

# 管理手冊

# Synology MailPlus Server

—

基於

Synology MailPlus Server 2.3



# 目錄

|                                             |    |
|---------------------------------------------|----|
| 簡介                                          | 01 |
| 第 1 章：部署指南                                  | 02 |
| 選擇 Synology NAS 機種                          |    |
| 預估所需的記憶體及儲存容量                               |    |
| 在同一台 NAS 上執行多個 I/O 密集型套件                    |    |
| 第 2 章：開始使用 MailPlus Server                  | 06 |
| 將 Synology NAS 連線至網際網路                      |    |
| 設定 DNS                                      |    |
| 設定 MailPlus Server                          |    |
| 設定 MailPlus 用戶端                             |    |
| 執行 MailPlus                                 |    |
| 第三方電子郵件用戶端                                  |    |
| 疑難排解                                        |    |
| 第 3 章：郵件移轉                                  | 19 |
| 在 MailPlus Server 新增郵件轉移任務                  |    |
| 將 Microsoft Exchange 系統設定匯入 MailPlus Server |    |
| 第 4 章：使用者授權                                 | 27 |
| 購買授權                                        |    |
| 安裝授權                                        |    |
| 使用者授權                                       |    |
| 第 5 章：帳號設定                                  | 31 |
| 帳號系統                                        |    |
| 啟動帳號                                        |    |
| 管理權限                                        |    |

|                    |     |
|--------------------|-----|
| 第 6 章：協定設定         | 47  |
| SMTP               |     |
| IMAP / POP3        |     |
| 網路介面               |     |
| 第 7 章：SMTP 設定      | 52  |
| 服務設定               |     |
| SMTP 安全連線          |     |
| 郵件轉送               |     |
| 第 8 章：網域設定         | 68  |
| 網域                 |     |
| 網域管理               |     |
| 第 9 章：安全性設定        | 85  |
| 防垃圾郵件              |     |
| 防毒掃描               |     |
| 身分認證               |     |
| 資料保護               |     |
| 內容掃描               |     |
| 第 10 章：監控設定        | 107 |
| 監控伺服器狀態            |     |
| 監控郵件佇列             |     |
| 監控郵件日誌             |     |
| 第 11 章：災難備援        | 127 |
| 高可用叢集              |     |
| 備份及還原信件            |     |
| 第 12 章：MailPlus 導覽 | 139 |
| 基本操作               |     |
| 進階設定               |     |



# 簡介

Synology MailPlus 套件組合提供進階且高可用性的安全郵件服務，該組合包含兩個套件：MailPlus Server 和 MailPlus。MailPlus Server 為提供多樣性設定的管理控制台；而 MailPlus 則是專為用戶端設計的郵件平台。

本管理手冊將引導您完成 MailPlus Server 的架設與細部設定，並提供 DNS 相關設定、舊有郵件服務移轉及其他安全性設定的調整。此外，為了讓您的 MailPlus 發揮最大效用，本手冊亦會說明以下主要功能：為穩定且不中斷的郵件服務所設計的 MailPlus 高可用架構、用以管理延遲郵件的郵件佇列、顯示 MailPlus 健康狀態的監控面板。



# 第 1 章：部署指南

本章節將說明部署 MailPlus 的最佳作法以確保郵件服務的穩定及效能，並將說明以下問題：如何為 MailPlus 選擇合適的 Synology NAS 機種、如何預估所需的記憶體及儲存容量、使用 SSD 快取的注意事項、在同一台 NAS 上同時執行 MailPlus 與多個 I/O 密集型套件的建議事項。

## 選擇 Synology NAS 機種

Synology 提供多款不同規格、功能、能力的 NAS 機種，但並非所有的機種皆適合使用 MailPlus Server。請參閱以下說明來挑選符合您需求的 Synology NAS 機種：

1. 您可以在 [MailPlus 授權頁面](#) 中檢視可支援的裝置清單，此清單將以最大同時上線人數及伺服器最大效能來分類 Synology NAS。
  - 最大同時上線人數為建議的 MailPlus 使用者數量上限。
  - 伺服器最大效能為每日 MailPlus Server 可處理的電子郵件數量上限。
2. 請參閱 [Synology 產品頁面](#) 來取得所有支援 MailPlus 的機種清單，並按一下欲檢視的機種以查看其詳細規格。

### 注意：

- 各項數據皆在 Synology 實驗室中測得，測試環境如下：
  - 測試最大同時上線人數時，CPU 及記憶體使用量均為 80% 以下。
  - 可擴充記憶體的機種皆已將記憶體容量加裝至上限。
  - 2 顆硬碟槽且配備雙 M.2 硬碟插槽的機種，皆已安裝兩顆 SSD 並配置為 SSD 快取。
  - 4 顆硬碟槽以上的機種皆已安裝兩顆 SSD 並配置為 SSD 快取。
  - FS 系列機種皆已安裝 12 個 SSD 並配置為 RAID F1。
  - 在 High Availability 模式下，由於兩台伺服器之間會同步資料，因此郵件系統的效能會略為下降。
  - 執行測試時已啟用下列功能：防垃圾郵件、防毒、DNSBL、灰名單、內容掃描、全文檢索（僅適用於英文）。
- 實際限制依系統配置而異，如欲達到相同效能，建議您加裝 SSD 並擴充記憶體。

## 預估所需的記憶體及儲存容量

諸多因素可能影響 NAS 的記憶體使用量，依據使用者的數量，建議的記憶體大小如下：

- 少於 250 位使用者：至少 8 GB 記憶體
- 250 至 500 位使用者：至少 16 GB 記憶體
- 500 至 1000 位使用者：至少 32 GB 記憶體
- 多於 1,000 位使用者：至少 64 GB 記憶體

### 預估記憶體使用量

記憶體使用量主要依據郵件服務的使用者數量而定，然而下列服務也可能會提高記憶體使用量：

- **防垃圾郵件**：Rspamd (預設的 MailPlus 防垃圾郵件引擎) 可能占用大量記憶體。
- **防毒引擎**：防毒服務 (例如：ClamAV 及 McAfee) 可能占用大量記憶體，特別是將離線病毒資料庫更新至最新版本時。
- **MailPlus 網頁用戶端**：當網頁用戶端在讀取郵件或儲存郵件草稿時，可能會同時對 MailPlus Server 發出多個請求。若使用者數量超過 Synology NAS 產品規格標示的**最大同時上線人數**，在 MailPlus Server 嘗試處理所有用戶端的請求時，記憶體使用量可能會突然飆升。

### 預估所需的儲存空間容量

您可以依照下列公式來預估 MailPlus 所需的儲存空間大小：

- 預估儲存空間大小 = [(每日收發電子郵件平均數量)\*(電子郵件平均大小)\*(使用者數量)\*(天數)]

電子郵件平均大小為 300 KB，每人每日平均收發的電子郵件為 100 封，而郵件服務通常會持續三到五年。

舉例來說，若 MailPlus 支援 200 位使用者，則所需的儲存空間大小為：

$$100 \text{ (每日收發電子郵件平均數量)} * 300 \text{ KB (電子郵件平均大小)} * 200 \text{ (使用者數量)} * 1095 \text{ (三年總天數)} \\ = 6.12 \text{ TB}$$

若您在計算所需儲存空間時遇到困難，請[聯絡我們](#)以取得建議。

### 使用 SSD 快取

SSD 快取可將經常存取的資料 (又稱熱資料) 暫時存放在部分或全部的 SSD 上，藉此提升系統效能。

MailPlus 會頻繁地讀取及寫入訊息，因此需要將小型檔案隨機地讀寫至硬碟。由於郵件平均大小相對較小，若將檔案存放在 SSD 快取中，讀寫速度將會明顯提升，即使僅存放部分檔案亦然。加裝 SSD 並利用 Synology SSD 快取能提升郵件服務的整體效能。

#### 注意：

- 企業級使用者若要取得最佳效能，必須使用 SSD 快取。
- 若要取得最佳效能，強烈建議您使用 FS 系列的 NAS 機種，並全數使用 SSD 來建立儲存空間。

## SSD 快取大小建議

SSD 適用於不同用途，選擇適合系統使用的 SSD 時，請一併考量以下條件：耐寫度、效能穩定性、斷電保護。

Synology SSD 為企業型 SSD，專為全年無休的 NAS 環境而打造，經過嚴謹的測試與驗證以確保與 Synology 系統間的相容性。此外，透過密集的 I/O 讀寫、頻繁的斷電與重啟、溫度測試，確保 Synology SSD 可為企業環境——尤其是重要服務如郵件伺服器——提供可靠且穩定一致的效能。

除了 Synology SSD，Synology 亦測試及驗證其他**第三方 SSD**。SSD 的效能可能因製造商而異。

若要了解更多關於為您的 SSD 快取選擇適合 SSD 的資訊，請參考[此文章](#)。

## SSD 快取大小建議

SSD 快取的實際大小取決於儲存空間上的熱資料數量，您至少需要兩顆 SSD 以組成 RAID 1 / 5 / 6 / 10 備援硬碟並使用讀寫快取，例如：若要建立 480 GB 的讀寫快取，需要至少兩顆相同的 480 GB SSD。

熱資料會暫存於 SSD 中，MailPlus Server 的熱資料主要為最近被存取，且經常被存取的郵件，通常約佔郵件服務儲存空間容量的 3% 至 6%。

- 例如：1 TB 郵件儲存空間內，熱資料的大小約為： $1,024 \text{ GB} \times 6\% = 61.4 \text{ GB}$

然而，SSD 快取容量需大於實際熱資料的大小以確保效能，因此 SSD 快取的實際容量應為熱資料預估大小的兩倍。

- 以上述例子而言，理想的快取大小為： $61.4 \text{ GB} \times 2 = 122.8 \text{ GB}$ 。

在此情況下，480 GB 的 SSD 快取已符合最低需求。

依據使用者數量，下列為建議的 SSD 快取預估大小：

- 少於 500 位使用者：480 GB\*2
- 500 至 1,000 位使用者：1 TB\*2
- 多於 1,000 位使用者：2 TB\*2

若您已有一台 Synology NAS，可透過**儲存空間管理員**的 SSD 快取建議來計算熱資料及合適的快取大小。

### 注意：

- 若要了解更多有關 SSD 快取的資訊，請參閱以下文章及文件：
  - [SSD 快取說明文章](#)
  - [使用 Synology SSD 快取的常見問題](#)
  - [白皮書：使用 Synology SSD 技術提升效能](#)
- 即使 MailPlus 的使用者數量未達產品規格標示的**最大同時上線人數**，仍建議您使用 SSD 快取以提升郵件處理速度。

## 在同一台 NAS 上執行多個 I/O 密集型套件

為確保效能及資料安全性，並有效地進行部署，應避免將 MailPlus Server、Synology Drive Server、Synology Chat Server 等 I/O 密集型套件安裝在同一台 Synology NAS 上，前述套件皆會消耗大量的 I/O 資源，且不同服務相互爭奪資源容易導致系統錯誤。然而，若並非所有套件皆為 I/O 密集型服務，Synology NAS 便能夠同時執行多項服務，例如：MailPlus Server 及 Synology Drive 應避免安裝在同一台 NAS 上，但 Synology Calendar 非 I/O 密集型服務，因此可與 MailPlus 同時執行。

## MailPlus Server 連接埠

MailPlus Server 的服務有指定的連接埠，請使用[此表格](#)以檢查並確認這些連接埠未用於其他服務。

# 第 2 章：開始使用 MailPlus Server

MailPlus Server 讓您的 Synology NAS 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。MailPlus 則為 DSM 使用者提供一個易於使用的網頁版郵件用戶端，方便您檢視、管理、傳送訊息。

本章節將引導您執行 MailPlus Server 及 MailPlus。

## 將 Synology NAS 連線至網際網路

Synology NAS 可透過以下三種方式連線至網際網路：直接連線、PPPoE 連線、路由器連線。如需透過網際網路存取 Synology NAS 的詳細資訊，請參考[此應用教學](#)。

對郵件系統而言，擁有靜態外部 IP 位址相當重要。雖然使用動態 IP 位址亦可架設郵件系統，但靜態 IP 位址可使伺服器更加穩定可靠。因此，建議您為郵件系統註冊一組靜態外部 IP 位址。若要了解更多資訊，請聯絡您的網路服務供應商 (ISP)。

### 設定固定 IP / PPPoE

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

- **PPPoE**：部分網路服務供應商 (ISP) 會提供免費固定 IP 位址，但用戶需要透過 PPPoE 連線以取得該固定 IP 位址的使用權。
  1. 登入 DSM。
  2. 前往**控制台 > 網路**。
  3. 在**網路介面**頁籤選擇 **PPPoE**，按一下**編輯**按鈕。
  4. 設定您要連接到數據機的網路埠。
  5. 輸入網路服務供應商 (ISP) 提供的使用者帳號與密碼。
- **固定 IP 位址**：若您已經擁有一組固定 IP 位址，可以直接將其輸入 Synology NAS。
  1. 登入 DSM。
  2. 前往**控制台 > 網路**。
  3. 在**網路介面**頁籤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 MailPlus Server，您需要一個有效且已註冊的網域名稱。電子郵件地址包含兩個部分，位於 @ 符號前方為使用者名稱，後方則為網域名稱。舉例來說，Alex 的電子郵件地址是「alex@example.com」，他的網域名稱即為「example.com」。為確保電子郵件地址「alex@example.com」能夠成功收發郵件，您必須設定 MX 記錄以及 A 記錄。您可以在網域供應商所提供的 DNS 伺服器上建立記錄。

### MX 記錄

MX 記錄，或稱郵件交換記錄 (Mail Exchanger record，MX record)，標示網際網路應如何透過簡單郵件傳輸協定 (Simple Mail Transfer Protocol，SMTP) 將電子郵件導引至目的地。每一筆 MX 記錄都包含主機名稱與優先順序數值，主機名稱指出郵件應抵達的正確伺服器，優先順序數值則指出各伺服器間的排序，數值越低者其優先度越高。

若您的網域內有多台郵件伺服器，您可以建立多筆 MX 記錄，並設定其優先順序數值。主要伺服器的優先順序數值應為最低 (例如：0)，以確保該郵件伺服器能在第一時間回應請求。當主要伺服器未回應請求時，網際網路便會依照優先順序數值的高低，逐一嘗試用以備援的其他伺服器。

舉例來說，若要確保 alex@example.com 能成功收發郵件，您必須將 MX 記錄指向負責接收 example.com 網域郵件的伺服器。因此，請將編輯中的網域填於主機欄位，並將 MailPlus Server 的主機名稱填於指向欄位。主要伺服器的優先順序數值應等於或近於零。

| 主機          | 指向               | 優先順序 |
|-------------|------------------|------|
| example.com | mail.example.com | 0    |

如此一來，example.com 的 MX 記錄查詢結果即是 mail.example.com。

當 MX 記錄查詢找到郵件伺服器後，網際網路會需要確切的 IP 位址來定位郵件的寄送目的地，因此你需要為郵件伺服器設定 A 記錄。

### A 記錄

A 記錄，或稱位址記錄 (Address record，A record)，用於將網域或子網域指向主機 IP 位址。當使用簡單易記的網域名稱時，網際網路能透過 A 記錄來辨識 IP 位址。

以 alex@example.com 為例，mail.example.com 為 example.com 的子網域，而主機則為執行 MailPlus 的 Synology NAS。

| 主機名稱             | 指向 IP 位址        |
|------------------|-----------------|
| mail.example.com | 111.116.172.181 |

| Type | Name             | Value           | TTL         |
|------|------------------|-----------------|-------------|
| A    | mail.example.com | 122.116.172.181 | 600 seconds |
|      |                  |                 |             |
|      |                  |                 |             |
|      |                  |                 |             |
|      |                  |                 |             |

**MX**

**Host \***  **Points to \***  **Priority \***

**TTL \***

範例與截圖僅作為參考之用。每家供應商的 DNS 記錄設定介面皆有所不同，若您在設定 DNS 記錄上遇到問題，請聯絡您的網域供應商。

## 設定反向 DNS

將 DNS 記錄指向網域名稱的過程稱為**正向 DNS**，可將網域名稱指向正確的伺服器。然而，除了正向 DNS 之外，還需要進行反向的設定，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，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。反向 DNS 亦可由 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？

反向 DNS 是架設郵件系統的必要設定之一，通常用於過濾垃圾郵件，以判斷郵件的來源 IP 位址是否為通過驗證的網域名稱；若其 IP 位址並非來自於可靠的網域，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郵件將會被大部分主要電子郵件供應商封鎖。若您無法自行設定反向 DNS，郵件發送又持續發生問題，請新增另一個 SMTP 伺服器以正常寄出郵件。建議您使用知名的 SMTP 伺服器，以免在寄送郵件時被視為垃圾郵件而封鎖。

### 如何設定反向 DNS？

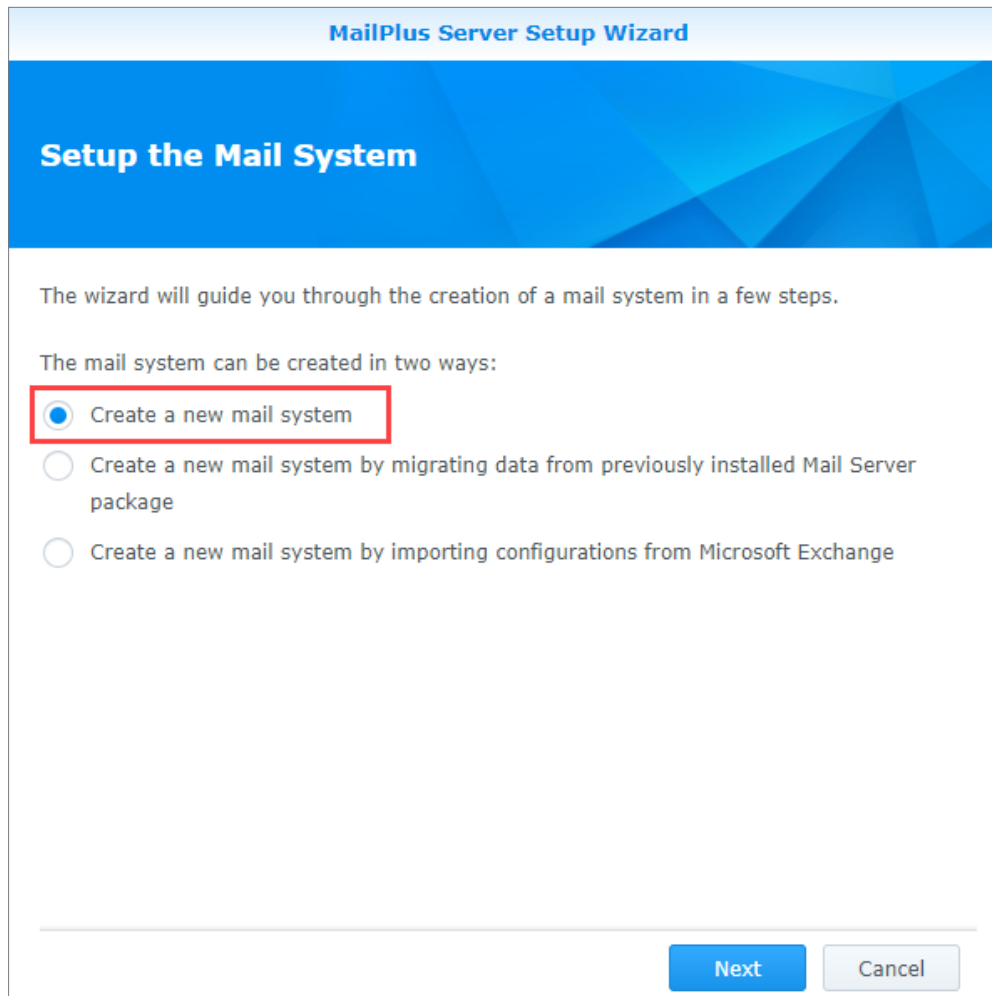
- **在自己的主機上設定反向 DNS：**特定網路服務供應商可能會提供部分區塊供您自行設定反向 DNS。您可修改 DNS 伺服器上的 PTR 記錄來設定反向 DNS，PTR 記錄是由發給您 IP 位址的單位負責管理。若主機授權您修改反向 DNS，負責管理 PTR 記錄的單位可能是您的主機或自己。PTR 記錄通常代表反向輸入的 IP，結尾為 in-addr.arpa。
- **透過您的網路服務供應商設定反向 DNS：**您的網路服務供應商或擁有您 IP 位址的其他單位，是唯一可增加 PTR 記錄的單位，您可能需要與他們聯絡，以進行反向 DNS 設定。



## 設定 MailPlus Server

使用 DSM 或 Virtual DSM 完成安裝 MailPlus Server 後，即可開始進行設定。在以下段落中，我們將介紹如何初步設定 SMTP (簡易郵件傳輸協定)。請注意，以下截圖僅供參考，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。請參閱[此應用教學](#)來了解如何將 Mail Server 轉移至 MailPlus Server。



**MailPlus Server Setup Wizard**

### Setup the Mail System

The wizard will guide you through the creation of a mail system in a few steps.

The mail system can be created in two ways:

- Create a new mail system
- Create a new mail system by migrating data from previously installed Mail Server package
- Create a new mail system by importing configurations from Microsoft Exchange

**Next** **Cancel**

### 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件使用的電子郵件位址，請確認該網域名稱與 DNS 設定中的 MX 記錄符合。
- **主機名稱 (FQDN)**：主機名稱是您的 MailPlus Server 位址，請確認該主機名稱與 DNS 設定中的 A 記錄符合。

**MailPlus Server Setup Wizard**

### Configure basic SMTP settings

Account type: Local users ⓘ

Network Interface: LAN 1 (192.168.1.102)

Domain name: example.com

Hostname (FQDN): mail.example.com

Volume: Volume 1

Back Next Cancel

### 4. 您可依需求修改下列設定：

- **帳號類型**：選擇可以使用 MailPlus 服務的使用者帳號類型 (本地、LDAP、網域使用者)。
- **網路介面**：選擇 MailPlus Server 使用的網路埠。
- **儲存空間**：選擇儲存 MailPlus Server 及其資料的儲存空間。

### 5. 按下一步來檢查設定摘要，再按一下**套用**來完成設定。

### 6. 初步設定完 MailPlus Server 後，您可以[啟動帳號](#)來設定可使用郵件服務的使用者。請注意，啟動五位以上的使用者需要額外購入授權碼。若想了解更多 MailPlus 授權機制的資訊，請參考[MailPlus 授權頁面](#)。

#### 注意：

- 系統預設會授予所有使用者 MailPlus Server 的應用程式權限，由於在**控制台**變更權限設定會影響 MailPlus Server 的運作，您應盡可能避免自行改動。如需詳細資訊，請參閱[啟動帳號](#)。
- 設定完 MailPlus Server 後，系統會自動將 **MailPlus** 共用資料夾新增至 Synology NAS。為確保用戶端使用者可以順利存取 MailPlus，該共用資料夾的權限設定應維持預設，不建議您自行改動權限設定。

## 設定 MailPlus 用戶端

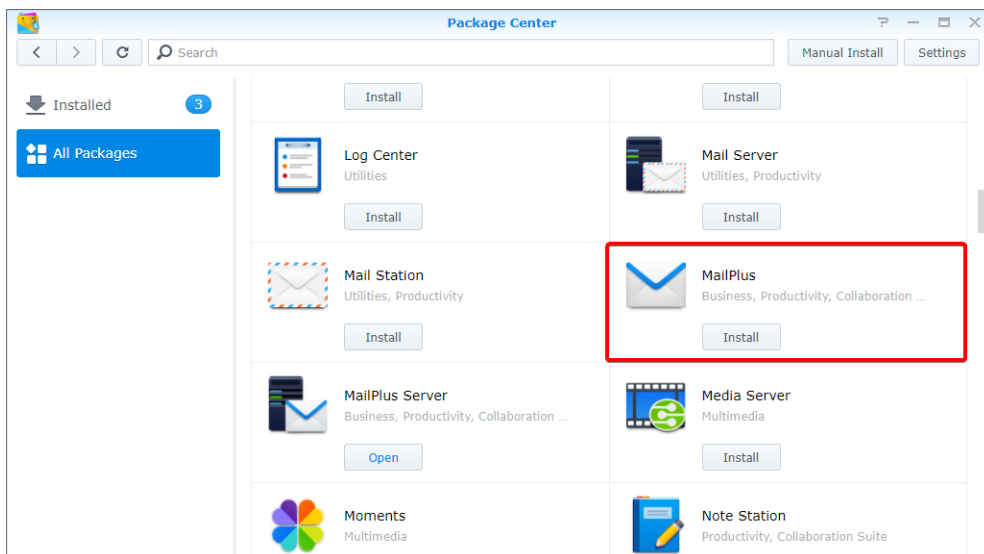
### 使用 MailPlus 存取 Synology NAS 上的電子郵件

MailPlus 是一款附加套件，讓用戶端使用者可以透過網頁介面存取並管理 Synology NAS 上的電子郵件。

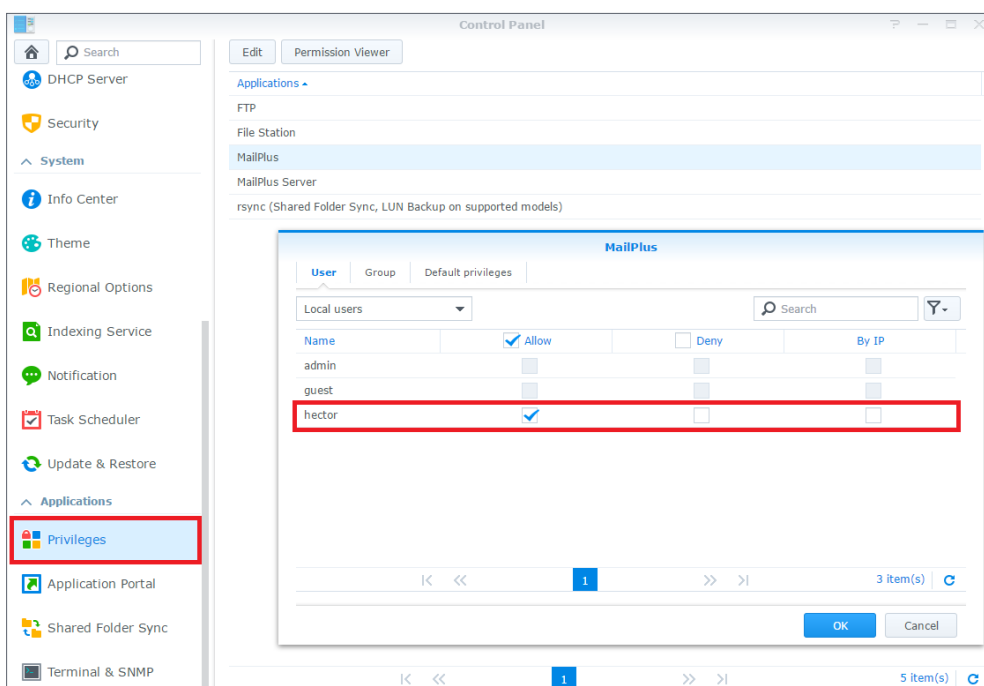
MailPlus 亦允許新增多個 POP3 帳號，藉此接收並儲存來自其它電子郵件服務的訊息 (例如：Mozilla® Thunderbird®、Gmail、Office 365)。

### 安裝 MailPlus

1. 前往套件中心安裝 MailPlus。



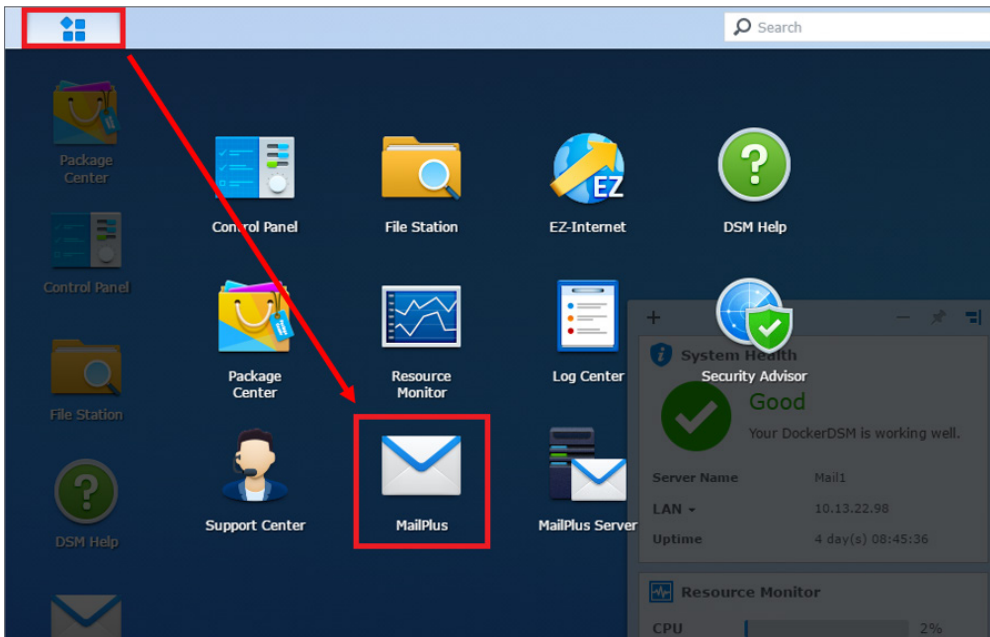
2. 前往控制台 > 權限來設定可以存取 MailPlus 的使用者或群組帳號。



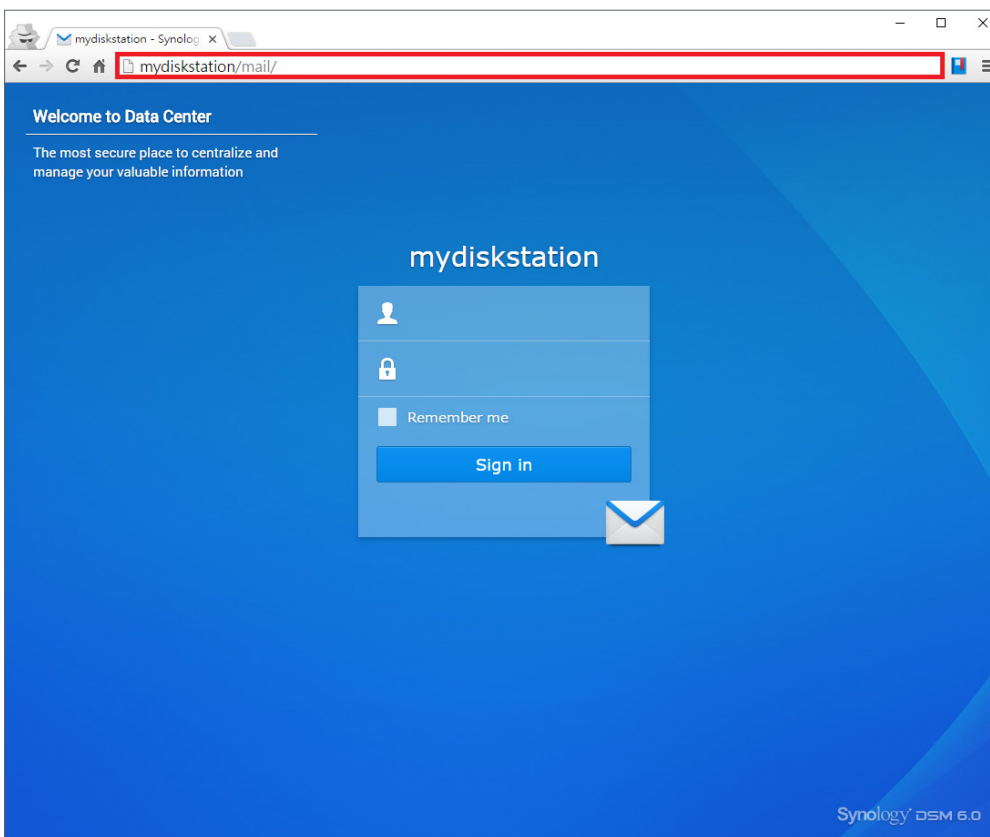
## 執行 MailPlus

1. 您可透過兩種方式前往 MailPlus 登入頁面：

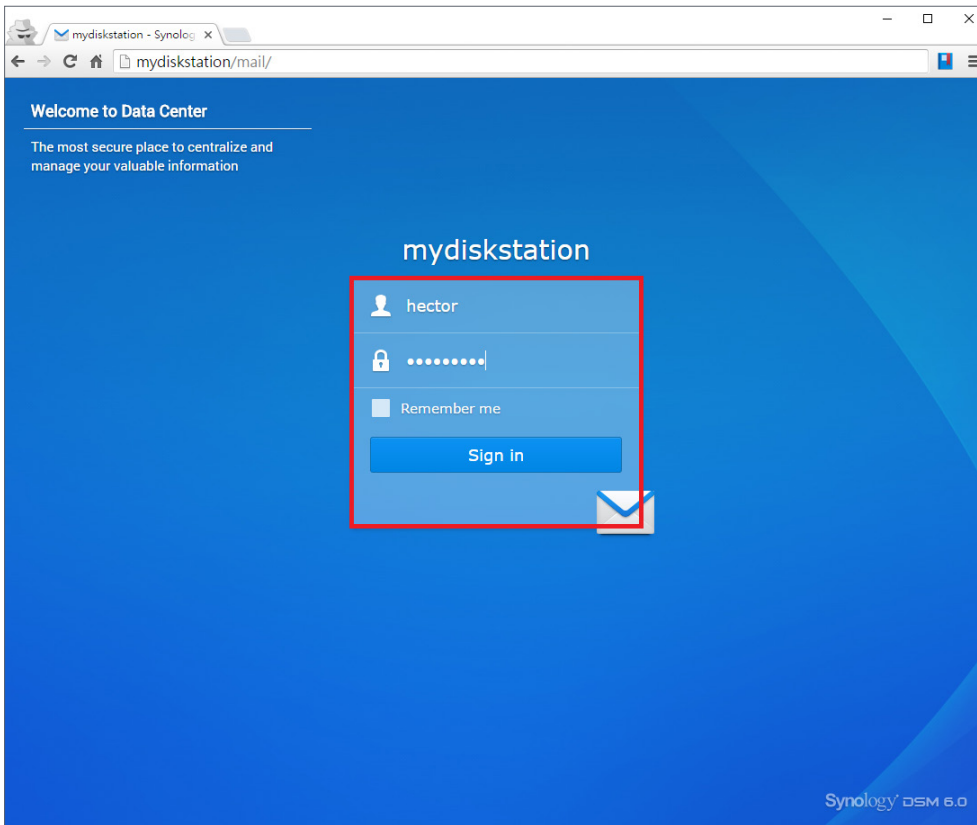
- 前往主選單 > MailPlus。



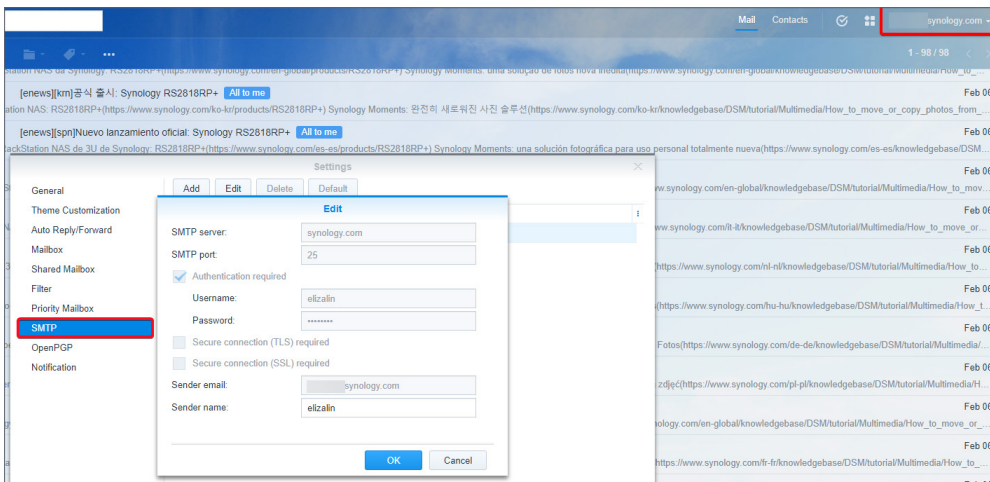
- 透過應用程式入口來存取 MailPlus。在網頁瀏覽器的網址列中輸入 Synology NAS 的名稱，後接「/mail」。例如：若您的 Synology NAS 名稱為 *mydiskstation*，則輸入 *mydiskstation/mail*。請參閱[此說明文章](#)以了解如何啟用應用程式入口。



2. 輸入您的 DSM 使用者帳號及密碼來登入。



3. 若在安裝 MailPlus 前已完成 MailPlus Server 的設定，MailPlus Server 的 SMTP 設定將自動套用至設定 > SMTP。

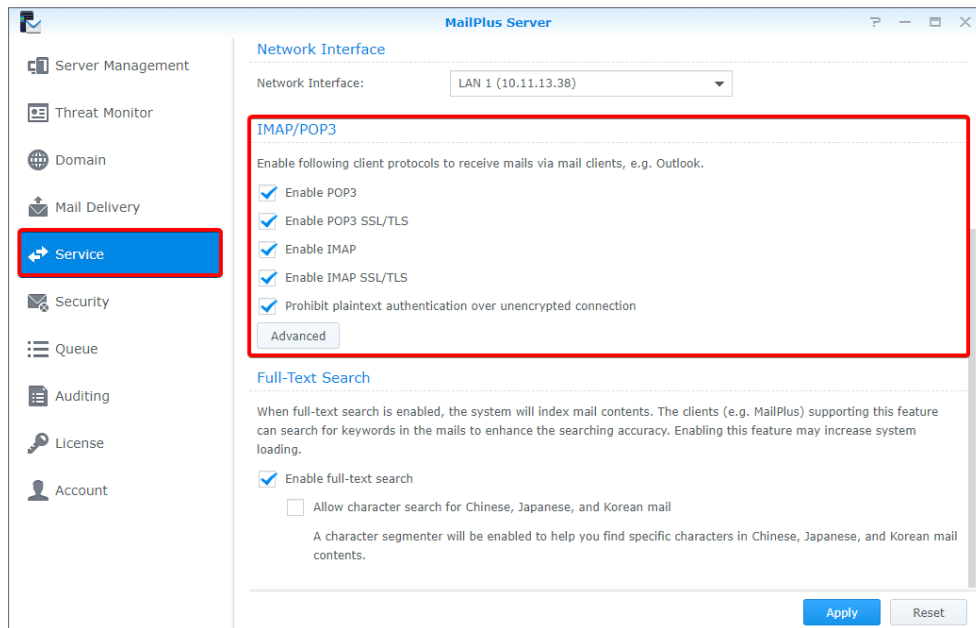


## 第三方電子郵件用戶端

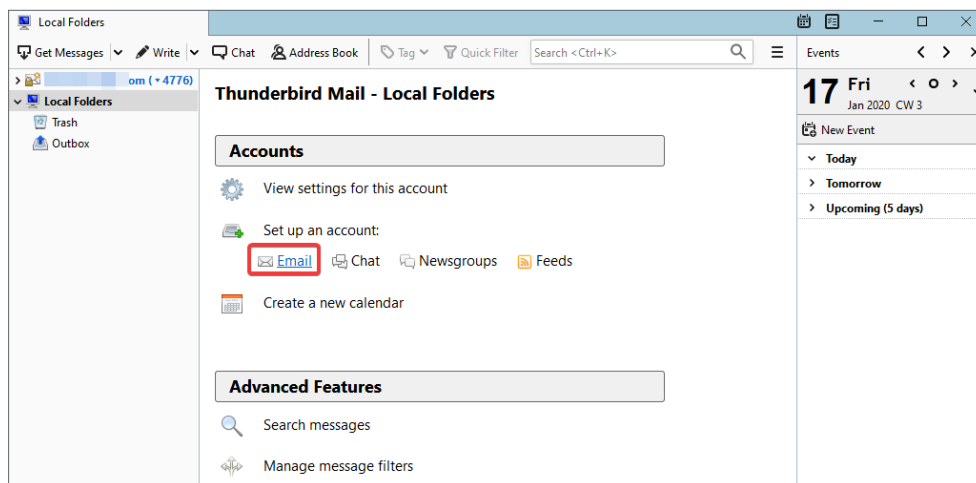
### 透過其他電子郵件用戶端存取 Synology NAS 上的郵件

Synology NAS 上的電子郵件帳戶可連結多種不同的郵件用戶端，例如：Microsoft® Outlook® 或 Mozilla® Thunderbird®。在下方範例中，我們將介紹如何使用 Thunderbird® 來存取 Synology NAS 上的電子郵件帳戶。

1. 開啟 MailPlus Server，前往服務頁面來啟用 IMAP 及 POP3。



2. 於您的本地裝置開啟 Thunderbird®。按一下電子郵件以開啟加入現有郵件帳號視窗。



3. 輸入名稱、MailPlus 帳號、DSM 使用者密碼。按一下繼續。

**Set Up an Existing Email Account** [X]

Your name:  Your name, as shown to others

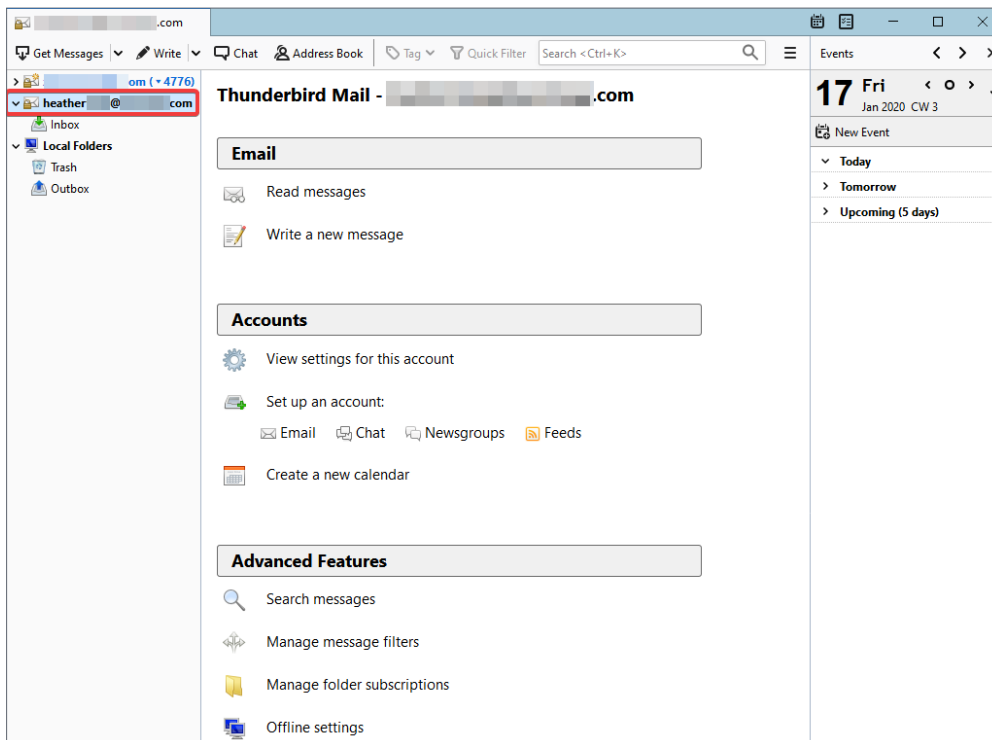
Email address:  Your existing email address

Password:   Remember password

[Manual config](#) [Continue](#) [Cancel](#)

4. Thunderbird® 會開始搜尋您的電子郵件帳戶。若設定正確，按一下完成以結束設定。

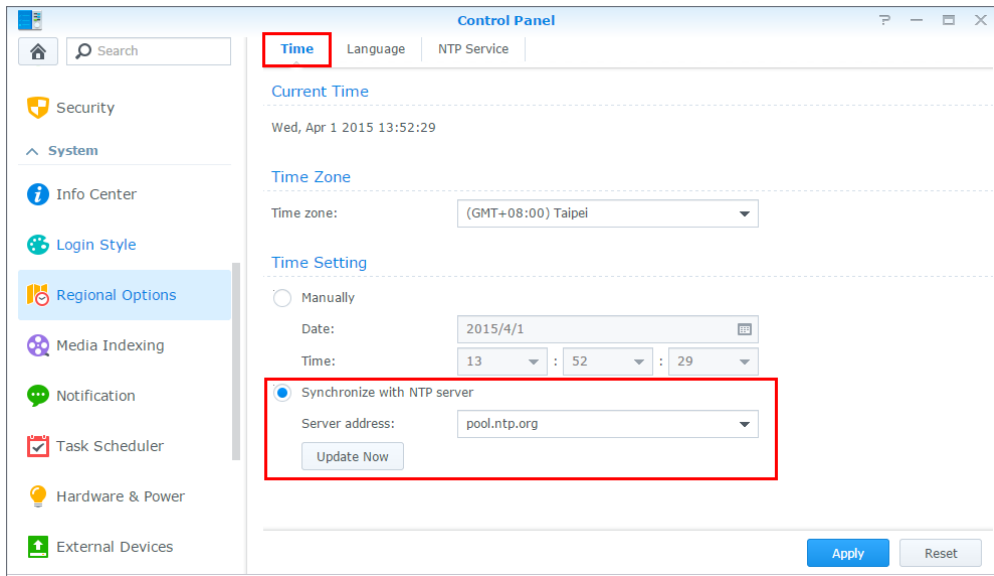
5. 設定完成後，您的 MailPlus 帳號便會出現在左側面板中。您可以在帳號上按兩下來展開所有郵件匣。



## 疑難排解

### 為什麼我無法用 MailPlus 的網頁介面收發電子郵件？

1. 請檢查 MailPlus 的 SMTP、DNS、MX 記錄等設定是否正確。
2. 請檢查 Synology NAS 的網路設定是否正確。前往**控制台** > **區域選項**，在**時間**頁籤下，勾選與 **NTP 伺服器同步**，再按一下**立即更新**按鈕以檢查網路設定是否正確。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. 請到 [Spamhaus](#) 查看您的 IP 位址是否被列為垃圾郵件發送者。若是，請將您的 IP 位址自該網站的封鎖名單中移除。

### 為什麼我無法從電子郵件用戶端收發電子郵件？

1. 請檢查您是否已啟用 IMAP 與 POP3 協定。
2. 請檢查使用者帳號與密碼是否正確。
3. 請檢查 MailPlus 的 SMTP、DNS、MX 記錄等設定是否正確。
4. 請檢查 Synology NAS 的網路設定是否正確。前往**控制台** > **區域選項**，在**時間**頁籤下，勾選與 **NTP 伺服器同步**，再按一下**立即更新**按鈕以檢查網路設定是否正確。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. 請到 [Spamhaus](#) 查看您的 IP 位址是否被列為垃圾郵件發送者。若是，請將您的 IP 位址自該網站的封鎖名單中移除。



### 為什麼我無法收取來自其他郵件伺服器 (例如：Gmail) 的電子郵件？

1. 請確認 DNS 的設定正確。您需將 MX 記錄與 A 記錄指向 Synology NAS，讓其他的郵件伺服器能找到 Synology NAS。
2. 請確認 Synology NAS 使用固定 IP 位址，且連線至網際網路，或者請確認網域名稱可正確指向動態 IP 位址。
3. 若 Synology NAS 是透過 NAT 防火牆或路由器連線至網際網路，請確認連接埠轉送設定是否正確。您可至 [CanYouSeeMe 網站](#) 輸入連接埠 25 以確認連接埠轉送設定。
4. 如果有退信的話，請查看被退回的郵件內容，了解錯誤發生的原因。

### 為什麼我寄信到某些網路郵件帳號(例如：Gmail 和 Hotmail 的帳號)，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，請與您的網路服務供應商 (ISP) 聯絡。也有可能您的 IP 位址被列入垃圾郵件封鎖清單中，請到 [Spamhaus](#) 查看您的 IP 位址是否遭到封鎖。

## 第 3 章：郵件移轉

MailPlus Server 內建郵件轉移工具，毋需複雜設定，即可從非 MailPlus 的郵件伺服器 (例如：Microsoft Exchange 及 IMAP 郵件伺服器) 或第三方服務 (例如：Gmail 及 Yahoo Mail) 轉移電子郵件。

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 為 DSM 6.0 或更新版本，並支援 MailPlus Server (相容機種請見[此處](#))。
- 已在 Synology NAS 上完成 MailPlus Server 設定，用以作為目的地郵件伺服器。
- 匯整來源帳號的使用者名稱及密碼與對應的 MailPlus 帳號名稱。

### 在 MailPlus Server 新增郵件轉移任務

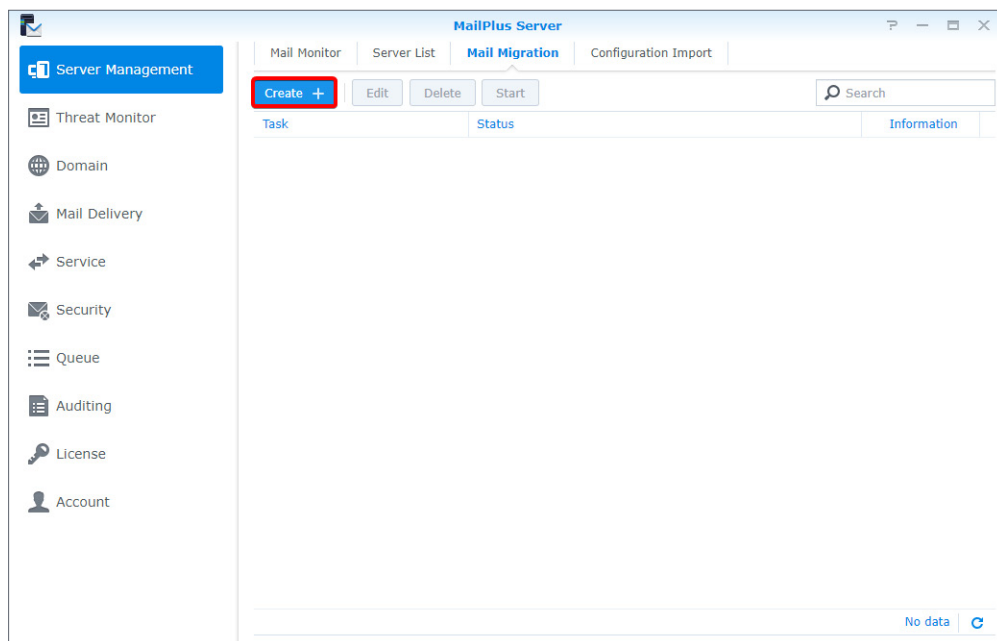
登入 MailPlus Server，前往**伺服器管理 > 郵件移轉 > 新增**來建立郵件轉移任務。本章節將以 Microsoft Exchange 為例。

**注意：**

- 若要了解如何從其他來源 (例如：Gmail 或 Yahoo Mail) 轉移郵件，請參閱[此說明文章](#)。

#### 進行一般任務設定

1. 前往**伺服器管理 > 郵件移轉**，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. 若您於來源伺服器上有代理帳號，且該帳號具備所有來源帳號的完整存取權限，選擇透過代理帳號移轉郵件並填入對應的帳號密碼，即可透過該帳號移轉郵件，不需取得各個來源帳號的存取權限。
5. 您可以依據來源伺服器的能力來設定各時段移轉的帳號數。

**Migration Settings**

**General** | User List | Filter | Notification

Task: Microsoft Exchange Migrate

Select the server type: Microsoft Exchange

Server address: mailtest.synology.com

Port: 993

Enable secure connection (SSL)

Verify SSL certificate

IMAP path prefix:

Test Connection

Migrate mail with the delegate account

Account: mail\_admin

Password: .....

