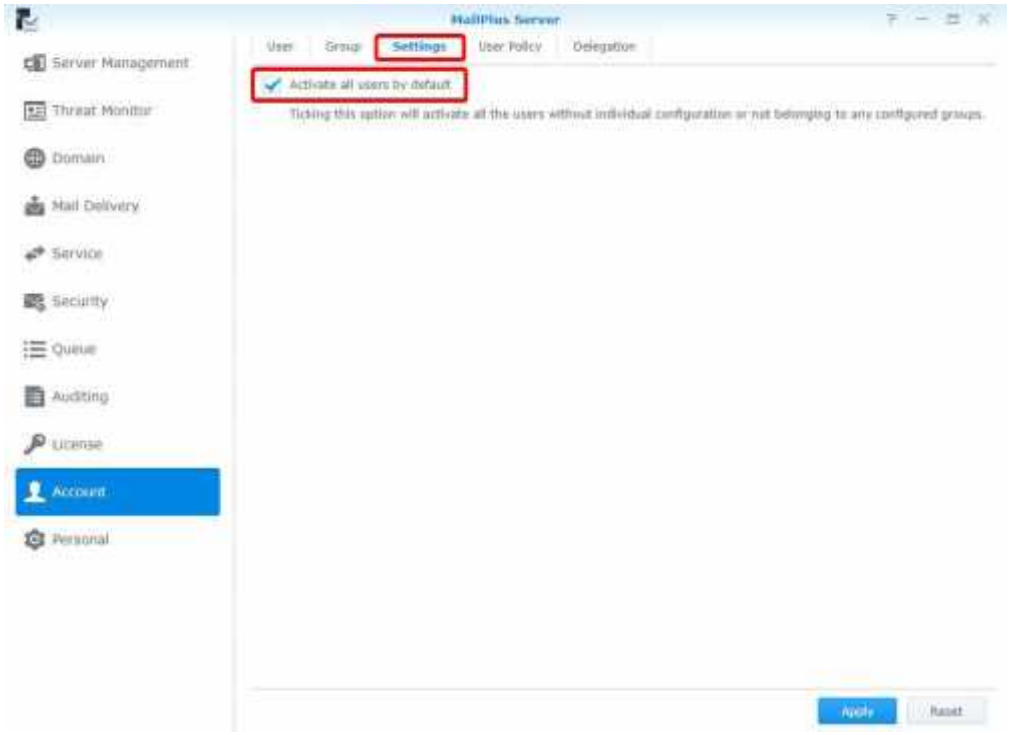
預設狀態

在帳號頁面的設定頁籤中，您可以查看您的預設狀態。

預設狀態會將預設的啟動資訊套用至尚未啟動或停用且狀態為正常的使用者帳號上。請參考下列步驟：

1 前往帳號 > 設定，選擇是否要勾選預設啟動所有使用者核取方塊。

注意：預設啟動將會消耗相對應的授權，請確認您有足夠的授權數量。



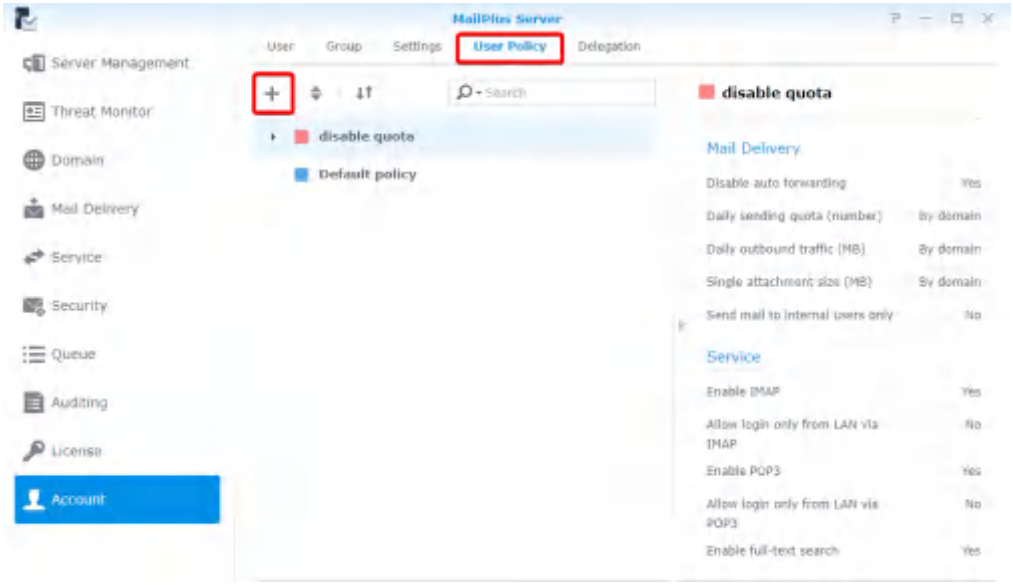
2 按一下套用來套用設定。

新增使用者規範

您可以在 MailPlus Server 上針對特定使用者或群組設定專屬的郵件服務使用規則。請參考以下步驟來新增使用者規範：

1 前往**帳號** > **使用者規範**。

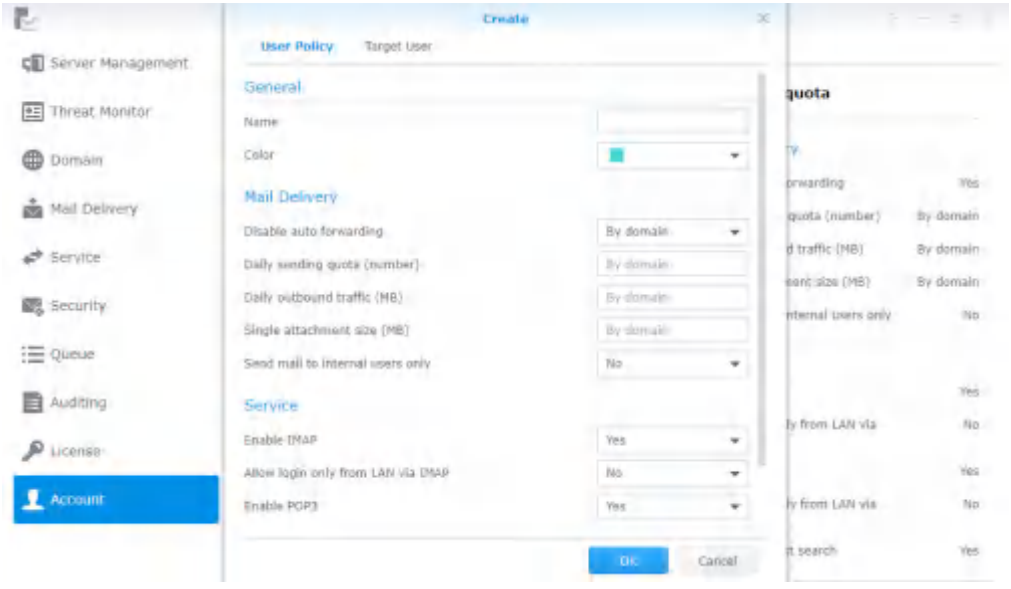
2 按一下加號按鈕來新增規範。



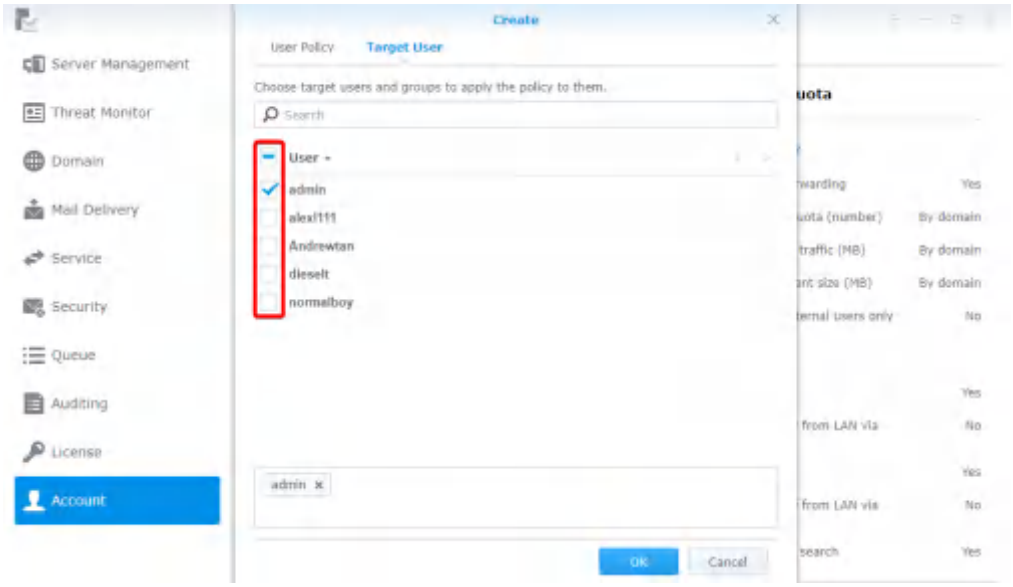
3 在**新增**視窗的**使用者規範**頁籤中，於**名稱**欄位中輸入規範的名稱。

4 從**顏色**的下拉式選單中選擇規範的顏色，方便日後管理。

注意：請參考**規範內容說明與限制**來了解更多規範功能的資訊。

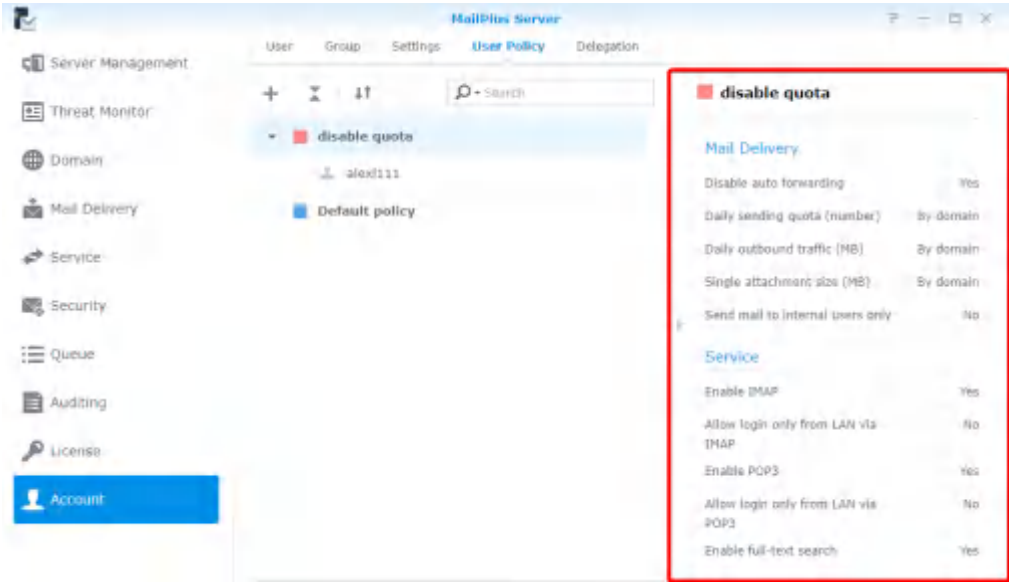


5 切換到**目標使用者**頁籤，選擇要套用此規範的使用者。您也可以透過上方的搜尋欄位來搜尋使用者。



6 按一下**確定**來完成。

7 完成新增後，您可以在**使用者規範**頁面中檢視已新增的規範。選擇規範後您可在右側面板中預覽規範的設定內容。

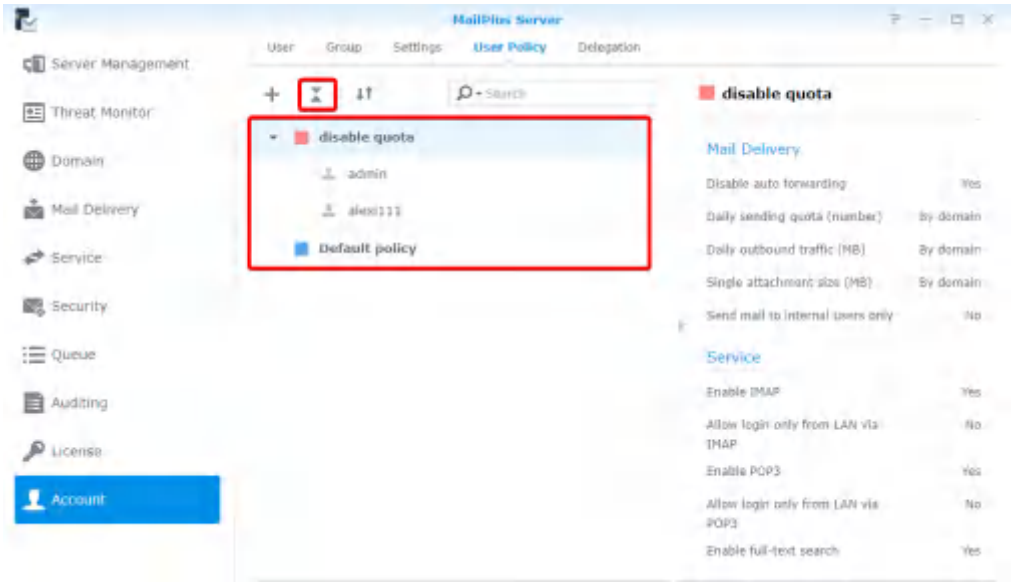


變更使用者規範優先權

使用者可能會同時被套用多個規範，但只有一個規範會生效，因此系統會根據使用者規範的優先權規則，決定套用至該使用者的規範。請參考以下步驟來變更使用者規範優先權：

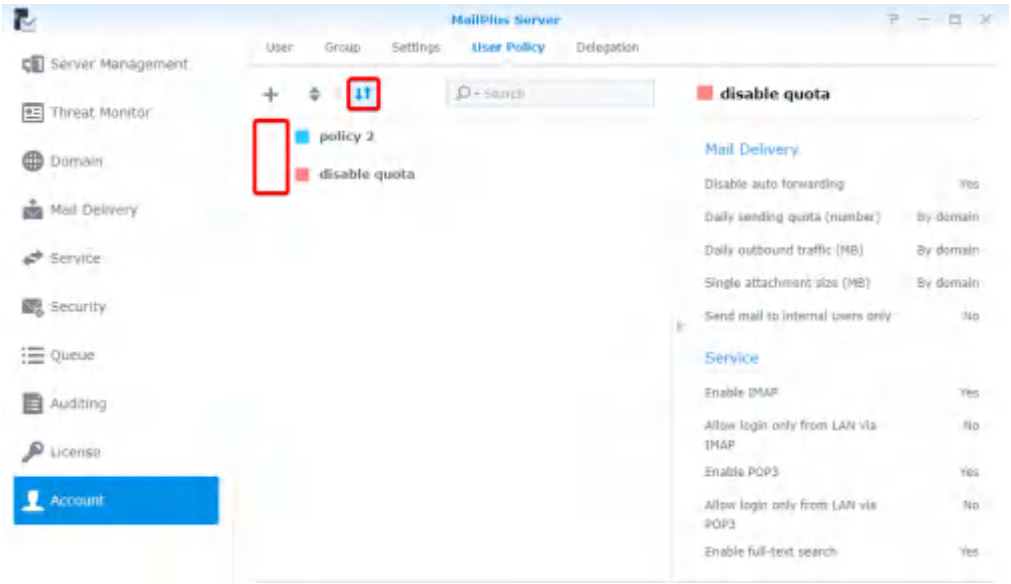
1 前往**帳號** > **使用者規範**，按一下雙三角形圖示來顯示或隱藏目標使用者 / 群組。

2 最高處的規範將比下方的規範更加優先被套用。(例如：圖中的優先權順序由高到低為：*Old policy*、*New policy*、*預設規範*，因此使用者 *admin* 會被套用 *Old policy* 而非 *New policy*。)



3 您可以按一下更換優先順序按鈕 (雙向箭頭圖示) 來調整優先權。

注意：如果您希望使用者套用特定規範，請確認欲套用的規範的優先權，高於其他同樣套用至此使用者的規範。



4 將滑鼠移至規範的左側，根據優先權拖拉規範至適合的位置。

5 按一下更換優先順序按鈕 (雙向箭頭圖示) 來關閉拖拉功能，讓新的優先順序生效。

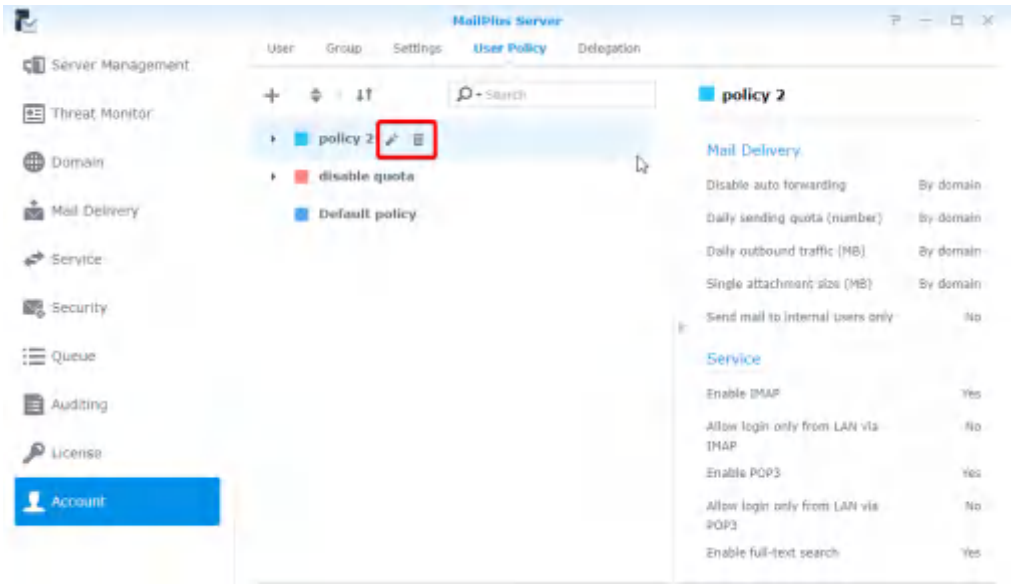
注意：預設規範的優先權永遠是最低的。請參考 預設規範來了解更多資訊。

編輯及刪除使用者規範

您可以修改規範的設定、增加或刪除規範內的使用者，或是更改規範的顏色。請參考以下步驟來編輯或刪除使用者規範：

1 前往帳號 > 使用者規範。

2 將滑鼠移至欲編輯的規範上時，會出現兩個按鈕。您可以按一下鉛筆圖示來編輯規範，或按一下垃圾桶圖示來刪除使用者規範。



預設規範

所有未被加入自訂規範的使用者，都會被套用預設規範。預設規範一開始就存在，您無法編輯、刪除或重新設定優先順序。請參考下列預設規範的設定資訊：

停用自動轉寄	預設為**依據網域設定**
每日寄送限額 (數量)	預設為**依據網域設定**
每日傳送流量 (MB)	預設為**依據網域設定**
單一附加檔案大小 (MB)	預設為**依據網域設定**
僅可寄送郵件給內部使用者	預設為**否**
啟動 IMAP	預設為**是**
僅允許從區域網路透過 IMAP 登入	預設為**否**
啟動 POP3	預設為**是**
僅允許從區域網路透過 POP3 登入	預設為**否**
啟動全文檢索	預設為**是**

因為所有使用者至少都會套用到預設規範，某些規範的限制可能並不符合您的預期。若您不希望特定限制生效，必須關閉相對應的限制，請參考**規範內容說明與限制**來了解更多資訊。

規範內容說明與限制

編號	規範	啟動效果	停用效果	依據網域設定
01	停用自動轉寄	使用者無法自動轉寄信件	使用者可以自動轉寄信件	規範會依據網域設定

注意：

1. 此規範不影響手動轉寄。

編號	規範	啟動效果	停用效果	依據網域設定
02	每日寄送限額 (數量)	使用者有數量額度限制	使用者沒有數量額度限制	規範會依據網域設定

注意：

1. 若信件在送出前就被拒的話，不會計入使用量。
2. 若信件在送出後被退回，則會計入使用量。
3. 預設規範的預設值與**網域**頁面**用量限制**頁籤中**每日配額**的**每日限額**設定值相同。
4. 設定值為 0 時，使用者將不受限制。
5. 您必須前往**郵件傳送** > **一般**，勾選**啟動 SMTP 驗證**核取方塊。

編號	規範	啟動效果	停用效果	依據網域設定
03	每日傳送流量 (MB)	使用者有流量額度限制	使用者沒有流量額度限制	規範會依據網域設定

注意：

1. 若信件在送出前就被拒的話，不會計入使用量。
2. 若信件在送出後被退回，則會計入使用量。
3. 預設規範的預設值與**網域**頁面**用量限制**頁籤中**每日配額**的**每日流量上限 (MB)** 設定值相同。
4. 設定值為 0 時，使用者將不受限制。
5. 您必須前往**郵件傳送** > **一般**，勾選**啟動 SMTP 驗證**核取方塊。

編號	規範	啟動效果	停用效果	依據網域設定
04	單一附加檔案大小 (MB)	使用者夾帶的檔案有大小限制	使用者夾帶檔案沒有大小限制	規範會依據網域設定

注意：

1. 預設規範的預設值與**郵件傳送**頁面**一般**頁籤中**單一信件大小限制 (MB)** 設定值相同。
2. 預設規範的設定值也適用於外部來信。

編號	規範	啟動效果	停用效果
05	僅可寄送郵件給內部使用者	使用者僅能寄送信件至內部網域的其他使用者。	使用者不受限制。

注意：目前沒有開放設定所有使用者皆僅能寄送郵件給內部使用者。

編號	規範	啟動效果	停用效果
06	啟動 IMAP	使用者可以使用 IMAP	使用者無法使用 IMAP

注意：若**服務**頁面中 **IMAP/POP3** 區塊下的**啟動 IMAP** 核取方塊未被勾選，則 IMAP 服務是關閉的，因此使用者規範也不會生效，不會因為使用者規範設定**啟動 IMAP** 就能登入。

編號	規範	啟動效果	停用效果
07	僅允許從區域網路透過 IMAP 登入	使用者只能從子網域透過 IMAP 登入	使用者登入 MailPlus 時不受限制。

注意：

1. 若**服務**頁面中 **IMAP/POP3** 區塊下的**啟動 IMAP** 核取方塊未被勾選，則 IMAP 服務是關閉的，因此使用者規範也不會生效，不會因為使用者規範設定**僅允許從區域網路透過 IMAP 登入**而能登入。
2. MailPlus 網頁用戶端不受此設定限制。

編號	規範	啟動效果	停用效果
08	啟動 POP3	使用者可以使用 POP3	使用者無法使用 POP3

注意：若服務頁面中 **IMAP/POP3** 區塊下的**啟動 POP3** 核取方塊未被勾選，則 POP3 服務是關閉的，因此使用者規範也不會生效，不會因為使用者規範設定**啟動 POP3** 而能登入。

編號	規範	啟動效果	停用效果
09	僅允許從區域網路透過 POP3 登入	使用者只能從子網域透過 POP3 登入	使用者登入 MailPlus 時不受限制

注意：

1. 若服務頁面中 **IMAP/POP3** 區塊下的**啟動 POP3** 核取方塊未被勾選，則 POP3 服務是關閉的，因此使用者規範也不會生效，不會因為使用者規範設定**僅允許從區域網路透過 POP3 登入** 而能登入。
2. 您仍能從外部網路登入 MailPlus (因為 MailPlus 是從內部直接與郵件伺服器連線)。

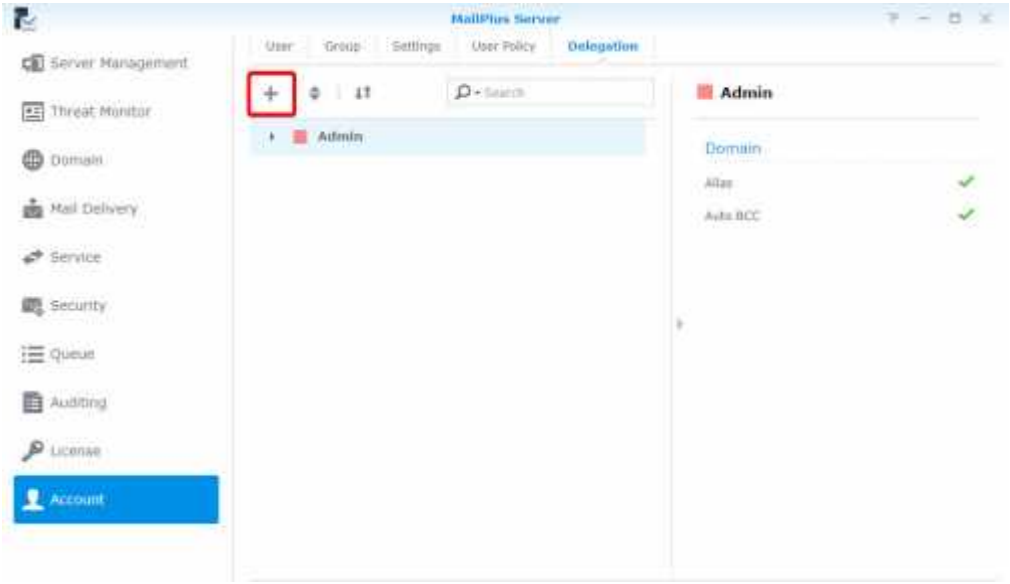
編號	規範	啟動效果	停用效果
010	啟動全文檢索	伺服器會為使用者的郵件內容進行索引	伺服器不會為使用者的郵件內容進行索引

注意：若服務頁面中**全文檢索**區塊下的**啟動全文檢索**核取方塊未被勾選，則使用者規範的設定不會生效，因此不會為任何使用者的郵件內容進行索引。

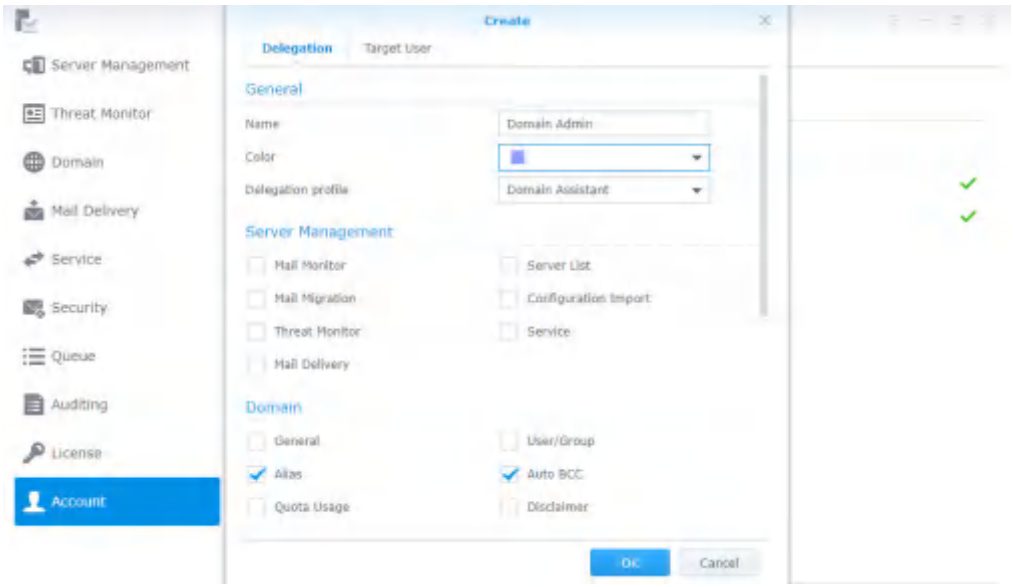
新增委派規範

在**管理委派**頁籤中，您可以讓其他使用者依照您指派給他們的管理委派模板，來管理 MailPlus Server 中伺服器管理、網域、安全性、稽核和帳號 (不包含授權) 的相關設定。本章節將以網域管理員為例。

1 前往**帳號** > **管理委派**，按一下上方的加號圖示。

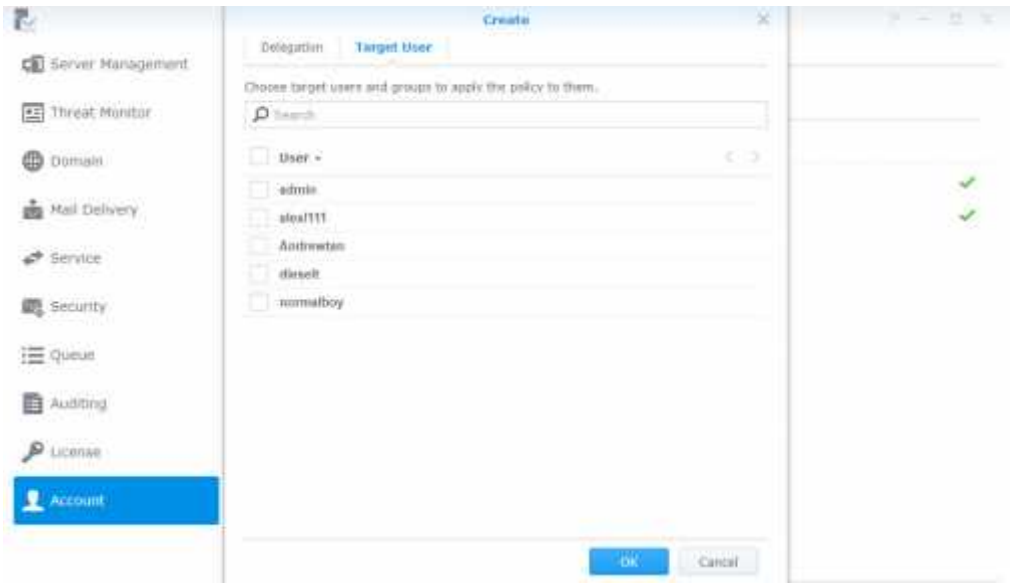


2 在跳出視窗的管理委派頁籤中輸入必要的資訊。系統會按照您選擇的管理委派模板，自動勾選下方的選項。若您勾選或取消勾選下方的選項，它會切換成自訂。請參考此篇文章來了解更多對應的委派權限。



例如：若您為網域管理員選擇網域總管，套用此委派規範的使用者就能管理現有網域的所有設定。但是，若您為網域管理員選擇網域助理，套用此委派規範的使用者就只能管理網域中的別名和自動密件副本設定。

3 前往目標使用者頁籤來選擇要套用訂定的委派規範的使用者 / 群組。



4 按一下確定來儲存設定。

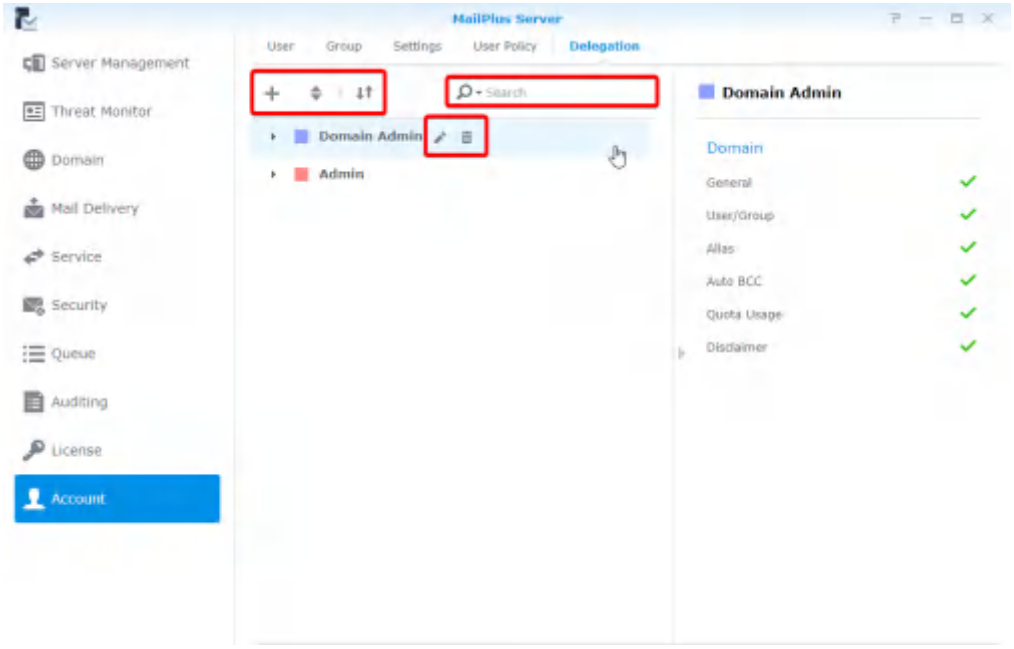
管理委派規範

1 前往帳號 > 管理委派。

2 選擇網域管理員，您就可以檢視、編輯或刪除該規範。

3 您可以使用上方工具列的按鈕和右方的預覽面板來管理委派規範：

- **設定規範優先權：**
  1 按一下雙向箭頭圖示來設定優先權。
  2 按一下網域管理員，並將它拖放至適合的位置。若使用者 / 群組套用了不只一個委派規範，系統會將清單中優先權最高的規範套用至該使用者 / 群組。
- **展開 / 收合委派規範：**按一下雙向箭頭圖示來展開或收合目標使用者 / 群組。
- **搜尋委派規範：**在上方的搜尋欄位輸入規範名稱或其包含的使用者。
- **預覽委派規範：**預覽委派規範的名稱、設定和其他細節。
- **編輯委派規範：**按一下鉛筆圖示來編輯規範。
- **刪除委派規範：**按一下垃圾桶圖示來刪除規範。



管理權限

MailPlus Server 的管理權限設定與 DSM 的管理權限同步，換言之，在 DSM 中屬於管理者群組的使用者也可以存取 MailPlus Server 的所有設定。一般使用者僅能檢視個人頁面。

協定設定

您可以在此找到與郵件服務協定相關的伺服器設定，亦可控制特定通訊協定的連接埠開關，或是重新綁定伺服器的網路介面。由於通訊協定的設定會影響整個伺服器對外的運作，請確認您的操作合乎您的需求。

SMTP 協定

SMTP 相關的協定使用了三個連接埠。在 MailPlus Server 中，顯示為 SMTP (連接埠編號 : 25)、SMTP-SSL (連接埠編號 : 465)、SMTP-TLS (連接埠編號：587)。這三個協定的角色分別為：

- **SMTP**：SMTP 通訊協定是負責接收外部郵件及寄送內部郵件的標準協定。MailPlus Server 使用 Post□x，在沒有特別指定 STARTTLS 時會以明碼傳送訊息。我們目前並沒有強制加密 SMTP 內容，如需設定加密，請參考此處。
- **SMTP-SSL**：**SMTP-SSL** 所支援的協定為 SMTPS。由於 DSM 不再支援 SSL 加密，因此 MailPlus Server 只能透過 TLS 連線至 SMTP-SSL。

注意：這與 SMTP 協定透過 STARTTLS 來加密並不同，SMTPS 必須在握手後便送出已加密的封包。若需要使用這個協定進行轉送，請參考此處來了解更多資訊。

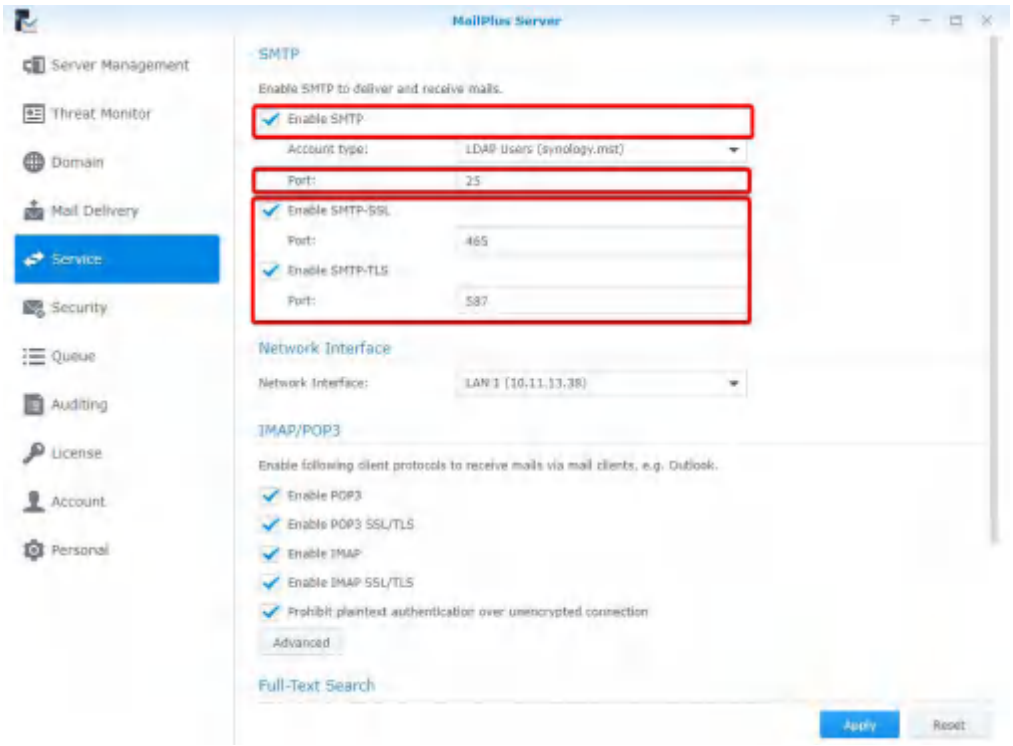
- **SMTP-TLS**：SMTP-TLS 所支援的協定為 SMTP，再透過 START-TLS 進行加密。期間，SMTP-TLS 需要進行身分驗證，因此常常用來做為用戶端與 MSA 之間的內部協定。

設定 SMTP 協定

請參考以下步驟來設定 SMTP 協定及相關的連接埠：

1 前往服務 > SMTP，勾選啟動 SMTP 核取方塊。

注意：這是郵件伺服器主要的協定。



2 您可以在連接埠欄位中變更埠號。

注意：若無特別原因，建議您使用預設的 25 連接埠。

3 您可以在此調整以下設定：

- **啟動 SMTP-SSL**：使用 SMTPS 協定，您可以在**連接埠**欄位中改變 SMTP-SSL 的埠號。
- **啟動 SMTP-TLS**：強制連線時，進行使用者身分驗證以及 STARTTLS 加密。您可以在**連接埠**欄位中改變 SMTP-TLS 的埠號。

4 按一下**套用**來儲存設定。

IMAP/POP3 協定

IMAP/POP3 提供加密與不加密的選項，因此使用了四個連接埠。在 MailPlus Server 中分別為 IMAP (143 連接埠)、IMAPS (993 連接埠)、POP3 (110 連接埠)、POP3S (995 連接埠)。您可以透過這兩種協定以不同的郵件用戶端來取得 MailPlus Server 上的信件資訊。

注意：兩者的加密皆是透過 START-TILS 來進行。由於 DSM 不再支援 SSL 加密連線，所以請不要在設定上透過 SSL 加密連線。

- **IMAP**：**IMAP 協定**是讓使用者存取郵件伺服器上儲存資訊的標準協定，相較 POP3 有更多利於郵件服務的支援選項。
- **POP3**：**POP3 協定**也是讓使用者存取郵件伺服器上儲存資訊的標準協定。

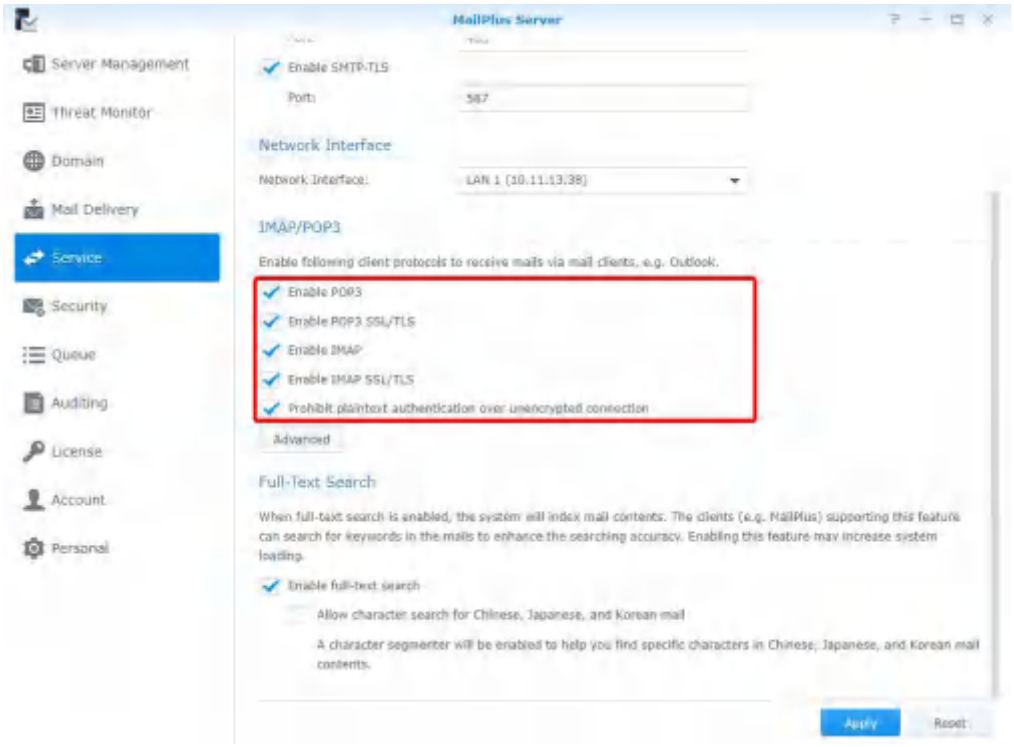
設定 IMAP/POP3 協定

請參考以下步驟來設定 IMAP 協定、POP3 協定及相關的連接埠：

1 前往**服務** > **IMAP/POP3**。

2 您可以在 **IMAP/POP3** 區塊中調整以下設定：

- **啟動 POP3**：用戶端郵件軟體透過 POP3 協定收取信件。
- **啟動 POP3 安全連線 (SSL/TLS)**：加密 POP3 連線。
- **啟動 IMAP**：用戶端郵件軟體透過 IMAP 協定收取信件。
- **啟動 IMAP 安全連線 (SSL/TLS)**：加密 IMAP 連線。



