

Administrator's Guide for Synology MailPlus Server

—
Based on

Synology MailPlus Server 2.2



Table of Contents

Introduction	01
Chapter 1: Deployment Guidelines	02
Select a Synology NAS	
Estimate RAM and Storage Requirements	
Running Multiple I/O Intensive Packages on the Same NAS	
Chapter 2: Getting Started with MailPlus Server	06
Connect Synology NAS to the Internet	
Set up DNS	
Set up MailPlus Server	
Set up MailPlus Client	
Run MailPlus	
Third-Party Email Clients	
Troubleshoot	
Chapter 3: Mail Migration	19
Create a Mail Migration Task in MailPlus Server	
Import System Configurations from Microsoft Exchange to MailPlus Server	
Chapter 4: User Licenses	27
Purchase Licenses	
Install Licenses	
Use Licenses	
Chapter 5: Account Settings	31
Account System	
Activate Accounts	
Manage Privileges	

Chapter 6: Protocol Settings	46
SMTP	
MAP/POP3	
Network Interface	
 Chapter 7: SMTP Settings	 50
Service Settings	
SMTP Secure Connection	
Mail Relay	
 Chapter 8: Domain Settings	 66
Domain	
Domain Management	
 Chapter 9: Security Settings	 83
Spam	
Antivirus Scan	
Authentication	
Content Protection	
 Chapter 10: Monitor Settings	 107
Monitor Server Status	
Monitor Mail Queue	
Monitor Mail Log	
 Chapter 11: Disaster Recovery	 127
High-Availability Cluster	
Back up and Restore Email	
 Chapter 12: MailPlus Navigation	 140
Basic Operations	
Advanced Settings	



Introduction

The Synology MailPlus suite provides advanced and secure mail service with high usability. This suite consists of two packages: MailPlus Server and MailPlus. MailPlus Server is an administration console that offers diverse settings, while MailPlus is an email platform for client users.

This administrator's guide will guide you through the MailPlus Server setup and give detailed configuration instructions including DNS settings, mail service migration, and other security adjustments. In addition, the following key features are also contained in this guide to help you achieve the best practices: MailPlus high-availability for stable and continuous mail service, the mail queue for deferred message management, and the monitoring console displaying an overview of the MailPlus health status.

Chapter 1: Deployment Guidelines

This chapter is a guide on best practices to follow when deploying MailPlus to ensure the stability and performance of mail services. The following is discussed below: how to select a Synology NAS suitable for MailPlus, how to estimate RAM and storage requirements, what to consider when utilizing SSD cache, and advice on the running of multiple I/O intensive packages alongside MailPlus on the same NAS.

Select a Synology NAS

Synology offers a variety of NAS in different form factors, functions, and capabilities. Not all of them are suitable for MailPlus Server. To help you choose a Synology NAS that meets your requirements, please see below:

1. View a list of supported devices on [the MailPlus licensing page](#) sorted by the maximum number of concurrent users and maximum server performance.
 - **Maximum number of concurrent users** refers to the recommended maximum number of MailPlus users.
 - **Maximum server performance** refers to the maximum number of emails that MailPlus Server can process per day.
2. Visit [Synology product page](#) to find a list of every model that supports MailPlus. By clicking on the desired model, you can view more details about its specifications.

Note:

- Figures are based on laboratory testing done internally by Synology. The test environment is listed as follows:
 - The CPU and RAM usage were both under 80% when testing the maximum number of concurrent users.
 - For models tested with expandable memory, the maximum amount of RAM was installed.
 - Models with 2 bays and dual M.2 drive slots were installed with two SSDs for SSD cache.
 - Models with more than 4 bays were installed with two SSDs for SSD cache.
 - FS series were installed with 12 SSDs in RAID F1 configuration.
 - The performance of the mail system will slightly decrease in high-availability mode due to data synchronization between the two servers.
 - Functions that were enabled in all of the tests above: anti-spam, anti-virus, DNSBL, greylist, content scan, full-text search (English only).
- Actual limitations may differ according to your system configuration. To achieve the same performance, please consider installing SSDs and expanding RAM.

Estimate RAM and Storage Requirements

Based on the multiple factors that will affect a NAS's memory usage, the recommended memory sizes based on the number of users are:

- for < 250 users: minimum of 8 GB RAM
- for 250 - 500 users: minimum of 16 GB RAM
- for 500 - 1000 users: minimum of 32 GB RAM
- for > 1,000 users: minimum of 64 GB RAM

Estimating RAM usage

The amount of memory used is mainly dependent on the number of mail service users. However, please take into consideration that the following services may also use high amounts of memory:

- **Anti-spam:** The default MailPlus anti-spam engine, Rspamd, can be memory intensive.
- **Antivirus:** Antivirus services such as ClamAV and McAfee can be memory intensive, especially when updating their offline virus database to the latest versions.
- **MailPlus web client:** MailPlus Server may simultaneously receive multiple requests from web clients when they are reading emails and saving email drafts. If the number of users exceeds the **Maximum Number of Concurrent Users** as specified by the specifications of the model of Synology NAS, sudden spikes in memory usage may occur as MailPlus Server tries to handle all client requests.

Estimating volume size requirements

Use the following formula to estimate the storage size requirements for MailPlus:

- Estimated storage size = [(the average number of incoming and outgoing emails per day)*(the average size of emails)*(the number of users)*(days)]

The average email size of an email is 300 KB, the average number of emails sent and received by a single person is 100 per day, and a mail service usually lasts for three to five years.

For example, if your MailPlus supports 200 users, the required storage size is:

100 (the average number of incoming and outgoing emails per day)*300 KB (the average size of an email)*200 (the number of users)*1095 (the number of days in three years) = 6.12 TB

If you have a problem estimating the required storage size, please [contact us](#) for custom suggestions.

Utilizing SSD Cache

SSD cache is a way of improving system performance by temporarily storing frequently accessed data (also known as hot data) on part of, or the entirety of, an SSD.

MailPlus involves frequently reading and writing messages, which would require small files being randomly read and written to the drive. Since the average email size is relatively small, the increase in read/write speed can be considerable when they are (or even partially) stored on an SSD cache. Installing an additional SSD and utilizing Synology SSD cache will enhance the overall performance of the mail service.

Note:

- It is essential that enterprise users utilize SSD cache for best performance.
- For optimal performance, it is strongly suggested to use an FS series NAS and create the volume with all SSDs.

Recommended size of SSD cache

SSDs are designed for different purposes, and you should take into consideration the following when selecting a suitable SSD to use in your system: endurance, consistent performance, and power loss protection.

Synology SSDs are enterprise-class SSDs that are built for 24/7 NAS environments and are verified through rigorous validation to be interoperable with Synology systems. Intensive tests, which include I/O stress, power cycling, and temperature trials, ensure that Synology SSDs can provide both reliability and consistent performance suitable for enterprise environments - especially for something as crucial as your mail server.

In addition to Synology SSDs, Synology has tested and verified several other [third-party SSDs](#). Depending on the manufacturer, an SSD's performance may vary widely.

To learn more about choosing an appropriate SSD for your SSD cache, please see [this article](#).

Recommended size of SSD cache

The actual size of the SSD cache depends on the amount of hot data of the volume. At least two SSDs are required to form a RAID 1/5/6/10 redundant drive to make use of a read-write cache. For example, if you want to create a 480 GB read-write cache, at least two identical 480 GB SSDs are required.

Hot data will be cached within the SSD; for MailPlus Server, hot data will consist mainly of recently-accessed emails that have a high probability of being frequently accessed. Hot data usually accounts for three to six percent of the total storage space used for mail services.

- For example, the hot data size on a 1 TB mail storage space is likely to be: $1,024 \text{ GB} \times 6\% = 61.4 \text{ GB}$

Introduction

However, SSD cache should have a larger capacity than the actual hot data size in order to ensure performance. We recommend that the actual size of the SSD cache be double the size of estimated hot data.

- Continuing with the above example, the ideal cache size is: $61.4 \text{ GB} \times 2 = 122.8 \text{ GB}$.

In this case, a 480 GB SSD cache will more than meets the minimal requirements.

The following guide provides a quick SSD cache size estimation based on the number of users:

- For < 500 users: $480 \text{ GB} \times 2$
- For 500 - 1,000 users: $1 \text{ TB} \times 2$
- For > 1,000 users: $2 \text{ TB} \times 2$

If you already have a Synology NAS, the hot data size and the appropriate cache size can be determined by using **SSD Cache Advisor** at **Storage Manager**.

Note:

- For more information on SSD cache, please refer to the following articles and documents:
 - [SSD Cache help article](#)
 - [Frequently asked questions about using Synology SSD cache](#)
 - [White paper: Using Synology SSD Technology to Enhance System Performance](#)
- SSD cache is recommended as a way to speed up email processing even if the number of MailPlus users does not reach the **Maximum Number of Concurrent Users** as specified in the model's specifications.

Running Multiple I/O Intensive Packages on the Same NAS

To ensure performance and data security, as a best practice, I/O intensive packages such as MailPlus Server, Synology Drive Server, and Synology Chat Server should not be installed on the same Synology NAS. As all of the above consume high I/O resources, system errors can easily result owing to resource competition between the different services. However, if the packages are not all I/O intensive services, a Synology NAS is capable of running multiple services at the same time. For example, MailPlus Server and Synology Drive should not be installed on the same NAS, but Synology Calendar can be run together with MailPlus as they are not I/O intensive services.

Chapter 2: Getting Started with MailPlus Server

With MailPlus Server, a Synology NAS can serve as a mail system that supports SMTP, POP3, and IMAP. User accounts and email messages can be centrally managed and archived on a Synology NAS. MailPlus, as a client package, provides mail service users with an easy-to-use and browser-based email platform for viewing, managing, and sending messages.

This chapter will help you get started with MailPlus Server and MailPlus.

Connect Synology NAS to the Internet

There are three ways to connect a Synology NAS to the Internet: direct connection, PPPoE connection, or connection through a router. For detailed instructions on how to access a Synology NAS via the Internet, you can refer to [this tutorial](#).

Having an external static IP address is crucial for a mail system. Although it is possible to run a mail system with a dynamic IP address, it is not as reliable as using a static one. We recommend registering an external static IP address for the mail system. For more information, please contact your Internet service provider (ISP).

Configuring static IP/PPPoE

There are two ways to set up external static IP addresses on Synology NAS:

- **PPPoE:** Some Internet service providers (ISP) provide free static IP addresses; however, users must connect via PPPoE to retrieve a static IP address.
 1. Sign in to DSM.
 2. Go to **Control Panel > Network**.
 3. At the **Network Interface** tab, select **PPPoE** and click the **Edit** button.
 4. Set up the modem and network port.
 5. Enter the username and password provided by your Internet service provider (ISP).
- **Static IP address:** If you already have a static IP address, you can enter it in Synology NAS.
 1. Sign in to DSM.
 2. Go to **Control Panel > Network**.
 3. At the **Network Interface** tab, select a network port and click the **Edit** button.
 4. Enter your static IP address.

Set up DNS

A valid and registered domain name is required to allow clients to deliver emails to MailPlus Server over the Internet. An email address has two parts. The part before @ is a username, and the one after @ indicates a domain name. For example, Alex's email address is "alex@example.com". His domain name is "example.com". To make sure an email address like "alex@example.com" works, you'll need to set up the MX record and A record to help emails reach MailPlus Server. You can configure these records on the DNS server of your domain providers.

MX record

MX record, or Mail Exchanger record specifies how the Internet should route your emails using Simple Mail Transfer Protocol (SMTP). Each MX record contains a hostname and a preference. A hostname guides emails to arrive at the right mail server. A preference points out the priority of multiple servers. The lower the preference number is, the higher the priority will be.

You can set up multiple MX records for a domain with multiple mail servers and assign each record a preference number. The primary server should have the lowest number, like zero, to ensure that this mail server responds to requests at first. When there is no response from the primary server, the Internet will try the other mail servers used for failover sequentially according to their preference numbers until one of them gives a response.

For example: if the email address is *alex@example.com*, you have to set up the MX record pointing to the mail server, which should receive emails on behalf of the domain *example.com*. Therefore, you should enter the domain you are editing in the **Host** field and the hostname of your MailPlus Server in the **Points to** field. The preference record that you assign to the primary server should be zero or closer to zero.

Host	Points to	Preference
example.com	mail.example.com	0

In this way, the MX lookup for *example.com* would return *mail.example.com*.

After the MX lookup finds the mail server, the Internet needs its IP address to locate the destination for mail delivery. That's why you need to set up A record for your mail server.

A record

A record, or Address record, points a domain or subdomain to the IP address of the host server. It allows the Internet to identify IP addresses when people use easy-to-remember domain names.

In the case of *alex@example.com*, *mail.example.com* is the subdomain of *example.com*, and the host server is the Synology NAS on which MailPlus Server is running.

From Hostname	To IP Address
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 *

example.com mail.example.com 0

TTL *
1 Hour

Save Cancel

The examples and the image are for demonstration purposes only. The DNS record interface that each provider offers may vary. If you have problems configuring DNS records, please contact your domain providers.

Reverse DNS setup

The process of assigning specific DNS records to a domain name is known as **forward DNS**. This is what leads a domain name to the exact server. There is also a reverse process, known as **reverse DNS**.

What is reverse DNS?

Reverse DNS refers to translating numeric addresses of a website (i.e., the IP address) to the domain/hostname, as opposed to the forward DNS process which translates a domain or hostname to an IP address. Reverse DNS also refers to locating which domain name/host belongs to a given IP address; that is why this process is often referred to as **reverse DNS lookup**. When a domain name has a valid reverse DNS, it can be accessed via an IP address.

What does reverse DNS do?

Reverse DNS is one of the basic requirements for a mail system. It is often used as a spam filter to determine whether the IP address of an incoming message matches an authenticated domain name, and to block the message if it doesn't. If you don't set up reverse DNS for your mail server, messages sent from your mail server will be blocked by most major email providers. If you cannot set up reverse DNS by yourself and keep experiencing mail delivery problems, please add another SMTP server for mail delivery. We recommend that you use a well-known SMTP server to avoid being taken as a spammer when sending emails.

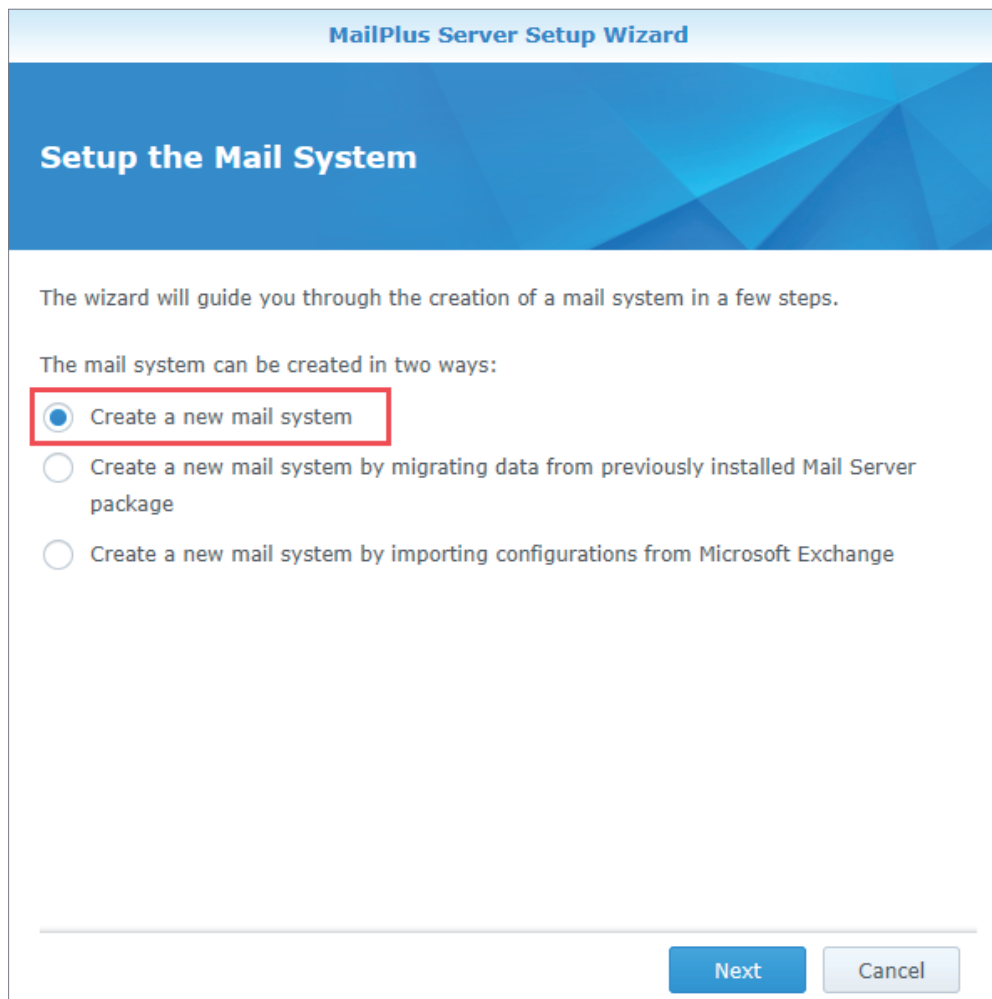
How to set up reverse DNS?

- **Set up reverse DNS on your own host:** Some ISPs may delegate a portion of the zone to users so that users can host their own reverse DNS. You can configure reverse DNS by determining PTR records in a DNS server. PTR records are managed by the entity that controls the IP address. It may be either your host or yourself if the host has delegated the reverse DNS for the IP space (containing one or multiple IP addresses) to you. A PTR record usually represents the IP entered backward, followed by an in-addr.arpa entry.
- **Set up reverse DNS with your ISP:** The ISP or entity that owns your IP address is the only one who can add appropriate PTR records. You may have to contact them for reverse DNS configurations.

Set up MailPlus Server

Once the installation is complete, you can start setting up MailPlus Server. In the section below, we will demonstrate how to configure basic SMTP (Simple Mail Transfer Protocol) settings. Please remember that the screenshots below are for reference only. Your settings may differ.

1. Go to **Package Center** to install **MailPlus Server**.
2. Launch **MailPlus Server** and select **Create a new mail system** if you want to set up a whole new mail system, and click **Next** to continue the setup. Otherwise, you can select **Create a new mail system by migrating the data from previously installed Mail Server**. Check [this tutorial](#) to see how to migrate Mail Server to MailPlus Server.



The screenshot shows the 'MailPlus Server Setup Wizard' window. The title bar says 'MailPlus Server Setup Wizard'. The main heading is 'Setup the Mail System'. Below this, it says 'The wizard will guide you through the creation of a mail system in a few steps.' and 'The mail system can be created in two ways:'. There are three radio button options: 'Create a new mail system' (which is selected and highlighted with a red rectangle), 'Create a new mail system by migrating data from previously installed Mail Server package', and 'Create a new mail system by importing configurations from Microsoft Exchange'. At the bottom right, there are 'Next' and 'Cancel' buttons.

3. Enter your domain name and hostname (FQDN):
 - **Domain name:** A domain name is a location or an address where email messages are received. Please check if the domain name matches the MX record in DNS settings.
 - **Hostname (FQDN):** A hostname is the address of your MailPlus Server. Please check if the hostname matches the A record in DNS settings.

MailPlus Server Setup Wizard

Configure basic SMTP settings

Account type:

Local users

Network Interface:

LAN 1 (192.168.1.102)

Domain name:

yourdomainname.synology.me

Hostname (FQDN):

mail.yourdomainname.synology.me

Volume:

Volume 1

Back

Next

Cancel

4. Modify the following settings according to your needs:

- **Account type:** Select a user account type (local, LDAP, or domain users) that will be allowed to use MailPlus services.
- **Network interface:** Select a LAN port used for MailPlus Server.
- **Volume:** Select a volume on which MailPlus Server and its data will be stored.

5. Click **Next** to check the setup summary and click **Apply** to finish the settings.

6. After setting up MailPlus Server, you can [Activate Accounts](#) to allow specific users to use mail service. Please note that activating more than five user accounts requires additional purchased licenses. For more information on the MailPlus license mechanism, please refer to [the MailPlus licensing page](#).

Note:

- The application privileges of MailPlus Server are granted to all users by default. Editing privilege settings at **Control Panel** can affect the functionality of MailPlus Server and therefore should be avoided. For more details, please refer to [Activate Accounts](#).
- After you set up MailPlus Server, a **MailPlus** shared folder will be automatically added to the Synology NAS. To ensure client users can access MailPlus, the permission settings of the shared folder should remain as default. We do not recommend that you edit the permissions on your own.

Set up MailPlus Client

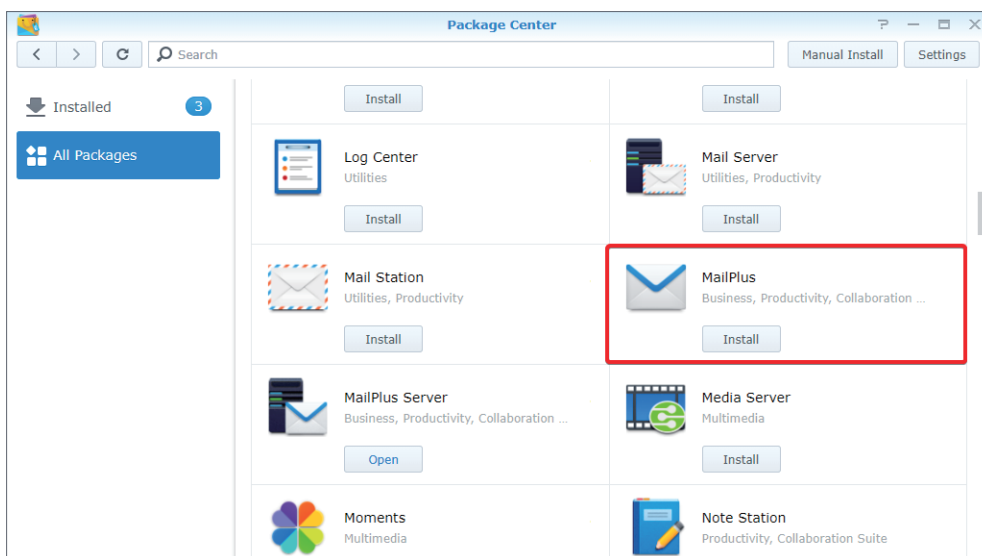
Access emails on Synology NAS with MailPlus

MailPlus is an add-on package that provides a web-based interface for client users to access and manage emails hosted on a Synology NAS.

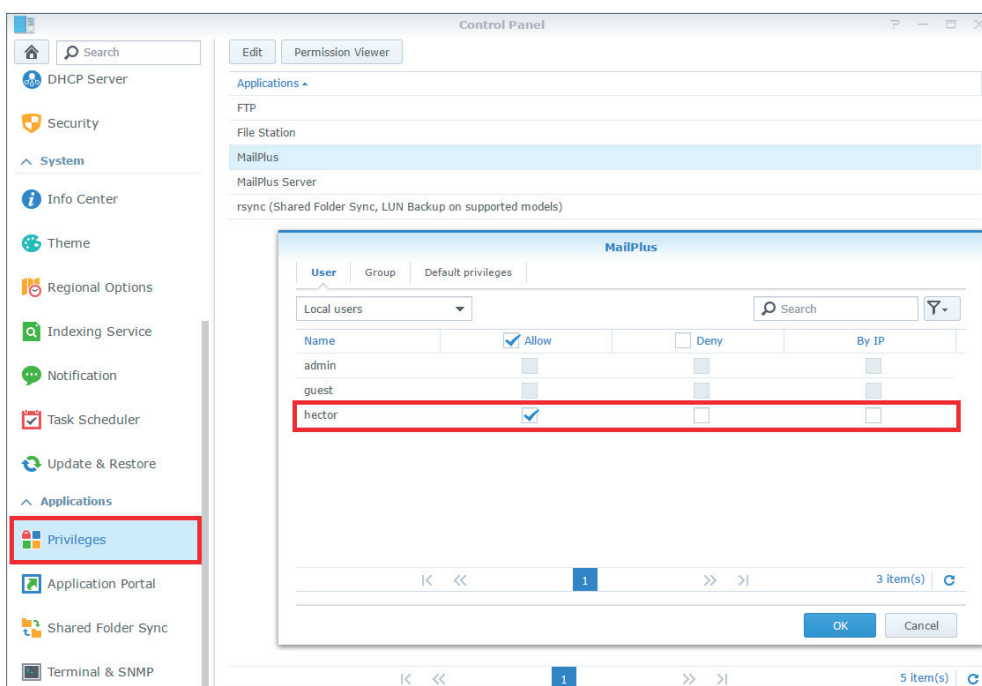
Multiple POP3 accounts can be created in MailPlus, allowing users to fetch messages via other mail service providers (e.g., Mozilla® Thunderbird®, Gmail, and Office 365).

Install MailPlus

1. Go to **Package Center** to install **MailPlus**.



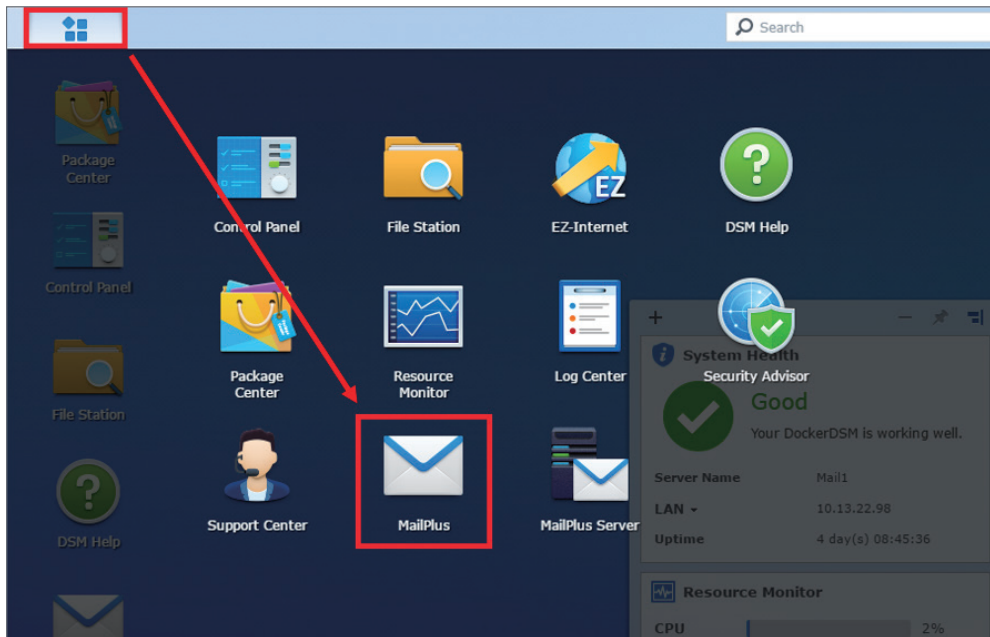
2. Go to **Control Panel > Privileges** to allow target users or groups to access **MailPlus**.