Accounts to migrate per time period: 5

Schedule email migration

From: 00 : 00

Save Close

### 匯入使用者清單

1. 依據下列規範，準備一份使用者清單：

- 透過文字編輯器生成 CSV 檔案格式的使用者清單。
- 一列只列一筆使用者帳號資訊。
- 從左至右，為每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 (,) 分隔各種類型的資訊。
- 當來源伺服器類型設定為 **Microsoft Exchange** 並啟用**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)。

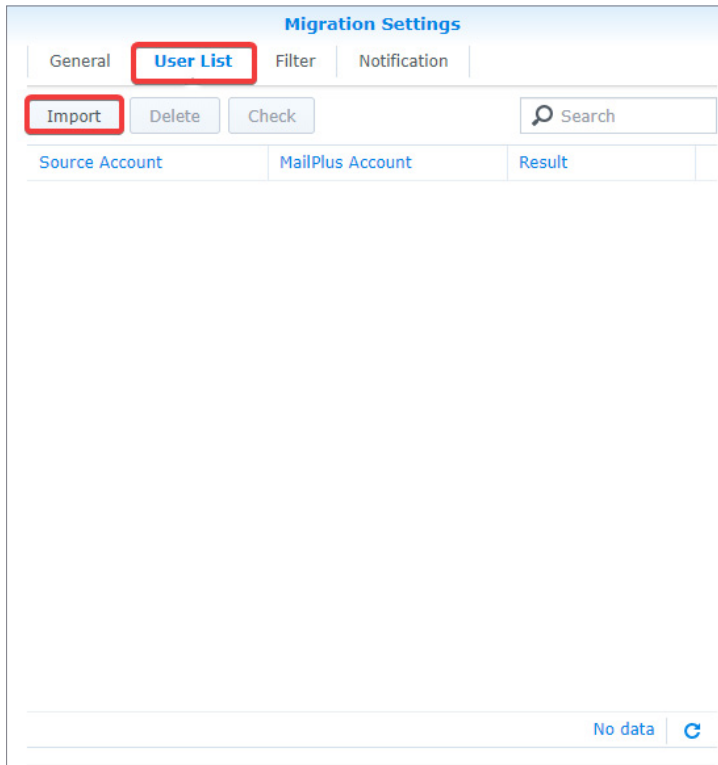
**注意：**

- Google Workspace 帳號須以 FQDA (即「使用者名稱 @ 網域名稱」的格式) 來指定。

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**頁籤來匯入清單。請先確認所有的帳號資訊正確，再匯入清單。



## 設定電子郵件及信件匣篩選器

1. 在篩選頁籤，指定條件來轉移或略過來源伺服器上的特定郵件或郵件匣。

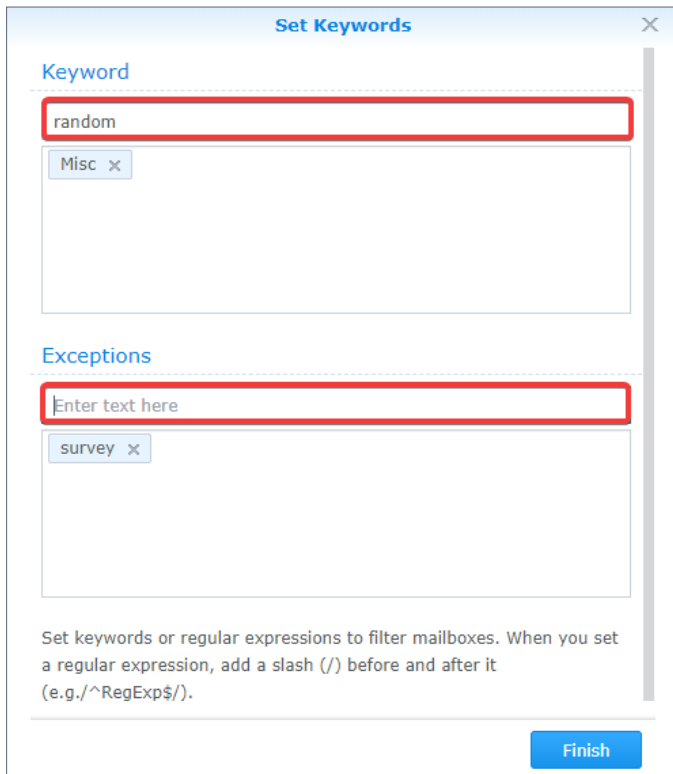
The screenshot shows the 'Migration Settings' dialog box with the 'Filter' tab selected. The 'Filter' tab is highlighted with a red box. The 'Enable mailbox filter' checkbox is checked. Underneath, 'Skip mailboxes by keyword' is selected with a radio button. A 'Set Keywords' button is visible below the radio buttons. Other settings include 'Discard mail received before the date' (checked, 2017-01-01), 'Discard mail received after the date' (unchecked, To), 'Skip trash mail' (unchecked), 'Skip spam mail' (checked), and 'Maximum size per email (KB)' (10240). 'Save' and 'Close' buttons are at the bottom.

2. 若要透過關鍵字篩選信件匣，勾選啟用信件匣篩選器並選擇篩選方式 (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：**輸入文字後，系統便會依據你設定的篩選方式處理相符的信件匣。
- **例外情況：**輸入文字後，系統便會略過相符的信件匣。

4. 您可以在這兩處輸入正規表示式，兩旁皆須加上斜線 (例如：/正規\_表示式/)。



**Set Keywords**

Keyword

random

Misc x

Exceptions

Enter text here

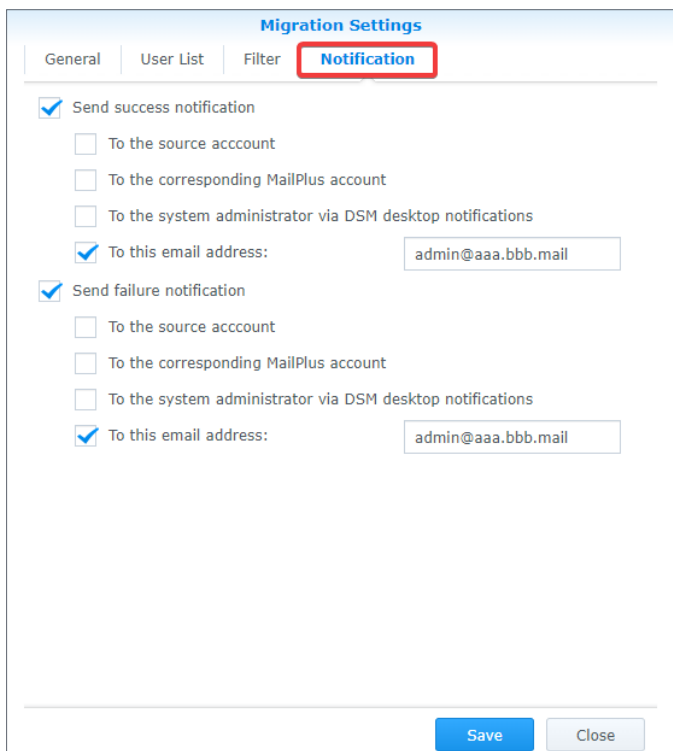
survey x

Set keywords or regular expressions to filter mailboxes. When you set a regular expression, add a slash (/) before and after it (e.g./^RegExp\$/).

Finish

## 設定轉移通知

1. 確認 MailPlus Server 上已勾選啟用 SMTP (位於服務)，以傳送通知訊息。
2. 在通知設定頁籤中，決定 MailPlus Server 是否應寄送各帳號的轉移結果，以及管理者在何處接收訊息。



**Migration Settings**

General | User List | Filter | **Notification**

Send success notification

- To the source account
- To the corresponding MailPlus account
- To the system administrator via DSM desktop notifications
- To this email address: admin@aaa.bbb.mail

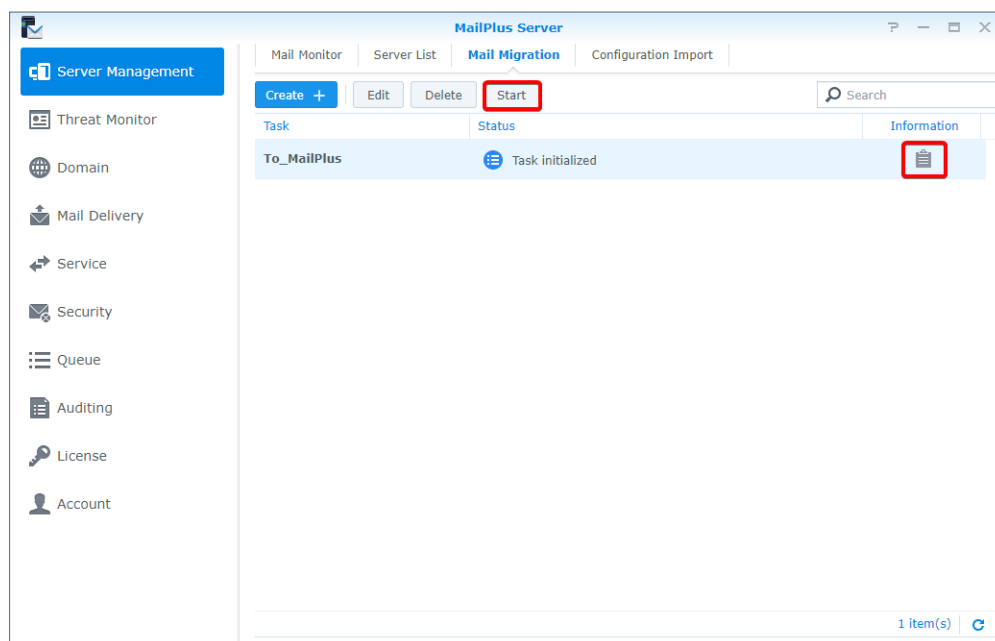
Send failure notification

- To the source account
- To the corresponding MailPlus account
- To the system administrator via DSM desktop notifications
- To this email address: admin@aaa.bbb.mail

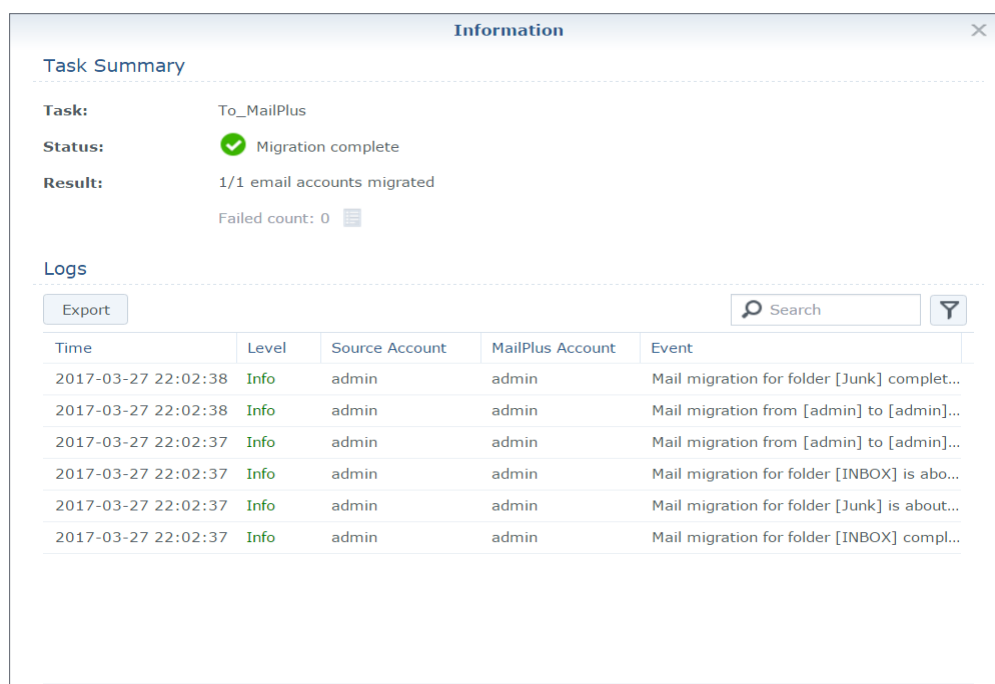
Save Close

## 執行郵件轉移任務

1. 在伺服器管理 > 郵件移轉選擇移轉任務，按一下開始來執行。為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. 按一下詳細資訊 (文件圖示) 來查看轉移任務的統計資料及日誌。



### 注意：

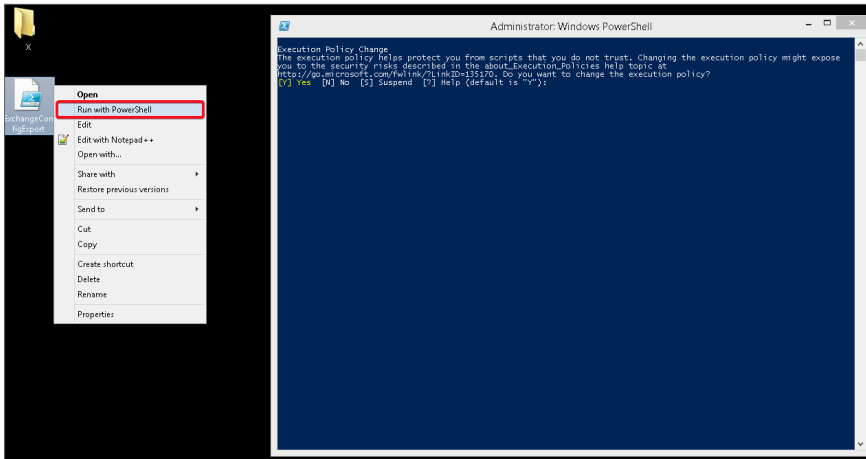
- 從 Google Workspace 轉移郵件時，會依您的 Google 標籤套用過濾器。

## 將 Microsoft Exchange 系統設定匯入 MailPlus Server

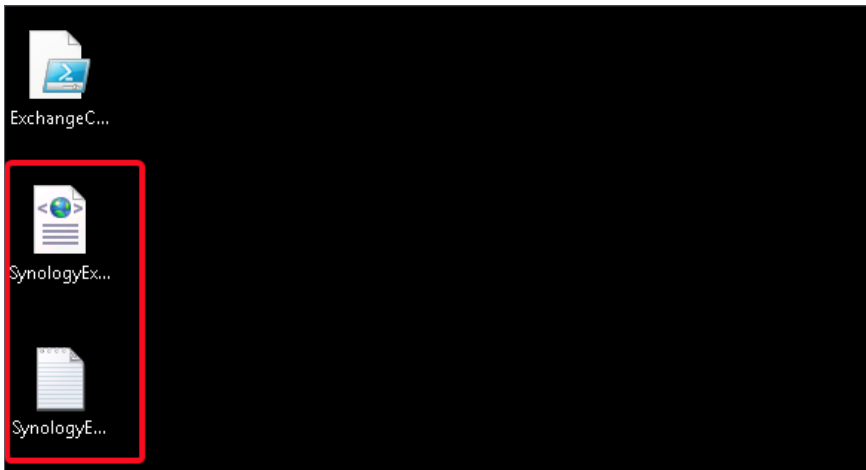
您可以將 Microsoft Exchange 的系統設定及別名匯出，再匯入到 MailPlus Server 繼續使用。

### 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. 將指令檔移動到該台 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 檔案移動至您的本機電腦。

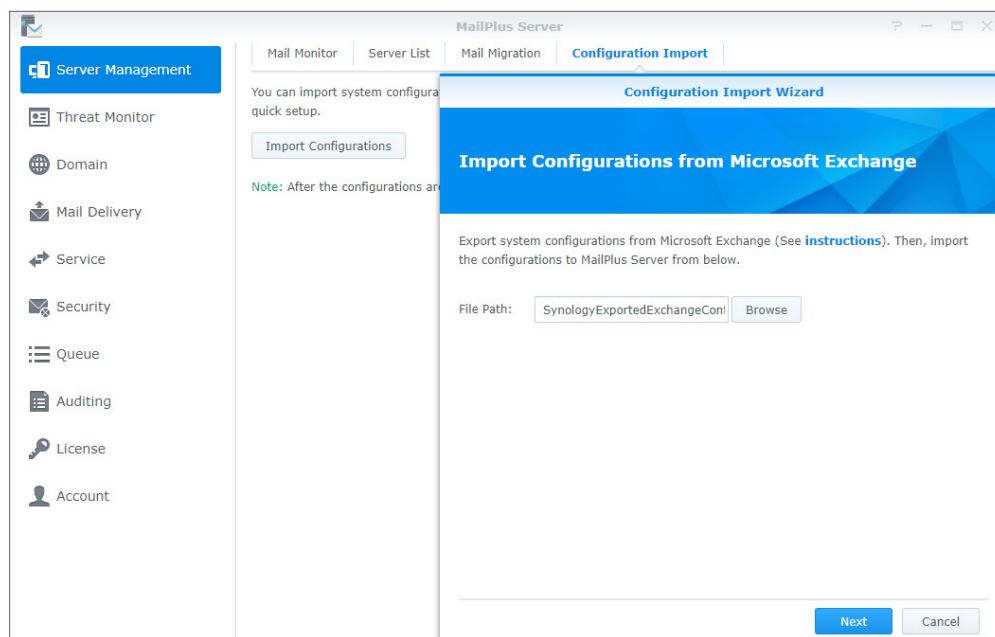


## 匯入系統設定至 MailPlus Server

1. 透過下列任一方式匯入：

- 當 MailPlus Server 尚未初始化時：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)，按一下匯入。

## 第 4 章：使用者授權

MailPlus Server 需要有足夠的授權數量才能正常運作，所需的授權數量依您啟動的帳號數量而定。MailPlus Server 預設提供五組免費的郵件帳號，若要增加更多使用者，須額外購買授權。

以下項目不會計入授權數量：

- **停用的帳號**：舉例來說，離職員工的授權可再套用至新進員工。
- **郵件別名**：由於別名郵件地址與已存在的使用者帳號綁定，因此每位使用者皆可新增別名且無須付費。
- **網域數量 (包含其他網域)**：MailPlus Server 支援多網域管理，因此使用多網域並不需要額外購買授權。
- **不屬於指定帳號系統的 DSM 使用者**：舉例來說，若帳號系統設為 LDAP 使用者，則本地使用者不會計入授權數量。

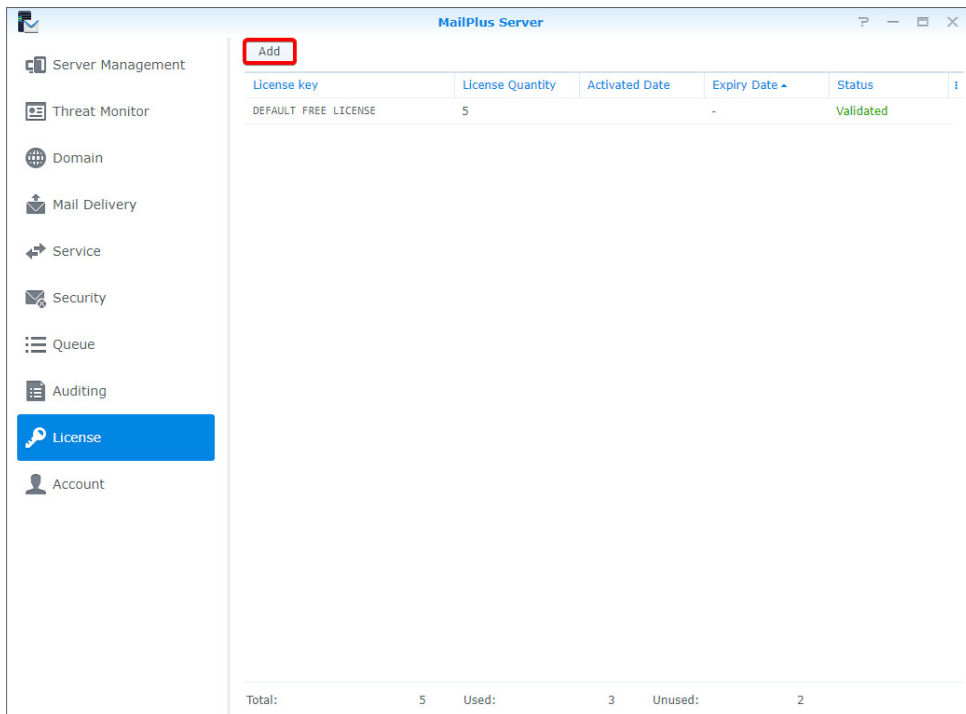
### 購買授權

MailPlus 授權分為 5 個或 20 個帳號為一組，可經由 [Synology 授權經銷商](#) 購買，如需 MailPlus 授權的詳細資訊，請參閱 [MailPlus 授權頁面](#)。

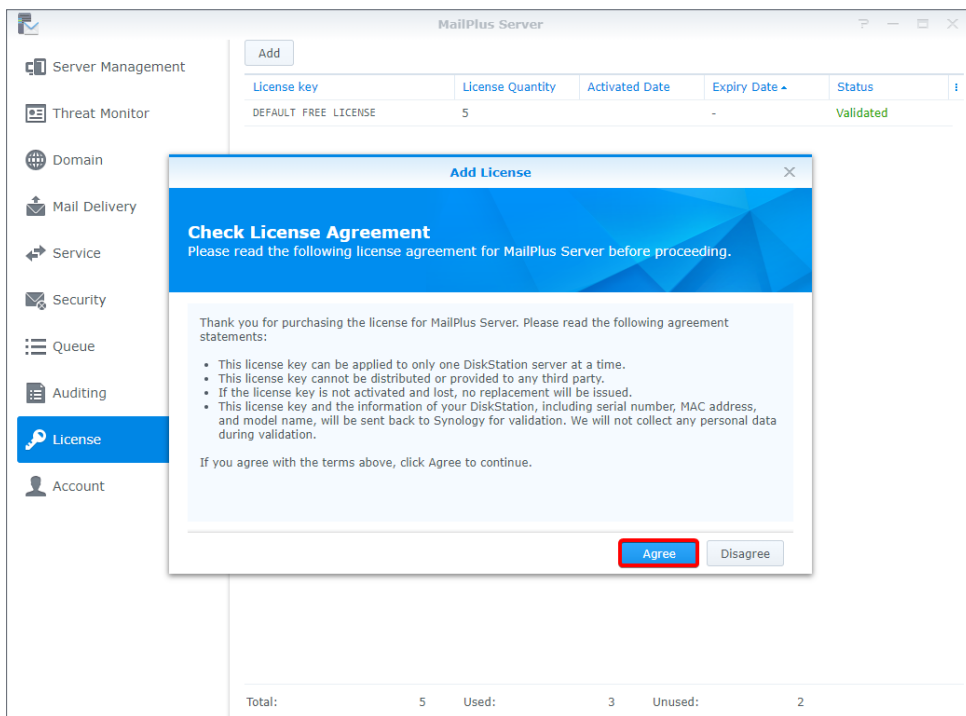
## 安裝授權

必須安裝購買的授權以啟動電子郵件帳號。請參考下列步驟：

1. 前往**授權**，按一下**新增**按鈕來加入授權。



2. 請詳閱**新增授權**視窗的 MailPlus Server 授權合約。確認並同意內容後，按一下**同意**。

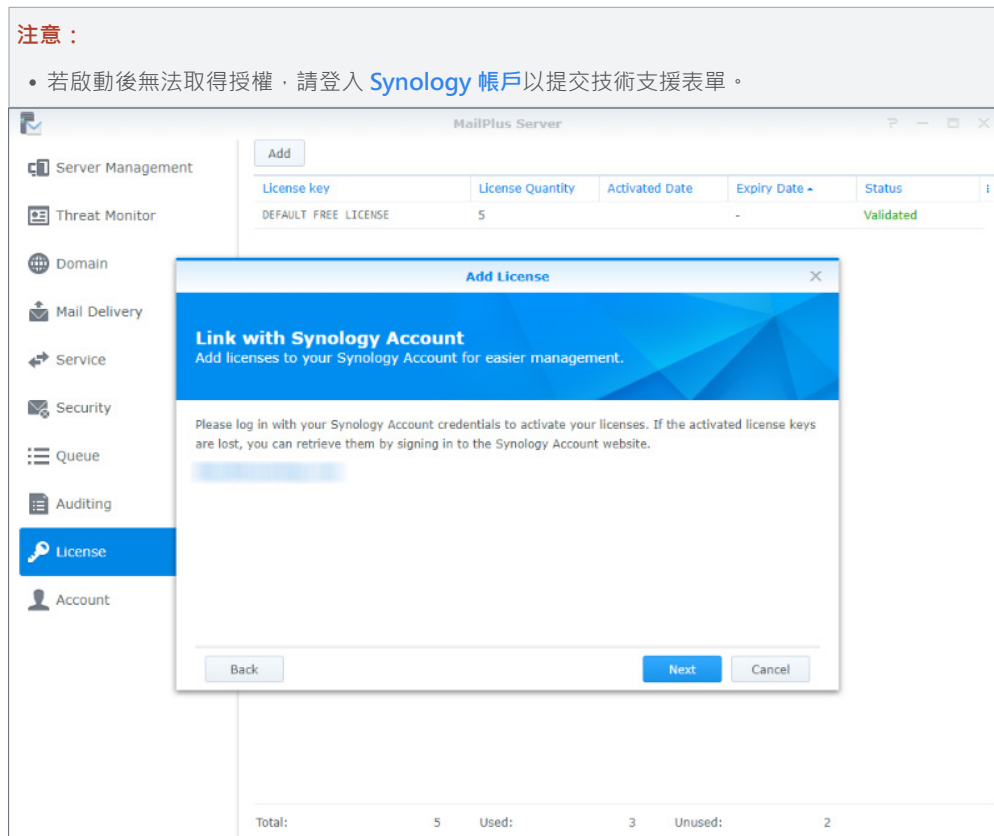


## 第 4 章：使用者授權

3. 登入 Synology 帳戶並按下一步。

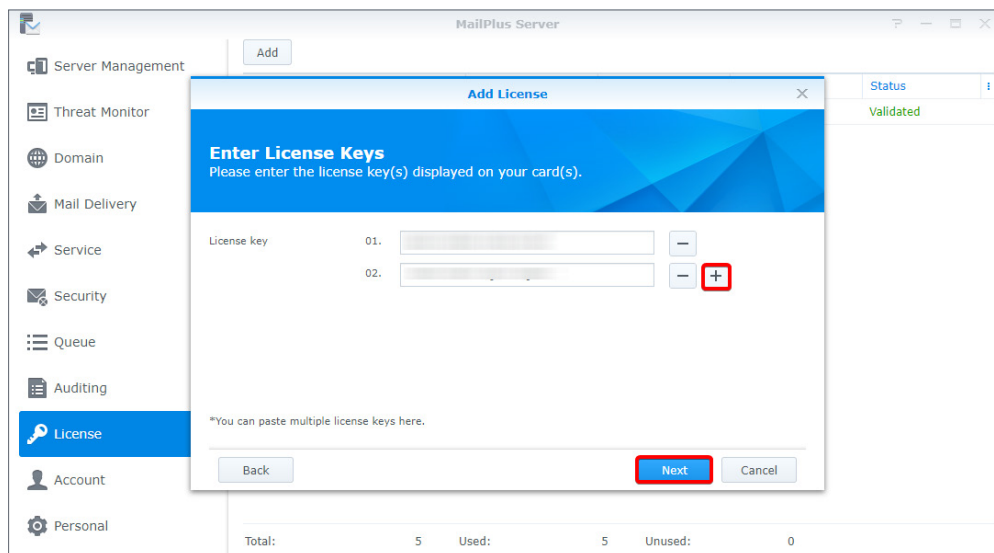
**注意：**

- 若啟動後無法取得授權，請登入 [Synology 帳戶](#) 以提交技術支援表單。



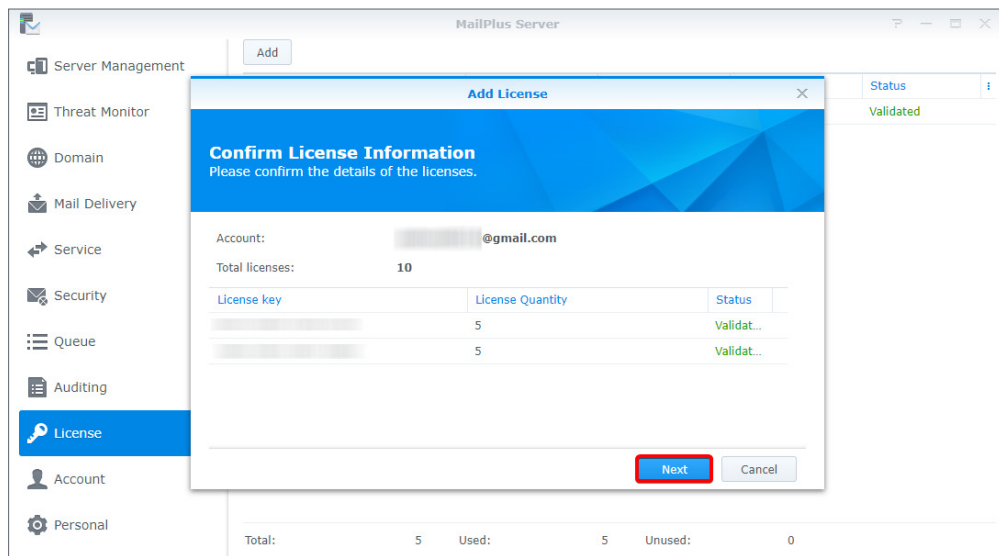
The screenshot shows the MailPlus Server interface with a sidebar on the left containing menu items: Server Management, Threat Monitor, Domain, Mail Delivery, Service, Security, Queue, Auditing, License (highlighted), and Account. The main area displays a table with columns: License key, License Quantity, Activated Date, Expiry Date, and Status. A single row is visible: DEFAULT FREE LICENSE, 5, -, Validated. An 'Add License' dialog box is open in the foreground. The dialog has a blue header and contains the text: 'Link with Synology Account', 'Add licenses to your Synology Account for easier management.', and 'Please log in with your Synology Account credentials to activate your licenses. If the activated license keys are lost, you can retrieve them by signing in to the Synology Account website.' Below the text are 'Back', 'Next', and 'Cancel' buttons. At the bottom of the main interface, a summary bar shows: Total: 5, Used: 3, Unused: 2.

4. 如下圖所示，將欲新增的授權碼輸入授權碼欄位中。如欲一次新增多組授權，您可以按一下加號圖示 (+) 來新增更多授權碼欄位。



The screenshot shows the same MailPlus Server interface as above. The 'Add License' dialog box is now titled 'Enter License Keys' and contains the text: 'Please enter the license key(s) displayed on your card(s)'. Below this text are two input fields labeled '01.' and '02.'. Each field has a minus sign (-) button to its right. The plus sign (+) button next to the '02.' field is highlighted with a red square. Below the input fields is the text: '\*You can paste multiple license keys here.' At the bottom of the dialog are 'Back', 'Next', and 'Cancel' buttons. The 'Next' button is highlighted with a red rectangle. The summary bar at the bottom of the main interface now shows: Total: 5, Used: 5, Unused: 0.

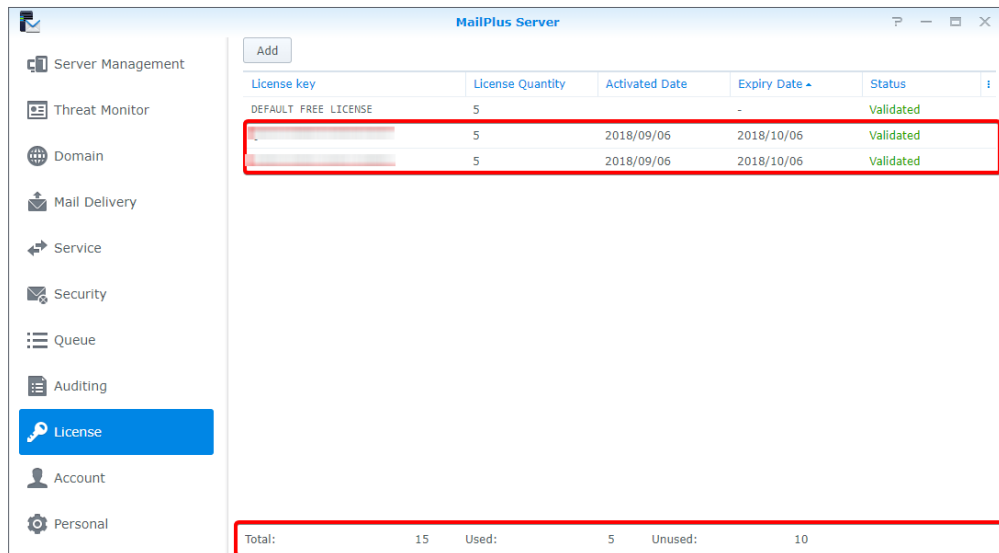
5. 確認安裝的授權數量以及其授權碼無誤。確認無誤後，按下一步來完成新增授權。



6. 新增授權後，您可以前往授權頁面以檢視各個授權的詳細資訊及狀態。

- 授權碼
- 每個授權提供的電子郵件帳號數量
- 授權啟動日期
- 授權過期日期
- 授權有效狀態

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



## 使用者授權

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。若要了解詳細步驟，請參閱[啟動帳號](#)。

# 第 5 章：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 上啟動 DSM 現有帳號中的使用者帳號。

除了本地使用者外，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 一次只能與一種目錄服務同步，因此 MailPlus Server 無法同時同步多種目錄服務。

### 注意：

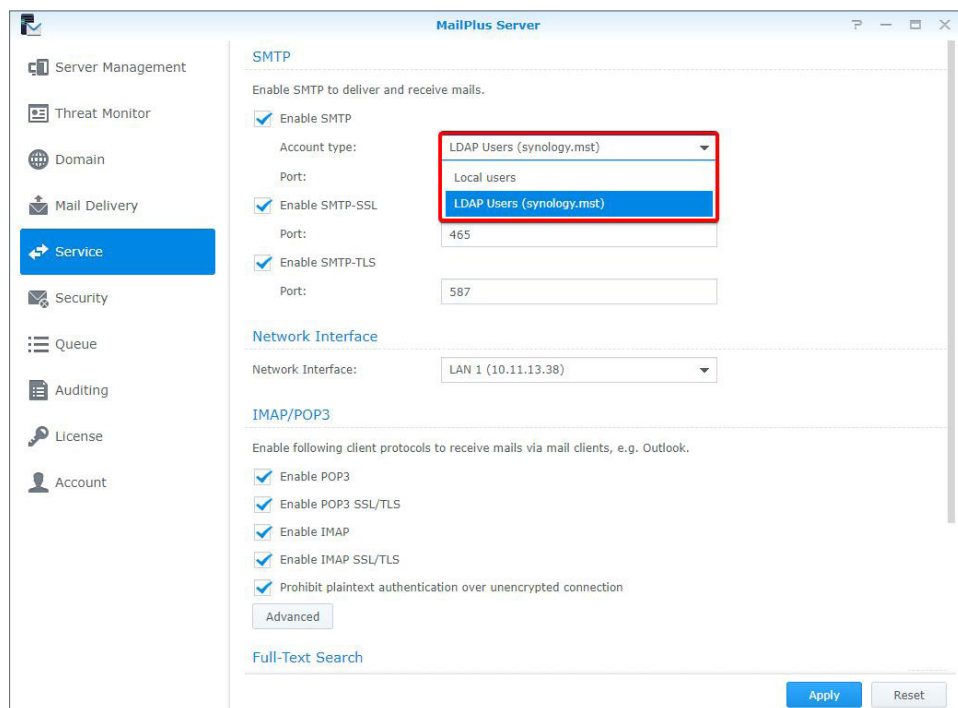
- 以下帳號類型中，MailPlus Server 一次只能選擇一種作為使用者帳號來源：本地、LDAP、網域。

## 修改帳號類型

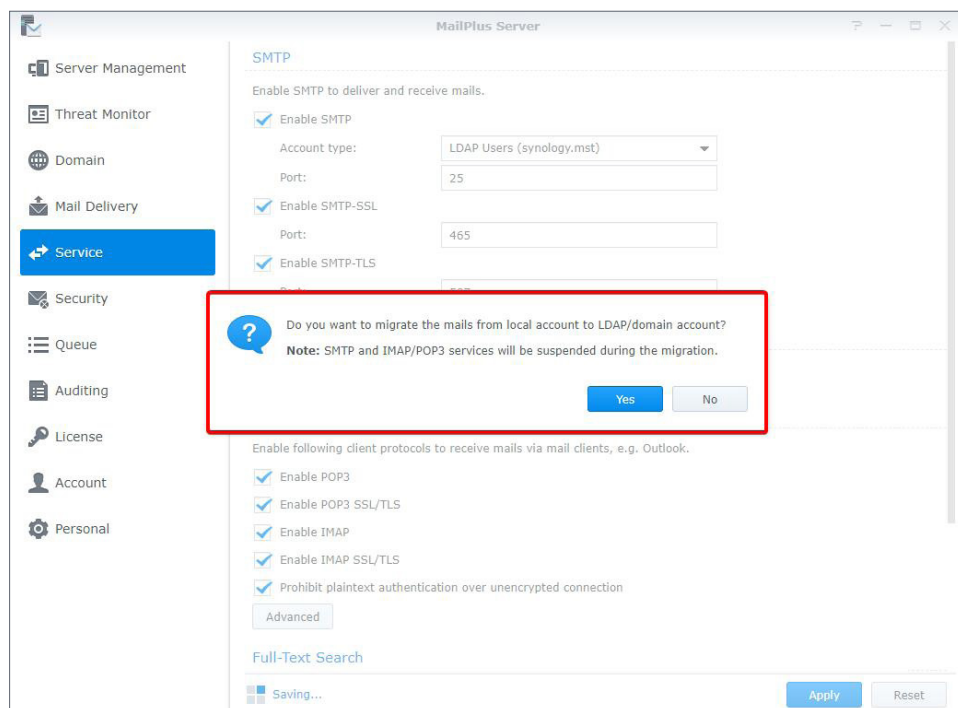
請依照下列步驟來完成設定：

1. 登入 DSM。
2. 前往**控制台 > 網域 / LDAP** 綁定選定的目錄服務。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，從帳號類型下拉式選單中選擇要使用的帳號類型(僅會顯示已在 DSM 上設定的目錄服務)。



5. 按一下套用來匯入目錄服務的使用者帳號。如下圖所示，若您從本地使用者切換至 LDAP 使用者或網域使用者，按一下套用後會出現提示視窗。



#### 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無法互通郵件。若要将本地使用者的郵件轉移至 LDAP 使用者或網域使用者，按一下是。系統僅會轉移在本地端與目錄服務同名使用者帳號的郵件。若無相同的使用者帳號，系統便會自動略過該帳號。

## 啟動帳號

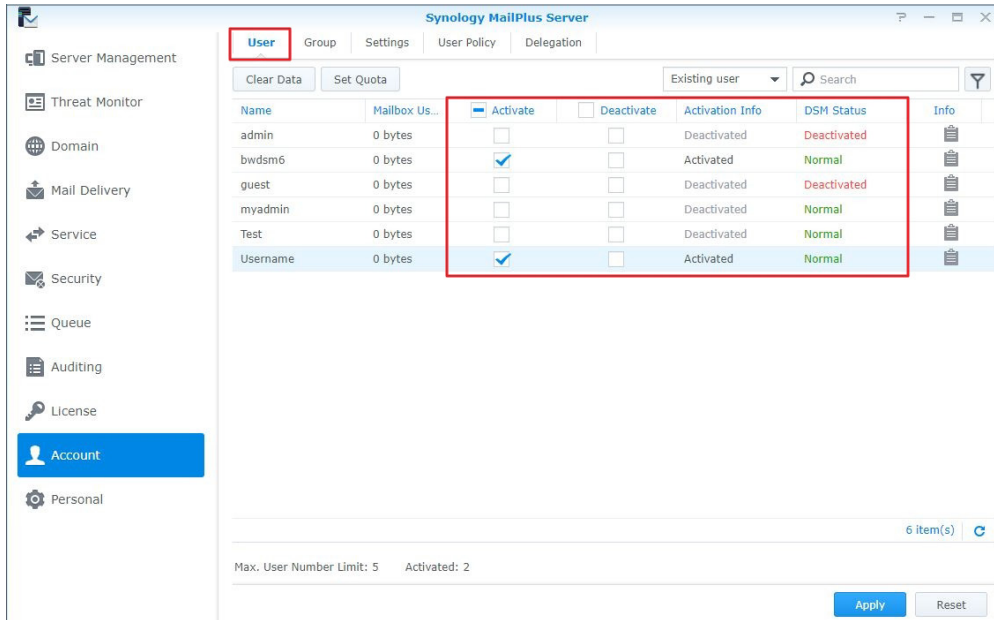
您必須先在 MailPlus Server 裡啟動使用者帳號，才能使用收發信件等郵件服務。因此，您會需要足夠的授權來啟動使用郵件服務的帳號。請參閱[使用者授權](#)段落來了解更多資訊。

若您已經啟動若干使用者，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該使用者或其並沒有 MailPlus 或 MailPlus Server 的權限。若要了解更多有關用戶端登入問題的資訊，請參考[此篇文章](#)。

### 啟動使用者帳號

啟動使用者需要充足的授權數量。請參考[使用者授權](#)段落來了解更多資訊。請依照下列步驟來啟動使用者帳號：

1. 前往 **帳號 > 使用者帳號**。
2. 選擇要啟動的使用者。若使用者的**啟動與停用**欄位下方的核取方塊皆未勾選，則該使用者為預設狀態。請參考[預設狀態](#)以了解詳細資訊。勾選**啟動**核取方塊後，可用授權數量將會減少。



3. **啟動資訊**欄位會顯示該使用者帳號是否已套用授權。
4. **狀態**欄位會顯示以下 DSM 使用者狀態：**正常**、**停用**、**使用者名稱不受支援**。

#### 注意：

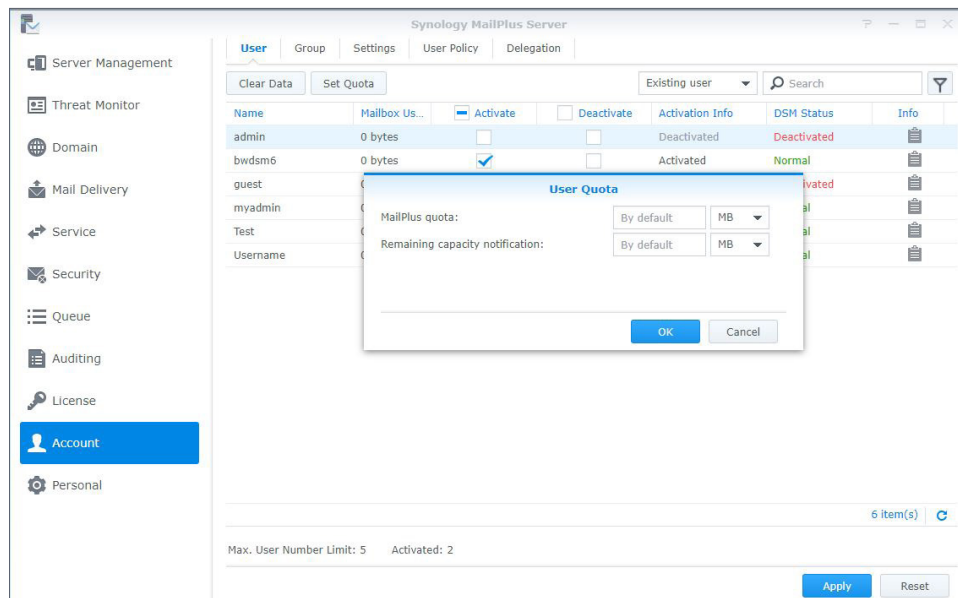
- 只有當**啟動資訊**為已啟動，且**狀態**為**正常**時，該使用者才能順利使用郵件服務。只要在此頁面調整帳號設定即可決定使用者的 MailPlus 權限，無須修改**控制台**中的設定。



5. 若要自訂郵件匣儲存空間，您可以選擇目標使用者並按一下**設定配額**來進行以下設定：

- MailPlus 配額：設定郵件匣的大小限制。
- 剩餘空間通知：設定警告閾值以通知使用者其郵件匣即將達到儲存空間限制。

6. 按一下**確定**以套用使用者的配額。



7. 資訊欄位會顯示該使用者的配額及已使用容量。

8. 按一下**套用**來啟動使用者帳號。

#### 注意：

- 針對已停用授權的使用者（例如：已離職員工），您可以選取該使用者並按一下**清除資料**來刪除其郵件及個人設定。

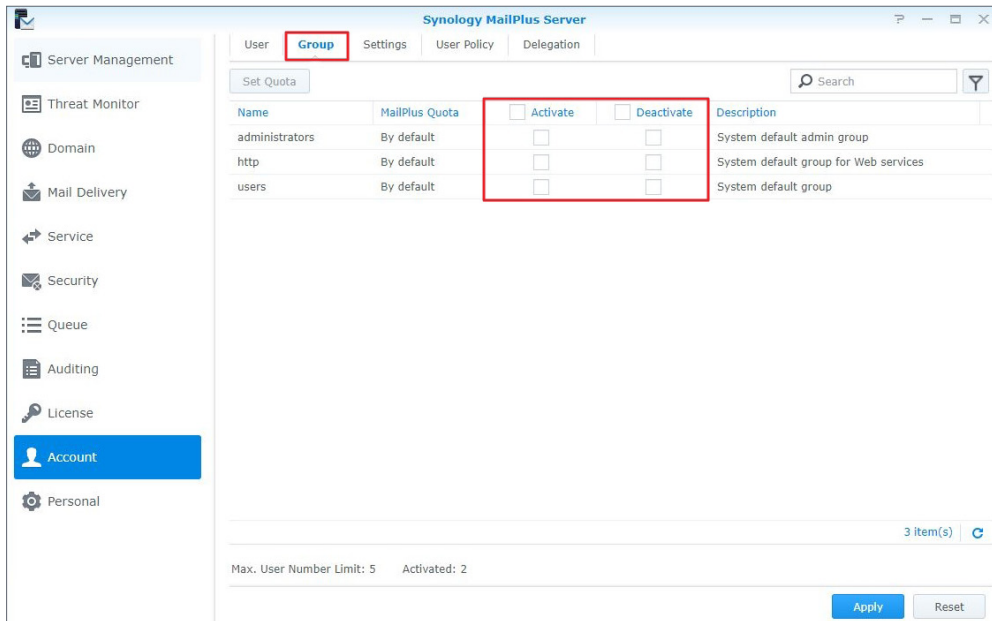
## 啟動群組

您可以在此處快速啟動或停用使用者群組，且設定會套用至群組中的每一位成員。請參考下列步驟：

1. 前往**帳號 > 使用者群組**來啟動或停用群組。

#### 注意：

- 判斷是否啟動使用者帳號的順序由高到低為：**使用者帳號設定**、**使用者群組設定**、**預設設定**。



2. 您可以為群組自訂郵件匣儲存空間配額，請選取目標群組並按一下**設定配額**來進行以下設定：

- MailPlus 配額：設定郵件匣的大小限制。
- 剩餘空間通知：設定警告閾值以通知使用者其郵件匣即將達到儲存空間限制。

3. 按一下**確定**以套用群組的配額。

4. 按一下**套用**來啟動群組中的使用者。

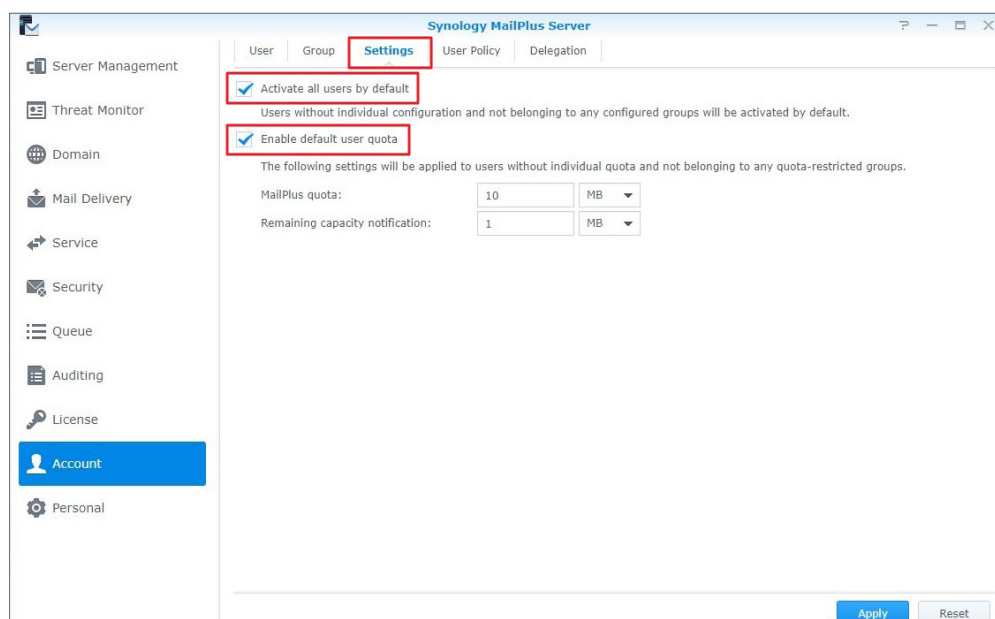
## 預設狀態

在**帳號**頁面的**設定**頁籤中，您可以調整預設狀態。預設狀態設定會套用到尚未啟動或停用且狀態為正常的**使用者帳號**。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**或**啟用預設使用者配額**核取方塊。