3 按一下**套用**來儲存設定。

網路介面

MailPlus Server 建立，會有一組預設的通訊協定設定。為使 MailPlus Server 支援 **High-availability 叢集**，在您安裝 MailPlus Server 或設置 High-availability 後， MailPlus Server 會與網路介面綁定，而您伺服器上的郵件服務便會運行在綁定的介面上。

網路介面綁定

當您的 MailPlus Server 在單台伺服器上運行時，您可以將 MailPlus Server 與區域網路、PPPoE 或結合的網路介面綁定。當您的 MailPlus Server 在 High-availability 架構下運行時，您可以將 MailPlus Server 與區域網路和及結合的網路介面綁定，且必須透過**手動設定網路組態**，取得該網路介面的 IP 位址。

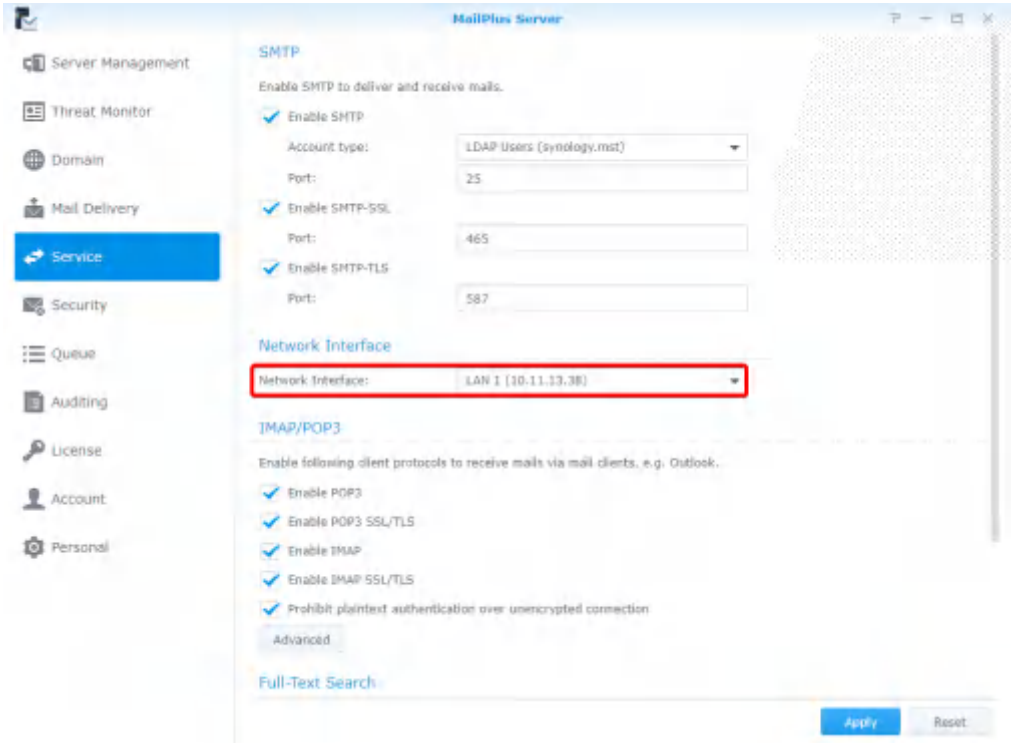
注意：當您的 MailPlus Server 與結合的網路介面綁定時，您無法解除連結該結合的網路介面。若要取消綁定已結合的網路介面，您需要先變更網路介面或是解除安裝 MailPlus Server。

變更網路介面

1 登入 **DSM**。

2 開啟 **MailPlus Server**。

3 前往**服務** > **網路介面**，在**網路介面**下拉式選單中切換網路介面。



4 按一下**套用**來儲存設定。

SMTP 設定

在安裝階段完成 MailPlus Server 必要的設定後，您可能仍需調整或修改郵件服務和細部設定，包含 SMTP 協定的連線安全等等，這些修改可以在此完成。

服務設定

您可以前往**郵件傳送**頁面來設定 **MailPlus Server** 的郵件收寄規定，例如單一信件大小限制和郵件訊息收件人數上限。

MailPlus Server 提供方便且快速的服務設定選項，包含：

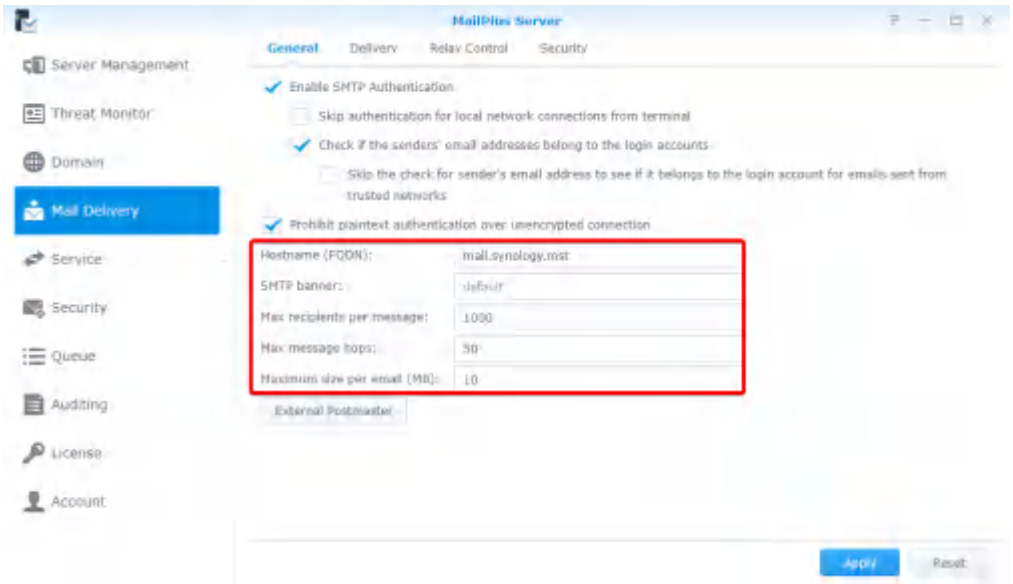
- **SMTP 規則**：您可以為 **MailPlus Server** 指定一個主機名稱、在用戶端的 Telnet 終端機上指定 SMTP 橫幅，亦可設定收發郵件的基本規則，例如單一信件大小限制、收件人數上限等等，避免一封信件佔用太多資源。
- **全文檢索**：全文檢索功能讓 **MailPlus** 網頁用戶端對信件進行索引，方便快速查找信件內容。另外，全文檢索支援以中文、日文及韓文字元搜尋。因為全文檢索會對所有信件內容進行索引，可能會略為增加伺服器的負載。您可以自行決定是否啟動全文檢索功能，或是停用特定使用者的全文檢索。請參考**新增使用者規範**來了解更多資訊。

設定 SMTP 規則

SMTP 規則包含 **MailPlus Server** 如何將信件寄送至其他郵件伺服器的準則。

1 前往**郵件傳送** > **一般**。

- **主機名稱 (FQDN)**：為 **MailPlus Server** 輸入 FQDN 格式的主機名稱，確認此名稱與 DNS 伺服器中的 IP 位址相符。
- **SMTP 橫幅**：輸入會出現在 SMTP 用戶端的 Telnet 終端機上的文字。
- **郵件訊息收件人數上限**：設定收寄郵件訊息的收件人數上限，超過此數量的郵件會被退回。
- **郵件訊息躍點 (hop) 數上限**：設定收寄郵件訊息的躍點 (例如郵件轉送) 數量上限，超過此數量的郵件會被退回。
- **單一信件大小限制 (MB)**：設定收寄郵件訊息的檔案大小上限，超過此大小的郵件會被退回。



2 按一下**套用**來儲存設定。

外部郵件管理者

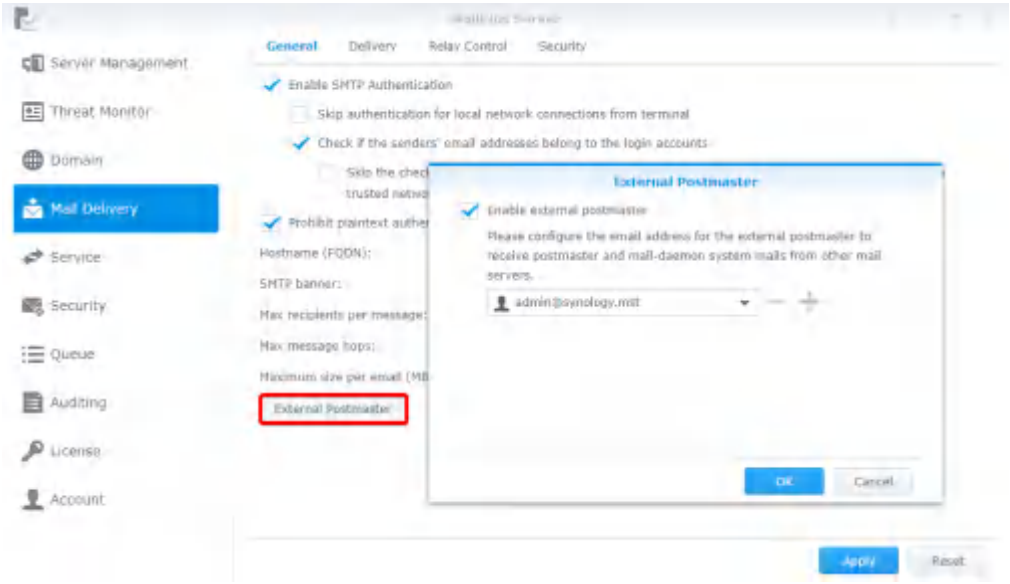
設定外部郵件管理者，來接收其他郵件伺服器寄至 Mailer- daemon 和 Postmaster 別名的系統郵件。

1 前往**郵件傳送** > **一般**。

2 按一下**外部郵件管理者**按鈕。

3 勾選**啟動外部郵件管理者**核取方塊。

4 按一下加號圖示來新增外部郵件管理者的郵件地址。



5 按一下**確定**來儲存設定。

全文檢索

啟動全文檢索功能時，伺服器會對每封信件的主旨、寄件人、收件人以及內文進行索引，讓您可以透過支援此功能的用戶端 (例如：MailPlus) 搜尋關鍵字，提升查看信件的方便性。

注意：若您收寄大量的信件，啟動此功能可能會增加伺服器的負載。

1 前往**服務**。

2 您可以在**全文檢索**區塊下調整以下設定：

- **啟動全文檢索：**勾選此選項後，您可以參考**新增使用者規範**來進一步停用特定使用者的全文檢索功能，以降低伺服器負載。
- **允許中文、日文、韓文郵件進行字元檢索：**在您勾選此選項後，會啟動斷字工具，以協助您尋找在中文、日文、韓文郵件中的特定字元。

3 按一下**套用**來儲存設定。

SMTP 安全連線

透過分析使用者的連線、登入資訊以及郵件內容，加強您的郵件伺服器的安全性和穩定性。您可以利用這部分的設定選項，訂定可以使用您的郵件伺服器所提供服務的使用者的條件。這不僅保障了您的服務品質，同時也能防止 MailPlus Server 成為垃圾郵件的轉運站，進而被列為黑名單。

- **SMTP 驗證**：啟動 SMTP 驗證後，使用者必須輸入 DSM 帳號及密碼來進行驗證，伺服器才會轉送信件。

注意：只有轉送時才需要進行身分驗證，這是為了避免伺服器成為垃圾郵件的轉運站。請參考此篇文章來了解更多資訊。

- **黑白名單**：若您的伺服器不斷收到垃圾郵件，您可以透過在黑名單中設置特定條件，來拒絕服務。另外，若您的伺服器有啟動**防毒掃描**、**認證**等掃描功能，可能會不小心退回某些您希望收到的信件；在此情況下，您可以透過制定白名單來跳過安全性掃描，確保能順利收到重要的信件。
- **寄件人規範**：掃描寄件人地址，並可以設定條件，拒絕不合格的格式或是無法驗證的地址。
- **連線規範**：在連線階段進行掃描，限制用戶 IP 數量，防止同一個 IP 位址佔用過多流量或製造大量攻擊。
- **進階設定**：在連線階段要求精確的指令及其他進階設定。參考**進階設定**來了解更多資訊。

啟動 SMTP 驗證

身分驗證可以阻止惡意使用者利用您的郵件伺服器來轉送垃圾郵件。建議您啟動 SMTP 驗證功能，讓未通過身分驗證的使用者無法轉送他們的信件，避免您的伺服器被列為黑名單。

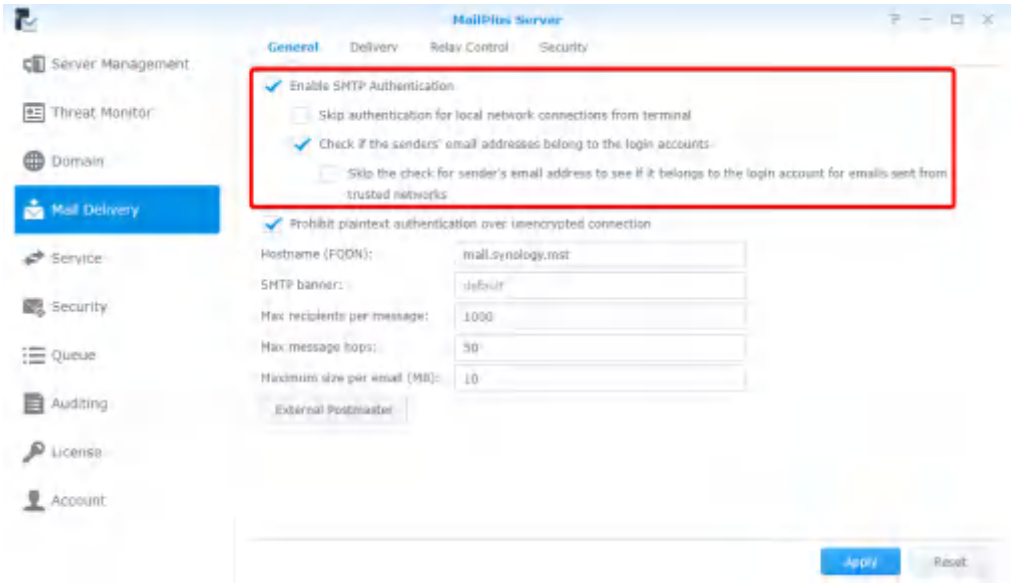
注意：MailPlus Server 中的部分功能需要通過身分驗證才能使用，例如**每日配額**。

1 前往**郵件傳送** > **一般**，選擇是否勾選**啟動 SMTP 驗證**核取方塊。

2 若您勾選**啟動 SMTP 驗證**核取方塊，可以再調整以下設定：

- **來自終端機的區域網路連線不需進行身份驗證**：使用區域網路存取郵件服務的使用者不需進行身份驗證。
- **檢查寄件人的郵件地址是否屬於登入帳號**：登入的使用者必須使用屬於該登入帳號的電子郵件地址來寄送信件。

  注意：若您勾選**一般**頁籤中的**檢查寄件人的郵件地址是否屬於登入帳號**核取方塊，**MailPlus Server** 可能會退回來自**信任名單**的信件。您可以前往**一般**頁籤，勾選**略過檢查由信任的網路寄出的信件寄件人電子郵件位址是否屬於登入帳號**核取方塊來跳過檢查。若您勾選**一般**頁籤中的**來自終端機的區域網路連線不需進行身份驗證**，來自區域網路的信件將不會被 **MailPlus Server** 封鎖。



3 按一下**套用**來儲存設定。

新增黑白名單

系統會對符合**黑白名單**中設定條件的郵件執行對應的動作。您可以參考以下步驟來新增黑白名單規則：

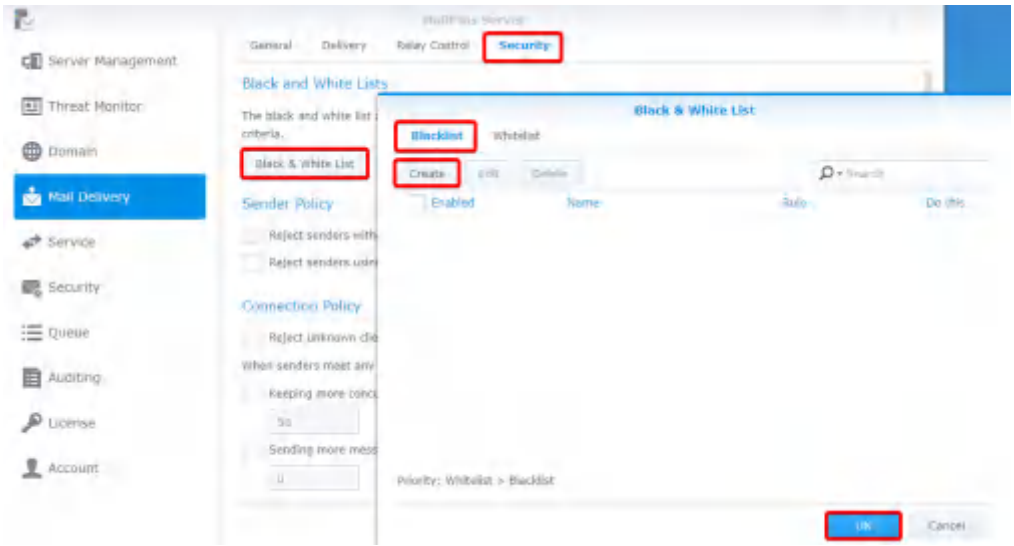
> **注意：**若一封郵件同時符合黑名單與白名單的條件，由於白名單的優先順序高於黑名單，該郵件會被收下。請參考**白名單的說明與限制**。

1 前往**郵件傳送** > **安全性**，按一下**黑 & 白名單**按鈕。

2 在**黑 & 白名單**視窗中，您可以管理**黑名單**和**白名單**，本章節將以**黑名單**為例來說明流程：

- **黑名單：**設定規則來拒絕 / 捨棄符合的郵件訊息。
- **白名單：**設定規則來允許符合的郵件訊息通過。

3 在**黑名單**頁籤中按一下**新增**。



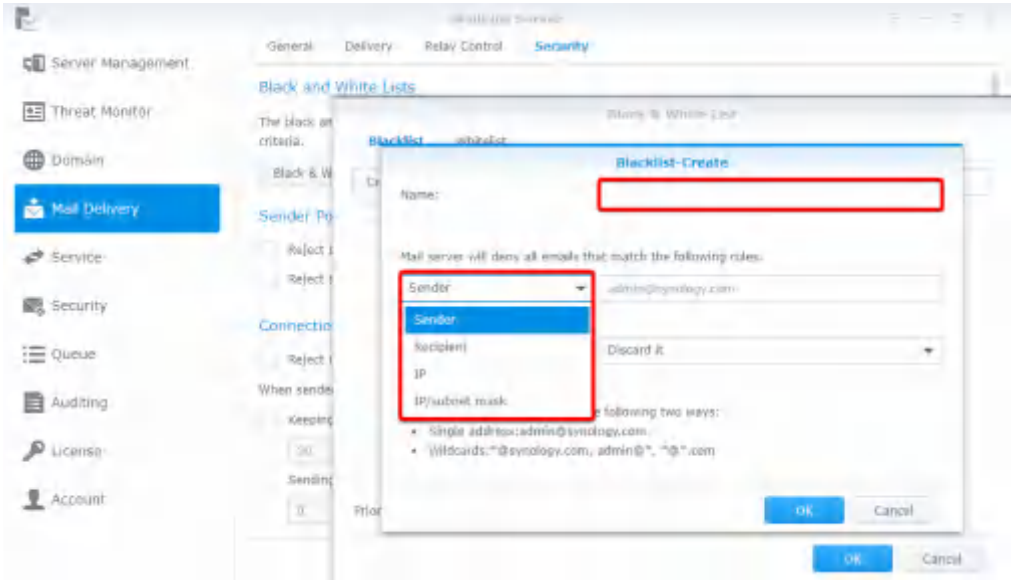
4 在**名稱**欄位中輸入黑 (白) 名單的規則名稱。

5 選擇規則的類別：

- **IP**：當寄件人的 IP 位址符合條件時，系統將執行指定的動作。
- **IP/ 子網路遮罩**：當寄件人的 IP 位址和子網路遮罩符合條件時，系統將執行指定的動作。
- **寄件人**：當寄件人的位址符合條件時，系統將執行指定的動作。
- **收件人**：當收件人的位址符合條件時，系統將執行指定的動作。
- **網域**：在**白名單**中可以看到這個選項。當寄件人的網域符合條件時，系統將執行指定的動作。

注意：

1. **寄件人**的地址是從信件的 **MAIL FROM** 資訊來判斷。
2. **收件人**的地址是從信件的 **RCPT TO** 資訊來判斷。

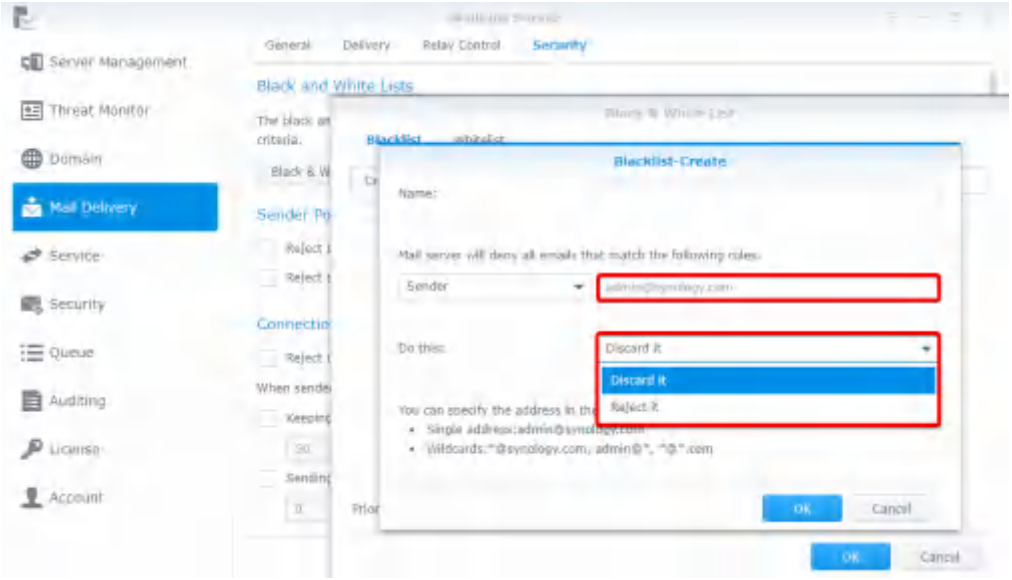


6 為選擇的規則類別輸入條件資訊。請參照浮水印的範例輸入正確的條件格式。寄件人和收件人地址條件支援萬用符號 (*)。

7 從**執行**下拉式選單中選擇符合條件時所採取的動作。

注意：白名單的動作只有無條件收下，因此這個選項不會出現在**白名單**。

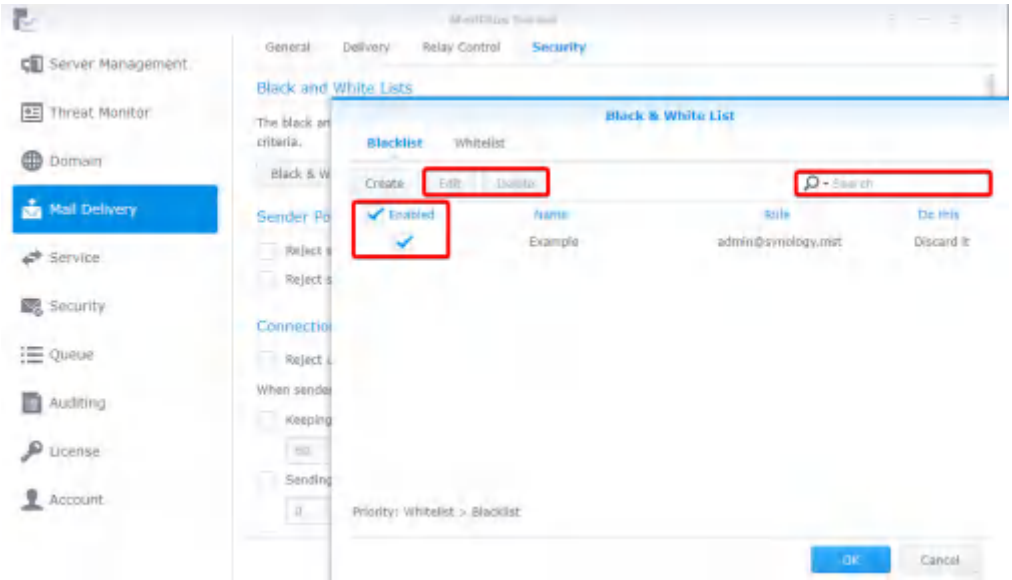
- **拒絕**：若選擇此選項，寄件人會收到他們的郵件被拒絕的通知。
- **捨棄**：若選擇此選項，寄件人不會收到他們的郵件被捨棄的通知。



8 按一下**確定**來完成設定。

編輯及刪除黑白名單

1 在右上角的搜尋欄位中輸入關鍵字來搜尋您想修改的**黑 & 白名單**。
2 您可以勾選**啟動**核取方塊，來選擇啟動或停用該規則。(不需將規則從黑白名單中移除)。
3 若您想要**編輯**或是**刪除**一條特定規則，先選取該規則，再按一下**編輯**或**刪除**按鈕。
4 按一下**確定**來儲存設定。



白名單的說明與限制

白名單的設定除了略過黑名單的檢查外，也會依據不同類型的設定略過 DNSBL、SPF、防毒掃描、DKIM 或 DMARC 的檢測。請參考以下表格以確認是否符合您的需求：

	DNSBL	SPF	防毒掃描	DKIM	DMARC	smtpd_*_restrictions
IP	v	v	v	v	v	v
IP/ 子網路遮罩	v	v		v	v	v
寄件人		v	v			v
收件人		v	v			v
網域		v	v	v	v	v

注意：

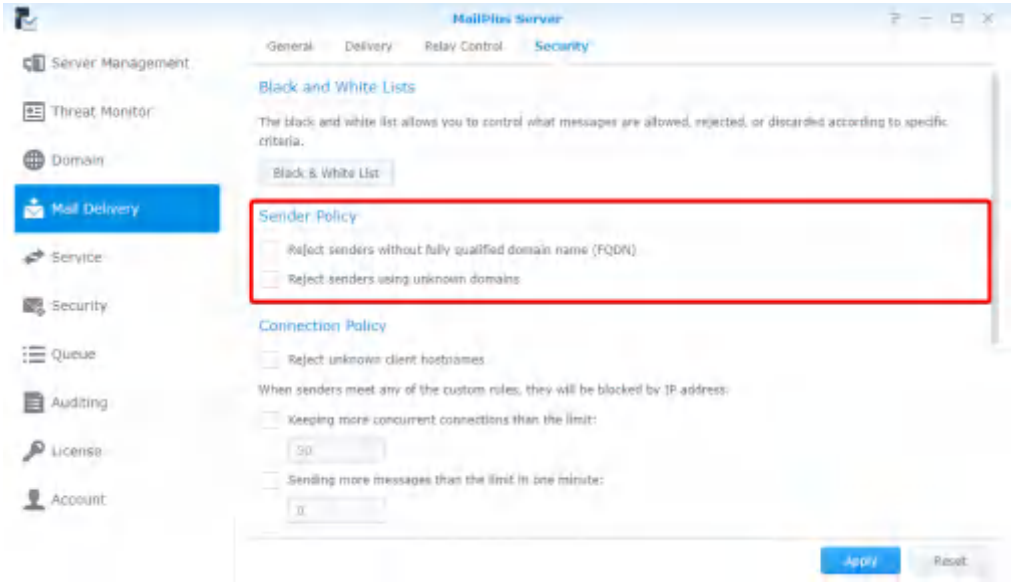
1. 有些檢測項目是白名單無法略過的，若信件無法通過該檢測，則會被退信。例如：若將 *admin@example.com* 加入寄件人的白名單，因寄件人這項條件不被 DNSBL、DKIM 和 DMARC 支援，因此該寄件人發出的信件必須通過 DNSBL、DKIM 和 DMARC 的檢測，才不會被退信。
2. 如果希望略過所有表格中列出的檢測項目，建議您設定白名單規則時將條件設定為 IP 位址。

寄件人規範

1 前往**郵件傳送** > **安全性**。

2 在**寄件人規範**區塊中，設定將郵件退回的條件。規範包含下列內容：

- **拒絕沒有完整網域名稱 (FQDN) 的寄件人**：若寄件人的 **MAIL FROM** 資訊中的網域名稱與 RFC 規範中的 FQDN 格式不符，便會將郵件退回。
- **拒絕使用未知網域的寄件人**：當 MailPlus Server 並非最後收件端，而且寄件人的 **MAIL FROM** 資訊中的網域名稱沒有對應的 DNS A 記錄、MX 記錄，或者有 MX 記錄但格式不正確時，便會將郵件退回。

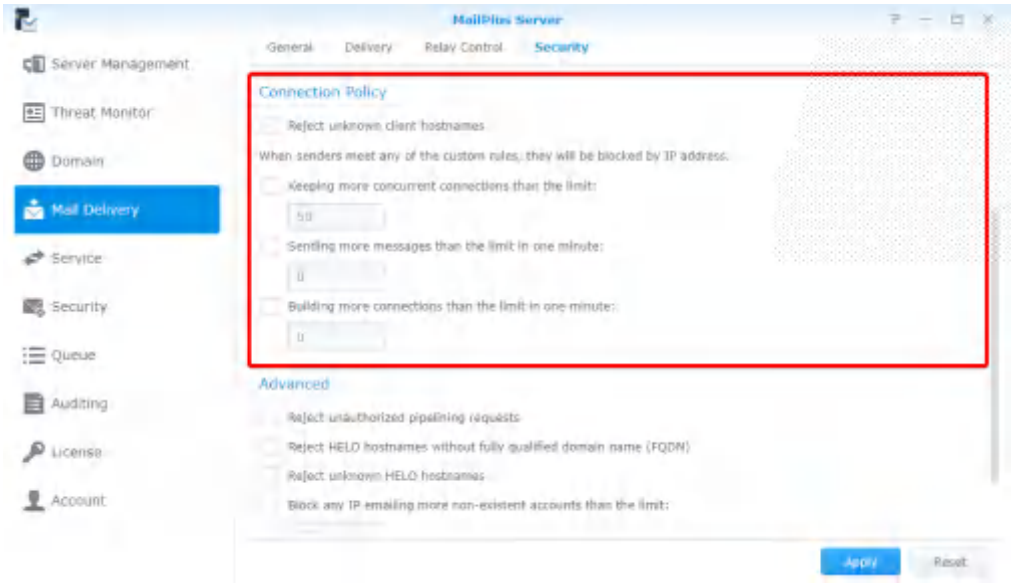


連線規範

1 前往**郵件傳送** > **安全性**。

2 在**連線規範**區塊中，設定當連線到 MailPlus Server 的用戶端出現某些狀況時，拒絕該用戶的連線或封鎖該用戶的 IP 位址。規範包含下列內容：

- **拒絕未知的用戶端主機名稱**：當用戶端的主機名稱或 IP 位址不正確或不存在時，拒絕讓該用戶連線到 MailPlus Server。
- **同一時間連線數量超過上限**：您可以設定單一用戶端主機最大的同時連線數量，若同一 IP 位址同時間連線數量超過此上限值，則之後的連線會被封鎖，直到連線數量低於上限值，才會允許新的連線加入。
- **一分鐘內寄送的郵件訊息數量超過上限**：您可以設定單一用戶端主機在一分鐘內可寄送的最大郵件數量，若同一 IP 位址在一分鐘內寄信數量超過此上限值，則該 IP 寄出的信件會被封鎖一分鐘。
- **一分鐘內建立的連線數量超過上限**：您可以設定單一用戶端主機在一分鐘內的最大連線數量，若同一 IP 位址在一分鐘內連線數量超過此上限值，則該 IP 的連線會被封鎖一分鐘。

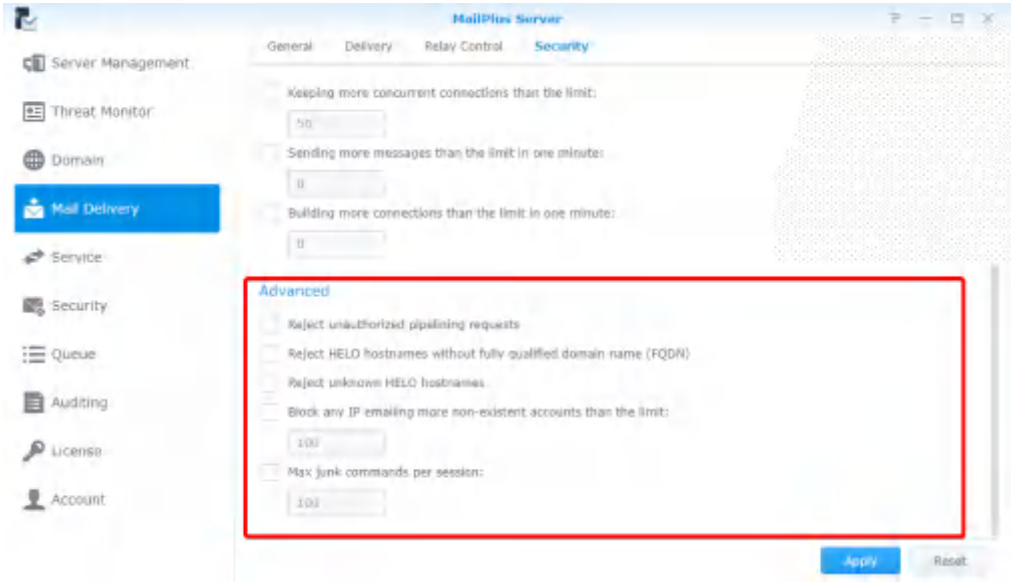


進階設定：

1 前往**郵件傳送** > **安全性**。

2 在**進階設定**區塊中您可以調整郵件傳送階段的安全性設定：

- **拒絕未授權的 pipelining 請求**：拒絕持續發送 SMTP 命令的連線。
- **拒絕沒有完整網域名稱 (FQDN) 的 HELO 主機名稱**：拒絕傳送 HELO/EHLO 命令且不具備完整網域名稱的主機連線。
- **拒絕未知的 HELO 主機名稱**：拒絕傳送 HELO/EHLO 命令且不具備 DNS A 紀錄或 MX 紀錄的主機連線。
- **寄送郵件至不存在的帳號 (數量超過上限) 時，立即封鎖 IP**：若位於同一 IP 位址的用戶在同一天寄送郵件至 MailPlus Server 上不存在的帳號超過設定值，則該用戶的 IP 會被封鎖一天。
- **工作階段內垃圾指令數上限**：若同一次連線內，連線的用戶端發出超過設定值的垃圾指令 (noop、vrfy、etrn 及 rset)，每十個垃圾指令會導致郵件傳送延遲一秒。



郵件轉送

當您希望透過其他伺服器寄送信件，或是替其他伺服器收寄郵件，您可以設定郵件轉送。轉送的過程也提供 SMTP 驗證和加密連線等安全性功能。

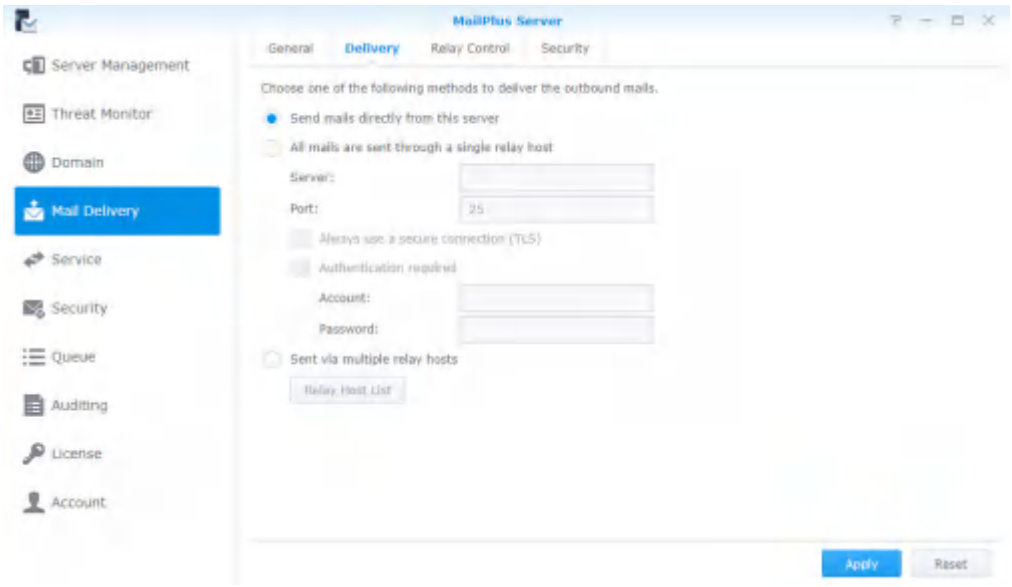
設定傳送控制

在**傳送**頁籤中，您可以設定 MailPlus Server 要透過哪台郵件伺服器來轉送郵件，讓所有寄出的信件經由指定的伺服器寄送。

1 前往**郵件傳送** > **傳送**。

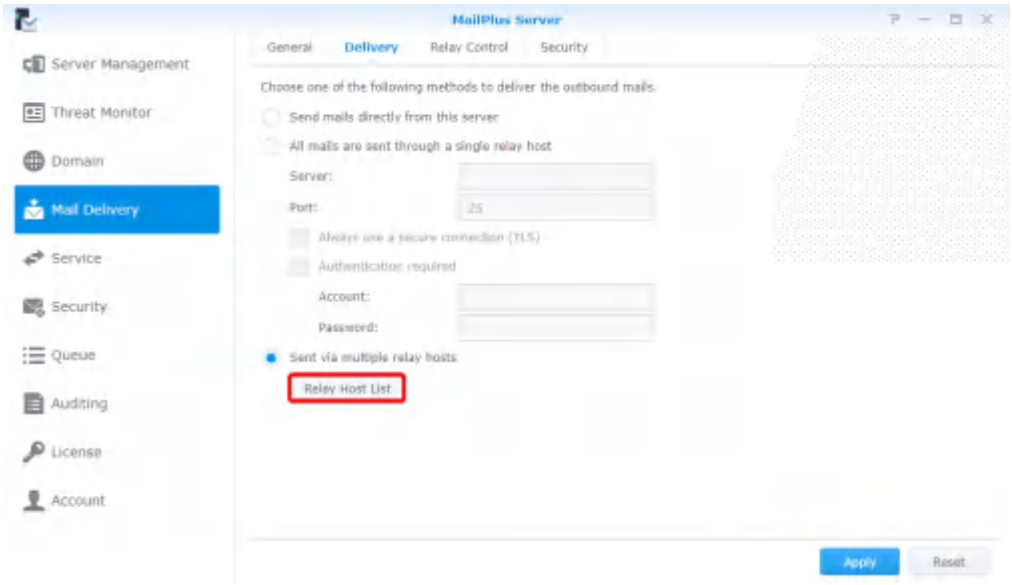
2 選擇規則：

- **直接從此伺服器寄送信件：**所有信件會直接從 MailPlus Server 寄出。
- **所有郵件均透過單一主機寄送信件：**勾選核取方塊來進行下列設定。在**伺服器**欄位中輸入您的轉送伺服器的 IP 位址或是主機名稱，並在**連接埠**欄位中輸入轉送伺服器的連接埠編號。勾選此選項後，您可以修改下列安全性設定：
  - **使用安全連線 (TLS)：**MailPlus Server 將會送出 STARTTLS 來啟動加密連線，若 MailPlus Server 是轉送伺服器，請參考此篇**文章**。MailPlus Server 的 TLS 安全層級預設是 **may**。
  - **需要身份驗證：**若您的轉送伺服器有啟動身分驗證，請在此輸入轉送伺服器的帳號與密碼，以使用該台伺服器轉送郵件。