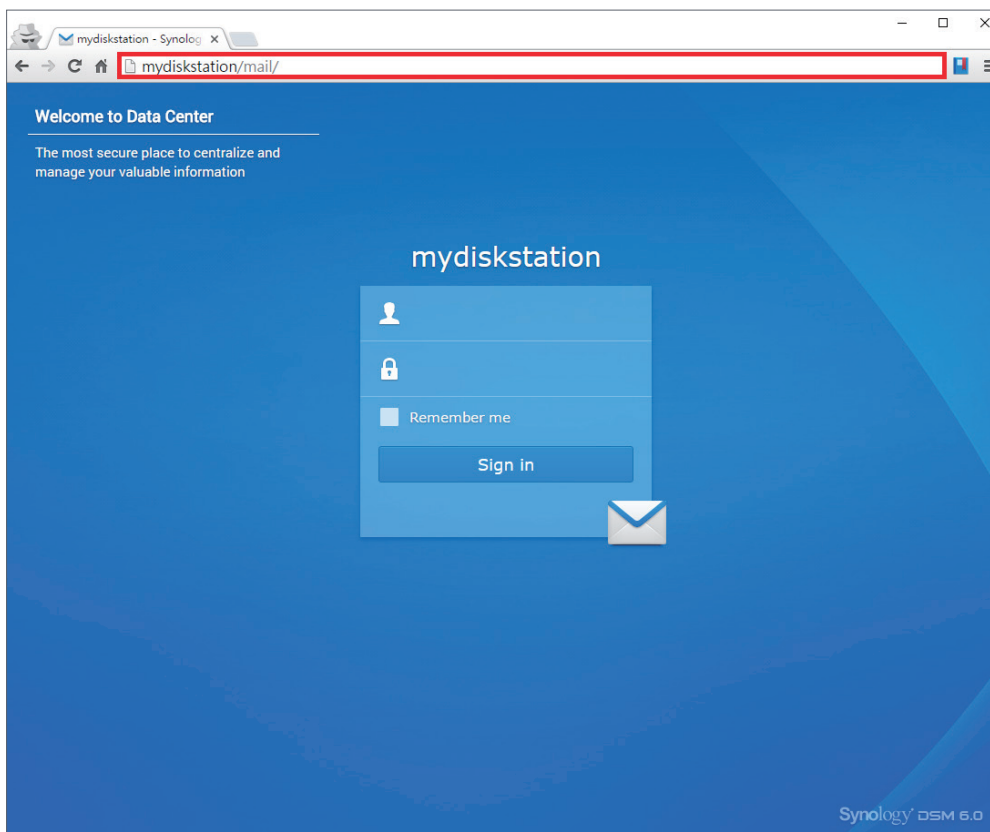
Run MailPlus

1. There are two ways to launch the MailPlus login page:

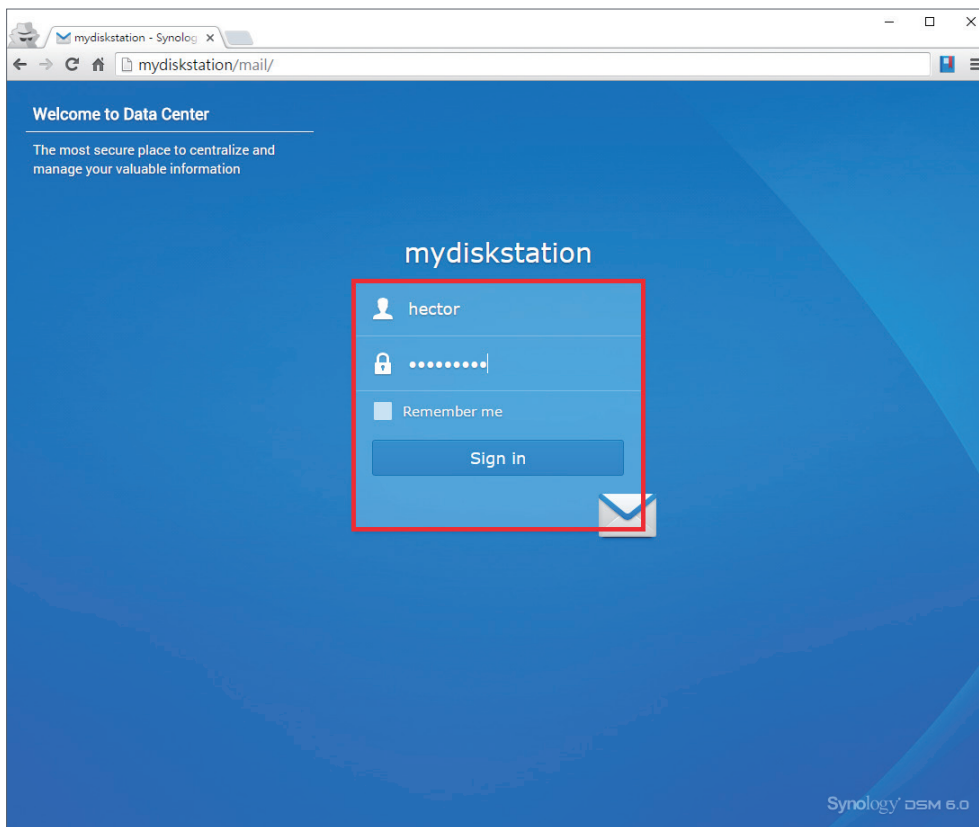
- Go to **Main Menu > MailPlus**.



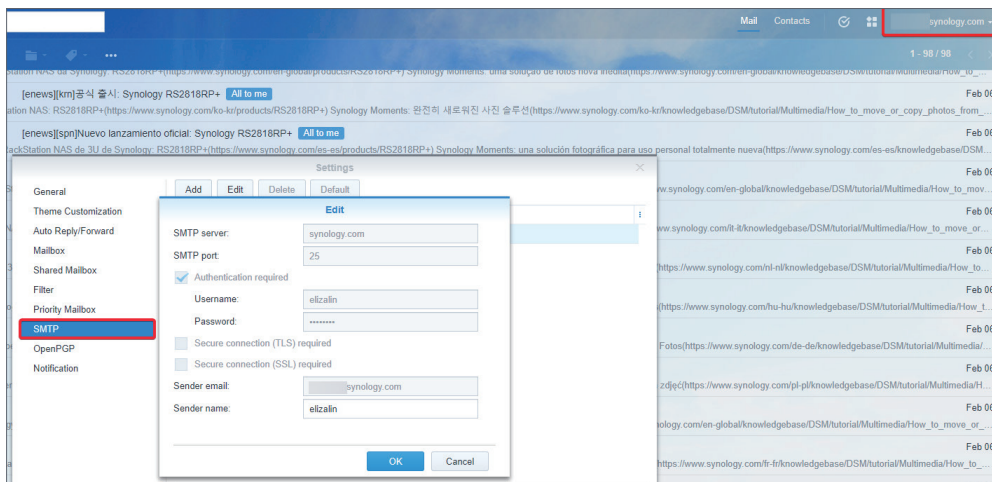
- Access MailPlus via **Application Portal**. Enter the name of the Synology NAS followed by "/mail" in the address bar of your web browser. For example, if the Synology NAS is called *mydiskstation*, enter *mydiskstation/mail*. Please refer to [this help article](#) to see how to enable **Application Portal**.



2. Enter your DSM username and password to sign in.



3. If the settings of MailPlus Server have been configured before the installation of MailPlus, the SMTP settings of MailPlus Server will automatically appear at **Settings > SMTP**.

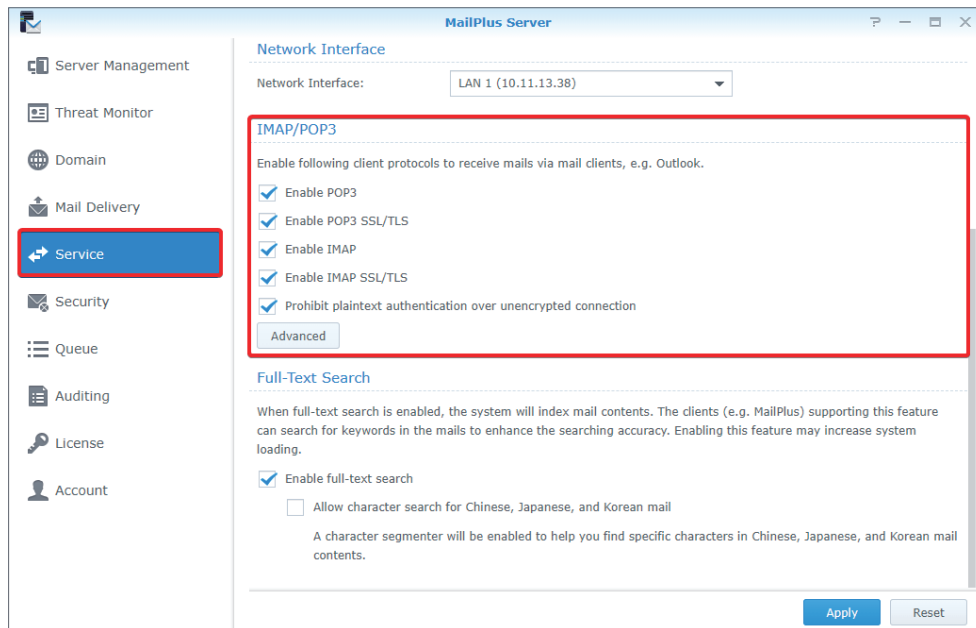


Third-Party Email Clients

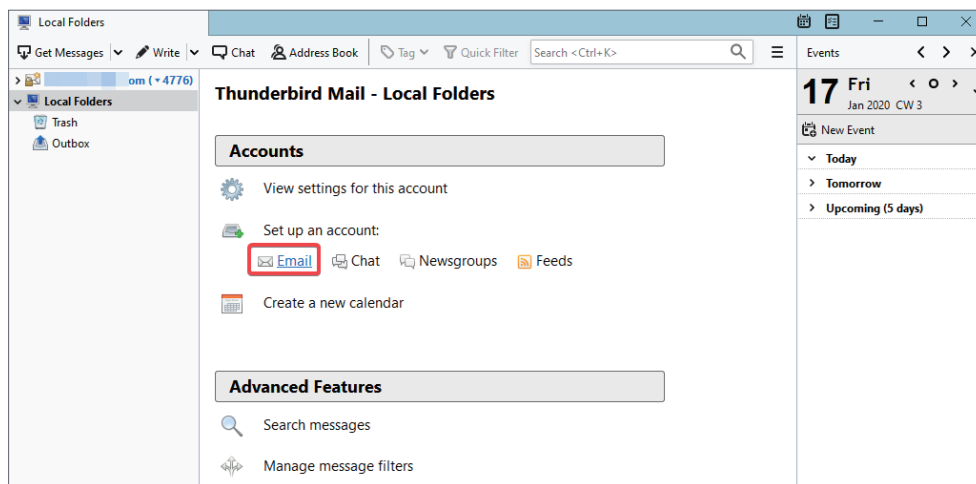
Access emails on Synology NAS with other email clients

Email accounts on a Synology NAS can be linked with various mail clients, such as Microsoft® Outlook® or Mozilla® Thunderbird®. In the example below, we'll show you how to use Thunderbird® to access an email account hosted on a Synology NAS.

1. Launch **MailPlus Server** and go to the **Service** page to enable IMAP and POP3.



2. Launch Thunderbird® on your computer and click **Email** to launch the **Set up an Existing Email Account** window.



- Enter the name, MailPlus address, and password for your DSM user account. Click **Continue**.

Set Up an Existing Email Account

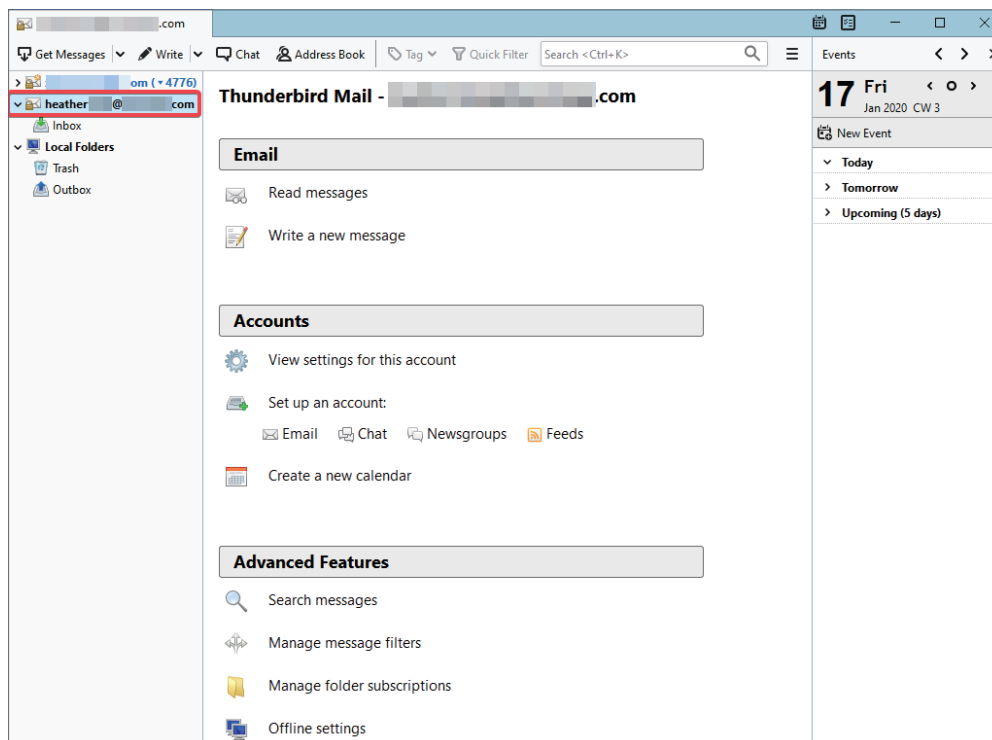
Your name: Your name, as shown to others

Email address: Your existing email address

Password: ☒ Remember password

Manual config **Continue** **Cancel**

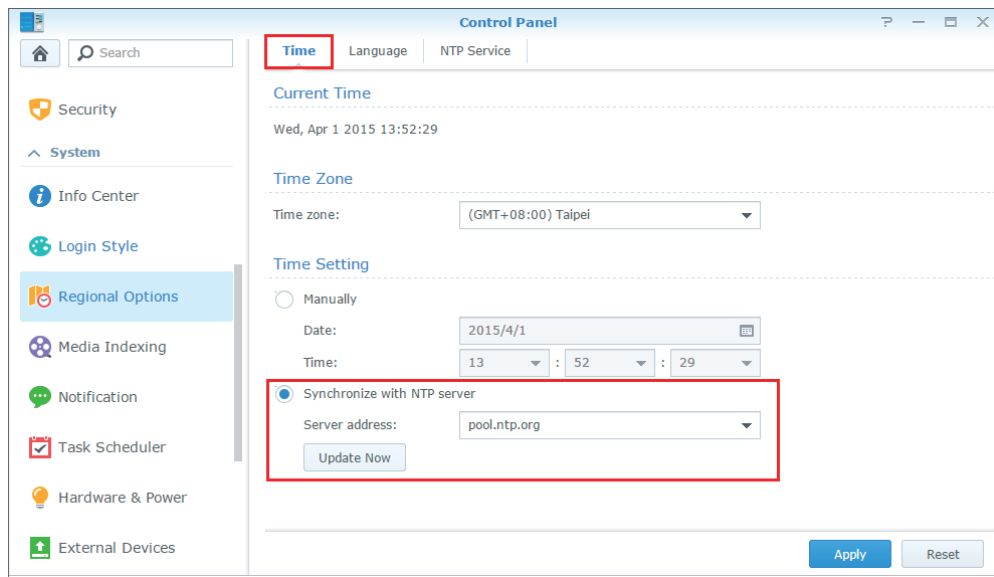
- Thunderbird® will search for your MailPlus account. If the settings are correct, click **Done** to finish the settings.
- Once the setup is complete, your MailPlus account will appear on the left panel. You can double-click the account to expand all mailboxes.



Troubleshoot

Why can't I send or receive emails via webmail from MailPlus?

1. Check if settings on your MailPlus such as SMTP, DNS, and MX are correct.
2. Check if the Internet settings of the Synology NAS are correct. Go to **Control Panel** > **Regional Options**. At the **Time** tab, tick **Synchronize with NTP server** and click the **Update Now** button to examine if the Internet settings are correct. If a result comes back successfully, the settings are correct.



3. Check if the port number on your router is correct.
4. Please visit [Spamhaus](#) to check if your IP is listed as a spammer. If so, remove your IP from the block list on the same website.

Why can't I send or receive emails via email clients?

1. Check if you have enabled IMAP and POP3.
2. Check if your username and password are correct.
3. Check if settings on your MailPlus such as SMTP, DNS, and MX are correct.
4. Check if the Internet settings of the Synology NAS are correct. Go to **Control Panel** > **Regional Options**. At the **Time** tab, tick **Synchronize with NTP server** and click on the **Update Now** button to examine if the Internet settings are correct. If the result comes back successfully, the settings are correct.
5. Check if the port number on your router is correct.
6. Please visit [Spamhaus](#) to check if your IP is listed as a spammer. If so, remove your IP from the block list on the same website.

Why can't I receive emails sent from another mail server (e.g., Gmail)?

1. Make sure DNS settings are correctly configured. You will need to point the MX and A records to the Synology NAS so that other mail servers can find the Synology NAS.
2. Make sure the Synology NAS has a static IP address and is connected to the Internet, or your domain name points correctly to your dynamic IP.
3. If the Synology NAS is set behind the NAT firewall/router, please make sure the port forwarding works properly. You can check whether the port forwarding works by going to [the CanYouSeeMe website](#) and inputting the port 25.
4. If any, check the message in a returned mail to find the detailed reason for an error.

Why do I get rejected when I send emails to certain webmail accounts, like those of Gmail or Hotmail?

Many free email providers do a reverse DNS lookup to check the validity of a sender. If your reverse DNS lookup doesn't correspond to the sending domain name, your emails will be rejected. Please check with your ISP. Another possibility is that your IP address is listed on a spam block list. You can check this by visiting [Spamhaus](#).

Chapter 3: Mail Migration

With a built-in mail migrator, MailPlus Server helps you migrate emails from non-MailPlus mail servers (e.g., Microsoft Exchange and IMAP mail servers) and third-party services (e.g., Gmail and Yahoo Mail) without complicated setup.

This chapter will guide you through how to migrate emails from Microsoft Exchange to MailPlus Server. Before you start, please make sure you have done the following:

- Check if the Synology NAS is running DSM 6.0 or later and supports MailPlus Server (see compatible models [here](#)).
- Set up MailPlus Server on the Synology NAS to make it the destination mail server.
- Collect usernames and passwords of source accounts and the corresponding MailPlus account names.

Create a Mail Migration Task in MailPlus Server

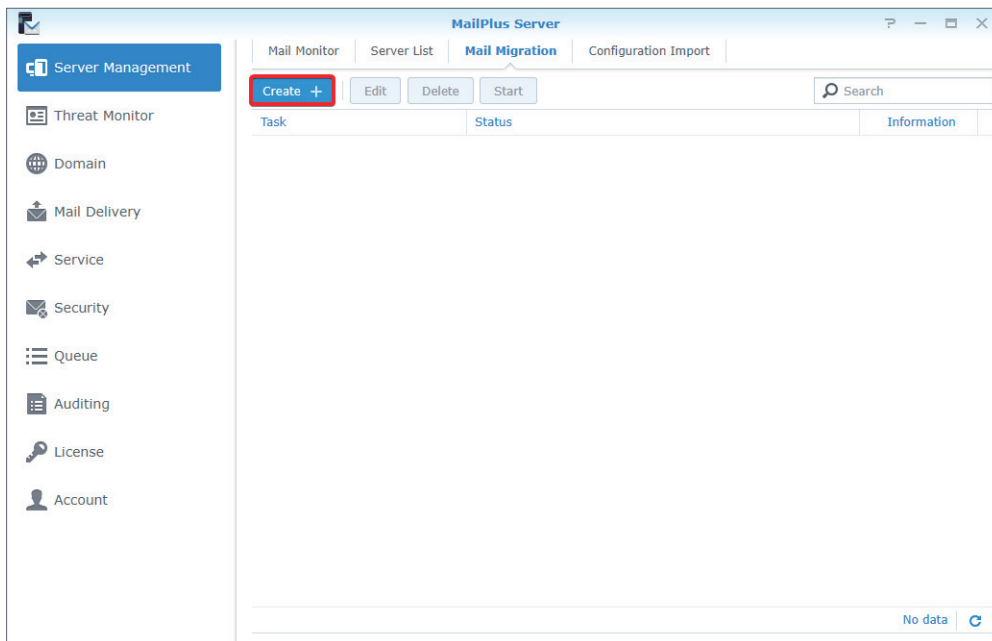
Sign in to MailPlus Server, go to **Server Management > Mail Migration**, and click the **Create** button to create a mail migration task. In this section, Microsoft Exchange will be used as an example for demonstration purposes.

Note:

- To know how to migrate emails from other sources (e.g., Gmail or Yahoo Mail), please see [this help article](#).

Configure general task settings

1. Go to **Server Management > Mail Migration** and click the **Create** button.



2. Go to the **General** tab in the **Migration Settings** window, set **Select the server type** to **Microsoft Exchange**, and fill in the required information of the Microsoft Exchange server.
3. The **IMAP path prefix** can be found within the settings of your Microsoft Exchange server.
4. If you have a delegate account on the source server that has full access permissions to all the other source accounts, select **Migrate mail with the delegate account** and fill in account credentials. This account allows you to migrate emails without asking for the access permissions to each source account.
5. You can specify **Accounts to migrate per time period** according to the source server's capability.

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: [Calendar Icon] 00 : 00

Save Close

Import a user list

1. Prepare a user list following the requirements below:

- Generate a user list in CSV format using Microsoft Excel, Google Sheets, etc.
- List one user account information in one row.
- List each user's following information from left to right: the source account, the source account password, and the corresponding MailPlus Server account.
- Separate each type of information with a comma (,).
- When the source server type is set to **Microsoft Exchange** and **Migrate mail with the delegate account** is enabled, you can omit the source account password (e.g., source_account_X,,MailPlus_Server_account_X).

2. A valid user list should look like the one below:

source_account_1,source_account_1_password,MailPlus_Server_account_1
source_account_2,source_account_2_password,MailPlus_Server_account_2
source_account_3,source_account_3_password,MailPlus_Server_account_3
...
source_account_N,source_account_N_password,MailPlus_Server_account_N

3. Go to **User List**, where you can import the list. Check if all account data are correct.

Migration Settings

General **User List** Filter Notification

Import Delete Check Search

Source Account	MailPlus Account	Result
No data		

Save Close

Set up email and mailbox filters

1. At the **Filter** tab, specify criteria to migrate or skip certain emails and mailboxes.

The screenshot shows the 'Migration Settings' dialog box with the 'Filter' tab selected. The 'Filter' tab is highlighted with a red rectangle. The settings are as follows:

- ☒ Discard mail received before the date: 2017-01-01
- ☐ Discard mail received after the date: To
- ☐ Skip trash mail
- ☒ Skip spam mail
- ☐ Maximum size per email (KB): 10240
- ☒ Enable mailbox filter
 - ☒ Skip mailboxes by keyword
 - ☐ Migrate mailboxes by keyword

At the bottom of the dialog box, there is a 'Set Keywords' button and 'Save' and 'Close' buttons.

2. To filter mailboxes with keywords, tick the **Enable mailbox filter** checkbox and select a filter policy (**Skip mailboxes by keyword** or **Migrate mailboxes by keyword**).
3. Click **Set Keyword** and enter text in the two areas:
 - **Keyword:** Enter text to process matching mailboxes according to the selected filter policy.
 - **Exceptions:** Enter text so that matching mailboxes will not be processed.
4. You can enter regular expressions in the two areas and they should be surrounded by a slash on each side (e.g., /REGULAR_EXPRESSION/).

Set Keywords

Keyword

random

Misc

Exceptions

Enter text here

survey

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

Set up migration notifications

1. Make sure **Enable SMTP** (at **Service**) is ticked in MailPlus Server to allow notification delivery.
2. At the **Notification** tab, determine whether MailPlus Server should send notifications about each account's migration results and where the administrator should receive them.

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

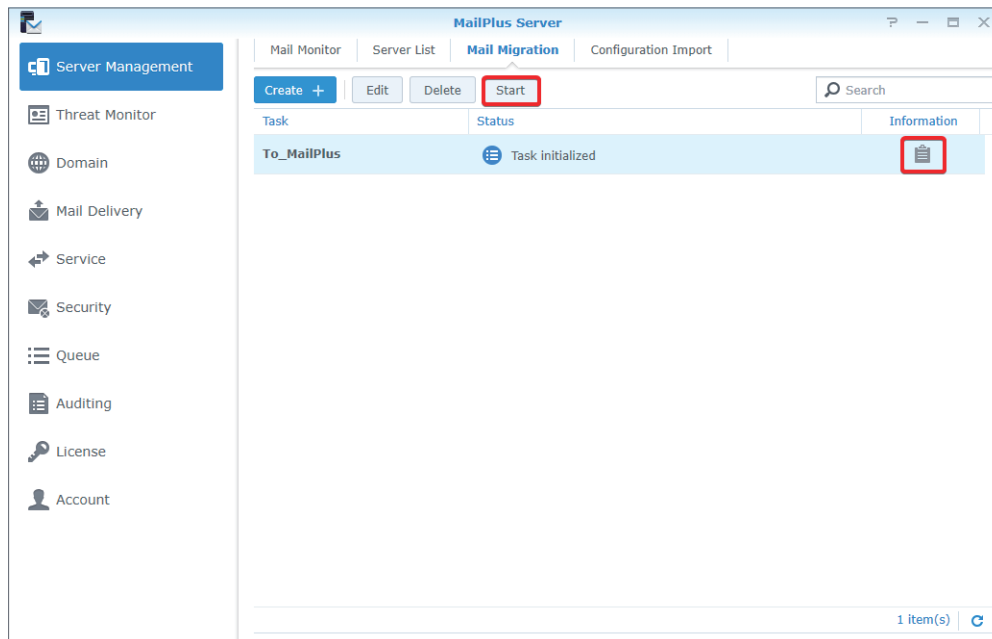
☒ Send failure notification

☐ 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

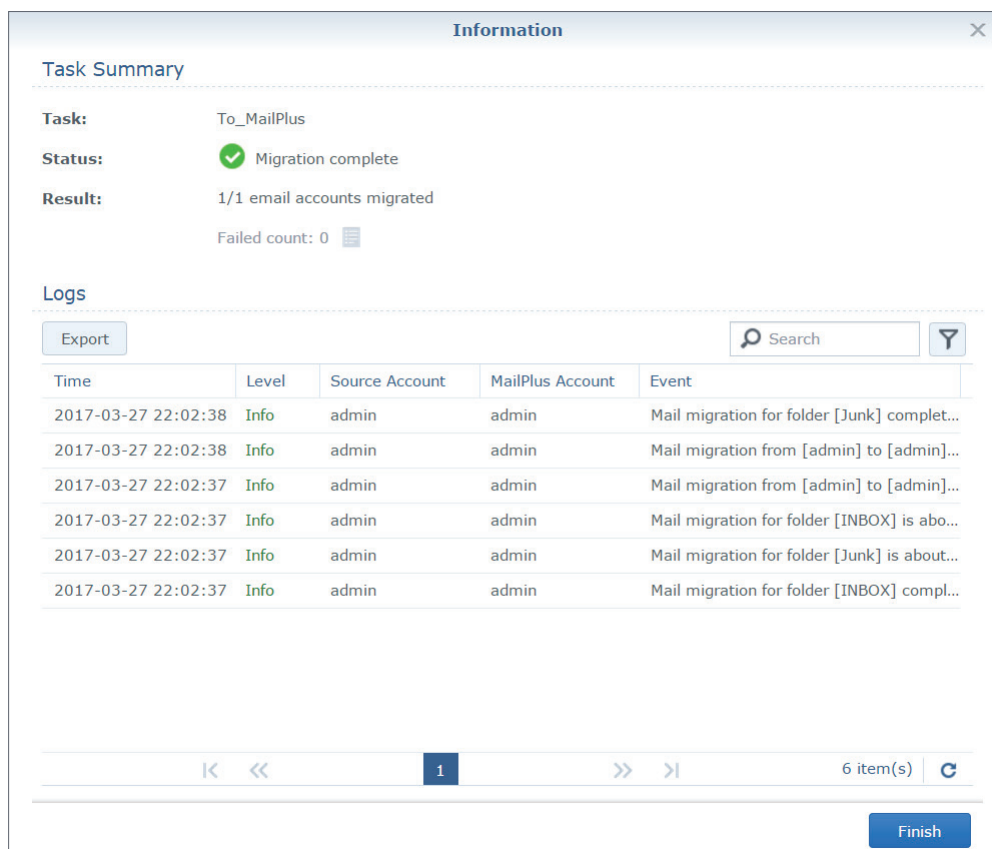
Save Close

Run a mail migration task

1. At **Server Management > Mail Migration**, you can select a migration task and click **Start** to run it. To avoid migration errors, do not change IMAP/POP3 settings in MailPlus Server or move/delete emails on the source mail server.