### 注意：

- 預設啟動可能會消耗大量授權，請確認您持有足夠的授權數量。

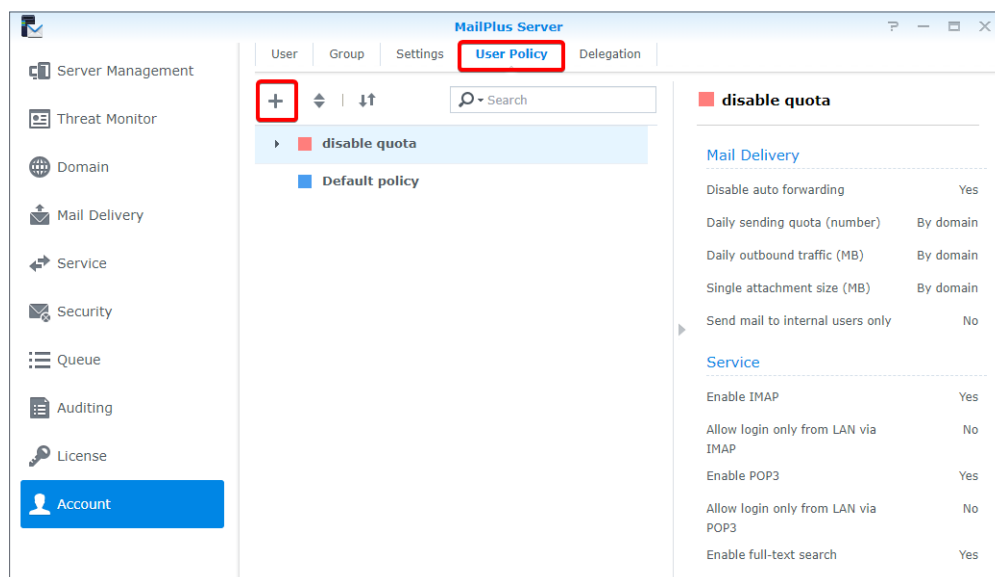


2. 按一下套用以儲存設定。

## 新增使用者規範

啟動使用者或群組後，您可以為特定的使用者或群組建立專用的郵件服務規範，以符合組織需求。請參考下列步驟來新增使用者規範：

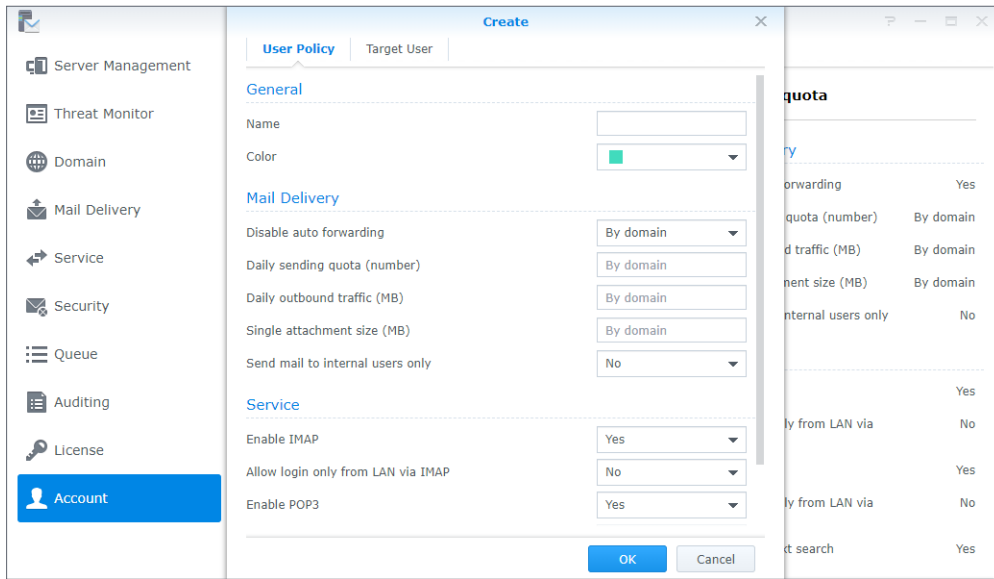
1. 前往帳號 > 使用者規範。
2. 按一下加號圖示 (+) 來新增規範。



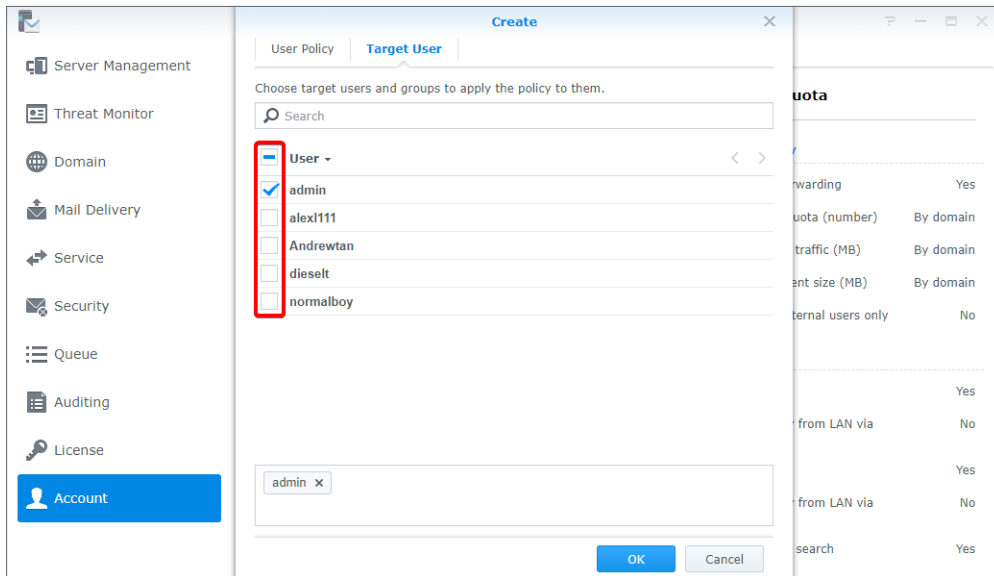
3. 在新增視窗中，前往使用者規範並於名稱欄位輸入規範名稱。
4. 從顏色的下拉式選單中選擇規範的顏色以方便辨識。

### 注意：

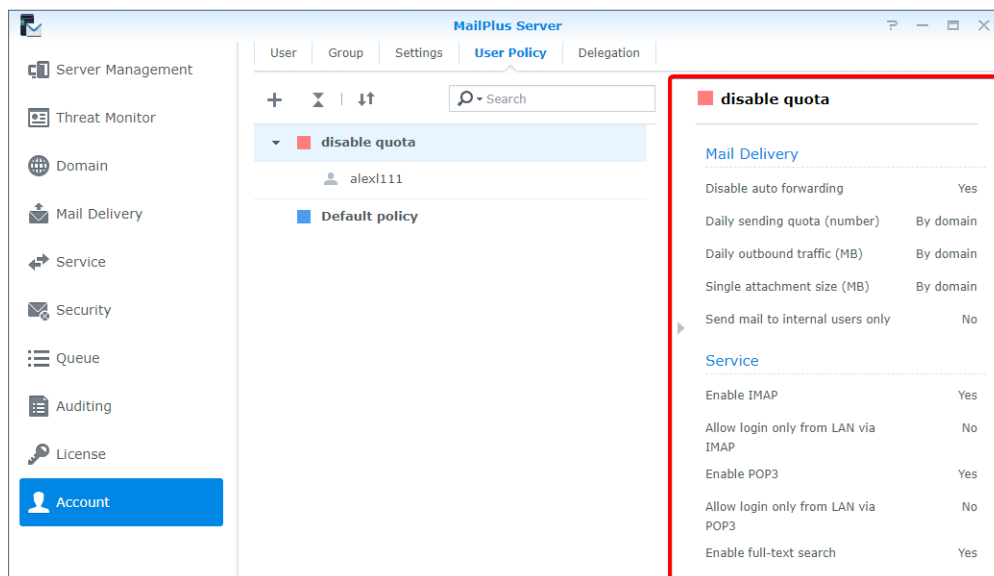
- 如需規範的詳細資訊，請參考[規範說明與限制](#)。



5. 切換到目標使用者頁籤，選擇要套用此規範的使用者或群組。您也可以透過上方的搜尋欄位來搜尋規範對象。



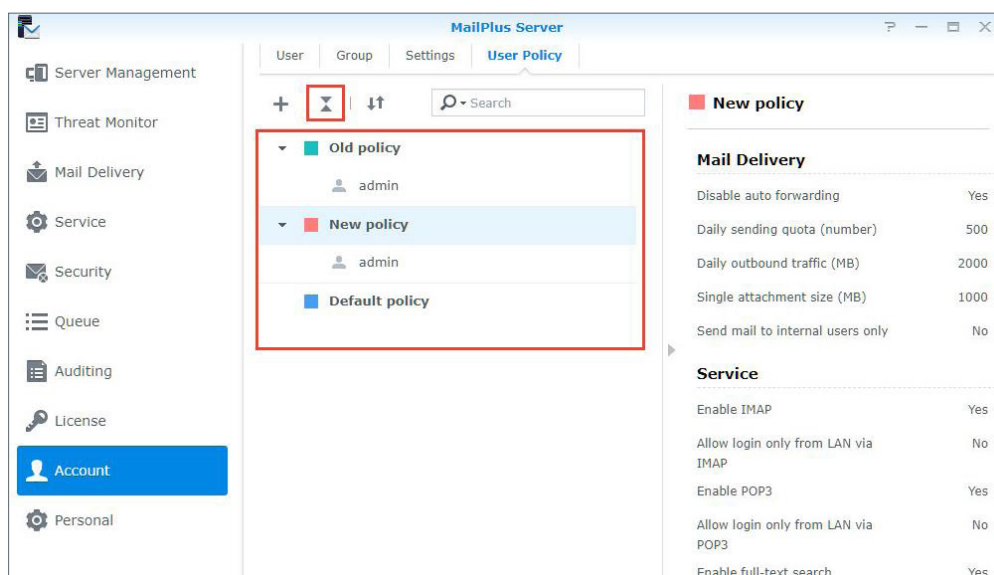
6. 按一下確定來完成設定。
7. 新增完成後，您可以在使用者規範頁面中檢視已新增的規範。點選規範便可在右側面板中預覽規範的設定內容。



### 變更使用者規範優先順序

單一使用者可能會套用多項規範，然而僅一項規範會生效，至於哪一項規範會生效則是依使用者規範的優先順序而定。請參考下列步驟來變更使用者規範的優先順序：

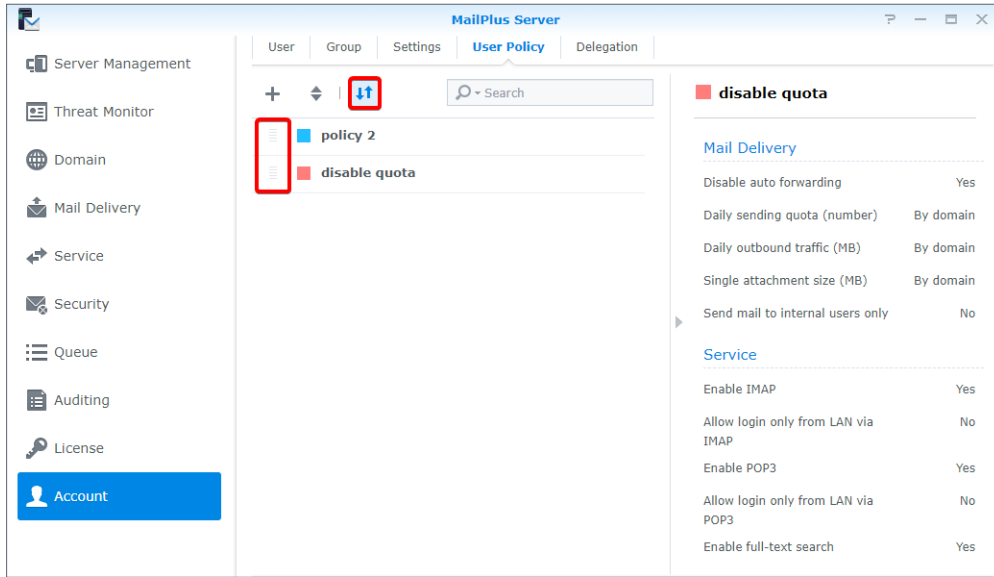
1. 前往帳號 > 使用者規範，按一下雙三角形圖示來顯示或隱藏目標使用者 / 群組。
2. 排序較高的規範比較低者有更高的優先順序。(例如：圖中規範的優先順序由高到低為：*Old policy*、*New policy*、*Default policy*，因此管理員將套用 *Old policy* 而非 *New policy*。)



3. 按一下雙向箭頭圖示來設定優先順序。

#### 注意：

- 若您希望使用者套用特定規範，請確認該項規範的優先順序高於其他規範。



4. 將滑鼠移至規範的左側，根據您理想的優先順序拖拉規範至適合的位置。
5. 按一下雙向箭頭圖示來關閉拖拉功能，讓新的優先順序生效。

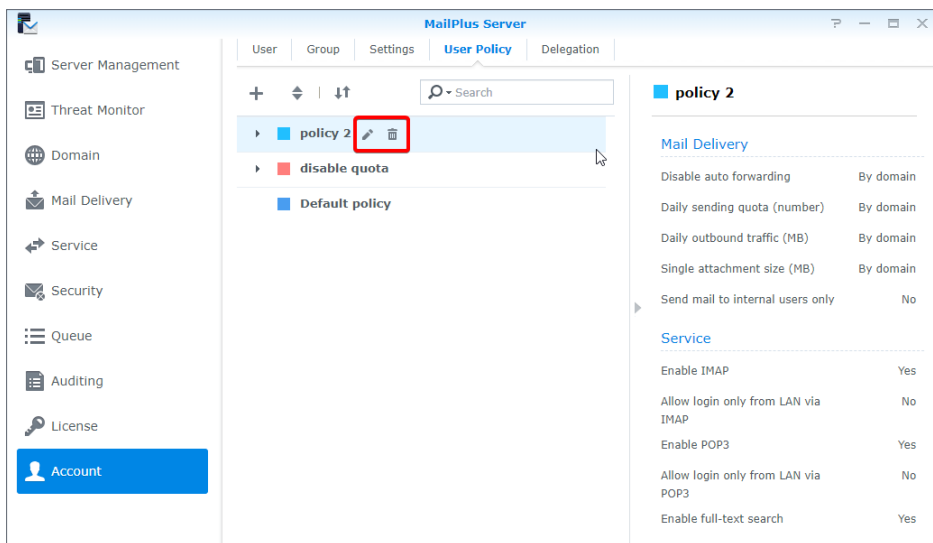
**注意：**

- 預設規範的優先權永遠是最低的。如欲了解更多資訊，請參閱[預設規範](#)。

### 編輯及刪除使用者規範

您可以修改規範的設定、增加或刪除套用規範的使用者、更改規範的顏色。請參考下列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，此時會出現兩個圖示，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

所有未套用自訂規範的使用者，都會套用預設規範。預設規範從一開始就存在，您無法編輯、刪除、重新設定優先順序。請參考下列預設規範的詳細資訊：

|                    |            |
|--------------------|------------|
| 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。      |
| 啟用 IMAP            | 預設為是。      |
| 僅允許從區域網路透過 IMAP 登入 | 預設為否。      |
| 啟用 POP3            | 預設為是。      |
| 僅允許從區域網路透過 POP3 登入 | 預設為否。      |
| 啟用全文檢索             | 預設為是。      |

因為預設規範會套用到所有使用者，某些規範的限制可能不符合您的預期。若您不希望特定限制生效，則必須停用該限制。

## 規範說明與限制

| 編號 | 規範     | 啟用結果         | 停用結果         | 依據網域設定     |
|----|--------|--------------|--------------|------------|
| 01 | 停用自動轉寄 | 使用者無法自動轉寄郵件。 | 使用者可以自動轉寄郵件。 | 規範會依據網域設定。 |

### 注意：

- 此規範不影響手動轉寄。

| 編號 | 規範          | 啟用結果          | 停用結果           | 依據網域設定     |
|----|-------------|---------------|----------------|------------|
| 02 | 每日寄送限額 (數量) | 使用者寄送郵件有數量限制。 | 使用者寄送郵件沒有數量限制。 | 規範會依據網域設定。 |

### 注意：

- 若郵件在送出前就被拒信的話，不會計入使用量。
- 若郵件在送出後才被退信，則會計入使用量。
- 預設規範的設定值與網域頁面的用量限制頁籤中，每日配額區塊的每日限額設定值相同。
- 設定值為 0 時，使用者將不受限制。
- 您必須前往郵件傳送 > 一般，勾選啟用 SMTP 驗證核取方塊。

| 編號 | 規範          | 啟用結果      | 停用結果       | 依據網域設定     |
|----|-------------|-----------|------------|------------|
| 03 | 每日傳送流量 (MB) | 使用者有流量限制。 | 使用者沒有流量限制。 | 規範會依據網域設定。 |

**注意：**

- 若郵件在送出前就被拒信的話，不會計入使用量。
- 若郵件在送出後才被退信，則會計入使用量。
- 預設規範的設定值與網域頁面的用量限制頁籤中，每日配額的每日流量上限 (MB) 設定值相同。
- 設定值為 0 時，使用者將不受限制。
- 您必須前往郵件傳送 > 一般，勾選啟用 SMTP 驗證核取方塊。

| 編號 | 規範            | 啟用結果           | 停用結果            | 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。 | 使用者夾帶的檔案沒有大小限制。 | 規範會依據網域設定。 |

**注意：**

- 預設規範的設定值與郵件傳送頁面的一般頁籤中，單一信件大小限制 (MB) 設定值相同。
- 預設規範的設定值也適用於外部來信。

| 編號 | 規範           | 啟用結果             | 停用結果                |
|----|--------------|------------------|---------------------|
| 05 | 僅可寄送郵件給內部使用者 | 使用者僅可寄送郵件給內部使用者。 | 不限制使用者僅能寄送郵件給內部使用者。 |

| 編號 | 規範      | 啟用結果          | 停用結果          |
|----|---------|---------------|---------------|
| 06 | 啟用 IMAP | 使用者可以使用 IMAP。 | 使用者無法使用 IMAP。 |

**注意：**

- 若服務頁面 IMAP/POP3 區塊中的啟用 IMAP 核取方塊未被勾選，則無法使用 IMAP 服務，使用者規範也不會生效，並不會因為使用者規範設定啟用 IMAP 就能使用 IMAP。

| 編號 | 規範                 | 啟用結果                 | 停用結果                  |
|----|--------------------|----------------------|-----------------------|
| 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：**

- 若服務頁面 IMAP/POP3 區塊中的啟用 IMAP 核取方塊未被勾選，則無法使用 IMAP 服務，使用者規範也不會生效，並不會因為使用者規範設定僅允許從區域網路透過 IMAP 登入就能透過 IMAP 登入。
- MailPlus 網頁用戶端不受此設定限制。



| 編號 | 規範      | 啟用結果          | 停用結果          |
|----|---------|---------------|---------------|
| 08 | 啟用 POP3 | 使用者可以使用 POP3。 | 使用者無法使用 POP3。 |

**注意：**

- 若服務頁面 IMAP/POP3 區塊下的**啟用 POP3** 核取方塊未被勾選，則無法使用 POP3 服務，使用者規範也不會生效，並不會因為使用者規範設定啟用 POP3 就能使用 POP3。

| 編號 | 規範                 | 啟用結果                 | 停用結果                  |
|----|--------------------|----------------------|-----------------------|
| 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：**

- 若服務頁面 IMAP/POP3 區塊下的**啟用 POP3** 核取方塊未被勾選，則無法使用 POP3 服務，使用者規範也不會生效，並不會因為使用者規範設定**僅允許從區域網路透過 POP3 登入**就能透過 POP3 登入。
- 您仍能從外部網路登入 MailPlus(MailPlus 是透過內部網路連線到郵件伺服器)。

| 編號  | 規範     | 啟用結果            | 停用結果             |
|-----|--------|-----------------|------------------|
| 010 | 啟用全文檢索 | 伺服器會索引使用者的郵件內容。 | 伺服器不會索引使用者的郵件內容。 |

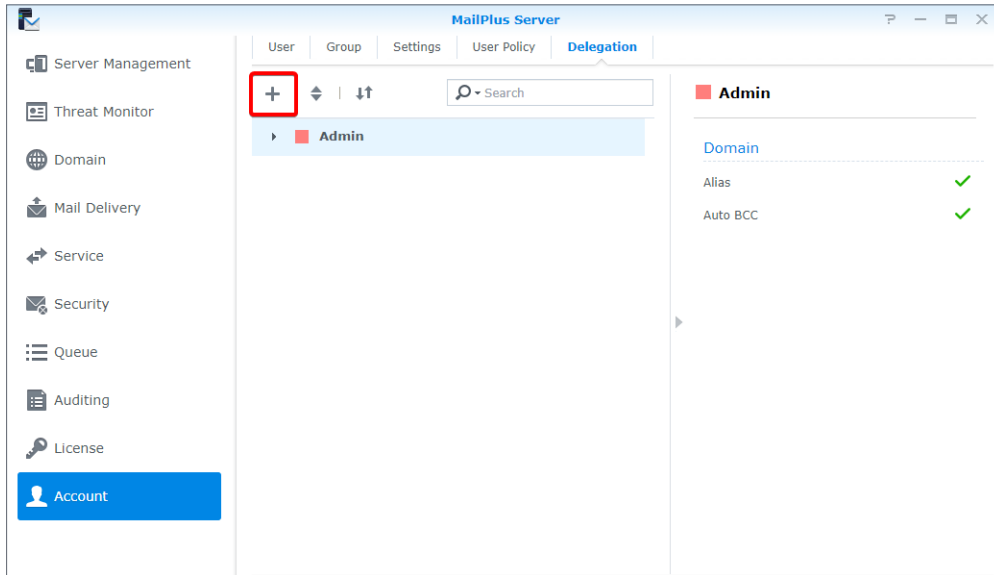
**注意：**

- 若服務頁面中**全文檢索**區塊下的**啟用全文檢索**核取方塊未被勾選，則使用者規範的設定無效，因此不會索引任何使用者的郵件內容。

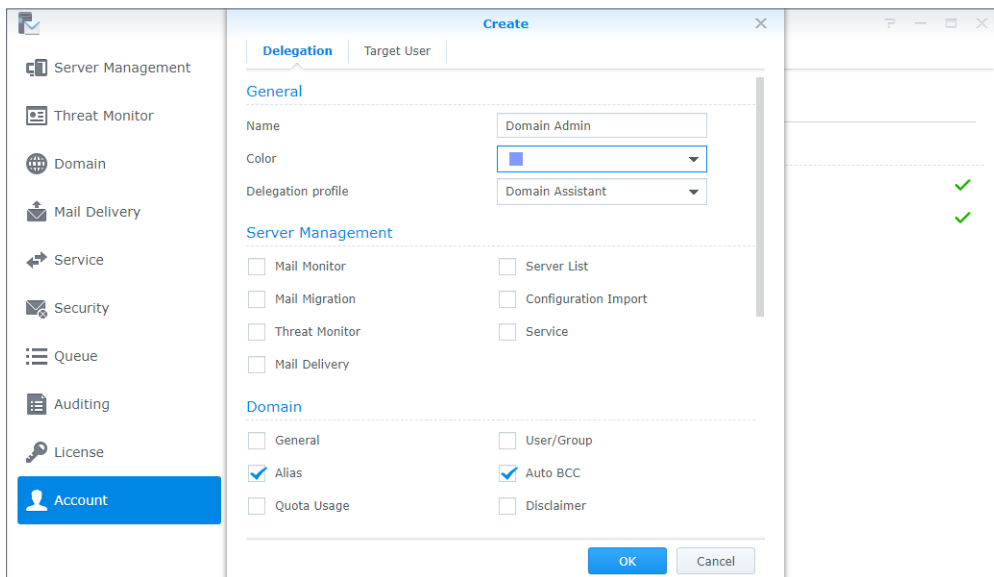
## 新增委派規範

在**管理委派**頁籤中，您可以讓其他使用者依照您指派的管理委派模板，來管理 MailPlus Server 中與伺服器管理、網域、安全性、稽核、帳號 (不含授權) 相關的設定。本章節將以 **Domain Admin** 為例。

1. 前往**帳號 > 管理委派**，按一下上方的加號圖示。

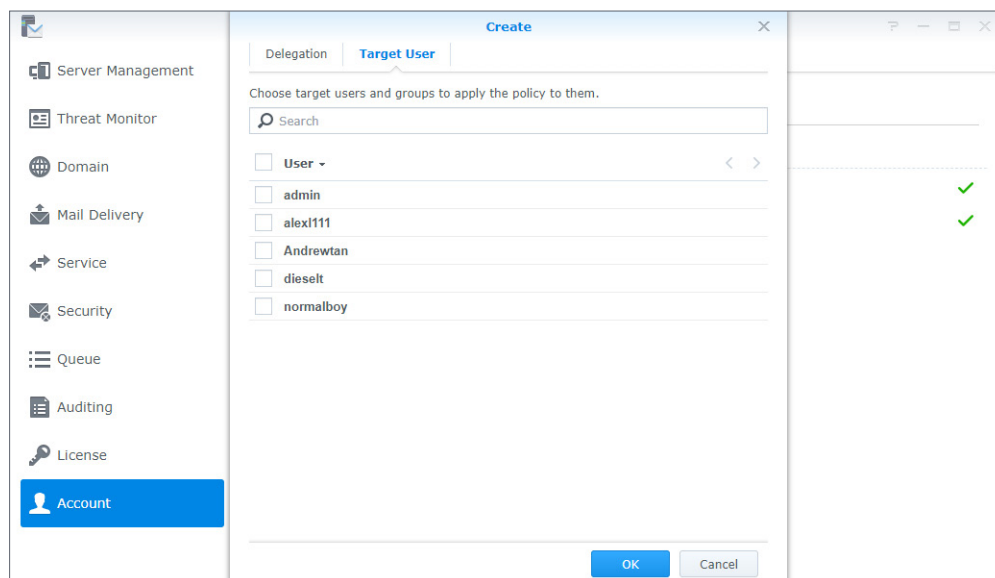


2. 在彈出視窗的**管理委派**頁籤輸入必要資訊。系統會按照您選擇的管理委派模板，自動勾選下方選項。若您勾選或取消勾選下方任一選項，模板會切換為**自訂**。請參考[此文章](#)來了解更多委派權限的資訊。



例如：若您為 **Domain Admin** 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。然而，若您為 **Domain Admin** 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委派規範的使用者或群組。



4. 按一下確定以儲存設定。

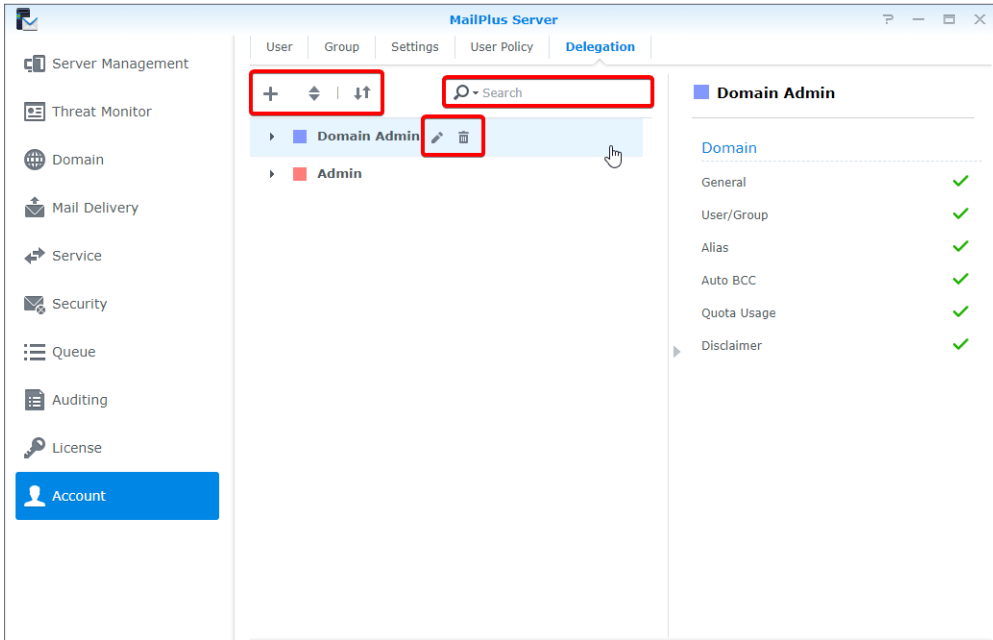
## 管理委派規範

1. 前往帳號 > 管理委派。

2. 選擇 *Domain Admin*，您就可以檢視、編輯、刪除該規範。

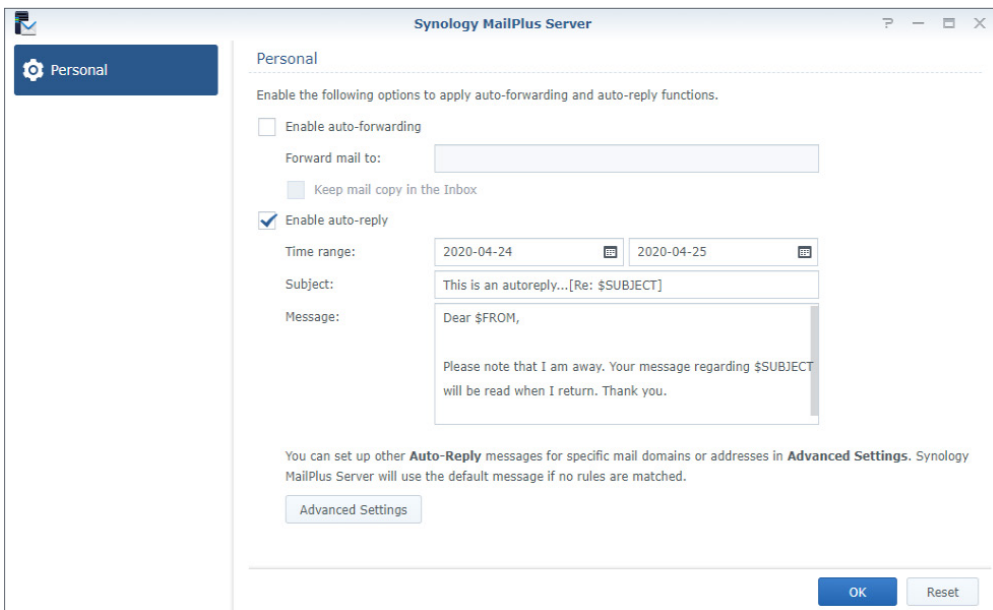
3. 您可以使用上方工具列的按鈕和右方的預覽面板來管理委派規範：

- 設定規範優先順序：
  - 按一下雙向箭頭圖示來設定優先順序。
  - 按一下 *Domain Admin*，並將它拖放至適合的位置。若您為單一使用者 / 群組設定多則委派規範，系統會將清單中優先順序最高的規範套用至該使用者 / 群組。
- 展開 / 收合委派規範：按一下雙三角形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使用者。
- 預覽委派規範：預覽委派規範的名稱、設定及其他細節。
- 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 的權限設定與 DSM 的權限設定同步。在 DSM 中屬於管理員群組的使用者也可以存取 MailPlus Server 的所有設定；而一般使用者僅會看到個人頁面 (如下圖)。



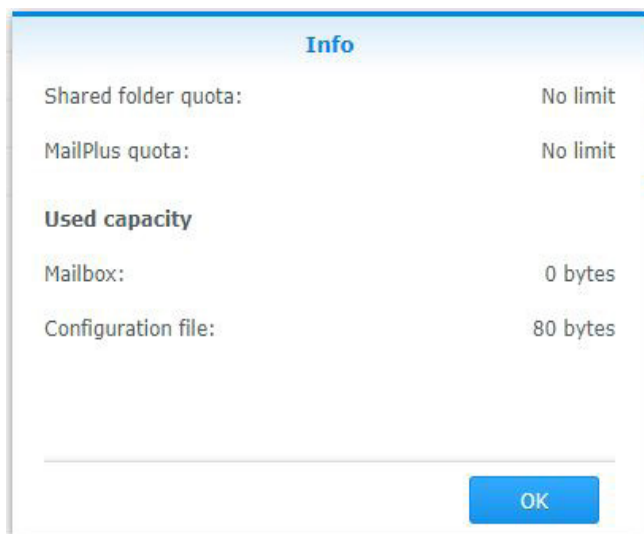
### 注意：

- MailPlus Server 在控制台的權限設定應維持預設，亦即每位使用者都需擁有 MailPlus Server 的權限，否則套件功能可能會受限制。

## 管理配額

MailPlus Server 讓管理員可以設定並管理每個使用者與群組的配額。若要設定配額：

1. 前往**帳號 > 使用者帳號**。
2. 選擇您想設定配額的使用者，按一下**設定配額**以進行以下設定：
  - **MailPlus 配額**：設定郵件匣的大小限制。
  - **剩餘空間通知**：設定警告閾值以通知使用者其郵件匣即將達到儲存空間限制。
3. 按一下**確定**以套用使用者的配額。
4. **資訊**欄位會顯示該使用者的配額及在 DSM 中的已使用容量。



5. 若要設定群組的配額，請按一下**群組**並執行上述步驟。

## 第 6 章：協定設定

MailPlus Server 提供集中管理郵件服務協定相關設定的介面。您可以開啟 / 關閉特定通訊協定的連接埠，或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的對外運作，請確認設定合乎您的需求。

MailPlus Server 的服務使用以下連接埠，請確認這些連接埠並未用於 MailPlus Server 以外的其他服務。

| 類型                     | 連接埠編號                        | 通訊協定      |
|------------------------|------------------------------|-----------|
| SMTP                   | 25、465、587、10025、10465、10587 | TCP       |
| ICAP                   | 1344                         | TCP       |
| Dovecot sieve          | 4190                         | TCP       |
| 灰名單                    | 5252                         | TCP       |
| Redis                  | 8500 - 8501                  | TCP       |
| Memcached              | 8502                         | TCP / UDP |
| 後端                     | 8503 - 8504                  | TCP       |
| Redis for rspamd       | 8505                         | TCP       |
| 叢集協商服務                 | 8506 - 8520                  | TCP       |
| DMARCS                 | 8893                         | TCP       |
| 日誌轉移                   | 9526 - 9529                  | TCP       |
| Memcached              | 11211                        | TCP       |
| Rspamd                 | 11332 - 11334                | TCP       |
| Dovecot 的 Postfix 配額狀態 | 12340                        | TCP       |
| Dsync                  | 24245                        | TCP       |
| Director               | 24246                        | TCP       |

## SMTP

SMTP 相關的協定使用三個連接埠，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** 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 Postfix，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，如須加密，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：

- 不同於 SMTP 協定透過 STARTTLS 來加密，SMTPS 必須在握手後送出加密封包。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-STARTTLS**：SMTP-STARTTLS 所支援的協定為 SMTPS，並透過 STARTTLS 進行加密。SMTP-STARTTLS 需要進行身分驗證，因此常常用來作為用戶端與 **MSA** 之間的內部協定。

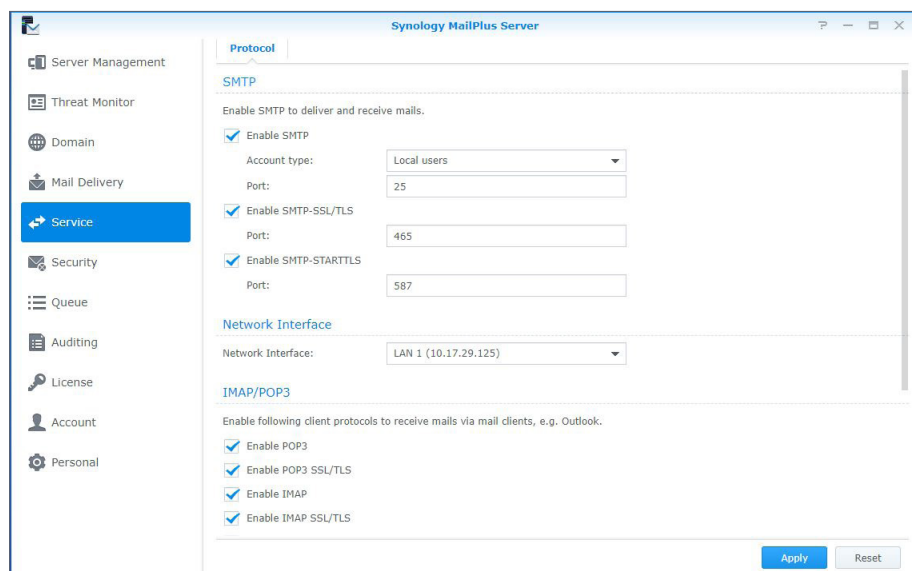
## 設定 SMTP

請參閱下列步驟來設定 SMTP 及其對應的連接埠：

1. 前往**服務 > 通訊協定 > SMTP**，勾選啟用 SMTP 核取方塊。

### 注意：

- SMTP 是郵件伺服器使用的主要協定。



2. 您可以在**連接埠**欄位中變更連接埠編號。

### 注意：

- 若無特別原因，建議您使用預設的 25 連接埠。

## 第 6 章：協定設定

3. 您可以在此調整以下設定：

- **啟用 SMTP-SSL / TLS**：勾選此選項來使用 TLS 加密 MailPlus Server 與其他郵件伺服器或用戶端間的 SMTP 連線。
- **啟用 SMTP-STARTTLS**：勾選此選項來使用 STARTTLS 加密 MailPlus Server 與其他郵件伺服器或用戶端間的 SMTP 連線。

4. 按一下**套用**以儲存設定。

## IMAP / POP3

IMAP 與 POP3 各自提供加密與不加密的選項，因此會使用四個連接埠。在 MailPlus Server 中分別為 IMAP (連接埠編號：143)、IMAPS (連接埠編號：993)、POP3 (連接埠編號：110)、POP3S (連接埠編號：995)。您可以透過這些協定以不同的郵件用戶端取得 MailPlus Server 上的郵件資訊。

### 注意：

- 兩種協定皆使用 STARTTLS 進行加密。由於 DSM 不再支援 SSL 加密連線，所以請不要設定 SSL 加密連線。
- **IMAP**：**IMAP** 是讓使用者存取郵件伺服器上存放資料資料的標準協定，IMAP 用戶端會直接修改存放在郵件伺服器上的郵件，被修改的郵件會鏡像複製到各個 IMAP 用戶端的郵件匣，因此所有變更都能即時同步到各個裝置。
- **POP3**：**POP3** 是讓使用者存取郵件伺服器上存放資料的標準協定，POP3 用戶端會從郵件伺服器下載郵件到本地端，因此對郵件所做的更動並不會同步到郵件伺服器。

## 設定 IMAP / POP3 協定

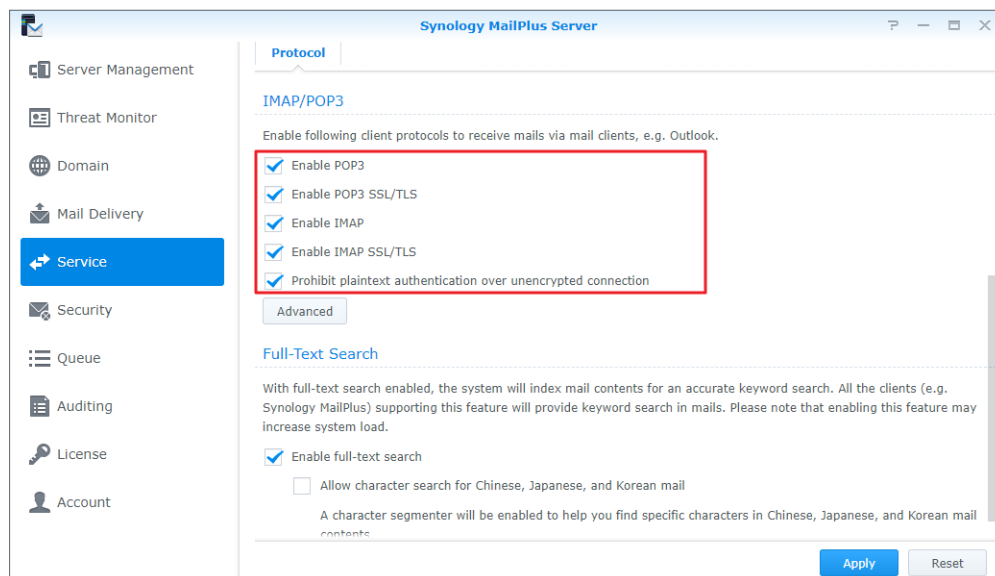
請參考下列步驟來設定 IMAP、POP3 及對應的連接埠：

1. 前往**服務 > IMAP/POP3**。

2. 您可以在 **IMAP/POP3** 區塊中調整以下設定：

- **啟用 POP3**：勾選以允許用戶端郵件軟體透過 POP3 收取郵件。
- **啟用 POP3 安全連線 (SSL/TLS)**：勾選以允許透過 SSL / TLS 保護 POP3 用戶端連線。
- **啟用 IMAP**：勾選以允許用戶端郵件軟體透過 IMAP 收取郵件。
- **啟用 IMAP 安全連線 (SSL/TLS)**：勾選以允許透過 SSL / TLS 保護 IMAP 用戶端連線。





3. 按一下套用以儲存設定。

## 網路介面

為支援[高可用叢集](#)，在您安裝 MailPlus Server 或設置高可用後，MailPlus Server 會與網路介面綁定，伺服器上的郵件服務將運行在綁定的網路介面上。

### 網路介面綁定

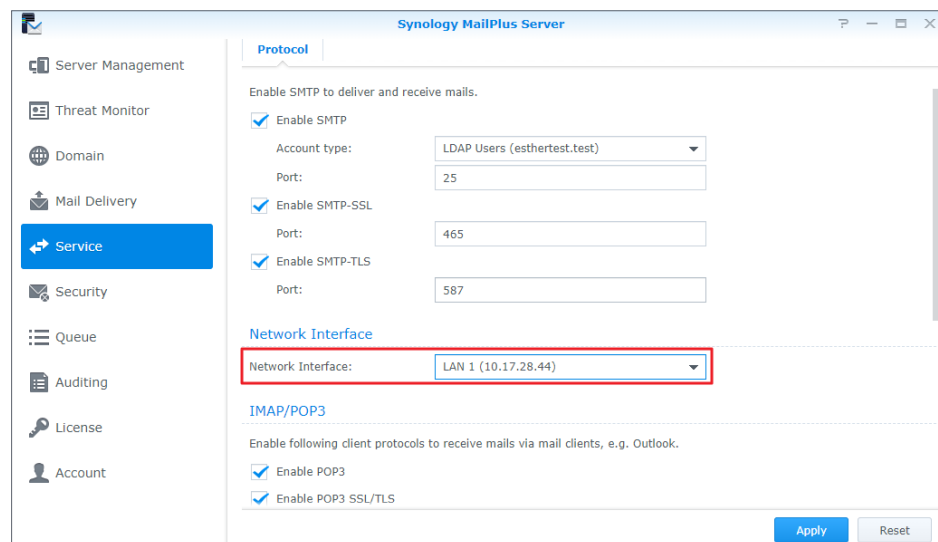
當 MailPlus Server 在單台伺服器上運行時，您可以將 MailPlus Server 與區域網路、PPPoE 或結合的網路介面綁定。當 MailPlus Server 在高可用架構下運行時，您可以將 MailPlus Server 與區域網路或結合的網路介面綁定，您可以透過[手動設定網路組態](#)來取得該網路介面的 IP 位址。

#### 注意：

- 一旦 MailPlus Server 與結合的網路介面綁定，便無法解除兩者間的連結。若要取消綁定已結合的網路介面，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. 按一下套用以儲存設定。

# 第 7 章：SMTP 設定

在安裝階段完成 MailPlus Server 基本設定後，您可能會需要針對使用者登入及接收 / 寄送郵件，設定相關的 SMTP 限制。

## 服務設定

您可以前往**郵件傳送**頁面來設立郵件收發規則。

MailPlus Server 提供快速且方便的服務設定選項，包含：

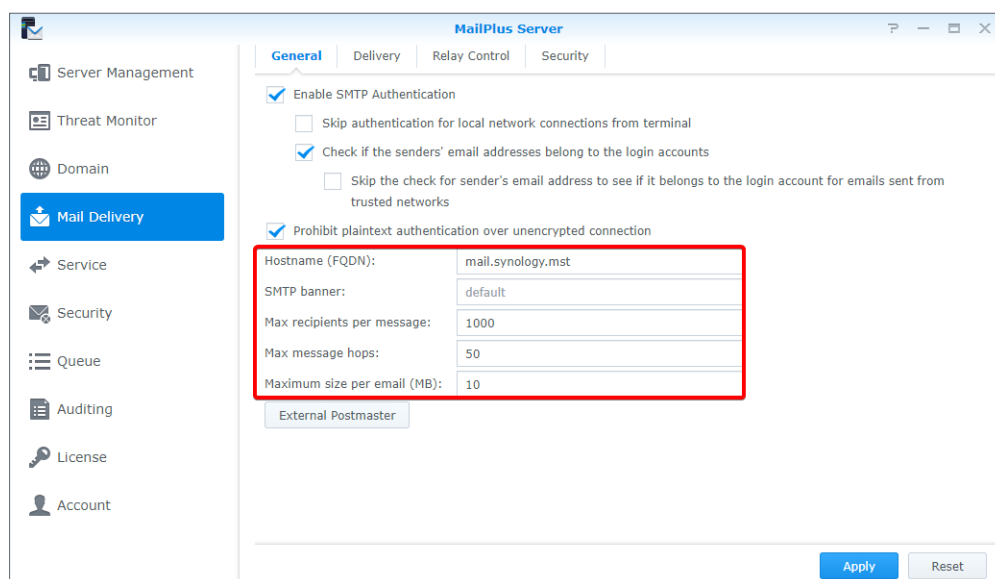
- **SMTP 規則**：您可以為 MailPlus Server 指定主機名稱、在用戶端的 Telnet 終端機上指定 SMTP 橫幅，亦可設定收發郵件規則，例如單一信件大小限制、收件人數上限等，避免佔用太多資源。
- **全文檢索**：您可以啟用全文檢索功能來提升查找郵件的效率，此功能讓 MailPlus 網頁用戶端對郵件進行索引，亦支援以中文、日文、韓文字元搜尋。由於全文檢索會對所有的郵件內容進行索引，可能會增加伺服器的負載，您可以自行決定是否啟用全文檢索功能，或是停用特定使用者的全文檢索功能。請參考[新增使用者規範](#)來了解更多資訊。

## 設定 SMTP 規則

SMTP 規則為 MailPlus Server 如何將郵件寄送至其他郵件伺服器的規則。

### 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，並確認此名稱與 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**：設定接收及寄送郵件訊息的收件人數上限，超過此數量的郵件會被拒絕。
- **郵件訊息躍點 (hop) 數上限**：設定接收及寄送郵件訊息的躍點 (亦即郵件轉送) 數量上限，超過此數量的郵件會被拒絕。
- **單一郵件大小限制 (MB)**：設定接收及寄送郵件訊息的檔案大小上限，超過此數量的郵件會被拒絕。

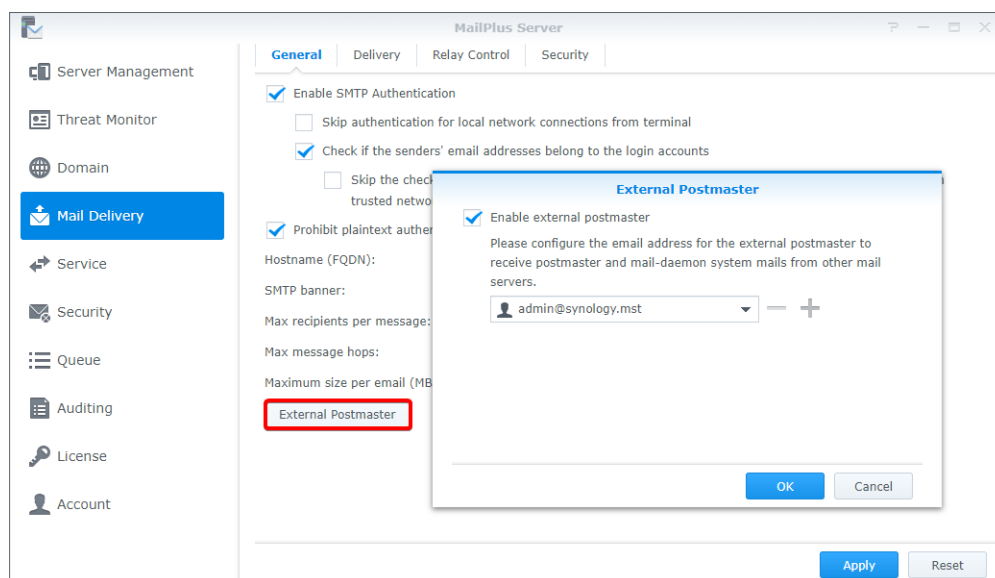


2. 按一下套用以儲存設定。

## 外部郵件管理者

外部郵件管理者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. 勾選啟用外部郵件管理者核取方塊。
4. 按一下加號圖示 / 新增來加入外部郵件管理者的郵件地址。



5. 按一下確定以儲存設定。

## 全文檢索

啟用全文檢索功能時，伺服器會對每封信的主旨、寄件人、收件人、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，提升系統查找郵件的速度。

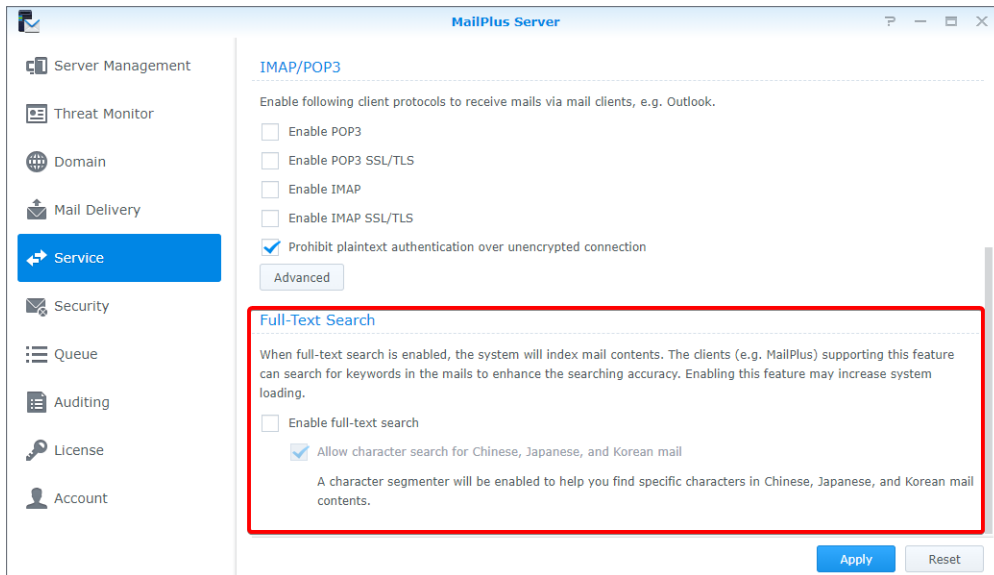
**注意：**

- 若您收發大量郵件，啟用此功能可能會增加伺服器負載。

1. 前往服務。

2. 您可以在全文檢索區塊調整以下設定：

- 啟用全文檢索：勾選此選項後，您可以參考[新增使用者規範](#)來了解詳細資訊。您可以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：勾選此選項後，會啟用斷字工具協助您尋找中文、日文、韓文郵件中的特定字元。