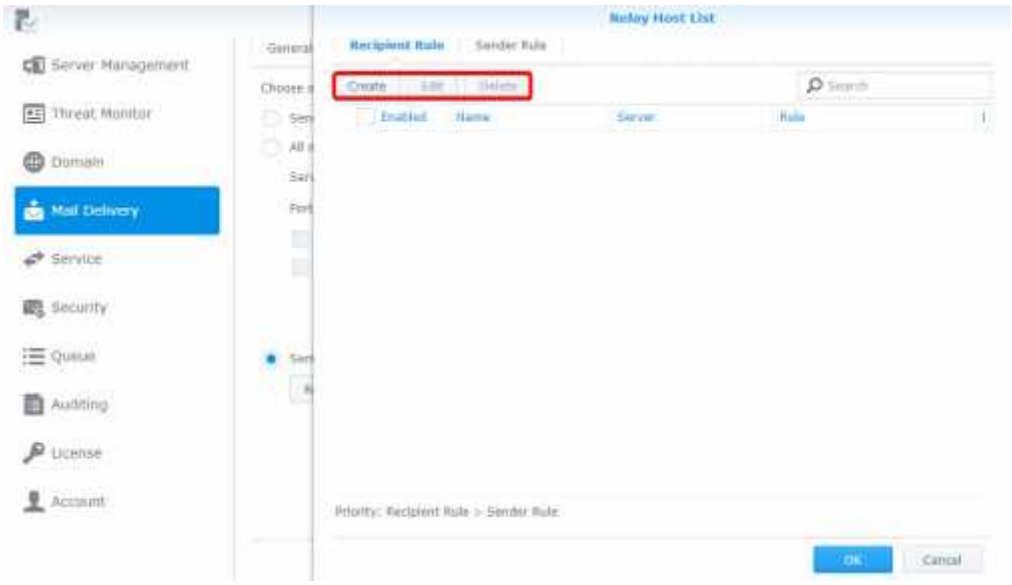
注意：STARTTLS 與 SMTPS 有所不同。目前 MailPlus Server 並沒有提供設定 SMTPS 的頁面，若希望使用 SMTPS，請參考 **wrappermode** 來進行設定。

- **透過多台轉送主機寄送：**符合特定條件的郵件會透過指定的轉送伺服器寄出。勾選此選項後，您可以按一下**轉送伺服器清單**按鈕來修改收件者與寄件者規則。

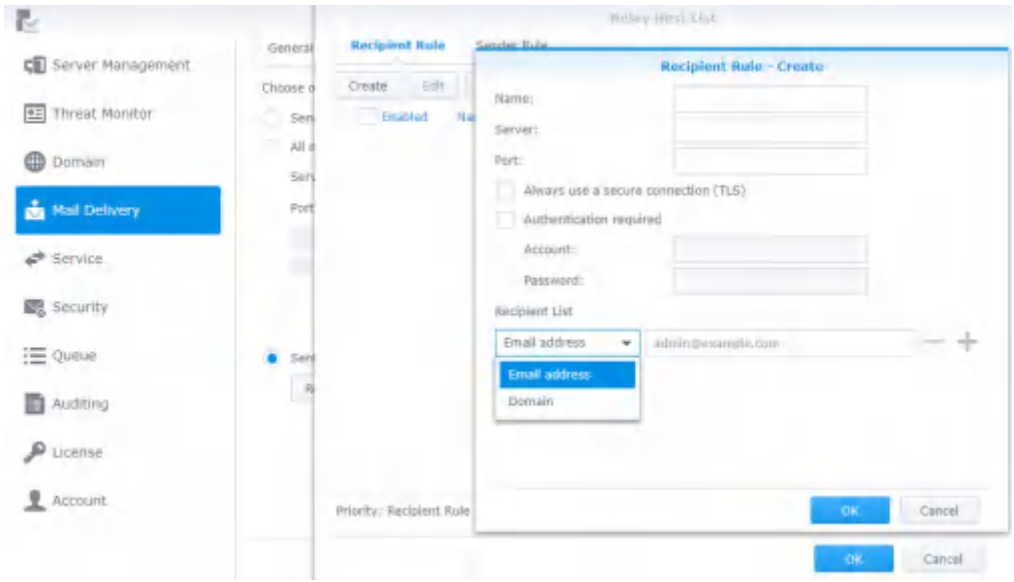


- **收件者規則：**寄送至指定郵件地址或網域的郵件會透過指定的轉送伺服器寄出。收件者規則的優先順序高於寄件者規則。
- **寄件者規則：**從指定地址或網域寄送的郵件會透過指定的轉送伺服器寄出。

1 按一下**新增**、**編輯**或**刪除**按鈕來管理收件者與寄件者規則。



2 輸入規則的名稱、轉送伺服器及連接埠。
3 選擇電子郵件地址或網域來編輯**收件者清單**，讓轉送的郵件被指定的郵件地址或網域收下。
4 按一下**確定**來儲存設定。



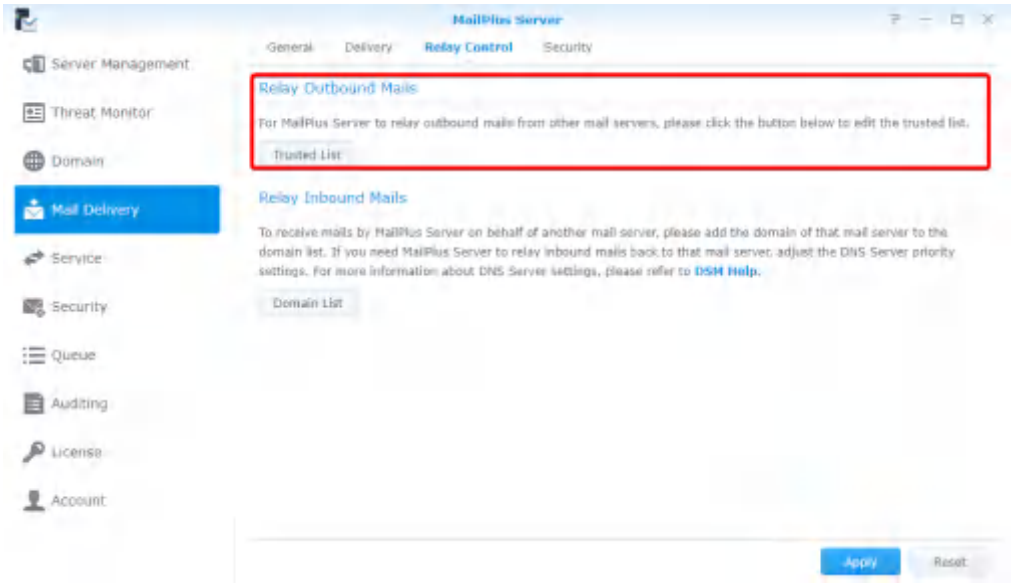
5 按一下**套用**來儲存設定。

設定轉送控制

您可以在**轉送控制**頁籤修改 MailPlus Server 的設定，讓它可以代替多個郵件伺服器收寄信件。

- **替其他郵件伺服器代寄郵件：**

1 前往**郵件傳送** > **轉送控制**。
2 按一下**代寄郵件**區塊的**信任清單**。
3 按一下**新增**，輸入名稱與其他郵件伺服器的 IP 位址或子網路遮罩。



4 按一下**確定**來儲存設定。

> **注意：**
> 若您勾選**一般**頁籤中的**檢查寄件人的郵件地址是否屬於登入帳號**核取方塊，**MailPlus Server** 可能會退回來自**信任名單**的信件。您可以前往**一般**頁籤，勾選**略過檢查由信任的網路寄出的信件寄件人電子郵件位址是否屬於登入帳號**核取方塊來跳過檢查。若您勾選**一般**頁籤中的**來自終端機的區域網路連線不需進行身份驗證**，來自區域網路的信件將不會被 **MailPlus Server** 封鎖。

替其他郵件伺服器代收郵件

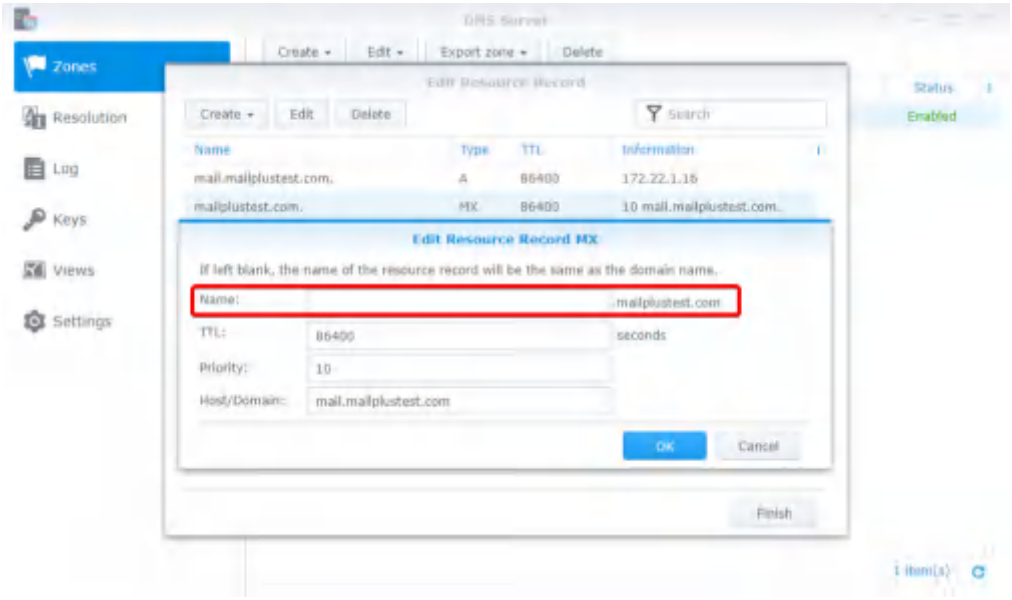
您需要先設定 DNS 紀錄，才能替其他郵件伺服器代收郵件。您可以參考以下步驟，再到**網域清單**來新增郵件伺服器。在此以一個外部伺服器和一個內部伺服器為例。

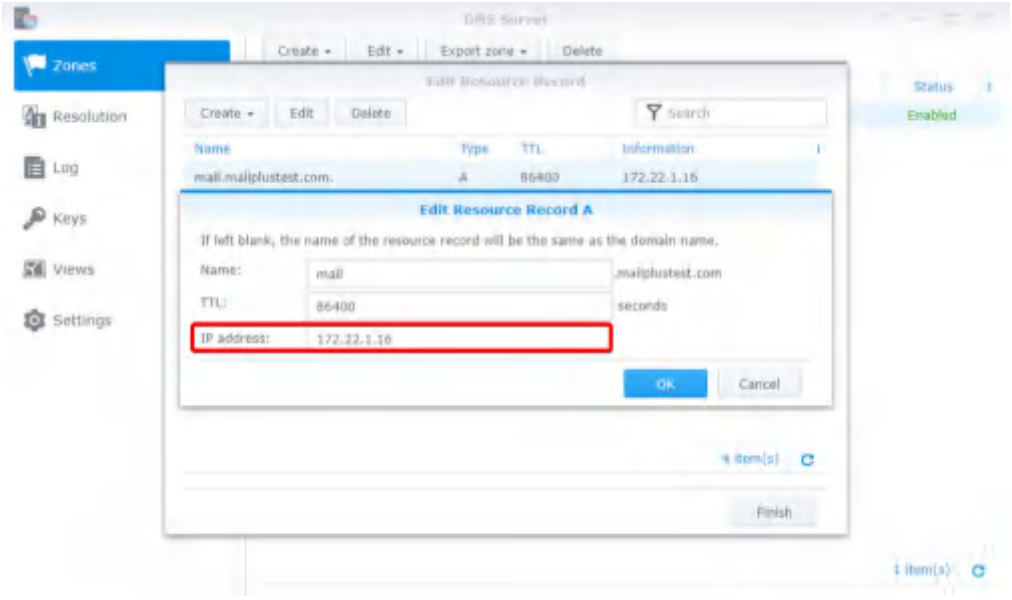
1 為 MailPlus Server 設定外部 DNS 伺服器。在此以 bluehost 為例。

2 登入 bluehost 後，修改以下設定：在外部 DNS 伺服器的 MX 紀錄輸入您的網域名稱，並將 MailPlus Server 的 IP 位址輸入至 A 紀錄。如此一來，其他郵件伺服器就可以依照這些 DNS 紀錄將郵件寄至 MailPlus Server。

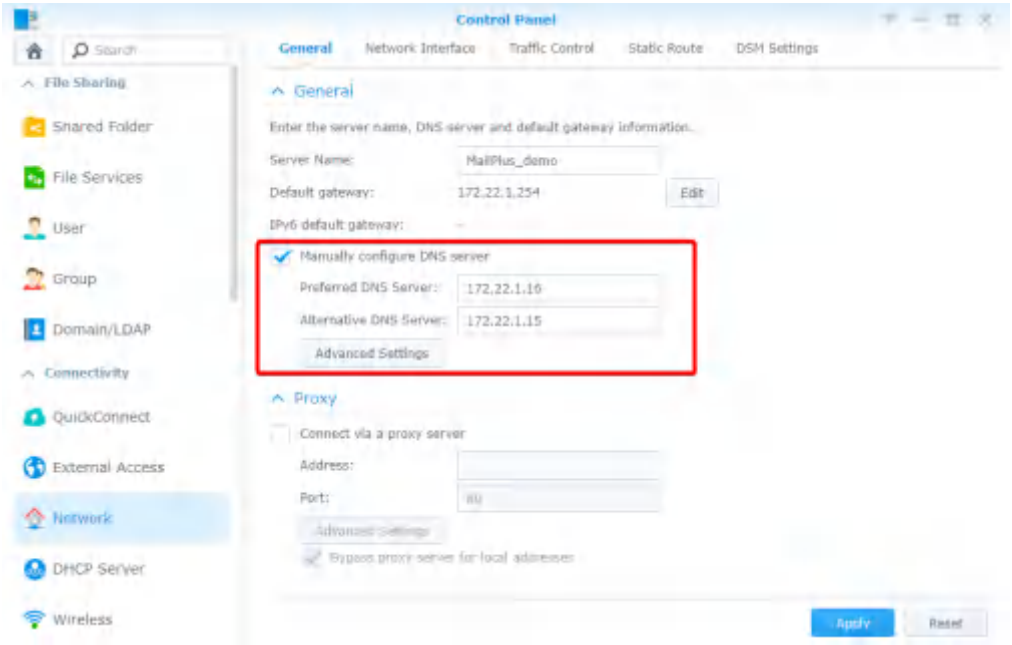
3 為 MailPlus Server 設定 Synology 內部 DNS 伺服器來找到您的主要郵件伺服器。

4 在內部 DNS 伺服器的 MX 紀錄輸入您的網域名稱，並將網域的 IP 位址輸入至 A 紀錄。在內部 DNS 伺服器上的 DNS 紀錄的優先順序必須高於外部 DNS 伺服器上的。

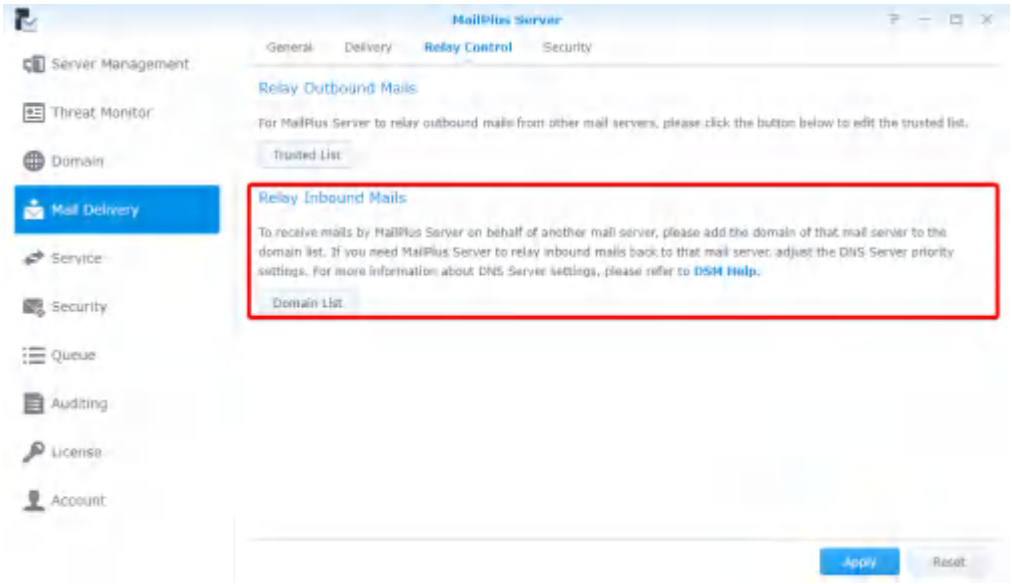




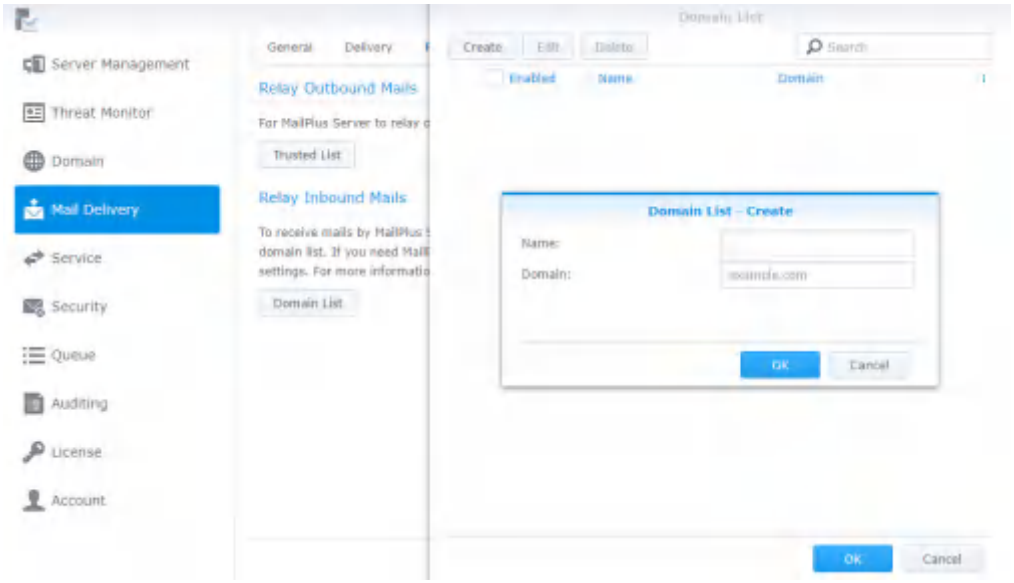
5 前往 **DSM** > **控制台** > **網路** > **一般**，**勾選手動設定網域名稱伺服器 (DNS)** 核取方塊，在**慣用 DNS 伺服器**欄位輸入內部 DNS 伺服器的 IP 位址，並在**替代 DNS 伺服器**欄位輸入外部 DNS 伺服器的 IP 位址，確保 MailPlus Server 的內部與外部連線皆正常運作。**MailPlus Server** 收到郵件後，會檢查兩台 DNS 伺服器的 MX 紀錄，並將郵件寄送至優先順序較高的郵件伺服器。



6 開啟 **MailPlus Server**，前往**郵件傳送** > **轉送控制**，在**代收郵件**區塊按一下**網域清單**按鈕。



7 按一下**新增**按鈕。



8 輸入名稱與網域。

9 按一下**確定**來儲存設定。

注意：

1. 雖然郵件是從內部寄送，您仍應在**安全性**的**垃圾郵件**和**防毒**頁籤進行安全性設定，以避免收到惡意郵件。
2. 由於安全性設定已開啟，您可以在**郵件傳送** > **安全性**中增加白名單，以避免封鎖郵件。
3. 所有伺服器的網路區段必須相同。

網域設定

8

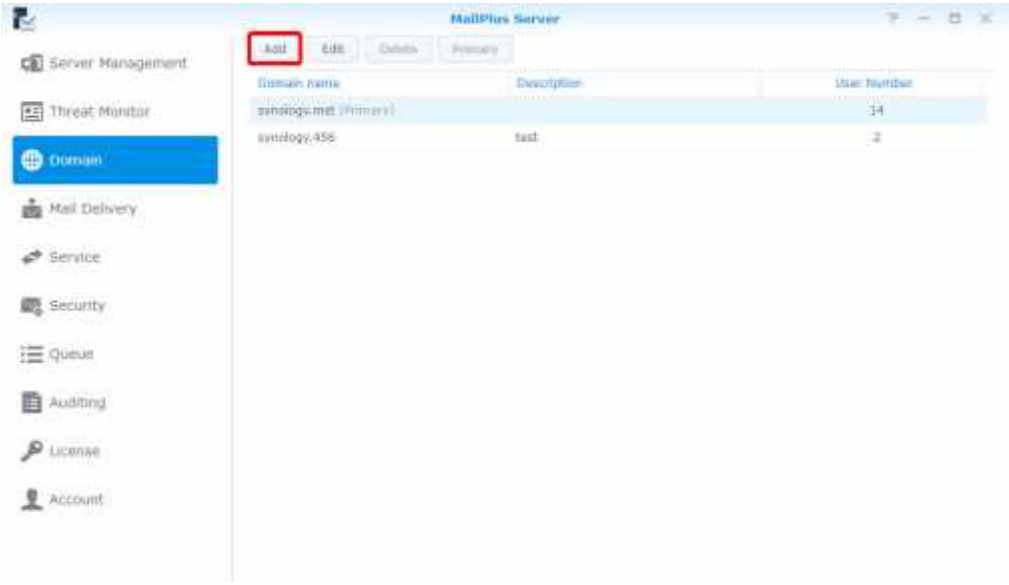
網域

完成數個網域設定後，您可以在單一 MailPlus Server 上架設多個郵件網域，集中管理寄送至您的網域的郵件。您亦可自訂各個網域的別名、自動密件副本、用量限制及免責聲明。

在 MailPlus Server 新增網域

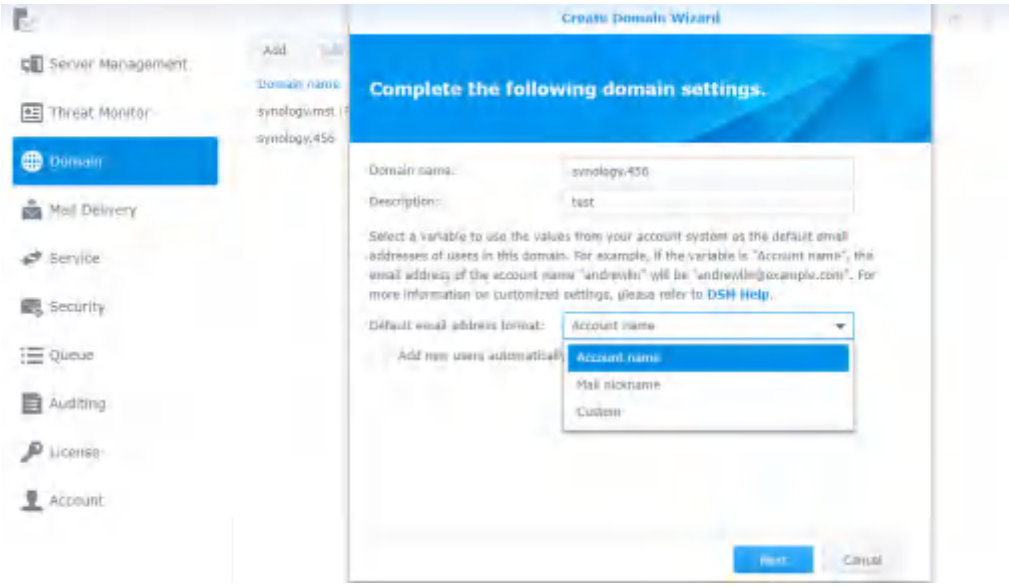
登入 MailPlus Server 並前往**網域**來新增網域。然後，依照指示在下列頁籤完成任務設定。本章節將以 synology.456 為例。

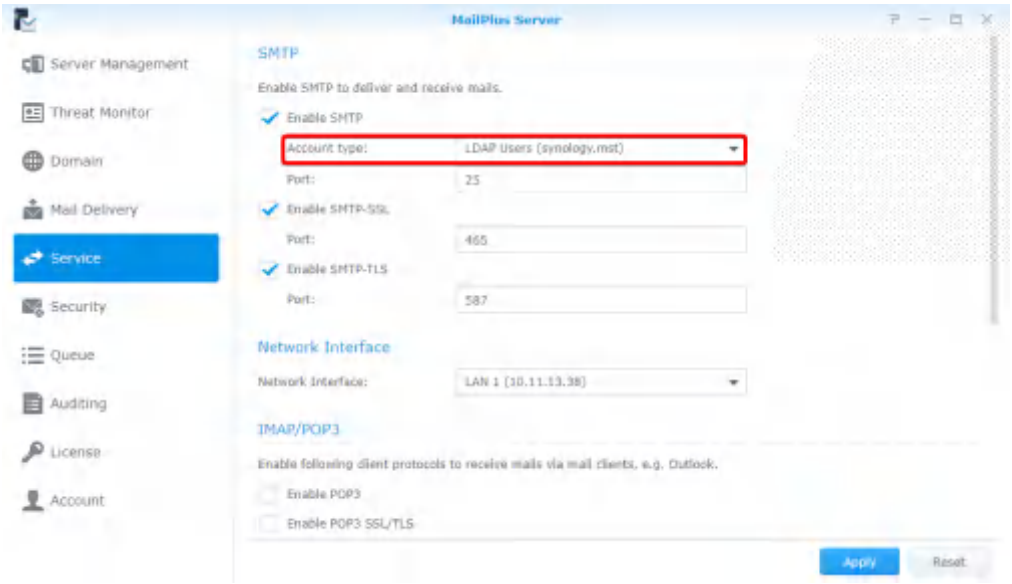
1 前往**網域**，按一下**新增**按鈕。



2 輸入網域名稱 synology.456 和描述。

3 當新增成員至網域時，MailPlus Server 會依照**預設電子郵件位址格式**的設定來從帳號系統抓取資訊。您可以依照您在**服務** > **SMTP** > **帳號類型**設定的帳號類型，選擇**帳號名稱**、**郵件暱稱**、**顯示名稱**或**自訂**。





以下表格列出 MailPlus Server 為不同使用者提供的預設設定：

帳戶類型	預設設定
本地使用者	帳號名稱 郵件暱稱
Synology LDAP 使用者	帳號名稱 郵件暱稱
網域使用者	帳號暱稱 顯示名稱 郵件暱稱

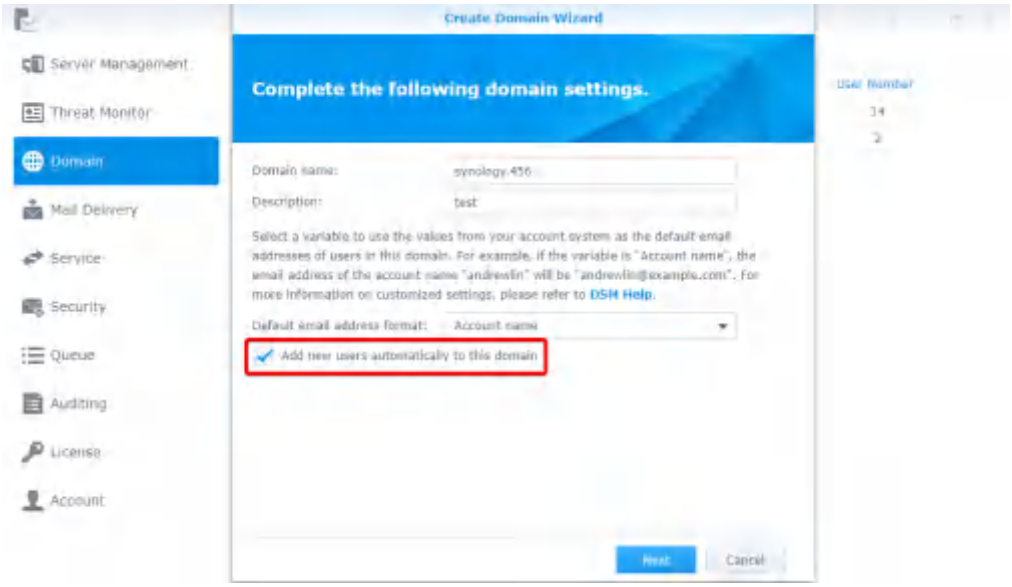
4 除了以上選項外，您也可以選擇**自訂**，在**自訂變數**欄位輸入變數，作為預設電子郵件位址格式。以下表格列出 MailPlus Server 支援的變數：

變數	值
<a>	帳號名稱
<g>	名字
<i>	中間名首字母
<s>	姓氏
<d>	顯示名稱
<m>	郵件暱稱
<xa>	使用帳號名稱的前 x 個字母。例如：若 x = 2，則使用帳號名稱的前兩個字母。
<xs>	使用姓氏的前 x 個字母。例如：若 x = 2，則使用姓氏的前兩個字母。
<xg>	使用名字的前 x 個字母。例如：若 x = 2，則使用名字的前兩個字母。
< 自訂變數 >	您也可以輸入您的帳號系統支援的變數，來抓取對應的值。請參考您的帳號系統使用手冊來了解更多資訊。

MailPlus Server 支援的變數會隨**服務** > **SMTP** 設定的帳號系統有所不同。請參考以下表格來了解更多資訊：

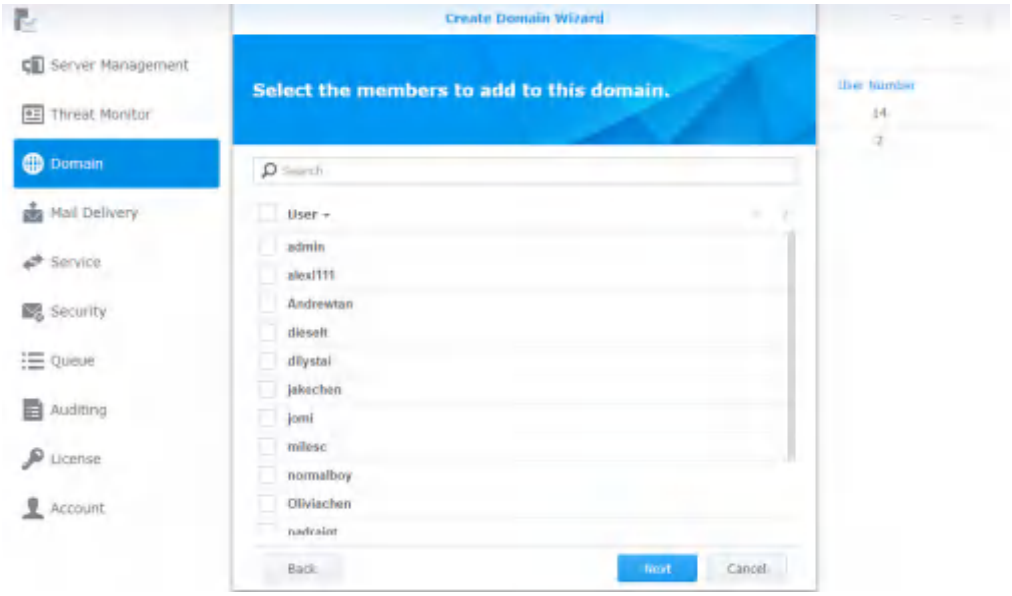
變數	本地使用者	LDAP 使用者	網域使用者
<a>	O	O	O
<g>	X	X	O
<i>	X	X	O
<s>	X	X	O
<d>	X	X	O
<m>	O	O	O
<xa>	O	O	O
<xs>	X	X	O
<xg>	X	X	O
< 自訂變數 >	X	O	O

5 使用者可以勾選**自動將新的使用者加入此網域**核取方塊，自動將新的使用者加入此網域。MailPlus Server 會使用從預設電子郵件位址格式抓取到的資訊，作為使用者的電子郵件位址。



6 設定完成後，按一下**下一步**。

7 將使用者加至此網域，再按一下**下一步**來確認在 synology.456 中的成員。



8 按一下**套用**來套用設定。

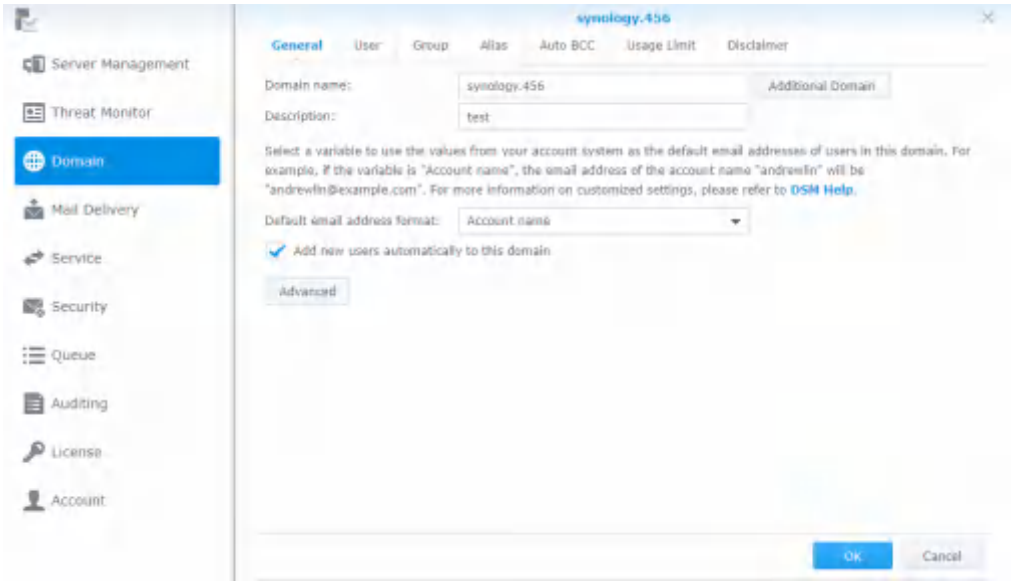
網域管理

MailPlus Server 提供管理員與使用者管理各個網域的設定選項。

- **一般**：您可以編輯網域名稱和網域描述、更改預設電子郵件地址格式、建立其他網域、針對寄出的郵件啟動 DKIM 簽署以及啟動 Catch-all 來接收寄送至不存在或未於該網域啟動之電子郵件位址的郵件。
- **使用者帳號**：您可以將新成員加至網域，並為該網域的使用者設定角色，例如網域管理者和一般使用者。
- **群組帳號**：您可以將群組加至網域，如此群組中的使用者就會擁有同樣的角色設定。
- **別名**：別名是最常見的服務設定之一。您可以為一個或多個收件人建立一組別名，當有信件寄至此別名時，伺服器會自動把信件配送至別名內的所有使用者。別名也可以包含外部的電子郵件位址。
- **自動密件副本**：自動密件副本的設定讓您能根據寄件人、收件人或所有訊息的條件，寄送一份密件副本至指定位址。
- **寄送限制與每日配額**：監測並限制使用者的寄出信件與流量。
- **免責聲明**：自動在寄出的郵件內文最後加上免責聲明。您可以設定套用免責聲明的條件，亦可自訂免責聲明內容，以符合不同的需求。

編輯網域的一般設定

在一般頁籤，您可以編輯網域資訊、修改預設電子郵件位址格式以及自動將新的使用者加入 synology.456。



建立與編輯其他網域

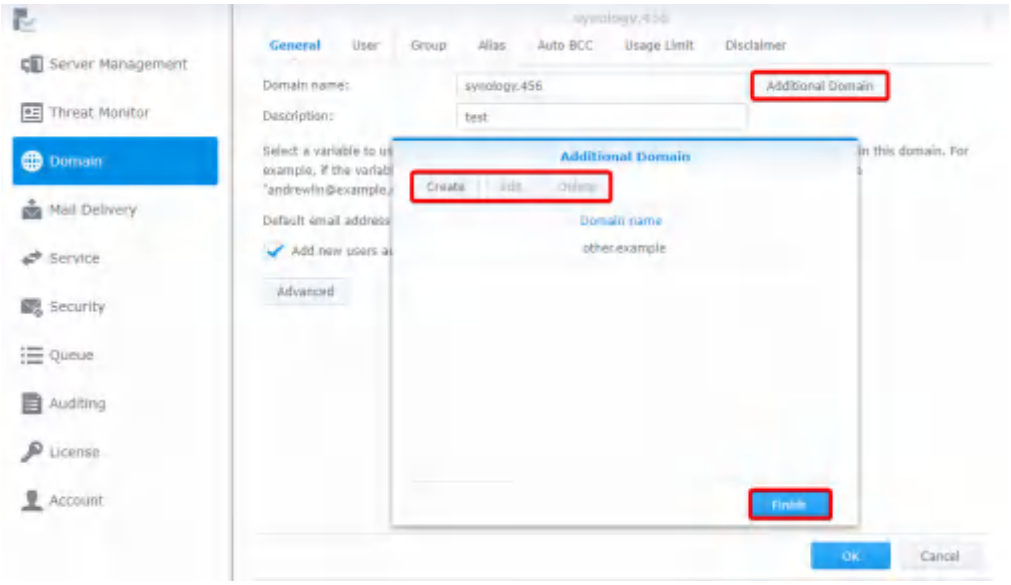
在其他網域中，您可以設定這台主機會額外收下哪些收件人網域名稱的信件。其他網域的設定與 synology.456 相同。

1 前往網域 > synology.456 > 一般，按一其它網域按鈕。

2 按一下新增來增加其他網域。如果您想要編輯或刪除網域，請選取您的目標網域後，再按相對應的按鈕進行操作。

3 在其它網域頁面中，您可以檢視您建立的所有其他網域名稱。以上述範例而言，除了接收 synology.456 網域的信件外，如果其他網域有包含在收件人中，您亦可收到該網域的信件。

4 按一下**完成**來儲存設定。



注意：可能需要相應地調整 DNS 伺服器上的 MX 記錄。

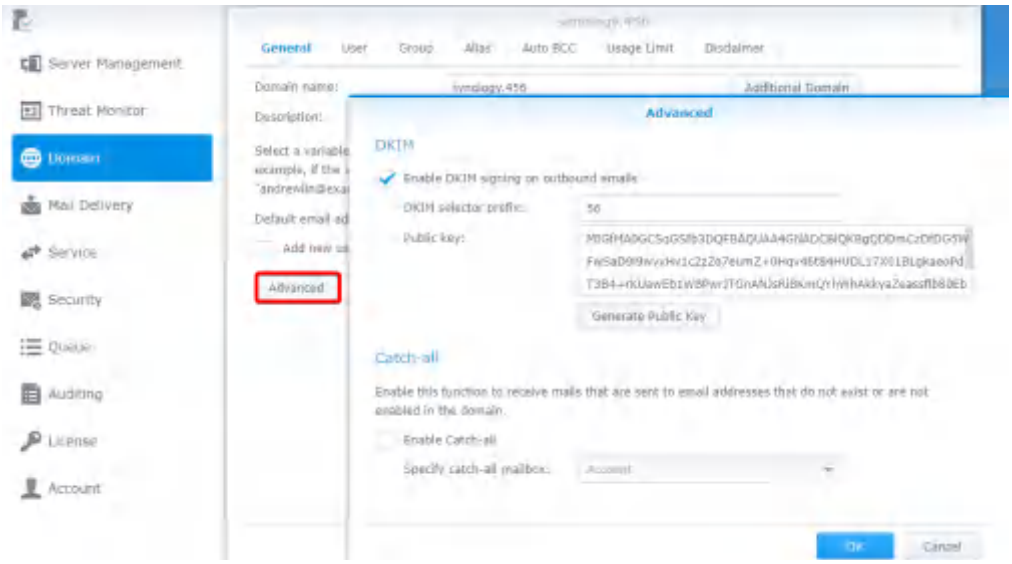
修改進階設定

1 前往**網域** > synology.456 > **編輯** > **一般**，按一下**進階設定**按鈕。

2 在**進階設定**的彈出視窗，您可以修改 synology.456 的 **DKIM** 和 **Catch-all** 設定。

- **DKIM**：您可以啟動 DKIM 驗證，防止信件在傳送途中被篡改，或是身分遭到冒用。
  1 若您想讓收件人信任您所寄出的信，並防止其他人冒用身分，請在 **DKIM** 區塊下勾選**針對寄出的郵件啟動 DKIM 簽署**，並在下方設定 DKIM 簽章：
    - **DKIM 選取器前置字串**：在 DKIM 簽章加上前置字串。您可以輸入一組自訂的 DKIM 選取器前置字串。
    - **公開金鑰**：顯示系統目前使用的公開金鑰內容。若啟動 DKIM 簽署時，系統尚未有公開金鑰與私密金鑰，則系統會自動產生。
  2 按一下**產生公開金鑰**按鈕來產生新的一組公開金鑰與私密金鑰，目前系統產生的金鑰長度為 1024 位元。