2. Click **Information** (the document icon) to see migration statistics and logs.

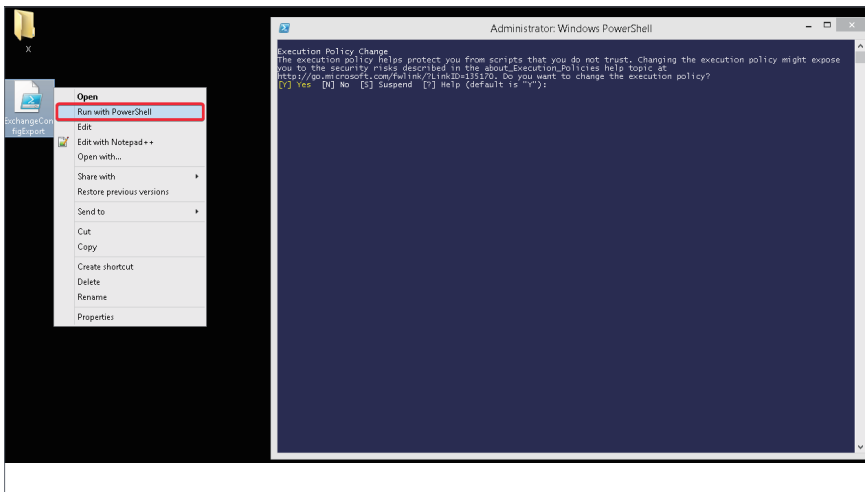


Import System Configurations from Microsoft Exchange to MailPlus Server

You can export system configurations and aliases from a Microsoft Exchange server and have them imported to MailPlus Server for continuous use.

Export system configurations and aliases from Microsoft Exchange

1. Download the script file (**ExchangeConfigExport.ps1**) from [here](#).
2. Log in as the system administrator to a Windows computer running the Microsoft Exchange server.
3. Move the script file to the Windows computer.
4. Execute the script file on the Microsoft Exchange server using Windows PowerShell.



5. When prompted to change the execution policy, choose **Yes** to allow script execution.
6. When execution completes, the Microsoft Exchange server will export the system configurations into a **SynologyExportedExchangeConf.xml** file and the aliases into a **SynologyExportedAlias.txt** file.



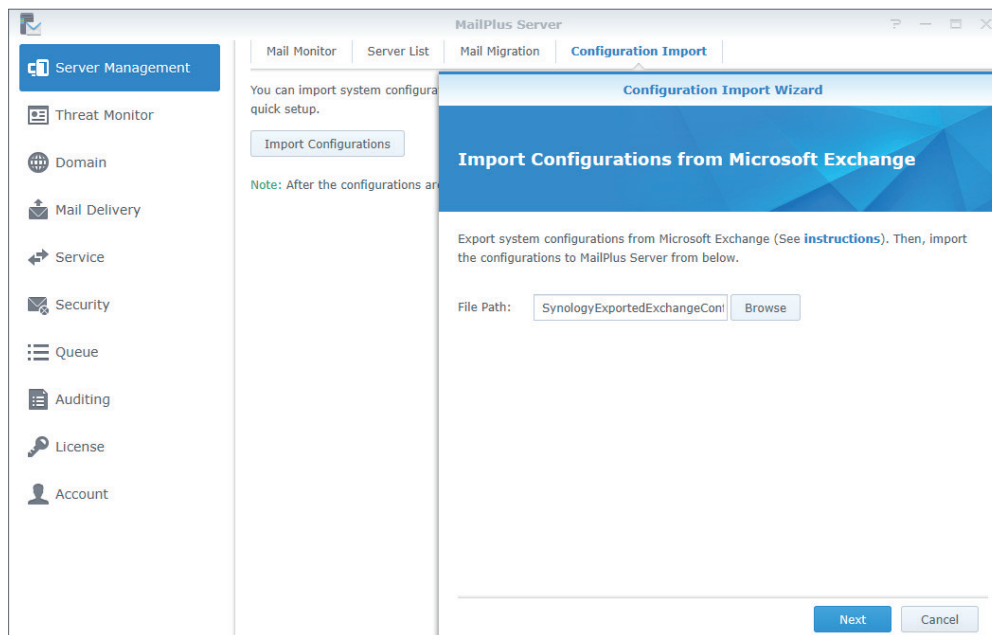
7. Move the generated .xml file and .txt file to your local computer.

Import system configurations to MailPlus Server

1. Begin the import process in either way below:

- When MailPlus Server is to be initialized: Launch MailPlus Server and select **Create a new mail system by importing configurations from Microsoft Exchange**.
- When MailPlus Server has already been initialized: Launch MailPlus Server and go to **Server Management > Configuration Import > Import Configurations**.

2. Click **Browse** to import the **SynologyExportedExchangeConf.xml** file from your local computer.



3. Click **Next** to check configuration details at **General Settings** (e.g., SMTP and security settings) and **Criteria** (e.g., blacklist and whitelist). Click **Import**.

Chapter 4: User Licenses

Sufficient licenses are required to run MailPlus Server. The number of required licenses is determined by the number of accounts that are to be activated. By default, MailPlus Server comes with five free email accounts and allows you to add more accounts with additional purchased licenses.

The number of license users will not be affected by the following:

- **Deactivated accounts:** For example, the license of a former employee can be applied to a new employee.
- **Email alias:** Each user can add aliases at no extra cost because alias email addresses are bound to existing user accounts.
- **Multiple domains (including other domains):** MailPlus Server can handle multiple domains, so using multiple domains does not require additional licenses.
- **DSM users that do not belong to the specified account type:** For example, when the account type is set to LDAP users, local users will not be counted as license users.

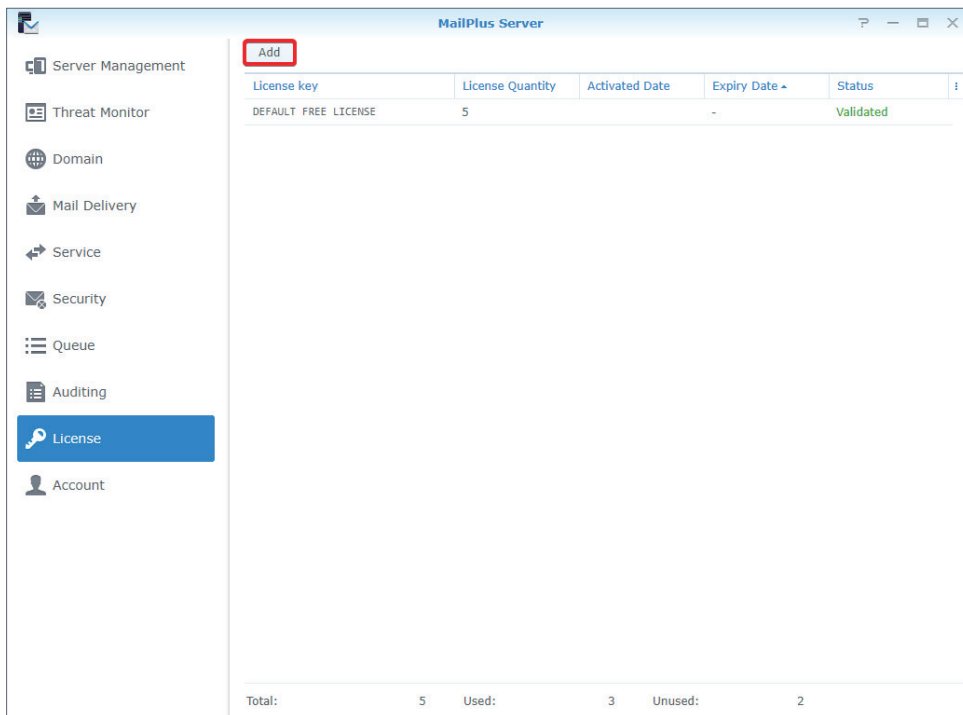
Purchase Licenses

MailPlus license packs include five or 20 units of email accounts and can be purchased through [Synology authorized resellers](#). For details on MailPlus license packs, please refer to the [MailPlus licensing page](#).

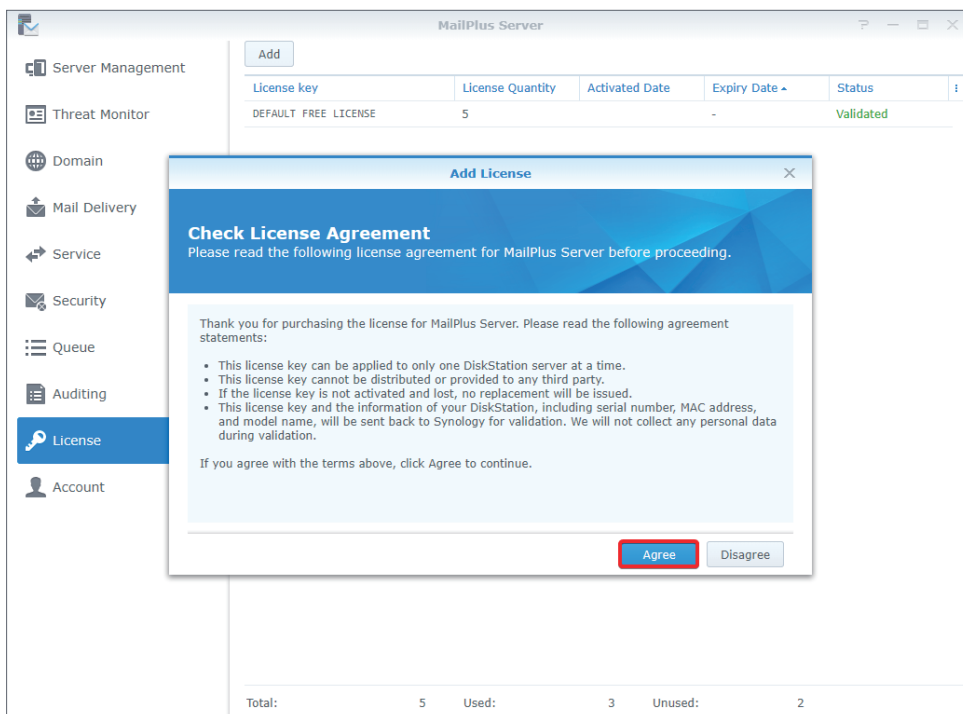
Install Licenses

Purchased licenses must be installed to activate email accounts. Please refer to the following steps:

1. Go to **License** and click the **Add** button to add licenses.



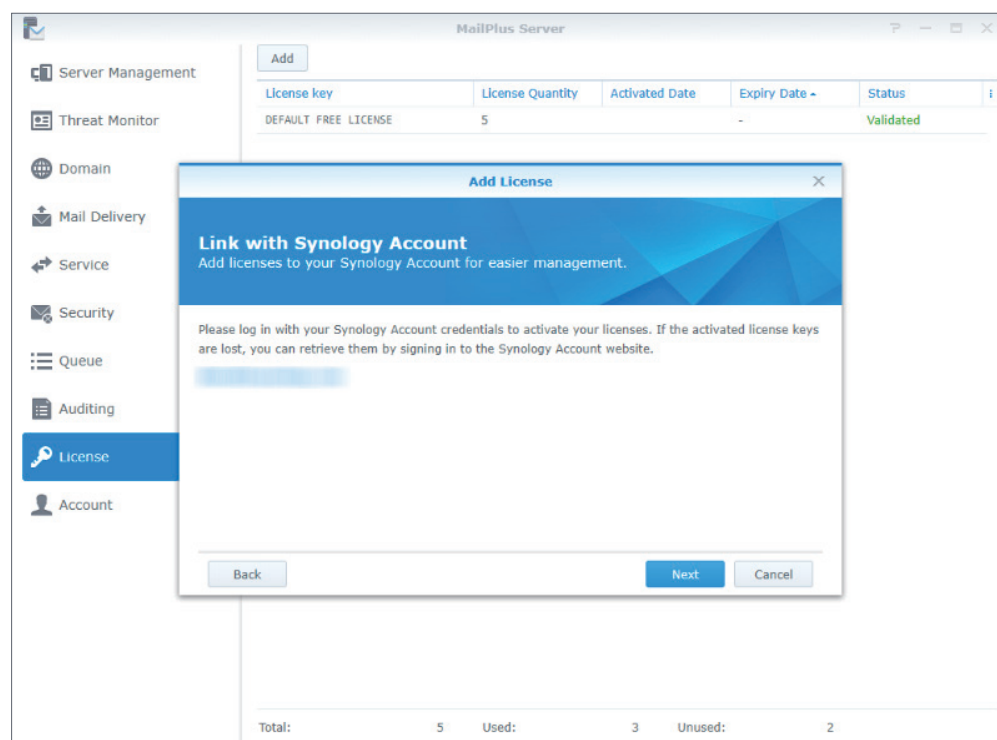
- In the **Add License** window, please carefully read the license agreement for MailPlus Server. After checking and confirming the content, click **Agree**.



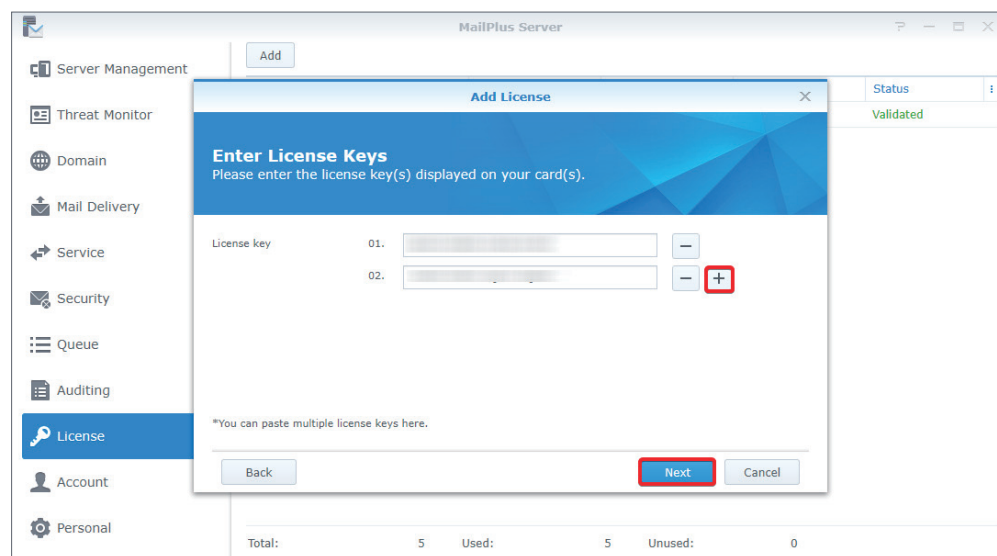
- Sign in to the Synology Account and click **Next**.

Note:

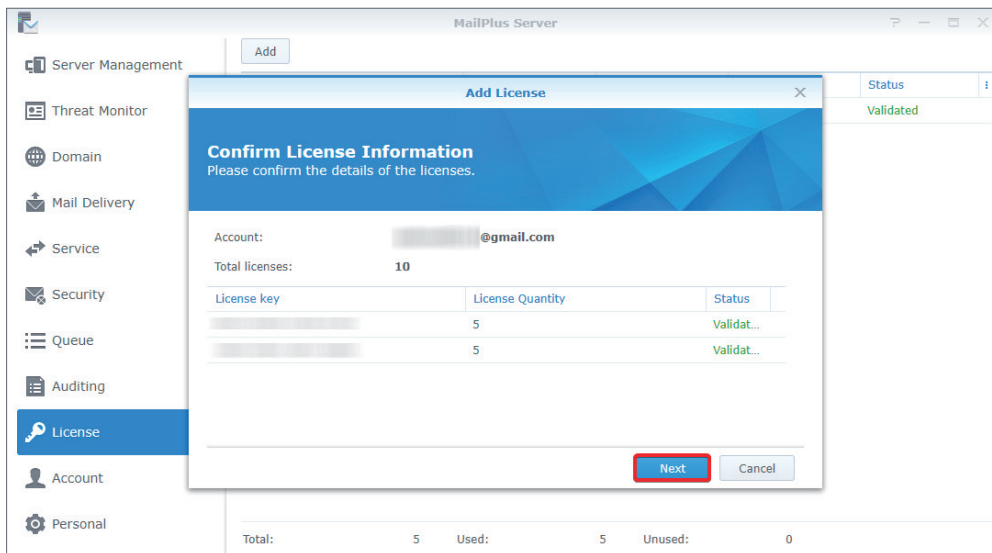
- Should there be situations where licenses are unable to be retrieved after being activated, sign in to the **Synology Account** to submit a technical support ticket.



4. Enter the license number in the **License Key** field as shown in the image below. If you need to add more than one license, click on the plus icon (+) to add more fields.



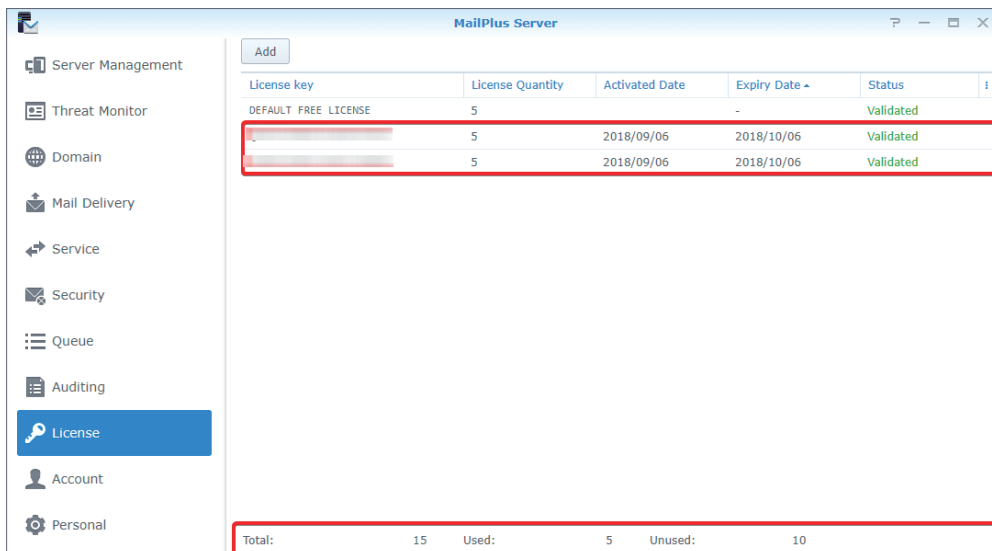
5. Check and confirm if the number of licenses to be installed and their respective license keys are correct. After confirming the information is correct, click **Next** to finish adding licenses.



6. After adding licenses, you can go to the **License** page to check the details and statuses of each license:

- License key
- The number of email accounts provided by each license
- License activation date
- License expiration date
- License validity status

7. In addition, at the bottom of the **License** page, you can view the total number of licenses installed on the MailPlus Server, as well as the number of used and unused licenses.



User Licenses

After adding licenses, you can go **Account > User** to choose which accounts to activate. For detailed instructions, please refer to [Activate Accounts](#).

Chapter 5: Account Settings

Account System

MailPlus Server uses the same account system as DSM; therefore, you can activate user accounts in MailPlus Server from existing user accounts on DSM.

In addition to activating user accounts from local users, you can activate user accounts from LDAP/domain users (go to **DSM > Control Panel > Domain/LDAP** to bind LDAP and domain accounts). However, DSM cannot synchronize more than one directory service at a time; therefore, MailPlus Server cannot simultaneously synchronize more than one directory service and account system either.

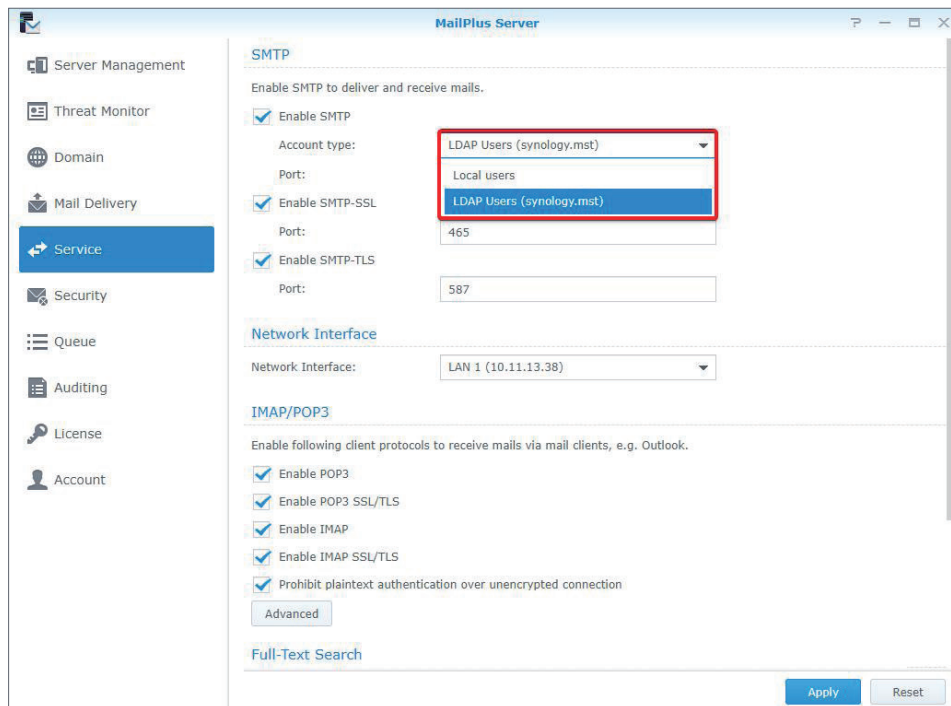
Note:

- MailPlus Server can only use one of the following account types at a time: **Local**, **LDAP**, or **Domain**.

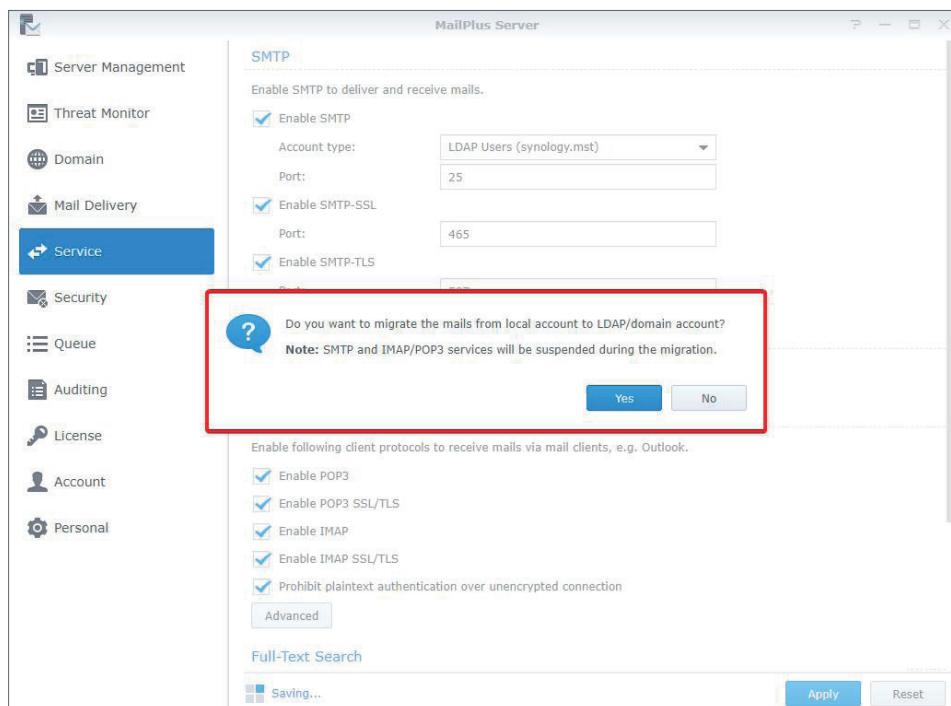
Modify account type

Please follow the steps below to modify account type:

1. Sign in to your DSM.
2. Go to **Control Panel > Domain/LDAP** to bind with a specific directory service. If you are using **Local users** as the account type, please skip this step.
3. Launch **MailPlus Server**.
4. Go to **Service** to select an account type from the **Account type** drop-down menu. (Only the directory service configured on DSM will be shown here.)



5. Click **Apply** to import user accounts from the directory service. As shown in the following image, if you switch from **Local users** to **LDAP Users** or **Domain Users** and click **Apply**, an alert window will appear.



Note:

- Different account types have different email addresses, so emails under different account types cannot be shared. If you want to migrate emails from **Local Users** to **LDAP Users** or **Domain Users**, please click **Yes**. The system will only migrate emails to directory service accounts with the same usernames as local users. Accounts with different usernames will be automatically ignored.

Activate Accounts

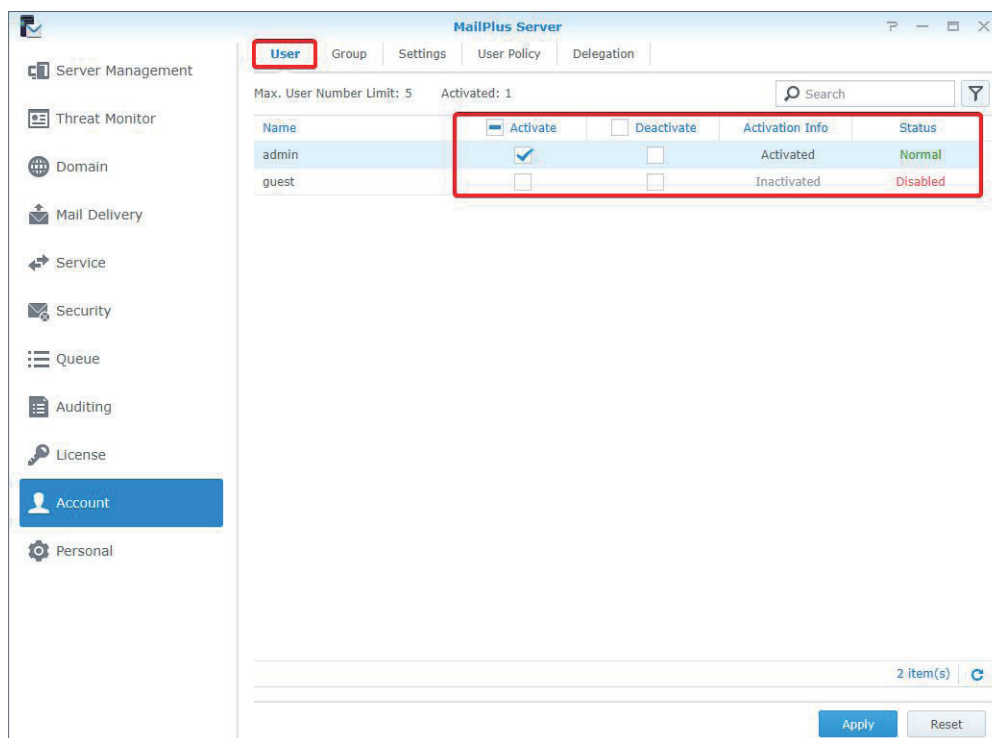
You must activate user accounts in MailPlus Server to start using mail services, such as sending and receiving emails. Therefore, you need sufficient licenses to activate the accounts that will use mail services. For more information, please refer to the [User Licenses](#) section.

If you have already activated some user accounts, and these users cannot sign in to DSM or launch MailPlus/MailPlus Server, please check if you have disabled any user accounts and whether these user accounts have privileges to the MailPlus or MailPlus Server. For more information on client login issues, please refer to [this article](#).

Activate user accounts

Activating user accounts requires a sufficient number of licenses. For more instructions, please refer to [User Licenses](#) section. Please follow the steps below to activate user accounts:

1. Go to **Account > User**.
2. Select the users you want to activate. If the checkboxes under the **Activate** and **Deactivate** columns are not ticked for a certain user, the status of this user will be set as the default status. For details, please refer to [Default status](#). Ticking the **Activate** checkbox will reduce the number of available licenses.



3. The **Activation Info** column displays if a license has been applied to the user.
4. The **Status** column displays the following DSM user statuses: **Normal**, **Disabled**, and **Username unsupported**.