3. 按一下套用以儲存設定。

## SMTP 安全連線

MailPlus Server 透過分析使用者連線、登入資訊、郵件內容，加強郵件伺服器的安全性和穩定性，不僅保障服務品質，同時也能防止 MailPlus Server 成為開放式的垃圾郵件轉發伺服器，而被列入黑名單。

- **SMTP 驗證**：啟用 SMTP 驗證後，在透過伺服器轉送郵件時，使用者需輸入 DSM 帳號及密碼來進行驗證。

**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開放垃圾郵件轉發。請參考[此篇文章](#)來取得更多資訊。

- **黑名單與白名單**：若您的伺服器持續收到垃圾郵件，您可以透過在黑名單中設置特定條件來拒絕來自特定來源的郵件服務。另一方面，MailPlus Server 進行**防毒掃描**、**身分驗證**或其他掃描功能時，可能會拒絕合法郵件，在此情況下，您可以使用白名單來跳過安全性掃描以確保重要郵件能夠成功寄達。
- **寄件人規範**：您可以設定條件來拒絕不合格的格式或是無法驗證的寄件人地址。
- **連線規範**：您可以限制來自無法辨識或可能造成 MailPlus Server 超載的用戶端主機連線。
- **進階速限**：在連線階段要求精確的指令及其他進階設定，請參閱**進階設定**以了解更多資訊。

## 啟用 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轉送垃圾郵件。建議您啟用 SMTP 驗證功能，讓未通過身分驗證的使用者無法轉送他們的郵件，避免您的伺服器被列入黑名單。

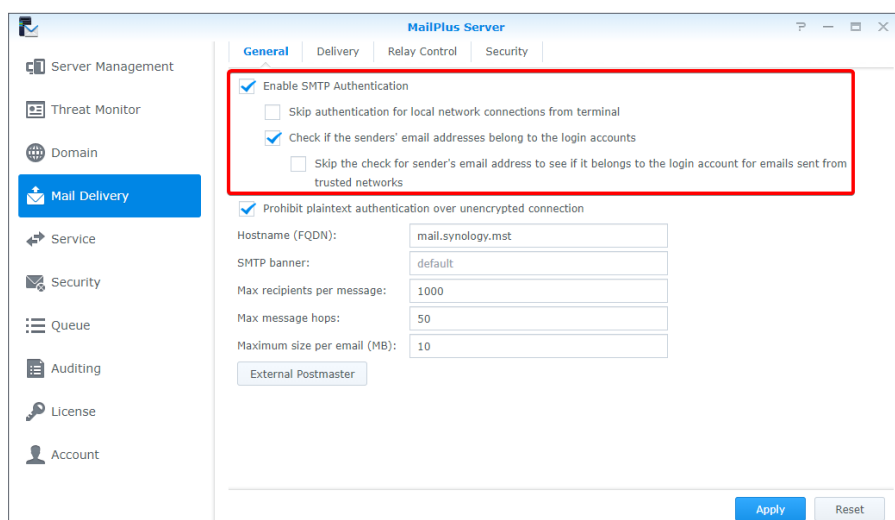
### 注意：

- MailPlus Server 中的部分功能（例如：**每日配額**）需通過身分驗證才能使用。

1. 前往**郵件傳送 > 一般**，選擇是否勾選**啟用 SMTP 驗證**核取方塊。
2. 若勾選**啟用 SMTP 驗證**核取方塊，您可以進一步調整以下設定：
  - **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**：使用者必須使用屬於該登入帳號的電子郵件地址來寄送郵件。

### 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 可能會拒絕來自**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分驗證**，MailPlus Server 將不會封鎖來自區域網路的郵件。



3. 按一下**套用**以儲存設定。

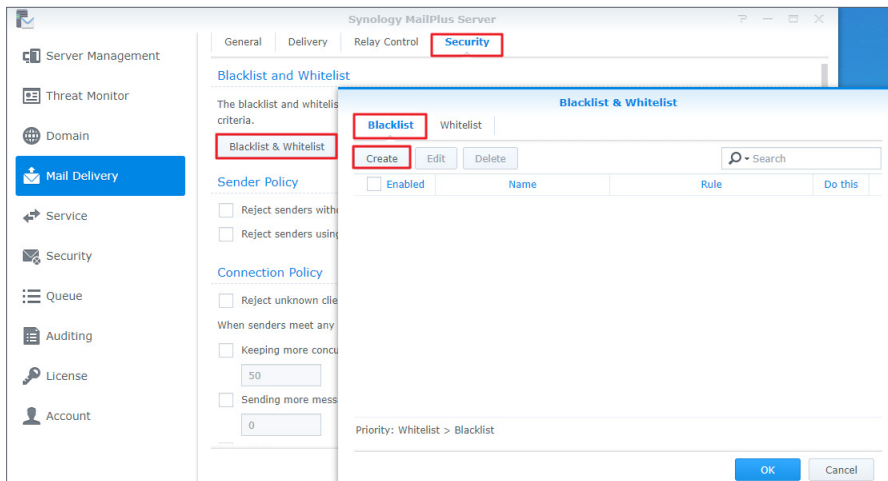
## 新增黑白名單

系統會對符合黑白名單條件的郵件採取相對應的動作。您可以參考下列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](#) 段落。

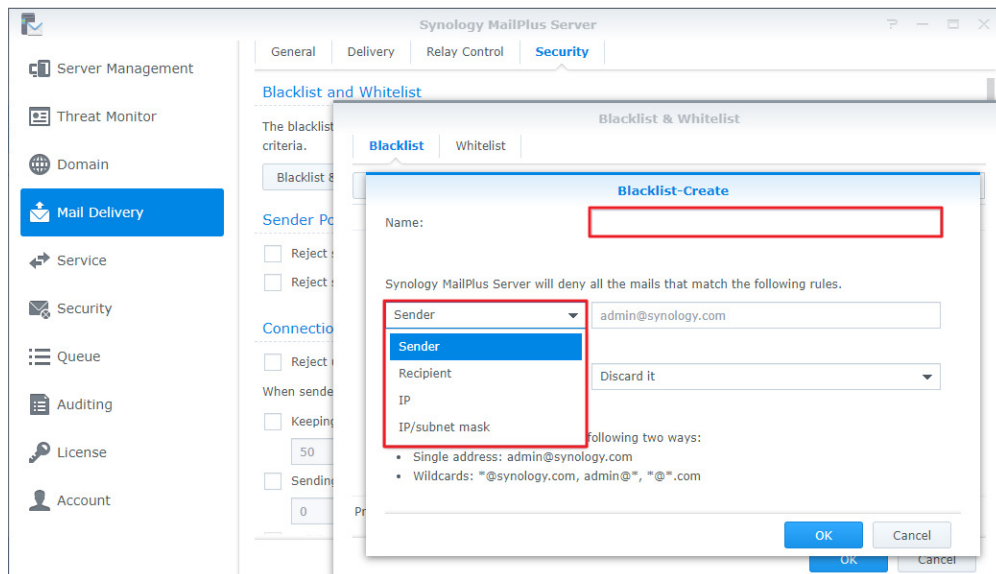
1. 前往郵件傳送 > 安全性，按一下黑 & 白名單。
2. 您可以在黑 & 白名單視窗中管理黑名單與白名單。此段落將以黑名單為例。
  - 黑名單：設定規則來拒絕 / 捨棄符合的郵件訊息。
  - 白名單：設定規則來允許符合的郵件訊息。
3. 在黑名單頁籤中按一下新增。



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：
  - 寄件人：當寄件人的郵件地址符合條件時，系統將採取指定動作。
  - 收件人：當收件人的郵件地址符合條件時，系統將採取指定動作。
  - IP：當寄件人的 IP 位址符合條件時，系統將採取指定動作。
  - IP/子網路遮罩：當寄件人的 IP 位址及子網路遮罩符合條件時，系統將採取指定動作。
  - 網域：當寄件人網域符合條件時，系統將採取指定動作。此選項僅適用於白名單。

**注意：**

- 寄件人的郵件地址是擷取自 MAIL FROM 資訊。
- 收件人的郵件地址是擷取自 RCPT TO 資訊。



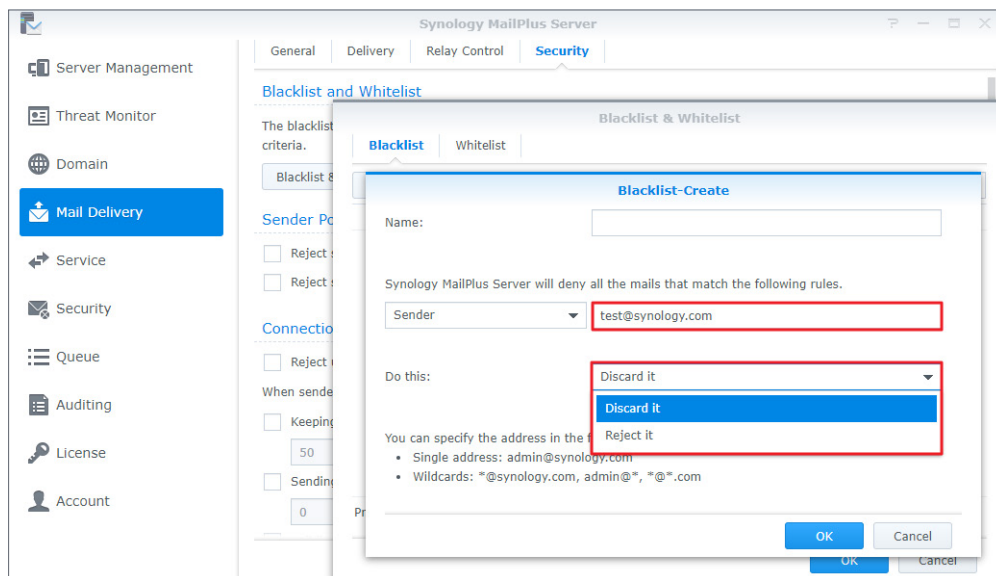
6. 為選擇的規則類別輸入條件，條件格式請參照灰字範例。寄件人和收件人地址支援萬用符號 (\*)。

7. 從執行下拉式選單中選擇符合條件時會採取的動作。

**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：寄件人會收到拒信通知。
- 捨棄：寄件人不會收到拒信通知。

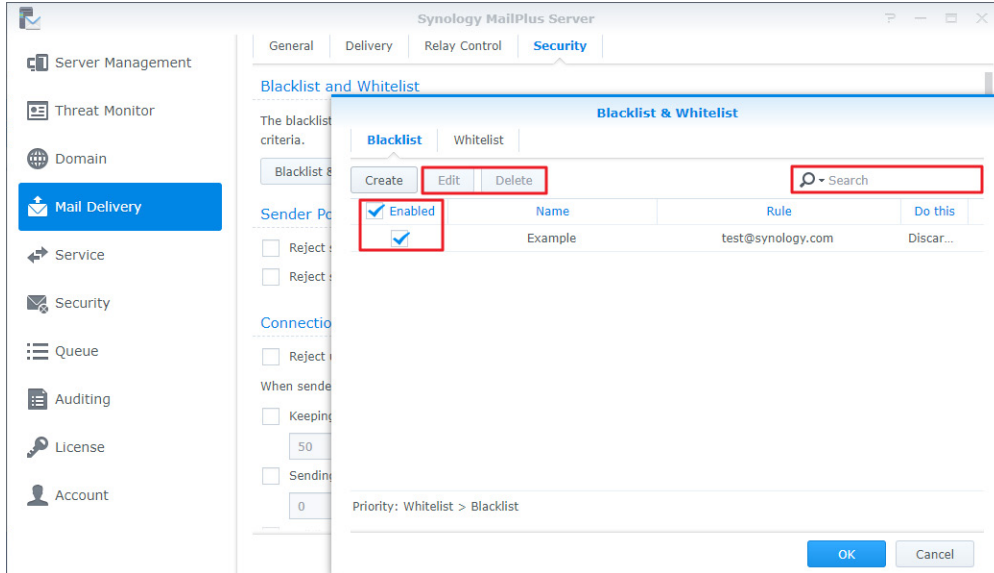


8. 按一下確定來完成設定。



### 編輯及刪除黑 & 白名單

1. 在黑 & 白名單視窗右上角的搜尋欄位輸入關鍵字來搜尋您想修改的黑名單或白名單。
2. 您可以勾選啟用核取方塊，來啟用或停用該規則(不需特地將規則從黑白名單中移除)。
3. 若您想要編輯或是刪除特定規則，請先選取該規則，再按一下編輯或刪除按鈕。
4. 按一下確定以儲存設定。



### 白名單的說明與限制

白名單設定可能會跳過黑名單的必要測試，此外，依據設定類型也有可能跳過 DNSBL、SPF、防毒掃描、DKIM、DMARC 檢測。下表顯示不同白名單設定所跳過的安全性檢測：

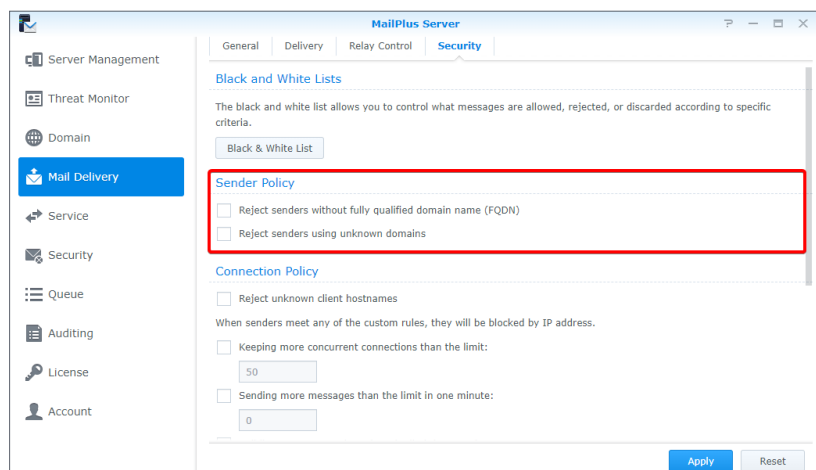
|          | DNSBL | SPF | 防毒掃描 | DKIM | DMARC | smtpd_*_restrictions |
|----------|-------|-----|------|------|-------|----------------------|
| IP 位址    | ✓     | ✓   | ✓    | ✓    | ✓     | ✓                    |
| IP/子網路遮罩 | ✓     | ✓   |      | ✓    | ✓     | ✓                    |
| 寄件人      |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

**注意：**

- 有些檢測項目是白名單無法跳過的，若郵件無法通過該檢測，便會被退信。例如：若寄件者 admin@example.com 列為白名單，由於寄件人條件不支援 DNSBL、DKIM、DMARC，因此必須通過 DNSBL、DKIM、DMARC 的檢測，才不會被退信。
- 若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。

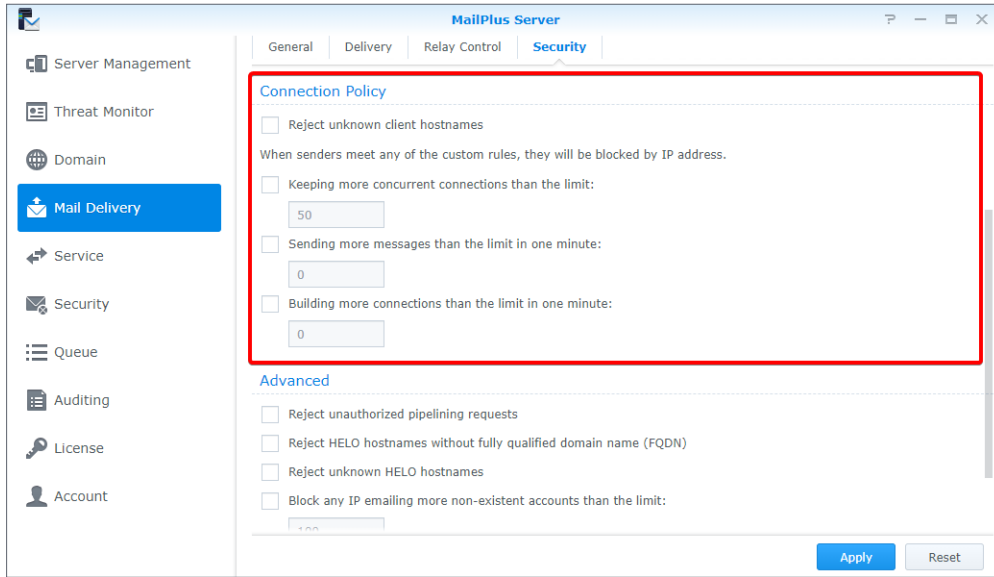
## 寄件人規範

1. 前往郵件傳送 > 安全性。
2. 在寄件人規範區塊中，設定條件以拒絕郵件。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 MAIL FROM 資訊中的網域名稱與 DNS A 記錄及 MX 記錄不相符，或者 MX 記錄不正確時，便會拒絕其郵件。



## 連線規範

1. 前往郵件傳送 > 安全性。
2. 於連線規範區塊中設定條件來限制用戶端連線或是阻擋可疑的 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 IP 位址或主機名稱不正確 / 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 位址的同時連線數量超過此上限值，則之後的連線會被封鎖，直到總連線數低於上限值時，才會開放新的連線加入。
  - 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 寄出的郵件會被封鎖一分鐘。
  - 一分鐘內建立的連線數量超過上限：您可以設定一分鐘內的最大連線數量，若同一 IP 位址在一分鐘內的連線數量超過此上限值，便會被封鎖連線一分鐘。

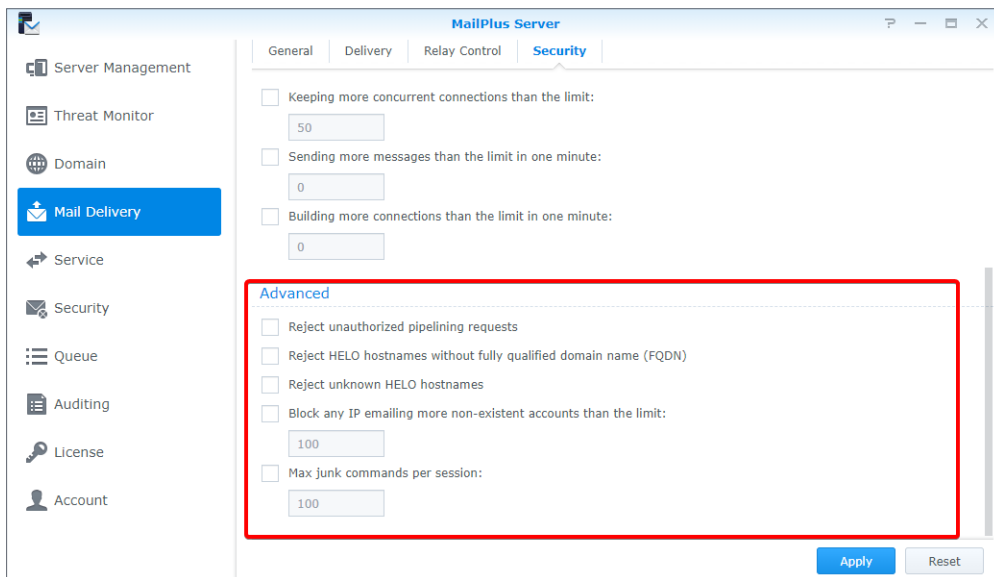


### 進階設定

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 記錄或 MX 記錄的主機連線。
- 寄送郵件至不存在的帳號 (數量超過上限) 時，立即封鎖 IP：若同一 IP 位址的用戶在一天內寄送郵件至 MailPlus Server 上不存在的帳號超過設定值，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 (亦即 NOOP、VRFY、ETRN、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郵件，或是替其他伺服器收發郵件，您可以設定郵件轉送、SMTP 驗證、加密及其他安全性設定。

### 設定傳送控制

在傳送頁籤中，您可以設定 MailPlus Server 要透過哪台伺服器來轉送郵件，讓所有寄出的郵件經由指定的伺服器寄送。

1. 前往郵件傳送 > 傳送 > 轉送設定。

2. 選擇規則類型：

- 直接從此伺服器寄送信件：所有信件皆直接從 MailPlus Server 寄出。
- 所有郵件均透過單一主機轉送郵件：所有信件會透過您在下方設定的轉送伺服器寄出。在伺服器欄位中輸入轉送伺服器的 IP 位址或主機名稱，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，您亦可修改下列安全性設定：
  - 使用安全連線 (TLS)：MailPlus Server 將會送出 STARTTLS 來啟用加密連線，若 MailPlus Server 是轉送伺服器，請參考[此處](#)。MailPlus Server 的 TLS 安全層級預設是 may。
  - 需要身分驗證：若您的轉送伺服器有啟用身分驗證，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。

Synology MailPlus Server

General Delivery Relay Control Security

Relay Settings

Choose one of the following methods to deliver the outbound mails.

Send mails directly from this server

All mails are sent through a single relay host

Server:

Port:

Always use a secure connection (TLS)

Authentication required

Account:

Password:

Relay Exceptions

Set up relay rules for specific addresses or domains.

Relay Host List

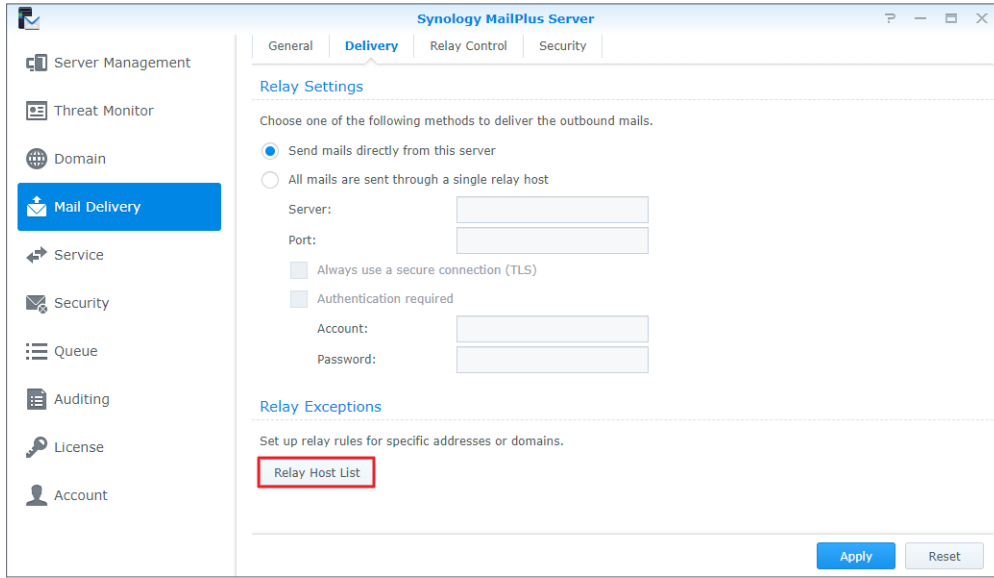
Apply Reset

#### 注意：

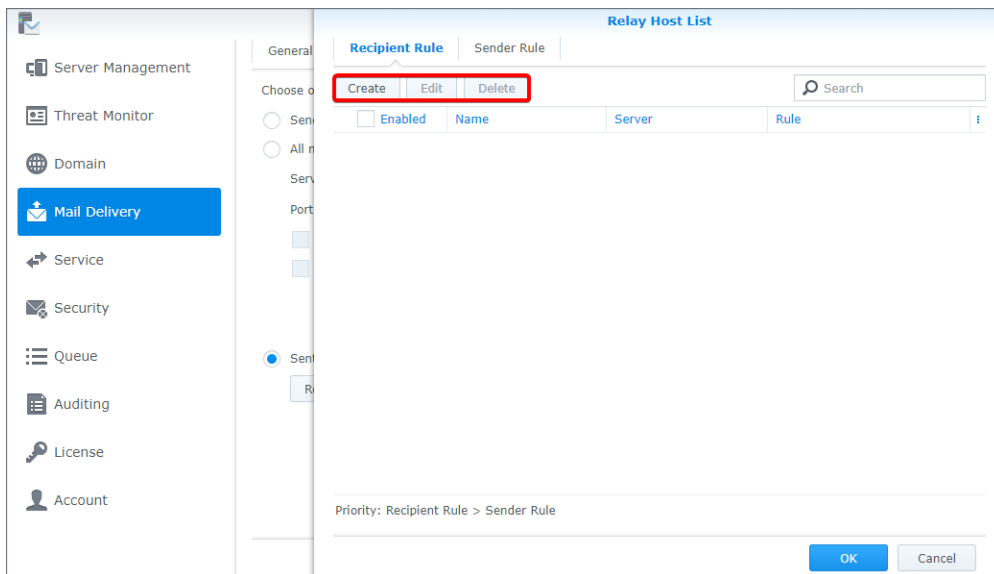
- STARTTLS 與 SMTPS 有所不同。目前 MailPlus Server 並沒有提供設定 SMTPS 的頁面，若希望使用 SMTPS，請參考 [wrappermode](#) 來進行設定。

## 第 7 章：SMTP 設定

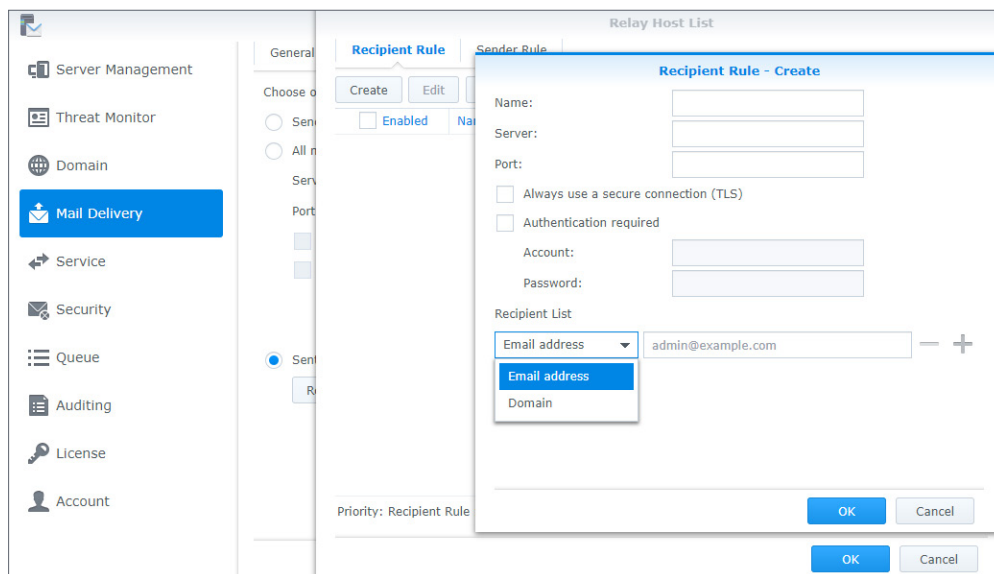
若郵件的郵件地址或網域符合特定規則，可透過指定的轉送伺服器寄出。您可以按一下**轉送例外**下方的**轉送伺服器清單**按鈕來調整收件者及寄件者規則。



- **收件者規則**：寄送至指定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。
  - a. 按一下**新增**、**編輯**、**刪除**按鈕來管理收件者與寄件者規則。



- b. 輸入規則名稱並指定轉送伺服器及連接埠。
- c. 選擇電子郵件地址或網域來編輯**收件者清單**，讓轉送到伺服器的郵件能被指定地址或網域收下。
- d. 按一下**確定**以儲存設定。



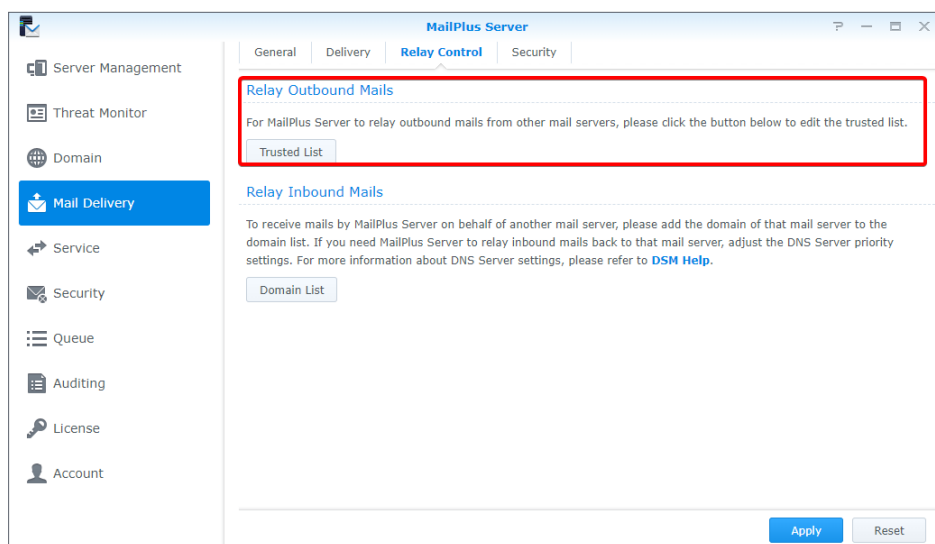
e. 按一下套用以完成設定。

## 設定轉送控制

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

• 若要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，輸入規則名稱。輸入其他郵件伺服器的 IP 位址或子網路遮罩。
4. 按一下確定以儲存設定。

**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 可能會拒絕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分驗證，MailPlus Server 將不會封鎖來自區域網路的郵件。

### 替其他郵件伺服器代收郵件

您需要先設定 DNS 記錄，才能替其他郵件伺服器代收郵件。您可以參考以下步驟建立記錄，再到網域清單新增郵件伺服器。此處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。此處將以 Bluehost® 為例。
2. 登入 Bluehost® 後，修改以下設定：在外部 DNS 伺服器的 MX 記錄輸入您的網域名稱，並將 MailPlus Server 的 IP 位址輸入至 A 記錄。如此一來，其他郵件伺服器就可以依照這些 DNS 記錄將郵件寄至 MailPlus Server。

Zone File Records

A (Host) [What's this?](#)

| Host Record | Points to     | TTL   | ACTION |
|-------------|---------------|-------|--------|
| mail        | 61.216.79.120 | 14400 |        |

CNAME (Alias) [What's this?](#)

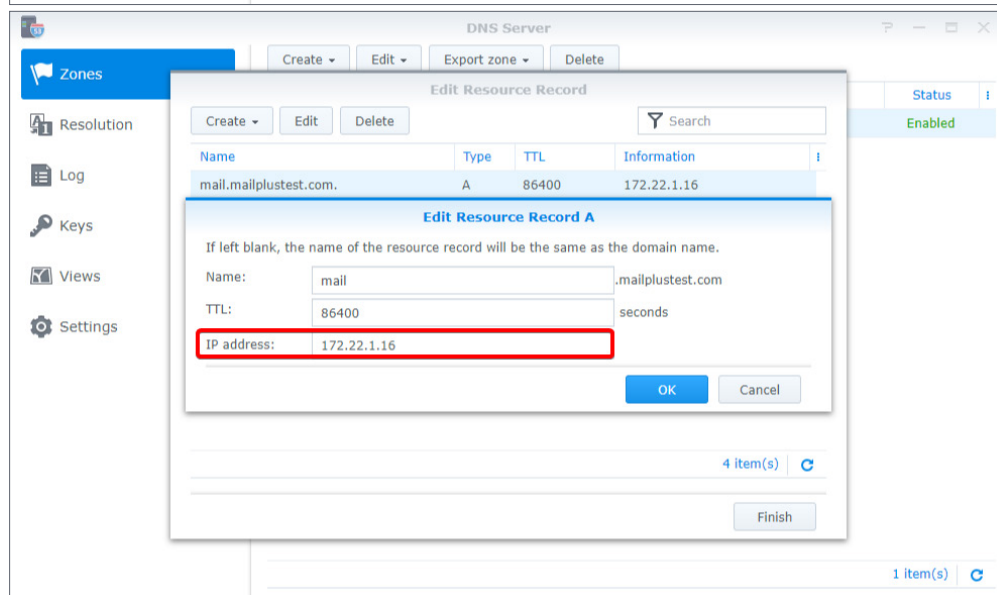
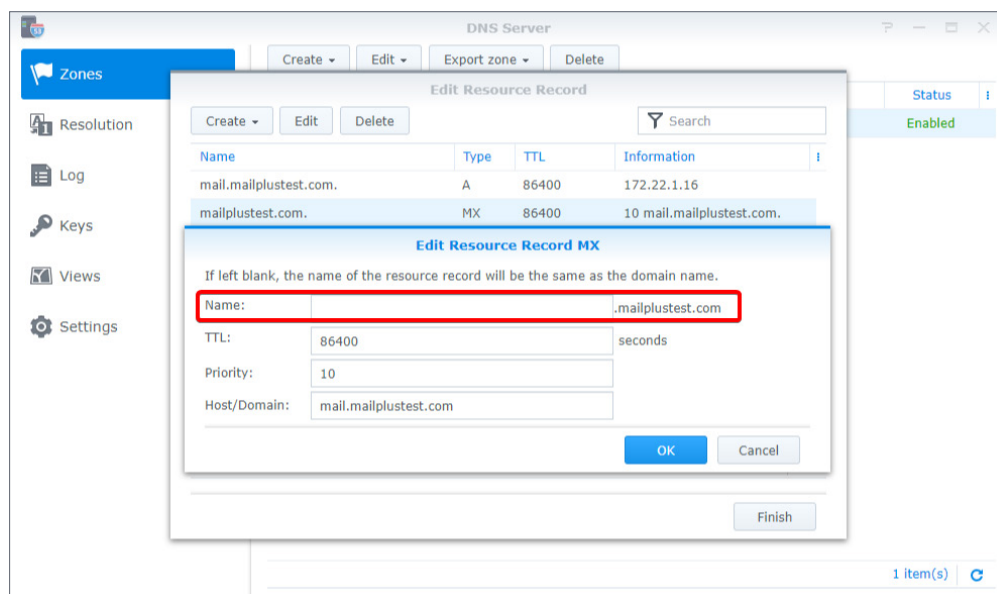
| Host Record | Points to             | TTL   | ACTION |
|-------------|-----------------------|-------|--------|
| www         | mailplustest.com      | 14400 |        |
| ftp         | mailplustest.com      | 14400 |        |
| cpanel      | mailplustest.com      | 14400 |        |
| webmail     | mailplustest.com      | 14400 |        |
| imap        | mail.mailplustest.com | 14400 |        |
| pop         | mail.mailplustest.com | 14400 |        |
| smtp        | mail.mailplustest.com | 14400 |        |

MX (Mail Exchanger) [What's this?](#)

Email Routing: Automatically Detect Configuration: Remote [more »](#)

| Priority | Host Record | Points to             | TTL   | ACTION |
|----------|-------------|-----------------------|-------|--------|
| 0        | @           | mail.mailplustest.com | 14400 |        |

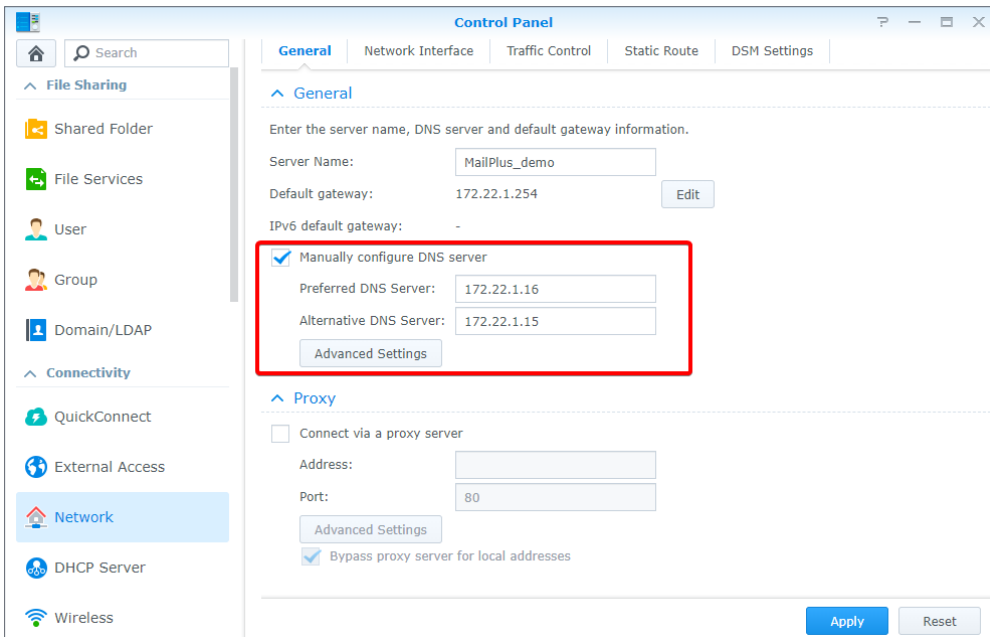
3. 為 MailPlus Server 設定 Synology 內部 DNS 伺服器來指引主要郵件伺服器。
4. 在內部 DNS 伺服器的 MX 記錄輸入您的網域名稱，並在 A 記錄輸入網域的 IP 位址。在內部 DNS 伺服器上的 DNS 記錄的優先順序必須高於外部 DNS 伺服器上的 DNS 記錄。



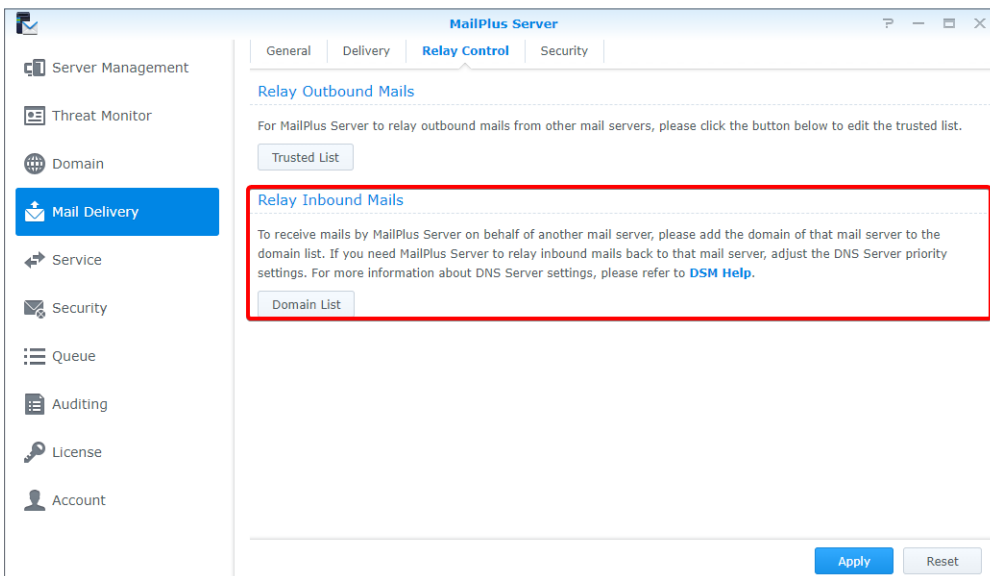


## 第 7 章：SMTP 設定

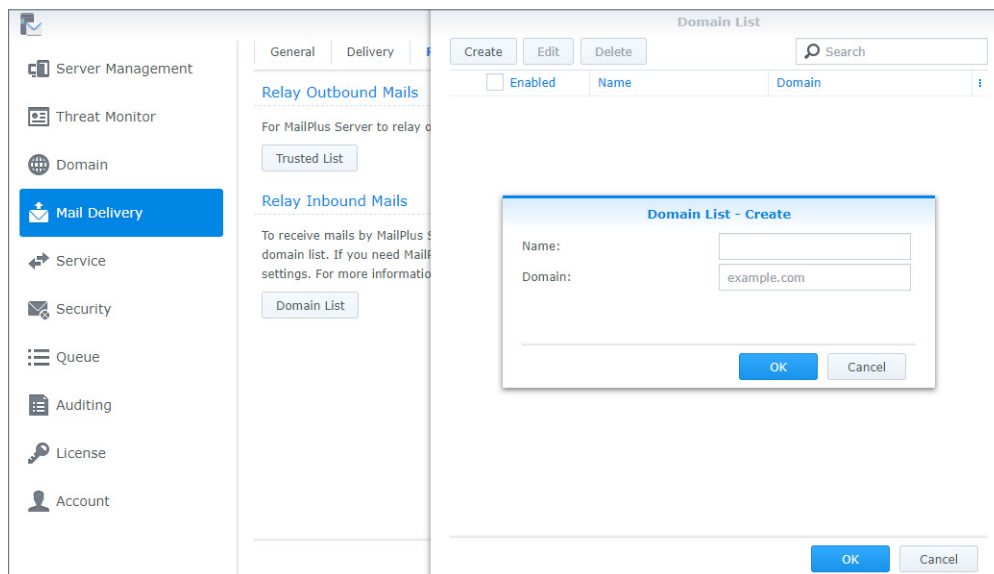
5. 前往 **DSM > 控制台 > 網路 > 一般**，勾選**手動設定網域名稱伺服器 (DNS)** 核取方塊，在慣用 **DNS 伺服器** 欄位輸入內部 DNS 伺服器的 IP 位址，並在**替代 DNS 伺服器** 欄位輸入外部 DNS 伺服器的 IP 位址，確保 MailPlus Server 的內部與外部連線皆正常運作。MailPlus Server 收到郵件後，會檢查兩台 DNS 伺服器的 MX 記錄，並將郵件送至優先順序較高的郵件伺服器。



6. 開啟 MailPlus Server 並前往**郵件傳送 > 轉送控制**。在代收郵件區塊中，按一下**網域清單**。



7. 按一下**新增**按鈕。
8. 輸入規則名稱與網域。



9. 按一下**確定**以儲存設定。

# 第 8 章：網域設定

**注意：**

- 雖然郵件是從內部寄送，您仍應在安全性頁面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。
- 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。
- 所有伺服器的網路區段必須相同。

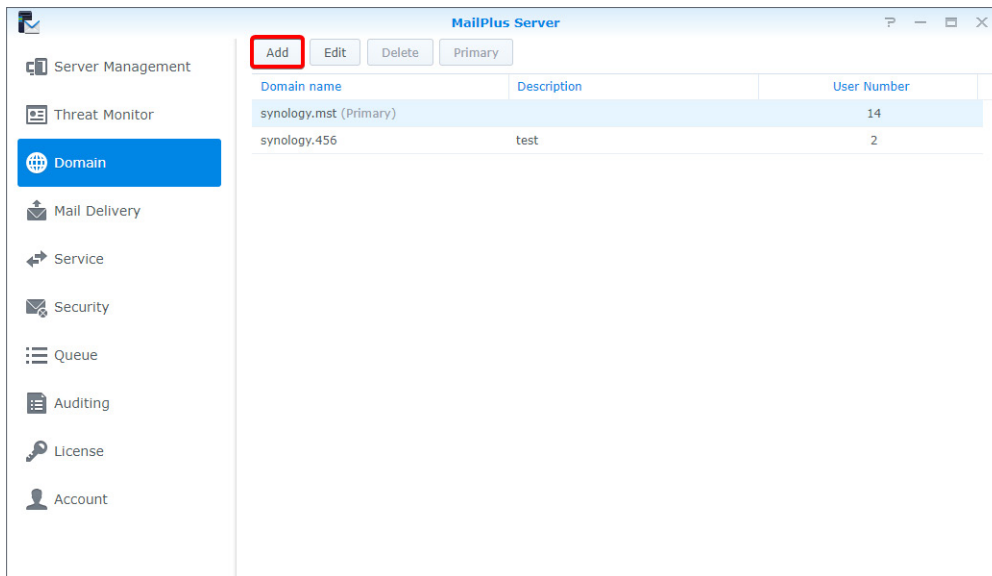
## 網域

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。您亦可為各個網域自訂別名、自動密件副本、用量限制、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。本章節將以 *synology.456* 為例。

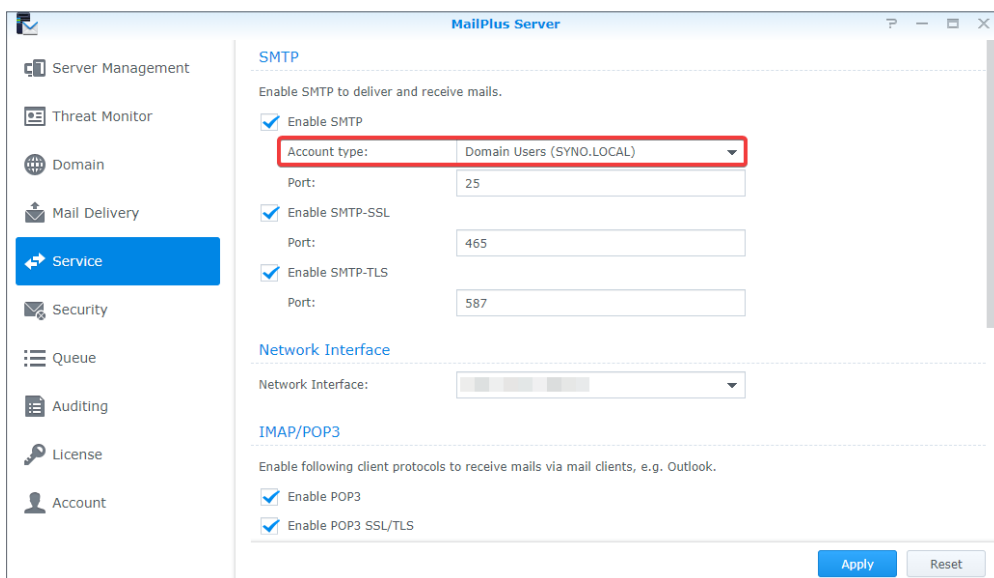
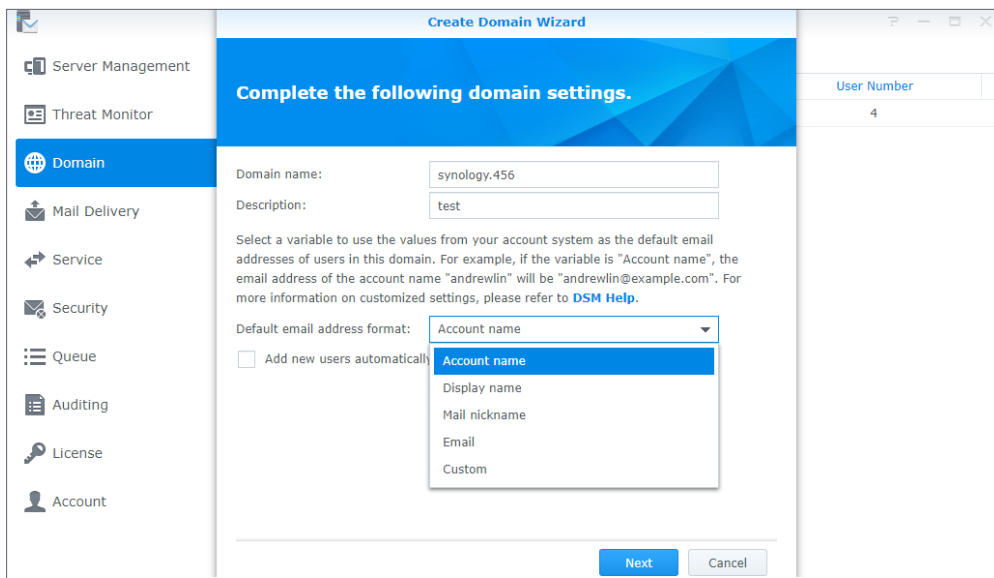
1. 前往網域，按一下新增按鈕。



2. 輸入網域名稱 *synology.456* 和描述。
3. 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。根據服務 > SMTP > 帳號類型的設定，您可以選擇帳號名稱、顯示名稱、郵件暱稱、電子郵件、自訂。

**注意：**

- 變更帳號名稱並不會改動既有的電子郵件地址。



以下表格列出 MailPlus Server 為不同使用者提供的預設設定：

| 帳號類型     | 預設設定                         |
|----------|------------------------------|
| 本地使用者    | 帳號名稱<br>郵件暱稱                 |
| LDAP 使用者 | 帳號名稱<br>郵件暱稱                 |
| 網域使用者    | 帳號暱稱<br>顯示名稱<br>郵件暱稱<br>電子郵件 |

4. 除了以上選項外，您也可以選擇自訂並在自訂變數欄位輸入變數，作為預設電子郵件位址格式。

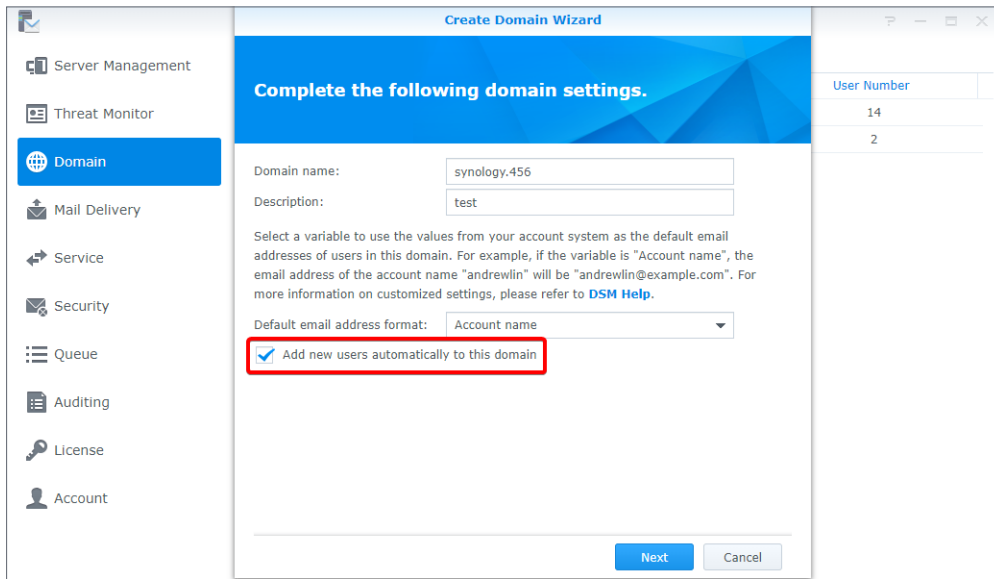
以下表格列出 MailPlus Server 支援的變數：

| 變數       | Value                                    |
|----------|------------------------------------------|
| <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。               |

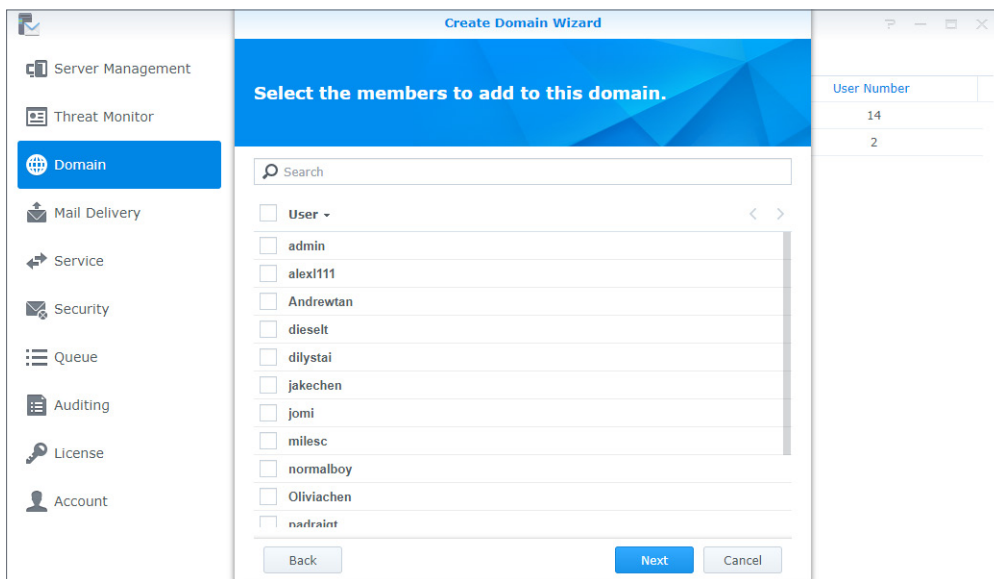
MailPlus Server 支援的變數會隨在服務 > SMTP 選擇的帳號系統而有所不同。請參考以下表格來了解更多資訊：

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

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，此後新增的使用者都會自動加入此網域。MailPlus Server 會根據預設電子郵件位址格式擷取資訊，作為使用者的電子郵件位址。



6. 設定完成後，請按下一步。
7. 將使用者加至此網域，再按下一步來確認在 *synology.456* 中的成員。



8. 按一下套用以儲存設定。

## 網域管理

MailPlus Server 為各個網域的管理員與使用者提供以下設定：

- **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、針對寄出的郵件啟用 DKIM 簽署、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地址的郵件。
- **使用者**：您可以將新成員加至網域，並為該網域的使用者設定角色，如**網域管理者**和**一般使用者**。
- **群組**：您可以將群組加至網域，群組中的使用者就會擁有同樣的角色設定。
- **別名**：您可以為一個或多個收件人建立一組別名，當有郵件寄至此別名時，伺服器會自動把郵件配送至別名內的所有使用者。別名也可以包含外部電子郵件位址。
- **自動密件副本**：您可以讓系統根據寄件人、收件人或所有訊息的條件，自動寄送一份密件副本至指定地址。
- **寄送限制與每日配額**：您可以限制使用者的寄出信件數量並設定流量控管。
- **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，以符合各種需求。依據您的設定，系統會在寄出的郵件內文末端自動加上免責聲明。

### 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、自動將新的使用者加入 *synology.456*。

The screenshot shows the MailPlus Server web interface. On the left is a navigation sidebar with icons for Server Management, Threat Monitor, Domain (highlighted), Mail Delivery, Service, Security, Queue, Auditing, License, and Account. The main content area is titled 'synology.456' and has several tabs: General, User, Group, Alias, Auto BCC, Usage Limit, and Disclaimer. The 'General' tab is active and contains the following fields and options:

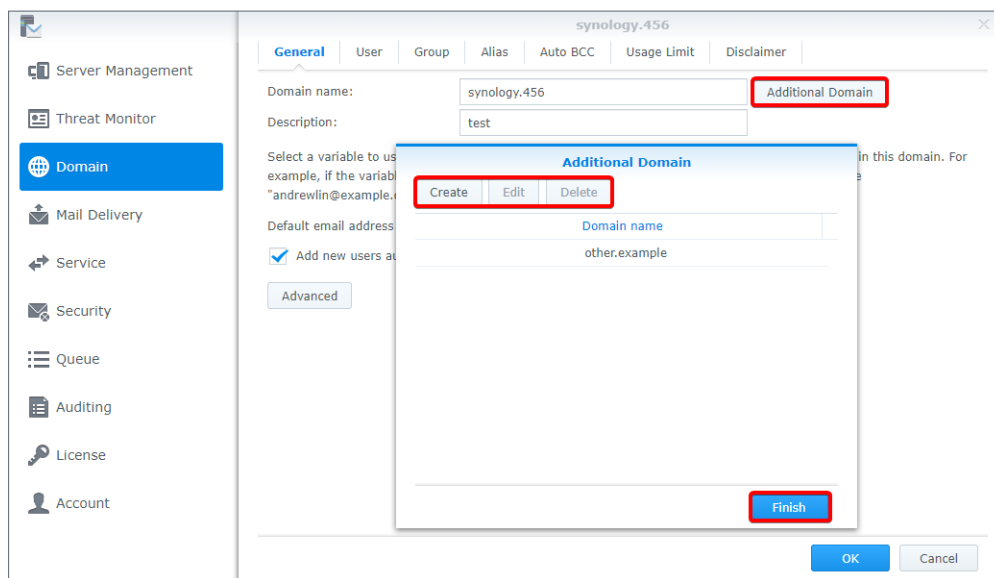
- Domain name:** A text input field containing 'synology.456' and an 'Additional Domain' button.
- Description:** A text input field containing 'test'.
- Default email address format:** A dropdown menu with 'Account name' selected. Below it is a checked checkbox labeled 'Add new users automatically to this domain' and an 'Advanced' button.