    注意：按下**產生公開金鑰**按鈕後，現有的金鑰將會被刪除。



3 按一下**確定**來儲存設定。此外，為確保 DKIM 簽章可以順利被收件端的伺服器驗證，您必須發佈一個 DNS TXT 類別記錄， DKIM 簽署機制才能正常運作：

- **TXT 紀錄值：**v=DKIM1; k=rsa; p=[DKIM 公開金鑰] 舉例來說，若 MailPlus Server 的網域為 example.com，您設定的 **DKIM 選取器前置字串**為 abc，系統產生的公開金鑰為 MIGfMA0GCSqGSIb3DQE，則您必須在 DNS 設定 TXT 類型記錄如下：
  - **TXT 記錄名稱：**abc._domainkey.example.com
  - **TXT 記錄值：**v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQE

- **Catch-all：**啟動 **Catch-all** 來將一個使用者帳號設為 Catch-all 的信箱，以接收寄送至不存在或未於該網域啟動之電子郵件位址的郵件。

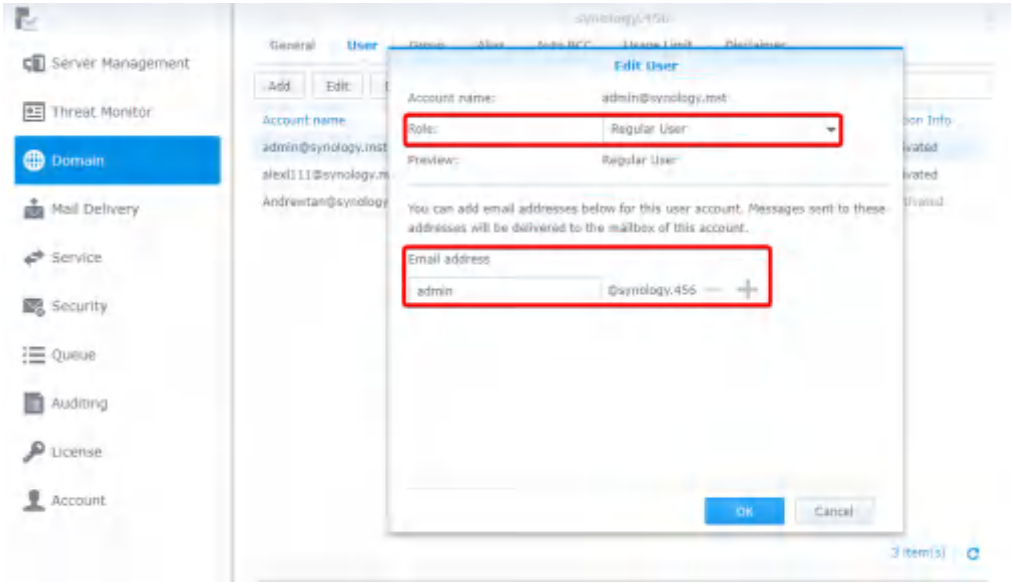
新增使用者帳號至網域

1 前往**網域**，選取 synology.456 並按一下**編輯**。
2 前往**使用者**頁籤，按一下**新增**。
3 選取使用者帳號。
4 確認已選取使用者帳號的電子郵件位址。

編輯與移除使用者帳號

1 前往**網域**，選取 synology.456 並按一下**編輯**。
2 前往**使用者**頁籤，選取一個帳號並按一下**編輯**。
3 在**編輯使用者**視窗中，調整以下設定：

- **角色：**從下拉式選單中選擇角色。
  - **網域管理者：**網域管理者可以管理除了新增 / 刪除網域以外的所有網域設定。
  - **一般使用者：**您可以將沒有權限管理網域的使用者設為一般使用者。
  - **依照群組設定：**依照網域中使用者群組的設定。
- **電子郵件地址：**您可以輸入多個電子郵件地址。寄送至這些電子郵件位址的郵件會被傳送至此帳號的信箱。



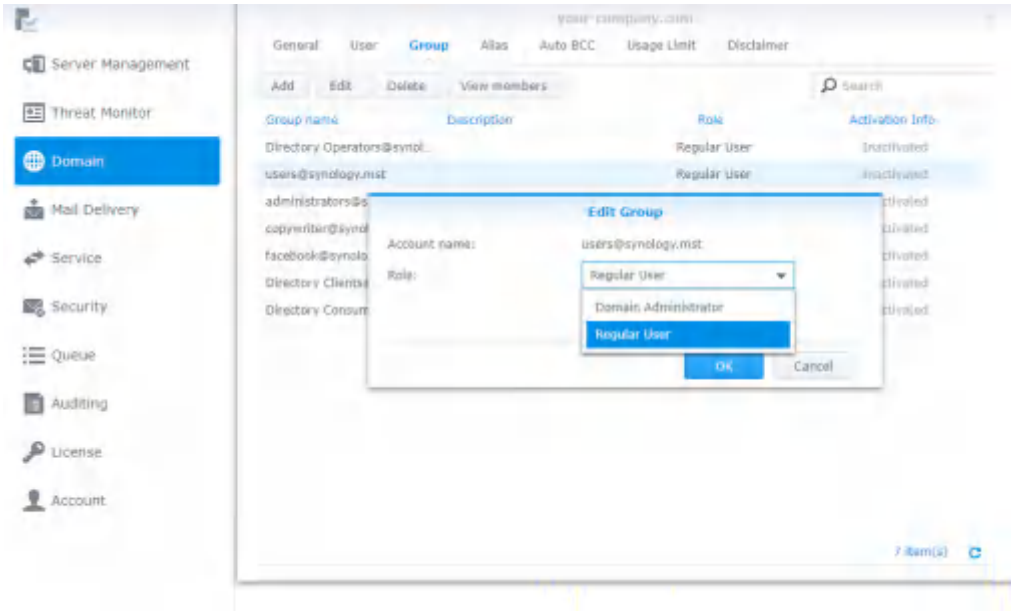
4 若要移除使用者帳號，選擇目標使用者並按一下**刪除**按鈕。

新增群組至網域

1 前往**網域**，選取 synology.456 並按一下**編輯**。
2 前往**群組**頁籤，按一下**新增**。
3 選擇使用者群組，按一下**下一步**。
4 確認成員的電子郵件地址，再按一下**套用**。

編輯與移除群組

1 前往**網域**，選取 synology.456 並按一下**編輯**。
2 前往**群組**頁籤，選取您想要編輯的使用者群組並按一下**編輯**。
3 在**編輯群組**視窗的**角色**下拉式選單選取**網域管理者**，如此在**群組**中的所有使用者就會擁有**網域管理者**的權限。

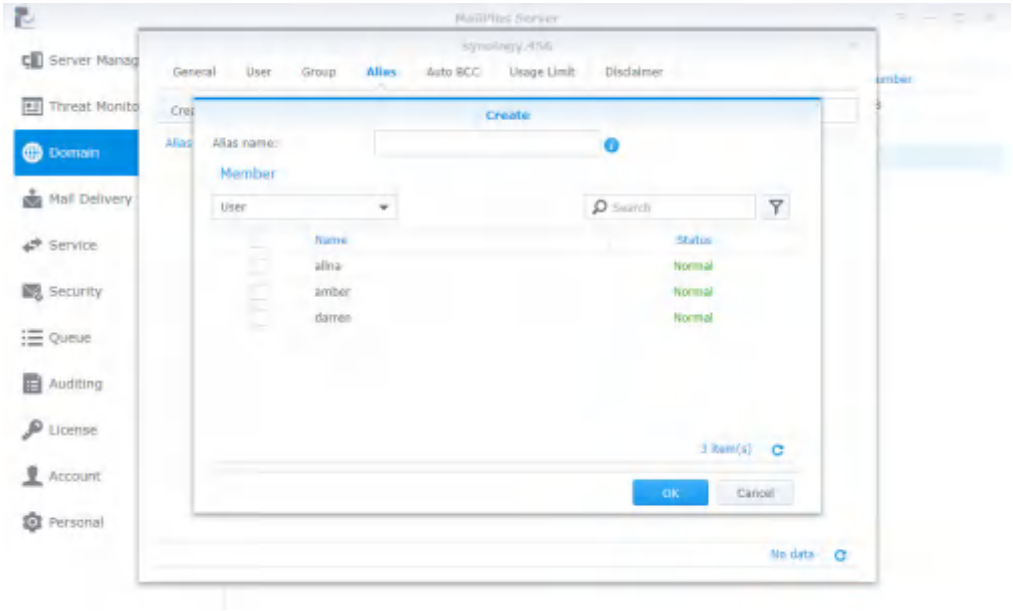


4 您可以選取想要移除的使者群組，再按一下**刪除**按鈕。
5 您可以按一下**檢視成員**按鈕，檢查屬於此群組的使用者是否不在此網域中。

新增別名

您可以新增別名，讓使用者可以透過寄信至單一別名，寄送給多位收件人。

1 前往**網域**，選取 synology.456 並按一下**編輯**。
2 前往**別名**頁籤，按一下**新增**按鈕。
3 在**別名名稱**欄位中輸入別名名稱。
4 按一下下方的下拉式選單來檢視別名、使用者帳號、使用者群組以及外部信箱，並將目標對象加入別名。



5 勾選核取方塊來選擇要加入別名的使用者。
6 您可以同時選擇多種來源的使用者，包含使用者帳號、使用者群組，甚至是其他別名。
7 按一下**確定**來儲存設定。

編輯與刪除別名

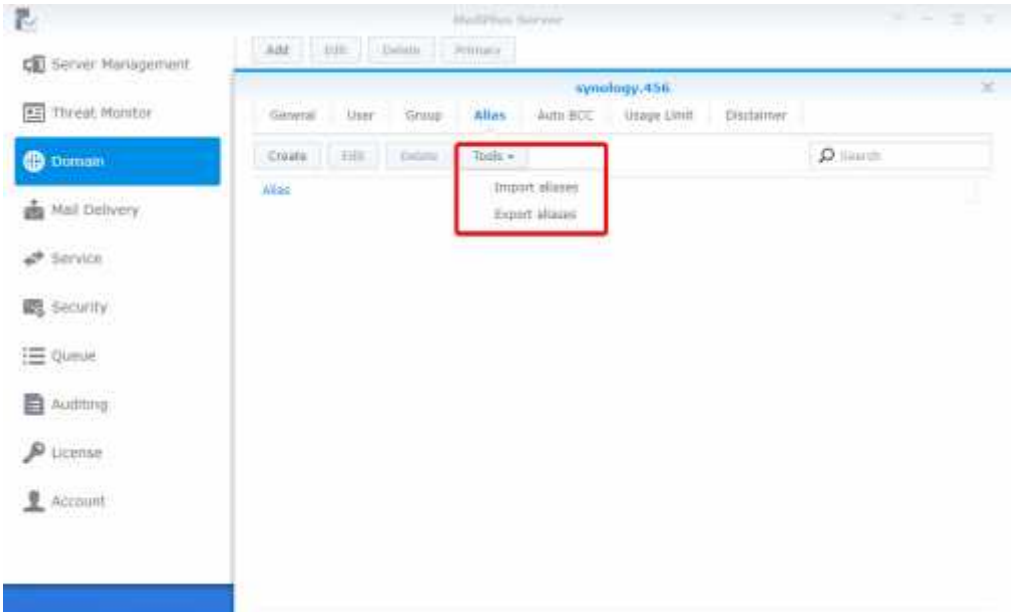
請參考以下步驟來編輯或刪除別名：

1 前往**網域**，選取 synology.456 並按一下**編輯**。
2 前往**別名**選擇您想要修改的別名 (您也可以透過右上角的搜尋欄位來搜尋別名)。
3 按一下**編輯**或**刪除**按鈕。

匯入/匯出別名

若您想匯入 / 匯出既有的別名清單或之前建立的別名清單，請參考以下步驟：

1 前往**網域**，選取 synology.456 並按一下**編輯**。
2 前往**別名**頁籤，按一下**工具**按鈕。
3 選擇匯入或匯出別名：
- **匯入別名**：若匯入的別名與現有的別名重複，該筆別名不會被匯入或更新。
- **匯出別名**：匯出並下載 Post□x 格式的別名檔案。



新增自動密件副本規則

自動密件副本的設定讓您能根據寄件人、收件人或所有訊息的條件，寄送一份密件副本至指定位址。請參考以下步驟來新增副本密件規則：

1 前往**網域**，選取 synology.456 並按一下**編輯**。

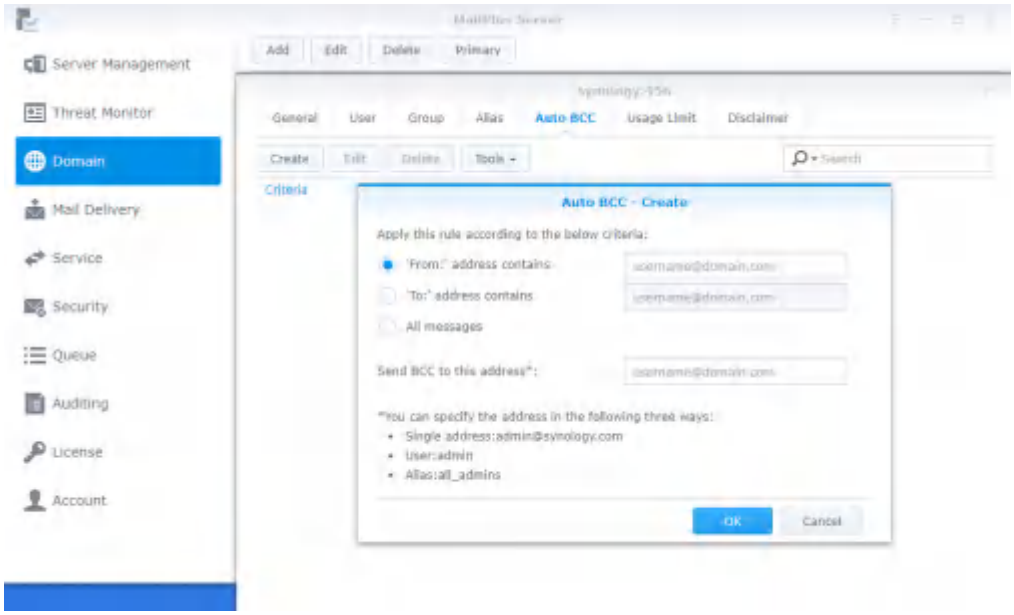
2 前往**自動密件副本**頁籤，按一下**新增**按鈕。

3 輸入自動寄送密件副本的條件：

- **「來自：」地址包含：**若原始信件內容的 MAIL FROM 資訊與此處輸入的資訊相符，便會自動寄送密件副本。
- **「寄至：」地址包含：**若原始信件內容的 RCPT TO 資訊與此處輸入的資訊相符，便會自動寄送密件副本。
- **所有訊息：**除了內部系統發出的通知郵件，其他郵件皆會自動寄送一份密件副本至指定的地址。

4 在**寄送密件副本至此地址 ***欄位中輸入自動寄送密件副本的目標地址。

5 您可以輸入郵件地址、使用者帳號以及別名。



6 按一下**確定**來儲存設定。

編輯與刪除自動密件副本規則

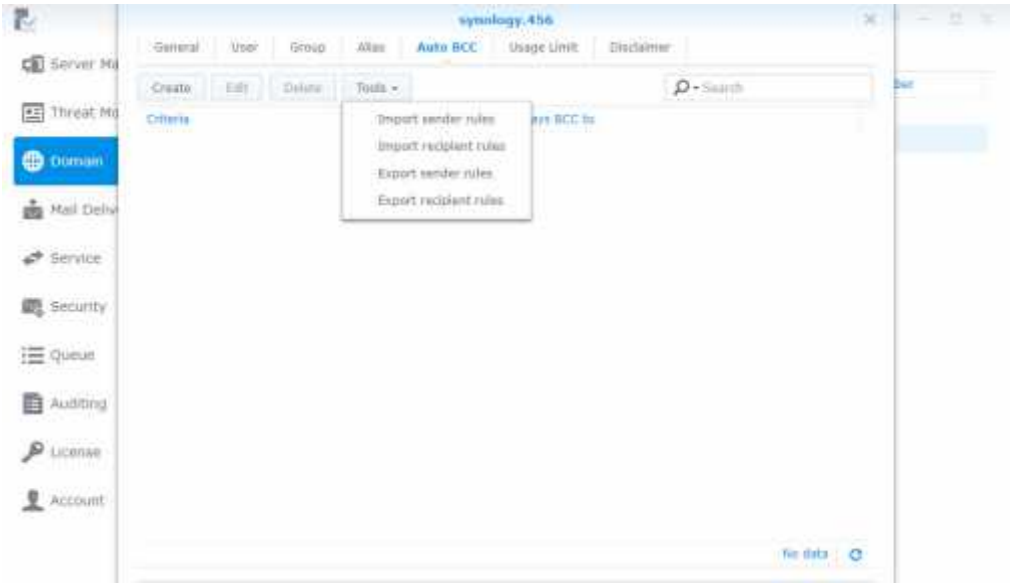
請參考以下步驟來編輯或刪除自動密件副本規則：

1 前往**網域**，選取 synology.456 並按一下**編輯**。
2 前往**自動密件副本**頁籤，選擇您要修改的自動密件副本規則。
3 按一下**編輯**或**刪除**按鈕。

匯入/匯出自動密件副本規則

請參考以下步驟來匯入或匯出自動密件副本規則：

1 前往**網域**，選取 synology.456 並按一下**編輯**。
2 前往**自動密件副本**頁籤，按一下**工具**按鈕。
3 選擇匯入或匯出寄件人或收件人的規則。

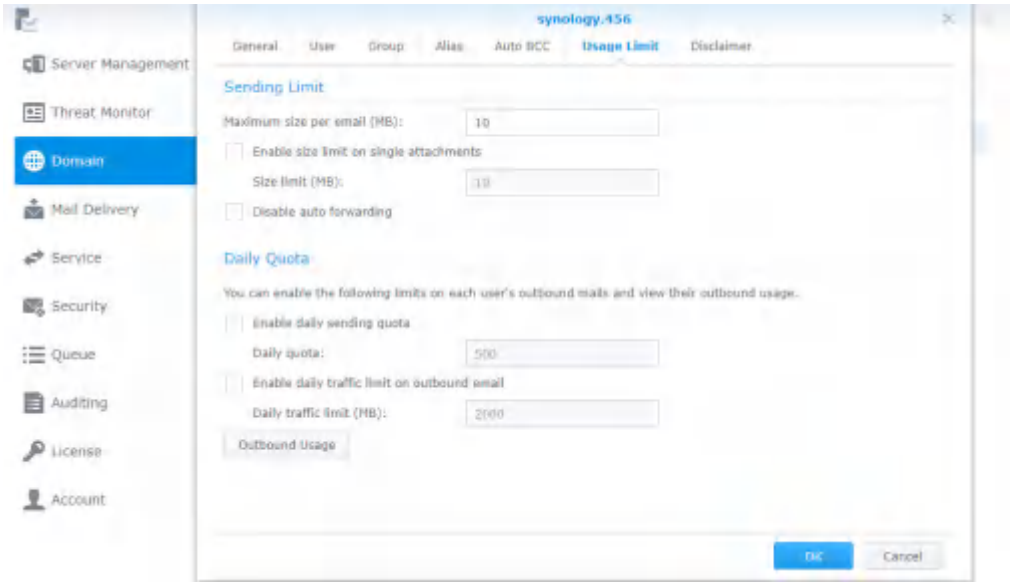


注意：此處沒有提供匯入 / 匯出所有訊息規則的選項，因為這個功能已直接寫在 Post□x 的主要**設定文件**內，請參考 **always bcc**。另外，請確認匯入的檔案為 Post□x 格式。

設定寄送限制與每日配額

1 前往**網域**，選取 synology.456 並按一下**編輯**。
2 前往**用量限制**頁籤。
3 在**寄送限制**區塊下調整以下設定：
- **單一信件大小限制 (MB)：**設定每位使用者每日可寄出郵件訊息的大小。
- **啟動單一附件大小限制：**勾選此選項來指定單一附件的大小限制，並在下方的**大小上限 (MB)** 欄位中輸入上限值。
- **停用自動轉寄：**勾選此選項來停用自動轉寄。

4 在**每日配額**區塊下調整以下設定：
- **啟動每日寄送限額：**勾選此選項來限制每位使用者每日可寄出的郵件訊息數量。
- **啟動每日可寄出的電子郵件流量上限：**勾選此選項來限制每位使用者每日可寄出的郵件訊息大小總和。
- **寄送使用量：**按一下此按鈕來檢視個別使用者的寄送使用量。



寄送使用量

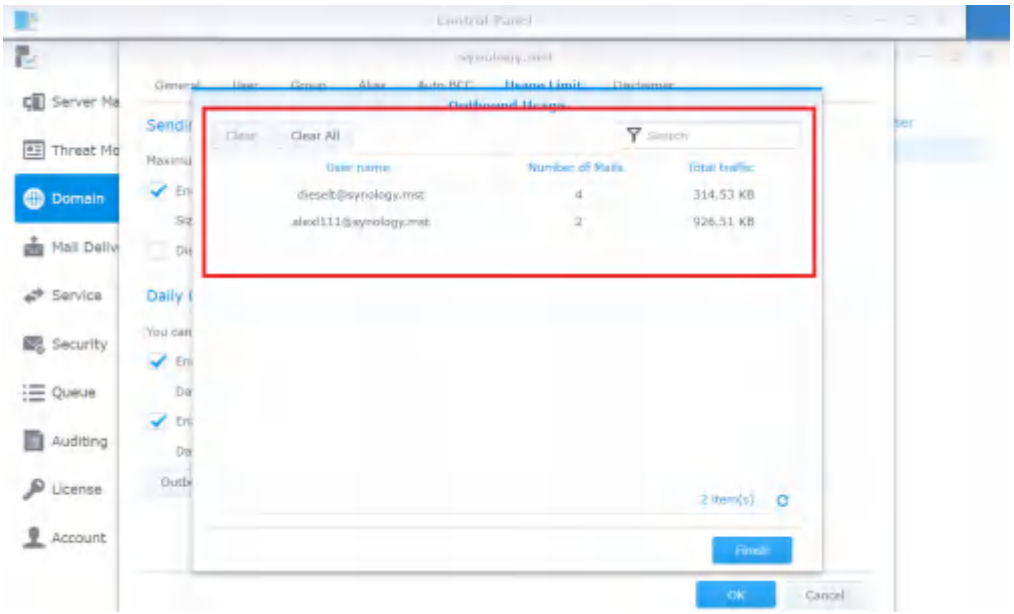
您可以在此檢視郵件訊息寄送總量記錄。若使用者已達到每日寄送限額，可以清除記錄來讓該使用者繼續寄信。

1 前往**網域**，選取 synology.456 並按一下**編輯**。

2 前往**用量限制**頁籤，按一下**寄送使用量**按鈕。

3 從清單中選擇特定使用者。您也可以透過右上角的搜尋欄位來搜尋使用者。

4 按一下**清除**按鈕來清除使用者的寄送使用量紀錄，並讓該使用者的使用量重新計算。按一下**全部清除**按鈕，則會清除全部使用者的使用量紀錄。



5 按一下**完成**來完成設定。

新增免責聲明

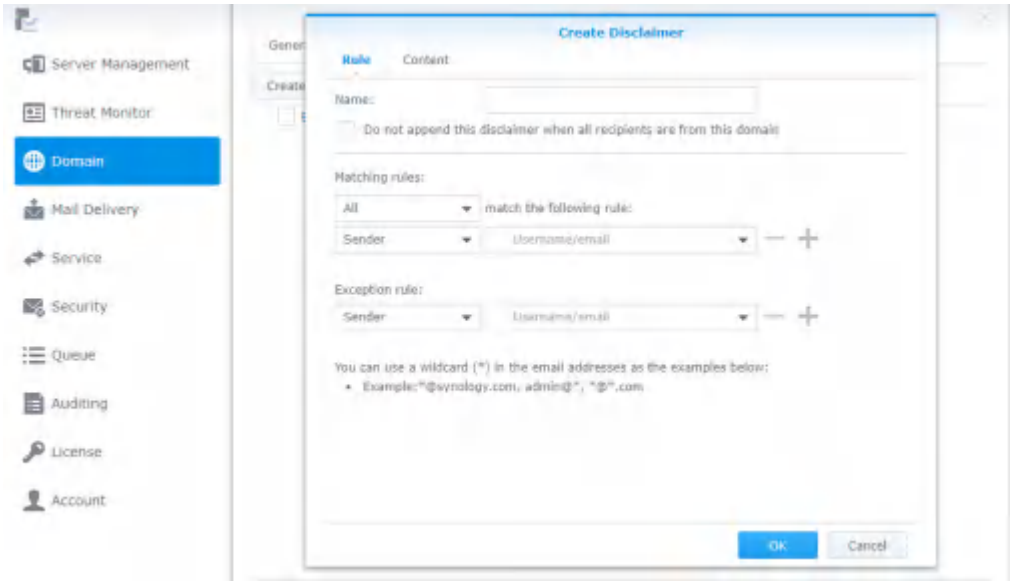
免責聲明功能可以自動幫使用者在寄出的信件尾端加上自訂的文字資訊。請參考以下步驟來新增免責聲明：

> **注意：**您可以擁有多個免責聲明和規則，但是一封信只能套用一個免責聲明，請參考**編輯**與**刪除**免責聲明。

1 前往**網域**，選取 synology.456 並按一下**編輯**。

2 前往**免責聲明**頁籤，按一下**新增**按鈕。

3 前往**新增免責聲明**視窗中的**規則**頁籤。



4 在**名稱**欄位中輸入免責聲明的名稱。

5 選擇是否勾選**當所有收件人皆來自此網域時，不附加此免責聲明**核取方塊：

- 當伺服器判斷信件為內部信件 (寄給其它內部使用者) 時，就不會加上免責聲明。

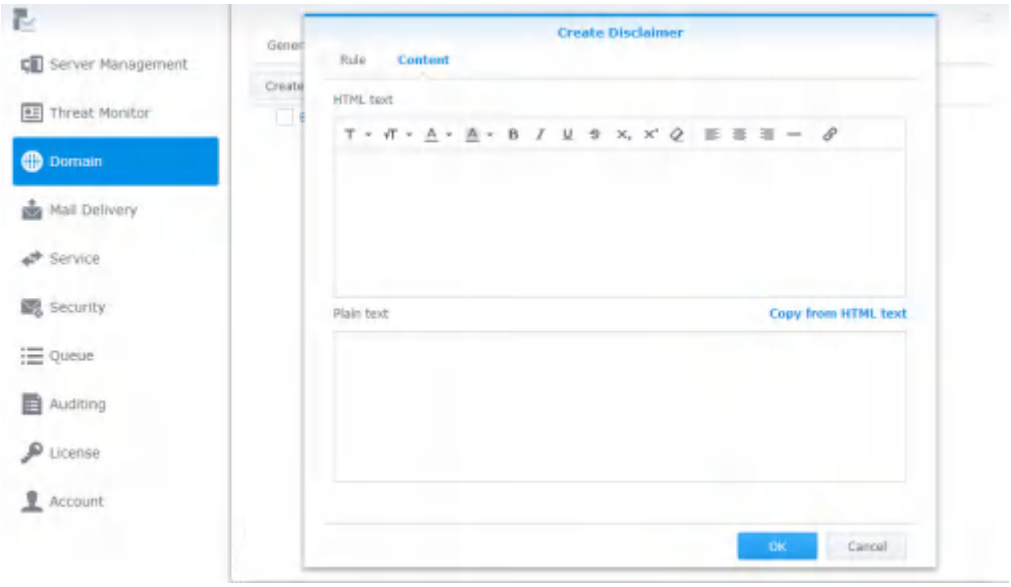
  > **注意：**若有任一收件人不是內部使用者，則仍會加上這則免責聲明。

6 透過以下選項設定條件：

- **比對規則：**包含**全部**、**任一項**兩個選項。若選取**全部**，則必須符合下列全數規則，才會加上免責聲明。若選取**任一項**，則只要符合其中一條規則，就會加上免責聲明。
- **符合下列規則：**請選擇您要根據**收件人**還是**寄件人**來加上免責聲明，此設定支援萬用字元 (*)。
- **例外規則**優先於**比對規則**，若**例外規則**成立，則即使符合**比對規則**也不會加上免責聲明。

7 按一下 **+** 按鈕來新增多個**比對規則**或**例外規則**，再按一下 **-** 按鈕來移除規則。

8 規則設定完成後，前往**內容**頁籤來編輯您的 **HTML 文字**及**純文字**內容，確保在客戶端能夠正確顯示。請參考此篇文章來了解更多資訊。



9 若您希望**純文字**與 **HTML 文字**內容相同，您可以直接按一下**從 HTML 文字複製**，來將 **HTML 文字**編輯器中的內容複製到**純文字**編輯器，並且移除所有 HTML 標籤。按一下**確定**來完成。

編輯與刪除免責聲明

因為免責聲明會依照優先順序套用，除了編輯與刪除免責聲明以外，您也可以在此調整優先順序設定。請參考以下步驟：

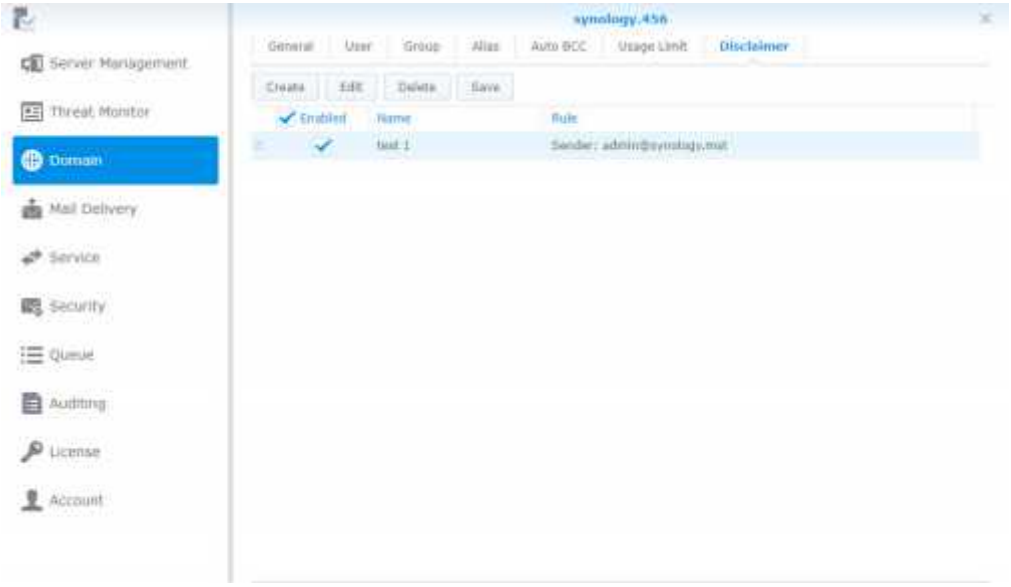
> **注意：**系統會由上到下判斷免責聲明的條件是否符合，若符合條件，這則免責聲明將被套用，條件檢查也會結束。

1 前往**網域**，選取 synology.456 並按一下**編輯**。

2 前往**免責聲明**頁籤。排序較高的免責聲明比較低者有更高的優先套用順序。若要更改優先順序，選擇目標再拖拉至合適的位置。

3 選擇是否啟動免責聲明規則。

4 選擇您要修改的免責聲明規則，再按一下**編輯**或**刪除**按鈕。



5 按一下**儲存**來套用設定。

安全性設定

MailPlus Server 的安全性功能涵蓋以下四大類別：**垃圾郵件**、**防毒**、**認證**及**內容掃描**。您可以調整設定以強化特定類別的防禦。

垃圾郵件

在阻檔垃圾郵件的機制方面，MailPlus Server 利用垃圾郵件的寄件特性，提供判定的準則來標示或拒絕遞送垃圾郵件。

- **Anti-Spam**：使用 SpamAssassin 作為引擎，提供使用者彈性的判定規則，並透過自動學習及回報機制，讓 MailPlus Server 依照您的使用環境阻檔垃圾郵件，達到最好的效果。
- **Postscreen**：根據垃圾郵件伺服器的寄件人特性以及公認的黑名單來拒絕服務垃圾郵件伺服器，減少收到垃圾郵件的機率。
- **灰名單**：同樣根據垃圾郵件伺服器的寄件人特性所制定的反制功能。由於使用灰名單將會影響郵件寄送速度，啟動此功能前請完整了解其機制。

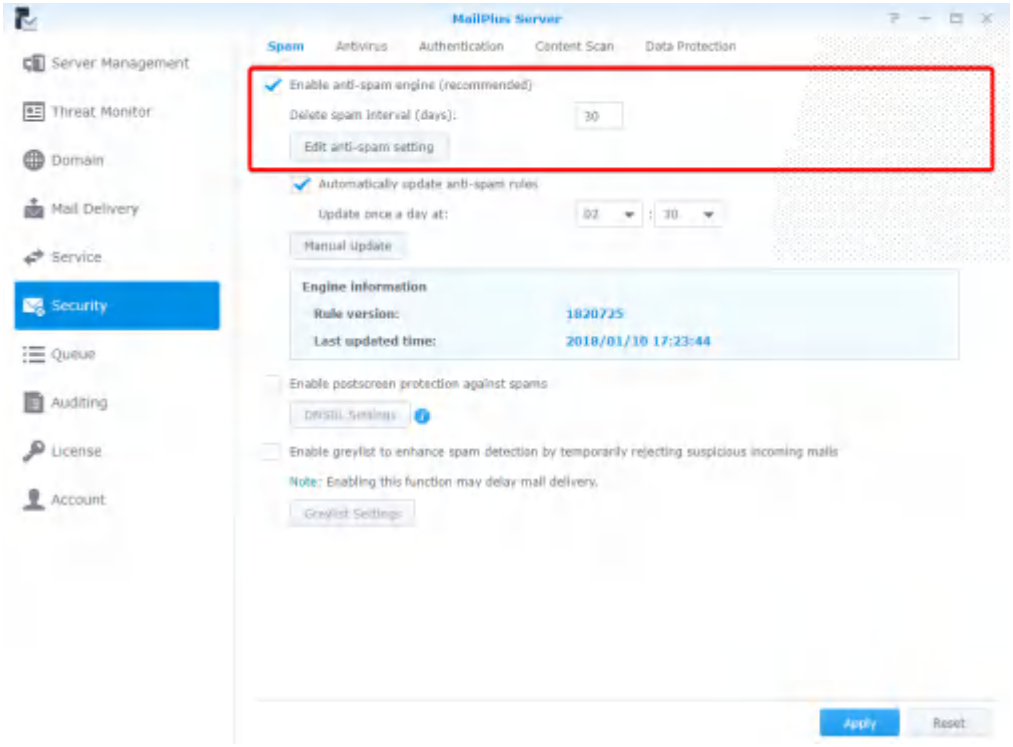
啟動 Anti-Spam

MailPlus Server 目前使用 SpamAssassin 作為 Anti-Spam 引擎。SpamAssassin 引擎內建的垃圾郵件偵測規則可利用垃圾郵件門檻分數來過濾垃圾郵件。若一信件符合您所設定的偵測規則時，會加上該規則所對應的分數，當累加總分超過垃圾郵件門檻分數時，此信件就會被標記為垃圾郵件。您可以使用 SpamAssassin 內建的規則，直接啟動 Anti-Spam。請參考以下步驟來啟動 Anti-Spam：

1 前往**安全性** > **垃圾郵件**來調整以下設定：

- **啟動 anti-spam 引擎**：勾選此選項來啟動 Anti-Spam。請參考 **Anti-Anti-Spam 一般設定**、**更新 Anti-Spam 規則**、**自定垃圾郵件過濾**、**自動學習與垃圾郵件回報設定**來取得更多資訊。
- **垃圾郵件清理週期 (日)**：被標示為垃圾郵件的信件會被放入垃圾信件匣，系統會自動定期清理垃圾郵件，因此收到的垃圾郵件在超過一段時間後會自動被刪除。您可以在此設定時間間隔，預設值為 30 天。

注意：即使沒有啟動 Anti-Spam，仍會定期清理垃圾郵件。

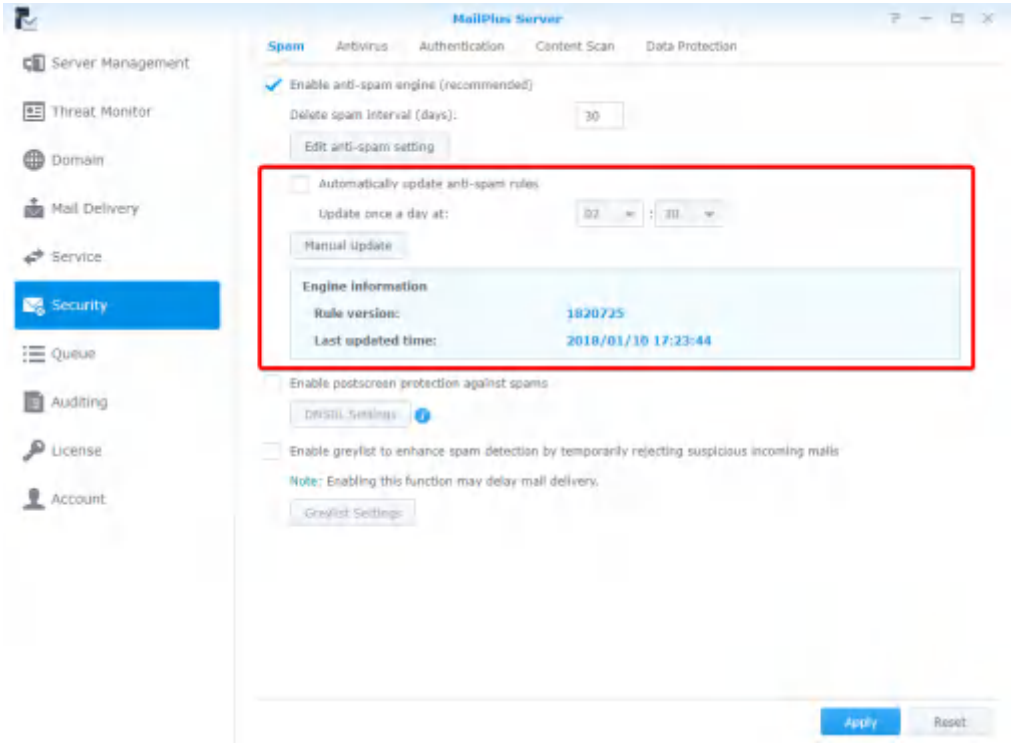


更新 Anti-Spam 規則

Anti-Spam 偵測垃圾郵件的規則來自 SpamAssassin 的資料庫，您需要定期更新規則來確保垃圾郵件防護功能保持在最新狀態。請參考以下步驟來更新 Anti-Spam 規則：

1 前往**安全性** > **垃圾郵件**來調整以下設定：

- **自動更新 anti-spam 規則**：勾選此選項來設定更新排程，系統會每日定時從 SpamAssassin 官網下載最新的垃圾郵件偵測規則。
- **每日更新時間**：設定每日下載規則的時間。
- **手動更新**：按一下**手動更新**按鈕來立即更新垃圾郵件偵測規則。按鈕下方的資訊欄位顯示最後一次更新的時間，以及目前垃圾郵件偵測規則的版本。



Anti-Spam 一般設定

Anti-Spam 功能提供許多自訂設定選項，您可以在此按照您的環境調整您的 Anti-Spam 引擎。請參考以下步驟來編輯 **Anti-Spam** 的一般設定：

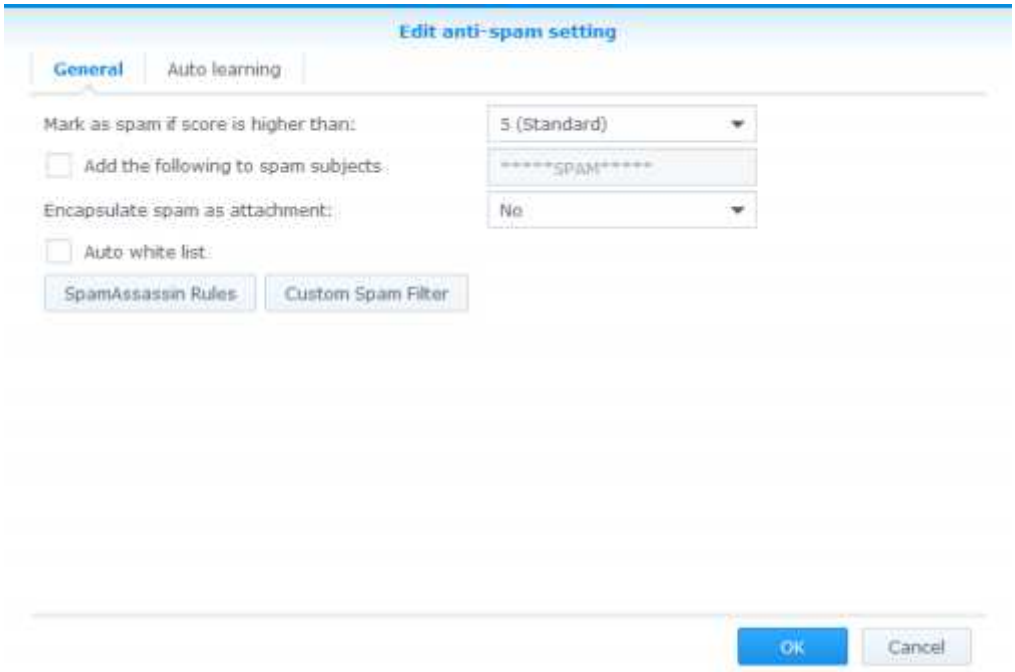
1 前往**安全性** > **垃圾郵件**，按一下**編輯 anti-spam 設定**按鈕。

2 在**編輯 anti-spam 設定**視窗中的**一般**頁籤中，您可以調整以下設定：

- **分數高於此數字則標記為垃圾郵件**：選擇一個垃圾郵件門檻分數。當信件的累加總分超過此數值時，就會被標記為垃圾郵件。
- **在垃圾郵件主旨加入下列內容**：當信件的分數超過門檻而被標記為垃圾郵件時，您可以選擇是否在信件主旨前加入特定內容，來提示使用者。勾選**在垃圾郵件主旨加入下列內容**核取方塊，並修改預設標示。
- **將垃圾郵件封裝為附件**：被判定為垃圾郵件之信件將會被封裝為附件，寄送給收件人。下拉式選單中包含：

選項	描述
否	不做處理，直接寄送給收件人。
是	將垃圾郵件封裝為附件，寄送給收件人。
是，僅為純文字	將垃圾郵件轉為純文字格式郵件，以避開網頁臭蟲或惡意指令碼，再封裝寄給收件人。.