Note:

- Users can use mail services properly only when an account is **Activated** under **Activation Info** and **Normal** under **Status**. Account setting can be left as the sole entry in MailPlus privilege without modifying the settings in **Control Panel**.

5. Click **Apply** to activate users.

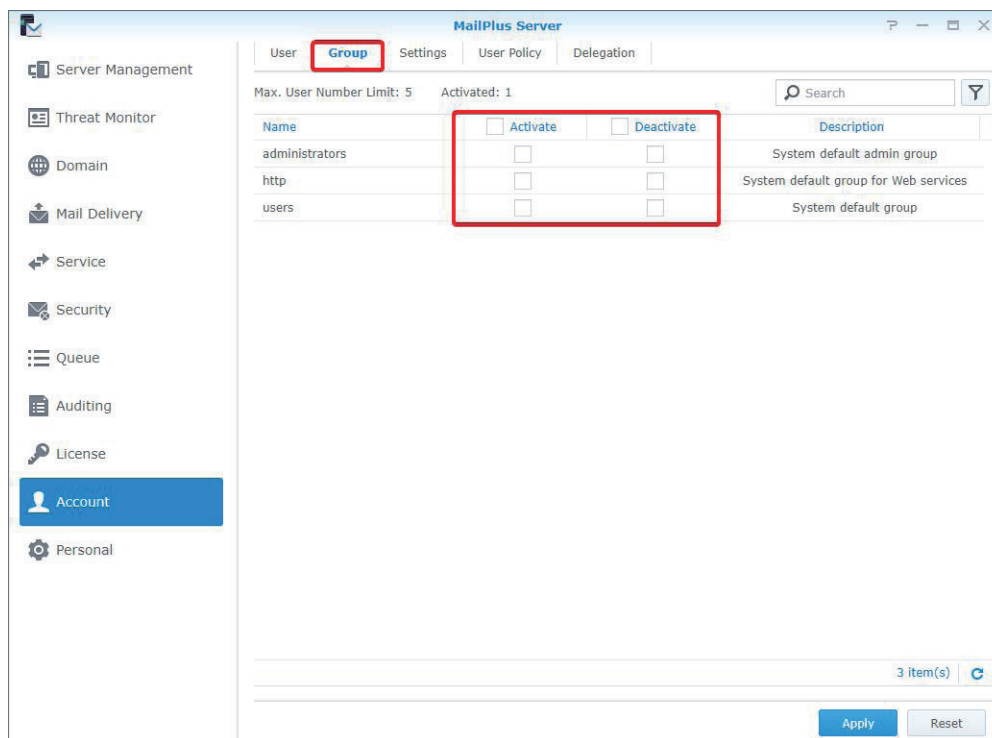
Activate groups

You can easily activate and deactivate user groups here. Settings will be applied to all members within the same group. Please refer to the following steps:

1. Go to **Account > Group** to activate or deactivate a group.

Note:

- The descending order of the priority for determining the last activated user account is as follows: **User** settings, **Group** settings, and **Default** settings.



2. Click **Apply** to activate users within the group.

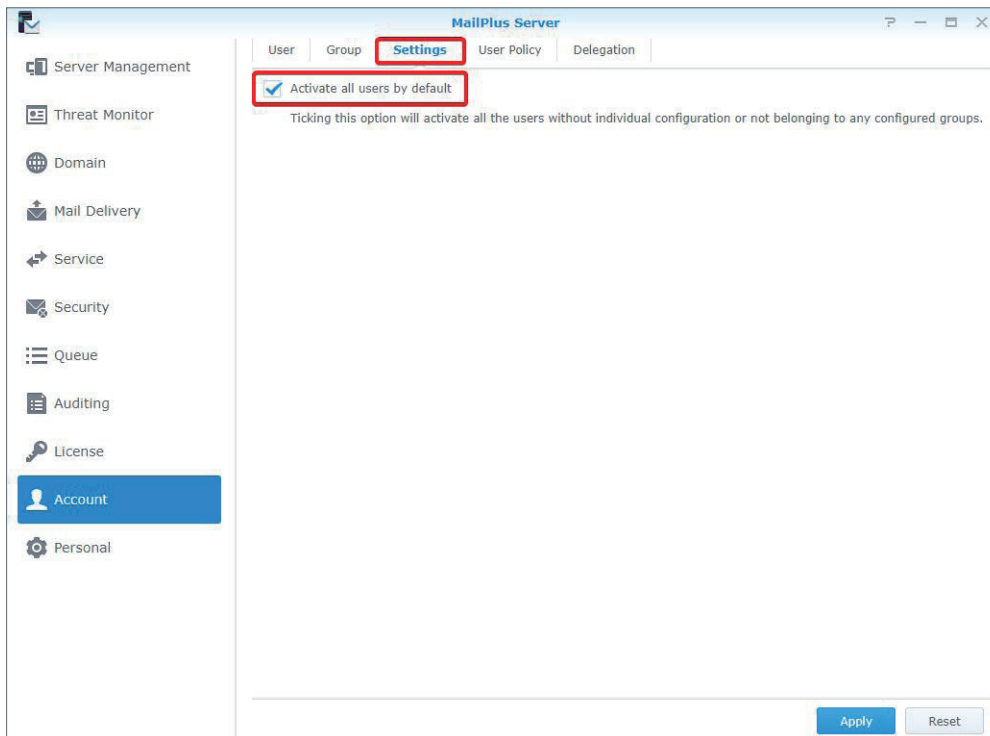
Default status

You can adjust the default status at the **Settings** tab in the **Account** page. The default status settings will be applied to user accounts in the **Normal** status that have not been activated or deactivated. Please refer to the following steps:

1. Go to **Account > Settings** and choose whether to tick the **Activate all users by default** checkbox.

Note:

- Activating by default may use a large number of licenses. Please make sure you have sufficient licenses.

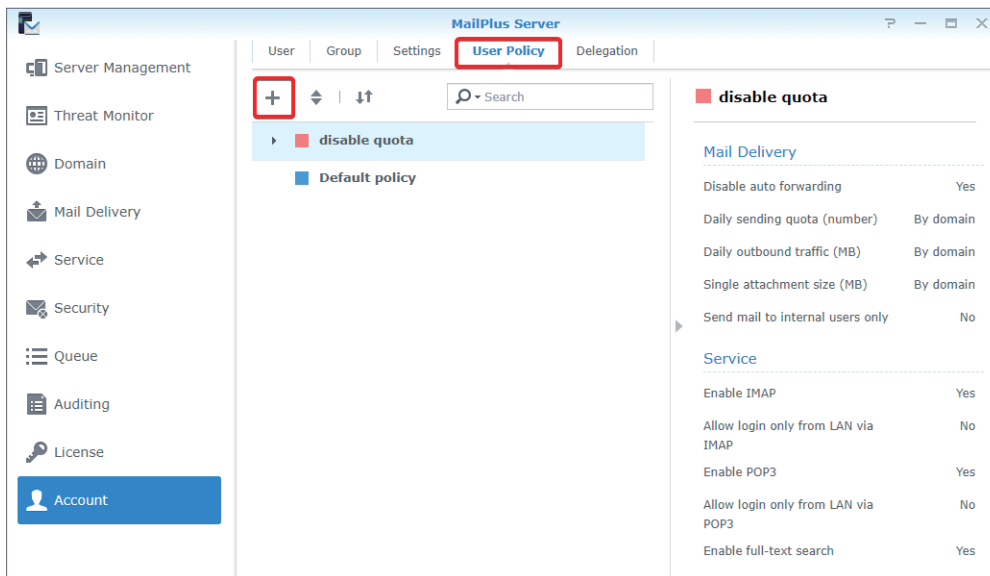


2. Click **Apply** to save the settings.

Create user policies

After activating users or groups, you can create dedicated mail service policies for certain users or groups to meet an organization's requirements. Please refer to the following steps to create user policies:

1. Go to **Account > User Policy**.
2. Click the plus icon (+) to create a new policy.

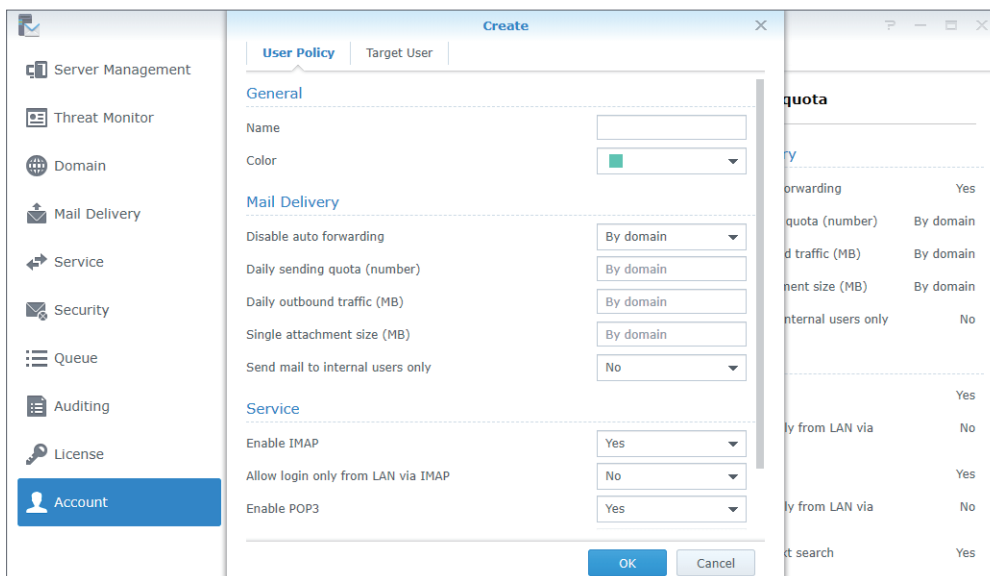


3. In the **Create** window, go to **User Policy** and enter a policy name in the **Name** field.

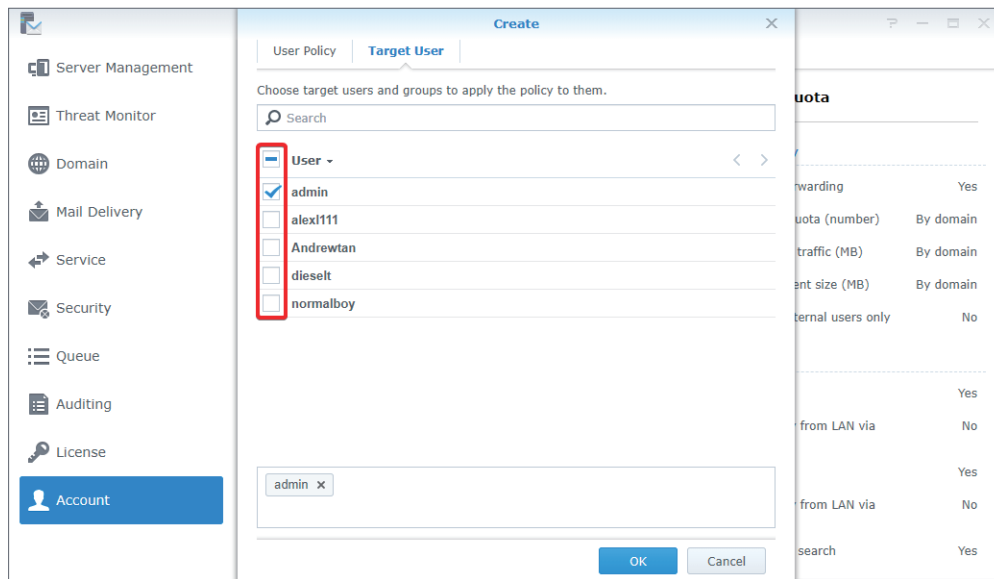
4. Select a color for the policy from the **Color** drop-down menu for easy identification.

Note:

- For details on policy information, please refer to [Policy information and restrictions](#).

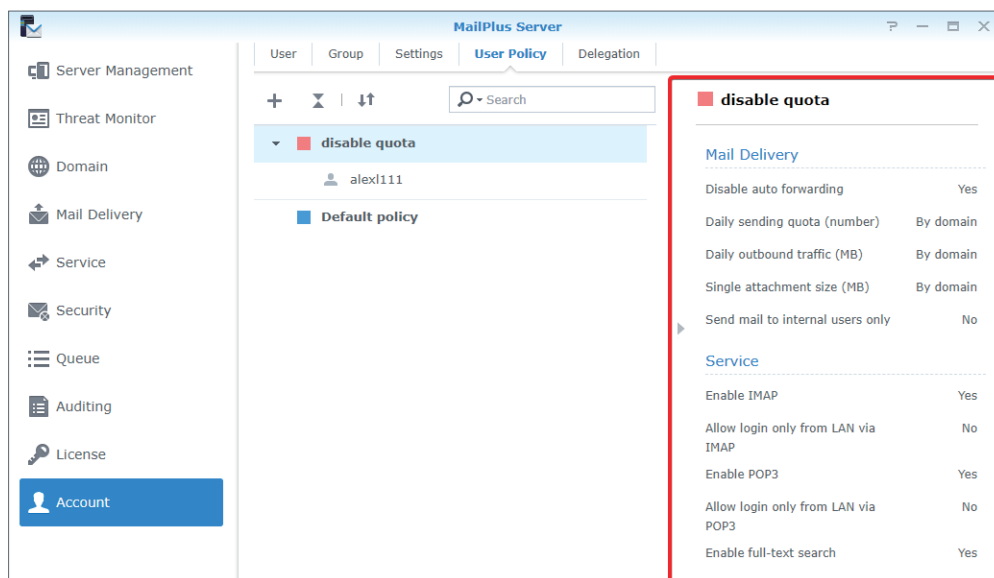


5. Switch to the **Target User** tab and select a user or group to apply the policy to. You can also use the search bar at the top of the window to find the target.



6. Click **OK** to finish the settings.

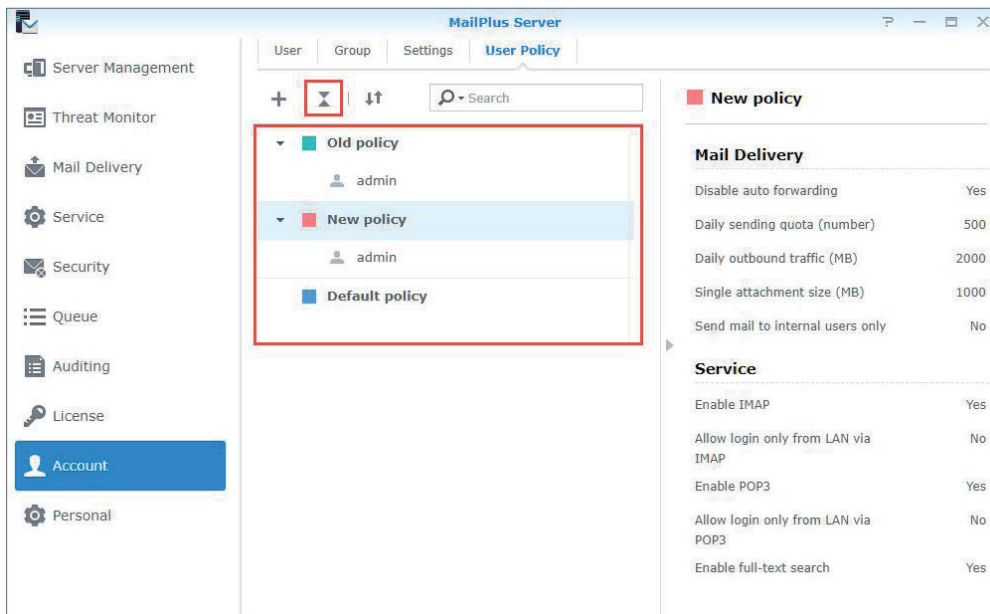
7. After a policy has been created, it will be listed in the **User Policy** page. Select a policy to preview policy details and settings on the right panel of the page.



Change user policy priority

Multiple user policies may be applied to one user; however, only one policy will take effect. Which policy will take effect depends on the priority settings of user policies. Please refer to the following steps to change the priority of a user policy:

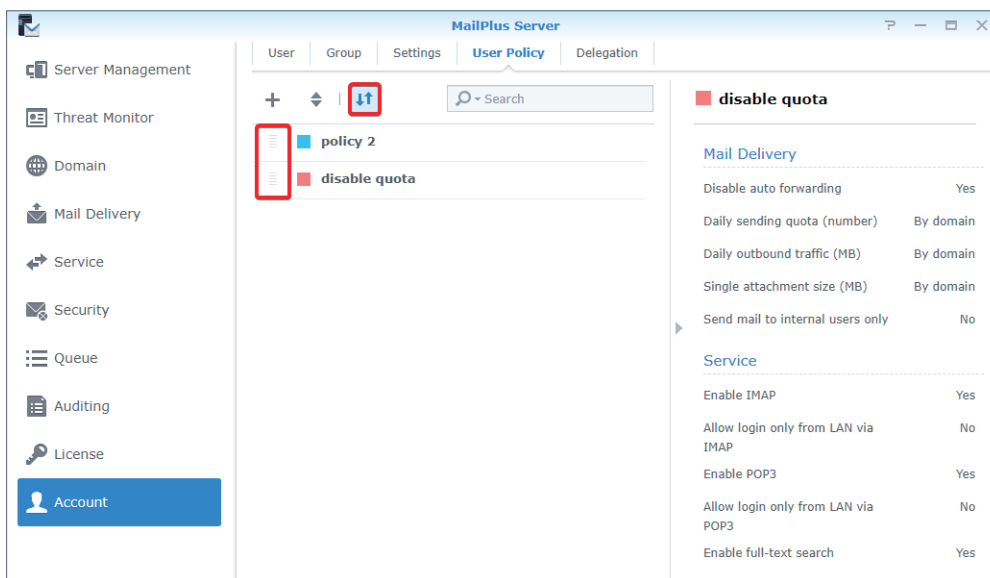
1. Go to **Account > User Policy** and click the double triangle icon to show or hide target users/groups.
2. Higher policies have greater priority over lower policies. (For example, in the image below, the priority in descending order will be as follows: *Old policy*, *New policy*, *Default policy*. Therefore, *Old policy* instead of *New policy* will be applied to the admin.)



3. Click the two-way arrow icon to change the policy priority.

Note:

- If you wish to apply a specific policy to a user, please make sure this policy has a higher priority over other policies.



4. Hover to the left of the policy and drag and drop it to a suitable position according to your desired order.

5. Click the two-way arrow icon to close the drag and drop function and make the new priority order take effect.

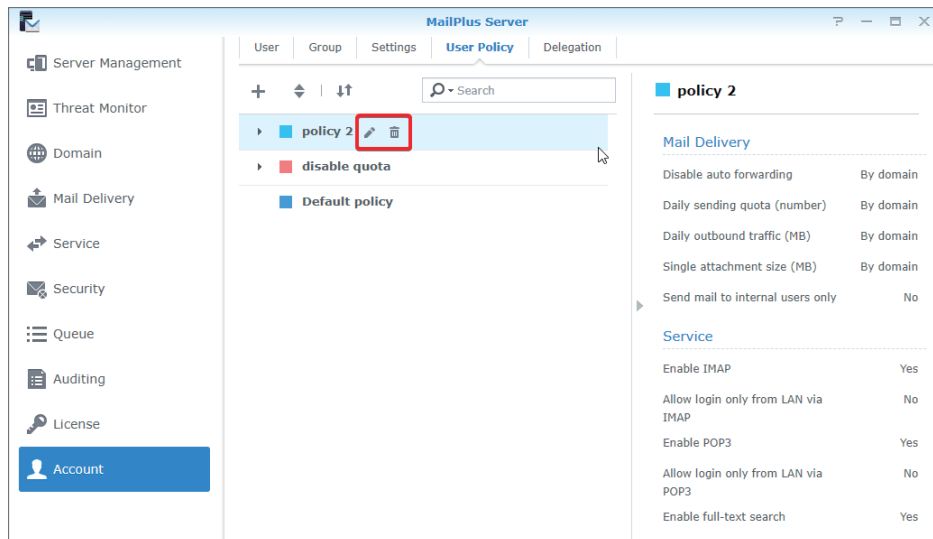
Note:

- **Default policy** will always have the lowest priority. For more information, please refer to [Default policies](#).

Edit and delete user policies

You can edit policy settings, add or delete users to a policy, or change policy color. Please refer to the following steps to edit or delete a user policy:

1. Go to **Account > User Policy**.
2. Hover to the policy you want to edit and two icons will appear. Click the pencil icon to edit the policy, or click the trash-can icon to delete the policy.



Default policies

The system default policy will be applied to users that are not regulated by any custom policy. The default policy is a pre-existing policy that cannot be edited, deleted, or re-prioritized. Please refer to the following setting details of the default policy:

Disable auto forwarding	The default is By Domain .
Daily sending quota (number)	The default is By Domain .
Daily outbound traffic (MB)	The default is By Domain .
Single attachment size (MB)	The default is By Domain .
Send mail to internal users only	The default is No .
Enable IMAP	The default is Yes .
Allow login only from LAN via IMAP	The default is No .
Enable POP3	The default is Yes .
Allow login only from LAN via POP3	The default is No .
Enable full-text search	The default is Yes .

Since the default policy will apply to all users, it may not meet your expectations regarding certain restrictions. If you do not want specific restrictions to take effect, you will need to disable these restrictions.

Policy information and restrictions

No.	Policy	Results of Enabling Policy	Results of Disabling Policy	By Domain
01	Disable auto forwarding	Users cannot auto-forward emails.	Users can auto-forward emails.	Policies will follow domain settings.

Note:

- This policy does not affect manual forwarding.

No.	Policy	Results of Enabling Policy	Results of Disabling Policy	By Domain
02	Daily sending quota (number)	Users will be restricted by a quota.	Users will not be restricted by a quota.	Policies will follow domain settings.

Note:

- If an email message has been rejected before being delivered, it will not be counted against the quota.
- If an email message has been returned after being delivered, it will be counted against the quota.
- The value set for the default policy is equal to the **Daily quota** value under the **Daily Quota** section of the **Usage Limit** tab in the **Domain** page.
- When the value is **0**, users will not have any restrictions.
- You must go to **Mail Delivery > General** and tick the **Enable SMTP authentication** checkbox.

No.	Policy	Results of Enabling Policy	Results of Disabling Policy	By Domain
03	Daily outbound traffic (MB)	Users will be restricted by outbound traffic.	Users will not be restricted by outbound traffic.	Policies will follow domain settings.

Note:

- If an email message has been rejected before being delivered, it will not be counted against the quota.
- If an email message has been returned after being delivered, it will be counted against the quota.
- The value set for the default policy is equal to the **Daily traffic limit (MB)** value under the **Daily Quota** section of the **Usage Limit** tab in the **Domain** page.
- When the value is **0**, users will not have any restrictions.
- You must go to **Mail Delivery > General** and tick the **Enable SMTP authentication** checkbox.

No.	Policy	Results of Enabling Policy	Results of Disabling Policy	By Domain
04	Single attachment size (MB)	Users will be restricted by attachment sizes.	Users will not be restricted by attachment sizes.	Policies will follow domain settings.

Note:

- The value set for the default policy is equal to the **Maximum size per mail (MB)** value at the **General** tab in the **Mail Delivery** page.
- The value set for the default policy will be applied to external emails.

No.	Policy	Results of Enabling Policy	Results of Disabling Policy
05	Send mail to internal users only	Users will be restricted to sending emails to internal users only.	Users will not be restricted to sending emails to internal users only.

No.	Policy	Results of Enabling Policy	Results of Disabling Policy
06	Enable IMAP	Users will be allowed to use IMAP.	Users will be restricted from using IMAP.

Note:

- If the **Enable IMAP** checkbox under the **IMAP/POP3** section in the **Service** page is not ticked, IMAP services will not be available and the user policy will not take effect. Users will not be able to use IMAP even when IMAP is enabled in the user policy.

No.	Policy	Results of Enabling Policy	Results of Disabling Policy
07	Allow login only from LAN via IMAP	Users will be restricted to only signing in from a subdomain via IMAP.	Users will have no restrictions when signing in to MailPlus.

Note:

- If the **Enable IMAP** checkbox under the **IMAP/POP3** section in the **Service** page is not ticked, IMAP services will not be available and the user policy will not take effect. Users will not be able to sign in via IMAP even when **Allow login only from LAN via IMAP** is enabled in the user policy.
- MailPlus web clients will not be restricted by this setting.

No.	Policy	Results of Enabling Policy	Results of Disabling Policy
08	Enable POP3	Users will be allowed to use POP3.	Users will be restricted from using POP3.

Note:

- If the **Enable POP3** checkbox under the **IMAP/POP3** section on the **Service** page is not ticked, POP3 services will not be available and the user policy will not take effect. Users will not be able to use POP3 even when POP3 is enabled in the user policy.

No.	Policy	Results of Enabling Policy	Results of Disabling Policy
09	Allow login only from LAN via POP3	Users will be restricted to only signing in from a subdomain via POP3.	Users will have no restrictions when signing in to MailPlus.

Note:

- If the **Enable POP3** checkbox under the **IMAP/POP3** section in the **Service** page is not ticked, POP3 services will not be available and the user policy will not take effect. Users will not be able to sign in via POP3 even when **Allow login only from LAN via POP3** is enabled in the user policy.
- You can still sign in with MailPlus using an external network. (MailPlus connects to the mail server using the internal network.)

No.	Policy	Results of Enabling Policy	Results of Disabling Policy
010	Enable full-text search	The server will index email content of users.	The server will not index email content of users.

Note:

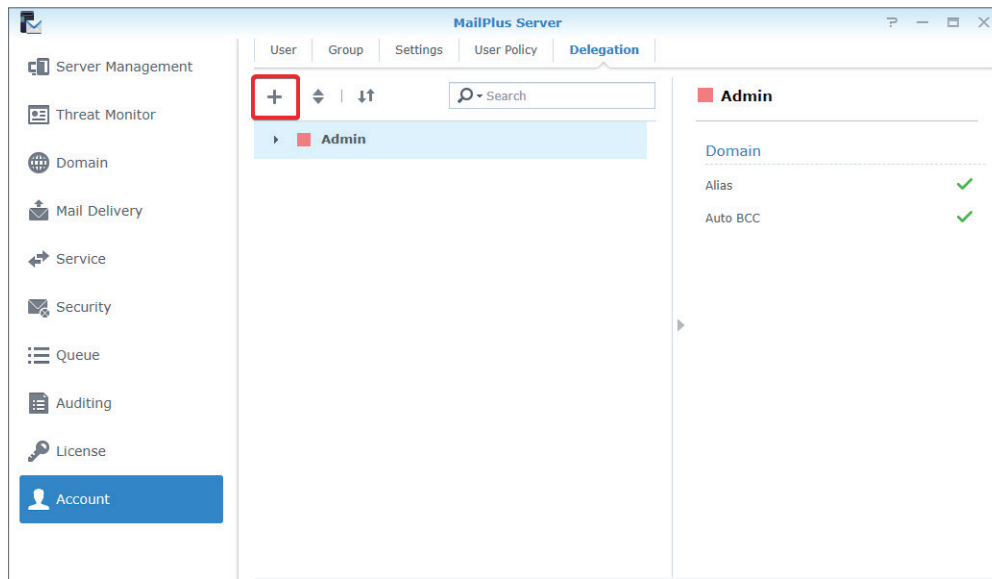
- If the **Enable full-text search** checkbox under the **Full-Text Search** section in the **Service** page is not ticked, the user policy will not take effect, and the email content of users will not be indexed.