At the bottom right of the main content area are 'OK' and 'Cancel' buttons.

## 建立與編輯其他網域

在**其他網域**視窗中，您可以設定這台主機會額外收下哪些網域名稱的郵件。其他網域的設定會依照 *synology.456* 的設定。

1. 前往**網域** > *synology.456* > **一般**，按一下**其他網域**按鈕。
2. 按一下**新增**來加入其他網域。若您想要編輯或刪除網域，請選取您的目標網域後，再按對應的按鈕進行操作。
3. 在**其他網域**頁面中，您可以檢視已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，若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**以儲存設定。



### 注意：

- 您可能需要相應調整 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。

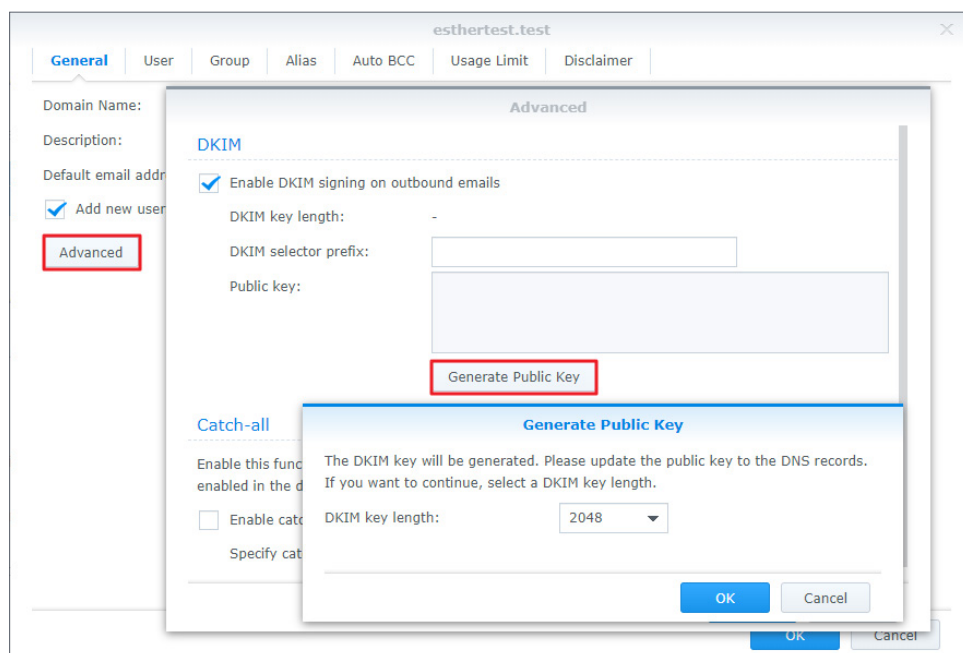


2. 在進階設定的彈出視窗中，您可以修改 *synology.456* 的 DKIM 與 Catch-all 設定。

- **DKIM**：您可以啟用 DKIM 簽署以免郵件在傳送途中被篡改，或是身分遭到冒用。
  - a. 若想讓對方信任您寄出的郵件並防止其他人冒用您的身分，請在 **DKIM** 區塊中勾選針對寄出的郵件啟用 DKIM 簽署，並調整 DKIM 簽章如下：
    - **DKIM 選取器前置字串**：DKIM 簽章的前置字串。您可依個人喜好自訂 DKIM 選取器前置字串。
    - **公開金鑰**：公開金鑰內容。若啟用 DKIM 簽署時未有公開金鑰與私密金鑰，系統會自動產生金鑰。
  - b. 按一下**產生公開金鑰**按鈕來獲得新一組公開金鑰與私密金鑰，系統產生的金鑰預設為 2048 位元(若您的 DKIM 金鑰遭到拒絕，請將金鑰長度變更為 1024 或 512 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。



- c. 按一下**確定**以儲存設定。此外，為確保收件端伺服器可以順利驗證 DKIM 簽章，您必須發佈 DNS TXT 記錄來讓 DKIM 簽署機制正常運作：

TXT 紀錄值的格式：**v=DKIM1; k=rsa; p=[DKIM 公開金鑰]**

舉例來說，若 MailPlus Server 的網域為 *example.com*，且您設定的 DKIM 選取器前置字串為 *abc*，系統產生的公開金鑰為 *MIGfMA0GCSqGS1b3DQE*，則 TXT 記錄如下：

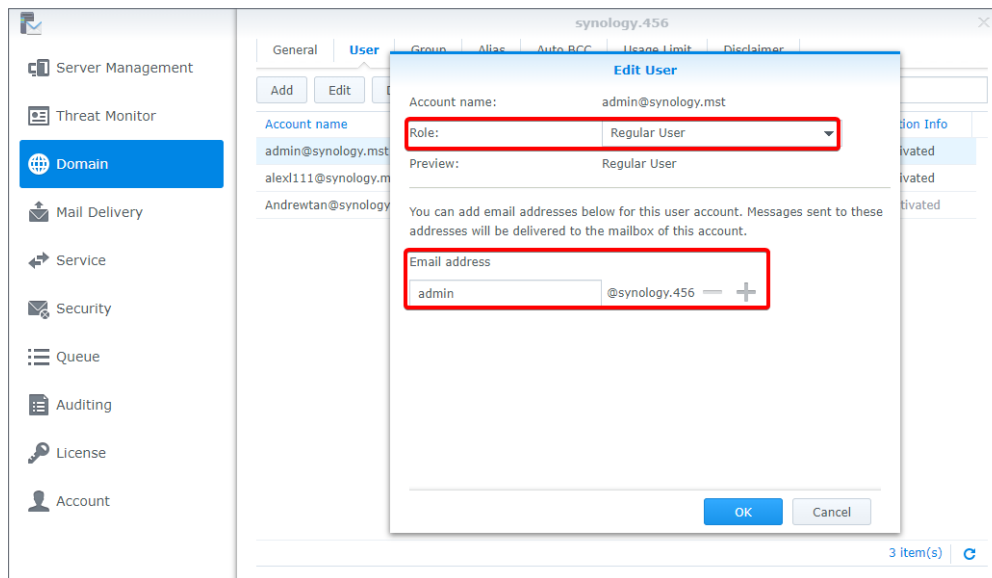
- **TXT 紀錄名稱**：*abc\_domainkey.example.com*
  - **TXT 紀錄值**：*v=DKIM1; k=rsa; p=MIGfMA0GCSqGS1b3DQE*
- **Catch-all**：啟用 **Catch-all** 來將一個使用者帳號設為 **Catch-all** 信箱，用以接收寄送至不存在或未於該網域啟用之電子郵件地址的信件。

## 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. 確認選取的使用者之郵件地址。

## 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. 在使用者頁籤選取一個帳號，按一下編輯。
3. 在編輯使用者視窗調整以下設定：
  - **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建立與刪除網域之外的所有設定。
    - **一般使用者**：一般使用者沒有網域的管理權限。
    - **依照群組設定**：權限依照該使用者所屬的群組設定。
  - **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地址的信件會被傳送至此帳號信箱。



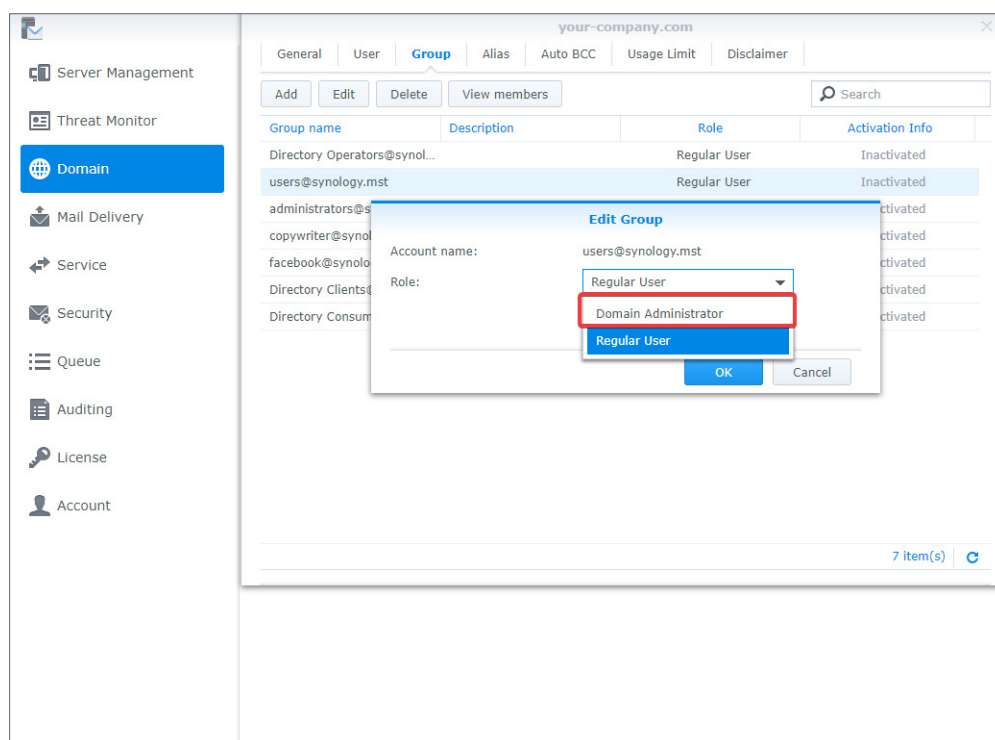
4. 若要移除使用者帳號，選取目標使用者並按一下刪除按鈕。

## 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，並按一下新增。
3. 選取使用者群組，再按下一步。
4. 確認成員的電子郵件地址。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，選取欲編輯的使用者群組並按一下編輯。
3. 在編輯群組視窗中，您可以在角色下拉式選單裡選擇網域管理者，所有在群組內的使用者便可擁有網域管理者權限。

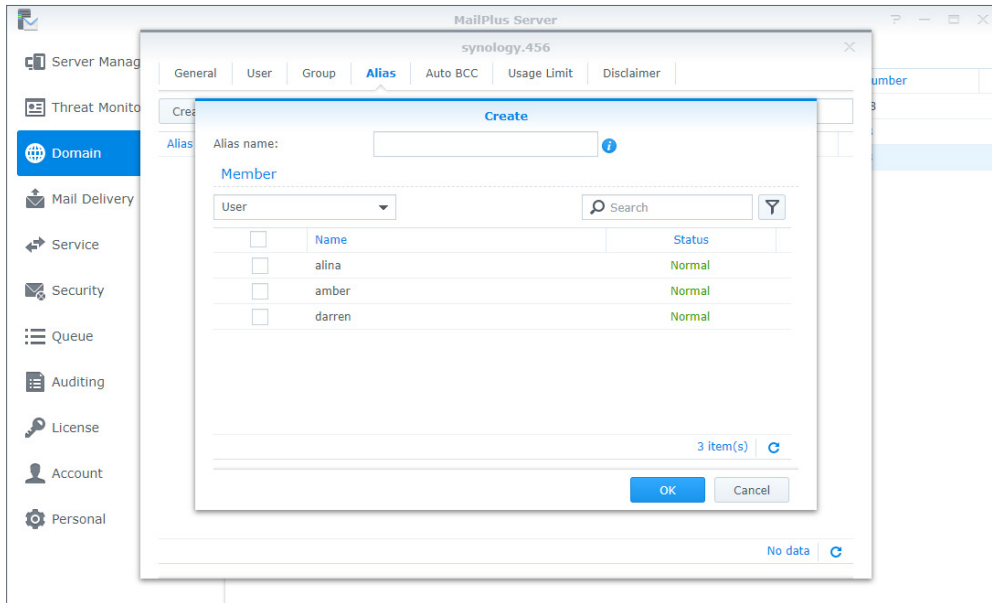


4. 您可以選取想要移除的使用者群組並按一下刪除按鈕。
5. 您可以按一下檢視成員按鈕，查看屬於此群組的使用者是否不在此網域中。

## 新增別名

您可以新增別名，讓使用者可以經由單一別名，來將郵件同時寄送給多位收件人。

1. 前往網域，選取 *synology.456* 並按一下編輯。
2. 前往別名並按一下新增按鈕。
3. 於別名名稱欄位輸入別名名稱。
4. 於下拉式選單中檢視別名、使用者帳號、使用者群組、外部信箱。



5. 勾選核取方塊來選擇別名應包含的使用者。
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、其他別名。
7. 按一下確定以儲存設定。

## 編輯與刪除別名

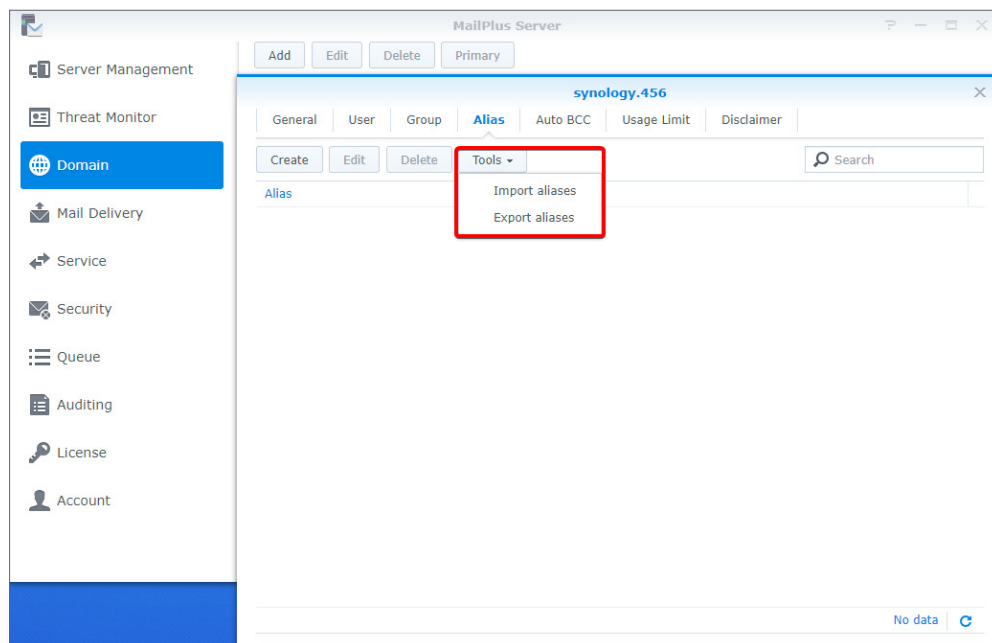
請參考以下步驟來編輯或刪除別名：

1. 前往網域，選取 *synology.456* 並按一下編輯。
2. 前往別名選擇欲修改的別名(您也可以透過右上角的搜尋欄位搜尋別名)。
3. 按一下編輯或刪除按鈕。

## 匯入 / 匯出別名

若您想匯入或匯出既有的別名清單或先前建立的別名清單，請參考以下步驟：

1. 前往網域，選取 *synology.456* 並按一下編輯。
2. 前往別名並按一下工具按鈕。
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，該筆別名既不會被匯入，也不會被更新。
  - 匯出別名：匯出並下載 Postfix 格式的別名檔案。

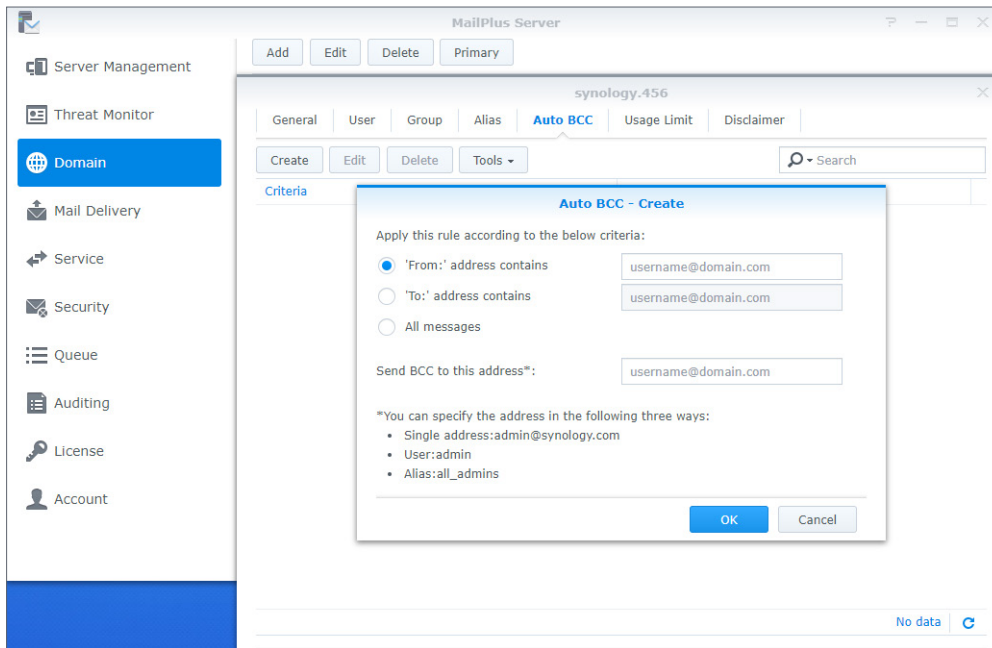


## 新增自動密件副本規則

自動密件副本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地址。請參考下列步驟來新增自動密件副本規則：

1. 前往網域，選取 *synology.456* 並按一下編輯。
2. 前往自動密件副本並按一下新增按鈕。
3. 指定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外，系統會自動為所有郵件寄送密件副本至指定地址。
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、別名。



6. 按一下確定以儲存設定。

## 編輯與刪除自動密件副本規則

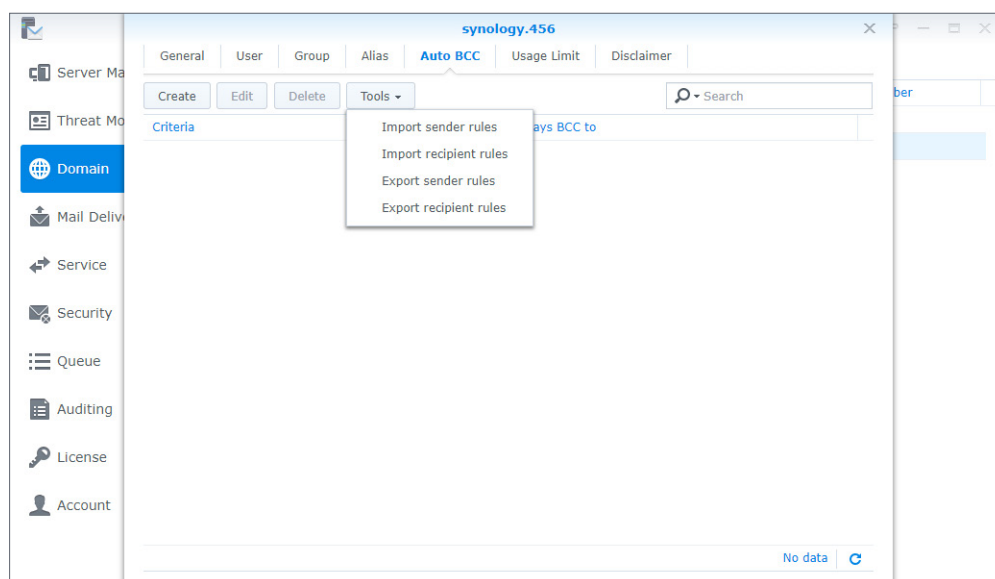
請參考下列步驟來編輯或刪除自動密件副本規則：

1. 前往網域，選取 *synology.456* 並按一下編輯。
2. 前往自動密件副本並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

請參考下列步驟來匯入或匯出自動密件副本規則：

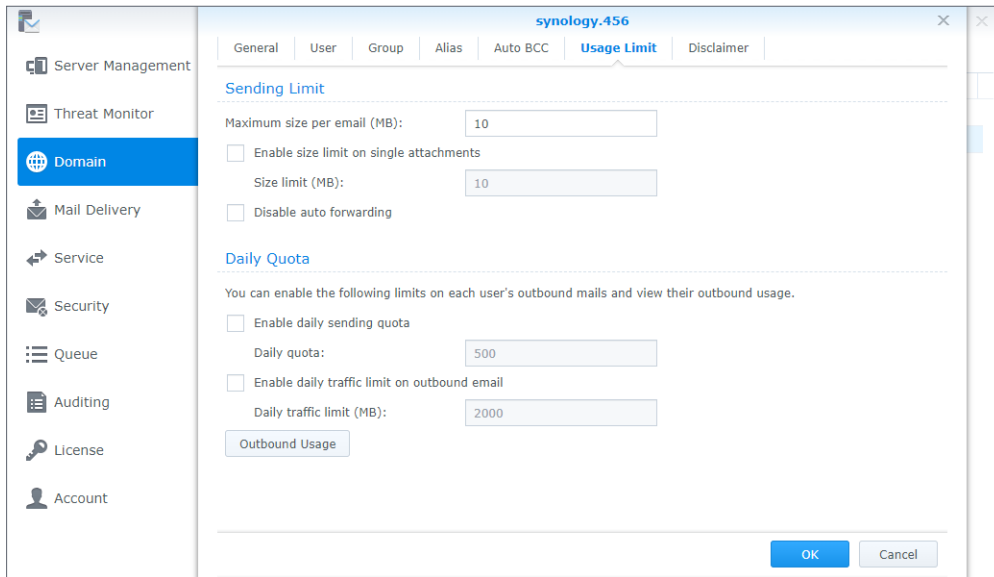
1. 前往網域，選取 *synology.456* 並按一下編輯。
2. 前往自動密件副本並按一下工具按鈕。
3. 選擇匯入或匯出寄件人或收件人規則。

**注意：**

- 此處沒有提供匯入 / 匯出所有訊息規則選項，因為這個功能已直接寫在 Postfix 的[主要設定文件](#)內，請參考 [Always Bcc](#)。
- 此外，請確認匯入的檔案為 Postfix 格式。

**設定寄送限制與每日配額**

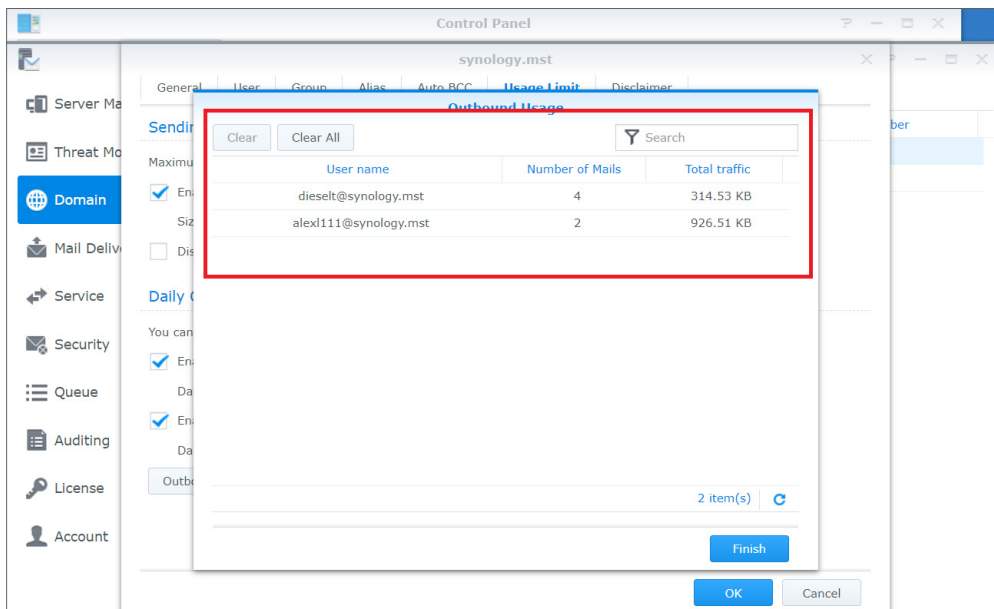
1. 前往網域，選取 *synology.456* 並按一下編輯。
2. 前往用量限制頁籤。
3. 在寄送限制區塊調整以下設定：
  - 單一郵件大小限制 (MB)：設定每位使用者寄出單一郵件訊息的大小上限。
  - 啟用單一附件大小限制：設定單一附件的大小限制，並在下方的大小上限 (MB) 欄位中輸入上限值。
  - 停用自動轉寄
4. 在每日配額區塊調整以下設定：
  - 啟用每日寄送限額：限制每位使用者每日可寄出的郵件數量。
  - 啟用每日可寄出的電子郵件流量上限：限制每位使用者每日可寄出訊息的總大小。
  - 寄送使用量：檢視個別使用者的寄送使用量。



## 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. 前往用量限制頁籤並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記錄，讓使用量重新計算。按一下全部清除按鈕來清除全部使用者的使用量記錄。



5. 按一下完成以結束設定。



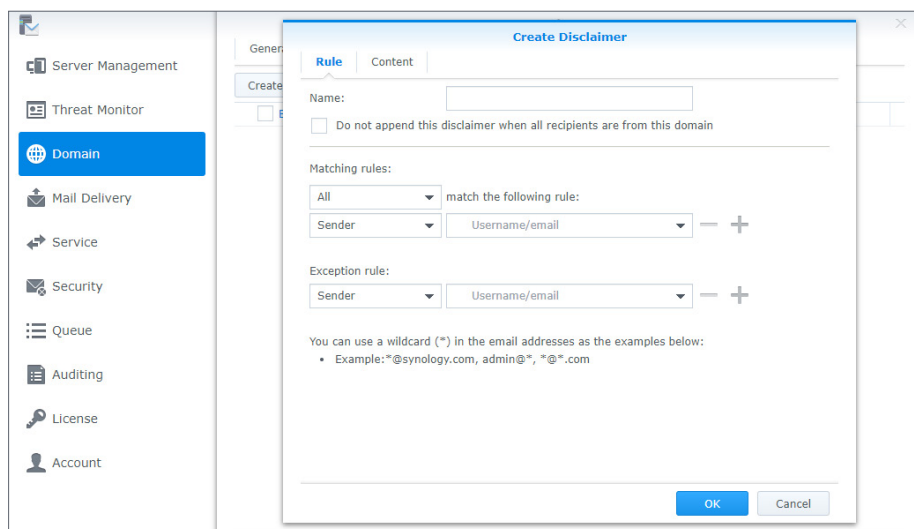
## 新增免責聲明

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文字內容。請參考下列步驟來新增免責聲明：

### 注意：

- 您可以設定多個免責聲明及規則，但是一封信只會套用一則免責聲明。

1. 前往網域，選取 *synology.456* 並按一下編輯。
2. 前往免責聲明頁籤並按一下新增按鈕。
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：

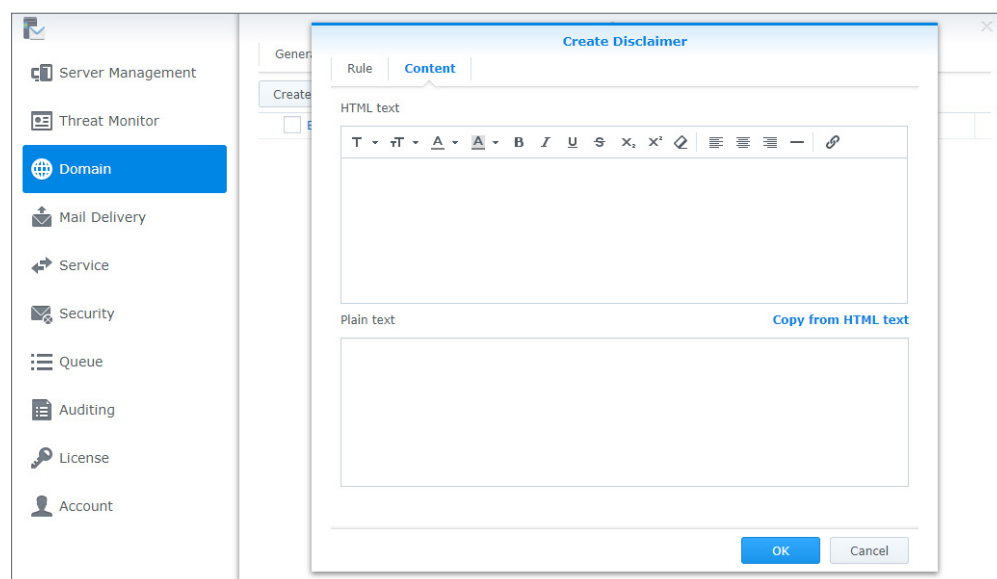
### 注意：

- 當伺服器判斷信件為內部信件（寄給其他內部使用者）時，就不會加上免責聲明。
- 若有任一收件人不是內部使用者，仍會加上免責聲明。

6. 透過以下選項設定條件：

- **比對規則：**選擇比對的標準：**全部**或**任一項**。若選取**全部**，則必須符合所有規則，才會加上免責聲明；若選取**任一項**，只要符合任一規則，就會加上免責聲明。
- **符合下列規則：**選擇寄件人或收件人作為附加免責聲明的依據。此處設定支援萬用符號 (\*)。
- **例外規則的優先順序高於比對規則。**若已為特定寄件人或收件人建立**例外規則**，即使符合**比對規則**也不會附加免責聲明。

7. 按一下加號圖示 (+) 來新增多個**比對規則**或**例外規則**；按一下減號圖示 (-) 來移除規則。
8. 規則設定完成後，前往內容頁籤來編輯 **HTML 文字**及**純文字**內容，確保文字內容在用戶端可以正確顯示。



9. 若您希望純文字與 HTML 文字內容相同，您可以按一下從 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，並移除所有 HTML 標籤。

10. 按一下確定來完成設定。

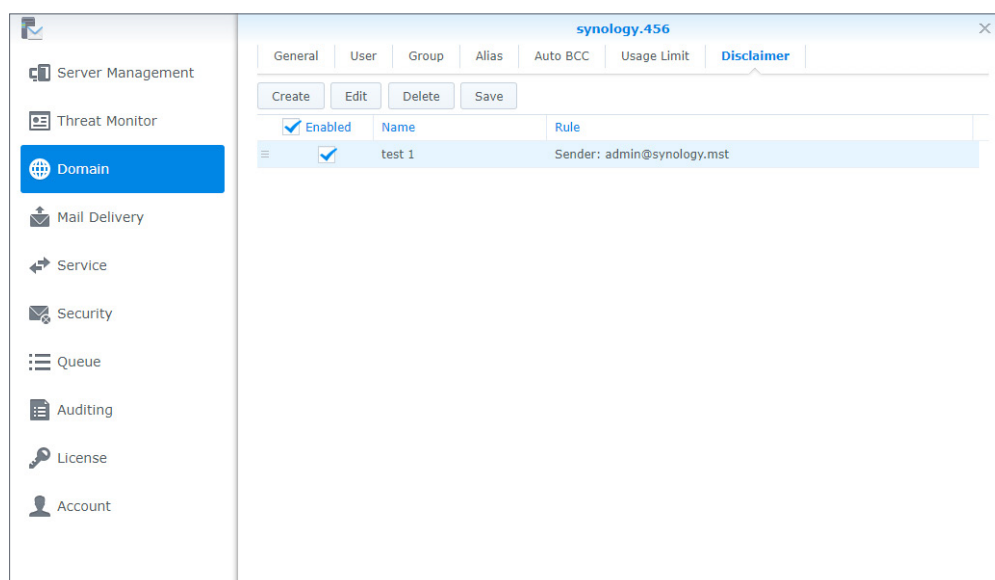
## 編輯與刪除免責聲明

因為系統會依照優先順序套用免責聲明，除了編輯與刪除免責聲明以外，您亦可調整其優先順序。請參考以下步驟來新增免責聲明：

### 注意：

- 系統會由上而下檢查各項聲明的套用條件，一旦符合條件，便會套用該免責聲明並結束條件檢查。

- 前往網域，選取 *synology.456* 並按一下編輯。
- 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順序。若要更改優先順序，選擇目標再拖拉至合適的位置。
- 選擇要啟用的免責聲明規則。
- 選擇您要修改的免責聲明規則，再按一下編輯或刪除按鈕。



- 按一下儲存來套用設定。

# 第 9 章：安全性設定

MailPlus Server 的安全性功能涵蓋以下四大類別：**防垃圾郵件**、**防毒掃描**、**身分認證**、**內容掃描**。您可以針對特定類別調整設定以加強保護。

## 防垃圾郵件

MailPlus Server 根據垃圾郵件的寄件特性，提供判定垃圾郵件的準則。下列為 MailPlus Server 提供的防垃圾郵件功能：

- **防垃圾郵件**：使用 Rspamd 及 SpamAssassin 作為防垃圾郵件引擎。此外，透過自動學習以及垃圾郵件回報機制，MailPlus Server 可以依您所需阻擋垃圾郵件。
- **Postscreen**：根據公開的黑名單及垃圾郵件伺服器的寄件人特性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**：根據垃圾郵件伺服器的寄件人特性所設計的反制功能。由於使用灰名單會影響郵件寄送速度，啟用此功能前請務必了解其運作機制。

## 啟用防垃圾郵件

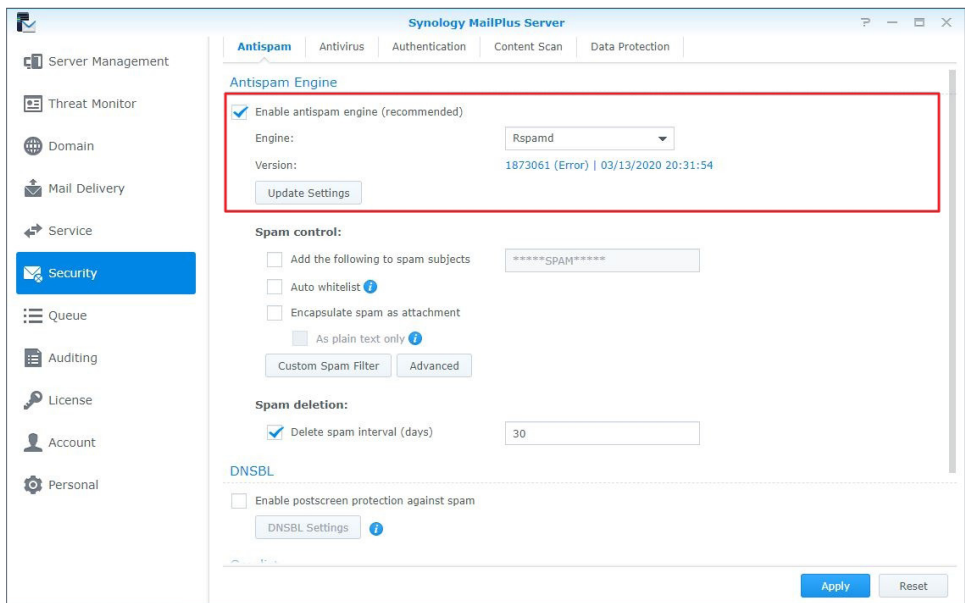
MailPlus Server 使用 Rspamd 作為防垃圾郵件引擎並套用 SpamAssassin 資料庫的規則，藉此依照垃圾郵件門檻分數過濾垃圾郵件。若有信件符合設定的偵測規則時，會加上該規則所對應的分數，當累加總分超過垃圾郵件門檻分數時，此信件就會被標記為垃圾郵件。請參考下列步驟來啟用防垃圾郵件：

1. 前往**安全性 > 防垃圾郵件**來調整以下設定：

- 勾選**啟用防垃圾郵件引擎**：若要了解更多關於垃圾郵件防護功能的資訊，請參閱[更新垃圾郵件防護規則](#)、[自訂垃圾郵件過濾](#)、[自動學習與垃圾郵件回報設定](#)。
- 勾選 **DNSBL (DNS-based Blackhole List)** 以阻擋透過網際網路網域名稱服務 (DNS) 散布的垃圾郵件。

### 注意：

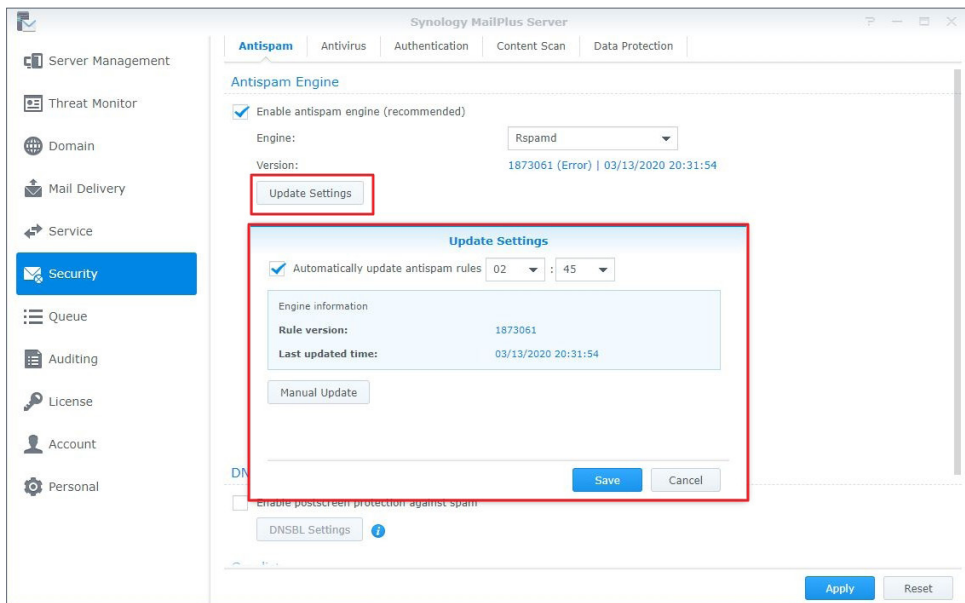
- 即使沒有啟用防垃圾郵件引擎，系統也會定期清理垃圾郵件。



### 更新垃圾郵件防護規則

您需要定期更新防垃圾郵件規則來確保垃圾郵件防護功能為最新版本。請參考下列步驟：

1. 前往安全性 > 防垃圾郵件，勾選更新設定按鈕以調整以下設定：
  - 自動更新垃圾郵件防護規則：勾選此選項以設定更新排程，系統會每日定時從 SpamAssassin 官網下載最新的垃圾郵件偵測規則。
  - 手動更新：按一下按鈕以立即更新垃圾郵件偵測規則。按鈕上方的引擎資訊欄位會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。

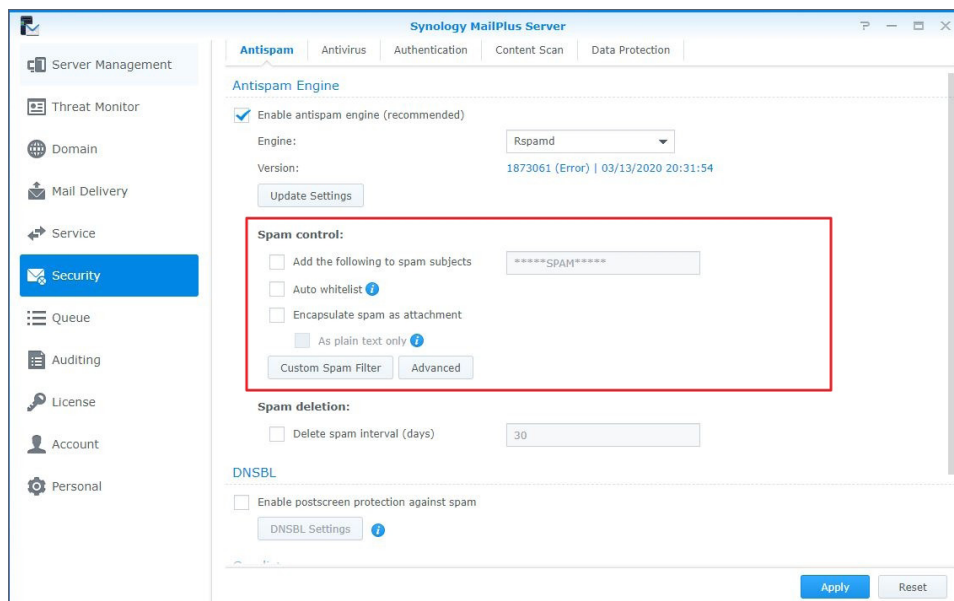


## 垃圾郵件管理設定

防垃圾郵件功能提供許多自訂設定選項，您可以依個人需求調整防垃圾郵件引擎。請參考以下步驟來編輯垃圾郵件管理設定：

1. 前往**安全性 > 防垃圾郵件**來調整以下設定：

- 在垃圾郵件主旨加入下列內容：當郵件分數超過門檻而被標記為垃圾郵件時，您可以在該主旨前加入特定內容，來警示使用者。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。
- **自動白名單**：來自 MailPlus 用戶曾回覆過的外部郵件地址之郵件的垃圾郵件分數將下降四分。
- **將垃圾郵件封裝為附件**：被判定為垃圾郵件之信件會被封裝為附件，再寄送給收件人。您可以勾選**純文字顯示**來避開網路臭蟲及惡意指令碼。



## 自訂垃圾郵件過濾

您可以設定以下兩種垃圾郵件過濾來避開可疑郵件：**地址過濾**與**附件過濾**。您可依個人需求自訂過濾器。請參考下列步驟來新增垃圾郵件過濾器：

1. 前往**安全性 > 垃圾郵件**，按一下**自訂垃圾郵件過濾**按鈕。
2. 前往**自訂垃圾郵件過濾**視窗中的**地址過濾**頁籤，按一下**新增**按鈕。

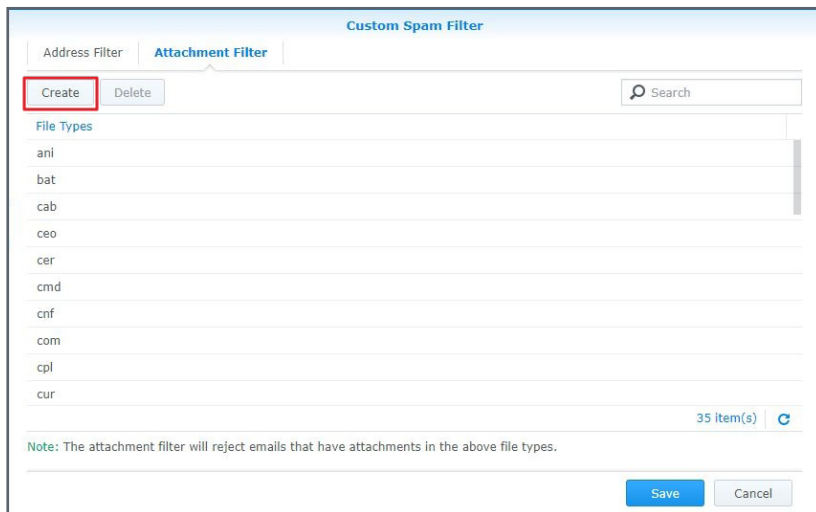
3. 針對寄件人及收件人地址設定條件，當條件符合時，信件會被標記為垃圾郵件或是非垃圾郵件。輸入地址支援萬用符號 (\*)。
4. 從**執行**下拉式選單中選擇標記為垃圾郵件或標記為非垃圾郵件。

### 注意：

- 系統會略過垃圾郵件分數而直接執行此處設定的動作。

5. 按一下**確定**來完成設定。

6. 前往附件過濾頁籤並按一下新增按鈕。
7. 輸入檔案類型以過濾附件檔案。
8. 按一下儲存以完成設定。



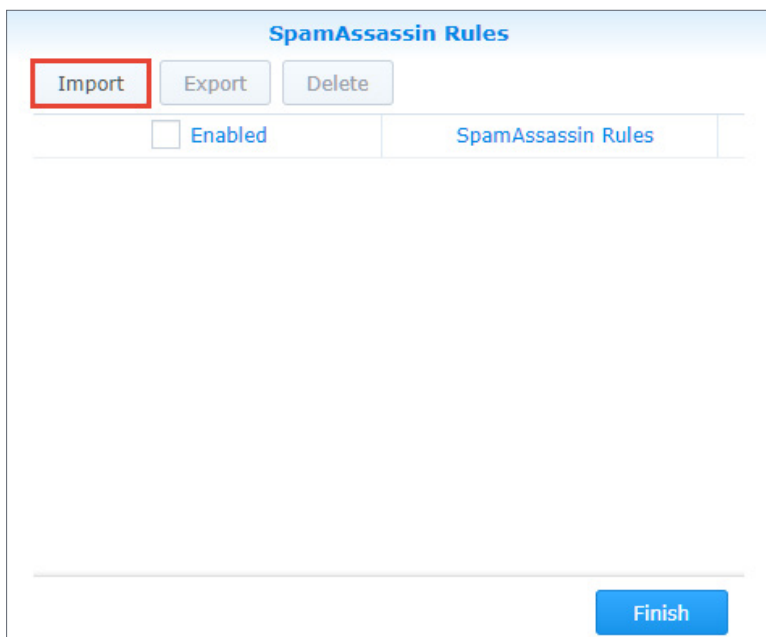
## 進階垃圾郵件防護規則

### SpamAssassin 規則

1. 前往安全性 > 防垃圾郵件，按一下進階設定按鈕。
2. 前往進階設定視窗中的一般頁籤，按一下 SpamAssassin 規則按鈕。
3. 按一下匯入按鈕以新增 SpamAssassin 規則。