- **自動白名單**：此功能會讓系統分析收寄的郵件通訊，來判斷外部寄件人和系統中的使用者是否有過信件往來，以避免將信件誤判為垃圾郵件。



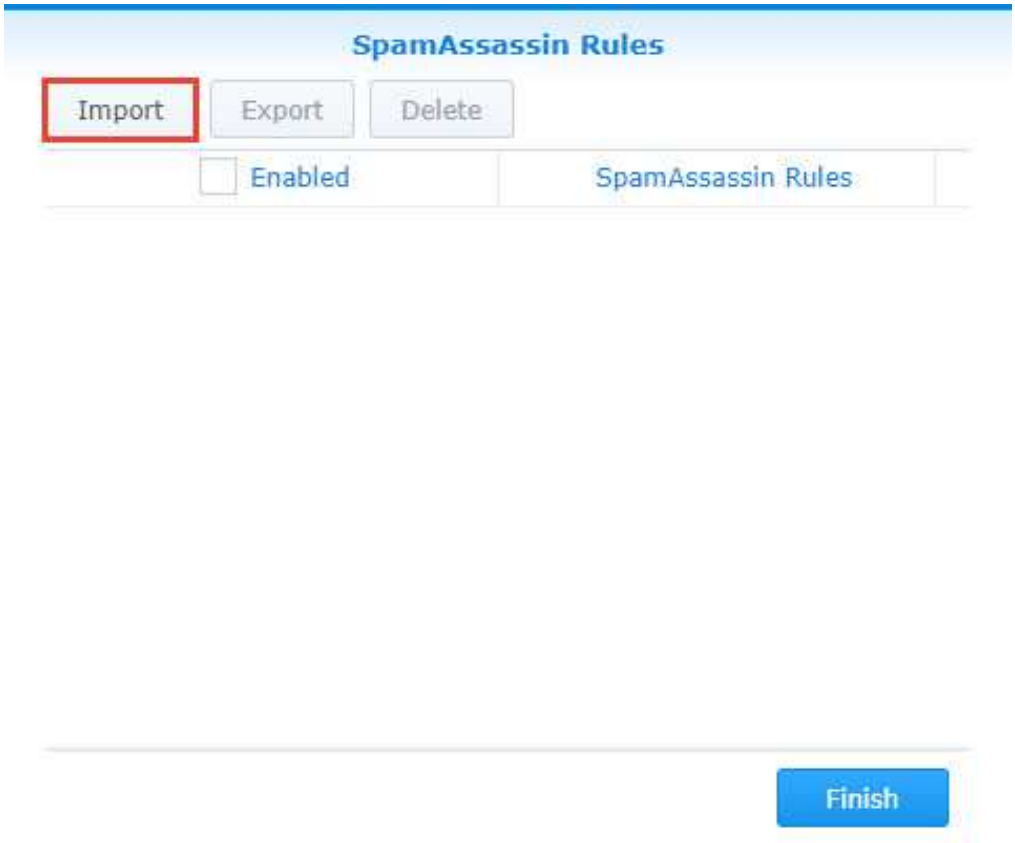
SpamAssassin 規則

1 前往**安全性** > **垃圾郵件**，按一下**編輯 anti-spam 設定**按鈕。

2 前往**編輯 anti-spam 設定**視窗中的**一般**頁籤，按一下 **SpamAssassin 規則**按鈕。

3 按一下**匯入**按鈕來新增 SpamAssassin 規則。

注意：匯入的檔案副檔名必須為 .cf 。匯入後的規則會直接啟動。您可以參考 SpamAssassin 提供的**規則**，或是根據**規則規範**來自行新增。



4 選取您要編輯的規則，進行**啟動**、**匯出**、**刪除**等相對應的操作。

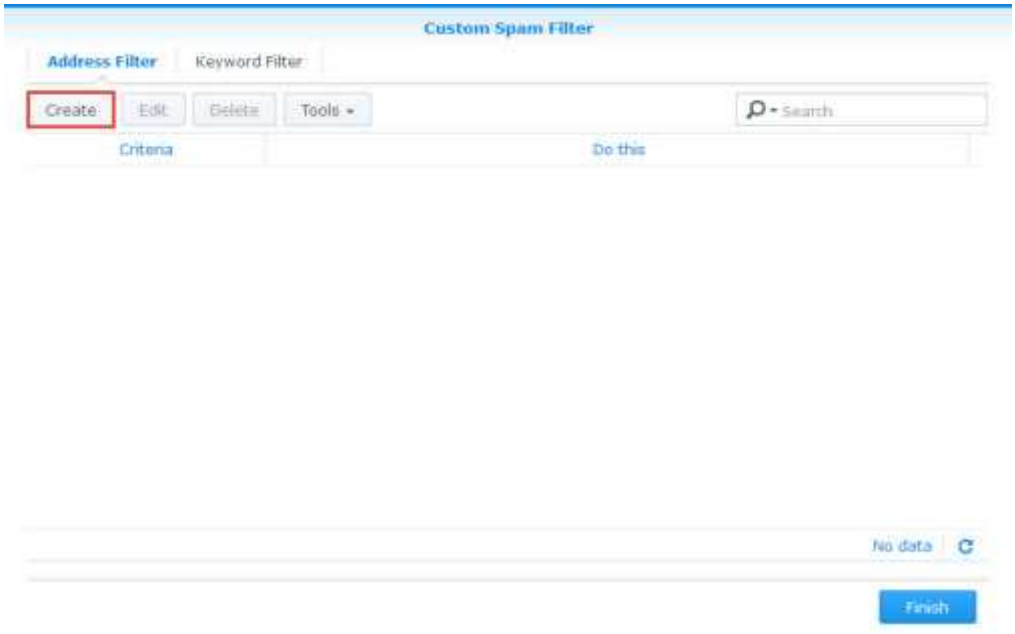
5 按一下**完成**來完成設定。

自定垃圾郵件過濾

1 前往**安全性** > **垃圾郵件**，按一下**編輯 anti-spam 設定**按鈕。

2 前往**編輯 anti-spam 設定**視窗中的**一般**頁籤，按一下 **自訂垃圾郵件過濾**按鈕。

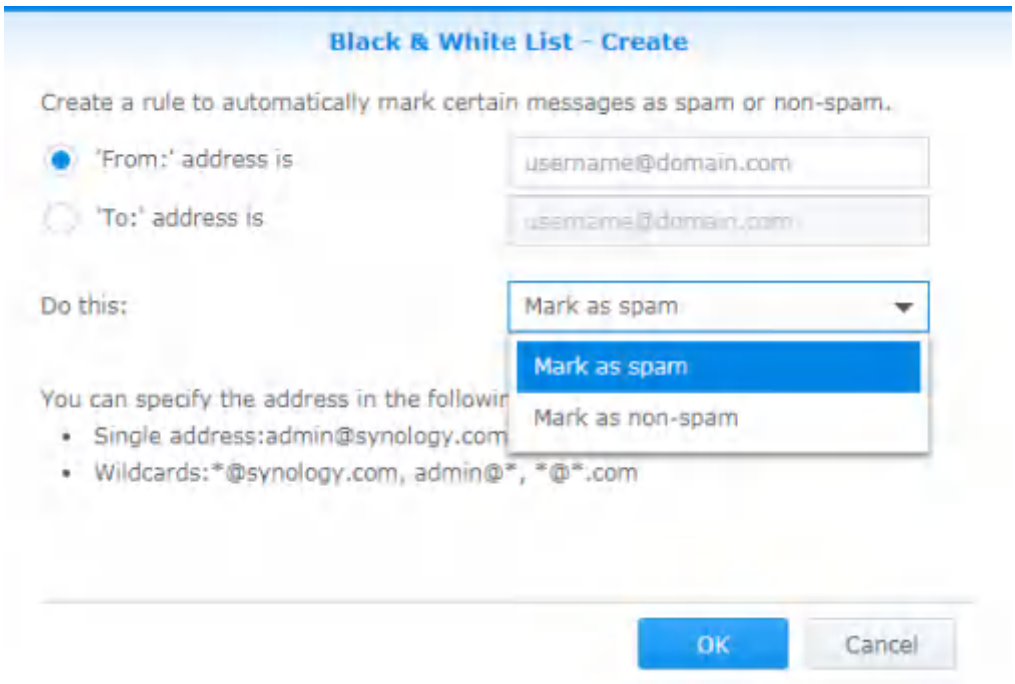
3 前往**自訂垃圾郵件過濾**視窗中的**地址過濾**頁籤，然後按一下 **新增**按鈕。



4 針對寄件人及收件人地址設定條件。當符合條件時，信件會被標記為垃圾郵件或是非垃圾郵件。地址支援萬用符號 (*)。

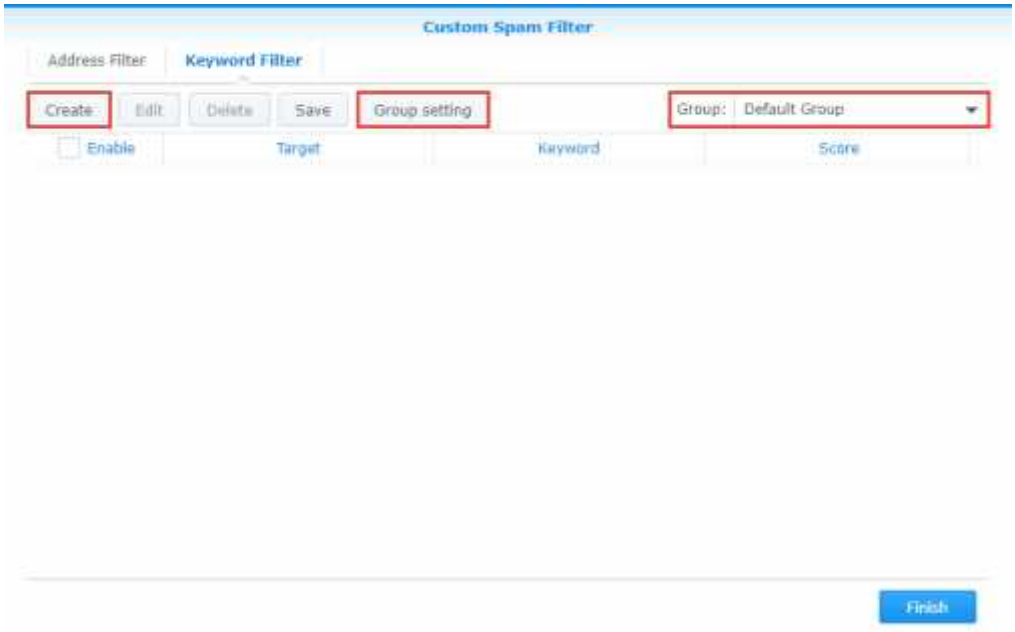
5 從**執行**下拉式選單中選擇**標記為垃圾郵件**或**標記為非垃圾郵件**。

注意：垃圾郵件分數會被略過而直接執行此動作。



6 按一下**確定**來完成設定。

7 前往**自訂垃圾郵件過濾**視窗中的**關鍵字過濾**頁籤。您可以透過群組管理您的關鍵字。按一下**群組設定**按鈕來新增群組。您亦可在右側的**群組**下拉式選單中選擇要編輯的群組。



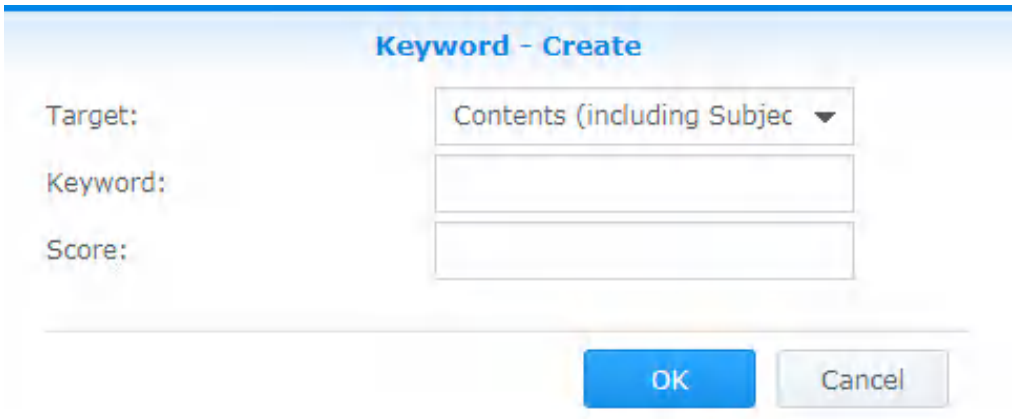
8 按一下**新增**按鈕來自訂規則：

- **目標**：您可以從**目標**下拉式選單中選擇要過濾的選項：

選項	描述
標題	信件的標題。
內容 (含主旨)	信件的內文和標題。

- **關鍵字**：輸入要過濾的內容，可使用正規表達式。請參考**此處**來了解更多正規表達式的資訊。
- **分數**：設定當郵件包含此關鍵字時，會加多少分到垃圾郵件分數上。

注意：若垃圾郵件分數總和超過垃圾郵件門檻分數，該郵件會被標記為垃圾郵件。



9 按一下**確定**來完成設定。

注意：修改設定後，您也許需要重新調整您的垃圾郵件門檻分數。請回到**編輯 anti-spam 設定**視窗中的**一般**頁籤，然後調整您的分數。門檻分數越高，則垃圾郵件判斷標準越寬鬆，信件較不容易被判定為垃圾郵件。門檻分數越低，則垃圾郵件判斷標準越嚴格，信件較容易被判定為垃圾郵件。

自動學習與垃圾郵件回報設定

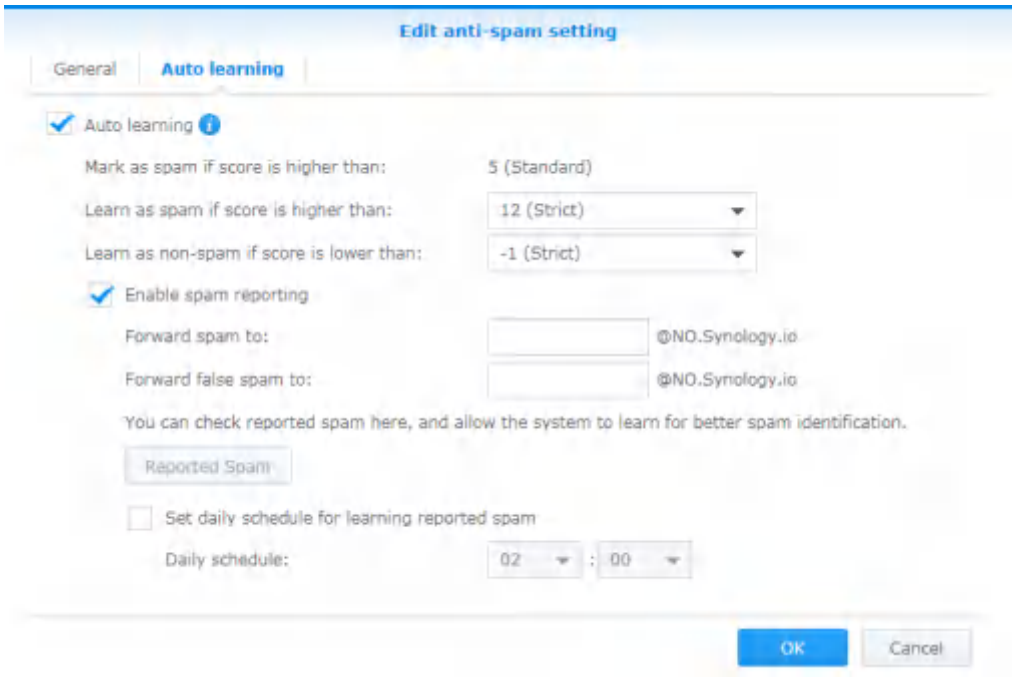
Anti-Spam 引擎開始執行後，您可以利用特別打造的演算法來訓練 MailPlus Server，讓垃圾郵件偵測更加精準。自動學習與垃圾郵件回報機制可以改善 Anti-Spam 的偵測結果，更加符合個別 MailPlus Server 的使用情境：

- **自動學習**：在 Anti-Spam 引擎偵測垃圾信件的過程中，系統會根據信件的分數，自動挑選出符合條件的信件，進一步分析與學習。
- **垃圾郵件回報**：Anti-Spam 引擎有時可能無法偵測出垃圾郵件，或是將正常信件誤判為垃圾郵件，此時使用者可以透過垃圾郵件回報機制，將沒有被正確分類的信件回報給 Anti-Spam 引擎，重新學習。

請參考以下步驟來設定自動學習與垃圾郵件回報：

1 前往**安全性** > **垃圾郵件**，然後按一下**編輯 anti-spam 設定**按鈕。

2 前往**編輯 anti-spam 設定**視窗中的**自動學習**頁籤。



3 勾選**自動學習**核取方塊來調整以下設定：

- **分數高於此數字則標記為垃圾郵件**：此分數為**一般**頁籤中設定的垃圾郵件門檻分數。
- **若分數高於此數字則記為垃圾郵件**：偵測垃圾信件時，若偵測到的分數高於此設定值，則 Anti-Spam 引擎會進一步分析信件中的關鍵字，擴充 Anti-Spam 引擎的資料庫並增進學習能力。日後若信件中出現相同關鍵字則較容易被判定為垃圾信。
- **若分數低於此數字則記為非垃圾郵件**：偵測垃圾信件時，若偵測到的分數低於此設定值，Anti-Spam 引擎會進一步分析信件中的關鍵字，擴充 Anti-Spam 引擎的資料庫並增進學習能力。日後若信件中出現相同關鍵字則較容易被判斷為非垃圾信。

4 勾選**啟動垃圾郵件回報**核取方塊來調整以下設定：

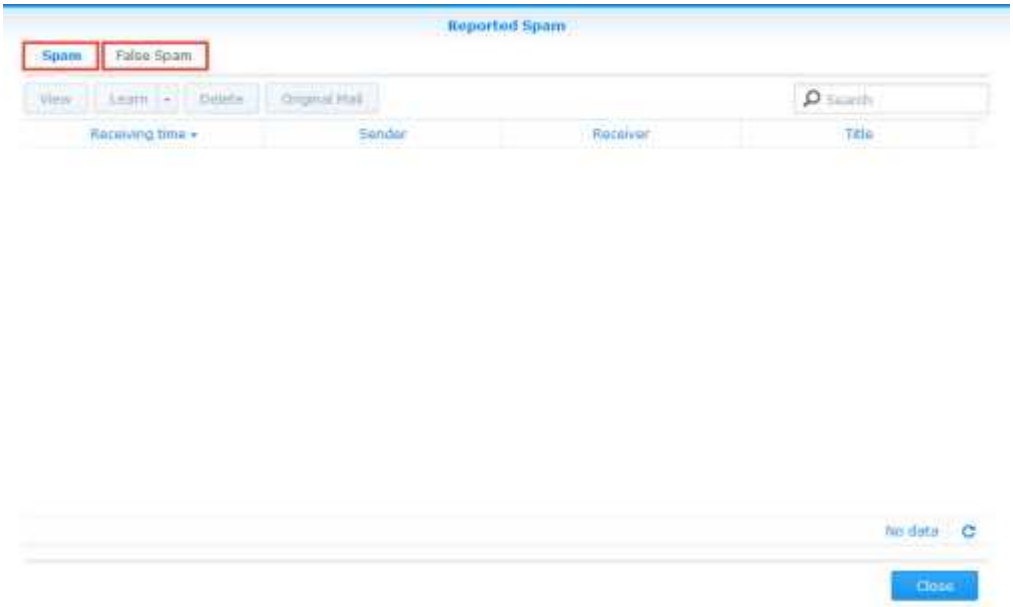
注意：回報機制會透過將垃圾信件收集至特定的信箱來學習。因此在垃圾郵件回報機制啟動後，使用者可以透過以下兩個方式回報垃圾郵件及非垃圾郵件：

1. 若使用者使用 MailPlus 來收信，轉寄的信箱已經設定好。使用者只需在 MailPlus 中標示垃圾郵件，或到 MailPlus 的垃圾郵件匣將信件標記為非垃圾郵件即可。
2. 若使用者使用第三方郵件用戶端來收信，則必須透過收信軟體內建的以附件轉寄功能，將原信件以附件形式轉寄至下面設定的回報信箱。

- **轉寄垃圾郵件至**：設定一個郵件地址，當使用者使用第三方郵件用戶端收信並需要回報垃圾郵件，則可將原信件以附件形式轉寄至此信箱。
- **轉寄誤報垃圾郵件至**：設定一個郵件地址，當使用者使用使用第三方郵件用戶端收信並發現有信件被誤報為垃圾郵件，則可將原信件以附件形式轉寄至此信箱。

- **回報垃圾郵件**：按一下**回報垃圾郵件**按鈕來檢視目前已回報的垃圾郵件與非垃圾郵件。在信件列表中，選擇您想要學習的信件然後按一下**學習**按鈕，即可改善 Anti-Spam 引擎對於此類型信件的偵測能力。學習過的信件將會被刪除。您可以針對垃圾郵件以及誤報垃圾郵件這兩個信箱內的信件進行回報學習。請參考以下方式進行回報垃圾郵件管理：

功能	描述
檢視	信件的標題
學習	讓 Anti-Spam 引擎馬上學習所選取的信件。被學習的信件會從信件列表上消失。
學習全部	您可以在**學習**按鈕旁的下拉式選單找到**學習全部**。按一下**學習全部**來學習所有回報的信件。
刪除	刪除所選擇的信件，此信件將不會被 Anti-Spam 引擎學習。
信件原始檔	開啟新的瀏覽器分頁檢視信件的原始檔內容。
搜尋	在右上角的搜尋欄位中輸入條件，針對寄件人、收件人、標題去搜尋符合規則的信件。



- **設定每日排程來學習回報的垃圾郵件**：勾選此選項來指定系統每日自動學習所有回報的垃圾郵件與非垃圾郵件的時間。

注意：

1. **轉寄垃圾郵件至**輸入的郵件地址不能和現有的使用者或別名重複，並且該郵件地址不會佔用授權數量，僅為系統內部收取郵件樣本之用。
2. **轉寄非垃圾郵件至**輸入的郵件地址不能和現有的使用者或別名重複。

5 按一下**確定**來完成設定。

Postscreen

Postscreen 會在連線階段對連線來源做額外的測試，判斷是否要繼續服務，主要包含兩個功能：

- 測試寄件人是否有遵照 smtp 協定規範，等到 smtp server greeting 結束後才發送寄信指令。若寄件人沒等 smtp server greeting 結束就發送寄信指令，則該寄件人會被阻擋。
- 針對寄件人的 IP 向其他 DNSBL (DNS-based Blackhole List) 伺服器進行查詢。若此 IP 有被其他的伺服器列為黑名單，則該寄件人會被阻擋。

DNSBL 設定

Postscreen 可以設定查詢多台 DNSBL 伺服器，而非只靠一台 DNSBL 伺服器作決定。當查詢伺服器的結果為命中時，會換來一定的分數，不同的伺服器查詢結果得到的分數會被合併計算。當累積的分數超過指定的 **DNSBL 分數門檻**值時，便拒絕服務。請參考以下步驟來調整 DNSBL 設定：

1 前往**安全性** > **垃圾郵件**，勾選**啟動 postscreen 防護機制來抵擋垃圾郵件**核取方塊。

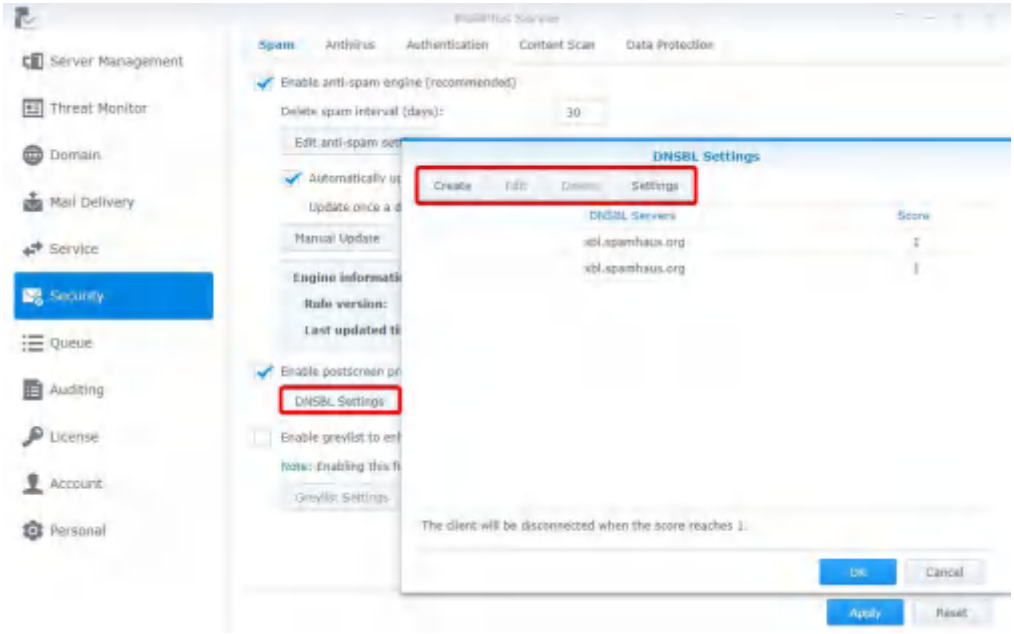
2 按一下 **DNSBL 設定**按鈕來編輯欲查詢的伺服器。

3 按一下**設定**按鈕來設定要被阻擋的 **DNSBL 分數門檻**。

4 按一下**新增**按鈕來新增欲查詢的伺服器。

> **注意：**您也可以在此加入 DNSWL (DNS-Based Whitelist) 伺服器，只要在對應的分數欄位中輸入負數的分數即可有對應效果。

5 您可以**編輯**或**刪除**選取的 DNSBL 伺服器。



6 按一下**確定**來完成設定。

啟動灰名單

灰名單機制是指當有新信進來時，系統會查看以前是否曾經有相同的 IP 位址、寄件人或收件人紀錄，如果查無記錄，此信件將被視為可疑信件，會先回傳錯誤訊息給寄件人，請他稍後再寄信。依照 smtp 協定規範，寄件人收到暫時錯誤的訊息後，會稍待一段時間再嘗試寄信，但是垃圾郵件的寄件人通常就會放棄寄送。當一般寄件人隔一段時間再寄信時，系統就會收下信件。灰名單機制就透過此方式阻擋垃圾郵件。

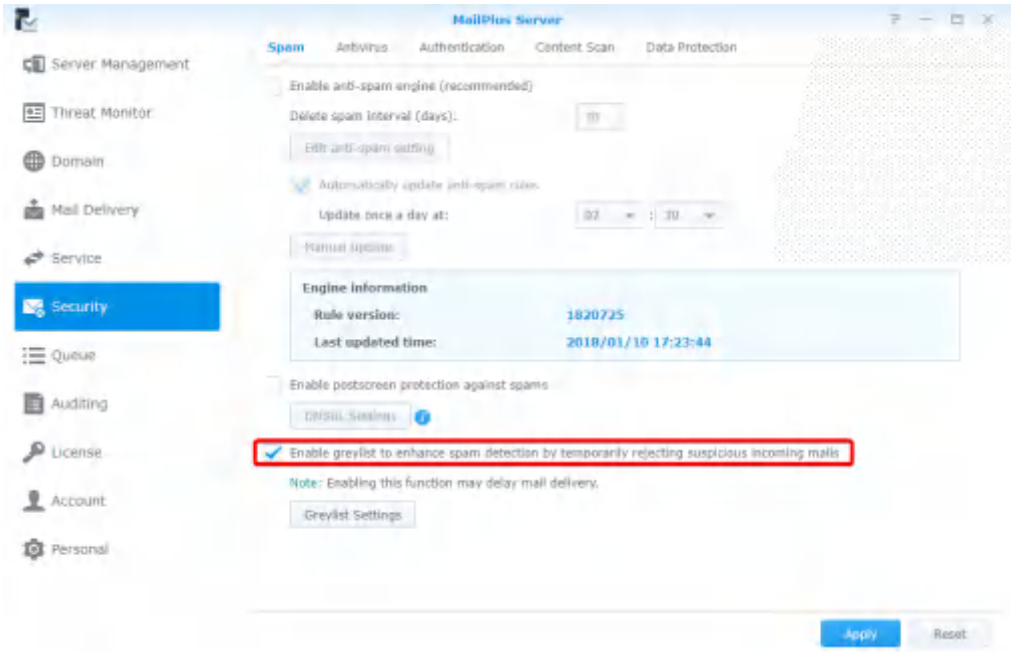
當啟動灰名單後，灰名單會針對所有來源執行預設動作，包括：

- **白名單**：直接通過檢查，不會回傳暫時錯誤訊息。
- **灰名單**：當過去沒有相同的收信記錄時，執行灰名單機制，回傳暫時錯誤訊息給寄件人。
- **黑名單**：直接拒絕收信。

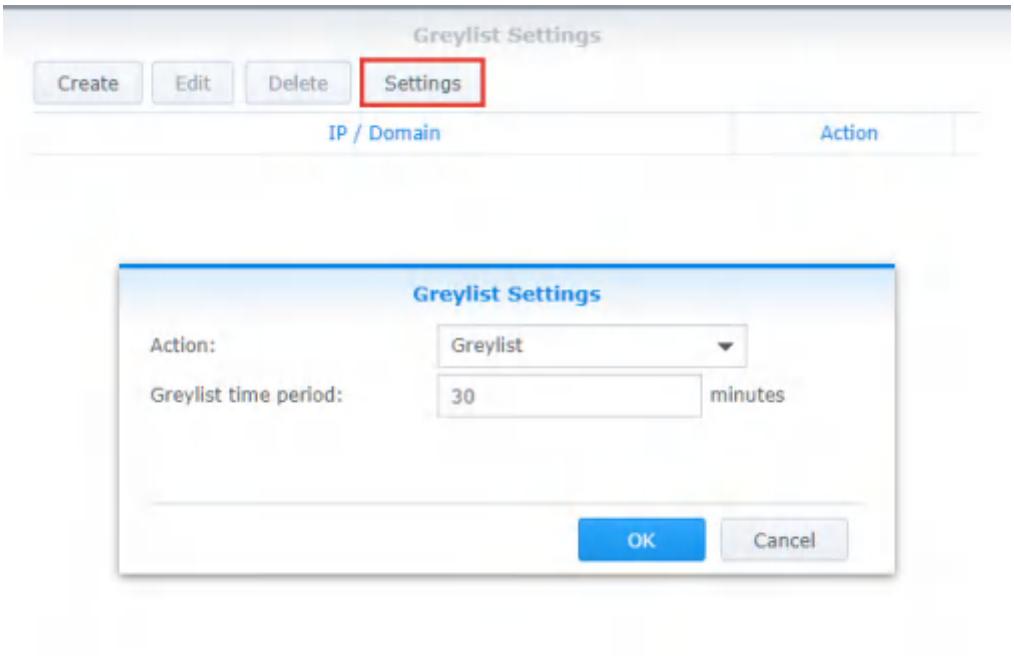
> **注意：**灰名單機制可能會造成一般的信件較晚送達。啟動此功能前，請確定您已完全了解灰名單機制可能帶來的影響。

請參考以下步驟來啟動灰名單。

1 前往**安全性** > **垃圾郵件**，勾選**啟動灰名單，暫時阻擋可疑信件以加強垃圾郵件偵測**核取方塊。

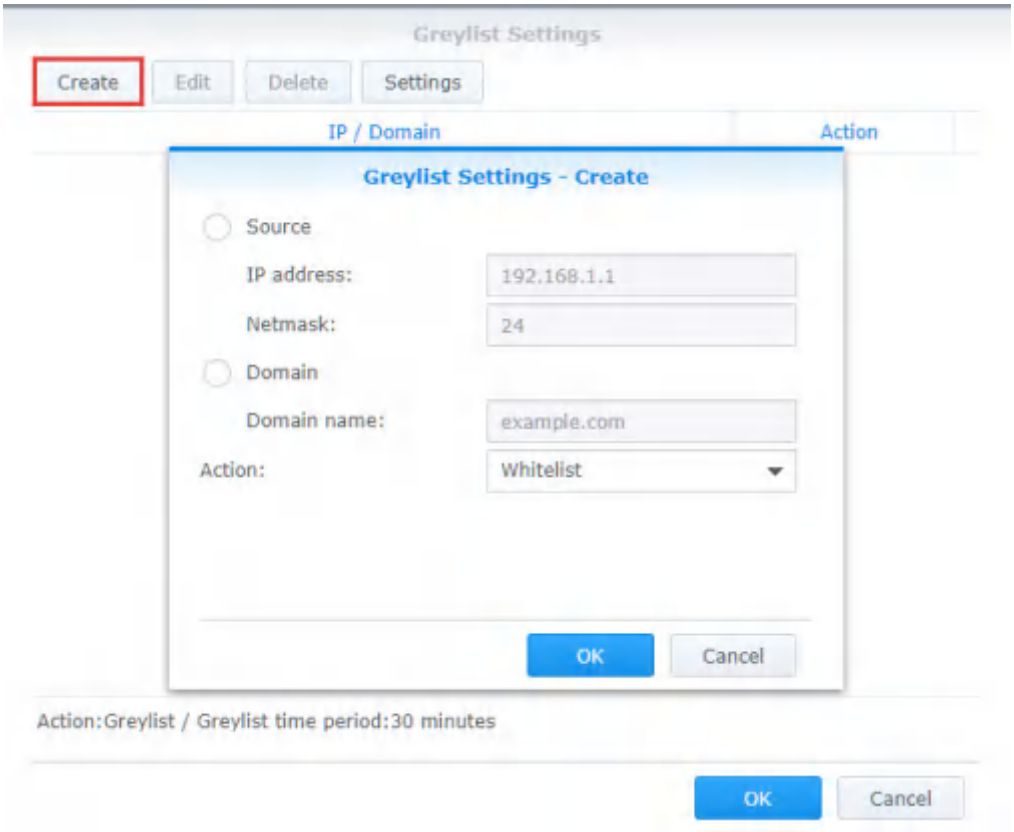


2 按一下**灰名單設定**按鈕來設定預設動作，或是設定針對特定 IP 位址或網域設定個別動作。



3 在**灰名單設定**視窗中按一下**設定**按鈕來對所有來源設定預設動作。

4 從**動作**下拉式選單中選擇一個預設動作。在**灰名單時間**欄位中輸入灰名單延遲時間，這將套用到所有執行灰名單的動作上。



5 按一下**新增**按鈕來為個別寄件來源設定不同的動作。您可以為特定使用者設定不同的灰名單，來採取預設動作以外的指令。

6 在彈出視窗中選擇寄件人的來源，然後從**動作**下拉式選單中選擇一個指定動作。

注意：此處的網域來源是透過 DNS 查詢其 IP 的網域名稱，而非透過信件內的 **MAIL FROM**。

7 按一下**確定**來完成設定。

防毒掃描

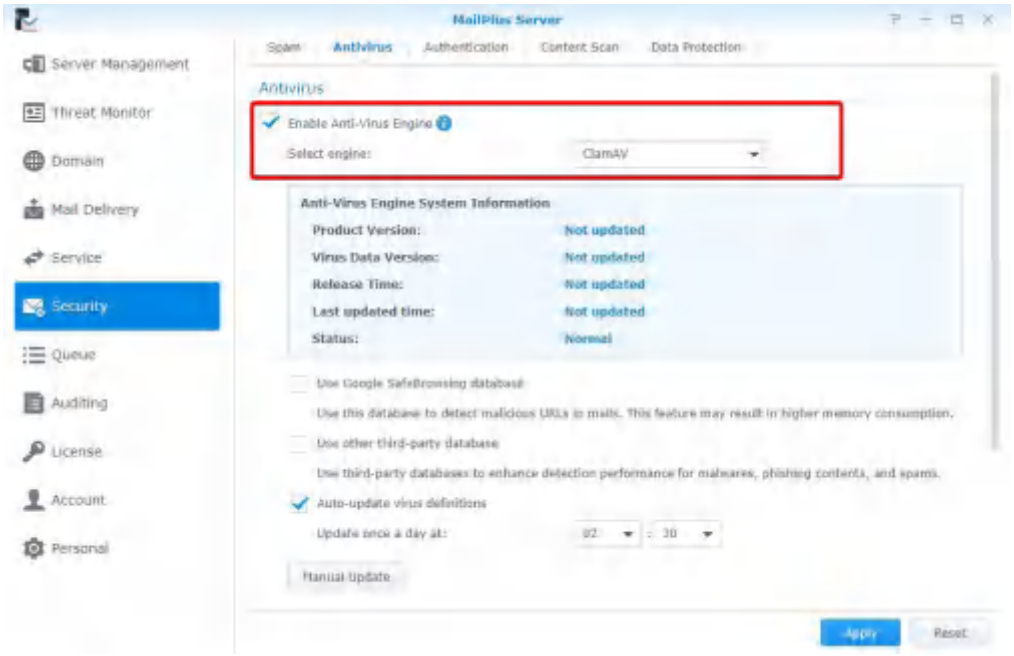
MailPlus Server 提供免費的 ClamAV 以及可付費訂閱的 McAfee 兩種防毒引擎來防範病毒威脅。您可以設定偵測到病毒後要執行的動作。

透過防毒軟體監測，您可以檢查您的信件是否藏有惡意程式或病毒。

- **ClamAV**：ClamAV 是 MailPlus Server 預設的防毒系統，提供您的伺服器免費的完整防護。
- **McAfee**：MailPlus Server 整合在 DSM 套件中心的付費防毒套件中心中。訂閱 **Antivirus by McAfee** 套件後，您可以在 MailPlus Server 中選擇 **McAfee** 作為您的防毒引擎，輕鬆管理防毒排程及日誌，並且使用更多進階的設定。

啟動防毒引擎

1 前往**安全性** > **防毒**，勾選**啟動防毒引擎**核取方塊。



2 從**選擇引擎**下拉式選單中選擇其中一種引擎：

- **ClamAV**： ClamAV 是 MailPlus Server 提供的免費防毒引擎。
- **McAfee**：McAfee 是需要付費訂閱及另外安裝的防毒引擎 (請前往**套件中心**來安裝 **Antivirus by McAfee**)。