Create delegation policies

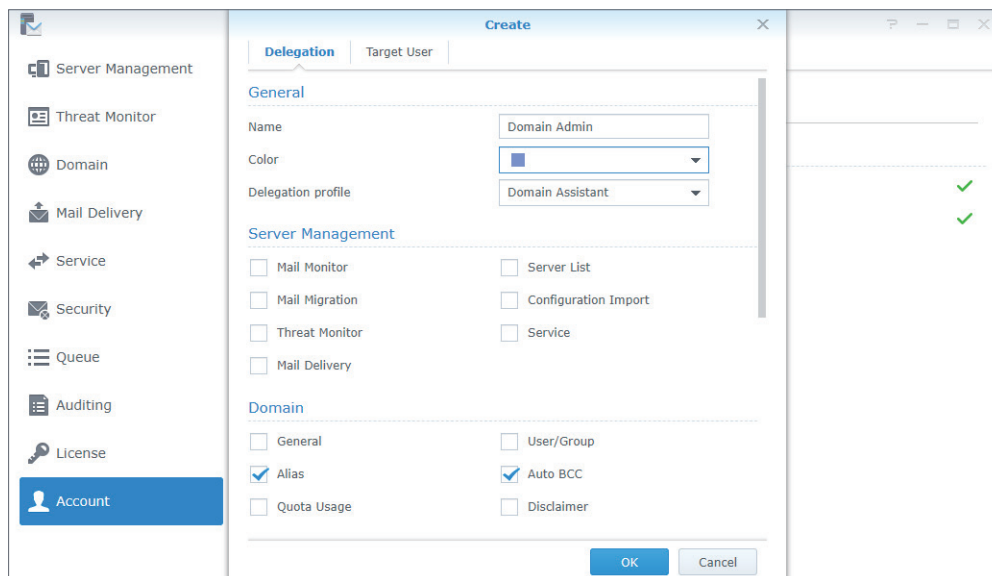
At the **Delegation** tab, you can delegate other users to manage settings related to server management, domain, security, auditing, and account (except for license) of MailPlus Server according to the delegation profile you assign them. In this chapter, *Domain Admin* will be

used as an example for demonstration purposes.

1. Go to **Account > Delegation** and click the plus icon on the top bar.

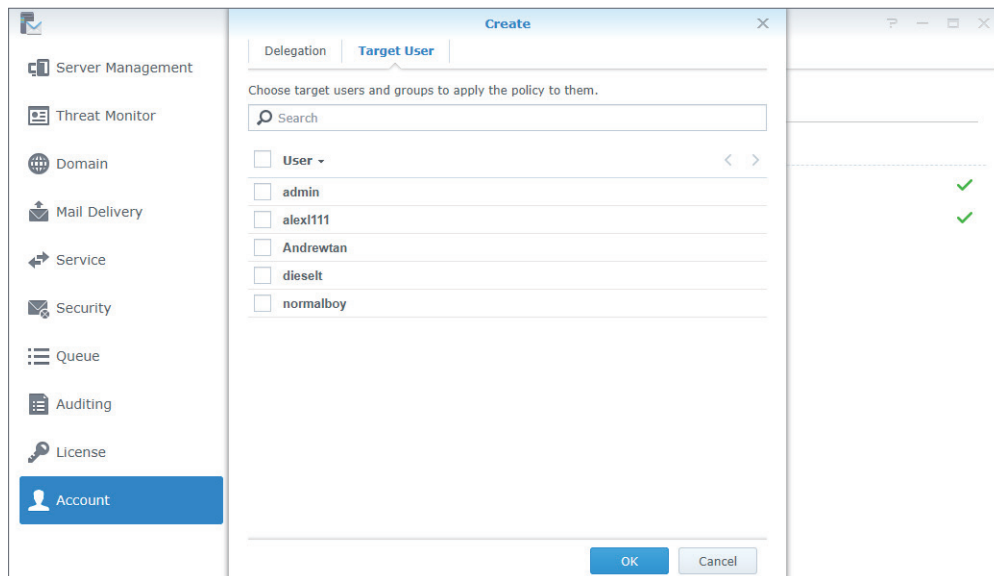


2. In the pop-up window, go to the **Delegation** tab and enter the required information. The system will automatically tick the options below based on the selected delegation profile. The profile will switch to **Custom** when you tick or untick any options below. Please refer to [this article](#) to know more about the delegated permissions.



For example, if you select **Domain Manager** for *Domain Admin*, users regulated by this delegation policy can manage all settings of existing domains. However, if you select **Domain Assistant** for *Domain Admin*, users under this delegation policy can only manage the alias and auto BCC of domains.

3. Go to the **Target User** tab to select the users/groups to be regulated under the defined delegation policy.



4. Click **OK** to save the settings.

Manage delegation policies

1. Go to **Account > Delegation**.
2. Select **Domain Admin** to view, edit, and delete a policy.
3. You can use the buttons on the top toolbar and the preview panel on the right to manage delegation policies:

- **Set policy priority:**

- Click the two-way arrow icon to set the priority.
- Click **Domain Admin** and drag and drop the policy to a suitable position. If a user/group is governed by more than one delegation policy, the system will apply the highest policy on the list to the user/group.

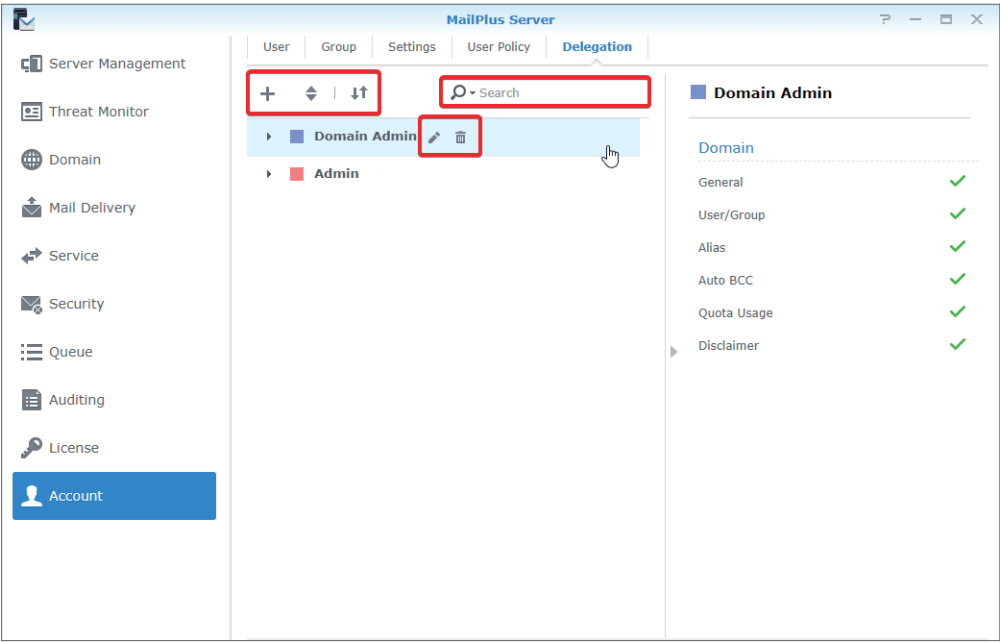
- **Expand/Collapse a delegation policy:** Click the double triangle icon to expand or collapse its target users/groups.

- **Search a delegation policy:** Enter the policy name or its users in the top search bar.

- **Preview a delegation policy:** Preview the name, profile, and other details of the delegation policy.

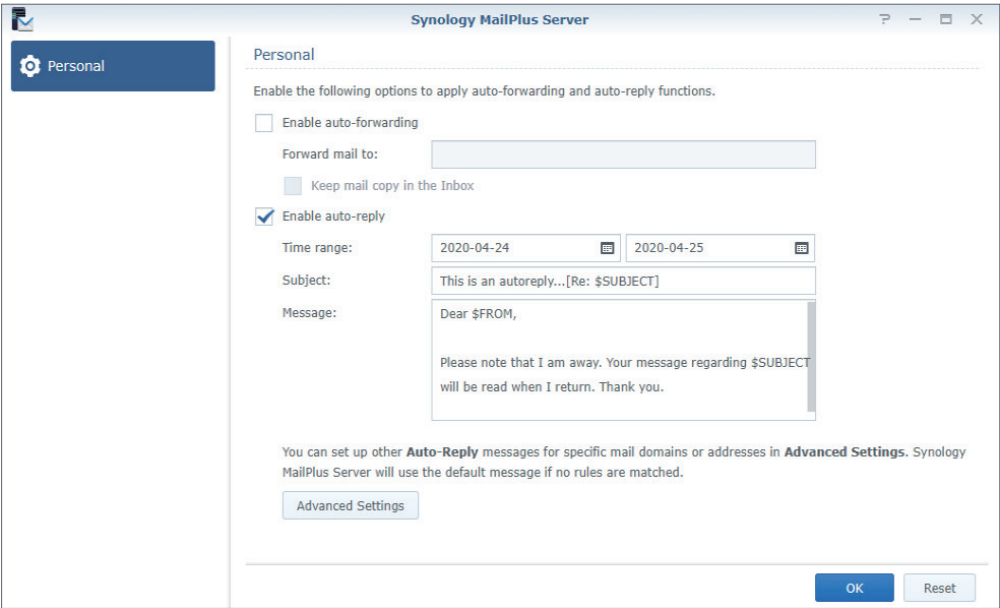
- **Edit a delegation policy:** Click the pen icon to edit the policy.

- **Delete a delegation policy:** Click the trash bin icon to delete the policy.



Manage Privileges

MailPlus Server privilege settings are synchronized with DSM settings. Users who are from the administration group on DSM can access all the MailPlus Server settings, while general users can only see the **Personal** page (as shown in the image below).



Note:

- The privilege settings of MailPlus Server should remain as default at **Control Panel**. All users should have privileges on MailPlus Server; otherwise, the package functionality would be limited.

Chapter 6: Protocol Settings

MailPlus Server provides a centralized configuration interface for mail service protocols. You can open/close ports for certain protocols or rebind the network interface of your server. Since protocol settings affect the external operations of the entire server, please make sure the settings are configured according to your needs.

SMTP

The SMTP uses three ports. In MailPlus Server, they are displayed as SMTP (port number: 25), SMTP-SSL (port number: 465), and SMTP-TLS (port number: 587). The three protocols and their respective roles are listed below:

- **SMTP:** **SMTP** is a standard protocol used to receive external emails and deliver internal emails. MailPlus Server uses Postfix and will deliver email messages using hamming code when **STARTTLS** is not specified. Currently, our SMTP is not encrypted. If you need encryption, please refer to [here](#).
- **SMTP-SSL:** SMTPS is a supported protocol for SMTP-SSL. Since DSM no longer supports SSL encryption, MailPlus Server can only connect to SMTP-SSL through TLS.

Note:

- This is different from encrypting SMTP through STARTTLS. SMTP must send encrypted packets out after a handshake. If you need to relay using this protocol, please refer to [here](#) for more information.
- **SMTP-TLS:** SMTPS is a supported protocol for SMTP-TLS and performs encryption through STARTTLS. SMTP-TLS requires authentication; therefore, it is often used for the internal protocol between client and [MSA](#).

Set up SMTP

Please refer to the following instructions on the configuration of SMTP and respective ports:

1. Go to **Service > Protocol > SMTP** and tick the **Enable SMTP** checkbox.

Note:

- SMTP is the main protocol for a mail server.

Synology MailPlus Server

Protocol

SMTP

Enable SMTP to deliver and receive mails.

☒ Enable SMTP

Account type: LDAP Users (esther.test.test)

Port: 25

☒ Enable SMTP-SSL

Port: 465

☒ Enable SMTP-TLS

Port: 587

Network Interface

Network Interface: LAN 1 (10.17.28.44)

IMAP/POP3

Enable following client protocols to receive mails via mail clients, e.g. Outlook.

☒ Enable POP3

Apply Reset

2. You can change the port number in the **Port** field.

Note:

- Unless there are special circumstances, we recommend that you use the default port 25.

3. You can adjust the following settings:

- **Enable SMTP-SSL:** Uses SMTPS as the protocol. You can change the SMTP-SSL port number in the **Port** field.
- **Enable SMTP-TLS:** Allows authentication and STARTTLS encryption during forced connection. You can change the SMTP-TLS port number in the **Port** field.

4. Click **Apply** to save the settings.

IMAP/POP3

IMAP/POP3 provides both encrypted and non-encrypted options, thereby using four ports. In MailPlus Server, these ports are IMAP (port number: 143), IMAPS (port number: 993), POP3 (port number: 110), and POP3S (port number: 995). Through these protocols, you can retrieve email information from MailPlus Server using different email clients.

Note:

- Both protocols encrypt through STARTTLS. Since DSM no longer supports SSL encrypted connection, please do not set up SSL for an encrypted connection.

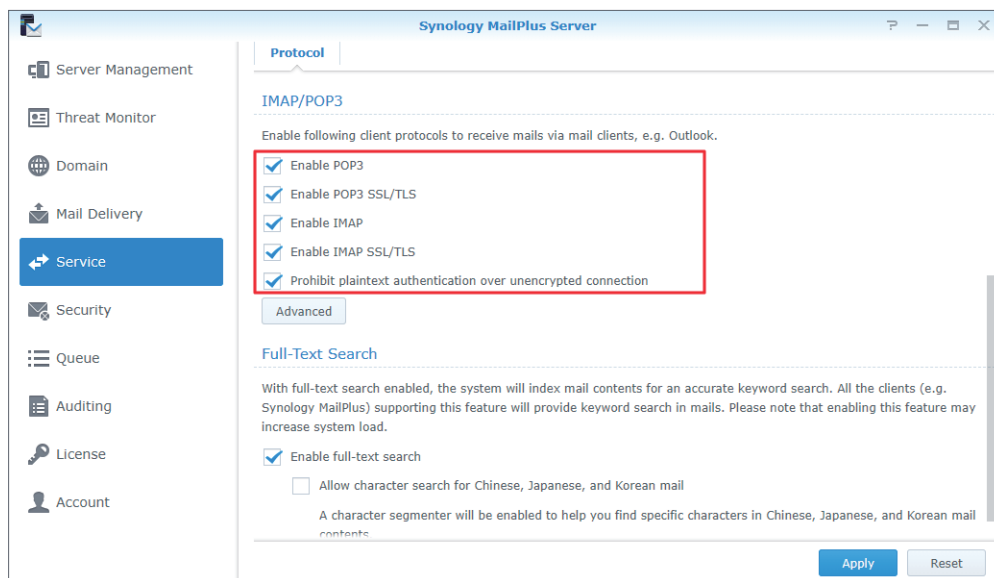
- **IMAP:** **IMAP** is a standard protocol that allows users to access data stored on a mail server. IMAP clients modify emails on the mail server, which will be mirrored to all IMAP client mailboxes; therefore, all the changes made to an email will be synchronized across multiple devices.

- **POP3:** **POP3** is a standard protocol that allows users to access data stored on a mail server. POP3 clients download emails from the server and save them locally, so changes made to an email will not be synchronized back to the mail server.

Set up IMAP/POP3

You can refer to the following steps to configure IMAP, POP3, and their respective ports:

1. Go to **Service > IMAP/POP3**.
2. You can adjust the following settings under the **IMAP/POP3** section:
 - **Enable POP3:** Tick to allow email client software to receive messages using POP3.
 - **Enable POP3 SSL/TLS:** Tick to allow POP3 client connection to be protected with SSL/TLS.
 - **Enable IMAP:** Tick to allow email client software to receive messages using IMAP.
 - **Enable IMAP SSL/TLS:** Tick to allow IMAP client connection to be protected with SSL/TLS.



3. Click **Apply** to save the settings.

Network Interface

After you install MailPlus Server or configure high-availability, MailPlus Server will bind with a network interface to support **High-availability cluster**. The mail service hosted on the server will run on this network interface.

Bind network interface

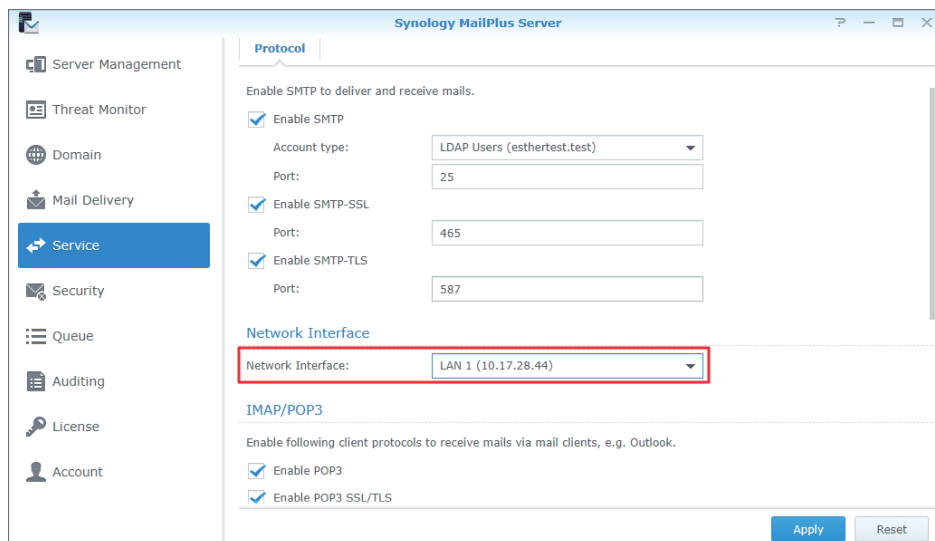
When your MailPlus Server is running on a single server, you can bind MailPlus Server with LAN, PPPoE, or a bonded network interface. When your MailPlus Server is running under a high-availability architecture, you can bind MailPlus Server with LAN or a bonded network interface. You can use **manual configuration** to retrieve the IP address of the network interface.

Note:

- When your MailPlus Server binds with a bonded network interface, you cannot unbind the bonded network interface. If you want to unbind the bonded network interface, you must first modify the network interface or uninstall MailPlus Server.

Modify network interface

- Sign in to DSM.
- Launch **MailPlus Server**.
- Go to **Service > Network Interface** and switch network interfaces from the **Network Interface** drop-down menu.



- Click **Apply** to save the settings.

After completing the basic MailPlus Server configuration during the installation stage, you may need to set up SMTP-related limits on users' login or inbound/outbound mail delivery.

Chapter 7: SMTP Settings

Service Settings

You can go to the **Mail Delivery** page to set up rules for sending and receiving emails.

MailPlus Server provides quick and convenient service setting options including the following:

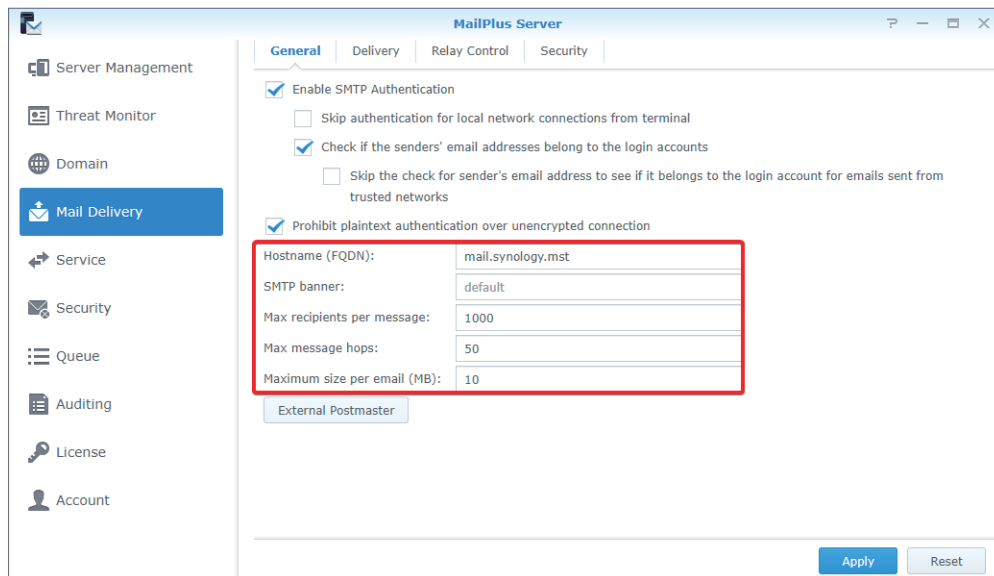
- **SMTP profile:** You can specify a hostname for MailPlus Server and an SMTP banner on a client's Telnet terminal. In addition, you can set up rules for sending and receiving emails such as specifying the maximum size per email and maximum recipients per message to avoid consuming excessive resources.
- **Full-text search:** You can enable the full-text search feature to improve the performance of mail search. This feature allows MailPlus web clients to index emails, including those with Chinese, Japanese, and Korean characters. Since the full-text search feature indexes all email content, it may require additional computing resources. You can decide whether or not to enable the full-text search feature, and further disable full-text search for specific users. For more information, please refer to [Create user policies](#).

Set up an SMTP profile

SMTP profile contains rules about how MailPlus Server sends emails to other mail servers.

1. Go to **Mail Delivery > General**.

- **Hostname (FQDN):** Specify the hostname of MailPlus Server in FQDN format. Make sure that the hostname matches the IP address in a DNS server.
- **SMTP banner:** Specify the text that will show up on an SMTP client's Telnet terminal.
- **Max recipients per message:** Set the maximum number of recipients in an inbound/outbound message. A message exceeding the limit will be rejected.
- **Max message hops:** Set the maximum number of hops (i.e., mail relays) made by an inbound/outbound message. A message exceeding the limit will be rejected.
- **Maximum size per email (MB):** Set the maximum size of an inbound/outbound message. A message exceeding the limit will be rejected.

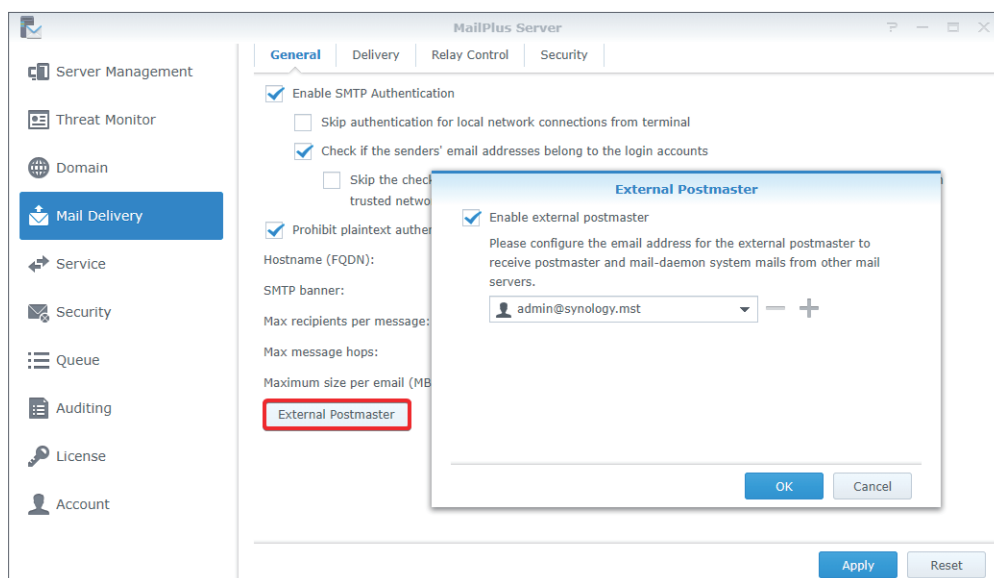


2. Click **Apply** to save the settings.

External postmaster

External postmaster is set to receive system emails sent to Mailer-daemon and Postmaster aliases from other mail servers.

1. Go to **Mail Delivery > General**.
2. Click the **External Postmaster** button.
3. Tick the **Enable external postmaster** checkbox.
4. Click the plus icon/Add button to add email addresses for external postmasters.



5. Click **OK** to save the settings.

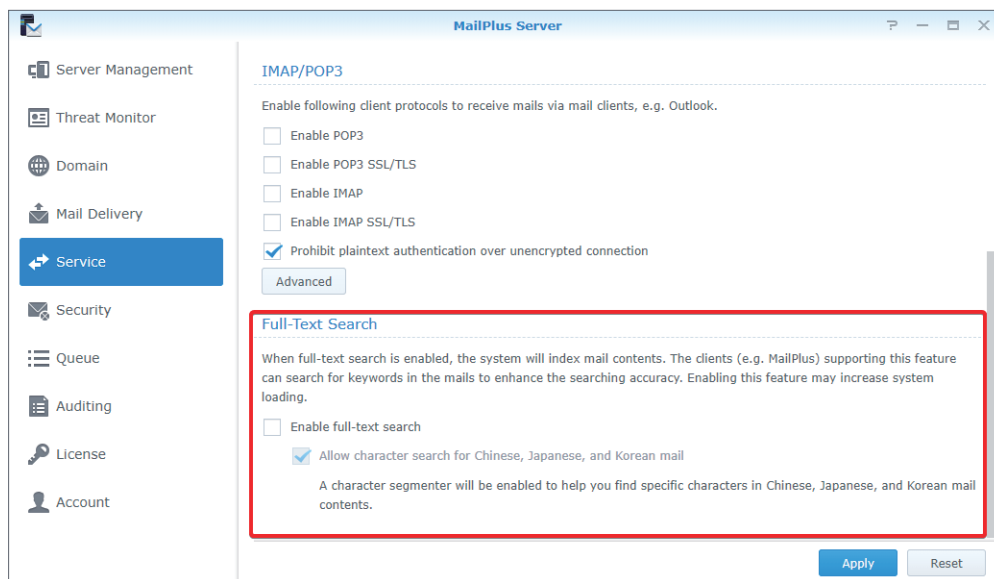
Full-text search

With full-text search enabled, the server will index email subject lines, senders, recipients, and message content, allowing you and client users to conveniently search keywords on clients supporting this feature (e.g., MailPlus).

Note:

- Enabling this feature may increase system loading when there is a large number of outbound and inbound messages.

1. Go to **Service**.
2. Under the **Full-Text Search** section, you can adjust the following settings:
 - **Enable full-text search:** When you tick this option, you can refer to [Create user policies](#) for detailed information. You can disable full-text search for specific users to avoid server load.
 - **Allow character search for Chinese, Japanese, and Korean mail:** When you tick this option, a character segmenter will be enabled to help you find specific characters in Chinese, Japanese, and Korean email content.



3. Click **Apply** to save the settings.

SMTP Secure Connection

MailPlus Server can enhance security and stability by analyzing user connection, login info, and email content. This will not only safeguard your service quality but also prevent MailPlus Server from becoming an open relay for spammers and being blacklisted consequently.

- **SMTP authentication:** With SMTP authentication enabled, users need to enter their DSM user accounts and passwords for authentication when relaying emails through the server.

Note:

- Authentication is only required for email relaying. This is to prevent becoming an open relay for spammers. For more information, please refer to [this article](#).

- **Blacklist and whitelist:** If your server continues to receive spam emails, you can set up blacklist rules to reject services for emails from certain sources. On the other hand, MailPlus Server may accidentally reject legitimate emails when [Antivirus scan](#), [Authentication](#), or other scanning features are enabled. In this case, you can use the whitelist to skip security scanning so that important emails can be received.
- **Sender policy:** You can set up criteria to reject unqualified formats or unauthenticated sender addresses.
- **Connection policy:** You can limit connections from the client IPs that cannot be identified or may cause MailPlus Server to overload.
- **Advanced settings:** During the connection phase, accurate commands and other advanced settings are required. Please refer to [Advanced settings](#) for more information.

Enable SMTP authentication

Authentication prevents malicious users from relaying spam through your mail server. We recommend enabling the user authentication feature. Users who do not pass authentication will be unable to forward their emails. This will prevent your server from being listed on blacklists.

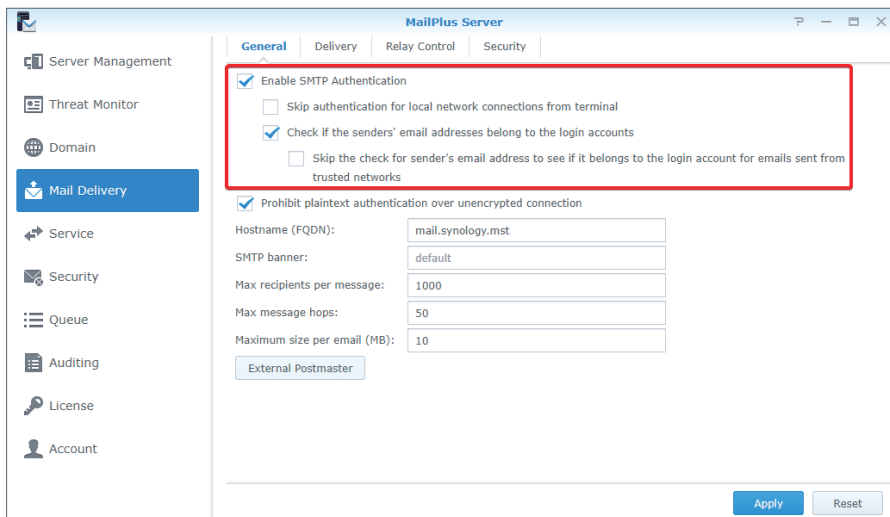
Note:

- Some features in MailPlus Server such as **Daily Quota** require authentication.