**注意：**

- 匯入的檔案副檔名必須為「.cf」。規則匯入後便會直接啟用。您可以參考 SpamAssassin 提供的規則，或是根據規則規範來新增規則。





4. 選取您要編輯的規則，進行啟用、匯出、刪除等操作。
5. 按一下完成以結束設定。

## 關鍵字過濾

1. 前往安全性 > 防垃圾郵件，按一下進階設定按鈕。
2. 前往進階設定視窗中的一般頁籤，按一下關鍵字過濾按鈕。
3. 按一下群組設定按鈕來新增群組。您可以設定多個群組來分類關鍵字過濾器並依群組個別管理：
  - 勾選啟用下方的核取方塊來啟用或停用整個群組。
  - 若要新增、編輯、刪除群組，請選擇群組並按一下上方工具列中的按鈕。
4. 新增過濾器前，必須先從下拉式選單中選取過濾器所屬的群組。

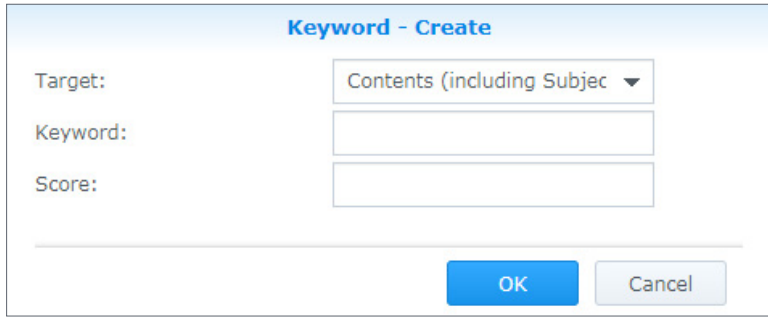
5. 按一下新增按鈕來自訂規則：
  - 目標：您可以從目標下拉式選單中選擇要過濾的選項：

| 選項       | 說明       |
|----------|----------|
| 標題       | 信件標題     |
| 內容 (含主旨) | 信件的内文和標題 |

- 關鍵字：輸入要過濾的關鍵字，可使用正規表達式。請參考[維基百科](#)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。



**注意：**

- 修改設定後，您也許需要重新調整垃圾郵件門檻分數。請回到編輯垃圾郵件防護設定視窗中的一般頁籤，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。

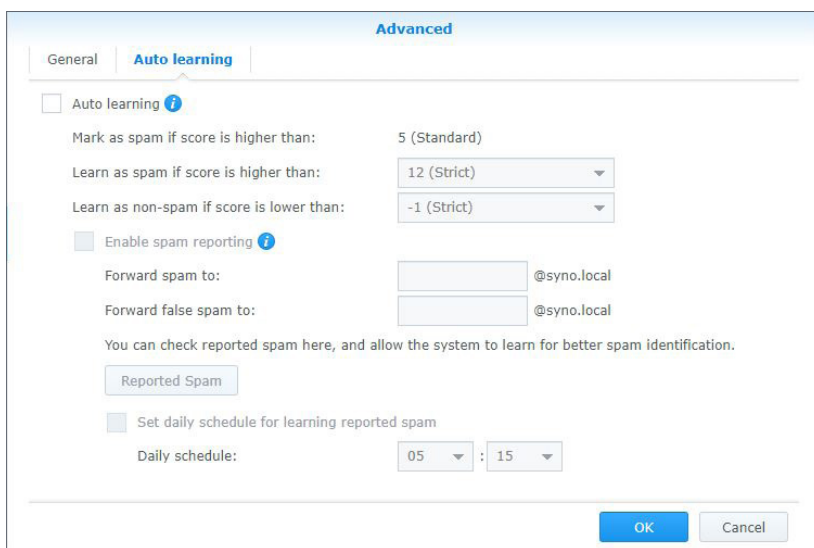
### 自動學習與垃圾郵件回報設定

防垃圾郵件引擎開始執行後，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能協助提升垃圾郵件偵測的準確性，並使其符合個人需求。

- **自動學習：**在防垃圾郵件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：**防垃圾郵件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，將沒有正確分類的信件回報給防垃圾郵件引擎引擎，讓其重新學習。

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 > 防垃圾郵件，按一下進階設定按鈕。
2. 前往進階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：偵測垃圾郵件時，若偵測到的分數高於此設定值，則防垃圾郵件引擎會進一步分析郵件中的關鍵字，擴充防垃圾郵件引擎的資料庫並增進學習能力，日後若有郵件出現相同關鍵字則較容易被判定為垃圾郵件。
- 若分數低於此數字則記為非垃圾郵件：偵測垃圾郵件時，若偵測到的分數低於此設定值，則防垃圾郵件引擎會進一步分析郵件中的關鍵字，擴充防垃圾郵件引擎的資料庫並增進學習能力，日後若有郵件出現相同關鍵字則較不會被誤判為垃圾郵件。

**注意：**

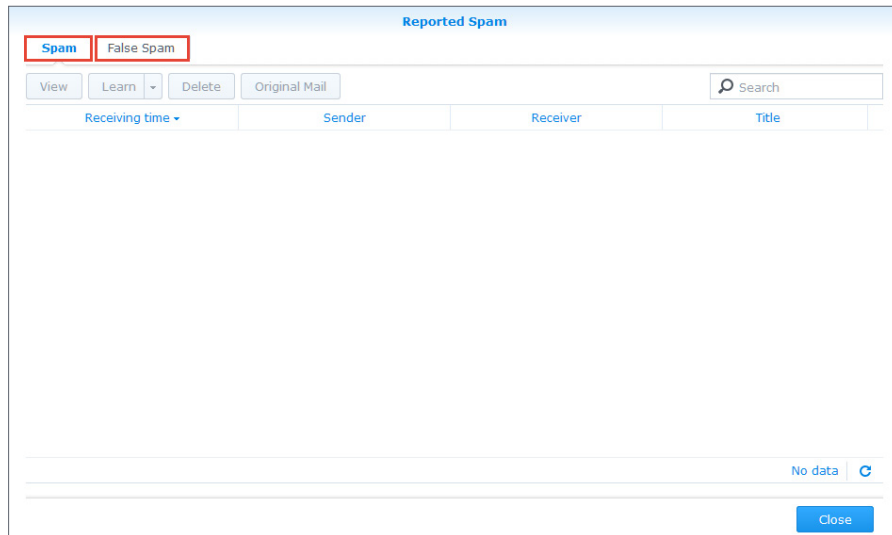
- MailPlus Server 需要至少各 200 封垃圾郵件及非垃圾郵件回報，才會將自動學習成果應用於垃圾郵件偵測。

## 4. 勾選啟用垃圾郵件回報核取方塊來調整以下設定：

**注意：**

- 回報流程中會蒐集垃圾郵件至特定信箱以進行學習。在垃圾郵件回報機制啟用後，使用者可以透過以下兩種方式來回報垃圾郵件及非垃圾郵件：
  - 若使用者使用 MailPlus 來收信，系統已為其設定轉寄信箱。使用者只需於 MailPlus 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。
  - 若使用者透過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，來將原信件以附件形式轉寄至下方設定的回報信箱。
- **轉寄垃圾郵件至**：設定一個郵件地址，當使用者透過第三方郵件用戶端收信並需要回報垃圾郵件時，原始信件便會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，當使用者透過第三方郵件用戶端收信，並發現有信件被誤判為垃圾郵件時，原始信件便會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。在信件清單中選擇信件並按一下**學習**按鈕，即可改善防垃圾郵件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。您可以讓系統針對垃圾郵件及誤報垃圾郵件內的信件進行回報學習。請參考下列垃圾郵件的處理方式：

| 功能    | 說明                                                       |
|-------|----------------------------------------------------------|
| 檢視    | 檢視訊息內容。                                                  |
| 學習    | 讓防垃圾郵件引擎快速學習所選信件，被學習的信件會從信件清單上消失。                        |
| 全部學習  | 讓防垃圾郵件引擎學習所有信件，您可以在 <b>學習</b> 按鈕旁的下拉式選單中找到 <b>全部學習</b> 。 |
| 刪除    | 刪除所選信件，此信件將不會被防垃圾郵件引擎學習。                                 |
| 信件原始檔 | 開啟新的瀏覽器分頁檢視信件原始檔內容。                                      |
| 搜尋    | 在右上角的搜尋欄位中輸入關鍵字（寄件人、收件人、標題）以搜尋符合條件的信件。                   |



- 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：**

- 轉寄垃圾郵件至欄位中輸入的郵件地址不能和現有的使用者重複。該郵件地址不會占用授權數量，僅為系統內部收取郵件樣本之用。
- 轉寄誤報垃圾郵件至欄位的郵件地址不能和現有的使用者重複。

5. 按一下**確定**來完成設定。

## DNSBL 設定

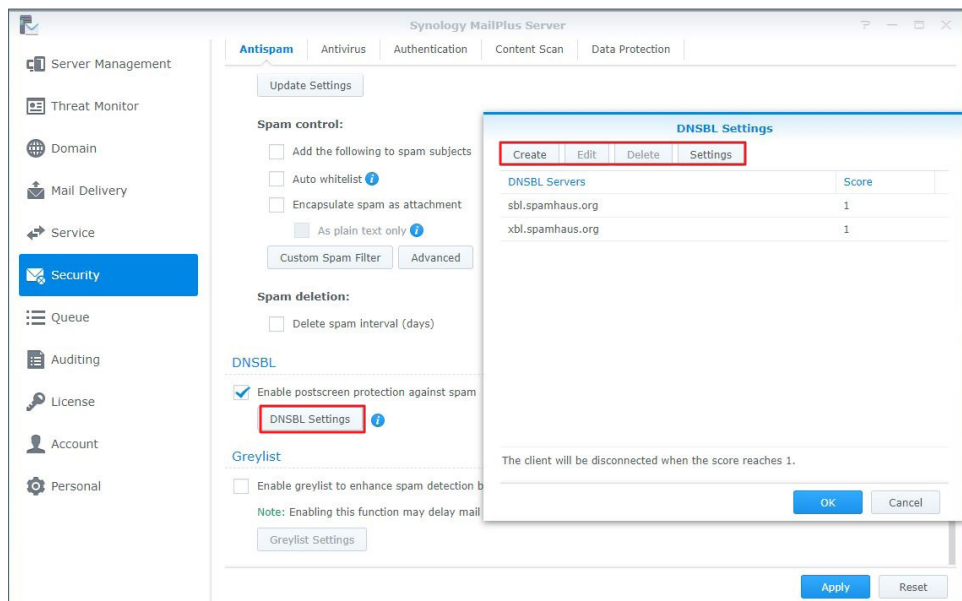
Postscreen 允許設定多台 DNSBL 伺服器，查詢伺服器時若發現該郵件符合條件即會產生垃圾郵件分數，各個伺服器的分數會加總計算，當累積分數超過指定的 **DNSBL 分數門檻**時，便拒絕服務。請參考以下步驟來調整 DNSBL 設定：

1. 前往**安全性 > 防垃圾郵件**，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** 按鈕來指定拒絕服務的 **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填入負分即可。

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。

## 啟用灰名單

灰名單機制是指收到新進信件時，系統會查看以前是否曾經有相同的 IP 位址、寄件人、收件人記錄。若查無記錄，此信件將被視為可疑信件，系統會先回傳錯誤訊息給寄件人，請他稍後再寄。依照 SMTP 規範，寄件人收到錯誤訊息後，會稍待一段時間再嘗試寄信，但是垃圾郵件的寄件人通常會直接放棄寄送。當一般寄件人隔一段時間再寄信時，系統就會收下信件。灰名單機制透過此方式阻擋垃圾郵件。

啟用灰名單後，灰名單會針對所有來源執行以下預設動作：

- **白名單**：直接通過檢查，不會回傳暫時錯誤訊息。
- **灰名單**：回傳錯誤訊息給沒有信件往來記錄的寄件人。
- **黑名單**：直接拒絕收信。

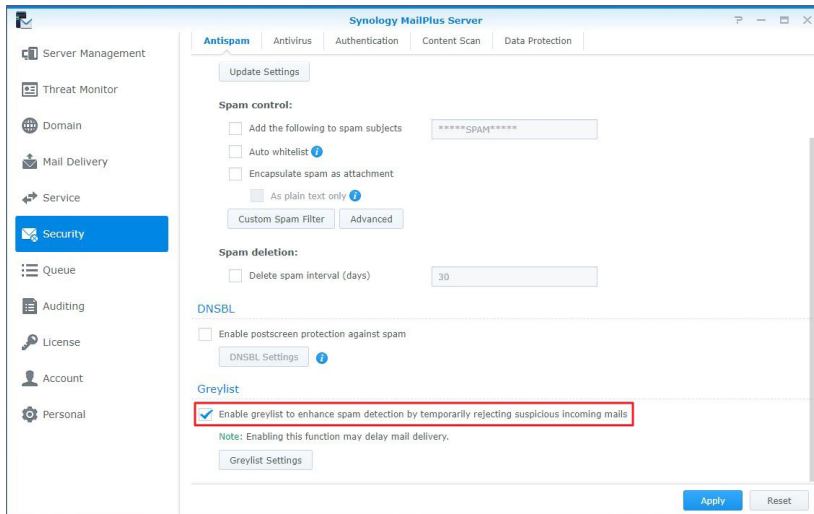
### 注意：

- 灰名單機制可能會造成一般信件較晚送達。啟用此功能前，請確定您已完全了解灰名單可能帶來的影響。

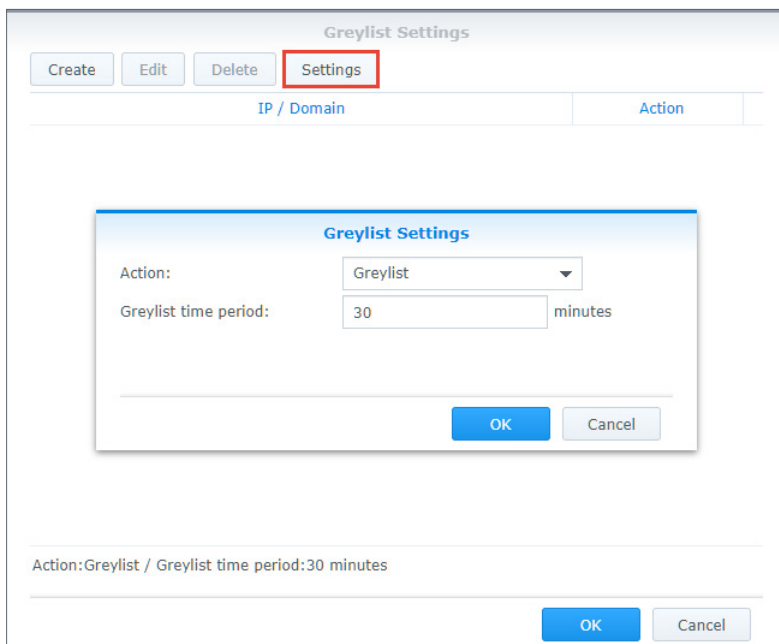
## 第 9 章：安全性設定

請參考下列步驟來啟用灰名單。

1. 前往**安全性 > 垃圾郵件**，勾選**啟用灰名單**，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**按鈕來設定對所有來源信件的預設動作，或是針對特定 IP 位址或網域的個別動作。
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，並在**灰名單時間**欄位中輸入郵件延遲時間。此處設定將套用到所有執行的灰名單動作上。

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來源，再從**動作**下拉式選單中指定動作。

**注意：**

- 此處的網域來源是透過 DNS 查詢其 IP 位址的網域名稱，而非來自信件的 **MAIL FROM** 資訊。

7. 按一下**確定**來完成設定。

## 防毒掃描

MailPlus Server 提供免費的 ClamAV 以及付費訂閱制的 McAfee 兩種防毒引擎來防範病毒威脅，您可以指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。

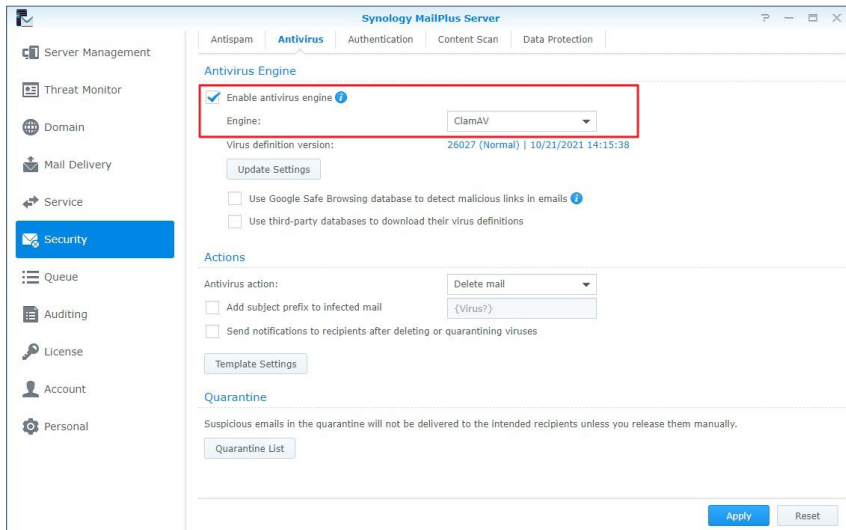
- **ClamAV**：ClamAV 是 MailPlus Server 預設的防毒系統，提供您的伺服器免費的完整防護。
- **McAfee**：MailPlus Server 與付費防毒套件 **Antivirus by McAfee** 整合，訂閱 **Antivirus by McAfee** 後，您可以選擇 **McAfee** 作為防毒引擎，輕鬆管理防毒排程及日誌，並使用更多進階的設定。請注意，MailPlus Server 會略過大於 20 MB 的郵件，以縮短掃描時間。

**注意：**

- 建議使用搭載 2 GB 或更多記憶體之 Synology NAS 機種，以確保安全引擎順利運作。

## 啟用防毒引擎：

1. 前往安全性 > 防毒，勾選啟用防毒引擎核取方塊。



2. 從引擎下拉式選單中選擇以下任一選項：

- **ClamAV**：ClamAV 是 MailPlus Server 支援的免費防毒引擎。
- **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**安裝 **Antivirus by McAfee**)。

3. 請參考以下章節來完成設定。

## ClamAV

若您選擇 ClamAV 作為防毒引擎，請參考以下步驟來進行設定：

1. 按一下**更新設定**以檢視防毒引擎資訊。請定期更新防毒引擎。

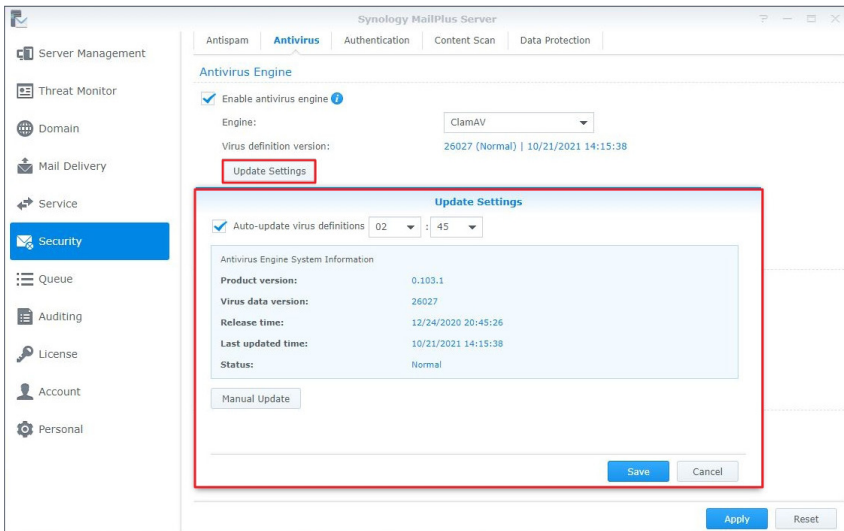
2. 您可以選擇自動或手動更新病毒定義檔：

- **自動更新病毒定義檔**：勾選核取方塊，系統將每日定時下載最新的病毒定義檔。
- **手動更新**：按一下按鈕以立即更新病毒定義檔。

3. ClamAV 使用以下外部資料庫來加強偵測精準度：

- **使用 Google Safe Browsing 資料庫來偵測郵件中的惡意連結**：使用整合的 Google 安全瀏覽 (Safe Browsing) 資料庫，來偵測信件中是否帶有惡意連結。
- **使用第三方資料庫來下載其病毒定義碼**：使用 Sanesecurity 等**第三方資料庫**，來增強病毒偵測能力。



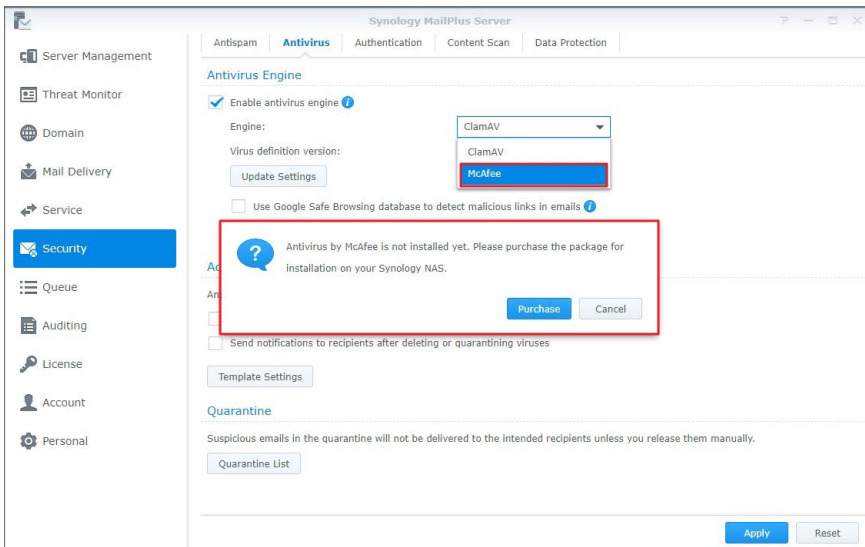


4. 按一下套用以儲存設定。

## McAfee

若選擇 McAfee 作為防毒引擎，您須前往套件中心購買 McAfee。

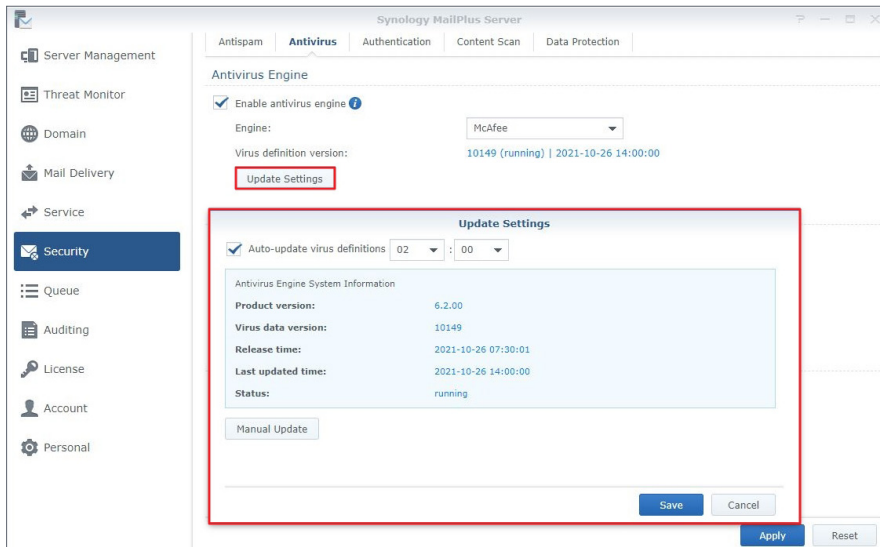
1. 若您未安裝 McAfee 或是授權已過期，會出現警示視窗。您需要至套件中心安裝 Antivirus by McAfee，並以 [Synology 帳戶](#) 購買授權。



2. 按一下更新設定以檢視 McAfee 的資訊。

### 注意：

- 您必須在 Antivirus by McAfee 套件中設定 McAfee。
- 若狀態顯示為異常（可能有授權問題或病毒碼檔案損毀等），Antivirus by McAfee 便不會掃描信件，請務必解決問題或是切換為 ClamAV。若使用者手動停用 Antivirus by McAfee，MailPlus Server 將會自動切換成 ClamAV。



3. 按一下套用以儲存設定。

## 病毒處理行動設定

1. 前往安全性 > 防毒。

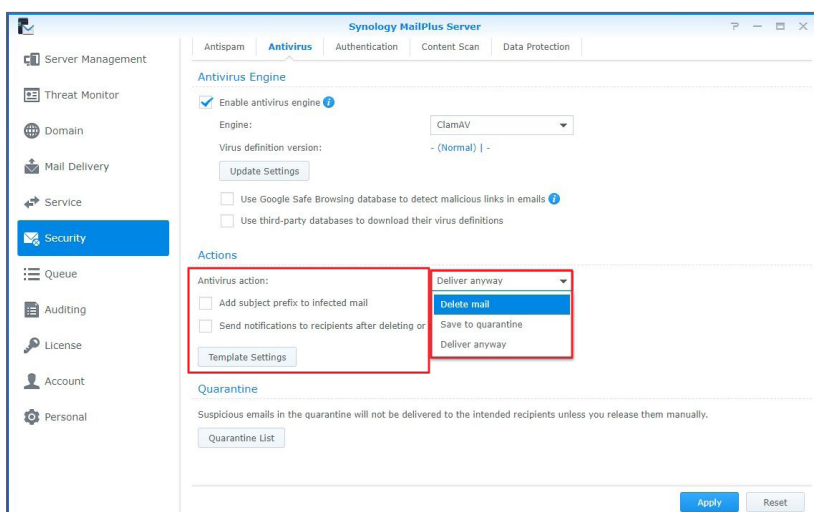
2. 在病毒處理行動下拉式選單中，選擇防毒引擎對於帶有病毒的信件應採取的行動：

- 刪除信件：直接刪除信件。
- 儲存至隔離區：攔截信件並儲存至隔離區。
- 照常傳送：寄出信件。

3. 為受感染的訊息勾選為感染郵件加上標題前置文字，再指定會出現在主旨中的文字。

4. 勾選刪除或隔離病毒後，寄送通知訊息給收件人核取方塊以通知此狀況。原始信件的收件人會收到一封通知訊息。您可以按下方的範本設定按鈕來為移除訊息及隔離訊息編輯通知信件的範本。

5. 若選擇照常傳送，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。

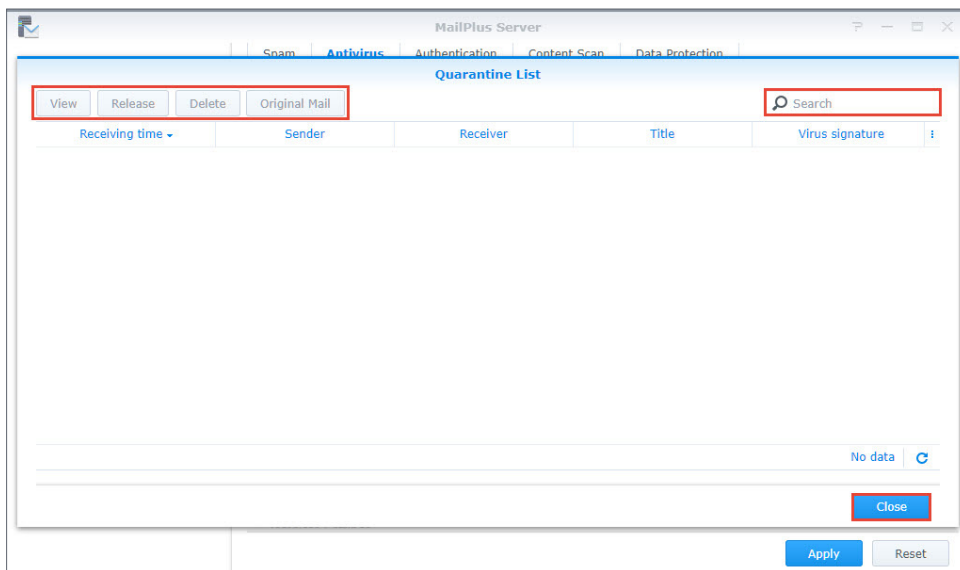


6. 按一下套用以儲存設定。

## 隔離清單

若您有信件存於隔離區，您可以檢視並管理被隔離的信件。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、病毒碼。
3. 選取一封隔離信件，按一下**檢視**或**信件原始檔**按鈕來確認內容。
4. 根據信件內容選擇下列動作：
  - **放行**：寄送信件給收件人。
  - **刪除**：直接刪除信件。



5. 按一下**關閉**來完成設定。

## 身分認證

認證目的為確認寄件人身份，避免收到假冒身份的信件，亦能避免您的身分遭到冒用。

- **SPF (Sender Policy Framework)**：SPF 機制檢查寄信端主機的合法性。有許多網域會透過 DNS 發佈 SPF 記錄，用以提供可以寄送此網域信件的主機位置，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，判斷該主機是否被允許寄送該網域的信件。當 SPF 驗證失敗時，該主機會根據 SPF 記錄被分類為 **fail** 或 **softfail**，系統會對兩種結果作不同處理。
- **DKIM (DomainKeys Identified Mail)**：DKIM 機制透過加密方式來驗證寄件人身份是否被冒用，以及信件內容是否有被竊改。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 DNS 記錄發佈出去，寄信時則使用私密金鑰為該信件加上數位簽章。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，接著用公開金鑰來驗證簽章，以確認寄件人身份以及信件是否有被竊改。
- **DMARC (Domain-based Message Authentication, Reporting & Conformance)**：DMARC 機制的執行基於 SPF 與 DKIM 驗證機制。系統收到信件時，會檢查該寄件人是否通過 SPF 跟 DKIM 驗證，藉此判斷是否有假冒寄件人的情況發生。

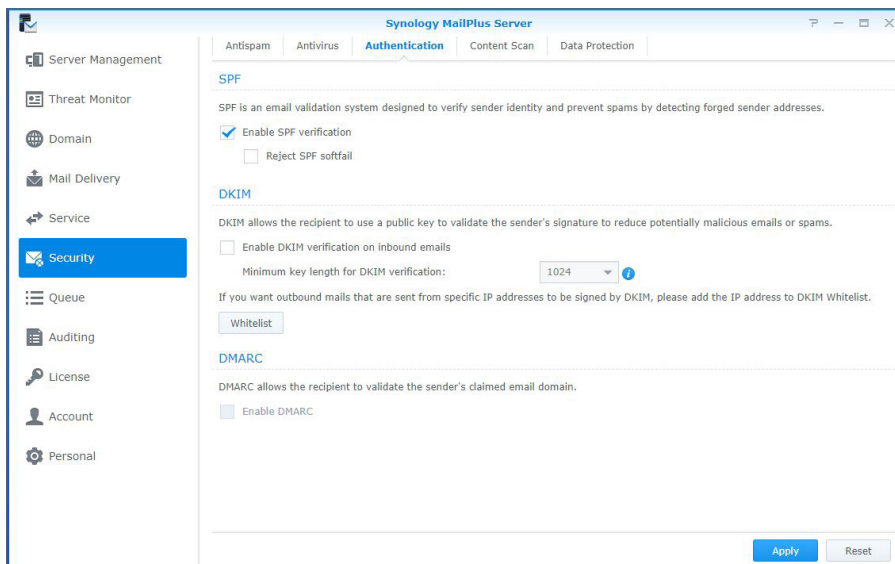
## SPF

啟用 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。SPF 驗證失敗時會顯示以下兩種結果之一：**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 區塊中勾選啟用 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**，您可以勾選拒絕 SPF **softfail** 核取方塊來拒絕驗證結果為 **softfail** 的信件，否則驗證結果為 **softfail** 的信件將會被接收。



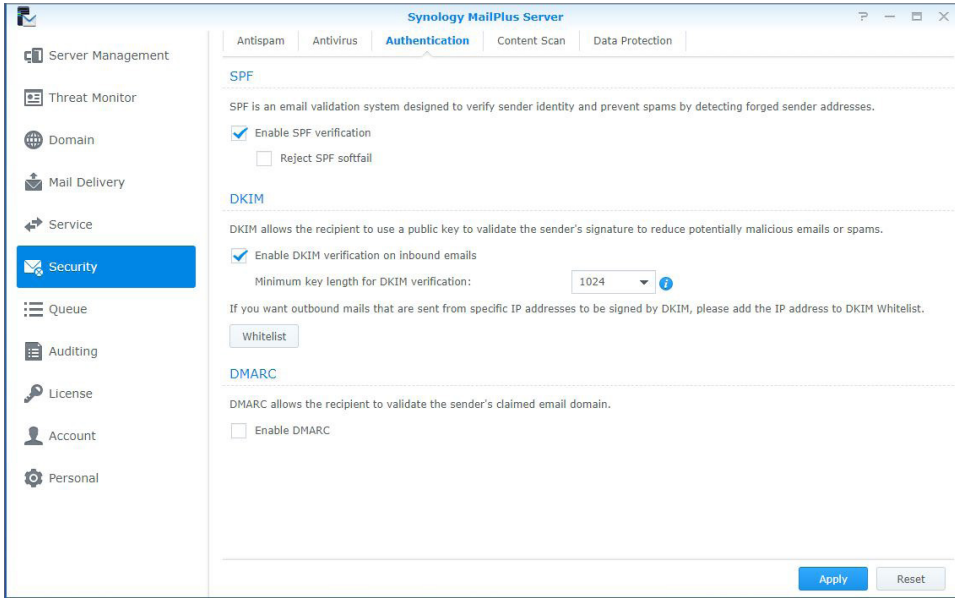
3. 按一下套用以儲存設定。

## DKIM

您可以啟用 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 區塊中勾選針對接收的郵件啟用 DKIM 驗證核取方塊。
3. 在通過 DKIM 驗證的金鑰長度需大於此字數選擇一個數值。若 DKIM 簽署的金鑰長度小於此處設定的數值，便會拒絕該信件，因此增加金鑰長度的最小值能預防來自安全性較低網域的信件通過 DKIM 驗證。

4. 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信件加上 DKIM 簽章。當範圍內的主機連線至 MailPlus Server 來對外寄信時，系統會為其加上 DKIM 簽章。



5. 按一下**套用**以儲存設定。

**注意：**

- 在 MailPlus 2.1 或以上版本，被 DKIM 拒絕的信件會移到**垃圾郵件**信箱，在 MailPlus 用戶端開啟此類信件時，會出現警告提醒使用者。

## DMARC

由於 DMARC 基於 SPF 和 DKIM 驗證，進行設定前，您必須為網域設定 SPF，並產生公開金鑰來啟用寄出信件的 DKIM 簽署。請參考下列步驟來啟用 DMARC 驗證：

1. 前往**安全性 > 認證**。
2. 勾選**啟用 DMARC** 核取方塊以啟用 DMARC。

**注意：**

- 在 MailPlus 2.1 或以上版本，被 DMARC 隔離的信件會移到**垃圾郵件**信箱，在 MailPlus 用戶端開啟此類信件時，會出現警告提醒使用者。

## 資料保護

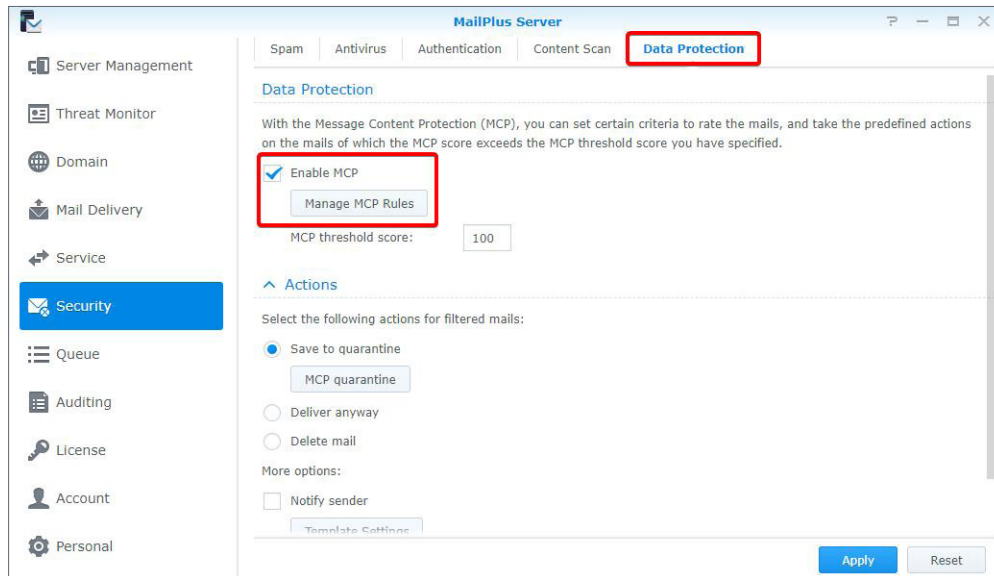
內容保護功能會根據您的設定過濾可疑信件。

- **MCP 規則**：根據信件原始內容進行搜尋，若發現過多可疑內容，則會將信件放入隔離區，或執行其他指定動作。
- **內容掃描**：加強掃描信件內容，拒絕或改寫含有釣魚連結或 HTML 標籤的郵件，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。當一封信件符合規則，該規則分數會計入 MCP 總分，若總分超過 MCP 門檻分數，則系統會過濾或阻擋該封信件。請參考下列步驟來啟用及管理 MCP：

1. 前往**安全性 > 資料保護**，在**資料保護**區塊中勾選**啟用 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：
  - **Name**：輸入規則名稱。
  - **目標**：從目標下拉式選單中指定信件的特定區塊作為比對目標：

| 區塊        | 說明        |
|-----------|-----------|
| 標題        | 信件標題      |
| 內容 (含主旨)  | 信件的内文和主旨  |
| 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 |

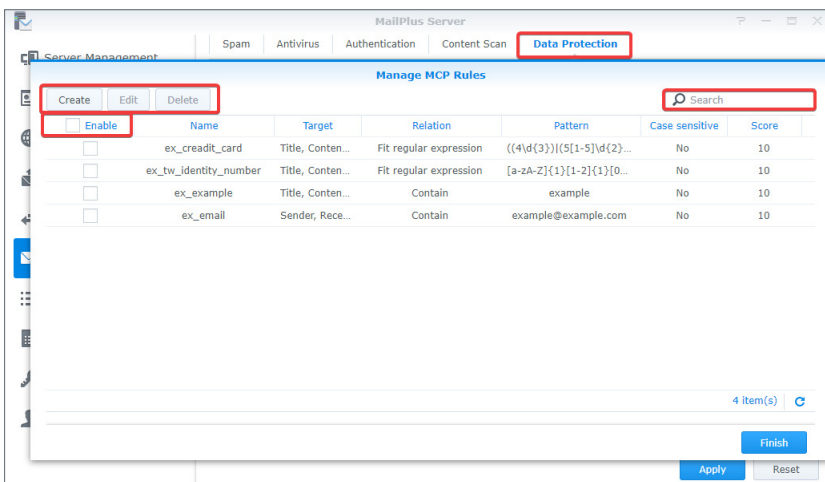
- **自訂 header**：當您在目標下拉式選單中選擇自訂 header，會出現自訂 header 欄位，請在此輸入特殊標頭。
- **關係**：從關係下拉式選單選擇比對的條件：

| 條件      | 說明                                  |
|---------|-------------------------------------|
| 包含      | 若信件的目標區塊包含比對內容，則符合規則。               |
| 等於      | 若信件的目標區塊與比對內容相同，則符合規則。              |
| 符合正規表達式 | 若信件的目標區塊包含比對內容，則符合規則。比對內容可以使用正規表達式。 |

- **樣式**：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**：設定符合規則時產生的分數。

6. 按一下**確定**來完成新增規則。

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



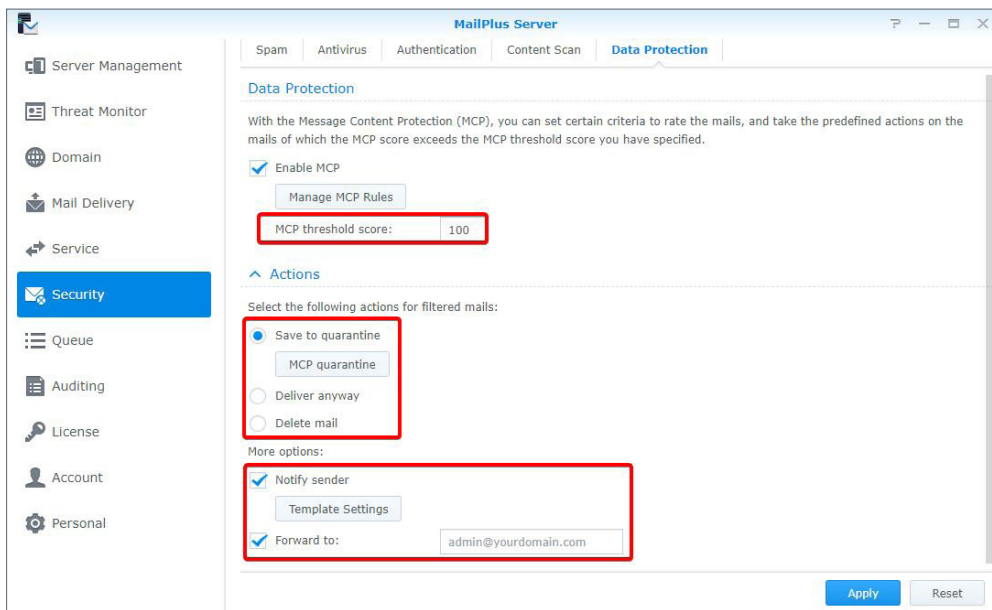
8. 按一下**完成**以結束設定。

## 動作

當規則總分超過 **MCP 門檻分數**時，將會執行指定動作。請參考下列步驟來設定動作：

1. 前往**安全性 > 資料保護**，在資料保護區塊的 **MCP 門檻分數**欄位中輸入一個值。
2. 在**動作**區塊，您可以設定超過 **MCP 門檻分數**時要執行的動作：
  - **儲存至隔離區**：攔截信件並儲存至隔離區。您可以按一下 **MCP 隔離區**按鈕以檢視被隔離的信件內容。有關管理隔離訊息的操作請參考**隔離清單**。
  - **照常傳送**：傳送該信件。
  - **刪除信件**：刪除該信件。
  - **更多選項**：通知寄件者或是將郵件轉寄至特定信箱。

| 功能    | 說明                                 |
|-------|------------------------------------|
| 通知寄件者 | 寄送通知知會寄件者信件已被攔截。您可以按一下範本設定來設定通知內容。 |
| 轉寄至   | 將原始信件轉寄至特定信箱。                      |



3. 按一下**套用**以儲存設定。



## 內容掃描

內容掃描功能會攔截或修改可疑信件。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，請確認啟用的功能符合您的需求。

1. 前往安全性 > 內容掃描。
2. 在內容掃描區塊中勾選啟用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 header 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含有釣魚連結時，會標示該連結以警示收件者。
  - 將 HTML 轉換為純文字：當信件為 HTML 格式時，會被轉換為純文字。
  - 您可以為各個標籤指定以下任一動作：

| 動作    | 說明            |
|-------|---------------|
| 允許    | 傳送該信件。        |
| 拒絕    | 拒絕該信件。        |
| 使標籤失效 | 讓標籤失效後，再傳送信件。 |

**注意：**

- 請針對每個標籤逐一設定。

# 第 10 章：監控設定

## 監控伺服器狀態

透過圖像化介面，您可以快速了解伺服器的運作狀態：

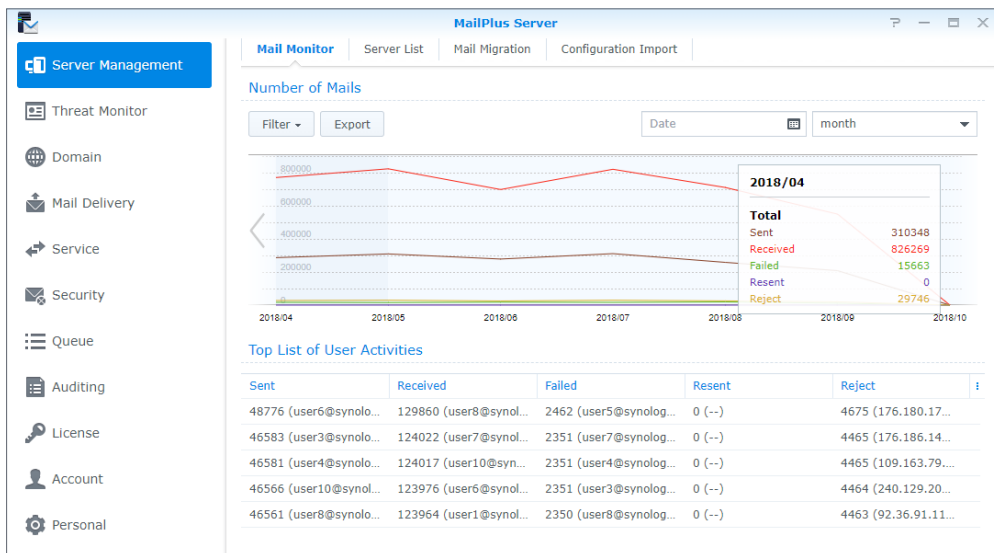
- **郵件流量監控**：監控伺服器在指定區間內處理的郵件流量。
- **威脅監控**：檢視伺服器的各項安全性設定為您擋下多少電子郵件威脅。您可以快速了解所有威脅來源並調整相應的安全性設定。
- **伺服器列表**：檢視伺服器叢集清單和他們的運作狀態。

## 郵件流量監控

伺服器管理的郵件監控頁籤顯示過去一段時間內的郵件活動數量統計，並於最高使用者活動清單區塊顯示各個流量類型中出現最多次的郵件地址。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**高可用叢集**，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、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

您可以透過以下兩種方式監控特定時間區段：

1. 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。
2. 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不同數量的郵件資料，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

在圖表中，詳細資料面板的內容會隨著游標的位置變動。您可以在郵件數量圖表上按一下左鍵，讓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. 在郵件數量區塊中按一下篩選按鈕，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

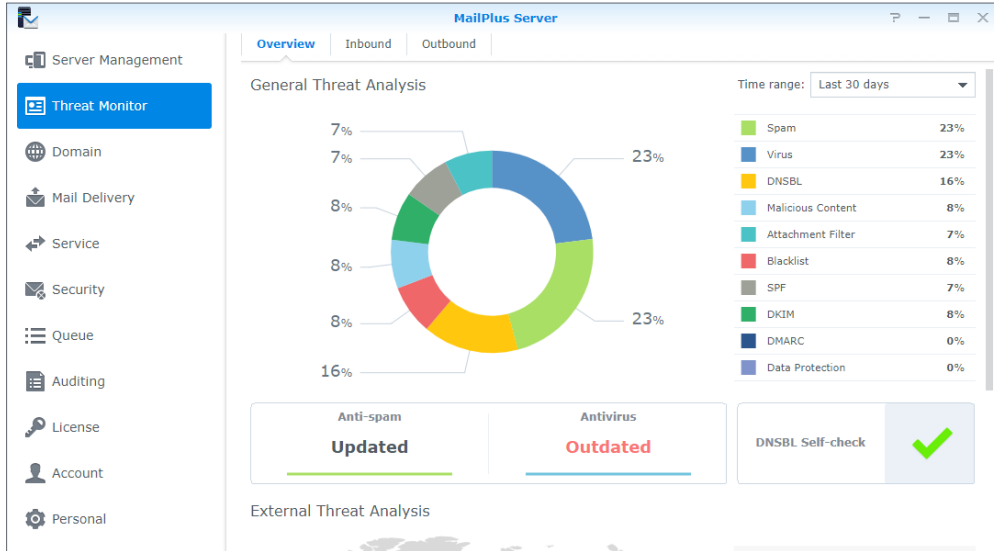
1. 前往伺服器管理 > 郵件監控。
2. 在郵件數量區塊的圖表中按一下您想進一步了解的時間區段。
3. 按一下上方的匯出按鈕。
4. MailPlus Server 會將資料匯出成 HTML 檔案。

## 威脅監控

威脅監控提供電子郵件威脅及其來源的詳細資料，您可以依據威脅分析調整設定，以加強 MailPlus Server 的安全性。

**注意：**

- 若您已設定 **高可用叢集**，請於主要伺服器檢視日誌。



## 檢視整體威脅分析

整體威脅分析以圖表呈現收發電子郵件的各類威脅統計資料。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其相關設定：
  - **時間範圍**：選取後便會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，請將滑鼠移至特定類型上方。
  - **威脅環狀圖**：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。
  - **垃圾郵件防護功能**：查看防垃圾郵件引擎的狀態。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。將滑鼠移到圓圈上，即可查看數量統計資料。
  - **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

您可於**接收**及**傳送**頁籤分別找到已阻擋的收寄電子郵件統計資料，還有此類郵件的主要寄件人及收件人。

1. 前往**威脅監控**。
2. 按一下**接收**或**傳送**頁籤。
  - **時間範圍**：選取時間範圍，查看特定時段內已阻擋的收寄郵件統計資料。
  - **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。

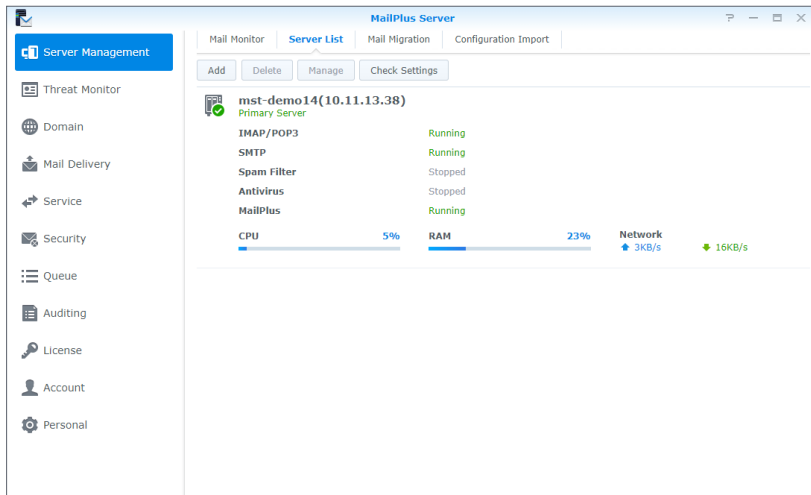
### 注意：

- 若要改變顯示的威脅類型，請選取或取消選取圖表下方的圖例。
- 若要查看各類威脅類型的數量統計資料，請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 資訊，包含CPU、記憶體、網路流量。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**：尚未啟用該功能。
- **異常**：該功能有異常狀況產生。
- **尚未安裝**：僅適用於 MailPlus，表示您尚未安裝 MailPlus。
- **準備就緒中**：表示您剛啟用或關閉該功能，該功能準備要切換狀態。
- **同步信件中**：當您建立或刪除 MailPlus 高可用叢集時，系統會進行信件同步，此狀態表示目前正在同步信件中。