3 請參考以下章節來完成設定。

ClamAV

若您選擇 ClamAV 為您的防毒引擎，請參考以下步驟來進行設定：

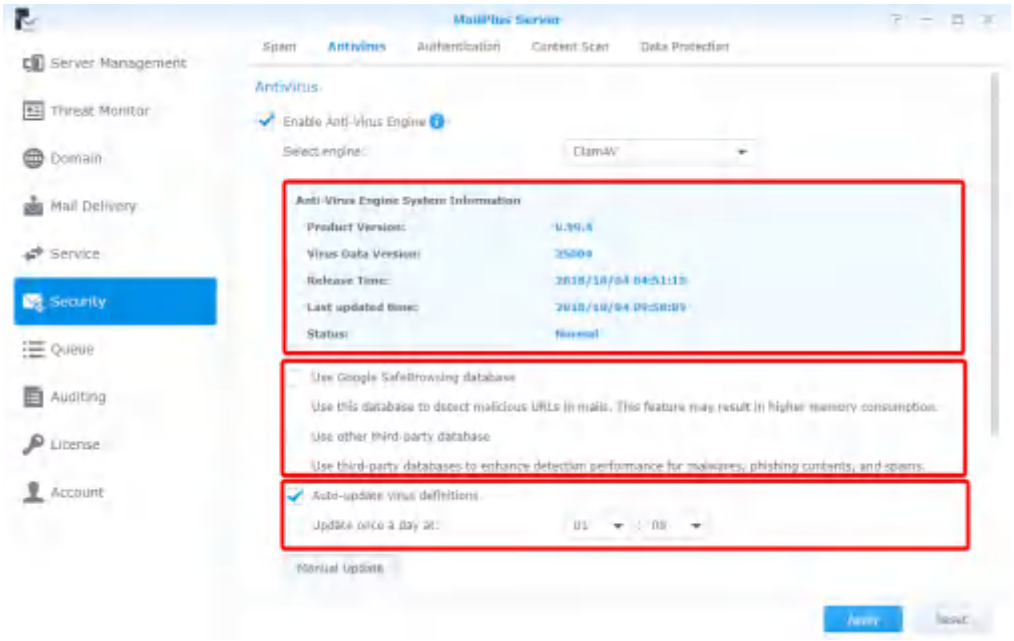
1 在**防毒引擎系統資訊**下檢視您目前防毒引擎的相關資訊。請定期更新您的防毒引擎。

2 ClamAV 使用外部的資料庫來強化部分功能：

- **使用 Google SafeBrowsing 資料庫**：使用 ClamAV 整合的 Google SafeBrowsing 資料庫，來偵測信件中是否有惡意連結。
- **使用其他第三方資料庫**：使用 Sanesecurity 等**第三方資料庫**，來增強病毒的偵測能力。

3 您可以選擇自動或是手動更新病毒定義檔：

- **自動更新病毒定義檔**：啟動自動更新，系統將每日定時下載最新的病毒定義檔，以增強病毒的偵測能力。
- **手動更新**：按一下**手動更新**按鈕，會立即更新病毒定義檔。

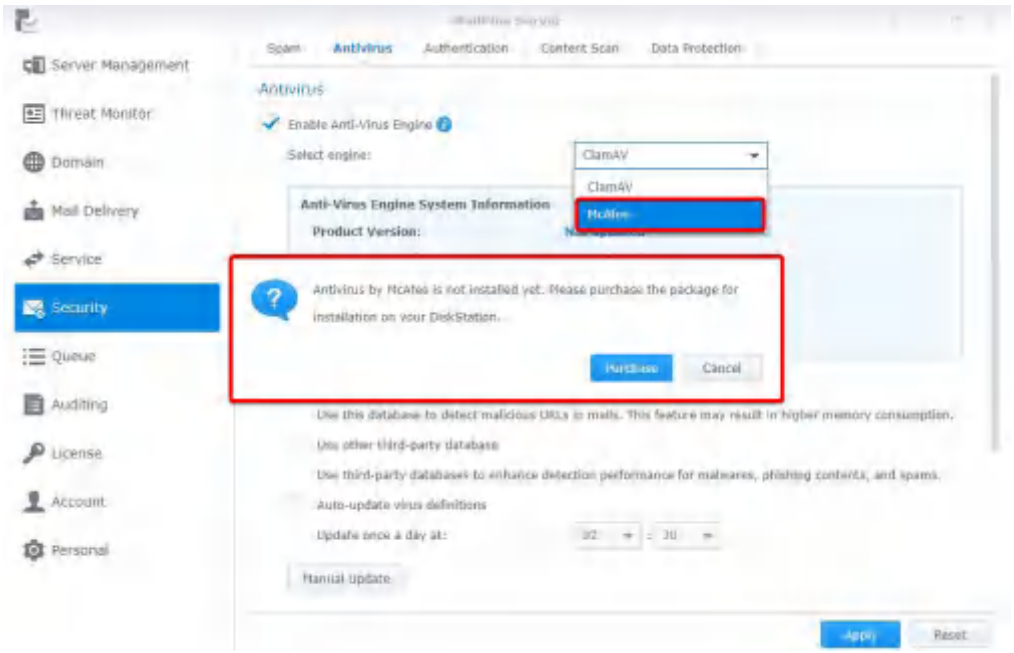


4 按一下套用來儲存設定。

McAfee

若選擇 McAfee 做為您的防毒引擎，則需要前往 DSM 套件中心安裝及購買 McAfee。

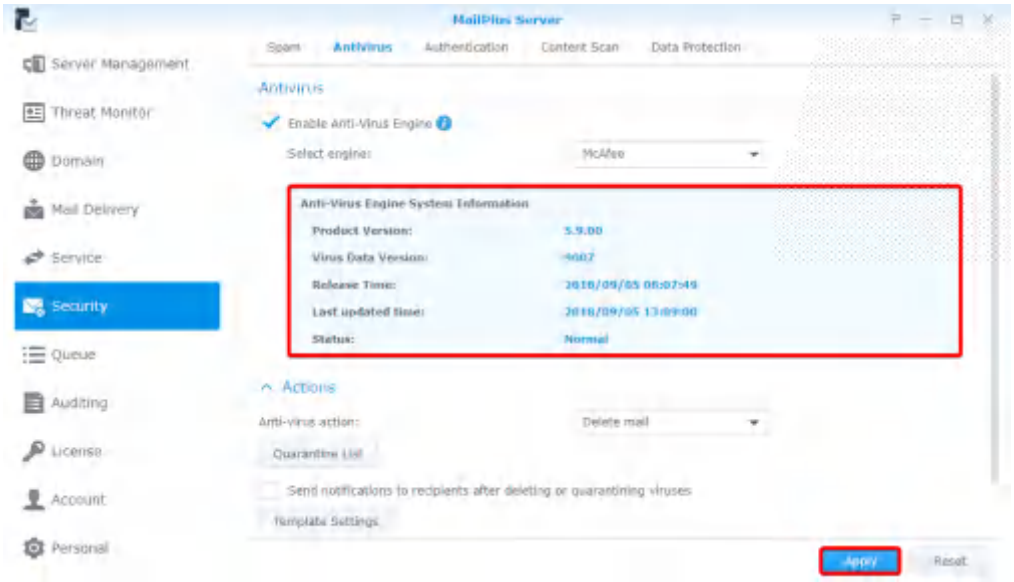
1 若您未安裝 McAfee 或是授權已過期，會出現警示視窗。您需要至套件中心安裝 **Antivirus by McAfee**，並以 **Synology Account** 購買授權。



2 在防毒引擎系統資訊下檢視 McAfee 的相關資訊。

注意：

1. 您必須至 **Antivirus by McAfee** 套件中設定 McAfee 的相關選項。
2. 如果狀態顯示為異常 (可能有授權問題或病毒碼檔案損毀等)，**Antivirus by McAfee** 將不會掃描信件，請務必解決問題或是切換回 ClamAV。若使用者手動停用 **Antivirus by McAfee**，MailPlus Server 將會自動切換成 ClamAV。



3 按一下**套用**來儲存設定。

病毒處理行動設定

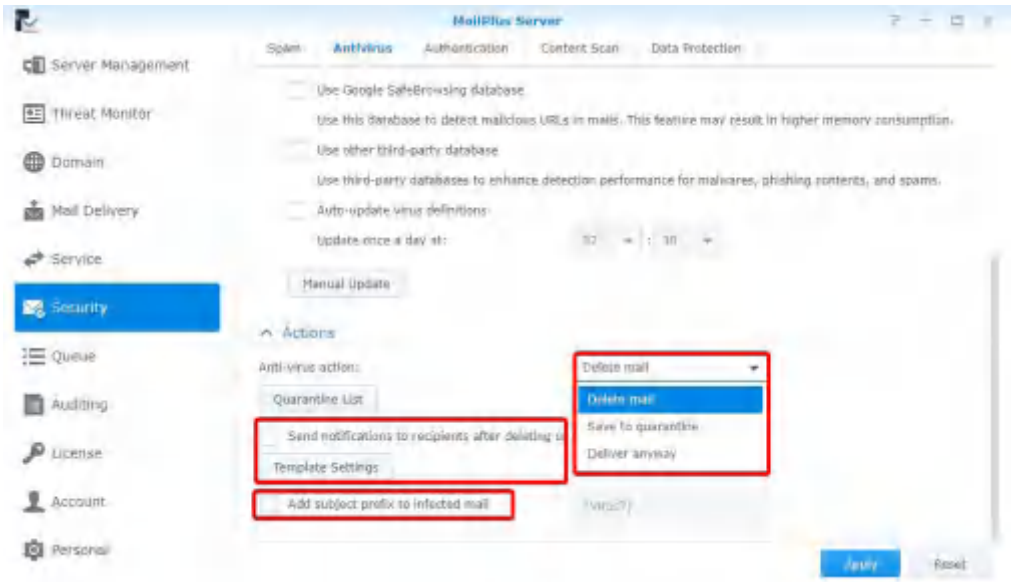
1 前往**安全性** > **防毒**。

2 在**病毒處理行動**下拉式選單中，選擇防毒引擎偵測到信件中有病毒時，將執行的動作：

- **刪除信件**：刪除該信件。
- **儲存至隔離區**：將信件攔截並儲存至隔離區，您可以對隔離區的信件進行操作。
- **照常傳送**：傳送該信件。

3 若您選擇**刪除信件**或**儲存至隔離區**，您可以選擇勾選**刪除或隔離病毒後，寄送通知訊息給收件人**核取方塊來幫助您了解狀況。當執行以上動作後，會寄送通知信件給原始信件的收件人。您可以按一下下方的**範本設定**按鈕來修改通知信件的範本。您可以在**範本設定**中，為隔離信件與刪除信件設定不同的通知訊息。

4 若您選擇**照常傳送**，您可以勾選**為感染郵件加上標題前置文字**核取方塊來標示可疑郵件。



5 按一下**套用**來儲存設定。

隔離清單

若您有信件被儲存至隔離區，您可以檢視及管理被隔離的信件。請參考以下步驟來調整隔離清單設定：

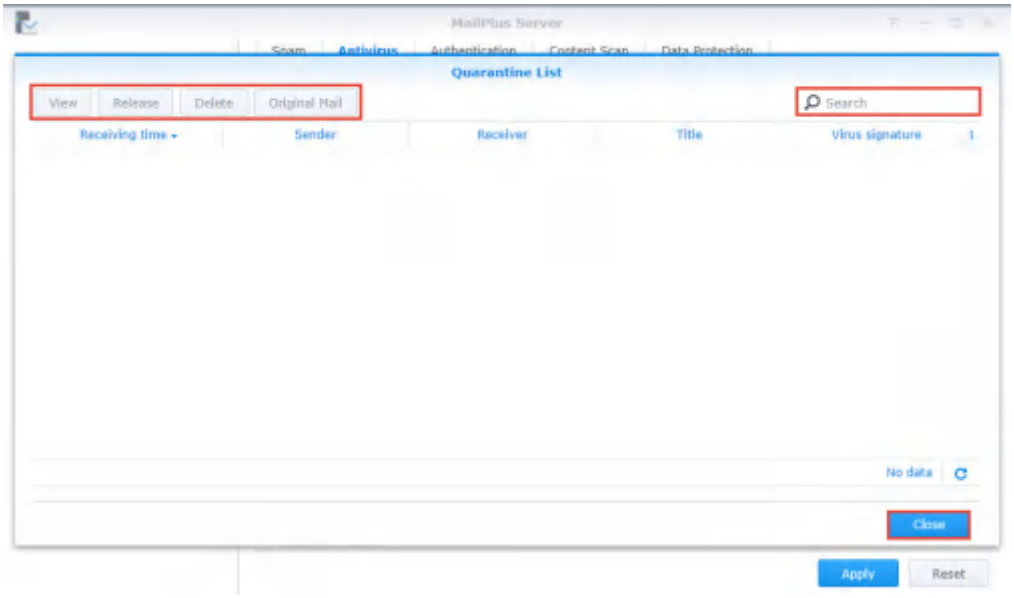
1 前往**安全性** > **防毒**，按一下**隔離清單**按鈕。

2 您可以透過**隔離清單**視窗右上角的搜尋欄位來搜尋寄件人、收件人、標題及病毒碼。

3 選取您要操作的隔離信件，按一下**檢視**或**信件原始內容**按鈕來確認內容。

4 根據信件內容選擇下列動作：

- **放行**：將信件寄送給收件人。
- **刪除**：刪除信件。



5 按一下**關閉**來完成設定。

認證

認證的目的為確認寄件人的身份，避免收到假冒身份的信件，亦避免其他人假冒您的身分。

- **SPF (Sender Policy Framework)**：是一套檢查寄信端主機是否合法的機制。目前，有許多網域會透過 DNS 發佈 SPF 記錄。SPF 記錄提供了可以寄送此網域的信件的主機位置。因此當網路上的主機要寄信至 MailPlus Server 時，系統會先透過 DNS 查詢寄件人網域的 SPF 記錄，並根據 SPF 記錄的內容，判斷要寄信進來的主機是否被允許寄送該寄件人網域的信件。當 SPF 驗證失敗時，該主機會根據 SPF 記錄被分類為 **fail** 或 **softfail**，系統會對兩種結果做不同處理。
- **DKIM (DomainKeys Identi□ed Mail)**：是一套透過加解密方式來驗證寄件人身份是否被假冒，以及信件內容是否有被竄改的機制。根據 DKIM 機制，寄信端主機會先產生一組公開金鑰及私密金鑰，並將公開金鑰透過設定 DNS 記錄的方式發佈出去，在寄信時則利用私密金鑰對該信件加上簽章。收信端主機收到信件時，會透過 DNS 查詢寄件人網域的公開金鑰，接著用公開金鑰對簽章做驗證，以確認寄件人身份以及信件是否有被竄改。
- **DMARC (Domain-based Message Authentication, Reporting & Conformance)**：是一套基於 SPF 與 DKIM 的驗證機制。當系統收到信件時，會根據信件所記載的寄件人，透過 DNS 查詢寄件人網域的 DMARC 記錄，而後根據 DMARC 記錄以及 SPF 跟 DKIM 的驗證結果，來判斷寄件人是否有被假冒。

SPF

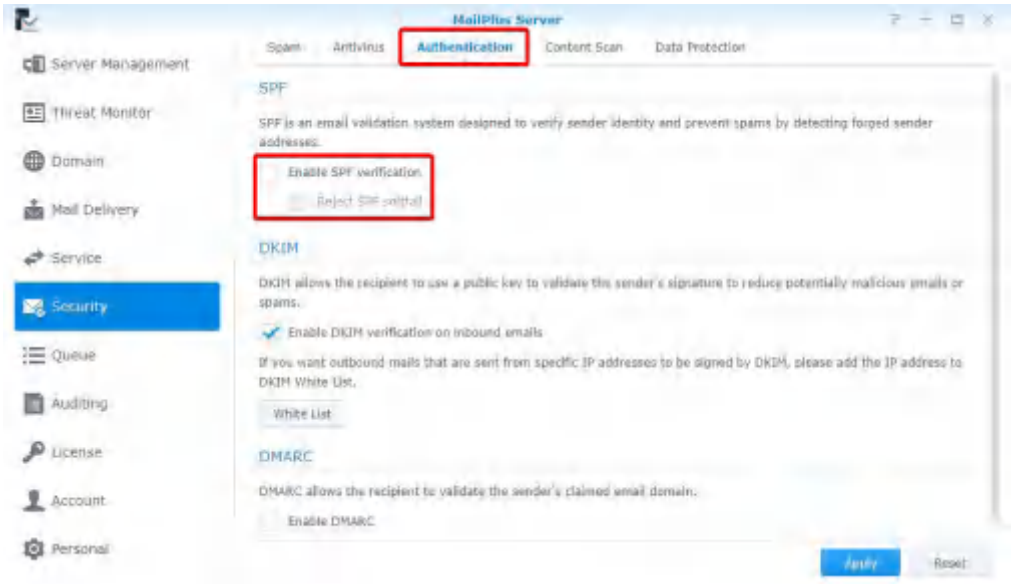
啟動 SPF 驗證讓系統檢查寄件人網域在 DNS 的 SPF 記錄，防止冒用網域寄信。當 SPF 驗證失敗時，結果會是 fail 或 softfail。請參考以下步驟來調整 SPF 驗證的設定：

注意：若您設定 MailPlus Server 接收其他郵件伺服器轉發過來的信，則 SPF 機制可能會攔截轉發的信件，因為轉發信件的郵件伺服器位置不在寄件人發佈的 SPF 記錄當中 (請參考此篇文章來了解更多資訊)。請將轉發的郵件伺服器加入白名單，或者停用 SPF 驗證。

1 前往**安全性** > **認證**。

2 在 **SPF** 區塊下勾選**啟動 SPF 驗證**核取方塊。

- 若 SPF 驗證結果為 **fail** 則拒絕該信件。
- 若 SPF 驗證結果為 **softfail**，您可以選擇勾選**拒絕 SPF softfail** 核取方塊來拒絕驗證結果為 **softfail** 信件，否則驗證結果為 **softfail** 的信件將會被接收。



3 按一下**套用**來儲存設定。

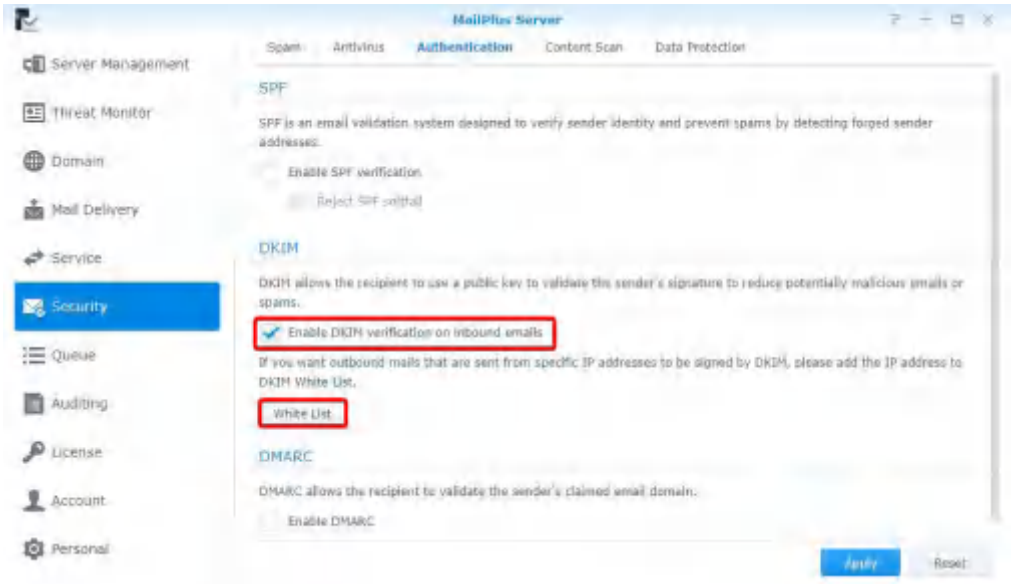
DKIM

您可以啟動 DKIM 驗證來防止信件在傳送途中被篡改，或是身分遭到冒用。請參考以下步驟來調整 DKIM 驗證的設定：

1 前往**安全性** > **認證**。

2 若您想在收件時驗證寄件人身分以減少來自不明來源的信件，在 **DKIM** 區塊下勾選**針對接收的郵件啟動 DKIM 驗證**核取方塊。

3 按一下**白名單**按鈕來新增特定 IP 範圍至白名單，以確保特定寄件人能通過身份驗證並將寄出的信件加上 DKIM 簽章。當此範圍內的主機連線至 MailPlus Server 以對外寄信時，系統會為其加上 DKIM 簽章。



4 按一下**套用**來儲存設定。

DMARC

由於 DMARC 是基於 SPF 和 DKIM 驗證，您必須為您的網域設定 SPF，並產生公開金鑰來啟動寄出信件上的 DKIM 簽署 。請參考以下步驟來啟動 DMARC 驗證：

1 前往**安全性** > **認證**。

2 勾選**啟動 DMARC** 核取方塊來啟動 DMARC。

內容保護

內容保護功能會根據您的設定來過濾可疑的信件。

- **MCP 規則**：根據信件原始內容進行搜尋，若發現過多的可疑內容，則會將信件放入隔離區，或執行其他相關動作。
- **附件過濾器**：依照附件檔案的類型來過濾信件。
- **內容掃描**：加強掃描信件內容和訊息，拒絕或改寫釣魚連結、HTML 標籤等，以確保安全性。

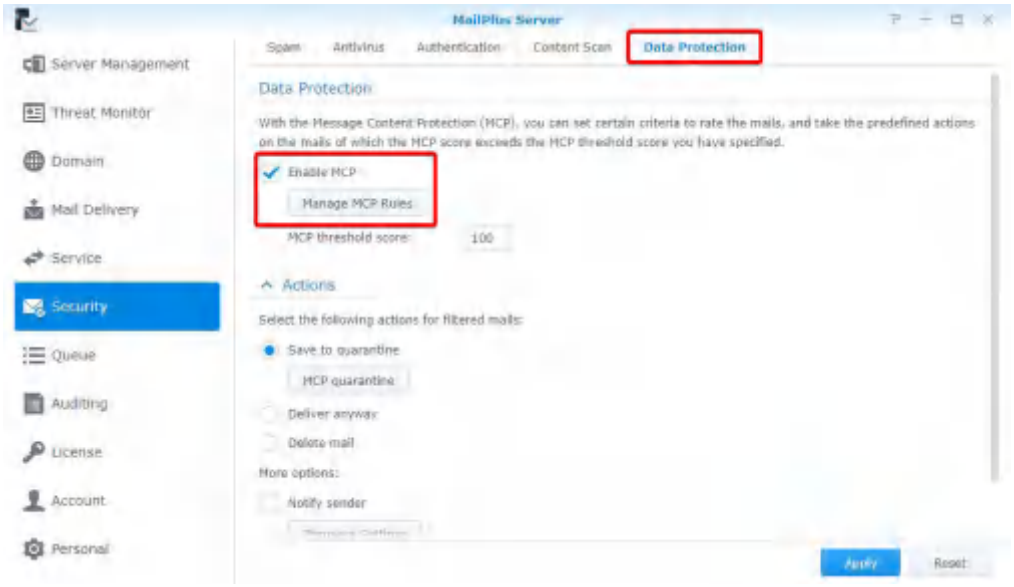
MCP 規則

設定 MCP (Message Content Protection) 規則，並制訂 MCP 門檻分數。當信件符合設定的條件時，該條件所對應的分數會被加總至 MCP 分數，若總和超過設定的 MCP 門檻分數，系統會過濾或封鎖該信件。請參考以下步驟來啟動及管理 MCP：

1 前往**安全性** > **資料保護**，在**資料保護**區塊中勾選**啟動 MCP** 核取方塊。

2 在 **MCP 門檻分數**欄位中輸入一個值。

3 按一下**管理 MCP 規則**按鈕來新增規則。



4 在**管理 MCP 規則**視窗中按一下**新增**按鈕。

5 **新增 MCP 規則**視窗包含以下項目：

- **名稱**：輸入方便識別的規則名稱。
- **目標**：從**目標**下拉式選單中選擇信件中的欄位做為比對的目標：

欄位	描述
標題	信件的標題。
內容 (含主旨)	信件的內文和主旨。
寄件者	信件的寄件者。
收件者	信件的收件者。
自訂 header	原始信件的特定標頭。

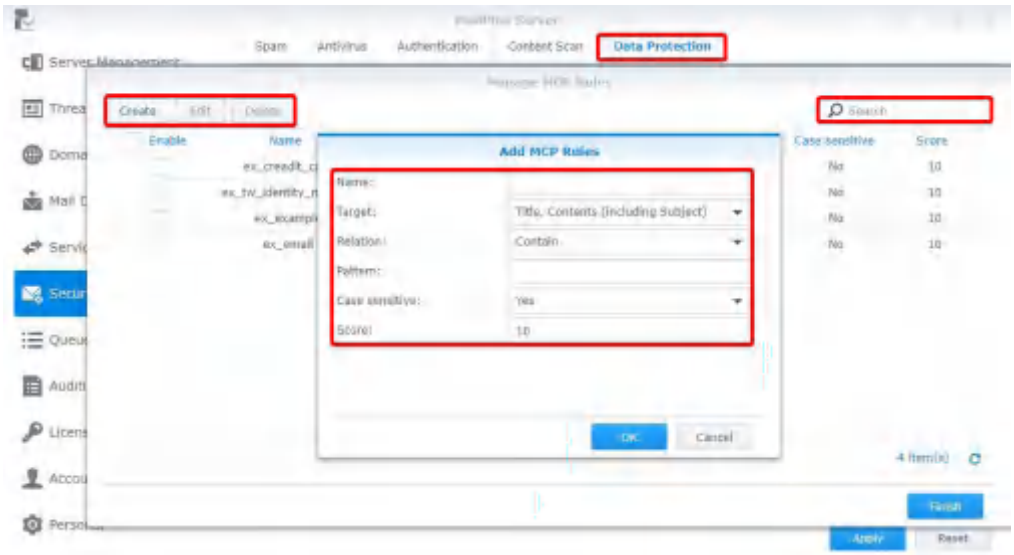
- **自訂 header**：當您從**目標**下拉式選單中選擇**自訂 header**，會出現**自訂 header** 欄位，請在此輸入特殊標頭。
- **關係**：從**關係**下拉式選單選擇比對的條件：

條件	描述
包含	若信件的目標欄位包含比對內容，則符合此規則。
等於	若信件的目標欄位與比對內容相同，則符合此規則。
符合正規表達式	若信件的目標欄位包含比對內容，則符合此規則。比對內容可以使用正規表達式。

- **樣式**：此規則的比對內容。
- **區分大小寫**：選擇**是**或**否**來決定此規則在比對內容時是否要區分大小寫。
- **分數**：當符合此規則的條件時產生的分數。

6 按一下**確定**來完成新增規則。

7 在**管理 MCP 規則**視窗中，您可以選擇**啟動**、**編輯**或**刪除**特定的規則。您也可以透過右上角的搜尋欄位來尋找規則。



8 按一下**完成**來完成設定。

動作

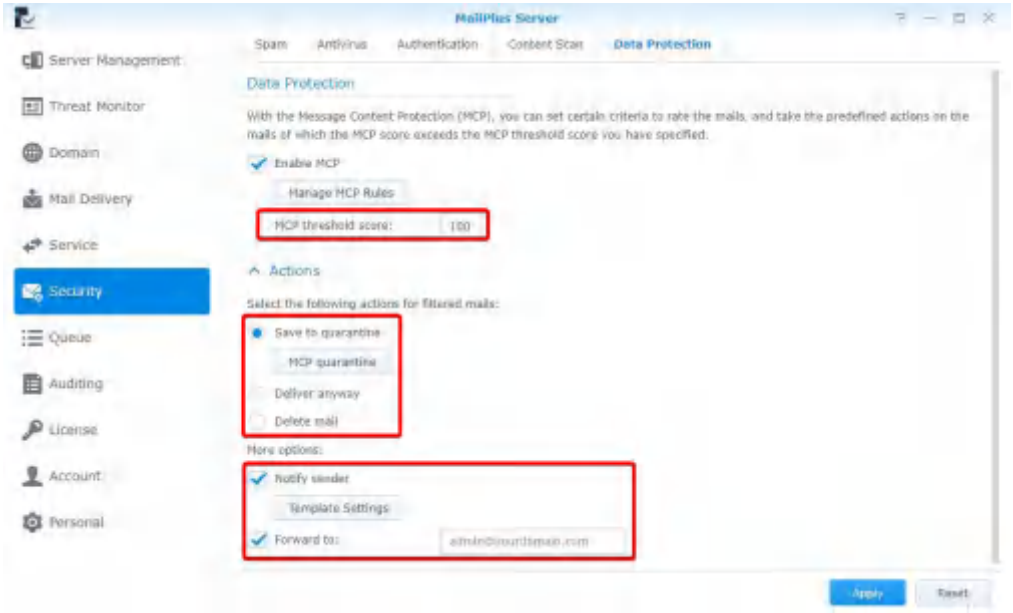
當您所設定的規則總分超過 **MCP 門檻分數**時，將會執行指定動作。請參考以下步驟來設定動作：

1 前往**安全性** > **資料保護**，然後在**資料保護**區塊的 **MCP 門檻分數**欄位中輸入 MCP 門檻分數。

2 在**動作**區塊下，您可以設定超過 **MCP 門檻分數**時盎要執行的動作：

- **儲存至隔離區**：將信件攔截並儲存至隔離區，您可以按一下 **MCP 隔離區**按鈕來檢視被隔離的信件內容。請參考**隔離清單**來了解更多關於管理隔離信件的資訊。
- **照常傳送**：傳送該信件。
- **刪除信件**：刪除該信件。
- **更多選項**：您可以設定當有信件超過門檻分數時，是否要通知特定使用者。

功能	描述
通知寄件者	寄一封通知信告訴寄件者，此信件已被攔截。同時，您可以按一下**範本設定**來設定通知的內容。
轉寄至	將原始信件轉寄至特定信箱。



3 按一下**套用**來儲存設定。

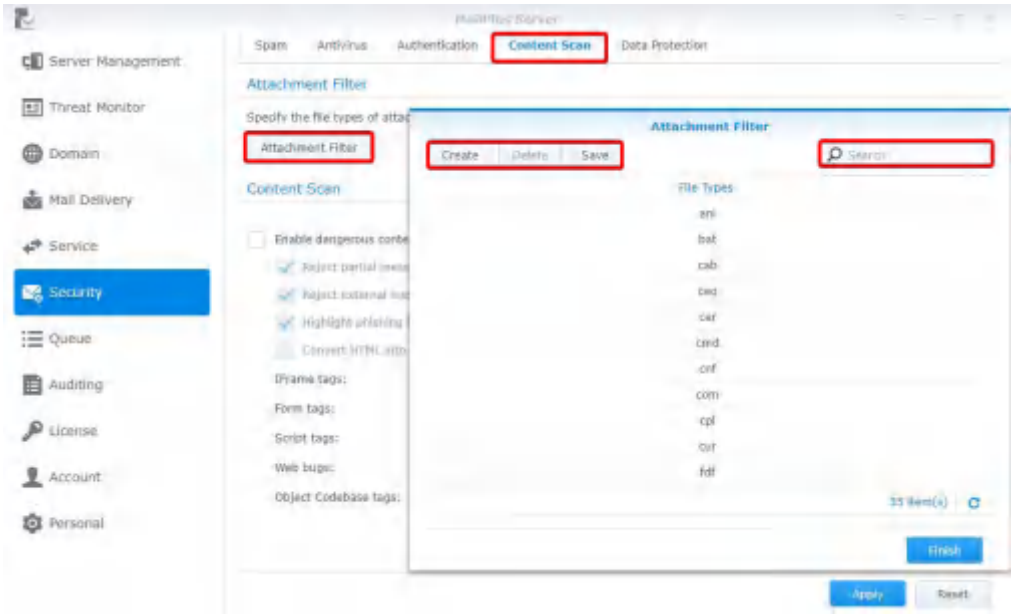
附件過濾器

附件過濾器功能會根據附件的檔案類型決定是否攔截該信件。請參考以下步驟來設定**附件過濾器**：

1 前往**安全性** > **內容掃描**。

2 在**附件過濾器**區塊下，按一下**附件過濾器**按鈕。

3 在**附件過濾器**視窗中按一下**新增**按鈕來增加新的檔案類型。您可以選擇特定的檔案類型進行**刪除**，或是透過右上角的搜尋欄位來搜尋特定檔案類型。



4 按一下**儲存**。

5 按一下**完成**來完成設定。

內容掃描

內容掃描功能會攔截或修改可疑的信件內容。請參考以下步驟來調整**內容掃描**設定：

注意：修改後的內容可能與預期不同，請確認您啟動的功能符合您的需求。

1 前往**安全性** > **內容掃描**。

2 在**內容掃描**區塊下勾選**啟動危險內容掃描**核取方塊後，您可以調整以下設定：

- **拒絕不完整訊息：**拒絕被切割為多個不完整訊息的信件 (指 Content-Type 值為 message/partial 的信件)。
- **拒絕外部郵件內容：**拒絕指向外部資源的信件 (指 Content-Type 值為 message/external-body 的信件)。
- **強調釣魚詐騙區塊：**當系統偵測到郵件中有釣魚連結時，會在將該連結標示出來，警示收件者並避免誤點。
- **將 HTML 轉換為純文字：**當信件為 HTML 格式時，會被轉換為純文字。您可以設定不同的標籤來執行不同的動作。

功能	描述
允許	傳送該信件。
拒絕：	拒絕該信件。
使標籤失效	使標籤失效後，再傳送該信件。

注意：請針對每個標籤進行設定。

監控設定

伺服器狀態監控

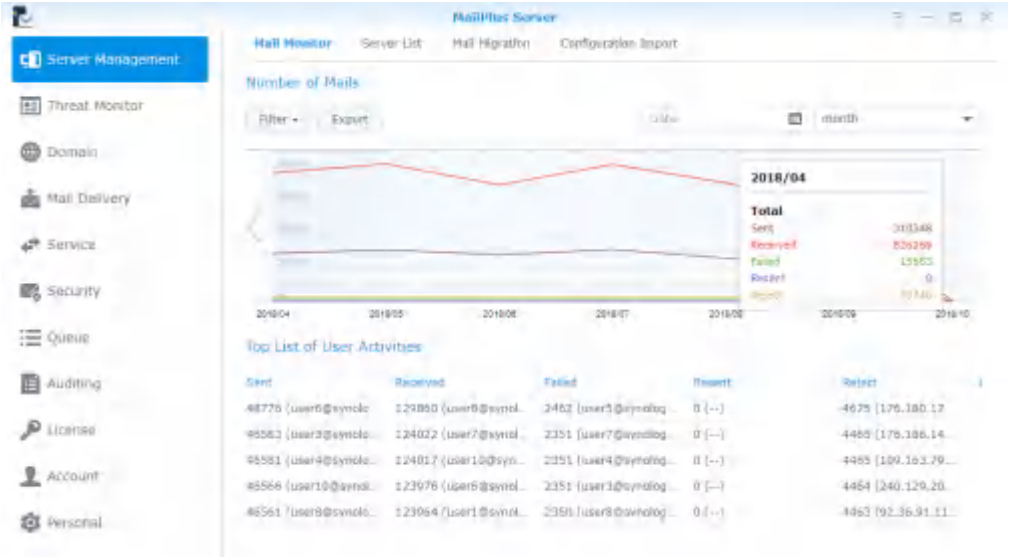
圖像化的介面讓您可以快速了解伺服器的運作狀態：

- **郵件流量監控**：以時間為單位，監控伺服器在這段區間所處理的郵件流量。
- **威脅監控**：您可以檢視伺服器的每個安全設定為您擋下了多少電子郵件威脅。在此亦可快速地了解所有威脅的來源，方便您依此調整安全性的設定。
- **伺服器清單**：在此檢視您的伺服器叢集清單和他們的運作狀態。

郵件流量監控

伺服器管理的郵件監控頁籤顯示了過去一段時間內的郵件活動數量統計，在最高使用者活動清單區塊下，顯示了各個流量類型中出現數量最多的郵件地址。請參考檢視郵件日誌來了解更多關於郵件流量類型的資訊。

注意：若您已設定 High-availability 叢集，請於主要伺服器檢視日誌。



依不同時間區段長度監控流量

MailPlus Server 的郵件流量監控時間區段單位為小時、天、週以及月，郵件數量圖表上的每個資料點代表在該時間區段內某個類型的郵件數量加總值。請參考以下步驟來調整時間區段：

1 前往伺服器管理 > 郵件監控。

2 在郵件數量區塊右上角的日期欄位及下拉式選單中選擇日期及時間區段。

監控特定時間區段的流量

您可以透過兩種方式監控特定的時間區段：

- 將游標移動到郵件數量圖表上的左端或右端，再按一下箭頭圖示即可向前或向後移動時間區段。
- 在郵件數量區塊右上角的日期欄位中選擇目標日期。

注意：MailPlus Server 為不同的時間區段長度保留了不同數量的資料，您只能切換到有可用資料的時間區段。

固定顯示特定時間的詳細資料

郵件數量圖表中的詳細資料面板顯示的資料會隨著您的游標在郵件數量圖表上移動而變動，您可以在郵件數量圖表上按一下左鍵，將詳細資料面板固定顯示某個時間區段。

顯示或隱藏特定流量類型的資料

1 前往**伺服器管理** > **郵件監控**。

2 在**郵件數量**區塊下按一下**篩選**按鈕，勾選核取方塊來選擇顯示或隱藏特定流量類型的資料。

匯出特定時間區段的資料

1 前往**伺服器管理** > **郵件監控**。

2 在**郵件數量**區塊下的圖表中按一下您想進一步了解的時間區段。

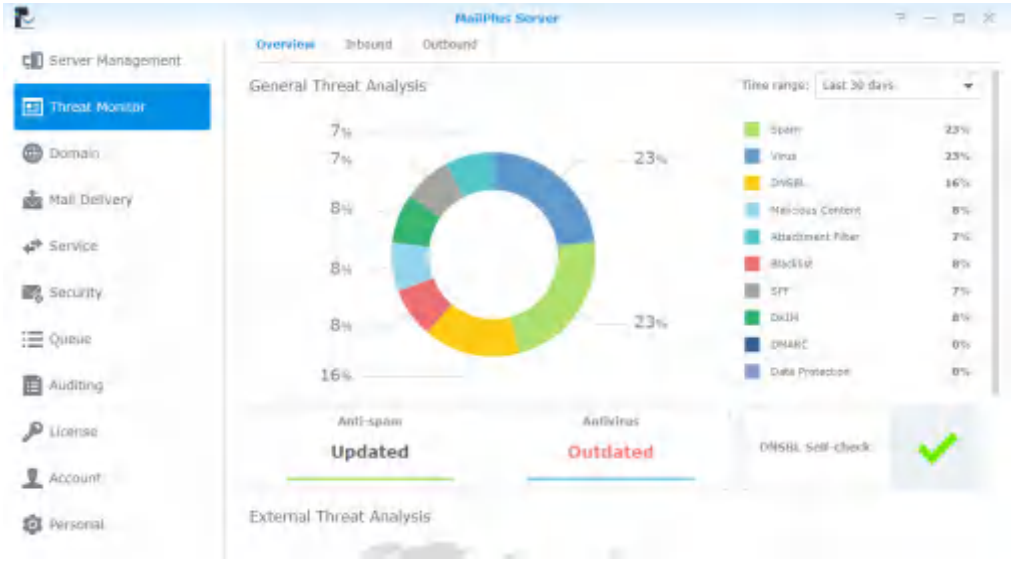
3 按一下上方的**匯出**按鈕。

4 MailPlus Server 將會把該時間區段的資料匯出成 Html 檔案。

威脅監控

威脅監控為您提供電子郵件威脅及其來源的詳細資料，您可以依據資料調整相關設定來可達到最佳安全性。

注意：若您已設定 **High-availability 叢集**，請於主伺服器檢視日誌。



檢視整體威脅分析

整體威脅分析提供收寄電子郵件的各類威脅統計資料，並以圖表呈現。請參考以下步驟來調整**整體威脅分析**設定。

1 前往**威脅監控** > **概觀**。

2 在**整體威脅分析**區塊中，您可以找到威脅統計資料及相關設定：

- **時間範圍：**選取後即可顯示特定時間範圍內的威脅統計資料。
- **威脅清單：**查看各個威脅類型的百分比統計資料。若要查看數量統計資料，將滑鼠移至特定類型上方。
- **威脅環狀圖表：**查看各個威脅類型的百分比統計資料。在右方清單中，可選取或取消選取威脅類型，以符合您的需求。
- **防垃圾郵件：**查看垃圾郵件防護引擎的狀態。若要修改相關設定，按一下即可跳至該頁面。
- **防毒：**查看防毒引擎的狀態。若要修改相關設定，按一下即可跳至該頁面。
- **DNSBL 自我檢查：**查看 Synology NAS 是否列在 DNSBL 黑名單中。按一下即可查看更多細節。

檢視外部威脅分析

外部威脅分析可顯示已攔截電子郵件的寄送來源及對應的數量統計資料。

1 前往**威脅監控** > **概觀**。

2 **外部威脅分析**區塊下方顯示威脅地圖及各個來源的數量統計資料：

- **威脅地圖**：各個圓圈代表一個威脅來源區域。若該區域寄出更多遭到阻擋的電子郵件，圓圈便會擴大。若要查看數量統計資料，將滑鼠移到圓圈上。
- **威脅來源**：此清單顯示已阻擋電子郵件的前六大主要來源和對應的數量統計資料。