1. Go to **Mail Delivery > General** and choose whether to tick the **Enable SMTP Authentication** checkbox.
2. With the **Enable SMTP Authentication** checkbox ticked, you can adjust the following settings:
 - **Skip authentication for local network connections from terminal:** Users who use the local network to access mail services do not require authentication.
 - **Check if the sender's email addresses belong to the login accounts:** Users have to use the email addresses that belong to their login accounts to send emails.

Note:

- If you tick the **Check if the senders' email addresses belong to the login accounts** checkbox at the **General** tab, emails from the **Trusted List** might be rejected by MailPlus Server. You can go to the **General** tab and tick the **Skip the check for sender's email address to see if it belongs to the login account for emails sent from trusted networks** checkbox to skip the check. If you tick the **Skip authentication for local network connections from terminal** checkbox at the **General** tab, emails from local networks will not be blocked by MailPlus Server.



3. Click **Apply** to save the settings.

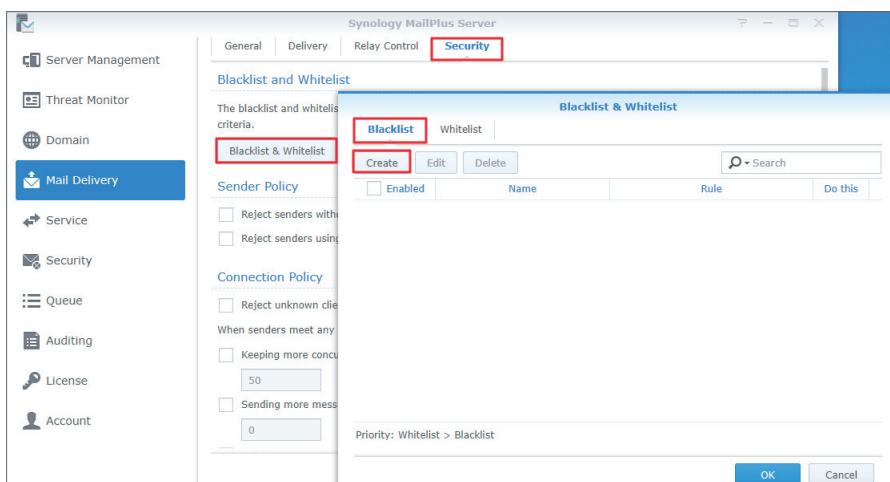
Create blacklist & whitelist

The system will take specific actions on certain messages based on various criteria specified in **Blacklist & Whitelist**. You can refer to the following steps to create rules for blacklist and white list:

Note:

- If an email message matches the criteria set in both the blacklist and whitelist, this email will be received since the whitelist takes priority over the blacklist. Please refer to the [Whitelist information and restrictions](#) section.

1. Go to **Mail Delivery > Security** and click **Blacklist & Whitelist**.
2. In the **Blacklist & Whitelist** window, you can manage your blacklist and whitelist. In this section, we will use **Blacklist** for demonstration purposes:
 - **Blacklist:** Set rules to reject/discard matching email messages.
 - **Whitelist:** Set rules to allow matching email messages to pass through.
3. At the **Blacklist** tab, click **Create**.



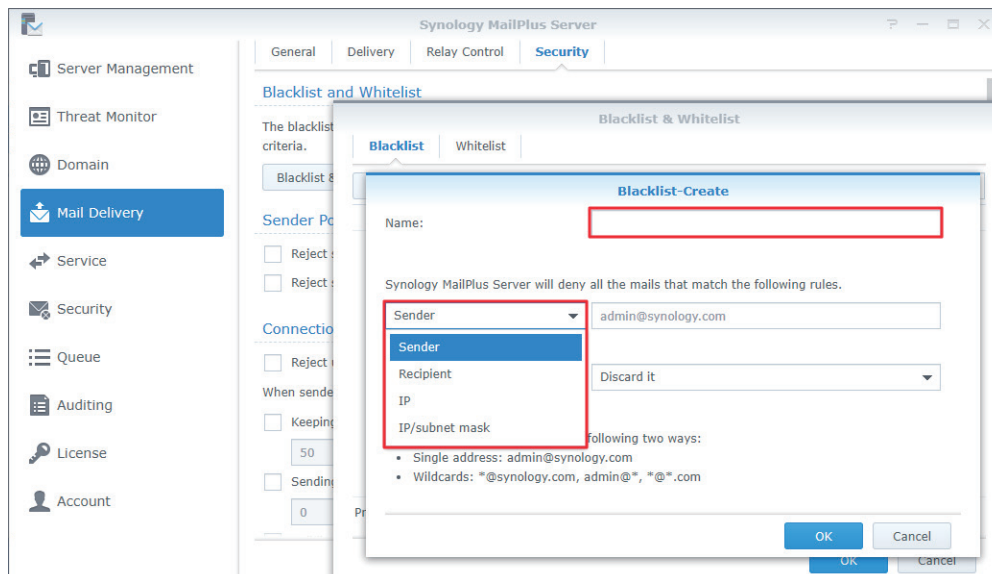
4. Name the blacklist (whitelist) rule in the **Name** field.

5. Choose a type of rule:

- **Sender:** Takes specific actions when a sender address matches the specified criteria.
- **Recipient:** Takes specific actions when a recipient address matches the specified criteria.
- **IP:** Takes specific actions when a sender IP address matches the specified criteria.
- **IP/subnet mask:** Takes specific actions when a sender IP address and its subnet mask match the specified criteria.
- **Domain:** Takes specific actions when a sender domain matches the specified criteria. This option is only available for **Whitelist**.

Note:

- The address in **Sender** is determined by the information retrieved from **MAIL FROM**.
- The address in **Recipient** is determined by the information retrieved from **RCPT TO**.

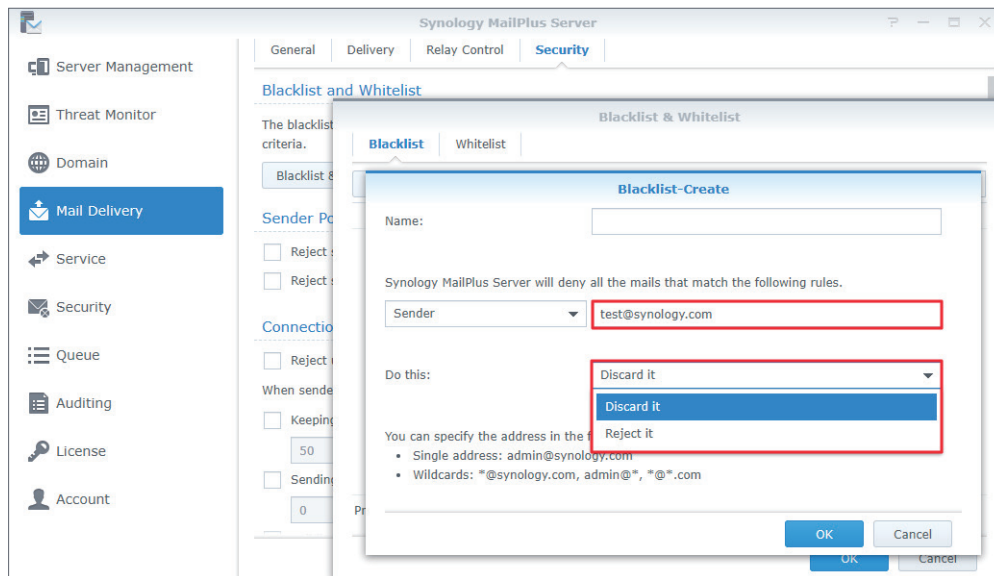


6. Specify the criteria for the selected rule type. Please refer to the grey text in the input field for the correct format. You can enter asterisks (*) when specifying the sender or recipient criteria.

7. Choose an action to take when the criteria are matched from the **Do this** drop-down menu.

Note:

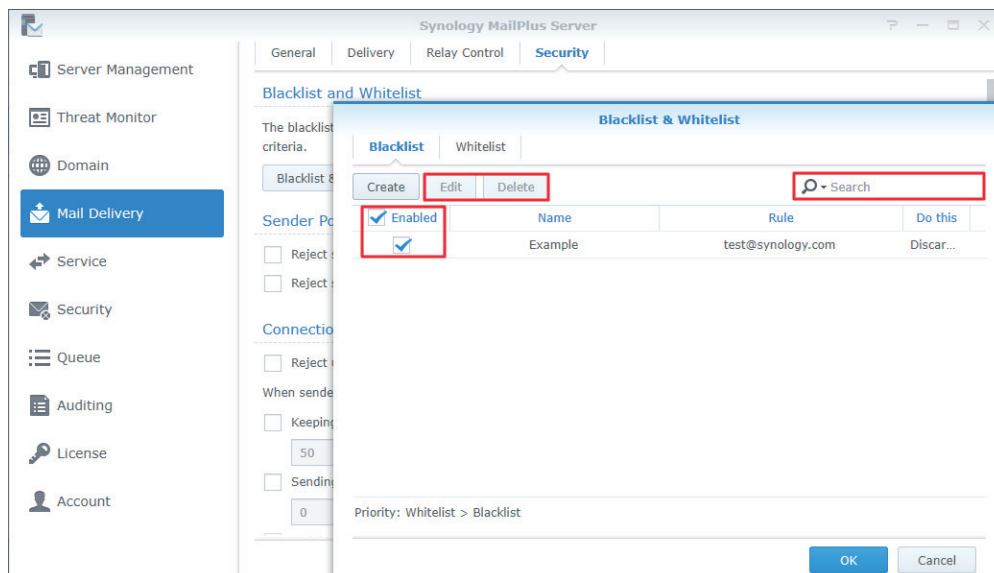
- **Whitelist** does not include this option since it always allows emails that match its criteria to be received.
- **Reject it:** Senders will be notified when their emails are rejected.
- **Discard it:** Senders will not be notified when their emails are discarded.



8. Click **OK** to complete the settings.

Edit and delete blacklist & whitelist

1. You can enter keywords in the search field in the upper-right corner of the **Black & White List** window to search for the blacklist or whitelist you want to modify.
2. You can tick the **Enabled** checkbox to enable or disable a rule. (You do not need to delete the rule from the blacklist or whitelist.)
3. When you need to edit or delete a specific rule, select the rule first and click **Edit** or **Delete**.
4. Click **OK** to save the settings.



Whitelist information and restrictions

Whitelist settings may skip the tests that are required for blacklists. Moreover, depending on the type of settings, it may also skip DNSBL, SPF, antivirus scans, DKIM, and DMARC tests. The following table shows which tests will be skipped based on the different whitelist settings:

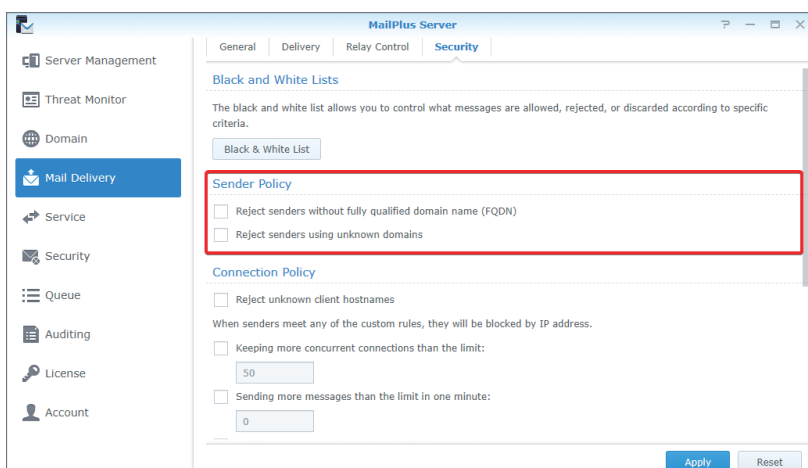
	DNSBL	SPF	Antivirus Scans	DKIM	DMARC	smtpd_*_restrictions
IP	✓	✓	✓	✓	✓	✓
IP/subnet mask	✓	✓		✓	✓	✓
Sender		✓	✓			✓
Recipient		✓	✓			✓
Domain		✓	✓	✓	✓	✓

Note:

- There are certain tests the whitelist will not skip, emails that do not pass these tests will fail to be delivered. For example, when the sender *admin@example.com* is on the whitelist, since the sender rule does not support DNSBL, DKIM, and DMARC, it must pass DNSBL, DKIM, or DMARC tests to avoid delivery failure.
- If you wish to skip all the tests listed in the table, we recommend that you set up whitelist rules based on IP address.

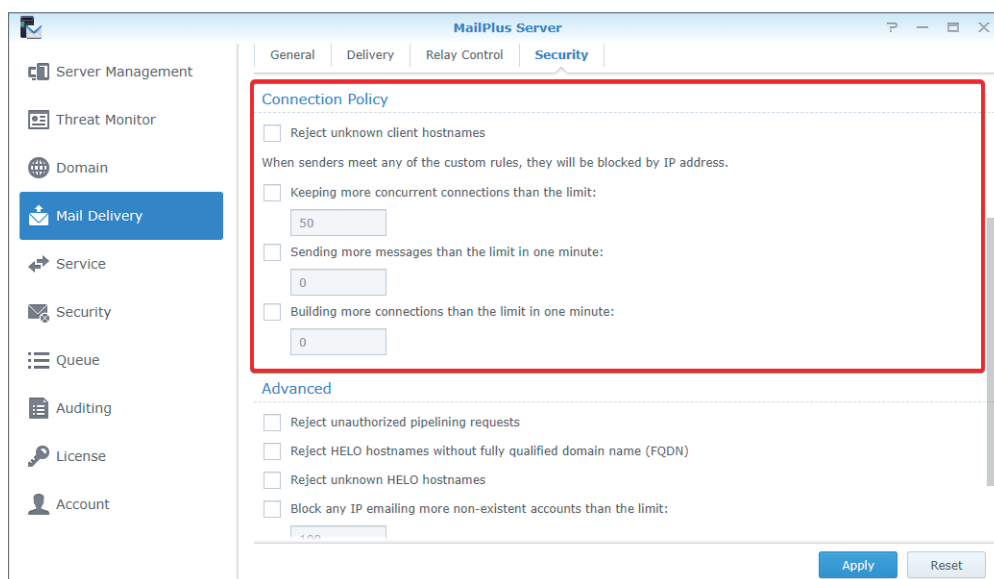
Sender policy

1. Go to **Mail Delivery > Security**.
2. Under the **Sender Policy** section, set up certain criteria to reject emails. The policies include the following:
 - **Reject senders without fully qualified domain name (FQDN):** When a sender's domain name from **MAIL FROM** does not match the RFC standard FQDN format, emails will be rejected.
 - **Reject senders using unknown domains:** When MailPlus Server is not the final receiving terminal and a sender domain from **MAIL FROM** does not match any DNS A record and MX record, or when the MX record is incorrect, emails will be rejected.



Connection policy

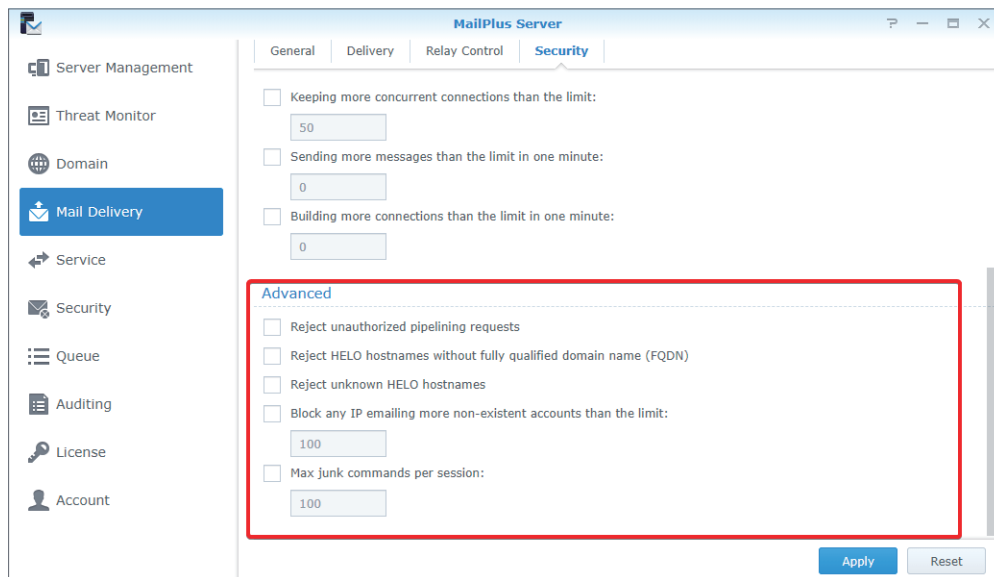
1. Go to **Mail Delivery > Security**.
2. Under the **Connection Policy** section, set up the criteria to restrict client connections or block suspicious IP addresses. The policies include the following:
 - **Reject unknown client hostnames:** When an IP address or a client hostname is incorrect or does not exist, the client connection to MailPlus Server will be rejected.
 - **Keeping more concurrent connections than the limit:** You can set the maximum concurrent connections for the server. When the number of concurrent connections with the same IP address exceeds this number, connections will be blocked until the total number is lower than the limit.
 - **Sending more messages than the limit in one minute:** You can set the maximum number of email messages that can be sent within one minute. When the number of emails sent within one minute from the same IP address exceeds this number, emails from this IP address will be blocked until the next minute starts.
 - **Building more connections than the limit in one minute:** You can set the maximum number of connections within one minute. When the number of connections with the same IP address exceeds this number within one minute, connections will be blocked until the next minute starts.



Advanced settings

1. Go to **Mail Delivery > Security**.
2. Under the **Advanced** section, you can adjust security settings for mail delivery:
 - **Reject unauthorized pipelining requests:** Rejects connections that keep sending SMTP requests.
 - **Reject HELO hostnames without fully qualified domain name (FQDN):** Rejects connection when hostnames have incomplete domain names during HELO or EHLO.

- **Reject unknown HELO hostnames:** Rejects connection when hostnames do not have DNS A record or MX record during HELO or EHLO.
- **Block any IP emailing more non-existent accounts than the limit:** Blocks the IP address of a user until the next day when the user using the same IP address on the same day sends emails, exceeding the specified limit, to non-existent accounts in MailPlus Server.
- **Max junk commands per session:** When the number of connected clients exceeds the specified number of junk commands (i.e., NOOP, VRFY, ETRN, and RSET) within the same session, every 10 junk commands will cause a one-second delay on mail delivery.



Mail Relay

If you want to send emails via other servers or send/receive emails for other servers, you can configure mail relay, SMTP authentication, encryption, and other provided security features.

Set up delivery control

At the **Delivery** tab, you can configure settings of MailPlus Server to relay emails through a specific server, allowing all outgoing emails to be sent through the specified server.

1. Go to **Mail Delivery > Delivery > Relay Settings**.
2. Select a rule type:
 - **Send mails directly from this server:** All emails will be sent by MailPlus Server directly.
 - **All mails are sent through a single relay host:** All emails will be sent by the relay server that you specify below. Enter the IP address or hostname of the relay server in the **Server** field and its port number in the **Port** field. After ticking this option, you can adjust the following security settings:

- **Always use a secure connection (TLS):** MailPlus Server sends STARTTLS to enable encrypted connections. If MailPlus Server is the relay server, please refer to [here](#). In MailPlus Server, the default TLS security level is **may**.
- **Authentication required:** If your relay server has enabled authentication, please enter the account and password of the relay server to use it for mail relay.

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

Note:

- STARTTLS and SMTPS differ. If you want to use SMTPS, MailPlus Server does not provide an interface to configure this. Please refer to [wrappermode](#) to configure the settings.

Emails matching a certain rule specific email addresses or domains can be sent through a designated relay server. You can click the **Relay Host List** button under **Relay Exceptions** to adjust recipient and sender rules.

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

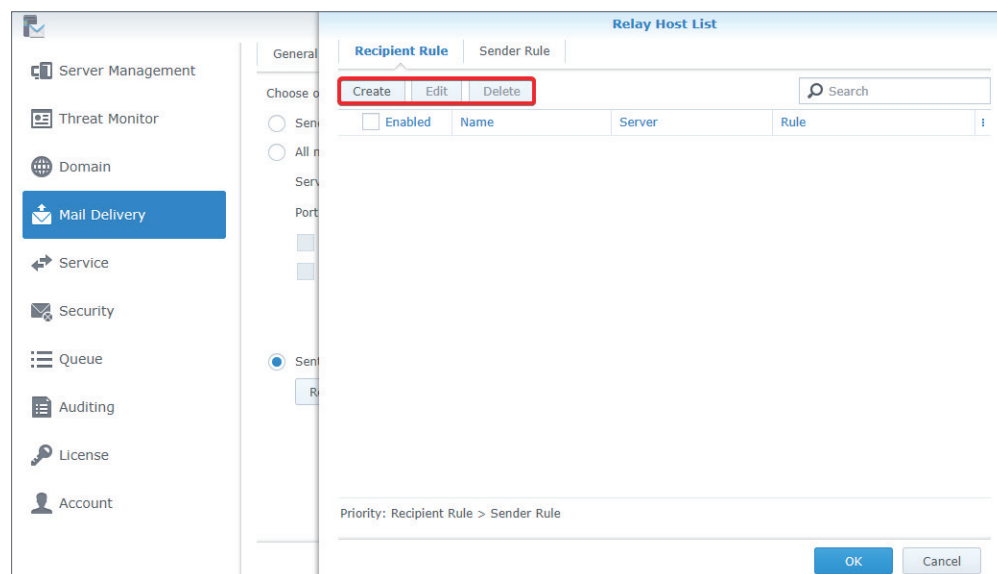
Set up relay rules for specific addresses or domains.

[Relay Host List](#)

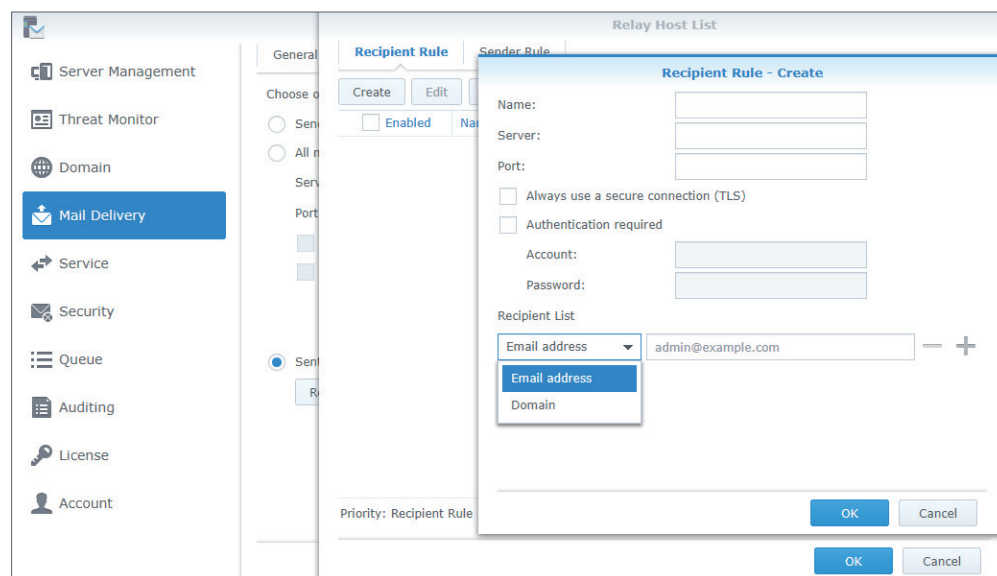
Apply Reset

- **Recipient Rule:** Emails sent to the specified email addresses or domains will be sent through a designated relay server. The priority of recipient rules will be higher than that of sender rules.

- **Sender Rule:** Emails sent from the specified addresses or domains will be sent through a designated relay server.
- Click the **Create**, **Edit**, or **Delete** button to manage recipient and sender rules.



- Enter a rule name and specify a relay server and port.
- Edit the **Recipient List** by selecting an email address or domain so emails relayed to the server will be received at the specified email addresses or domains.
- Click **OK** to save the settings.



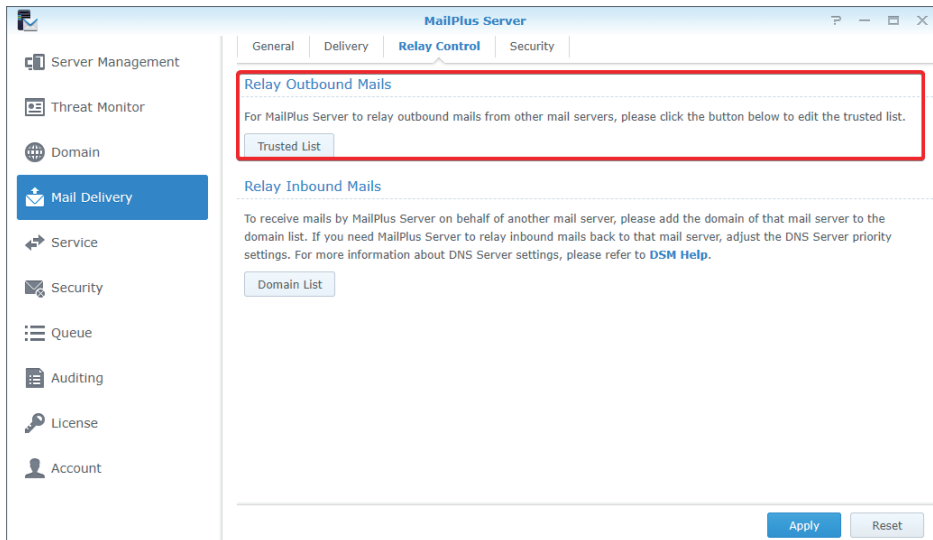
- Click **Apply** to finish the settings.

Set up relay control

At the **Relay Control** tab, you can adjust MailPlus Server settings, so it can send or receive emails for multiple mail servers.

- **Relay outbound emails for other mail servers:**

1. Go to **Mail Delivery > Relay Control**.
2. Click the **Trusted List** button under the **Relay Outbound Mails** section.



3. Click **Create** and enter a rule name. Specify the IP address or subnet mask of other mail servers.
4. Click **OK** to save the settings.

Note:

- If you tick the **Check if the senders' email addresses belong to the login accounts** checkbox at the **General** tab, emails from the **Trusted List** might be rejected by MailPlus Server. You can go to the **General** tab and tick the **Skip the check for sender's email address to see if it belongs to the login account for emails sent from trusted networks** checkbox to skip the check. If you tick the **Skip authentication for local network connections from terminal** checkbox at the **General** tab, emails from local networks will not be blocked by MailPlus Server.

Relay inbound emails for other mail servers

To relay inbound emails for other mail servers, please set up a DNS record first. You may refer to the following steps and go to **Domain List** to add a mail server. Here we use one external server and one internal server as an example.

1. Set up an external DNS server for MailPlus Server. Here we use Bluehost® as an example.
2. After logging in to Bluehost®, adjust the following settings. Enter your domain name in the MX record on the external DNS server and enter the IP address of MailPlus Server in the A record. In this way, other mail servers will be able to send emails to MailPlus Server based on these DNS records.

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	

- Set up an internal Synology DNS Server for MailPlus Server to find your primary mail server.
- Enter your domain name in the MX record on the internal DNS server and enter the IP address of the domain in the A record. The priority of the DNS records on the internal DNS server must be higher than that on the external DNS server.

DNS Server

Zones

Resolution

Log

Keys

Views

Settings

Create

Edit

Export zone

Delete

Status

Enabled

Edit Resource Record

Create

Edit

Delete

Search

Name	Type	TTL	Information
mail.mailplustest.com.	A	86400	172.22.1.16
mailplustest.com.	MX	86400	10 mail.mailplustest.com.