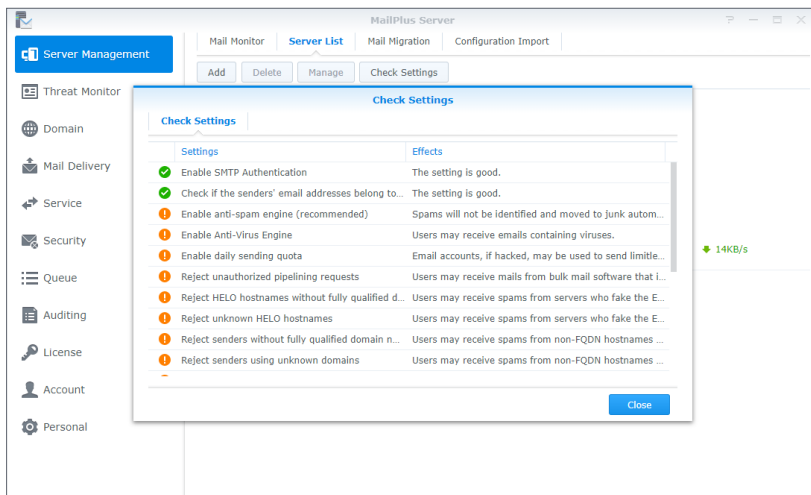
**注意：**

- 若您啟用防毒或 MCP 功能，即使沒有啟用防垃圾郵件功能，垃圾郵件過濾也會跟著啟用，但不會真的進行垃圾郵件掃描。

## 檢查設定

您可以按一下檢查設定按鈕來檢查 MailPlus Server 設定與 Synology 的建議設定是否相同，並檢視設定相異可能會造成的影響。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。



## 監控郵件佇列

查看待處理的郵件狀態，並決定要執行的動作。

### 監控郵件佇列中的訊息

在佇列頁面，您可以檢查所有等待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。

此頁會顯示目前佇列中郵件的下列訊息：

- 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 (原因欄位會顯示郵件訊息傳送失敗的原因)。

| Queue  | Date       | Time     | Sender             | Recipient       | Description |
|--------|------------|----------|--------------------|-----------------|-------------|
| active | 2018-09-12 | 14:10:36 | admin@synology.biz | mk@synology.biz |             |

佇列中的郵件分為下列三種類型：

- **待處理**：郵件訊息等待處理中。
- **處理中**：處理郵件訊息中。
- **延遲傳送**：系統無法順利傳送郵件訊息，稍後將重新寄送。

#### 注意：

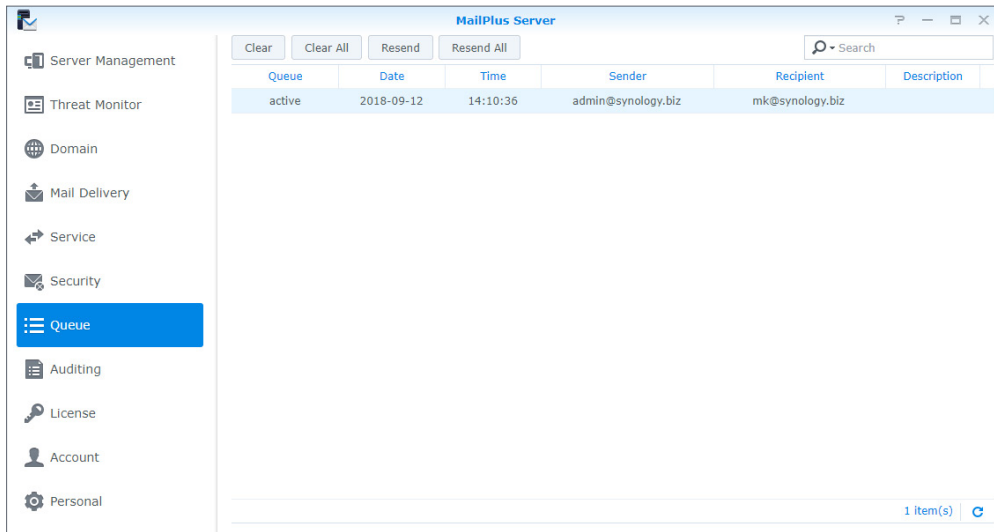
- 延遲傳送的郵件若在接下來的五天內皆重新寄送失敗，會被退回寄件人信箱。

## 管理郵件佇列中的訊息

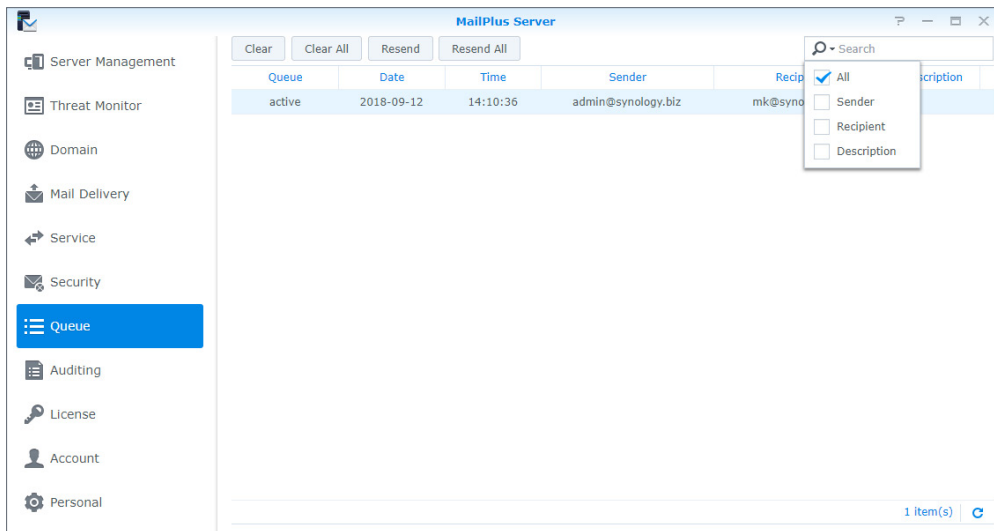
您可以選擇立即重新傳送或取消傳送佇列中的郵件。請參考以下步驟來管理郵件佇列中的郵件訊息：

1. 前往佇列並進行以下操作：

- 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檢視特定郵件的狀態。





## 監控郵件日誌

郵件日誌詳細記錄伺服器發生過的所有事件，您可以透過日誌內容了解問題根源以及相應的解決方法。請注意，日誌會占用一定的儲存空間。

您可以在**稽核**頁面中，進行詳細的日誌設定。

- **檢視日誌**：查看、搜尋、分析日誌記錄的郵件訊息。
- **封存與管理日誌**：進行相關管理設定，包含封存日誌週期、設定備份與輪替規則、傳送日誌到次要伺服器。
- **日誌報表**：定期以信件通知寄送日誌。

### 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、狀態。郵件日誌的狀態分為以下類型：
  - **接收**：表示 MailPlus 使用者收到一封信件。若 MailPlus 使用者寄信給另一位 MailPlus 使用者，則日誌的狀態會顯示為**接收**。若多位 MailPlus 使用者收到同一封訊息，則會產生多筆日誌記錄。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，仍只會記錄一筆收件人為別名地址的日誌。若啟用自動轉寄，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**：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的郵件地址，則會產生多筆日誌記錄。
  - **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 之後的版本將不再顯示此狀態。
  - **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**自動密件副本規則**、**自動轉寄**、**自動回覆**，可能會有額外的日誌內容產生。
- 若您已設定**高可用叢集**，請於主要伺服器檢視日誌。

### 檢視安全性日誌

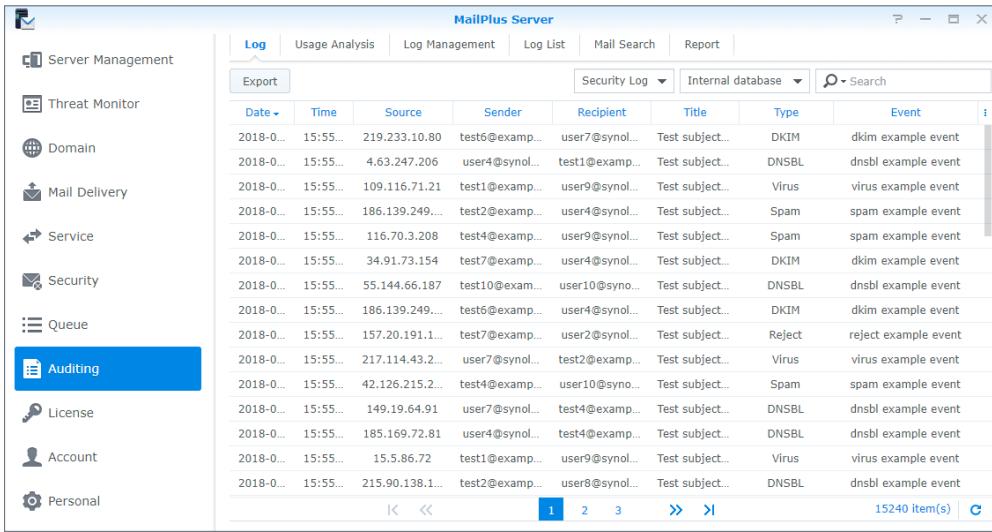
安全性日誌會顯示事件的產生日期和時間、來源、寄件人、收件人、標題、類別、事件說明。安全性日誌可分類為以下類型：**拒絕**、**垃圾郵件**、**病毒**、**DNSBL**、**惡意內容**、**附件過濾器**、**黑名單**、**SPF**、**DKIM**、**DMARC**、**資料保護**，皆與 MailPlus Server 的安全性設定相關。**拒絕**類型為 MailPlus Server 在完整分析信件後決定拒絕的信件。請參考以下步驟來檢視郵件日誌：

#### 注意：

- 若您已設定**高可用叢集**，請於主要伺服器檢視日誌。

## 第 10 章：監控設定

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和內部資料庫。



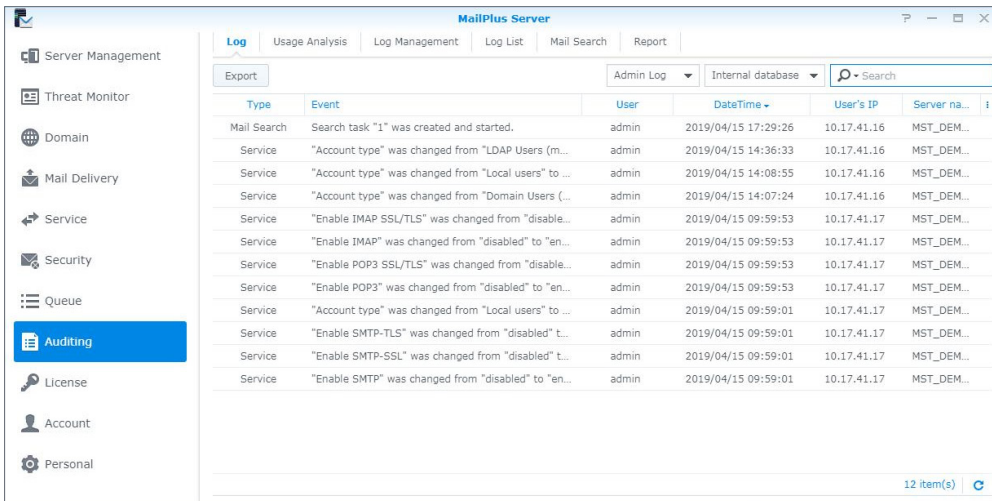
The screenshot shows the MailPlus Server interface with the 'Log' tab selected. The 'Security Log' dropdown is active, and the 'Internal database' is selected. The table displays a list of security events with columns for Date, Time, Source, Sender, Recipient, Title, Type, and Event. The table contains 15 rows of data, and the total number of items is 15240.

| Date      | Time     | Source          | Sender         | Recipient      | Title           | Type   | Event                |
|-----------|----------|-----------------|----------------|----------------|-----------------|--------|----------------------|
| 2018-0... | 15:55... | 219.233.10.80   | test6@examp... | user7@synol... | Test subject... | DKIM   | dkim example event   |
| 2018-0... | 15:55... | 4.63.247.206    | user4@synol... | test1@examp... | Test subject... | DNSBL  | dnsbl example event  |
| 2018-0... | 15:55... | 109.116.71.21   | test1@examp... | user9@synol... | Test subject... | Virus  | virus example event  |
| 2018-0... | 15:55... | 186.139.249...  | test2@examp... | user4@synol... | Test subject... | Spam   | spam example event   |
| 2018-0... | 15:55... | 116.70.3.208    | test4@examp... | user9@synol... | Test subject... | Spam   | spam example event   |
| 2018-0... | 15:55... | 34.91.73.154    | test7@examp... | user4@synol... | Test subject... | DKIM   | dkim example event   |
| 2018-0... | 15:55... | 55.144.66.187   | test10@exam... | user10@syno... | Test subject... | DNSBL  | dnsbl example event  |
| 2018-0... | 15:55... | 186.139.249...  | test6@examp... | user4@synol... | Test subject... | DKIM   | dkim example event   |
| 2018-0... | 15:55... | 157.20.191.1... | test7@examp... | user2@synol... | Test subject... | Reject | reject example event |
| 2018-0... | 15:55... | 217.114.43.2... | user7@synol... | test2@examp... | Test subject... | Virus  | virus example event  |
| 2018-0... | 15:55... | 42.126.215.2... | test4@examp... | user10@syno... | Test subject... | Spam   | spam example event   |
| 2018-0... | 15:55... | 149.19.64.91    | user7@synol... | test4@examp... | Test subject... | DNSBL  | dnsbl example event  |
| 2018-0... | 15:55... | 185.169.72.81   | user4@synol... | test4@examp... | Test subject... | DNSBL  | dnsbl example event  |
| 2018-0... | 15:55... | 15.5.86.72      | test1@examp... | user9@synol... | Test subject... | Virus  | virus example event  |
| 2018-0... | 15:55... | 215.90.138.1... | test2@examp... | user8@synol... | Test subject... | DNSBL  | dnsbl example event  |

## 檢視管理日誌

管理日誌記錄 MailPlus Server 設定的變更，每筆日誌會顯示事件的簡短描述、類型、使用者帳號、日期和時間、使用者的 IP 位址、伺服器名稱。請參考以下步驟來檢視管理日誌：

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。



The screenshot shows the MailPlus Server interface with the 'Log' tab selected. The 'Admin Log' dropdown is active, and the 'Internal database' is selected. The table displays a list of administrative events with columns for Type, Event, User, DateTime, User's IP, and Server name. The table contains 12 rows of data, and the total number of items is 12.

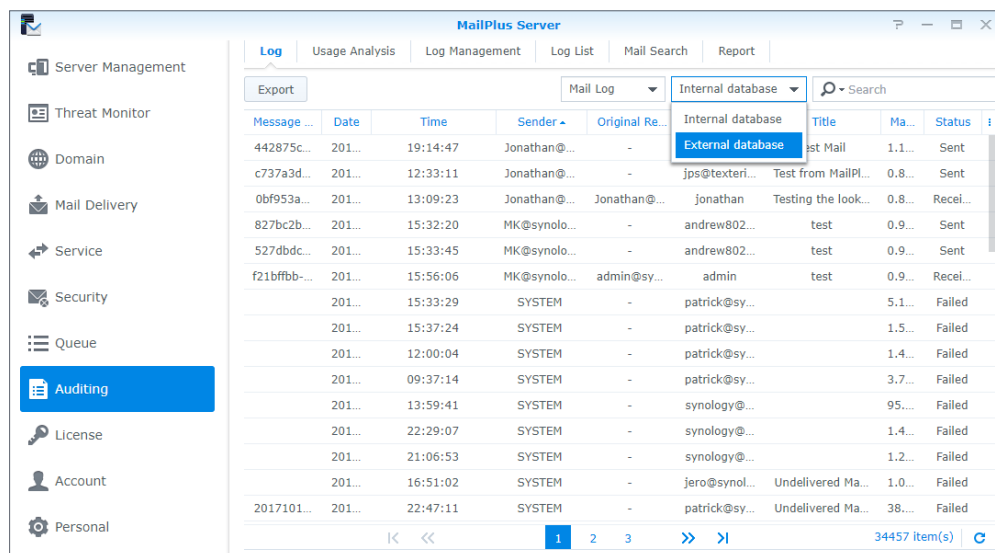
| Type        | Event                                                | User  | DateTime            | User's IP   | Server na... |
|-------------|------------------------------------------------------|-------|---------------------|-------------|--------------|
| Mail Search | Search task "1" was created and started.             | admin | 2019/04/15 17:29:26 | 10.17.41.16 | MST_DEM...   |
| Service     | "Account type" was changed from "LDAP Users (m...    | admin | 2019/04/15 14:36:33 | 10.17.41.16 | MST_DEM...   |
| Service     | "Account type" was changed from "Local users" to ... | admin | 2019/04/15 14:08:55 | 10.17.41.16 | MST_DEM...   |
| Service     | "Account type" was changed from "Domain Users (...   | admin | 2019/04/15 14:07:24 | 10.17.41.16 | MST_DEM...   |
| Service     | "Enable IMAP SSL/TLS" was changed from "disable...   | admin | 2019/04/15 09:59:53 | 10.17.41.17 | MST_DEM...   |
| Service     | "Enable IMAP" was changed from "disabled" to "en...  | admin | 2019/04/15 09:59:53 | 10.17.41.17 | MST_DEM...   |
| Service     | "Enable POP3 SSL/TLS" was changed from "disable...   | admin | 2019/04/15 09:59:53 | 10.17.41.17 | MST_DEM...   |
| Service     | "Enable POP3" was changed from "disabled" to "en...  | admin | 2019/04/15 09:59:53 | 10.17.41.17 | MST_DEM...   |
| Service     | "Account type" was changed from "Local users" to ... | admin | 2019/04/15 09:59:01 | 10.17.41.17 | MST_DEM...   |
| Service     | "Enable SMTP-TLS" was changed from "disabled" t...   | admin | 2019/04/15 09:59:01 | 10.17.41.17 | MST_DEM...   |
| Service     | "Enable SMTP-SSL" was changed from "disabled" t...   | admin | 2019/04/15 09:59:01 | 10.17.41.17 | MST_DEM...   |
| Service     | "Enable SMTP" was changed from "disabled" to "en...  | admin | 2019/04/15 09:59:01 | 10.17.41.17 | MST_DEM...   |

## 檢視外部資料庫

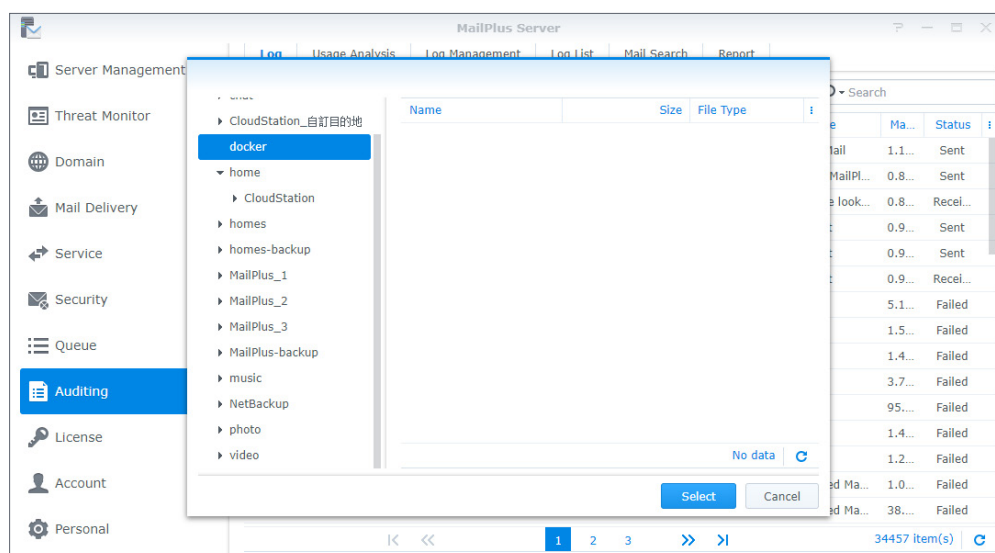
若您有封存日誌、產生日誌資料庫、下載日誌檔案，您可以檢視外部資料庫中存放的日誌內容。

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、安全性日誌、管理日誌，再選取外部資料庫。



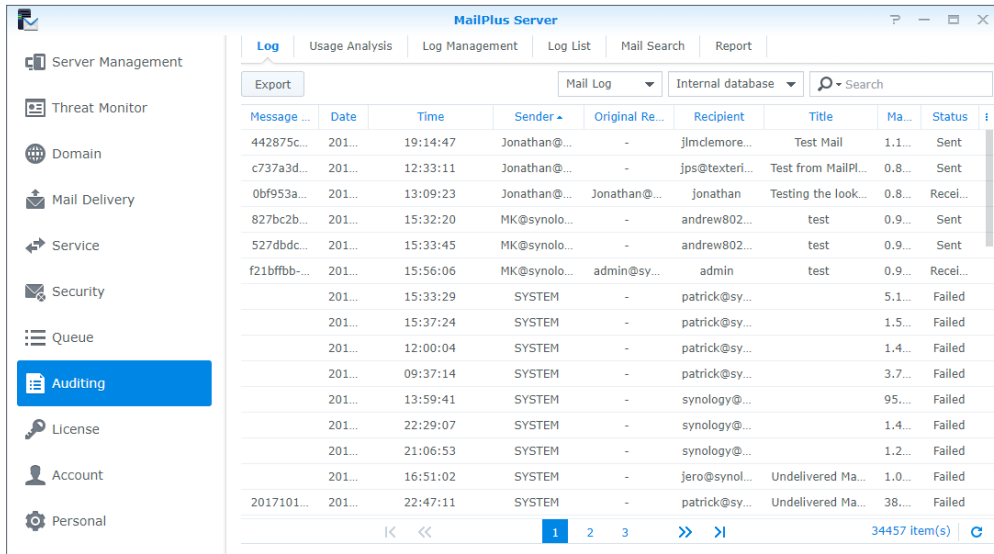
3. 找到您的外部資料庫在 Synology NAS 上的所在位置。
4. 按一下選擇按鈕。



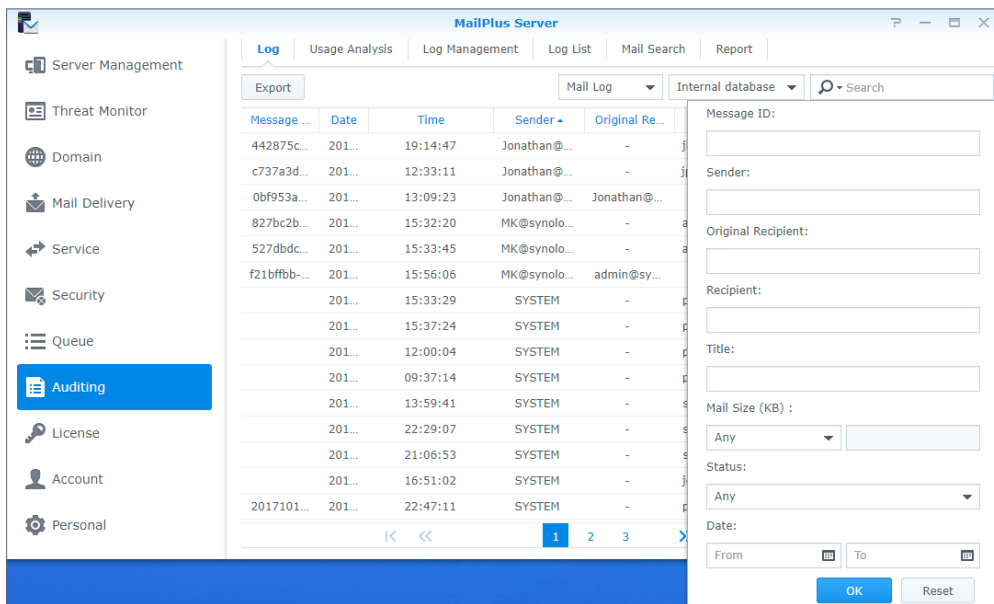
### 搜尋日誌

您可以前往稽核 > 日誌，透過簡易搜尋或進階搜尋來查找日誌。

- 簡易搜尋：在頁面右上角的搜尋欄位中輸入關鍵字：
  - 針對郵件日誌，此關鍵字用於比對 Message ID、寄件人、收件人、標題欄位。
  - 針對安全性日誌，此關鍵字用於比對來源、寄件人、收件人、標題、事件欄位。
  - 針對管理日誌，此關鍵字用於比對類型、事件、使用者帳號、使用者 IP 位址、伺服器名稱欄位。



- 進階搜尋：按一下頁面右上角搜尋欄位中的放大鏡圖示，並設定各個欄位的搜尋條件以執行精細的進階搜尋，完成後按一下確定。您可以在狀態下拉式選單中選擇網域內部來搜尋內部使用者之間互相寄送的信件。

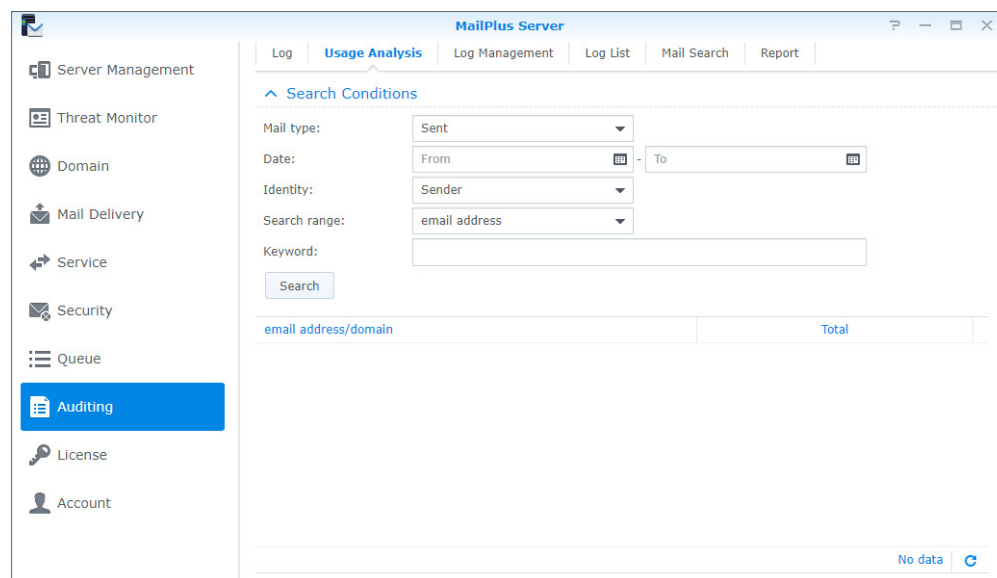


## 匯出日誌內容

在**稽核 > 日誌**，您可以將日誌匯出為 HTML 檔案。若您在搜尋後按一下**匯出**，將會匯出目前的搜尋結果。詳情請參考[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網域所收寄的信件。

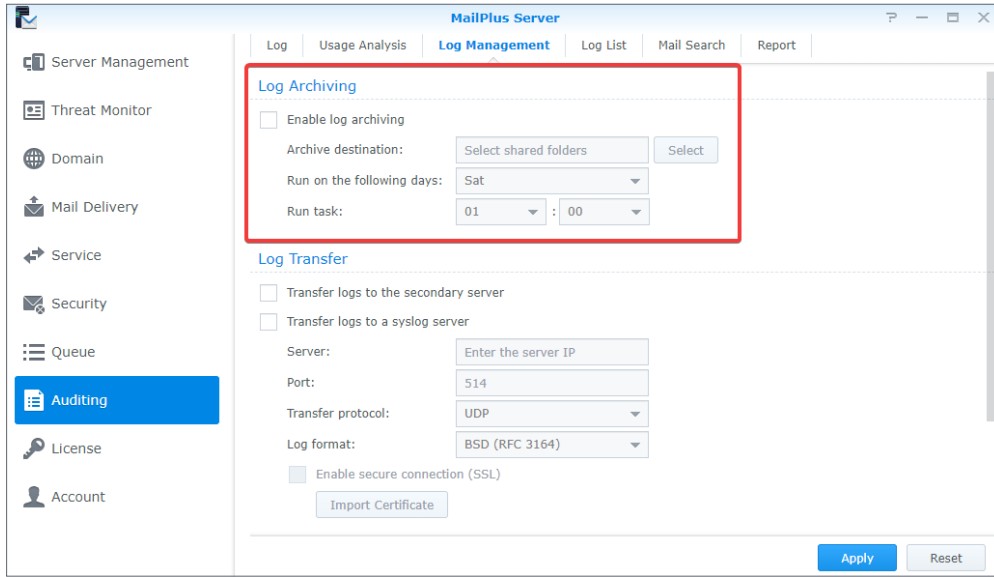


## 封存日誌

您可以設定日誌封存，讓 MailPlus Server 依照使用者自訂排程來封存郵件日誌、安全性日誌、Postfix 日誌。請注意，一旦您無法存取共用資料夾，系統便會自動停用封存功能。

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**區塊中勾選**啟用日誌封存**核取方塊。
3. 按一下**封存目的地**欄位旁的**選擇**按鈕，選取您要存放封存檔案的位置。
4. 選擇執行封存任務的時間。
5. 按一下**套用**以儲存設定。



### 將日誌傳送至次要伺服器

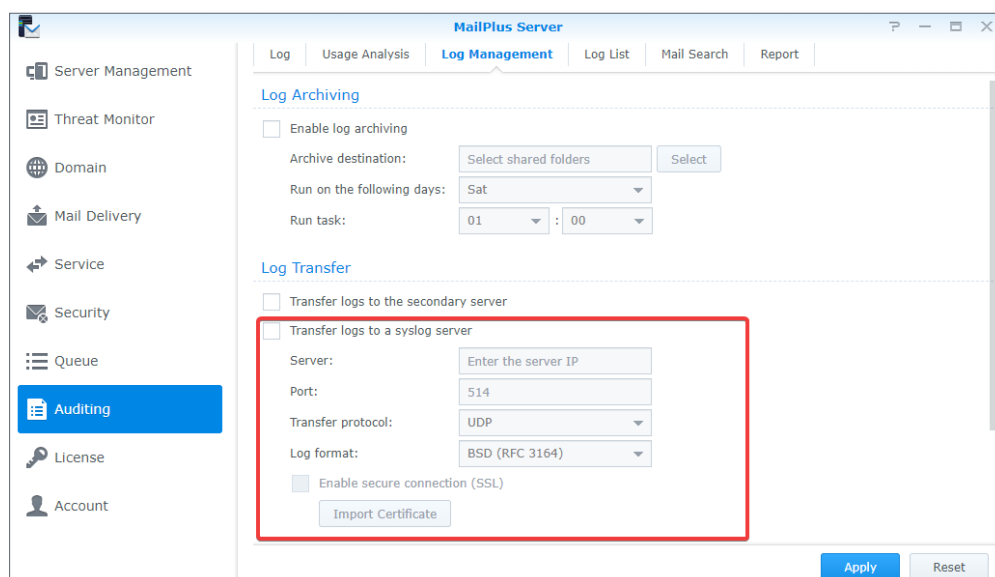
高可用叢集建立後，日誌會存放於主要伺服器。您亦可傳送副本至次要伺服器，但必須先產生日誌資料庫才能將日誌傳送至次要伺服器 (請參考 [產生日誌資料庫](#))。請參考以下步驟將日誌傳送至次要伺服器：

1. 前往稽核 > 日誌管理。
2. 在日誌傳送區塊中勾選將日誌傳送至次要伺服器核取方塊。
3. 按一下套用以儲存設定。

### 將 Postfix 日誌傳送至其他 syslog 伺服器

請參考以下步驟來將 Postfix 日誌傳送到其他 syslog 伺服器：

1. 前往稽核 > 日誌管理。
2. 在日誌傳送區塊中勾選將日誌傳送至 syslog 伺服器核取方塊。
3. 輸入 syslog 伺服器的 IP 位址。
4. 若您勾選啟用安全連線 (SSL) 核取方塊，可能需要按一下匯入憑證按鈕來匯入該 syslog 伺服器的憑證，才能正常傳送日誌。
5. 按一下套用以儲存設定。

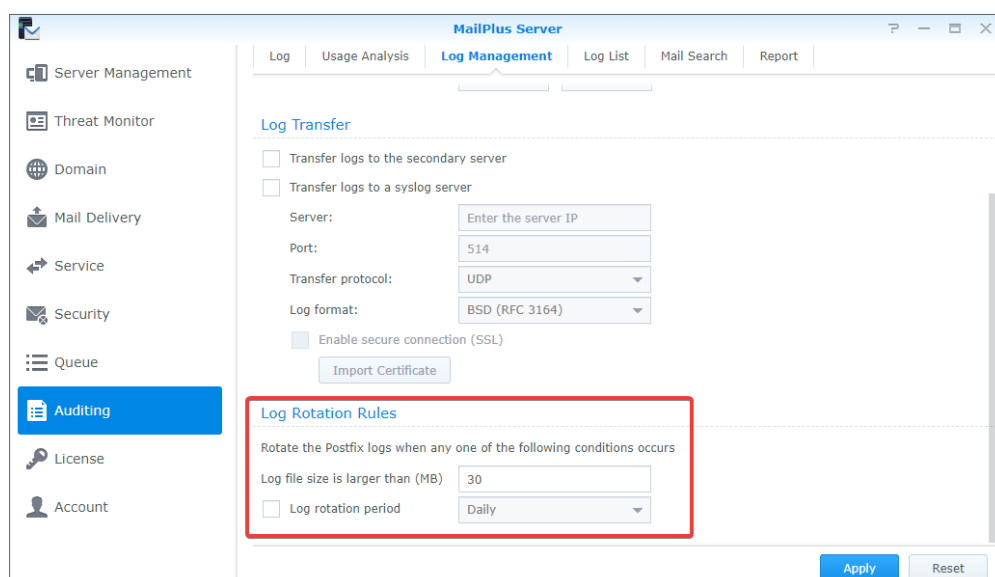


## 設定日誌輪替規則

您可以設定 Postfix 日誌的輪替週期以及檔案大小限制；郵件日誌以及安全性日誌則會固定保存最近的四百萬筆資料。

請參考下列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的日誌檔案大小大於 (MB) 欄位中輸入您的 Postfix 日誌檔案大小上限。
3. 在日誌輪替規則區塊中勾選日誌輪替週期核取方塊，再從下拉式選單選擇輪替週期。
4. 按一下套用以儲存設定。

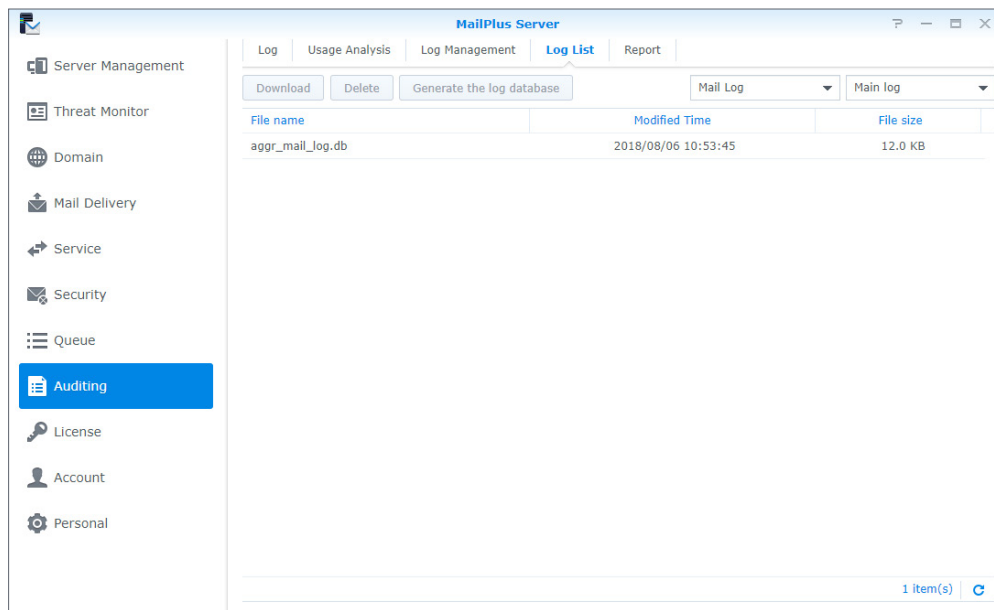


## 下載與刪除日誌檔案

您可以在**稽核 > 日誌清單**下載或刪除 MailPlus Server 內的郵件日誌、安全性日誌、管理日誌、Postfix 日誌。

請參考下列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**、**管理日誌**、**Postfix 日誌**。
3. 若您已設置 MailPlus 高可用叢集並啟用**將日誌傳送至次要伺服器**，可在次要伺服器的下拉式選單中選擇**已接收日誌**；否則請選擇**主要日誌**。
4. 選擇日誌檔案後，可以按一下**下載**按鈕來下載檔案，或按一下**刪除**按鈕來將伺服器上的檔案刪除。

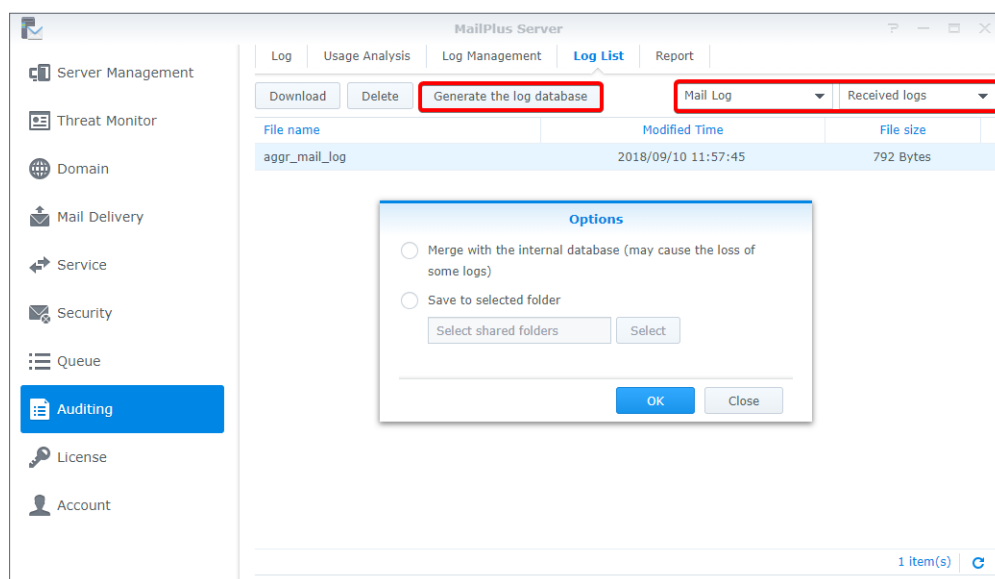


## 產生日誌資料庫

若已啟用**將日誌傳送至次要伺服器**，您可以透過**產生日誌資料庫**功能來將接收到的日誌內容轉換成資料庫檔案，之後您便可以在**稽核 > 日誌檢視外部資料庫**，以查看日誌內容。

1. 前往**稽核 > 日誌清單**。
2. 從下拉式選單中選擇**郵件日誌**、**安全性日誌**，或 **Postfix 日誌**。
3. 請從下拉式選單中選擇**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，並選擇目的地資料夾。
6. 按一下**確定**來完成設定。



**注意：**

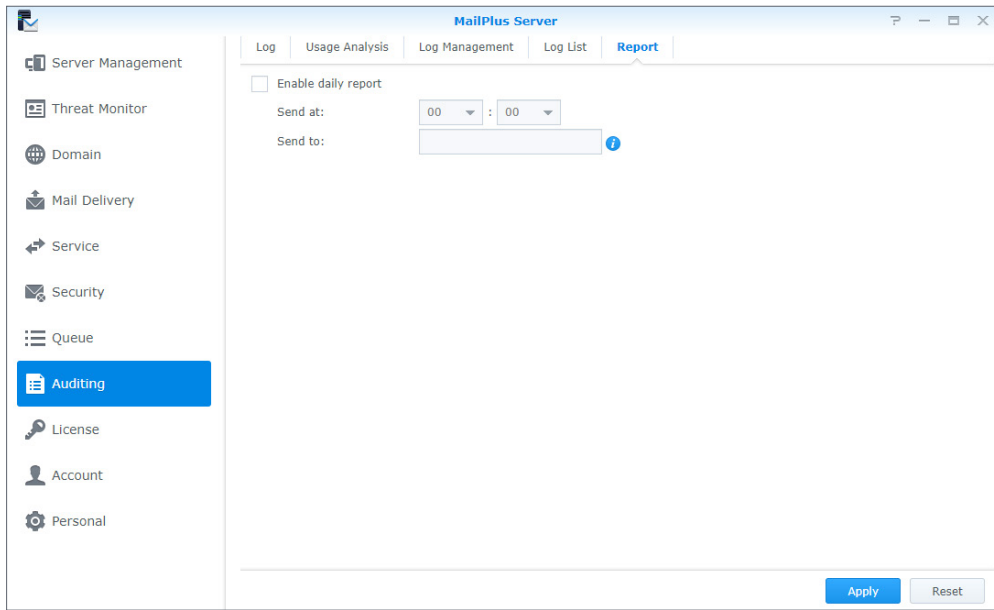
- 您不需要為管理日誌建立資料庫，一旦啟用將日誌傳送至次要伺服器，兩台伺服器上皆可檢視管理日誌。
- 僅有在啟用將日誌傳送至次要伺服器後產生的日誌會同步至他台伺服器。

**設定每日報表**

您可以啟用每日報表功能，MailPlus Server 會將前一天的 Postfix 日誌寄送至指定郵件地址。

請參考下列步驟來設定每日報表：

1. 前往稽核 > 報表。
2. 勾選啟用每日報表核取方塊。
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，最多可指定兩個郵件地址，請以分號 (;) 區隔地址。



### 設定郵件搜尋

您可以搜尋 MailPlus Server 上所有索引過的信件，亦可檢視、刪除、匯出搜尋結果。

請參考下列步驟來新增郵件搜尋任務：

1. 前往稽核 > 郵件搜尋。
2. 按一下加號圖示 (+) 來新增任務。
3. 輸入任務名稱。
4. 設定搜尋條件：
  - 預定條件：您可以為單一任務設定多條搜尋規則。從下拉式選單中選擇要搜尋符合全部或是任一項規則的郵件，並依據寄件人、收件人、主旨、關鍵字、郵件大小 (MB)、日期來輸入應包含或不包含的關鍵字。
  - 自訂：您可以使用搜尋運算子及關鍵字來自訂搜尋條件。舉例來說，若要找到 2018/5/25 之後所收到的 GDPR 相關信件，且其寄件人為 admin@synology.com，則可以輸入 after:2018/05/25 AND from:admin@synology.com AND GDPR 作為搜尋條件。

| 搜尋運算子    | 用途          | 範例          |
|----------|-------------|-------------|
| from:    | 來自指定寄件者的信件  | from: 小美    |
| to:      | 寄給指定收件者的信件  | to: 小明      |
| subject: | 主旨含有特定字詞的信件 | subject: 晚餐 |

| 搜尋運算子              | 用途                     | 範例                      |
|--------------------|------------------------|-------------------------|
| OR                 | 含有多個指定字詞的信件            | from: 小美 OR<br>from: 小明 |
| - 或 NOT            | 應從搜尋結果中移除的信件           | 晚餐 - 電影                 |
| ()                 | 含有指定字詞組合的信件            | subject:(晚餐 電影)         |
| in:                | 特定郵件匣內的信件              | in:" 功能建議 "             |
| label:             | 包含特定標籤的信件              | label: 朋友               |
| before: 或 after:   | 特定期間內收發的信件             | after:2004/04/16        |
| larger: 或 smaller: | 大於或小於特定大小的信件 ( 單位為 MB) | larger:10M              |
| filename:          | 夾帶特定名稱或特定檔案類型的附件       | filename:pdf            |
| has:attachment     | 夾帶附件的信件                | has:attachment          |
| is:starred         | 標記星號信件                 | is:starred              |
| is:unread          | 未讀信件                   | is:unread               |

5. 設定目標使用者。若未指定目標使用者，則任務預設會搜尋所有使用者。
6. 按下**確定**後會立即執行任務。
7. 若要停止進行中的任務，點選該任務，並按一下右側面板的**停止任務**。若要重新執行任務，按一下**搜尋**。
8. 您可以透過點選相對應圖示來**編輯**、**複製**、**刪除**任務。

**Add**

**Search Conditions** | Target User

Task name:

Search Conditions:

Pre-defined conditions  Custom

All match the following rule:

Sender contains admin@synology.com

Add

OK Cancel

### 檢視郵件搜尋結果

1. 前往稽核 > 郵件搜尋，選擇一個已完成任務。
2. 在右側面板，您可以下載任務報告或查看結果來檢視詳細資訊或執行進一步操作。任務報告會記錄任務的詳細資訊，包含搜尋的郵件數量和被刪除的郵件。
3. 在查看結果視窗，您可以檢視、刪除、匯出個別郵件。當您點選郵件時，該郵件的詳細資訊會出現在右方區塊中，您亦可下載原始郵件或其附件，或在新視窗中開啟郵件。

**Search Result**

Delete Export Search

|                          | Subject | Sender | Recipient |
|--------------------------|---------|--------|-----------|
| <input type="checkbox"/> |         |        |           |
| <input type="checkbox"/> |         |        |           |
| <input type="checkbox"/> |         |        |           |
| <input type="checkbox"/> |         |        |           |
| <input type="checkbox"/> |         |        |           |

5 item(s)

**DSM and packa...**

From

To

Cc

Bcc -

Date 2019-10-07 02:04:21

Attachment -

Close

## 匯出郵件搜尋結果

我們建議您匯出重要的搜尋結果作為備份檔案，並將其存放於本地裝置以供日後使用。

1. 前往**稽核 > 郵件搜尋**，選擇一個已完成任務。
2. 選擇一個任務並按一下右側面板的**查看結果**。
3. 請選擇欲匯出的搜尋結果，按一下**匯出**。
4. 您可以按一下**匯出**按鈕旁的箭頭符號，來指定是否要一併匯出信件清單及原始信件。
5. 信件清單會匯出為 **export.zip** 檔案，您可透過支援 CSV 檔案格式的文件編輯器來修改檔案。若要分發稽核任務，您可以將該記錄分成多個檔案。原始信件則會匯出為 EML 檔案，您可以在 **eml** 資料夾中找到該檔案。

## 匯入郵件搜尋結果

若您之前曾經匯出郵件搜尋結果並存放於本地裝置上，隨時都可以匯入信件清單來檢視郵件。

1. 前往**稽核 > 郵件搜尋**。
2. 按一下垃圾桶圖示旁的**匯入任務**按鈕。
3. 上傳 CSV 格式的信件清單並輸入任務名稱。
4. 按一下**匯入**。
5. 一旦匯入完成，該任務就會出現在任務清單頂端。

# 第 11 章：災難備援

## 高可用叢集

MailPlus Server 提供兩種解決方案：單一節點設置與高可用設置。單一節點設置僅需一台 Synology NAS 來執行郵件服務；高可用設置則是以兩台 Synology NAS 組成高可用 (HA) 叢集，避免非預期的故障引發郵件服務中斷。

**注意：**

- MailPlus HA 僅適用於 MailPlus。若要了解更多關於 MailPlus 高可用機制的資訊，請參閱 [MailPlus 高可用白皮書](#)。

### 高可用 (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會連線到 MailPlus HA 叢集的主要 IP 位址，主要伺服器持有 MailPlus HA 叢集的主要 IP 位址並接受所有服務請求，此請求會再分配給主要伺服器或次要伺服器處理。

主要伺服器以及次要伺服器之間會進行雙向同步，以確保兩台伺服器上的郵件資料及伺服器設定保持一致，當兩台伺服器分別處理不同的服務需求，或當您於其中一台伺服器修改 MailPlus Server 設定時，雙向同步功能可降低資料不一致的可能性。

不同於郵件資料及伺服器設定，在 HA 叢集之下的日誌會存放於主要伺服器，如欲在次要伺服器檢視日誌內容，請參閱[將日誌傳送至次要伺服器](#)來寄送副本。

HA 設置可減少伺服器故障所造成的服務中斷，當主要伺服器故障時，次要伺服器會暫時接手所有郵件服務請求，待主要伺服器修復後，這段期間內的郵件資料變動會同步更新到主要伺服器上。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，待次要伺服器修復後，故障期間內的郵件資料變動也將同步更新到次要伺服器上。

**注意：**

- MailPlus 高可用叢集與 Synology High Availability (SHA) 為兩個不同的叢集系統，兩者無法同時在同一台 Synology NAS 上運作。
- VDSM 上無法使用 MailPlus HA 與 SHA。如需詳細資訊，請參閱 [VDSM 管理手冊](#)。
- Synology High Availability 支援 MailPlus Server 2.2 或以上的版本。
- 若有服務不中斷的需求，建議您使用專為郵件服務設計的 MailPlus 高可用叢集，此架構可確保高可用叢集恢復正常後，伺服器間的郵件資料維持一致，不會遺失在腦裂 (Split-brain) 錯誤發生期間更新的資料。
- 在 SHA 架構下，兩台 MailPlus 伺服器將被視為一台，並共用 5 個免費授權；相對地，在 MailPlus HA 架構下，可使用 10 個免費授權。
- 在高可用環境中，您可以在任一台伺服器上檢視授權，但建議於主要伺服器上管理授權以維持狀態的一致性。