檢視已阻擋的接收與傳送郵件

在**接收**及**傳送**，您可分別找到已阻擋的接收及傳送電子郵件的統計資料，還有此類郵件的主要寄件人 / 收件人。

1 前往**威脅監控**。

2 按一下**接收**或**傳送**頁籤。

- **時間範圍**：選取後，即可依特定時間範圍顯示已阻擋的傳送及接收郵件統計資料。
- **已阻擋郵件統計**：依據所選的時間範圍，顯示已接收郵件 (在**接收**頁籤) 或已傳送郵件 (在**傳送**頁籤) 的各種威脅類型趨勢圖。

注意：

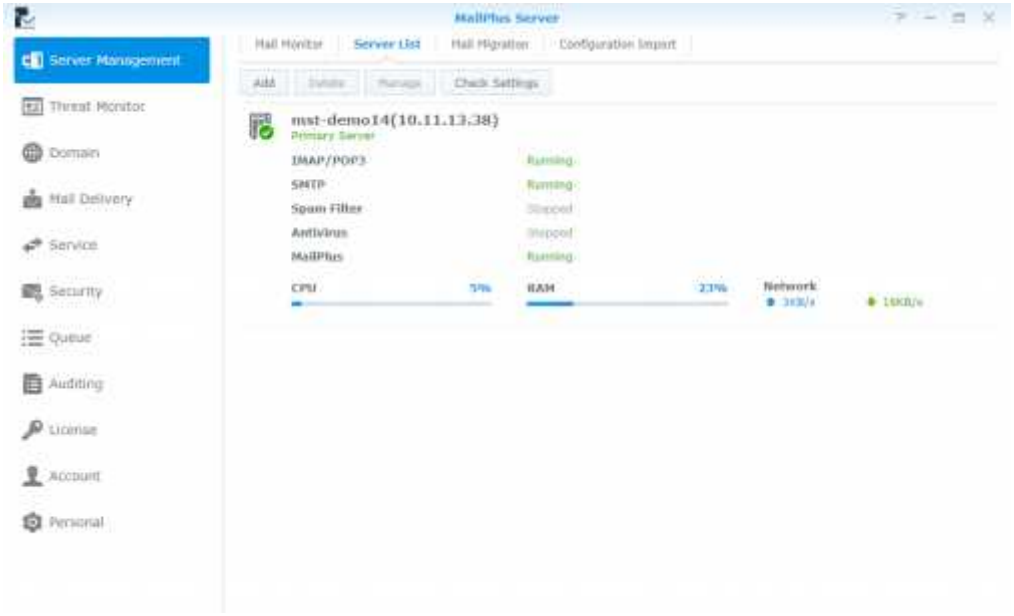
1. 若要改變顯示的威脅類型，選取或取消選取圖表下方的圖例。
2. 若要查看各類威脅類型的數量統計資料，將滑鼠移至圖表上方。

- **已阻擋郵件的主要來源**：顯示已阻擋的接收郵件 (在**接收**頁籤) 或傳送郵件 (在**傳送**頁籤) 前十大主要寄件者，並提供數量統計資料。若要取得完整清單，按一下**顯示全部**。
- **已阻擋郵件的主要目標**：顯示已阻擋的接收郵件 (在**接收**頁籤) 或傳送郵件 (在**傳送**頁籤) 前十大主要收件者，並提供數量統計資料。若要取得完整清單，按一下**顯示全部**。

伺服器列表

在**伺服器管理**的**伺服器列表**頁籤，您能快速掌握 MailPlus Server 的伺服器資訊，包含伺服器所使用的 CPU、記憶體以及網路流量等資訊。請參考下列清單來了解 MailPlus Server 各項功能可能會顯示的狀態：

- **執行中**：該功能正常執行中。
- **已停止**：尚未啟動該功能。
- **異常**：該功能有異常狀況產生。
- **尚未安裝**：只會出現在 MailPlus 欄位中，表示您尚未安裝 MailPlus 套件。
- **準備就緒中**：表示您剛啟動或關閉該功能，該功能正在切換狀態。
- **同步信件中**：當您建立或刪除 MailPlus Server High-availability 叢集時，系統會進行信件同步，此狀態表示目前仍在同步信件中。



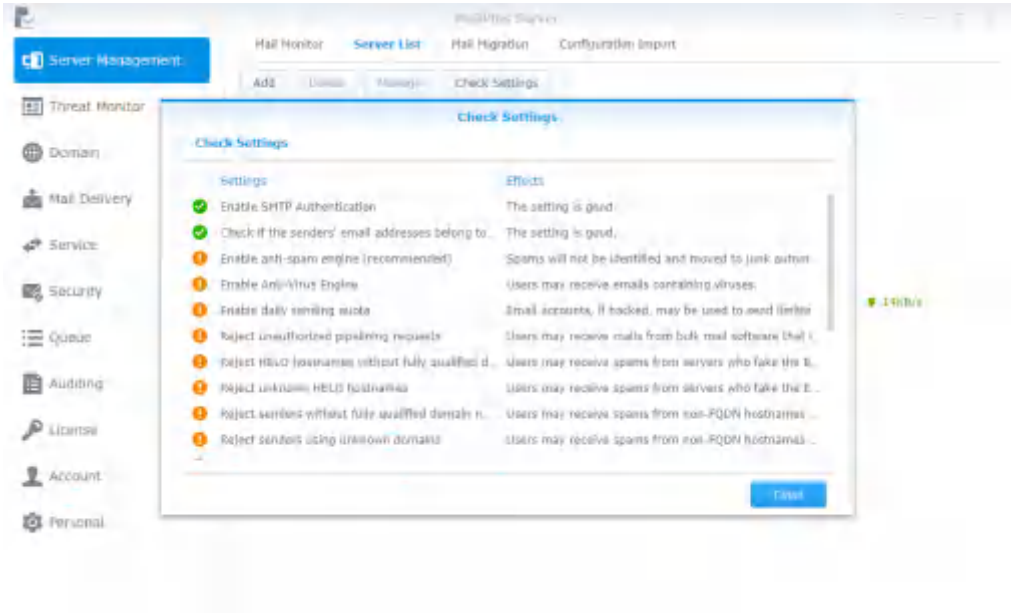
注意：若您啟動了防毒或 MCP 功能，即使沒有啟動 Anti-Spam 功能，垃圾郵件過濾也會跟著啟動，但不會真的進行垃圾信件的掃描。

檢查設定

您可以透過**檢查設定**來檢查您的 MailPlus Server 設定與 Synology 建議的設定是否相同，並檢視若設定不同可能造成的影響。請參考下列步驟：

1 前往**伺服器管理** > **伺服器列表**。

2 按一下**檢查設定**按鈕。



郵件佇列監控

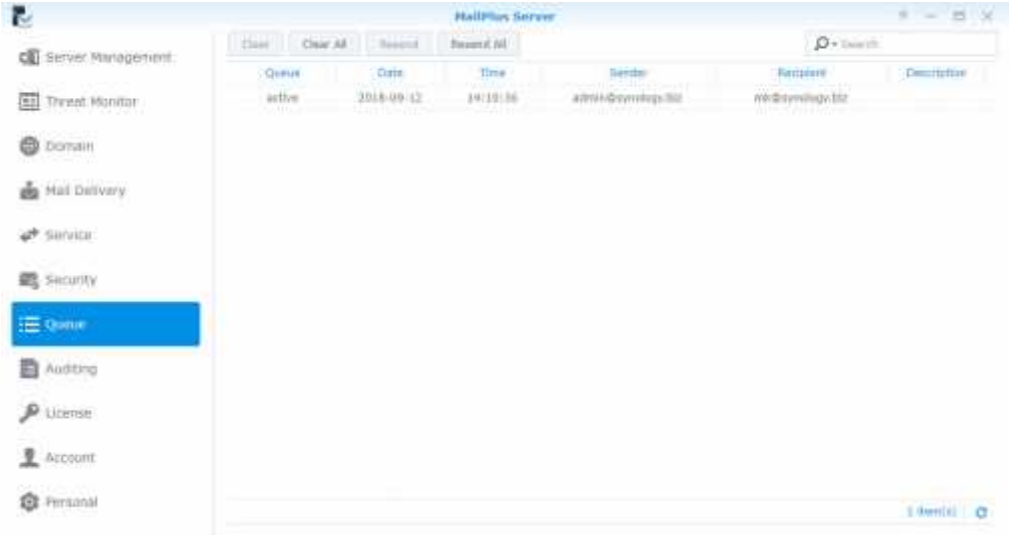
查看尚在處理的郵件狀態，並決定要執行的動作。

監控郵件佇列中的訊息

在**佇列**頁面，您可以檢查所有在佇列中等待被傳送到其他伺服器的郵件，或是被其他伺服器拒絕後重新傳送的郵件。

此頁會顯示目前在佇列中郵件的相關訊息：

- 郵件進入佇列的日期及時間
- 郵件的寄件人及收件人
- 郵件在佇列中等待的原因 (**原因**欄位中會顯示郵件訊息傳送失敗的原因。)



在佇列當中的郵件被分類為下列三種類型：

- **待處理**：郵件訊息正待處理。
- **處理中**：正在處理郵件訊息中。
- **延遲傳送**：系統無法順利傳送郵件訊息，稍候將重新寄送。

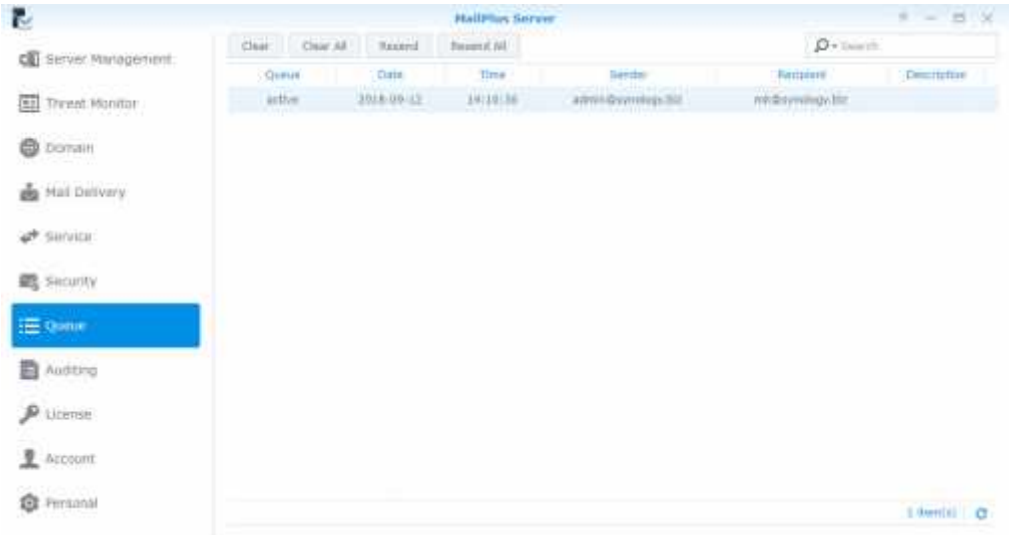
注意：延遲傳送的郵件若在 5 天內皆重新寄送失敗，會被退回至寄件人的信箱。

管理郵件佇列中的訊息

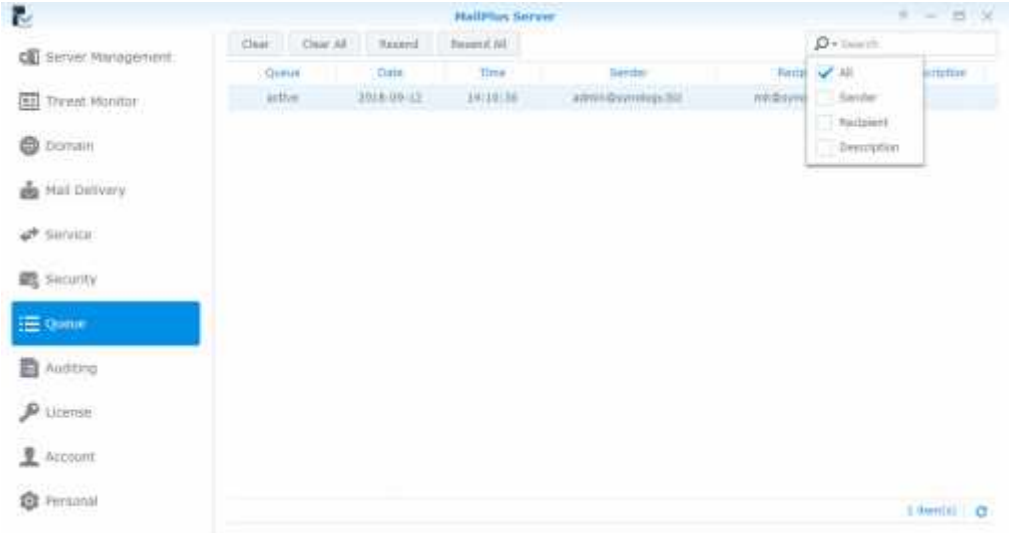
您可以選擇立即重新傳送或取消傳送佇列中的郵件。請參考以下步驟來管理郵件佇列中的郵件訊息：

1 前往**佇列**，然後進行以下操作：

- 若要重傳郵件，在郵件佇列中選擇郵件，再按一下**重新寄送**按鈕，該郵件狀態會從**待處理**切換成**處理中**。
- 若要清除郵件，在郵件佇列中選擇郵件，再按一下**清除**按鈕，該郵件將從佇列當中移除。
- 若要重傳所有郵件，按一下**重新寄送全部**按鈕。
- 若要清除所有郵件，按一下**全部清除**按鈕。



2 您亦可透過右上角的搜尋欄位來尋找特定郵件的狀態。



郵件日誌監控

郵件日誌詳細記錄了伺服器發生過的所有事件，您可以透過日誌的內容了解一些問題的根源，以及相應的解決方案。日誌會產生龐大的檔案，您可以在稽核頁面中，進行詳細的監控設定。

- **檢視日誌**：查看、搜尋以及分析您的日誌，並快速地找到日誌中記錄的相關郵件訊息。
- **封存與管理日誌**：設定日誌封存的週期、備份、輪替規則以及傳送日誌到次要伺服器等彈性的管理方式。
- **日誌報表**：定期以信件的方式寄送日誌，讓您快速了解日誌內容。

檢視郵件日誌

請參考以下步驟來檢視郵件日誌：

1 前往稽核 > 日誌。

2 在上方的下拉式選單中選擇郵件日誌和內部資料庫。

3 郵件日誌會顯示信件的 Message ID、日誌產生的日期和時間、寄件人、收件人、標題、大小以及狀態。郵件日誌的狀態分為以下類型：

- 接收：表示 MailPlus Server 上的使用者收到一封信件。若 MailPlus Server 上的使用者寄信給 MailPlus Server 上的另一個使用者，則日誌的狀態會顯示為接收。若有多個 MailPlus Server 上的使用者收到同一封信件，則會有多筆日誌紀錄；但若信件是寄給 MailPlus Server 上的別名地址，就算別名包含多個收件人且有些收件人來自其他伺服器，還是只會紀錄一筆收件人為別名地址的日誌。若您啟動自動轉寄，無論是否有勾選在收件匣中保留郵件副本核取方塊，都會產生狀態為接收的日誌。
- 發送：表示當寄信給其他伺服器上的郵件地址時，若收件人包含多個其他郵件伺服器上的郵件地址，則會產生多筆日誌紀錄。
- 重新發送：表示曾多次嘗試重新寄送信件給其他伺服器上的郵件地址，MailPlus Server 1.3.0-0370 之後的版本將不再使用此狀態。
- 退信：表示寄送給其他伺服器的信件傳送失敗。

注意：若您有設定自動密件副本 (新增自動密件副本規則) 、**自動轉寄**或**自動回覆**可能會有額外的日誌內容產生。若您已建立 **High-availability 叢集**，請於主要伺服器檢視日誌。

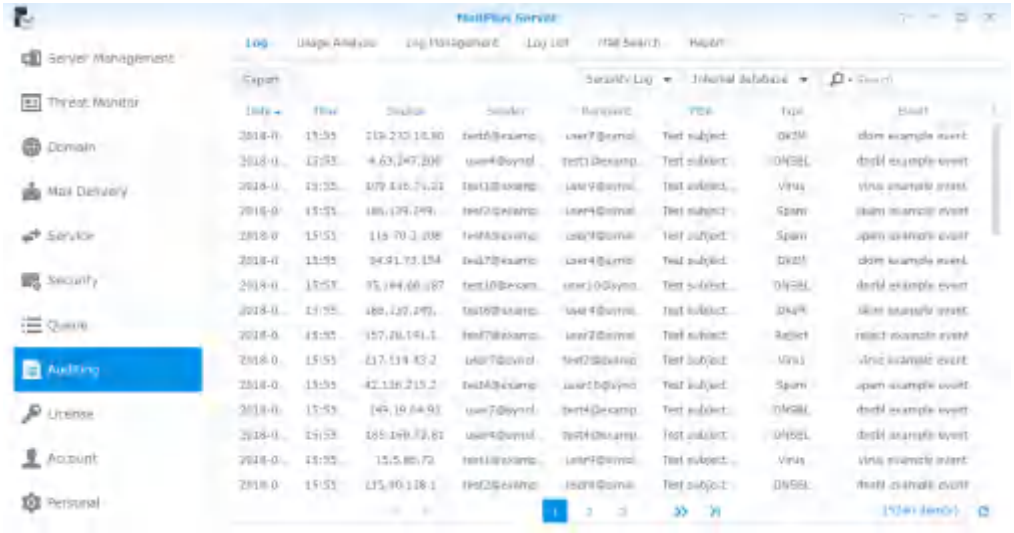
檢視安全性日誌

安全性日誌會顯示事件的產生日期和時間、來源、寄件人、收件人、標題、類別以及事件說明。安全性日誌被分類為以下類型：拒絕、垃圾郵件、病毒、DNSBL、惡意內容、附件過濾器、黑名單、SPF、DKIM、DMARC 以及資料保護，皆與安全性設定中的功能相關，僅拒絕表示經過完整分析後，MailPlus Server 拒絕此封信件。您可以參考以下步驟來檢視安全性日誌：

注意：若您已建立 **High-availability 叢集**，請於主伺服器檢視日誌。

1 前往稽核 > 日誌。

2 從上方的下拉式選單中選擇安全性日誌以及內部資料庫。

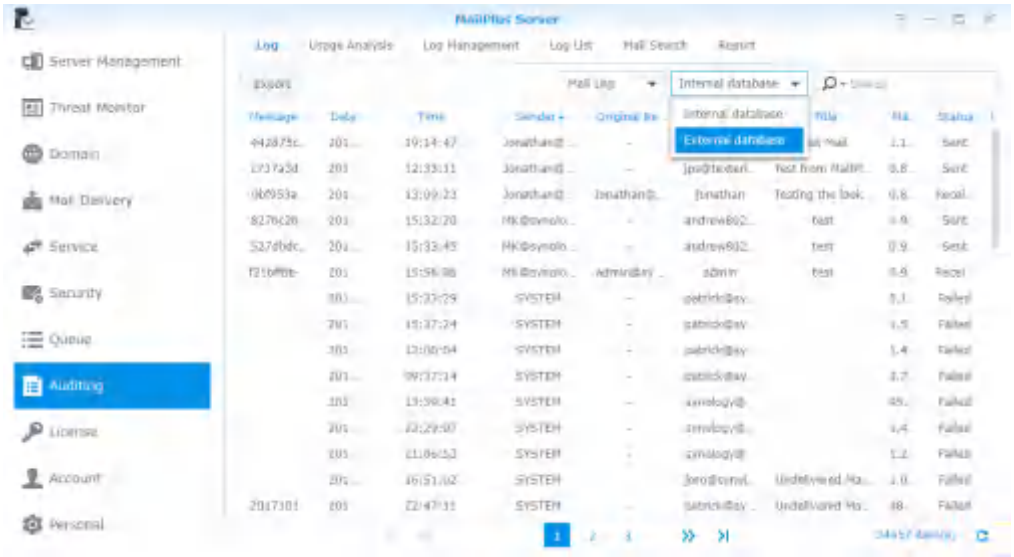


檢視外部資料庫

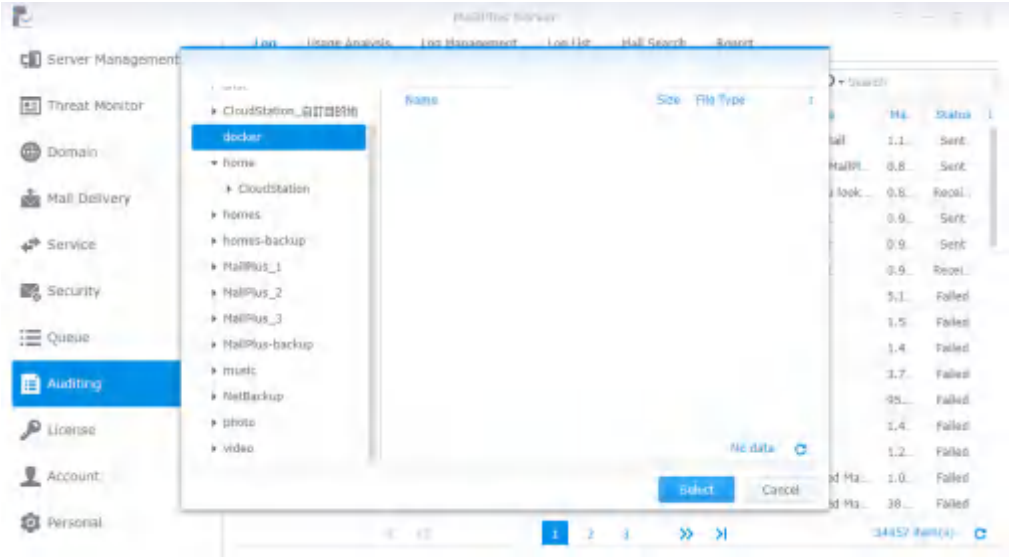
若您有封存日誌、產生日誌資料庫或是下載日誌檔案，您可以透過外部資料庫功能來檢視該資料庫的日誌內容。請參考下列步驟來檢視外部資料庫：

1 前往稽核 > 日誌。

2 從上方的下拉式選單中選擇郵件日誌或安全性日誌，再選取外部資料庫。



3 找到您的外部資料庫在 Synology NAS 上所在位置。

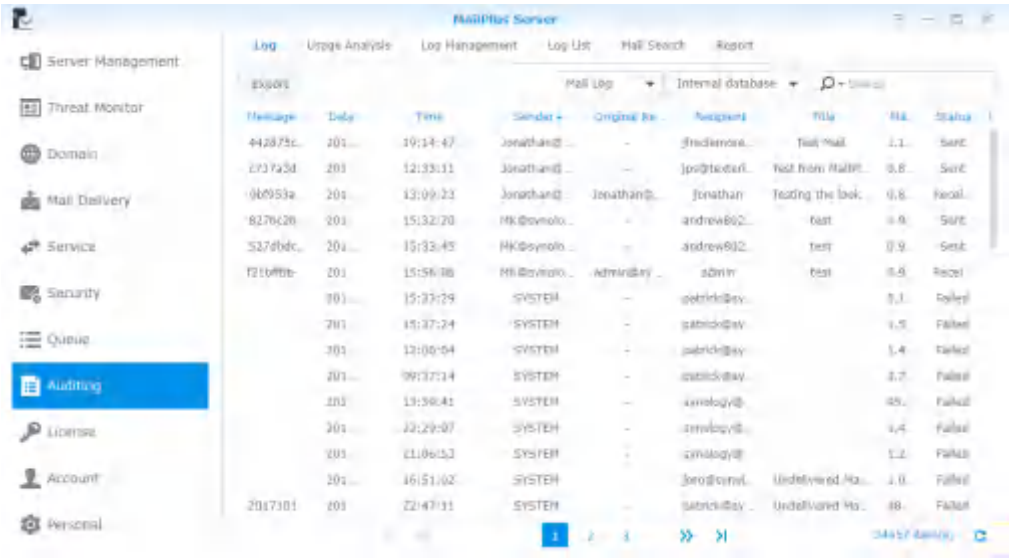


4 按一下**選擇**按鈕。

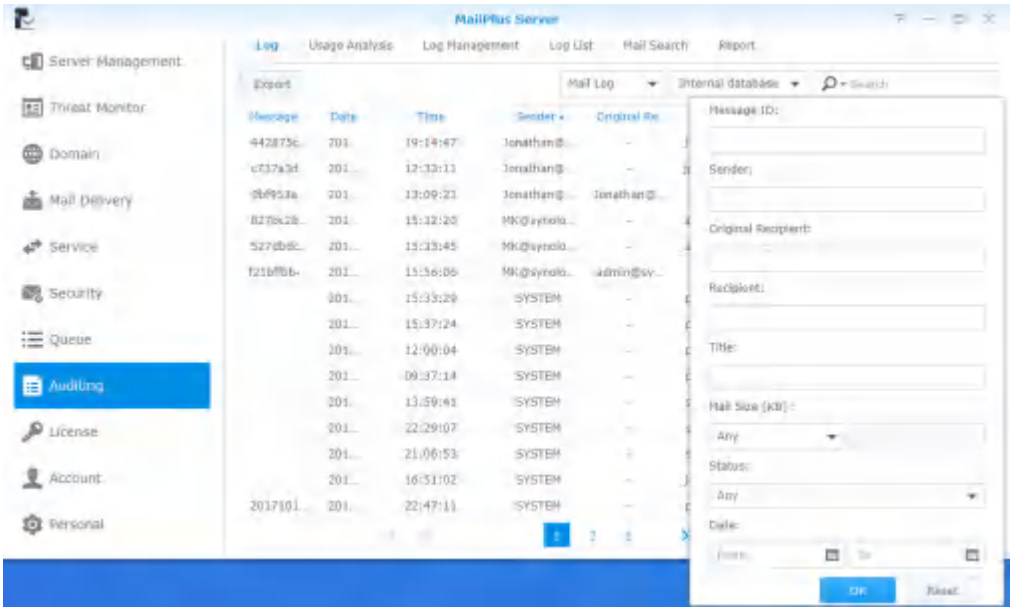
搜尋日誌

在**稽核** > **日誌**，您可以按照各項條件，透過簡易搜尋或進階搜尋來尋找有興趣的日誌內容。

- **簡易搜尋：**在頁面右上角的搜尋欄位中輸入關鍵字。當您檢視郵件日誌時，此關鍵字將會比對 Message ID、寄件人、收件人、標題等欄位。當您檢視安全性日誌時，此關鍵字將會比對來源、寄件人、收件人、標題以及事件等欄位。



- **進階搜尋**：按一下頁面右上角的搜尋欄位中的放大鏡圖示，並設定各個欄位的搜尋條件來進階搜尋，完成後按一下**確認**。您可以在**狀態**下拉式選單中選擇**網域內部**來搜尋那些由 MailPlus Server 上的使用者寄給其他內部使用者的信件。

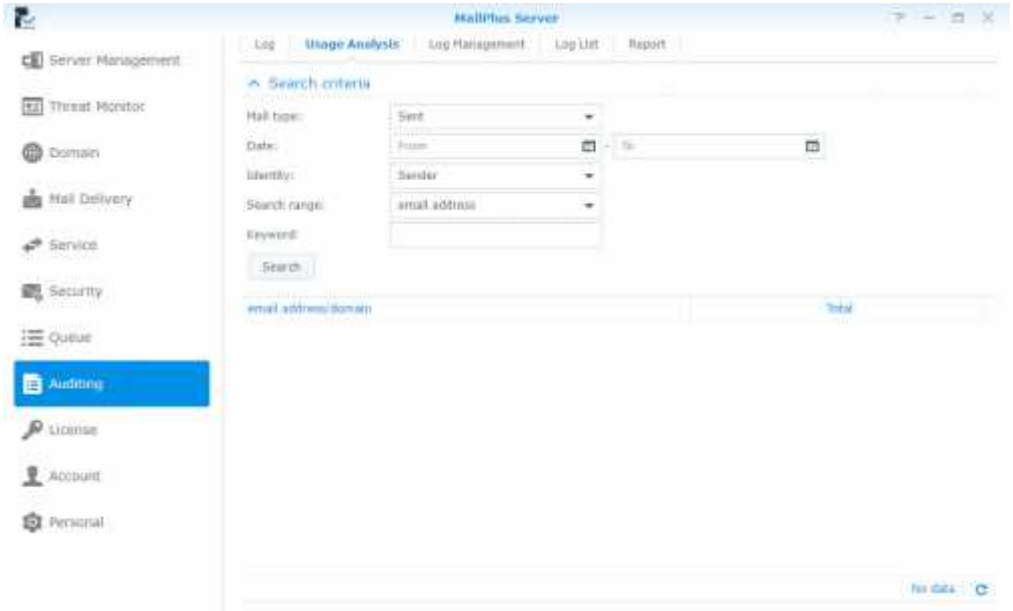


匯出日誌內容

在**稽核** > **日誌**，您可以將日誌匯出為 html 檔案。若您在搜尋後按下**匯出**，將會匯出您目前的搜尋結果。請參考**搜尋日誌**。

使用分析

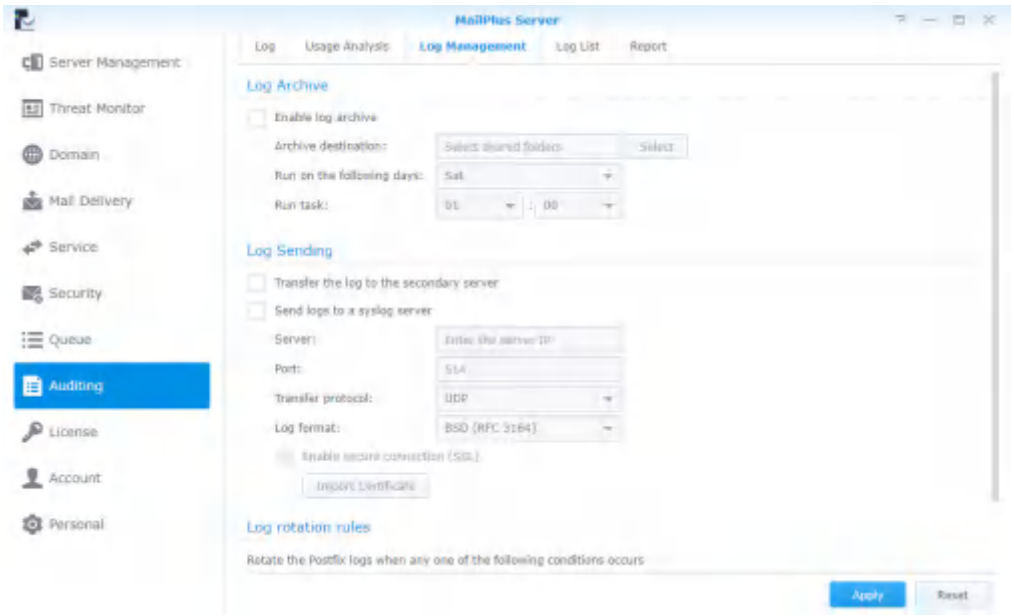
在**稽核** > **使用分析**，您可以進行使用狀況分析，並分析各個電子郵件地址或是電子郵件網域收寄的信件。



封存日誌

您可以設定日誌封存，MailPlus Server 會在您指定的時間，將郵件日誌、安全性日誌以及 Post□x 日誌封存到您所指定的共用資料夾中。若無法存取您的共用資料夾，封存功能將自動停用。請參考以下步驟來封存日誌：

1 前往稽核 > 日誌管理。
2 在日誌封存區塊下勾選啟動日誌封存核取方塊。
3 按一下封存目的地欄位旁的選擇按鈕，並選擇您要存放封存檔案的位置。
4 選擇您要執行封存任務的時間。
5 按一下套用來儲存設定。



傳送日誌到次要伺服器

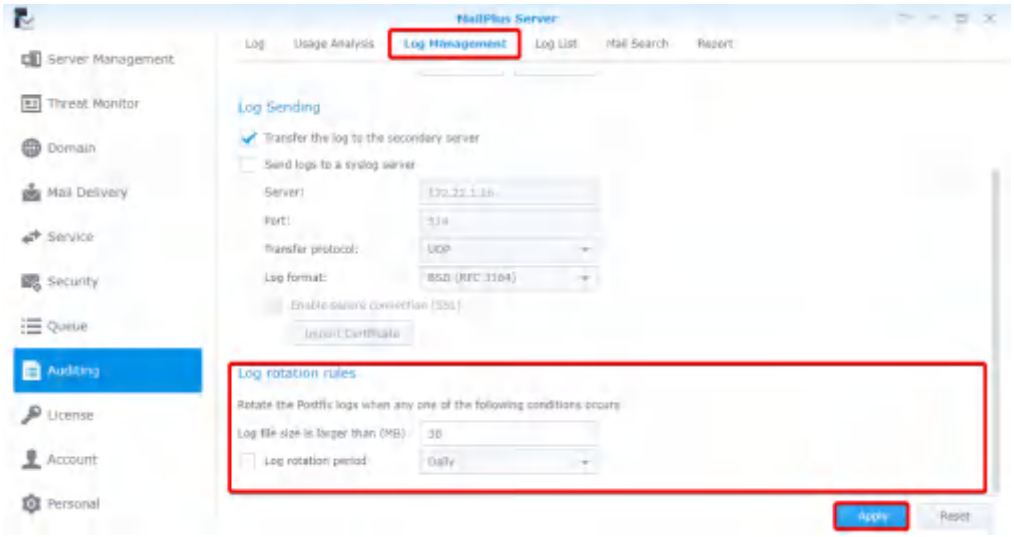
當您完成 High-availability 叢集設置後，日誌會被統一收集到主要伺服器，您亦可選擇傳送一份副本到次要伺服器。您需要產生日誌資料庫才能將日誌的傳送到次要伺服器 (請參考產生日誌資料庫)，之後就可以在稽核 > 日誌檢視外部資料庫。請參考以下步驟將日誌傳送到次要伺服器：

1 前往稽核 > 日誌管理。
2 在日誌傳送區塊下勾選傳送日誌到次要伺服器核取方塊。
3 按一下套用來儲存設定。

將 Post□x 日誌傳送到其他 Syslog 伺服器

請參考以下步驟來將 Post□x 日誌傳送到其他 Syslog 伺服器：

1 前往稽核 > 日誌管理。
2 在日誌傳送區塊下勾選傳送日誌到 syslog 伺服器核取方塊。
3 輸入 Syslog 伺服器組態設定。
4 若您勾選啟動安全連線 (SSL) 核取方塊，您可能需要按一下匯入憑證按鈕來匯入該 syslog 伺服器的憑證，才能正常傳送。
5 按一下套用來儲存設定。



設定日誌輪替規則

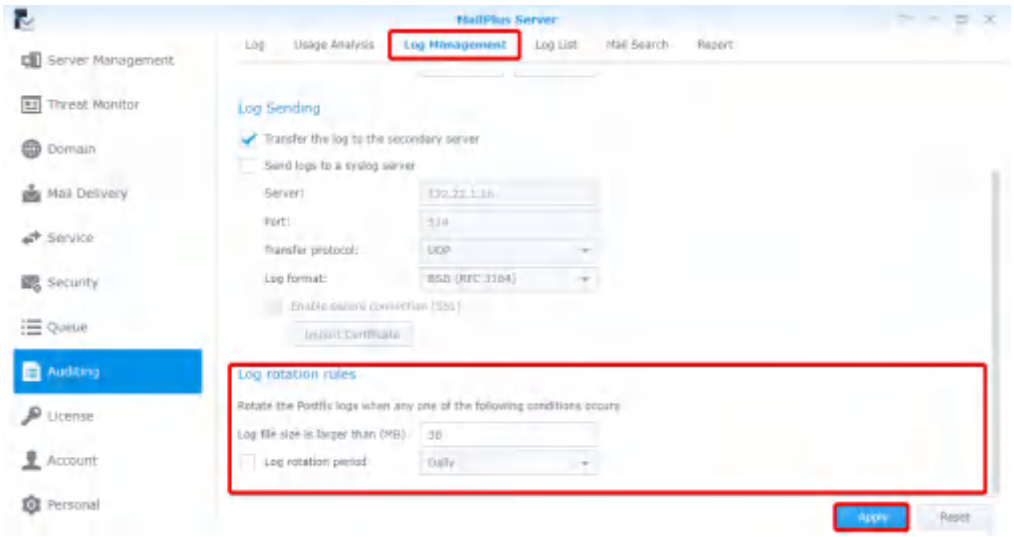
您可以設定 Post□x 日誌的輪替週期以及檔案大小限制，郵件日誌資料庫以及安全性日誌資料庫則會保存最近的四百萬筆資料。請參考以下步驟來設定日誌輪替規則：

1 前往**稽核** > **日誌管理**。

2 在**日誌輪替規則**區塊下的**日誌檔案大小大於 (MB)** 欄位中輸入您的 Post□x 日誌檔案大小上限。

3 在**日誌輪替規則區塊**下勾選**日誌輪替週期**核取方塊，然後從下拉式選單選擇日誌輪替週期的選項。

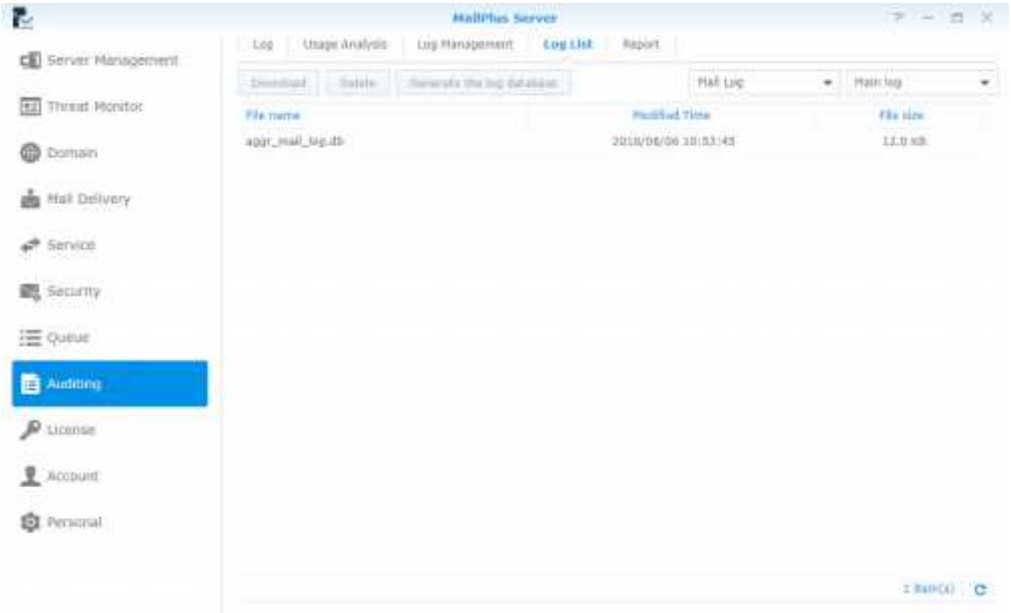
4 按一下**套用**來儲存設定。



下載與刪除日誌檔案

您可以下載保存 MailPlus Server 內的郵件日誌資料庫、安全性日誌資料庫和 Post□x 日誌，您也可以在稽核 > 日誌檢視外部資料庫。請參考以下步驟來下載及刪除日誌檔案：

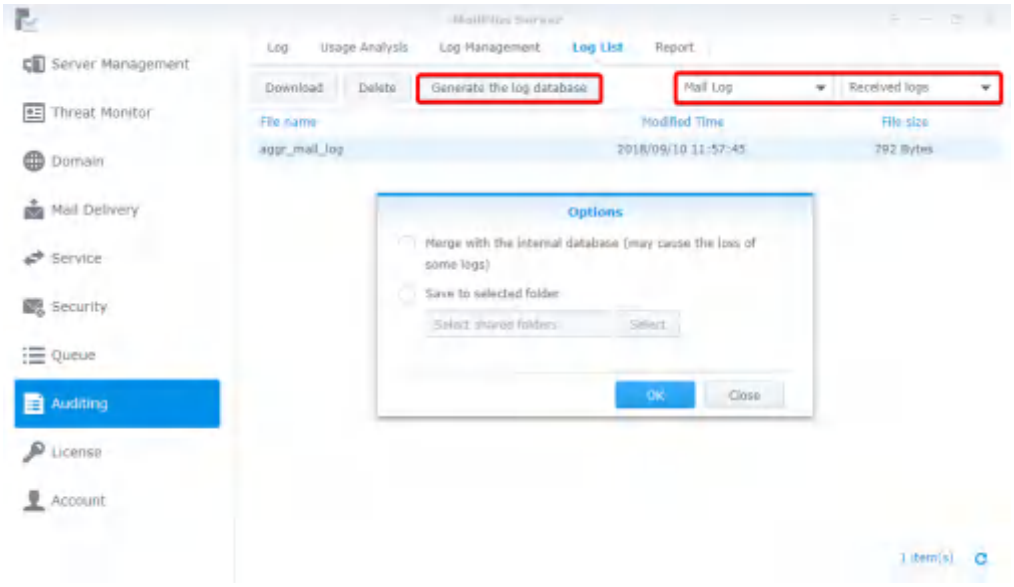
1 前往稽核 > 日誌清單。
2 從上方的下拉式選單中選擇郵件日誌、安全性日誌，或 Post□x 日誌。
3 若您已完成 MailPlus Server High-availability 設置並啟動傳送日誌到次要伺服器 (請參考傳送日誌到次要伺服器)，在次要伺服器上，您可在上方的下拉式選單選擇已接收日誌；否則保持選擇主要日誌。
4 選擇日誌檔案後，您可以按一下下載按鈕來下載檔案，或按一下刪除按鈕將伺服器上的檔案刪除。