Edit Resource Record MX

If left blank, the name of the resource record will be the same as the domain name.

Name:

mailplustest.com

TTL:

86400

seconds

Priority:

10

Host/Domain:

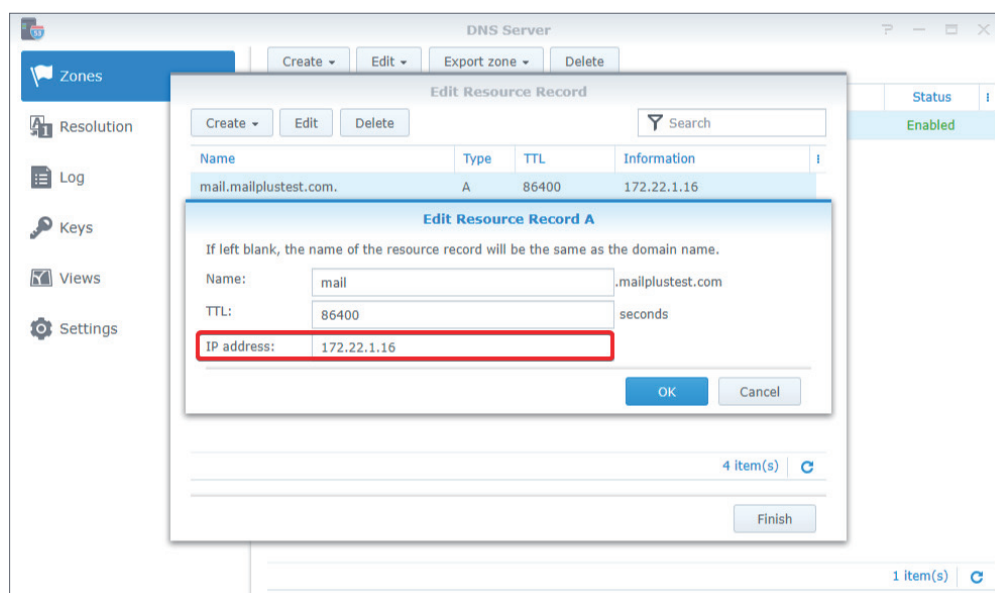
mail.mailplustest.com

OK

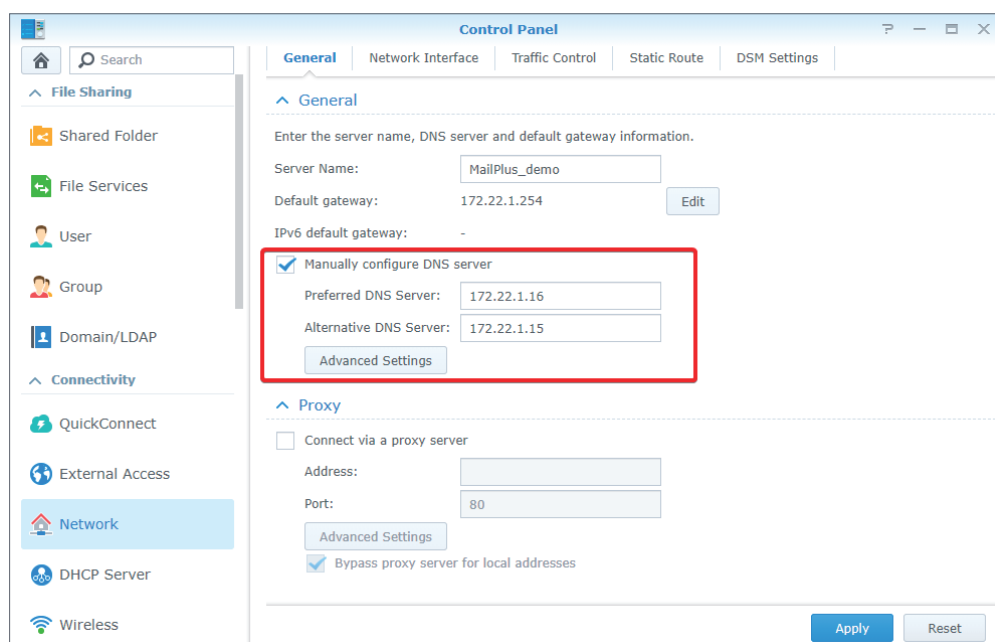
Cancel

Finish

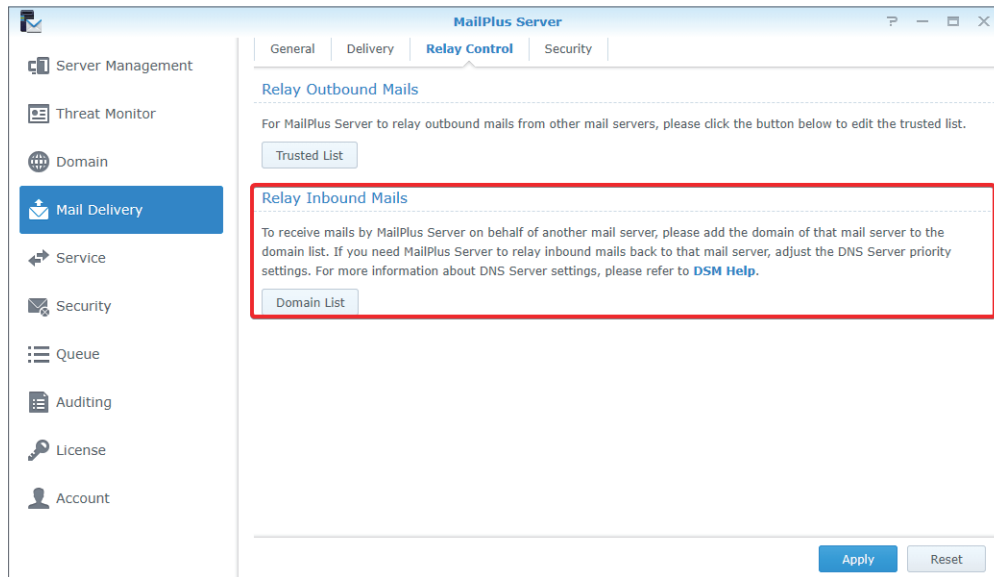
1 item(s)



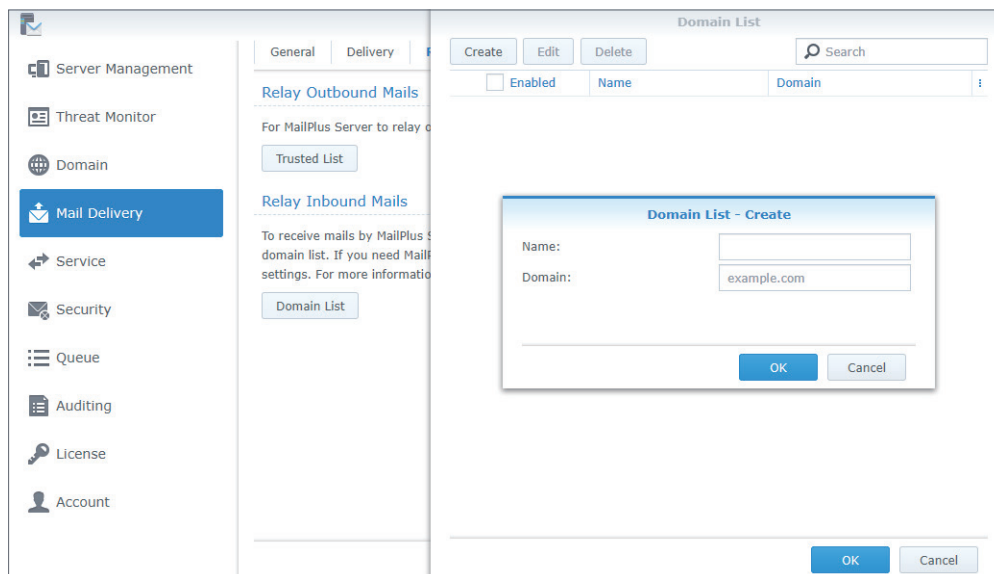
- Go to **DSM > Control Panel > Network > General** and tick the **Manually configure DNS server** checkbox. Enter the IP address of the internal DNS server in the **Preferred DNS Server** field and the IP address of the external DNS server in the **Alternative DNS Server** field to make sure the internal and external connections of MailPlus Server can work properly. After MailPlus Server receives emails, it will check the MX records of the two DNS servers and send emails to the mail server with the higher priority.



- Launch MailPlus Server and go to **Mail Delivery > Relay Control**. Under the **Relay Inbound Mails** section, click the **Domain List** button.



- Click the **Create** button.
- Enter the rule name and domain.



- Click **OK** to save the settings.

Note:

- Although emails are sent internally, you should configure the security settings at the **Spam** and **Antivirus** tabs of the **Security** page to avoid malicious emails.
- Since security settings are turned on, you can add emails to the whitelist at **Mail Delivery > Security** to avoid blocking.
- The network segment of all servers should be the same.

Chapter 8: Domain Settings

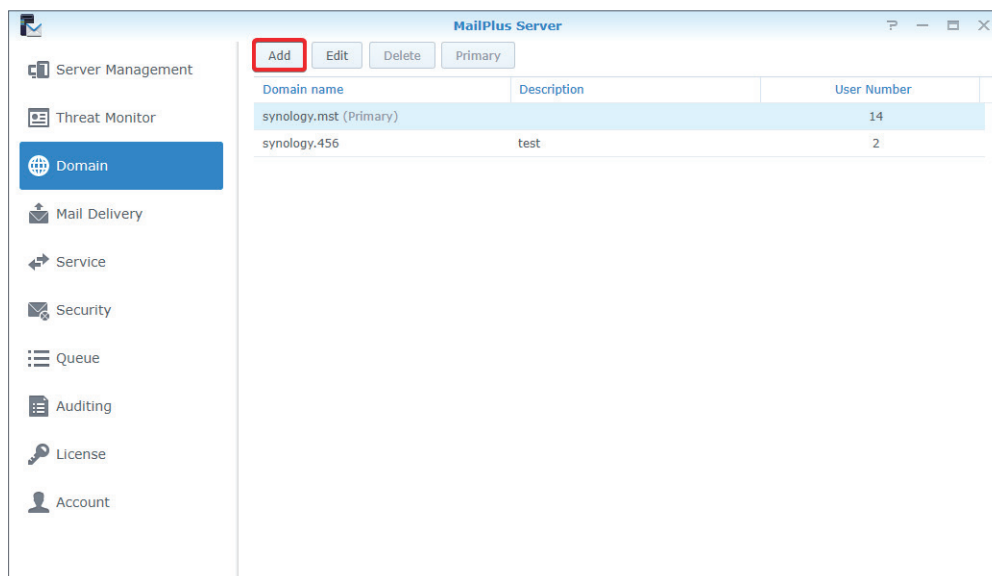
Domain

You can host multiple email domains in a single MailPlus Server to centralize emails sent to your domains. You can also customize aliases, auto BCC, usage limits, and disclaimers for each domain.

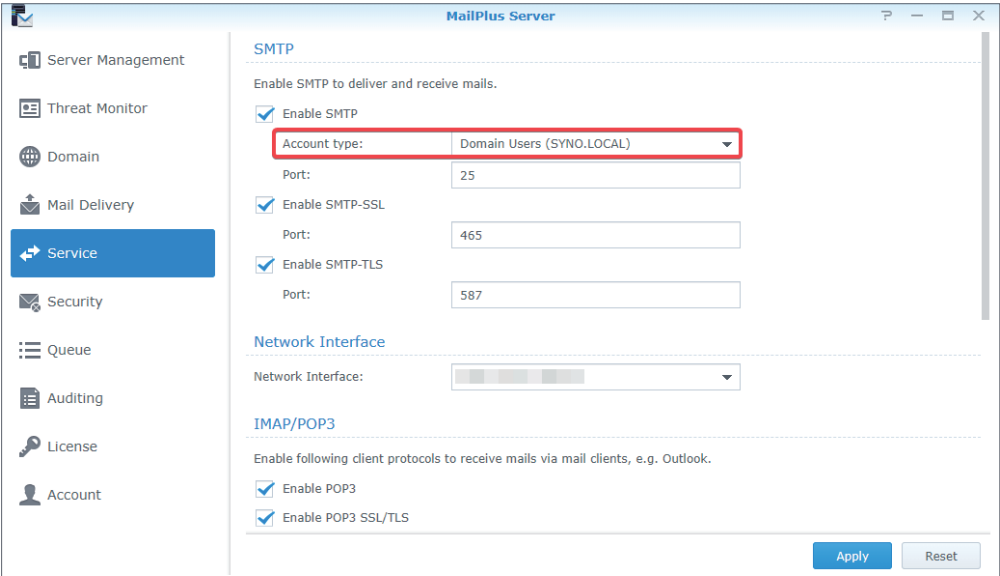
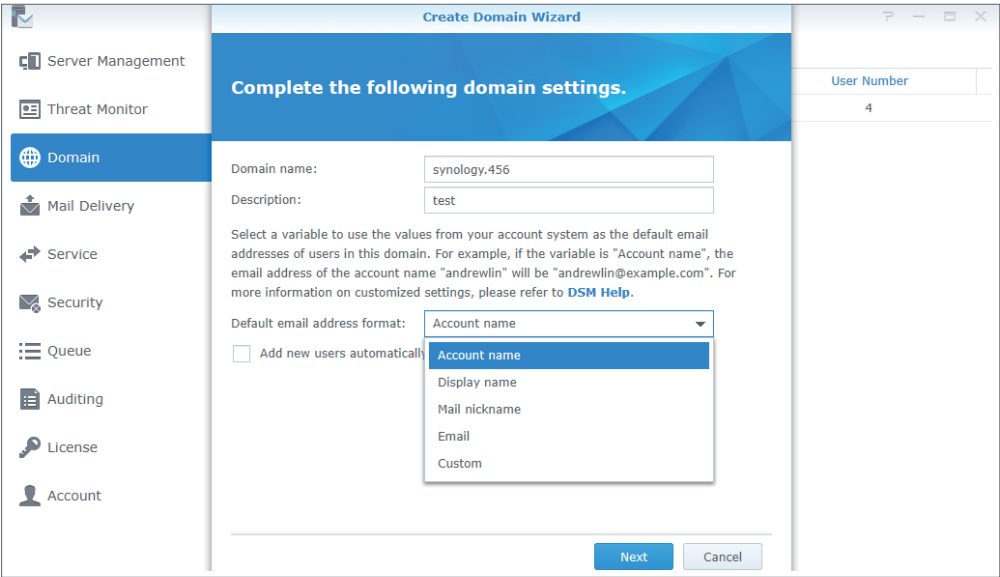
Create a domain in MailPlus Server

Sign in to MailPlus Server and go to **Domain** to create a new domain. In this chapter, *synology.456* will be used for demonstration purposes.

1. Go to **Domain** and click the **Add** button.



2. Fill in the domain name *synology.456* and its description.
3. When adding members to the domain, MailPlus Server will fetch information from the account system based on the settings of **Default email address format**. You may choose **Account name**, **Display name**, **Mail nickname**, **Email**, or **Custom** according to the account type you set at **Service > SMTP > Account type**.



The following table shows the default settings MailPlus Server provides for each account type.

Account type	Default settings
Local users	Account name Mail nickname
LDAP users	Account name Mail nickname
Domain users	Account name Display name Mail nickname Email

4. In addition to the above options, you can select **Custom** to enter variables in the **Custom variables** field as the default email address formats. The following table shows the variables that MailPlus Server supports:

Variable	Value
<a>	Account name
<g>	Given name
<i>	Middle initial
<s>	Surname
<d>	Display name
<m>	Mail nickname
<xa>	Uses the first x letters of an account name. For example, if x = 2, the first two letters of the account name will be used.
<xs>	Uses the first x letters of a surname. For example, if x = 2, the first two letters of the surname will be used.
<xg>	Uses the first x letters of a given name. For example, if x = 2, the first two letters of the given name will be used.
<custom attribute>	You can also enter a variable supported by your account system to fetch the corresponding value.

The variables supported by MailPlus Server vary according to the selected account system at **Service > SMTP**. For more details, please refer to the following table:

Variable	Local Users	LDAP Users	Domain Users
<a>	O	O	O
<g>	X	X	O
<i>	X	X	O
<s>	X	X	O
<d>	X	X	O
<m>	O	O	O
<xa>	O	O	O
<xs>	X	X	O
<xg>	X	X	O
<custom attribute>	X	O	O

5. Users can tick the **Add new users automatically to this domain** checkbox to add new

users automatically to the domain. MailPlus Server will fetch the information to compose user email addresses based on the default email address format.

The screenshot shows the 'Create Domain Wizard' window with the title 'Complete the following domain settings.' The left sidebar contains navigation links: Server Management, Threat Monitor, Domain (selected), Mail Delivery, Service, Security, Queue, Auditing, License, and Account. The main content area has the following fields and options:

- Domain name:
- Description:
- Text: Select a variable to use the values from your account system as the default email addresses of users in this domain. For example, if the variable is "Account name", the email address of the account name "andrewlin" will be "andrewlin@example.com". For more information on customized settings, please refer to [DSM Help](#).
- Default email address format:
- ☒ Add new users automatically to this domain (highlighted with a red box)

At the bottom right are 'Next' and 'Cancel' buttons. On the right side of the window, there is a 'User Number' table:

User Number
14
2

6. After the setup, click **Next**.

7. Add users to this domain and click **Next** to check the members in *synology.456*.

The screenshot shows the 'Create Domain Wizard' window with the title 'Select the members to add to this domain.' The left sidebar is the same as in the previous screenshot. The main content area has the following elements:

- Search:
- List of users with checkboxes:
 - ☐ User (dropdown)
 - ☐ admin
 - ☐ alex1111
 - ☐ Andrewtan
 - ☐ dieselt
 - ☐ dilystai
 - ☐ jakechen
 - ☐ jomi
 - ☐ milesc
 - ☐ normalboy
 - ☐ Oliviachen
 - ☐ nadtraint

At the bottom are 'Back', 'Next', and 'Cancel' buttons. The 'User Number' table on the right is the same as in the previous screenshot.

8. Click **Apply** to save the settings.

Domain Management

MailPlus Server provides management settings for administrators and users in each domain.

- **General:** You can edit domain name and domain description, change default email address format, create an additional domain, enable DKIM signing on outbound emails, and activate Catch-all to receive emails sent to non-existent email addresses or email addresses not activated in a specific domain.
- **User Accounts:** You can add new members to a domain and select roles such as **Domain Administrator** and **Regular User** for users under this domain.
- **Group Accounts:** You can add members as a group to a domain so the users in this group can have the same role settings.
- **Alias:** You can create an alias for one or multiple recipients. When an email is sent to an alias, the server will automatically deliver it to all users in the alias. External email addresses can be included in an alias.
- **Auto BCC:** You can let the system automatically send a BCC (Blind Carbon Copy) to a specific address based on certain criteria for senders, recipients, or all messages.
- **Sending Limit and Daily Quota:** You can restrict the number of outbound messages and set up traffic limits.
- **Disclaimer:** You can configure conditions to apply disclaimers and customize the content to meet different requirements. A disclaimer will be automatically appended to the end of outbound email content based on the settings you set.

Edit general settings for a domain

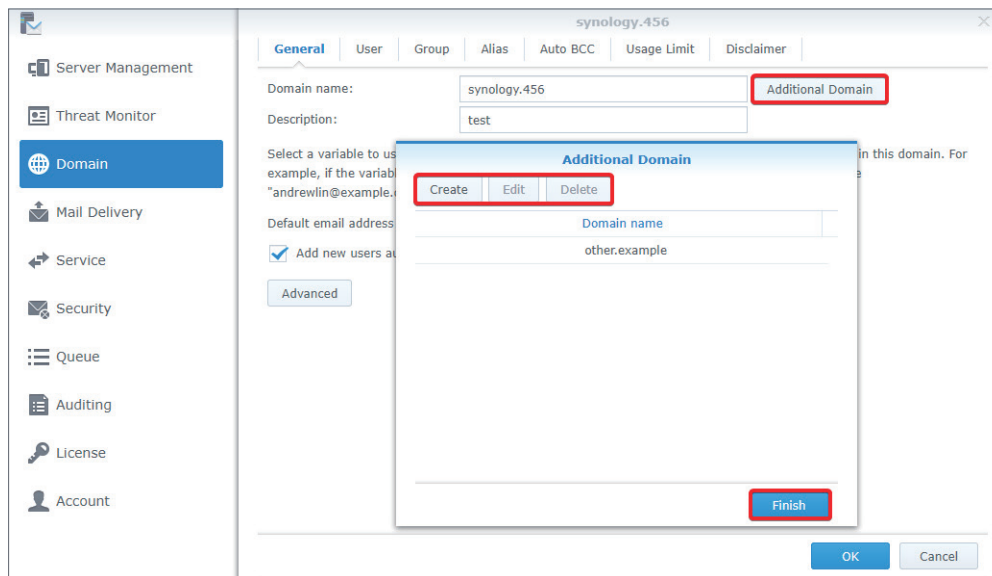
At the **General** tab, you can edit domain information, adjust default email address format, and add new users automatically to *synology.456*.

The screenshot shows the 'General' tab of the domain settings for 'synology.456'. The left sidebar contains navigation links: Server Management, Threat Monitor, Domain (selected), Mail Delivery, Service, Security, Queue, Auditing, License, and Account. The main panel has tabs for General, User, Group, Alias, Auto BCC, Usage Limit, and Disclaimer. The 'General' tab is active, showing fields for 'Domain name' (synology.456) and 'Description' (test). Below these is a text area explaining variable selection for the default email address format, with a dropdown menu set to 'Account name'. A checkbox 'Add new users automatically to this domain' is checked. An 'Advanced' button is visible. At the bottom right are 'OK' and 'Cancel' buttons.

Create and edit additional domains

In the **Additional Domain** window, you can create additional domain names for the host to receive emails. The settings of additional domains will follow the settings of *synology.456*.

1. Go to **Domain** > *synology.456* > **General** and click the **Additional Domain** button.
2. Click the **Create** button to create an additional domain. If you want to edit or delete, please select your target domain and click the corresponding action buttons.
3. In the **Additional Domain** page, you can view all the additional domains you have created. Using the example above, in addition to receiving emails from domain *synology.456*, you can receive emails of an additional domain if it is included as a recipient.
4. Click **Finish** to save the settings.



Note:

- MX records on DNS Server may require relevant adjustments.

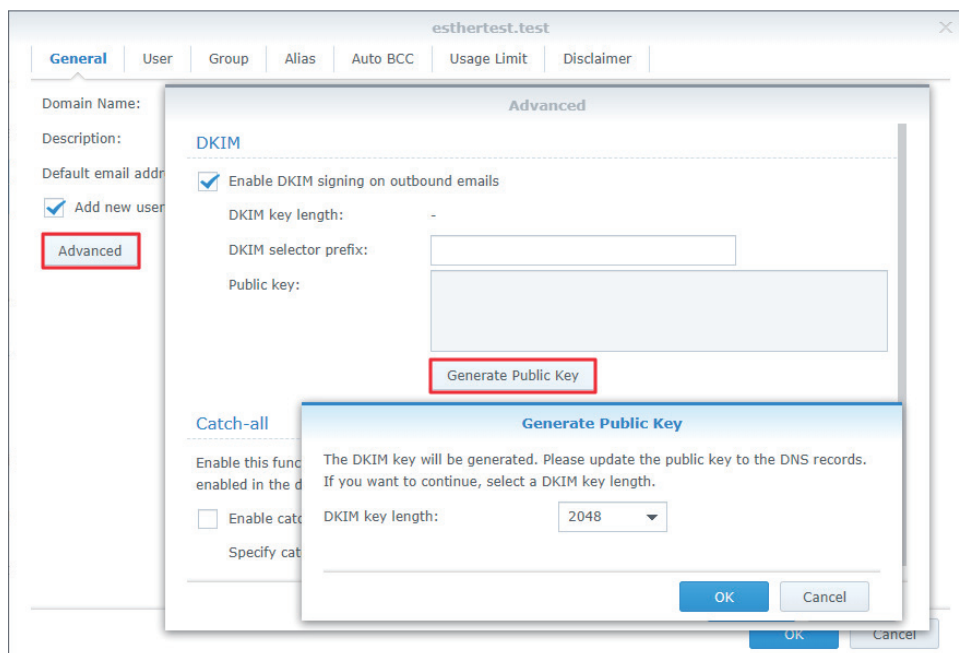
Adjust advanced settings

1. Go to **Domain** > *synology.456* > **Edit** > **General** and click the **Advanced** button.
2. In the pop-up **Advanced** window, you can adjust the settings of **DKIM** and **Catch-all** for *synology.456*.

- **DKIM:** You can enable DKIM signing to prevent messages from being modified and also avoid identity theft.
 - a. Under the **DKIM** section, tick the **Enable DKIM signing on outbound emails** checkbox if you want to prevent identity theft and make recipients trust your delivered messages. You can adjust the DKIM signature as below:
 - **DKIM selector prefix:** The prefix added to a DKIM signature. You can enter a DKIM selector prefix as you like.
 - **Public key:** The content of a public key. If the system does not have a public key and private key when you enable DKIM signing, keys will be automatically generated.
 - b. Click the **Generate Public Key** button to generate a new set of the public key and private key. By default, the system generates 2048-bit keys. (If the DKIM key gets rejected, please change the key length to 1024 or 512 bits.)

Note:

- Existing keys will be deleted after you click the **Generate Public Key** button.



- c. Click **OK** to save the settings. In addition, to ensure that DKIM signatures can be authenticated by other receiving servers, you need to create a DNS TXT record to allow DKIM authentication:

The format of a TXT record value: **v=DKIM1; k=rsa; p=DKIM public key**

For example, if the domain of MailPlus Server is *example.com*, the DKIM selector prefix is *abc*, and the public key generated by the system is *MIGfMA0GCSqGSIb3DQE*, your TXT record should be as follows:

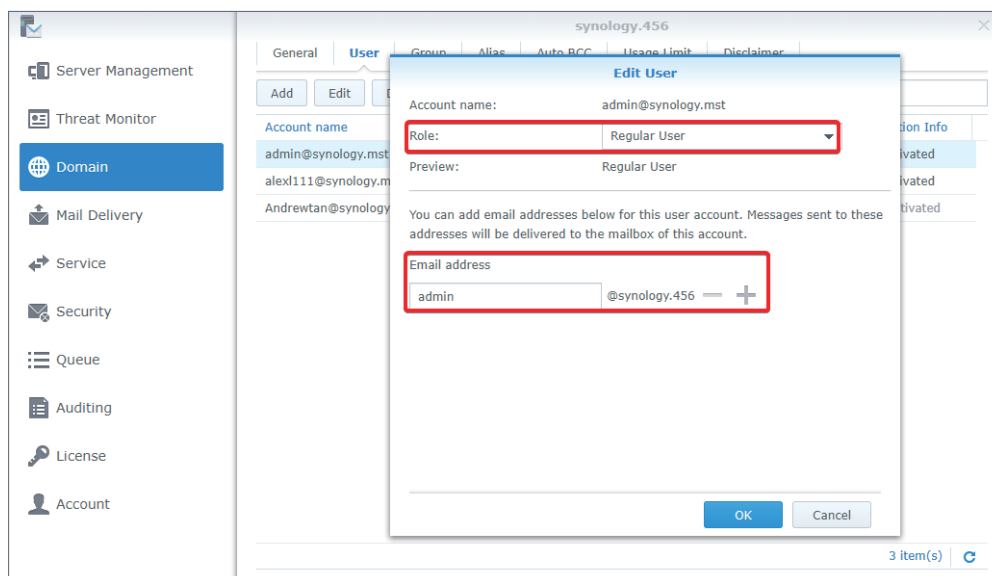
- **TXT record name:** *abc_domainkey.example.com*
- **TXT record value:** *v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQE*
- **Catch-all:** Enable **Catch-all** to make a user account serve as the catch-all mailbox to receive emails that are sent to email addresses that do not exist or are not enabled in the domain.