**設置高可用 (HA) 前的注意事項****1. 準備兩台 Synology NAS：**

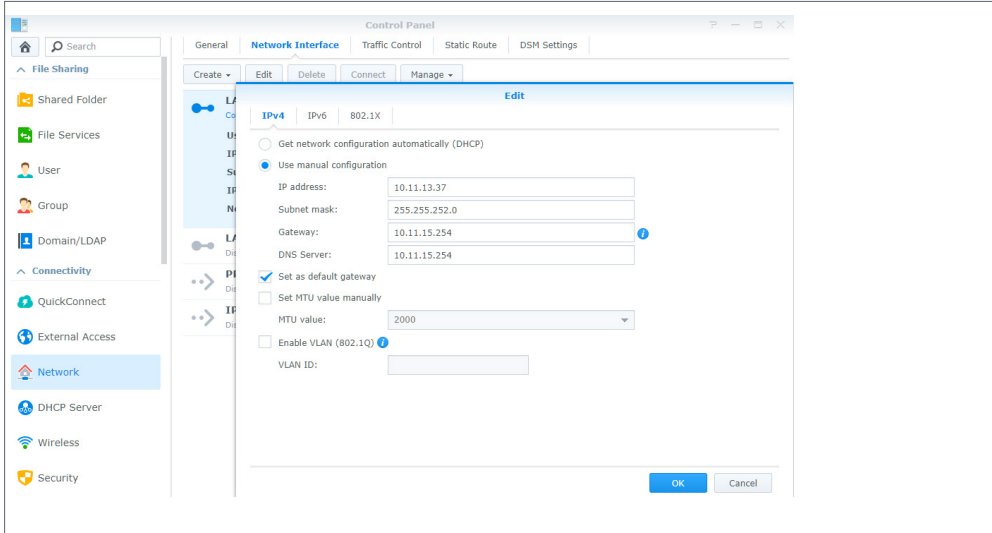
- 前往**控制台** > **資訊中心** > **Synology 帳戶**，讓兩台 Synology NAS 登入相同的 Synology 帳戶。
- 前往**控制台** > **區域選項** > **時間**，同步兩台 Synology NAS 的系統時間。
- 前往**套件中心**，在兩台 Synology NAS 上安裝並啟動 **MailPlus Server** 與 **MailPlus**。如需建立 MailPlus Server 的相關資訊，請參閱[設定 MailPlus Server](#)。
- 設定完 MailPlus Server 後，系統會自動將 **MailPlus** 共用資料夾新增至 Synology NAS，為確保用戶端可以順利存取 MailPlus，不建議您自行修改權限設定，請讓 **MailPlus** 共用資料夾的權限設定維持預設。
- 前往**控制台** > **權限**，設定目標使用者或群組對於 MailPlus Server 及 MailPlus 的權限。兩台 Synology NAS 的權限設定應相同。

**注意：**

- 兩台 Synology NAS 安裝 MailPlus Server 的儲存空間大小應相同，此外，由於所有的收發信件會同步到兩邊的儲存空間，請確認儲存空間大小符合郵件所需的儲存空間容量。
- 若您已在兩邊的儲存空間掛載 SSD 快取，請注意以下事項：
  - 應為 RAID 1 配置下的讀寫快取。
  - 快取大小應相同。
- HA 叢集建立期間，次要伺服器必須暫時停用兩步驟驗證功能。
- 由於所有郵件皆會在兩台機器上完整同步及儲存，建議使用相同大小且具備充足空間的 DSM 儲存空間。
- 建議保留 MailPlus 共用資料夾的預設權限設定。MailPlus Server 安裝後，建立 MailPlus 共用資料夾時會自動設定權限。
- 若儲存空間皆安裝 SSD 快取，建議為 R/W 快取建立 RAID 時皆使用相同配置。

2. 指定兩組固定 IP 給主要與次要伺服器：

- 兩台 Synology NAS 的 IP 位址必須位於同一個區域網路 (Local Area Network · LAN)。
- 不能為透過 PPPoE 或 DHCP 取得的 IP 位址。
- 該 IP 位址的網路介面卡必須設定為手動設置網路組態。



3. 兩台 Synology NAS 必須加入同一網域：

- 兩台 Synology NAS 必須加入相同的 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 伺服器。
- 若您的環境中並沒有 Windows Active Directory 或 LDAP 伺服器，您可以前往[套件中心](#)安裝 **Synology Directory Server** 或 **LDAP Server** 來建立網域或 LDAP 伺服器，以進行帳號管理。請注意，當執行目錄服務的 Synology NAS 狀態異常或沒有回應時，自架的 LDAP 或網域服務會有導致郵件服務中斷的風險。

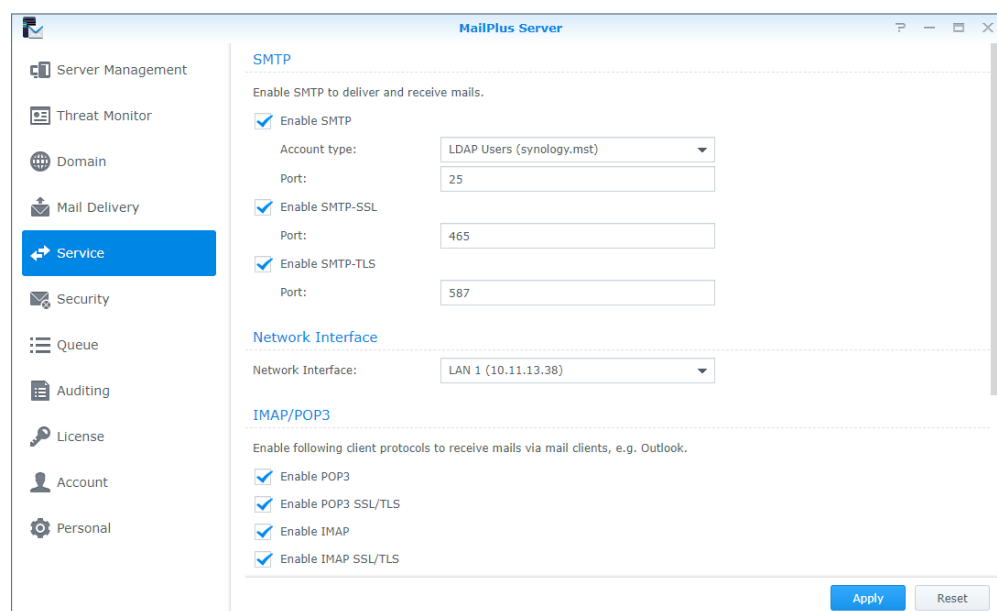
4. 準備一組 HA 叢集使用的內部與外部 IP 位址：

- 為 HA 叢集保留一個未使用的固定內部 IP 位址，該 IP 位址需與兩台 Synology NAS 的 IP 位址處於相同的區域網路，並保留一個未使用的外部 IP 位址。
- 在路由器上設定連接埠轉送規則，以轉送叢集的內部及外部 IP 位址之間的流量。
- 在公共 DNS 伺服器上註冊叢集的外部 IP 位址。

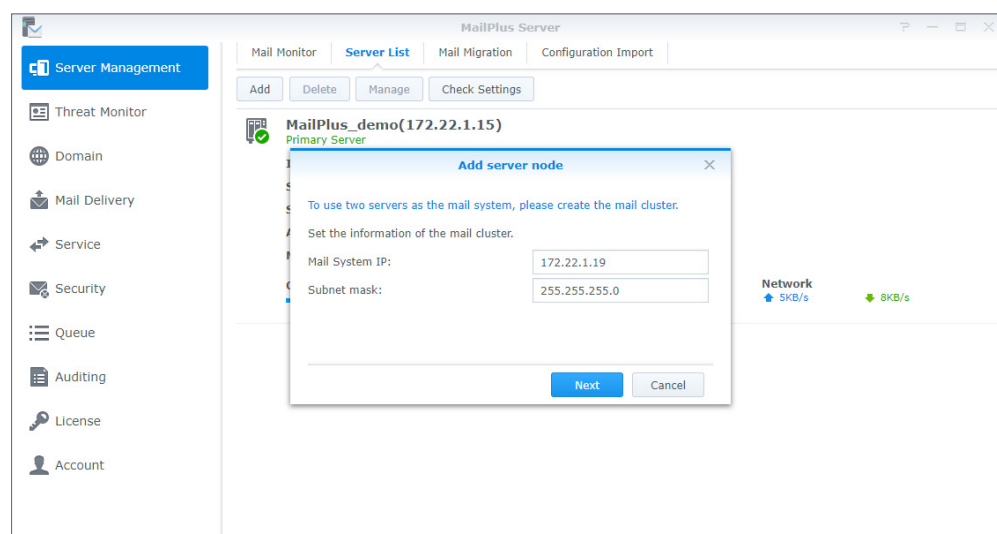


## 設置高可用 (HA)

1. 開啟設定好的 MailPlus Server。
2. 前往服務，確認已在 SMTP 區塊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，按一下新增按鈕。
4. 輸入 HA 叢集的主要內部 IP 位址，再按下一步。



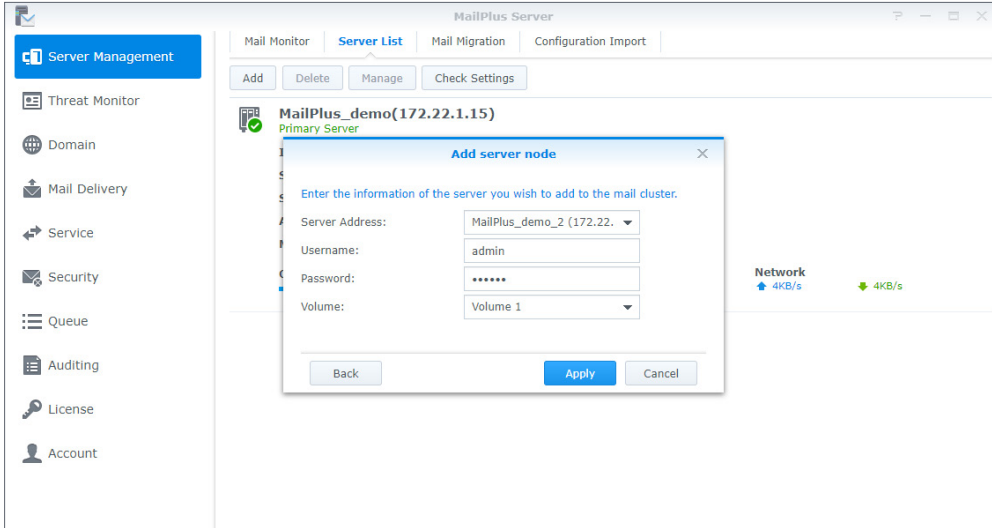
5. 在伺服器位址欄位中輸入次要伺服器的 IP 位址，或是從伺服器位址下拉式選單中選擇一台 Synology NAS 作為次要伺服器使用。位於同一區域網路內的 Synology NAS 會列於下拉式選單。

### 注意：

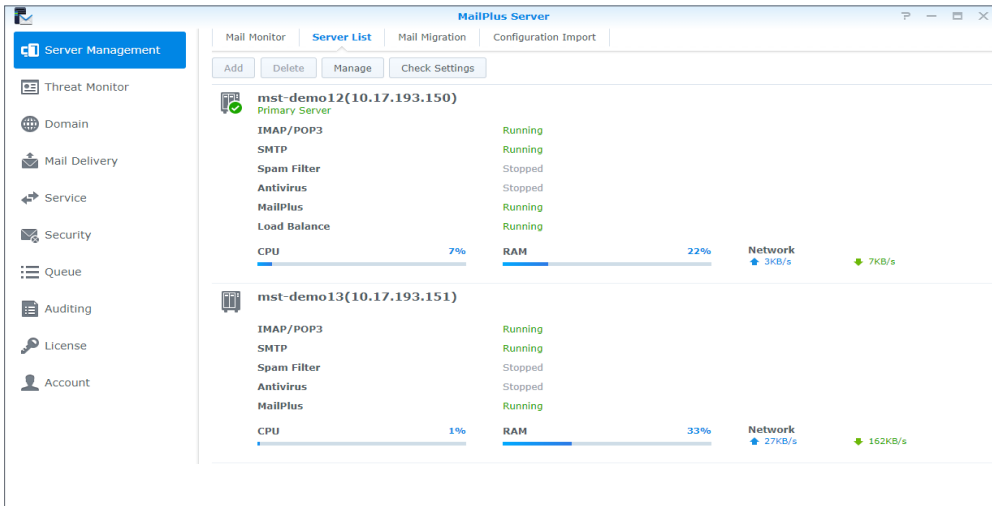
- 次要伺服器需要綁定一組網路介面，您需要輸入該綁定網路介面的 IP 位址。

## 第 11 章：災難備援

6. 在使用者帳號和密碼欄位輸入次要伺服器管理員的帳號密碼。請注意，在 HA 叢集建立期間，次要伺服器必須暫時停用兩步驟驗證功能。
7. 儲存空間下拉式選單將列出次要伺服器上已建立的儲存空間，請選擇在次要伺服器上用來儲存信件資料及 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，信件會開始同步到次要伺服器上，同步所需時間視主要伺服器上存放的信件數量而定。同步過程中，您仍然可以收寄信件，主要伺服器會在同步完成前處理所有服務需求，待同步完成後，主要伺服器以及次要伺服器將分擔郵件服務工作。



### 注意：

- 第一次同步通常會出現伺服器高負載的情況，此期間雖然可以使用 MailPlus 服務，但相對緩慢。因此若您已使用 MailPlus Server 長達一段期間且信件總數龐大，建議您可預先使用 **Hyper Backup** 來將大多數的信件複製到次要伺服器，以縮短載入時間並加快同步速度。若要了解使用 **Hyper Backup** 備份信件的詳細資訊，請參閱 [備份及還原信件](#)。

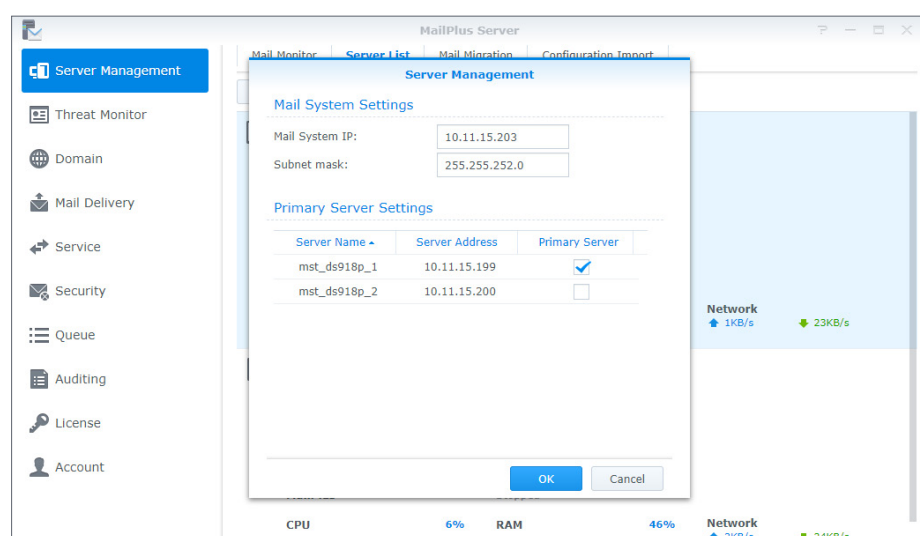
## 變更高可用 (HA) 叢集設定

1. 開啟設定好的 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 HA 叢集的 IP 位址及其子網路遮罩設定。

### 注意：

- 修改過的 IP 位址必須與主要伺服器及次要伺服器的 IP 位址位於相同的區域網路。

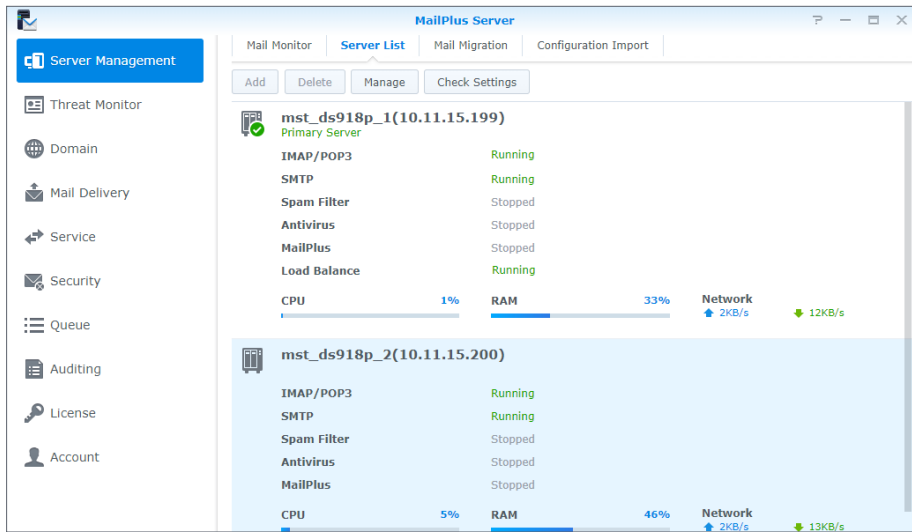
5. 在主要伺服器設定區塊中，您可以選擇一台 Synology NAS 作為 HA 叢集的主要伺服器，主要伺服器會持有 HA 叢集的內部 IP 位址並接受所有郵件服務請求，此請求會再分配給主要伺服器或次要伺服器處理。



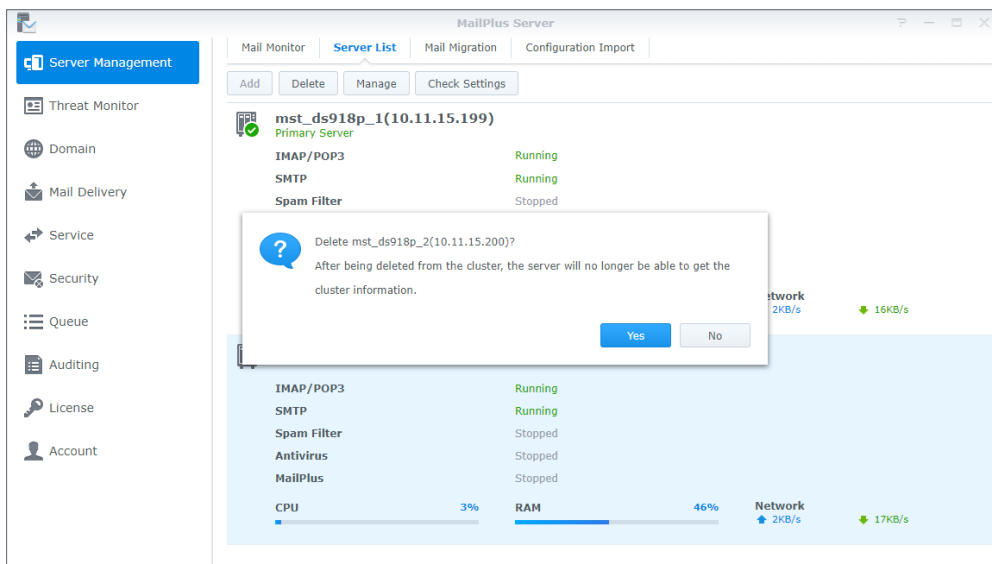
## 移除高可用 (HA) 設置

移除 HA 設置時，郵件資料將會自動同步，以確保兩台 Synology NAS 上的郵件資料一致。設定解除後，HA 叢集的對內 IP 位址將不會由任何一台 Synology NAS 所持有，因此，您可能需要調整防火牆裝置的連接埠轉送和非軍事區 (DMZ) 設定，或是更改 DNS 記錄。請參考以下步驟來移除 HA 叢集內的其中一台 Synology NAS：

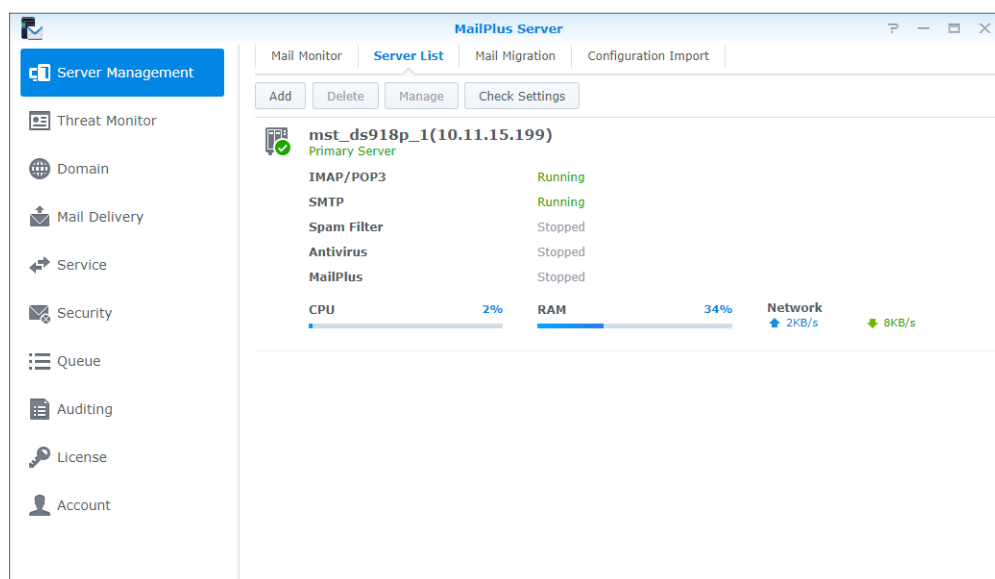
1. 在欲保留的 Synology NAS 上登入 DSM，開啟 MailPlus Server。
2. 前往伺服器管理 > 伺服器列表。
3. 選擇欲刪除的 Synology NAS。



4. 按一下刪除按鈕。
5. 在彈出視窗中按一下是。



6. 郵件同步完成後，HA 叢集便會解除，您欲保留的伺服器仍然會持續接受並處理郵件服務請求。請確認是否需要調整防火牆裝置的連接埠轉送和非軍事區 (DMZ) 設定，或是更改 DNS 記錄。



## 伺服器故障

當 HA 叢集內的其中一台 Synology NAS 發生故障時，另一台將持續提供郵件服務。以下所提到的主要伺服器及次要伺服器指的都是當初進行 HA 設置時分配的原始角色，而非切換後的伺服器角色。

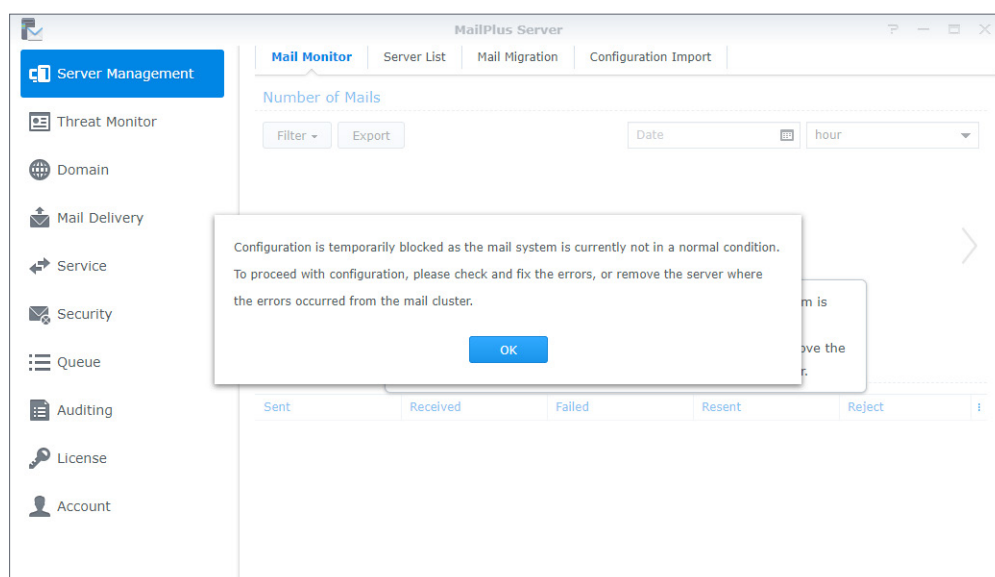
### 注意：

- 若您將一個節點變更至新裝置，請重新設定 MailPlus 高可用叢集。

## 主要伺服器故障

當原本的主要伺服器故障，原本的次要伺服器會接手 HA 叢集的內部 IP 位址，並獨自接收及處理郵件服務請求。在此情況下，當您開啟次要伺服器上的 MailPlus Server 時，會跳出郵件系統警示視窗，且無法變更 MailPlus Server 的任何設定。

請盡速修復主要伺服器。若無法修復原本的主要伺服器，請參考[移除高可用 \(HA\) 設置](#)來移除主要伺服器。移除後，MailPlus Server 將回到單一節點設置。



## 次要伺服器故障

當原本的次要伺服器故障，原本的主要伺服器會繼續持有 HA 叢集的內部 IP 位址，並獨自接收及處理郵件服務請求。請盡速修復次要伺服器。若無法修復原本的次要伺服器，請參考[移除高可用 \(HA\) 設置](#)來移除次要伺服器。移除後，MailPlus Server 將回到單一節點設置。

## 備份及還原信件

您可以透過 DSM 的備份功能來備份 MailPlus Server。MailPlus Server 備份包含：

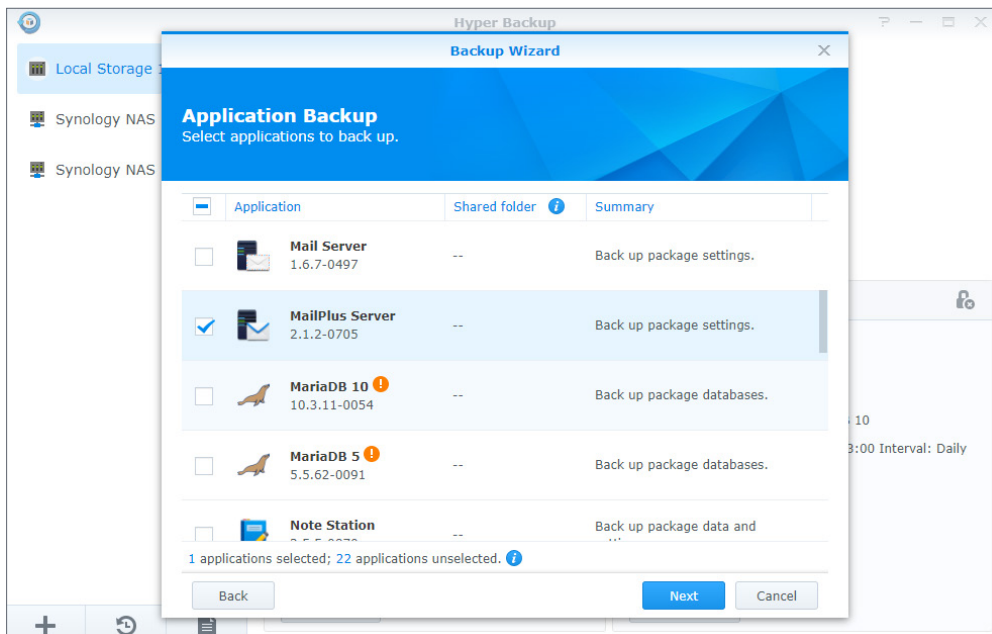
- 系統設定備份
- 郵件匣與電子郵件備份

通常 MailPlus Server 的系統設定較少更動，因此建議您使用 **Hyper Backup** 進行排程備份任務；但郵件系統中的郵件匣與電子郵件會不斷變動，使用排程備份可能會因時間間隔而造成資料遺失，因此建議您透過**共用資料夾**同步的方式備份。

## 備份系統設定

使用 Hyper Backup 套件，即可將郵件系統設定備份至與 MailPlus 相容的 Synology NAS。

1. 在來源 Synology NAS 上開啟 **Hyper Backup**。
2. 按一下左下角的加號圖示 (+) 來新增資料備份任務。
3. 選擇備份目的地類型：
  - **本地資料夾及 USB**：設定將會備份到本地 Synology NAS，或是外接的 USB / SD 儲存裝置。
  - **遠端 NAS 裝置**：須先於該遠端目的地安裝並執行 Hyper Backup Vault 套件。
4. 編輯任務設定，請參考[此篇說明文章](#)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. 備份任務設定完成後，下列 MailPlus Server 頁籤內的設定將會被備份：

- 網域
- 郵件傳送
- 服務
- 安全性
- 稽核
- 授權
- 帳號

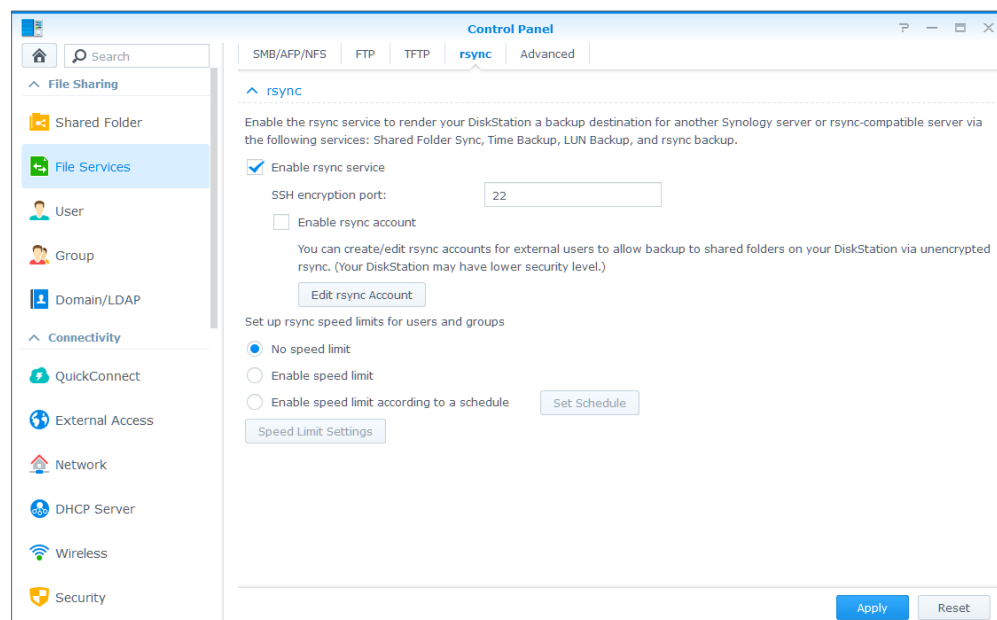
## 郵件匣與電子郵件備份

請參閱以下段落來透過同步任務將整個郵件匣與所有郵件備份至與 MailPlus 相容的 Synology NAS。

### 啟用共用資料夾同步

您必須在目的地 Synology NAS 上啟用共用資料夾同步。

1. 登入 DSM。
2. 前往控制台 > 檔案服務 > rsync。
3. 勾選啟用 rsync 服務核取方塊以啟用共用資料夾同步。



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. 選擇欲同步的共用資料夾。
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 傳輸加密所使用的連接埠。
  - **啟用 SSH 傳輸加密**：傳輸資料時加密資料。此選項能確保較高的安全性，但非加密傳輸的效能較佳。
  - **啟用傳輸壓縮**：傳輸資料時壓縮資料。此選項能節省頻寬用量，但會增加 CPU 工作量。
  - **啟用段落分塊 (block-level) 同步化**：僅同步資料變更的部分，而非整個檔案。此選項能節省頻寬用量，但會增加 CPU 工作量。
6. 依提示選擇下列任一選項，決定何時要從來源端同步至目的地：
  - **資料異動時自動進行同步**：來源共用資料夾內的資料有改動時立即同步。
  - **手動執行同步化**：在您按下按鈕時從來源共用資料夾同步。
  - **進階排程**：依據您設定的排程來同步。按一下**設定排程**以指定何時執行同步任務。
7. 按一下**套用**。現在，您可以在**任務清單**上看到同步任務，系統會根據指定的排程自動執行任務。

### 管理同步任務

登入來源 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，便可執行下列操作：
  - 按一下**編輯**按鈕來編輯任務。
  - 按一下**刪除**按鈕來刪除任務。
  - 若同步任務尚未進行，請按一下**立即同步**按鈕來立刻執行任務。
  - 若同步任務正在進行，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**，待第一次同步任務完成後，僅會同步修改的部分，但您仍可按一下**完整同步**按鈕來手動重新同步所有資料。



**注意：**

- 若同步任務的排程設定為**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，若同步任務涵蓋的任何共用資料夾內容更動，共用資料夾同步功能會繼續進行任務。
- 請勿使用 Synology Drive、Cloud Station Server、Cloud Sync 進行備份，其同步功能可能會導致資料損毀。
- 若目的地上已存在 **MailPlus** 共用資料夾，備份完成後，該資料夾將重新命名為 **MailPlus\_1**。
- 若要使用 **MailPlus\_1** 內的資料，請手動將資料移至 **MailPlus** 共用資料夾。
- 為避免帳號錯誤，請將目的地連接到來源端使用的目錄伺服器（例如：LDAP 伺服器或 Windows Active Directory 網域）。

## 還原系統設定、郵件匣、電子郵件

當目的地 Synology NAS 的本地共用資料夾內已存有系統設定、郵件匣、電子郵件，您便可以參考以下步驟來還原系統設定、郵件匣、電子郵件：

1. 開始進行前，請先於要還原的 Synology NAS 上執行以下操作：
  - 在套件中心停用 Synology MailPlus Server 及 Synology MailPlus。
  - 重新命名「MailPlus」共用資料夾，避免因資料夾同名而導致錯誤。
2. 開啟 **Hyper Backup**。
3. 從本地共用資料夾還原備份的設定，請參考[此篇說明文章](#)來取得更多資訊。
4. 還原完成後，目前的 MailPlus Server 設定皆會被覆寫。
5. 備份的郵件匣及電子郵件可立即使用，不須進行還原。

**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。

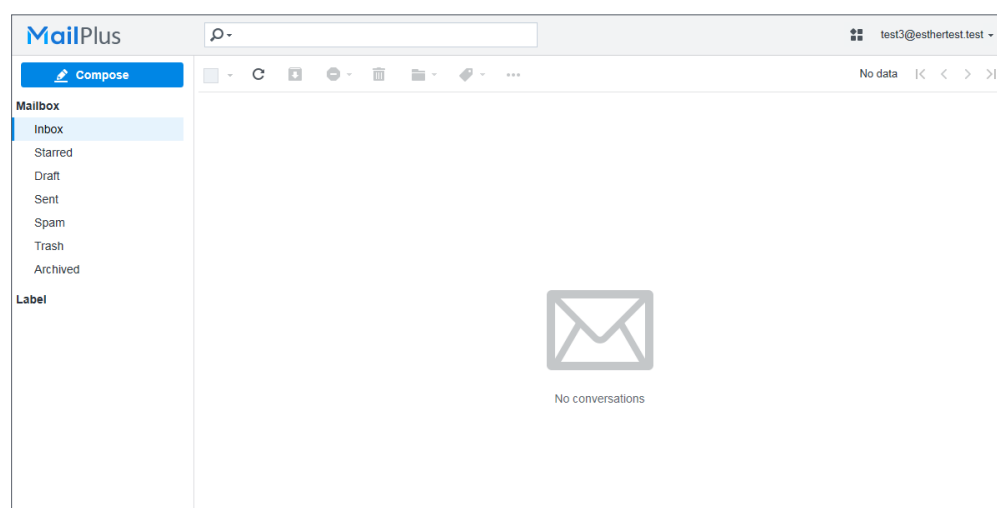
## 第 12 章：MailPlus 導覽

MailPlus 為用戶端提供易於使用的網頁版郵件服務，方便您檢視、管理、傳送訊息。若需要設定 MailPlus 的詳細說明，請參考[設定 MailPlus 用戶端](#)段落。

此章節會引導您設定 MailPlus 並提供介面導覽。若要了解詳細步驟，請參閱[此篇說明文章](#)。

### 基本操作

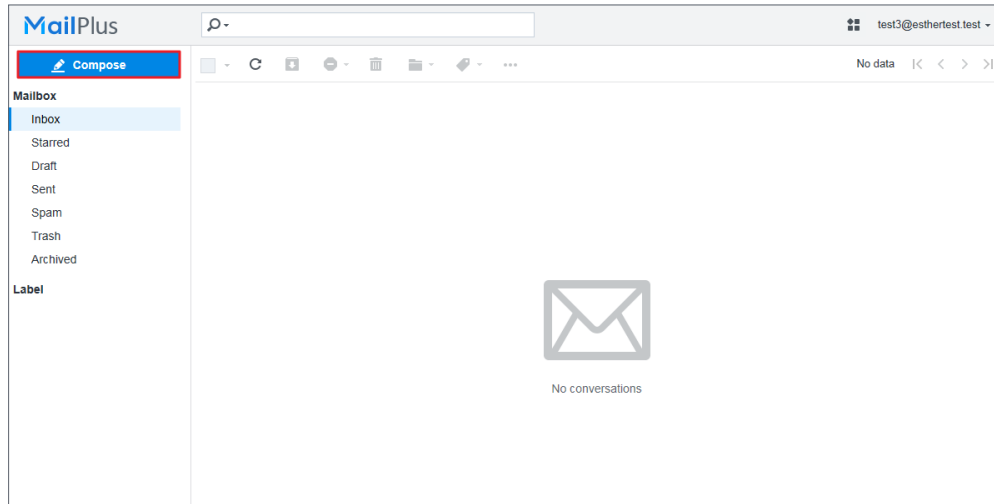
系統預設您會在登入後看見郵件匣。



## 存取並管理信件

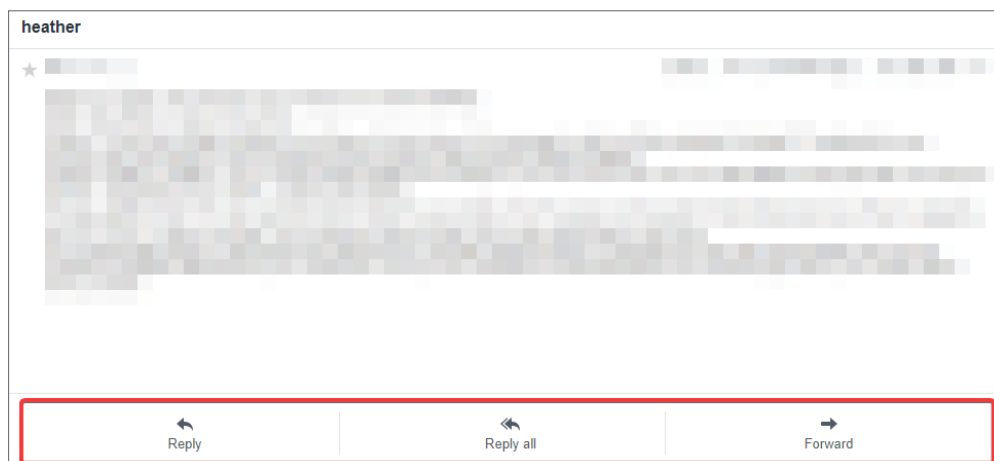
您可以在郵件匣執行以下動作：

- **撰寫郵件**：按一下左上角的**撰寫**按鈕來編寫信件草稿。MailPlus 會自動儲存郵件草稿，因此您可以隨時關閉**撰寫**視窗，只要前往**草稿**郵件匣開啟該草稿，便可從上次中斷的地方繼續撰寫。



- **回覆信件**：MailPlus 支援三種回信方式：

- **回覆**：按一下**回覆**來回信給寄件者。
- **回覆所有人**：按一下**回覆所有人**，即可一次回覆所有收件人 (包含副本收件人)。
- **轉寄**：按一下**轉寄**來回信給原始收件人之外的人。



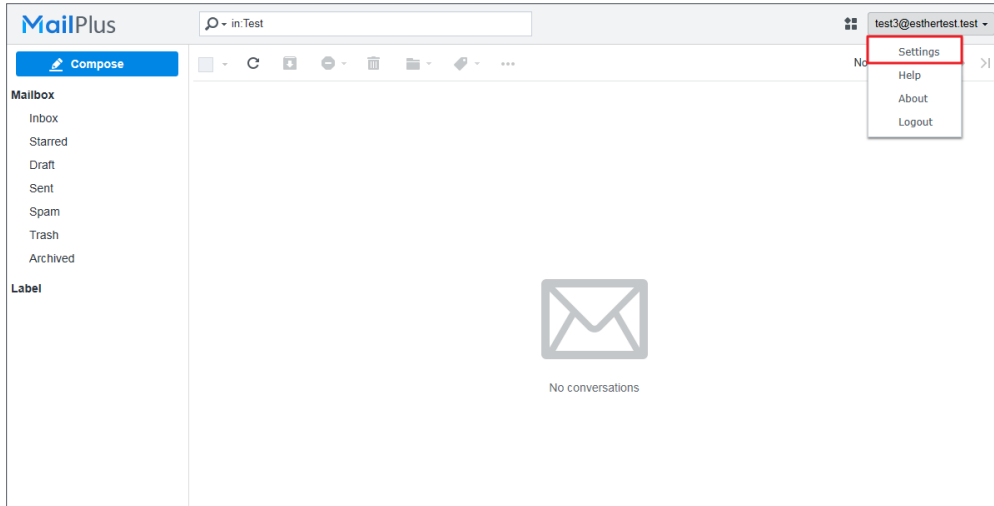
- **以郵件匣組織信件**：您可依個人需求新增多個郵件匣。將游標移動到左上角的**郵件匣**，旁邊即會出現加號圖示 (+)，按一下加號圖示 (+) 來新增郵件匣。
- **以標籤管理信件**：您可以自訂標籤以分類郵件。將游標移動到左側面板的**標籤**，旁邊即會出現加號圖示 (+)，按一下加號圖示 (+) 來新增標籤。請選擇上層標籤、輸入名稱，並選擇標籤顏色以方便辨識。

## 進階設定

MailPlus 用戶端使用者可以自訂網頁版郵件介面、自動回覆及轉寄訊息、郵件匣設定、甚至是郵件傳送時使用的協定 (例如：SMTP 及 OpenPGP)；Synology MailPlus Server 中的 MailPlus 管理員則能管理套用至所有使用者的一般設定。可在應用程式啟動器中找到 **Contacts** 及其相關設定。

本章節將引導您設定 **SMTP**、**OpenPGP**、**黑 / 白名單**。若您需要其他設定的詳細說明，請參閱 [此篇說明文章](#)。

按一下左上角的帳戶名稱，並從下拉式選單中選擇**設定**來開始設定您的 MailPlus。



## 新增 SMTP 伺服器

MailPlus 支援使用多個 SMTP 伺服器作為郵件傳送之用，若沒有新增其他的 SMTP 伺服器，MailPlus Server 便會成為預設 SMTP 伺服器，用以寄送所有信件。該伺服器除了**寄件人名稱**外，無法編輯任何設定。

使用者可以新增其他 SMTP 伺服器來在 MailPlus 上寄送電子郵件。舉例來說，您可以在 MailPlus 上新增 Google SMTP 伺服器來透過您的 Google 帳號寄送電子郵件。請依照下列步驟新增 SMTP 伺服器：

1. 前往**設定 > SMTP**。

2. 輸入以下資訊：

- **SMTP 伺服器**：請參閱郵件服務提供者的教學文章或說明文章來取得 SMTP 伺服器。
- **SMTP 連接埠**：連接埠編號將會自動更新為使用 SSL / TLS 加密 SMTP 連線的所需編號。使用 SSL 加密的 SMTP 連線預設連接埠編號為 465；而使用 TLS 加密的 SMTP 連線預設連接埠編號為 587。若未勾選 SSL 及 TLS 安全連線的任一核取方塊，用於 SMTP 連線的標準連接埠編號為 25。
- **需要驗證**：若您所使用的 SMTP 伺服器需要身分驗證，請勾選此核取方塊。
  - **使用者帳號**：輸入您的電子郵件地址。
  - **密碼**：輸入您的電子郵件密碼。
- **需要安全連線 (TLS)**：勾選核取方塊來使用 TLS 加密增加連線安全性。

- **需要安全連線 (SSL)：**勾選核取方塊來使用 SSL 加密增加連線安全性。
- **寄件人信箱：**輸入您的電子郵件地址。請注意，若與上方輸入的**使用者帳號**不同，您的電子郵件可能會被視為垃圾郵件。
- **寄件人名稱：**輸入寄件人名稱以方便收件人辨識您的身分。

**Create**

SMTP server:

SMTP port:

Authentication required

Username:

Password:

Secure connection (TLS) required

Secure connection (SSL) required

Sender email:

Sender name:

3. 按一下**確定**以儲存設定。

4. 現在，應可以在清單上看到方才新增的 SMTP 伺服器帳號。

- 您可以透過上方工具列的按鈕來編輯或是刪除伺服器，或是將其設為預設 SMTP 伺服器。

**Settings**

General  
Theme Customization  
Auto Reply/Forward  
Mailbox  
Shared Mailbox  
Filter  
Priority Mailbox  
**SMTP**  
OpenPGP  
Notification  
Blacklist/Whitelist

Add Edit Delete Default

| Sender email | Default SMTP server |
|--------------|---------------------|
| ...com       | Default             |
| ...gmail.com |                     |

- 撰寫郵件時，您可以在寄件者欄位切換 SMTP 伺服器。

**Compose**

To: Recipients Cc Bcc

From: heatherfang <...@gmail.com>

Subject: heatherfang <...@gmail.com>

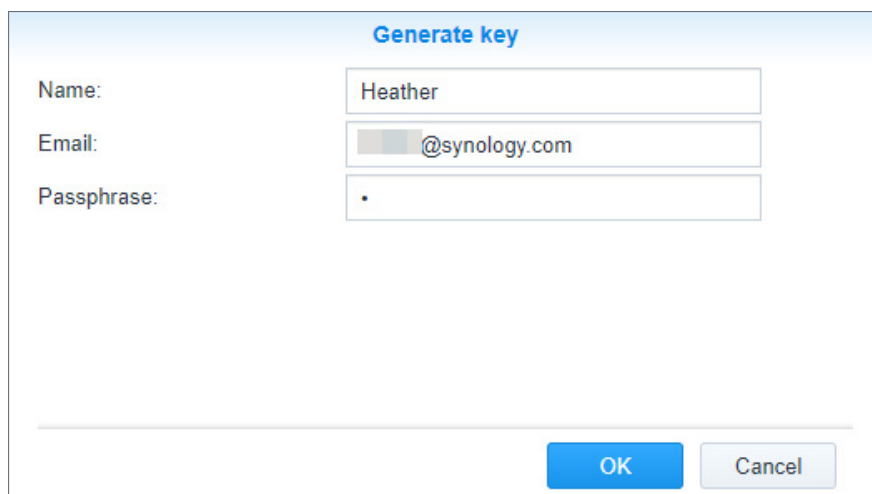
Heather <...@gmail.com>

## 使用 OpenPGP 加密信件

OpenPGP (Pretty Good Privacy) 為用於電子郵件加密的金鑰加密技術。郵件經 OpenPGP 加密後，僅目標收件者可以存取郵件內容，以避免機密郵件與傳輸資料外洩。

### 生成 OpenPGP 金鑰

1. 勾選啟用 OpenPGP，再按一下**金鑰管理**按鈕。
2. 按一下**產生**來生成新的 OpenPGP 金鑰。
  - **Name**：輸入欲使用的名稱。
  - **電子郵件**：輸入您的 MailPlus 帳號。
  - **通行碼**：輸入用來加密及解密私密金鑰的密碼。



The screenshot shows a dialog box titled "Generate key". It contains three input fields: "Name" with the text "Heather", "Email" with the text "@synology.com", and "Passphrase" with a single dot. At the bottom right of the dialog are two buttons: "OK" and "Cancel".

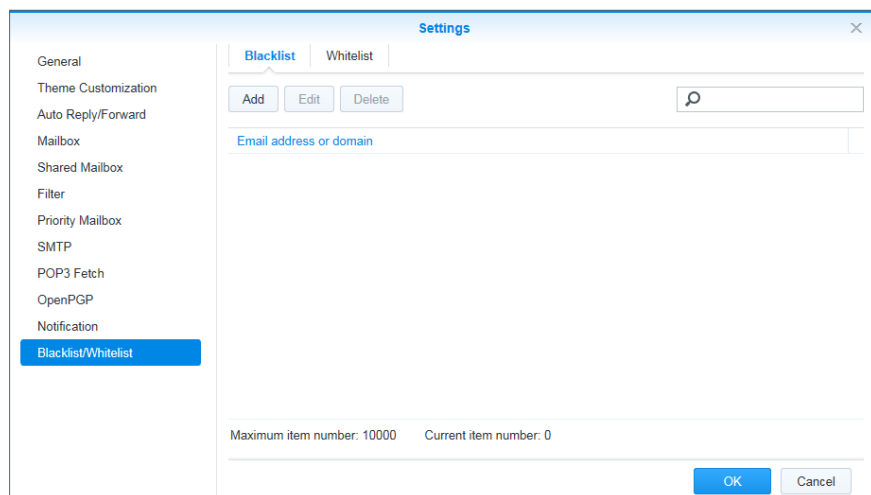
3. 按一下**確定**來生成一組公開金鑰與私密金鑰。

### 管理 OpenPGP 金鑰

- **公開金鑰**：按一下**匯出**來下載公開金鑰，並將其給予需要寄加密郵件給您的寄件方。
- **私密金鑰**：私密金鑰是用來解密寄給您的加密郵件，請儲存在安全的地方。
- 若您有寄加密郵件給他人的需求，請按一下**匯入**按鈕，即可從檔案或文字輸入來匯入他人的公開金鑰。

### 管理黑 / 白名單。

您可以在**黑 / 白名單**頁面建立個人的黑名單和白名單，以封鎖或允許特定電子郵件地址 / 網域。您可以將持續寄送垃圾郵件的電子郵件地址或網域加入**黑名單**以封鎖；若發現有合法郵件被封鎖，則可將該電子郵件地址或網域加入**白名單**。



### 新增電子郵件地址或網域名稱

1. 按一下新增按鈕以將新項目加入您的黑 / 白名單。
2. 輸入電子郵件地址或網域名稱，再按一下**確定**以儲存設定。
3. 現在，應可以在清單上看到方才新增的電子郵件地址或網域名稱。

### 刪除現存電子郵件地址或網域名稱

1. 按一下您想移除的電子郵件地址或網域名稱，再按一下**刪除**。
2. 按一下**是**來確認，或**否**來取消。

### 編輯現存電子郵件地址或網域名稱

1. 按一下您想編輯的電子郵件地址或網域名稱，再按一下**編輯**。
2. 進行變更，再按一下**確定**。
3. 現在，該電子郵件地址或網域名稱已從清單移除。



SYNOLOGY  
INC.

新北市板橋區  
遠東路 1 號 9 樓  
台灣  
電話 : +886 2 2955 1814

SYNOLOGY  
AMERICA CORP.

3535 Factoria Blvd SE, Suite #200,  
Bellevue, WA 98006  
USA  
電話 : +1 425 818 1587

SYNOLOGY  
UK LTD.

Unit 5 Danbury Court, Linford Wood,  
Milton Keynes, MK14 6PL  
United Kingdom  
電話 : +44 (0)1908048029

SYNOLOGY  
FRANCE

102 Terrasse Boieldieu (TOUR W)  
92800 Puteaux  
France  
電話 : +33 147 176288

SYNOLOGY  
GMBH

Grafenberger Allee 295  
40237 Düsseldorf  
Deutschland  
電話 : +49 211 9666 9666

SYNOLOGY  
SHANGHAI

200070 中國上海市  
靜安區天目西路 511 號輔  
房 201 室  
中國

SYNOLOGY  
JAPAN CO., LTD.

4F, No. 3-1-2, Higashikanda,  
Chiyoda-ku, Tokyo, 101-0031  
Japan

Synology®



[synology.com](https://synology.com)

Synology 可能隨時修改產品規格與說明，恕不另行通知。Copyright © 2020 Synology Inc. 保留一切權利。®  
Synology 及其他群暉科技股份有限公司 (Synology Inc.) 所有產品之名稱，均為群暉科技股份有限公司所使用或註冊  
之商標或標章。本軟體產品所提及之產品及公司名稱可能為其他公司所有之商標。