產生日誌資料庫

若您已啟動傳送日誌到次要伺服器 (請參考傳送日誌到次要伺服器)，您可以透過產生日誌資料庫功能將接收到的日誌內容轉換回資料庫檔案。您可以在稽核 > 日誌檢視外部資料庫，檢視產生的日誌資料庫檔案。

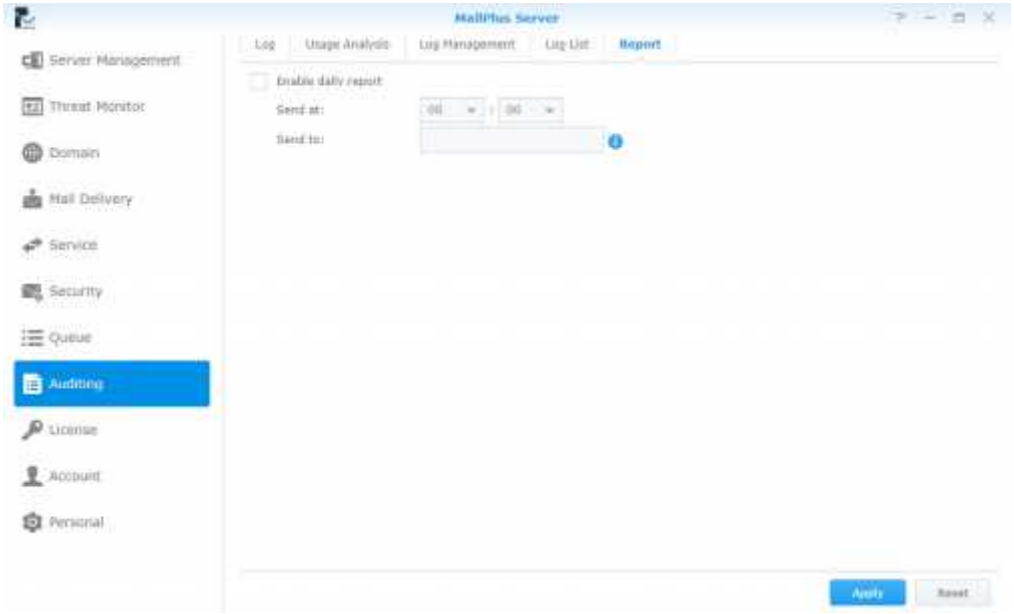
1 前往稽核 > 日誌清單。
2 從上方的下拉式選單中選擇郵件日誌、安全性日誌或 Post□x 日誌。
3 從上方的下拉式選單中選擇已接收日誌。
4 選擇日誌檔案，按一下產生日誌資料庫按鈕。
5 選擇合併至內部資料庫 (可能導致部分日誌遺失) 或儲存至選取的資料夾選項，然後選擇目的地資料夾。
6 按一下確定來完成。



設定每日報表

您可以啟動每日報表功能，MailPlus Server 會將前一天的 Post□x 日誌寄送至指定的郵件地址。請參考以下步驟來設定每日報表：

1 前往稽核 > 報表。
2 勾選啟動每日報表核取方塊。
3 選擇寄送時間。
4 在寄送至欄位中輸入每日報表的寄件地址，您可以指定最多兩個郵件地址，請以分號 (;) 區隔。



災難備援

High-availability 叢集

Synology MailPlus Server 提供兩種解決方案：**單一節點**設置，或 **High-availability** 設置。單一節點設置僅需一台 Synology NAS 來執行郵件服務。High-availability 設置則是以兩台 Synology NAS 組成 High-availability (HA) 叢集，確保在遭遇非預期故障時，郵件服務不中斷。

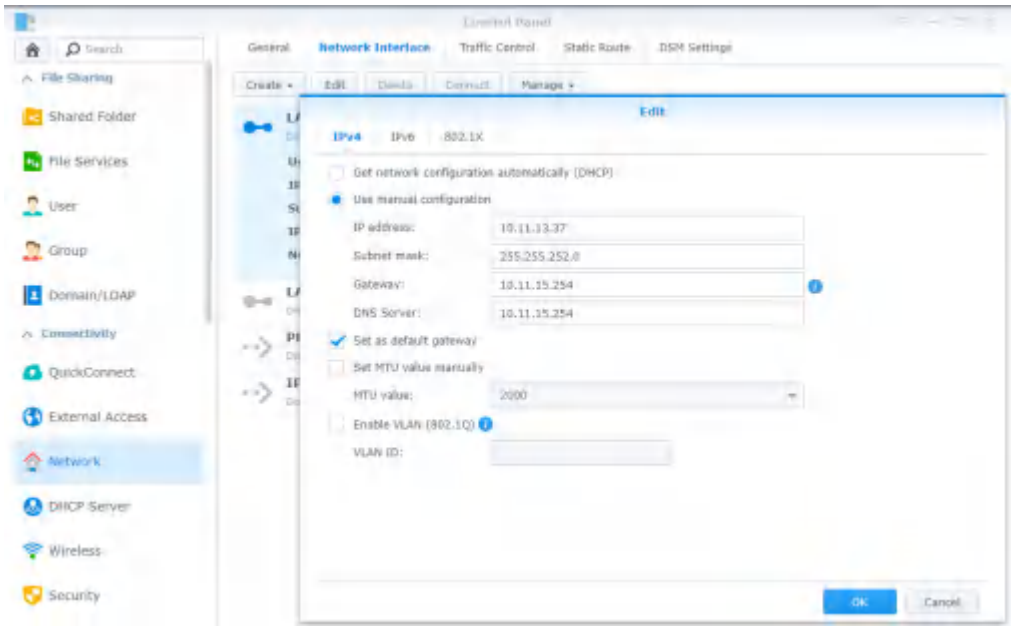
High-availability (HA) 設置介紹

HA 設置使用兩台 Synology NAS 來組成叢集，其中一台擔任「主要伺服器」，另一台則為「次要伺服器」。使用者和其他郵件伺服器連線到 MailPlus Server HA 叢集的主 IP 位址，主要伺服器持有 MailPlus Server HA 叢集主 IP 並接受所有郵件服務請求，此請求會再被分配給主要伺服器或次要伺服器處理，主要伺服器以及次要伺服器上的郵件資料將進行**雙向同步**，不論由主要 / 次要伺服器處理信件請求，最後兩台伺服器上的信件資料將會保持一致，您也可以在任一台伺服器上新增或編輯 MailPlus Server 內的設定，新的設定將會套用到主要伺服器以及次要伺服器上。HA 設置可減少因伺服器故障而造成的服務中斷，當主要伺服器故障時，次要伺服器將會暫時擔任主要伺服器並接手所有郵件服務請求，待主要伺服器回復正常後，這段期間內的郵件資料變動也將同步回主要伺服器上。當次要伺服器故障時，所有的郵件服務請求將由主要伺服器獨自處理，待次要伺服器回復正常後，故障期間內的郵件資料變動也將同步到次要伺服器上。

注意：MailPlus High-availability 叢集與 Synology High Availability (SHA) 為兩個不同的叢集系統，兩者無法同時運作在 Synology NAS 上。若有服務不中斷需求，建議您使用專為郵件服務設計的 MailPlus High-availability 叢集架構，可在 High-availability 叢集恢復正常後，確保伺服器間的郵件資料一致性，避免次要伺服器在 split-brain 錯誤發生期間遺失更新資料。

設置 High-availability (HA) 前的注意事項

- **準備兩台 Synology NAS：**在兩台 Synology NAS 上安裝 MailPlus Server 套件，其中一台 Synology NAS 的 MailPlus Server 必須先初始化，這台 Synology NAS 將擔任「主要伺服器」，請參考**設定 MailPlus Server** 來了解更多設定 MailPlus Server 的資訊。而另外一台 Synology NAS 的 MailPlus Server 則必須保持未初始化的狀態，這台 Synology NAS 將是「次要伺服器」。
- **指定兩組固定 IP 給主要與次要伺服器：**兩台 Synology NAS 的 IP 位址必須位在**相同區域網路**下，該 IP 位址不能是透過 PPPoE 或 DHCP 等方式所取得的，且擁有該 IP 位址的網路介面卡必須設定為**手動設置網路組態**類型。

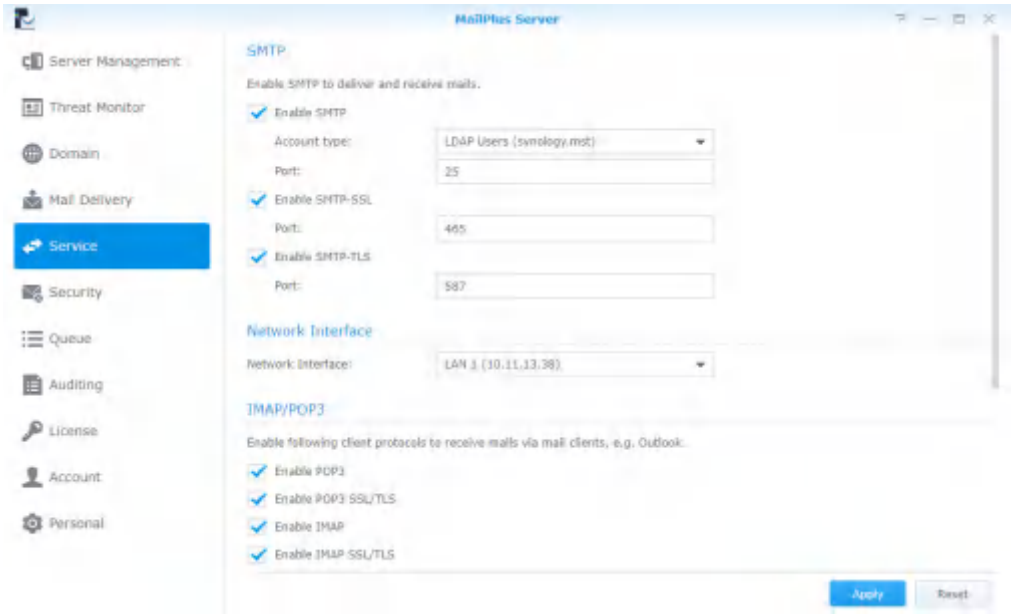


- 次要伺服器必須停用**兩階段驗證**功能。
- **兩台伺服器必須加入同一網域**：兩台 Synology NAS 必須先加入相同的 Windows Active Directory 或 LDAP 伺服器。請參考此篇**應用教學**來了解如何加入 Windows Active Directory。請參考此篇**說明文章**來了解如何加入 LDAP。若您的環境中並沒有 Windows Active Directory 或 LDAP 伺服器，您可以安裝**套件中心**中的 **Active Directory Server** 或 **Directory Server** 來建立自己的 Windows Active Directory 或 LDAP 伺服器，進行帳號管理。
- **準備另一組相同網域的對外 IP**：您必須準備一組與主要 / 次要 Synology NAS 位於相同區域網路下的 IP 位址當做 MailPlus Server HA 叢集的對外 IP，當手動切換或故障造成主要伺服器切換時，使用者仍然能透過此 IP 來存取服務。

設置 High-availability (HA)

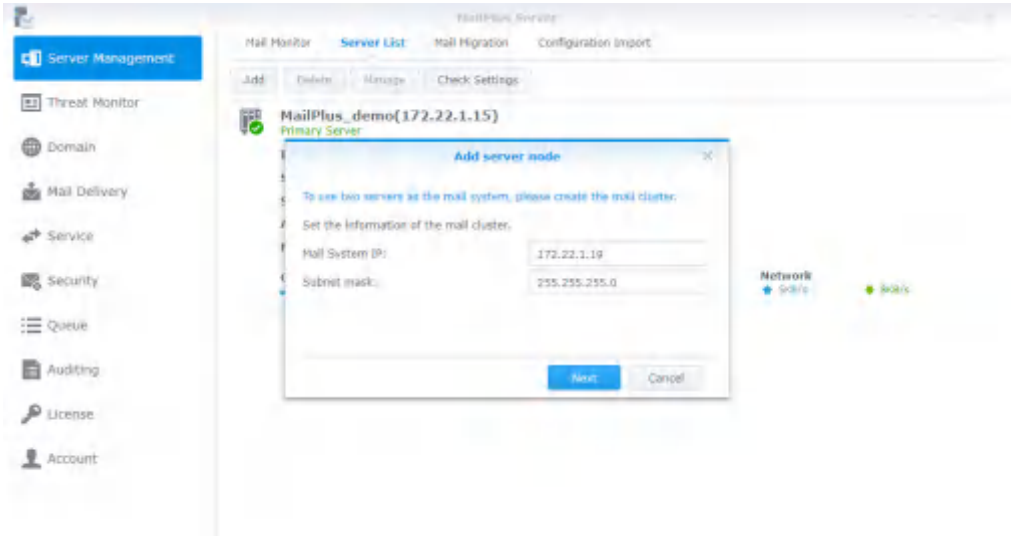
1 開啟已設定好的 **MailPlus Server**。

2 前往**服務**，確認已在 **SMTP** 區塊下的**帳號類型**下拉式選單中選擇**網域使用者**或 **LDAP 使用者**。



3 前往**伺服器管理** > **伺服器列表**，然後按一下**新增**按鈕。

4 輸入 HA 叢集的主要對外 IP 位址，再按一下**下一步**。



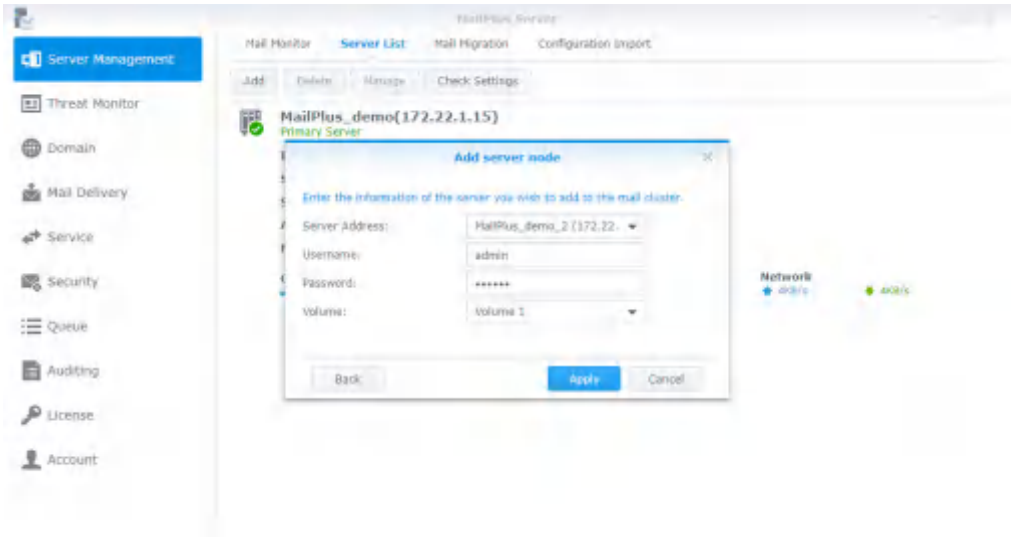
5 在**伺服器位址**欄位中輸入次要伺服器的 IP 位址，或從包含同區域網路內的所有可搜尋 Synology NAS 的**伺服器位址**下拉式選單選擇一台 Synology NAS 作為次要伺服器。

注意：次要伺服器需要綁定一組**網路介面**，您需要輸入綁定網路介面的 IP 位址。

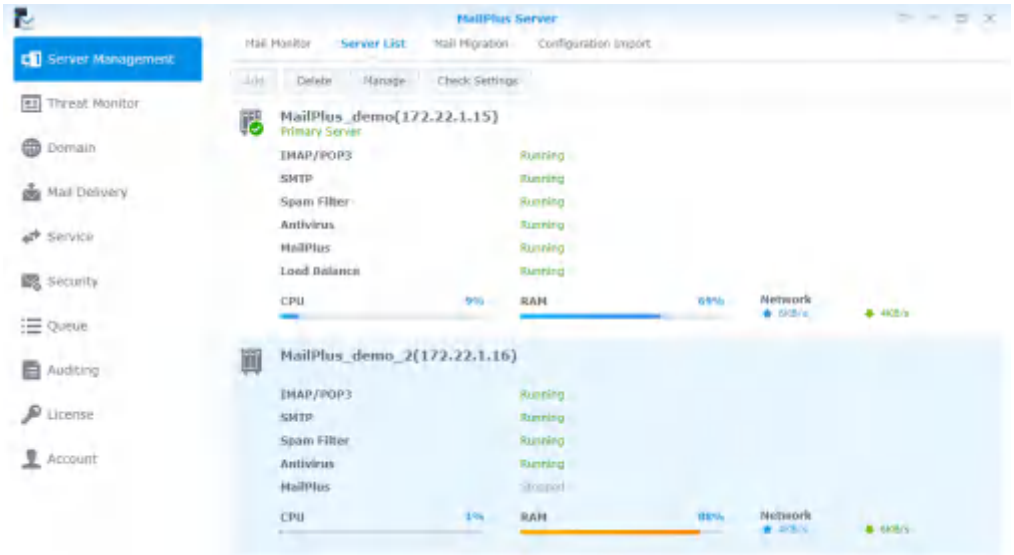
6 在**使用者帳號**和**密碼**欄位輸入次要伺服器的管理員帳號密碼或其他屬於管理員群組的帳號密碼資訊。

7 在**儲存空間**下拉式選單中，將列出次要伺服器上已建立的儲存空間清單，請選擇在次要伺服器上用來儲存信件資料以及 MailPlus 相關檔案的儲存空間。

8 確認設定無誤後，按一下**套用**。



9 設定完成後，信件將會同步到次要伺服器上，**同步所需時間視主要伺服器上的信件數量而定**，在進行信件同步時，您仍可以正常收發信件，此時將由主要伺服器處理所有郵件服務的相關請求，待同步完成後，主要伺服器以及次要伺服器將分擔處理郵件服務的負載。



變更 High-availabilty (HA) 叢集設定

1 開啟已設定好的 **MailPlus Server**。

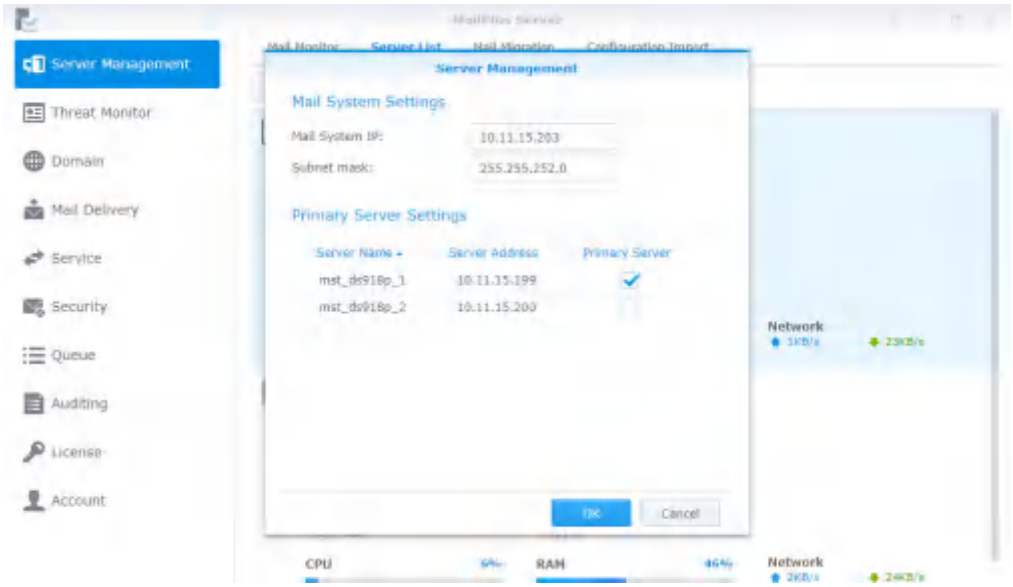
2 前往**伺服器管理** > **伺服器列表**。

3 按一下**管理**按鈕。

4 在**郵件系統設定**區塊當中，您可以變更您的郵件系統 (HA 叢集) IP 位址及其子網路遮罩設定。

注意：您變更後的郵件系統 IP 位址以及子網路遮罩設定跟主要 / 次要伺服器所使用的 IP 位址必須位於同一個子網路中。

5 在主要伺服器設定區塊下，您可以選擇任一 Synology NAS 做為 HA 叢集中的主要伺服器，主要伺服器持有 HA 叢集對外 IP 位址並接受所有郵件服務請求，此請求會再分配給主要伺服器或次要伺服器處理。



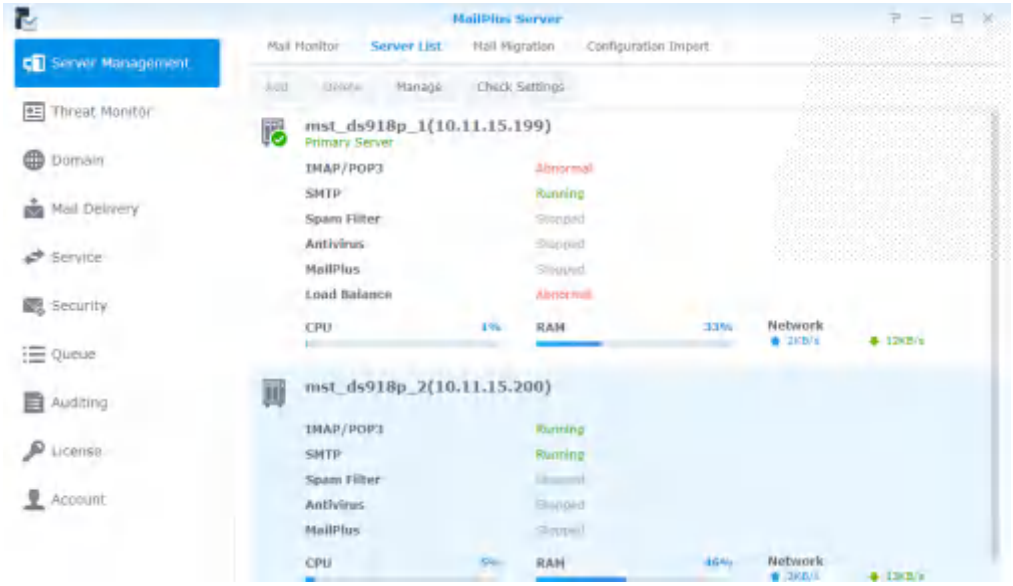
移除 High-availabtility (HA) 設置

解除 HA 設置時，郵件資料將會自動同步一次，確保兩台 Synology NAS 上的郵件資料一致。解除設定後，HA 叢集的對外 IP 位址將不會被任何一台 Synology NAS 所持有，您可能需要調整您的防火牆機器上的連接埠轉送和非軍事區 (DMZ) 設定，或是更動您的 DNS 紀錄。請參考以下步驟來移除 HA 叢集內的其中一台 Synology NAS：

1 登入您欲保留的 Synology NAS 的 **DSM**，開啟 **MailPlus Server**。

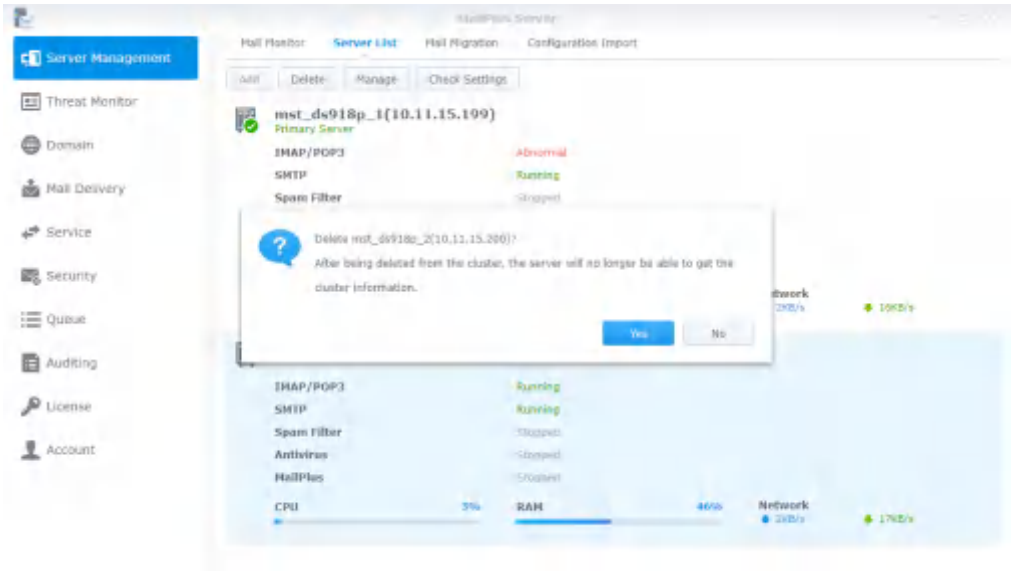
2 前往**伺服器管理** > **伺服器列表**。

3 選擇欲刪除的 Synology NAS。

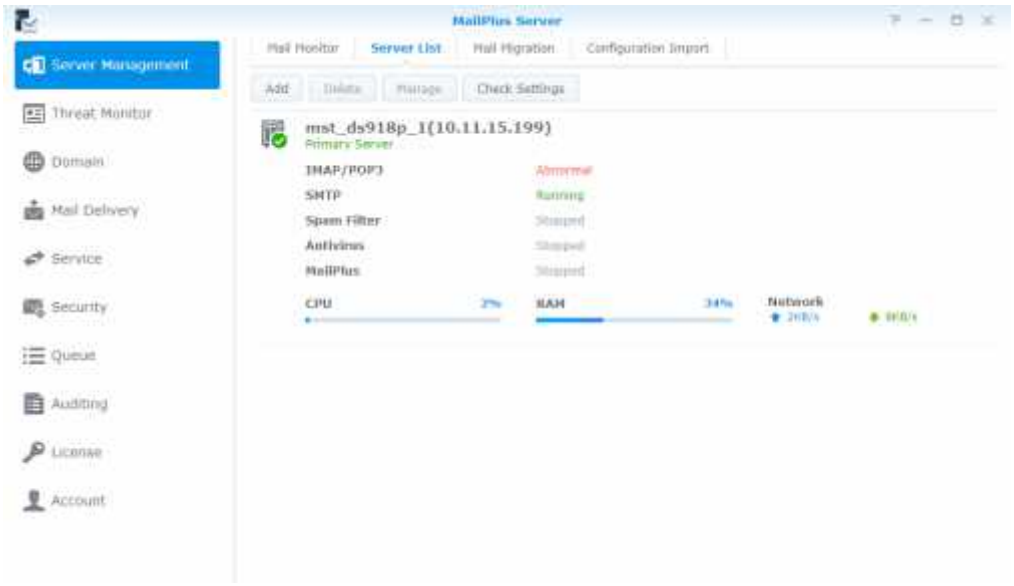


4 按一下**刪除**按鈕。

5 在確認視窗中按一下**是**。



6 信件同步完成後，即完成解除 HA 設置。在信件同步的過程中，您欲保留的伺服器仍然會持續接受以及處理郵件服務請求。請確認是否需要調整防火牆機器上的連接埠轉送和非軍事區 (DMZ) 設定，或是更動您的 DNS 紀錄。

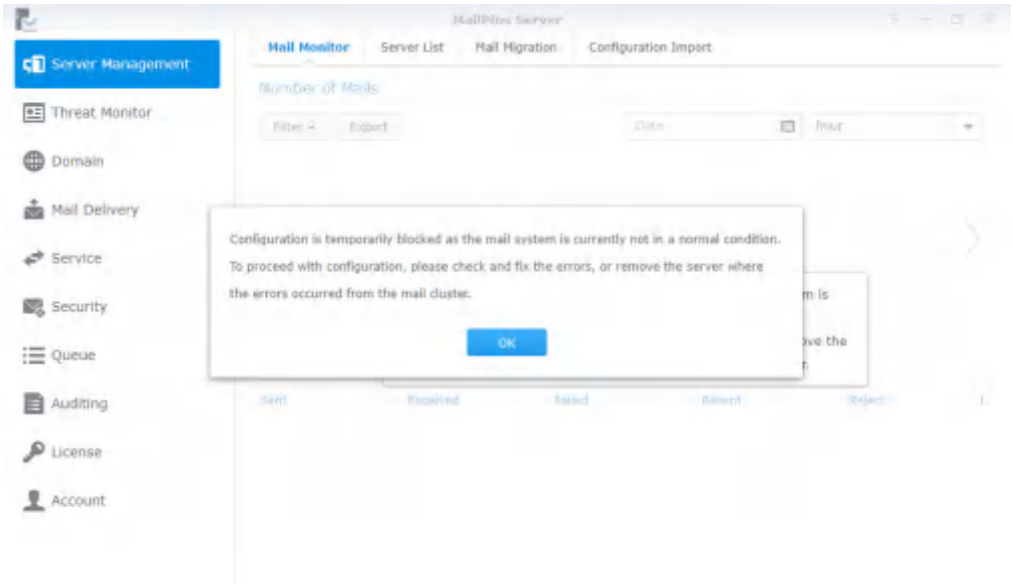


伺服器故障

當 HA 叢集內的 Synology NAS 故障時，若只有一台機器發生故障，另一台機器將持續提供郵件服務。以下所提到的主要伺服器以及次要伺服器指的都是當初在進行 HA 設置時機器所對應的角色，並非是切換伺服器後的角色。

主要伺服器故障

當原始的主要伺服器故障時，原始的次要伺服器會接手 HA 叢集對外 IP 位址，並獨自接受以及處理郵件服務請求，當您開啟原始次要伺服器上的 MailPlus Server 時，會看到郵件系統的警示視窗，且無法進行任何 MailPlus Server 設定的變更，因此請盡速修復您的原始主要伺服器。若原始的主要伺服器已經無法修復，請參考**移除 High-availabtility (HA) 設置**來刪除原始主要伺服器。刪除後，MailPlus Server 將回到**單一節點**設置。



次要伺服器故障

當原始的次要伺服器故障時，原始的主要伺服器將會持有 HA 叢集對外 IP 位址並獨自接受以及處理郵件服務請求，請盡速修復您的原始次要伺服器。若原始的次要伺服器已經無法修復，請參考**移除 High-availabtility (HA) 設置**來刪除原始次要伺服器，刪除後，MailPlus Server 將回到**單一節點**設置。

備份與復原郵件

您可以透過 Synology DSM 的備份功能來備份郵件伺服器，MailPlus Server 的備份包含：

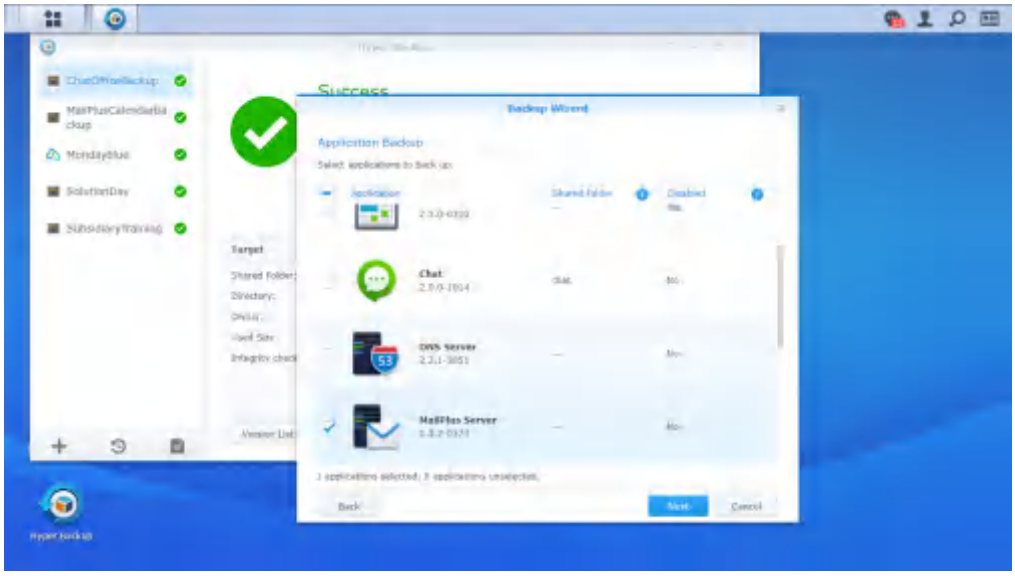
- MailPlus Server **系統設定**備份
- MailPlus Server **信件匣**與**電子郵件**備份

MailPlus Server 當中的系統設定更動較少，因此可使用 **Hyper Backup** 進行排程備份任務；但郵件系統中的信件匣與電子郵件持續在更動，使用排程備份可能因時間間隔而造成資料遺失，因此建議透過**共用資料夾同步**的方式備份。

備份系統設定

使用 **Hyper Backup** 套件，即可備份郵件系統設定至與 MailPlus 相容的 Synology NAS。

1. 在來源 Synology NAS 上開啟 **Hyper Backup**。
2. 按一下左下角的 **+** 來建立資料備份任務。
3. 選擇備份目的地類型：
   - **本地共用資料夾 & 外部儲存空間**：設定將會備份到本地 Synology NAS，或是外接的 USB/SD 儲存裝置。
   - **遠端 Synology NAS**：設定將會備份到遠端 Synology NAS，該遠端目的地上必須安裝、執行 **Hyper Backup Vault** 套件。
4. 輸入其他任務設定來結束設定。請參考**說明文章**來了解更多建立備份任務的相關資訊。
5. 當系統請您選擇要備份的應用程式時，請選擇 **MailPlus Server**。



6 備份任務設定完成並開始順利執行後，下列 MailPlus Server 頁籤內的設定將會被備份：

- 郵件傳送
- 服務
- 安全性
- 稽核
- 授權
- 帳號

備份信件匣與電子郵件

可備份所有信件匣及電子郵件訊息至與 MailPlus 相容的 Synology NAS。請參考以下段落來取得更多資訊。

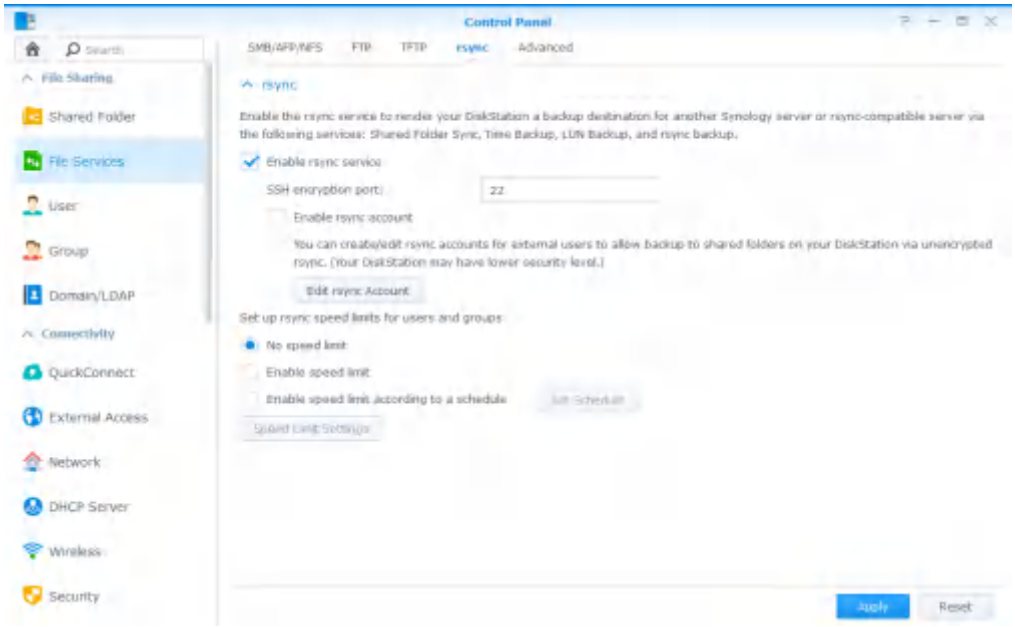
啟動共用資料夾同步

您必須在目的地 Synology NAS 上啟動**共用資料夾同步**。

1 登入 **DSM**。

2 前往**控制台** > **檔案服務** > **rsync**。

3 勾選**啟動 rsync 服務**核取方塊來啟動**共用資料夾同步**。



4 按一下**套用**。

新增同步任務

登入來源 Synology NAS，並參考以下步驟來新增同步任務：

1 前往**控制台** > **共用資料夾同步**，按一下**任務清單**按鈕。
2 在**任務清單**視窗中按一下**新增**按鈕。
3 在**任務名稱**欄位中輸入任務的名稱。
4 選擇您欲同步至目的地的共用資料夾。
5 指定目的地 Synology NAS 及下列同步選項：
- **自訂 SSH 加密連接埠**：指定 SSH 傳輸加密的連接埠。
- **啟動資料傳輸加密**：傳輸資料時進行資料加密。此選項提供較高的安全性，但非加密傳輸的效能較佳。您可根據個人需要選擇。
- **啟動傳輸壓縮**：傳輸資料時進行資料壓縮。此選項可節省頻寬，但會增加 CPU 工作量。
- **啟動段落分塊 (block-level) 同步化**：僅同步資料修改的部分，而非整個檔案。此選項可節省頻寬，但會增加 CPU 工作量。

6 請依提示，選擇下列任一選項，決定何時要從來源同步至目的地：
- **資料異動時自動進行同步**：來源共用資料夾的資料有改變時立即執行同步。
- **手動執行同步化**：手動從來源共用資料夾執行同步任務。
- **進階排程**：按一下**設定排程**，指定何時執行同步任務。

7 按一下**套用**。現在，可在任務清單上看到同步任務，系統會根據指定的排程執行任務。

管理同步任務

登入來源端 Synology NAS，並參考以下步驟來管理同步任務：

1 前往**控制台** > **共用資料夾同步**，按一下**任務清單**按鈕。
2 在**任務清單**視窗中選擇任務，並執行下列任何操作：
- 按一下**編輯**按鈕來編輯任務。
- 按一下**刪除**按鈕來刪除任務。
- 如果同步任務尚未進行，請按一下**立即同步**按鈕來立即執行任務。
- 如果同步任務正在進行，請按一下**取消**按鈕來停止正在進行的任務。
- 第一次執行同步任務時，**共用資料夾同步**會執行**完整同步**。第一次同步完成之後，僅會同步變更的部份，按一下此按鈕可以讓您再次手動同步所有資料。

注意：
1. 如果同步任務的排程是設定為**資料異動時自動進行同步**，按一下**取消**會停止進行中的同步任務。然而，如果同步任務監控的任何共用資料夾內容改變，**共用資料夾同步**會繼續進行同步任務。
2. 請勿使用 Cloud Station Server 套件進行備份。其雙向同步運作方式可能導致資料損毀。
3. 如果目的地上已存在 **MailPlus** 共用資料夾，備份完成後，該資料夾將被重新命名為 **MailPlus_1**。
4. 若要使用 **MailPlus_1** 內的資料，請手動將資料移動到 **MailPlus** 共用資料夾。
5. 若要避免帳號錯誤，請將目的地連接到來源所使用的目錄伺服器 (例如：LDAP 伺服器或 Windows Active Directory 網域)。

還原系統設定、信件匣與電子郵件

前往目的地 Synology NAS，在其本地共用資料夾內已儲存設定、信件匣及電子郵件備份。請參考以下步驟來還原系統設定、信件匣，及電子郵件：

1 開啟 **Hyper Backup**。
2 從本地共用資料夾還原備份的設定，請參考此篇**說明文章**來了解更多資訊。
3 還原完成後，目前的 MailPlus Server 設定皆會被覆寫。
4 備份的信件匣及電子郵件可立即使用，不須進行還原。
5 聯絡 **Synology 技術支援**來從來源 Synology NAS 移轉 MailPlus Server 授權至目的地 Synology NAS。
6 移轉授權後，目的地便會開始執行郵件服務。

注意：目前備份及還原功能支援 MailPlus Server 1.0-164 (或以上版本) 搭配 DSM 6.0 (或以上版本) 環境。