Add user accounts to a domain

1. Go to **Domain**, select *synology.456*, and click **Edit**.
2. Go to the **User** tab and click **Add**.
3. Select user accounts.
4. Confirm the email addresses of the selected users.

Edit and remove user accounts

1. Go to **Domain**, select *synology.456*, and click **Edit**.
2. At the **User** tab, select an account and click **Edit**.
3. In the **Edit User** window, adjust the following settings:
 - **Role:** Select a role from the drop-down menu:
 - **Domain Administrator:** Domain administrators can manage all domain settings except for creating and deleting domains.
 - **Regular User:** Regular users do not have the privilege to manage domains.
 - **Follow group settings:** The privileges will be determined by the user's group settings in the domain.
 - **Email address:** You can enter multiple email addresses. Messages sent to these addresses will be delivered to the mailbox of this account.



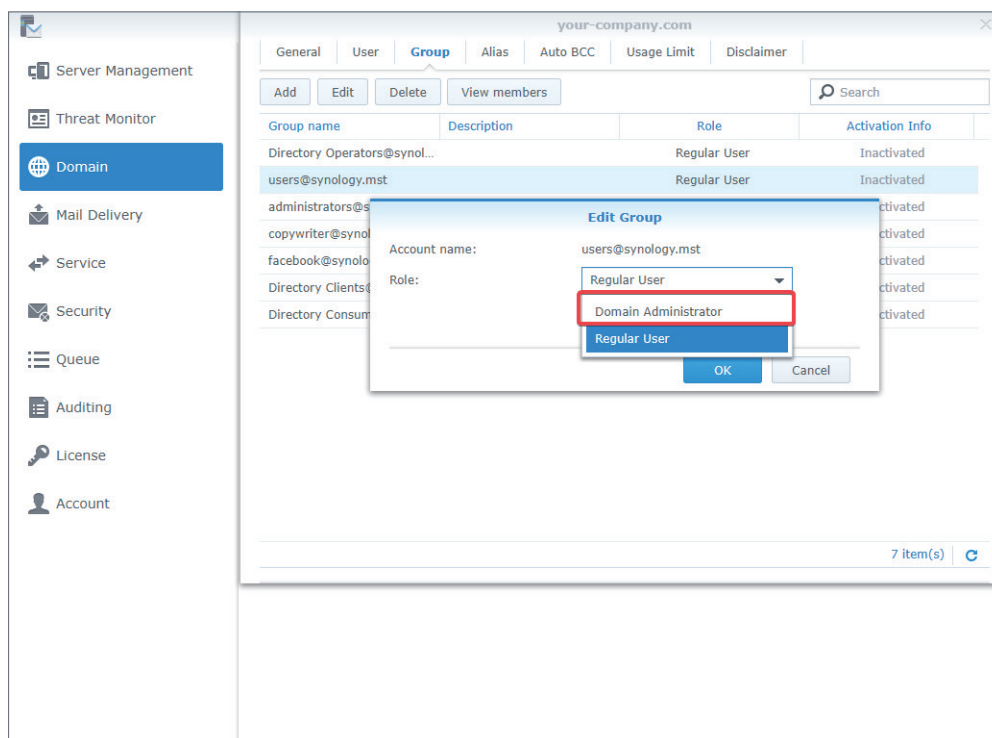
4. If you want to remove a user account, select the target user account and click the **Delete** button.

Add groups to a domain

1. Go to **Domain**, select *synology.456*, and click **Edit**.
2. Go to the **Group** tab and click **Add**.
3. Select user groups and click **Next**.
4. Confirm the email addresses of the members. Click **Apply**.

Edit and remove groups

1. Go to **Domain**, select *synology.456*, and click **Edit**.
2. At the **Group** tab, select a group you want to edit and click **Edit**.
3. In the **Edit Group** window, you can select **Domain Administrator** from the **Role** drop-down menu, so all the users in the group will have the **Domain Administrator** permission.

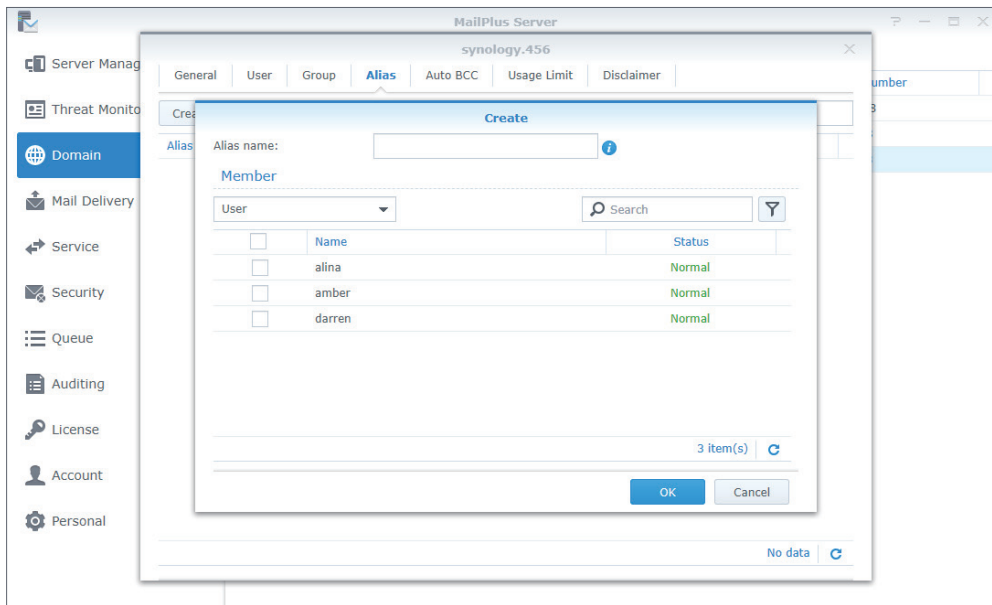


4. You can select the group you want to remove and click the **Delete** button.
5. You can click the **View members** button to check if certain users belonging to the group are not in this domain.

Create aliases

You can create aliases to allow users to send emails to multiple recipients using one alias.

1. Go to **Domain**, select *synology.456*, and click **Edit**.
2. Go to **Alias** and click the **Create** button.
3. Enter the name of the alias in the **Alias name** field.
4. Select from the drop-down menu to view aliases, users, groups, or external mailboxes.



5. Add users to the alias by ticking the checkboxes.
6. You can choose users from more than one source, including user accounts, group accounts, and other aliases.
7. Click **OK** to save the settings.

Edit and delete aliases

Please refer to the following steps to edit or delete an alias:

1. Go to **Domain**, select *synology.456*, and click **Edit**.
2. Go to **Alias** and select the alias you want to modify. (You can also search for aliases in the search bar in the upper-right corner of the page.)
3. Click the **Edit** or **Delete** button.

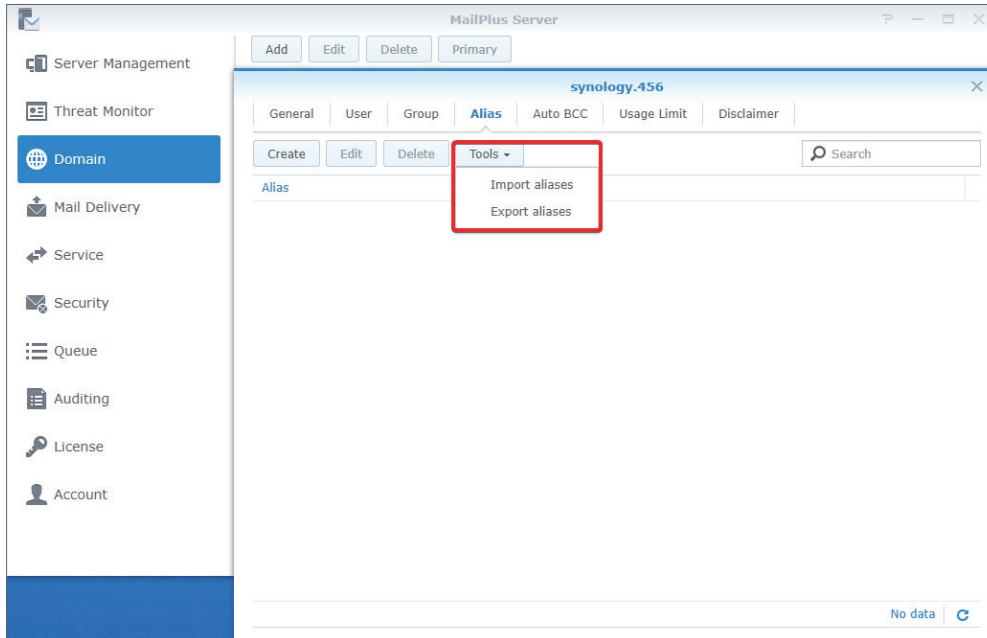
Import/export aliases

If you want to import existing alias lists or alias lists that you previously created, please refer to the following steps:

1. Go to **Domain**, select *synology.456*, and click **Edit**.
2. Go to **Alias** and click the **Tools** button.

3. Choose to import or export aliases:

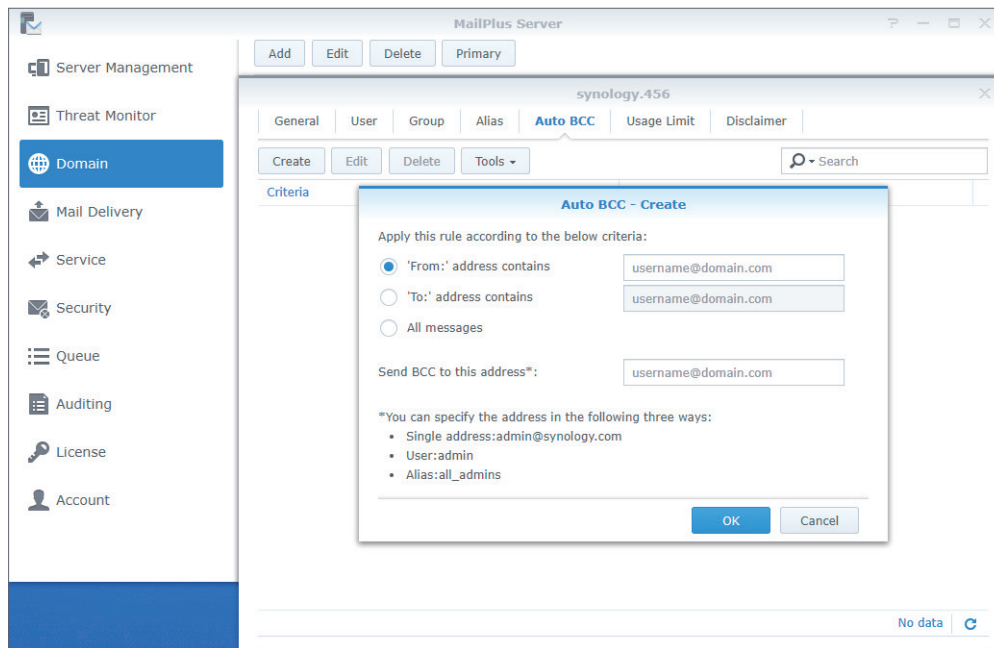
- **Import aliases:** If an imported alias name already exists, this alias will not be imported or updated.
- **Export aliases:** Alias files will be exported and downloaded in the Postfix format.



Create Auto BCC rules

The Auto BCC settings allow you to send a BCC (Blind Carbon Copy) to a specific address based on certain criteria for senders, recipients, or all messages. Please refer to the following steps to create an Auto BCC rule:

1. Go to **Domain**, select *synology.456*, and click **Edit**.
2. Go to **Auto BCC** and click the **Create** button.
3. Specify the Auto BCC criteria:
 - **From:' address contains:** BCC will be automatically sent if the **MAIL FROM** information in the original email content matches the information entered here.
 - **To:' address contains:** BCC will be automatically sent if the **RCPT TO** information in the original email content matches the information entered here.
 - **All messages:** BCC will be automatically sent for all emails except for notification emails from the internal system.
4. Enter the address where the BCC will be automatically sent to in the **Send BCC to this address*** field.
5. You can enter email addresses, user accounts, or aliases.



6. Click **OK** to save the settings.

Edit and delete Auto BCC rules

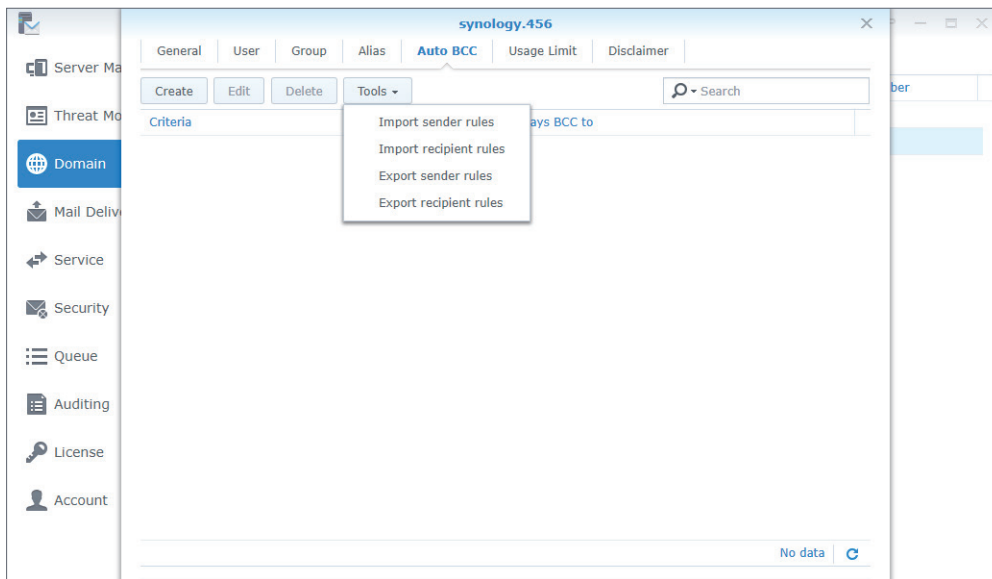
Please refer to the following steps to edit or delete Auto BCC rules:

1. Go to **Domain**, select *synology.456*, and click **Edit**.
2. Go to **Auto BCC** and select the Auto BCC rule you want to modify.
3. Click the **Edit** or **Delete** button.

Import/export Auto BCC rules

Please refer to the following steps to import or export Auto BCC rules:

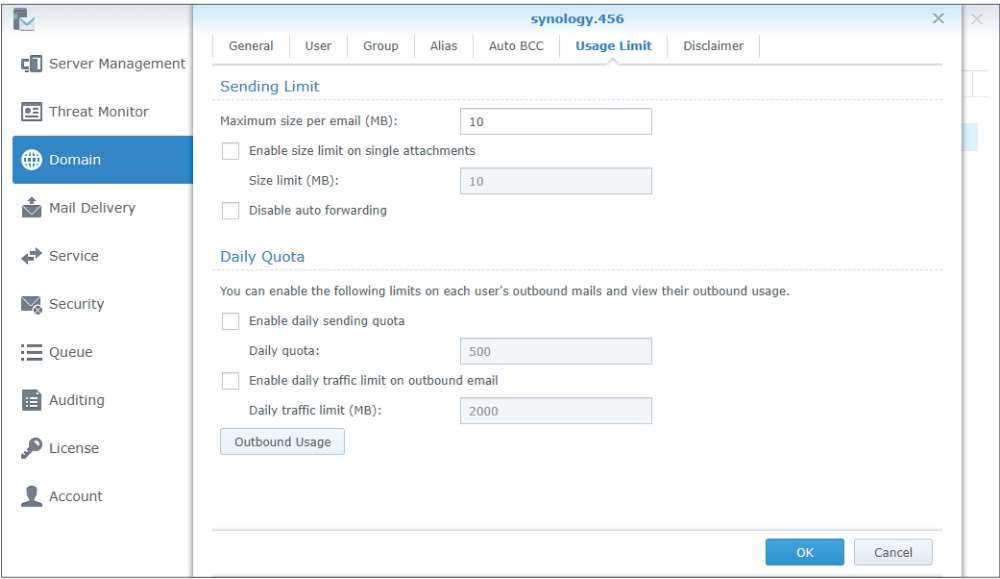
1. Go to **Domain**, select *synology.456*, and click **Edit**.
2. Go to **Auto BCC** and click the **Tools** button.
3. Choose to import or export sender or recipient rules.

**Note:**

- **Importing and exporting all message rules** is not available here since this feature is already written in the [main configuration documentation](#) of Postfix. Please refer to [always bcc](#).
- Please make sure the imported files are in the Postfix format.

Set up sending limit and daily quota

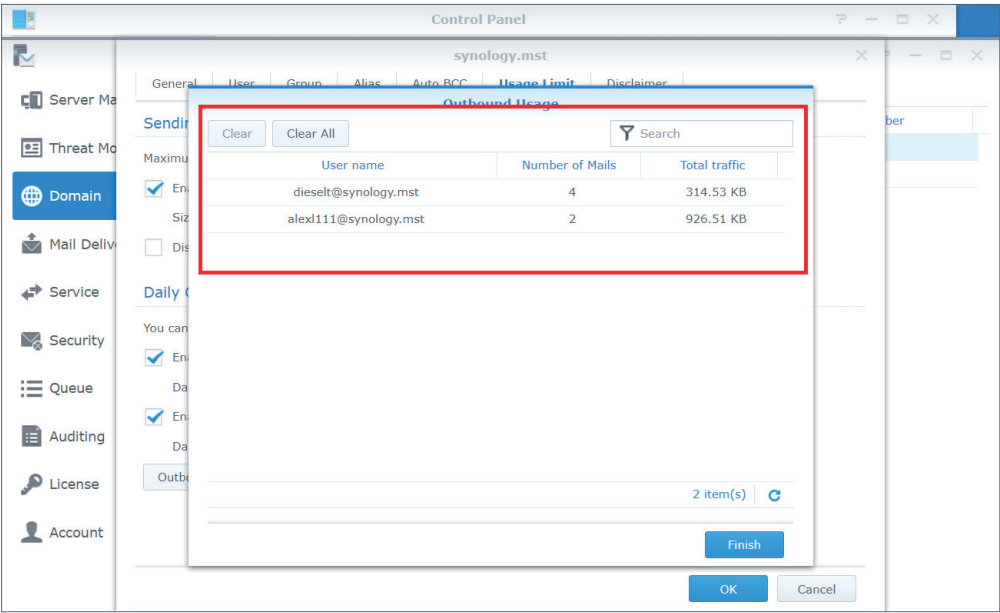
1. Go to **Domain**, select *synology.456*, and click **Edit**.
2. Go to the **Usage Limit** tab.
3. Under the **Sending Limit** section, adjust the following settings:
 - **Maximum size per email (MB)**: Specify the size limit for an outbound email.
 - **Enable size limit on single attachments**: Specify the size limit for a single attachment. Enter a value in the **Size limit (MB)** field below.
 - **Disable auto forwarding**
4. Under the **Daily Quota** section, adjust the following settings:
 - **Enable daily sending quota**: Limit the number of outbound messages a user can send every day.
 - **Enable daily traffic limit on outbound email**: Limit the total size of outbound messages a user can send every day.
 - **Outbound Usage**: View the outbound email usage of an individual user.



Outbound usage

You can view the total number of recorded outbound messages here. If a user has reached the daily quota, you can clear records to allow the user to continue sending emails.

- 1. Go to **Domain**, select *synology.456*, and click **Edit**.
- 2. Go to the **Usage Limit** tab and click the **Outbound Usage** button.
- 3. Select a specific user from the list. You can also search for users in the search field in the upper-right corner of the page.
- 4. Click the **Clear** button to clear user outbound usage records and reset usage records. Click the **Clear All** button to clear usage records of all the users on the list.



- 5. Click **Finish** to complete the settings.

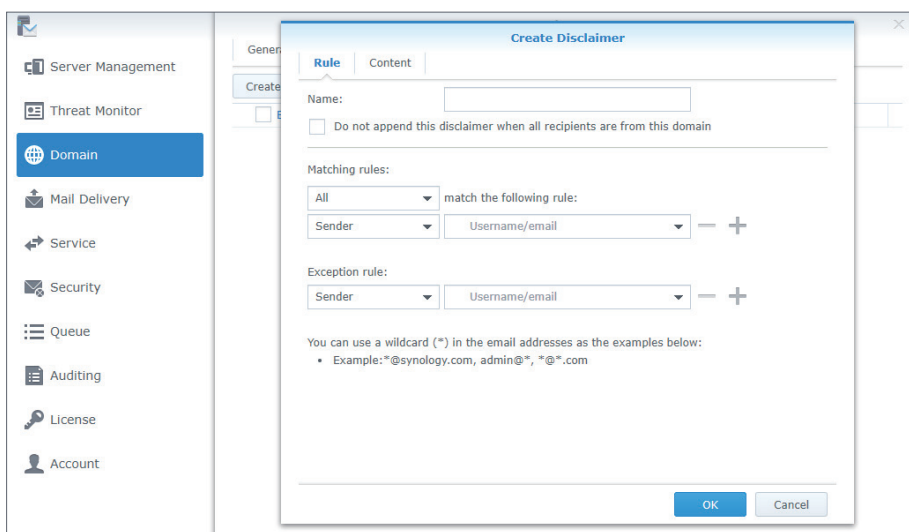
Create disclaimers

This disclaimer function allows users to automatically add custom text to the bottom or end of outbound emails. Please refer to the following steps to create disclaimers:

Note:

- You can have multiple disclaimers and rules; however, only one disclaimer can be applied to one email.

1. Go to **Domain**, select *synology.456*, and click **Edit**.
2. Go to the **Disclaimer** tab and click the **Create** button.
3. Go to the **Rules** tab in the **Create Disclaimer** window.



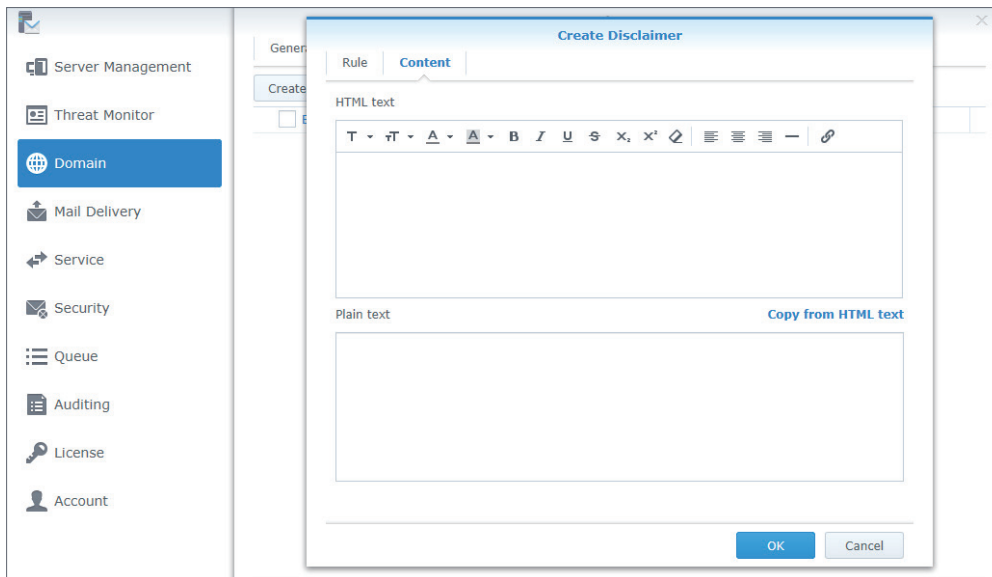
4. Enter the disclaimer name in the **Name** field.
5. Choose whether to tick the **Do not append this disclaimer when all recipients are from this domain** checkbox:

Note:

- When an email is detected as an internal email (emails sent to internal users) by the server, the disclaimer will not be appended.
- If one of the recipients is not an internal user, the disclaimer will still be appended.

6. Set the criteria using the following options:
 - **Matching rule:** Choose the definition for matching: **All** or **any**. When you select **All**, the disclaimer will be appended only if all rules are met. When you select **any**, the disclaimer will be appended if at least one rule is met.
 - **match the following rule:** Choose to append the disclaimer based on **Recipient** or **Sender**. The settings support wildcard characters (*).
 - **Exception rule** takes priority over **Matching rules**. When an **Exception rule** is created, disclaimers will not be appended even when the criteria for **Matching rules** are matched.

- Click the plus icon (+) to create more than one **Matching rule** or **Exception rule** and click the minus icon (-) button to remove a rule.
- After setting up the rules, go to the **Content** tab to edit the content of **HTML text** and **Plain text** to make sure the content displays correctly on the client end.



- If you want your **Plain text** content to be the same as the **HTML text** content, click **Copy from HTML text** to copy the content from the **HTML text** editor into the **Plain text** editor to remove all HTML tags.
- Click **OK** to finish the settings.

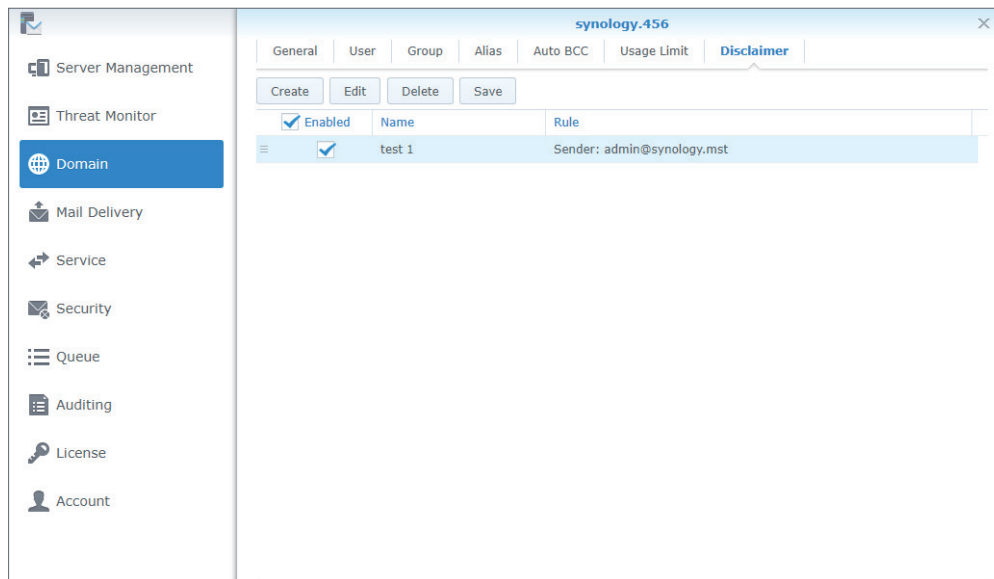
Edit and delete disclaimers

In addition to editing and deleting disclaimers, since disclaimers are applied based on their priority, you can adjust the priority settings here. Please refer to the following steps to manage disclaimers:

Note:

- The system checks which disclaimer to append from top to bottom. When the criteria for a disclaimer have been met, the disclaimer will be applied, thereby ending the check.

- Go to **Domain**, select *synology.456*, and click **Edit**.
- Go to the **Disclaimer** tab. Higher disclaimers have priority over lower ones. To change their priority, select a desired one and drag and drop it to a suitable position.
- Choose the disclaimer rule to enable.
- Select a disclaimer rule you want to modify and click the **Edit** or **Delete** button.



5. Click **Save** to apply the settings.

Chapter 9: Security Settings

MailPlus Server security features cover the following four areas: **Spam**, **Anti-virus scans**, **Authentication**, and **Content protection**. You can adjust settings to enhance protection for a specific area.

Spam

MailPlus Server provides spam detection standards based on the delivery nature of spam messages. The following anti-spam techniques are available in MailPlus Server:

- **Anti-spam:** Uses Rspamd and SpamAssassin as the anti-spam engines. In addition, through the auto-learning and spam reporting mechanisms, MailPlus Server can block spam messages according to your needs.
- **Postscreen:** Reduces the probability of receiving spam by rejecting services for spam servers according to open blacklists and the characteristics of senders from spam servers.
- **Greylist:** Takes actions based on the characteristics of senders from spam servers. Since the greylist will affect the delivery speed of messages, please fully understand the greylist mechanism before enabling this feature.

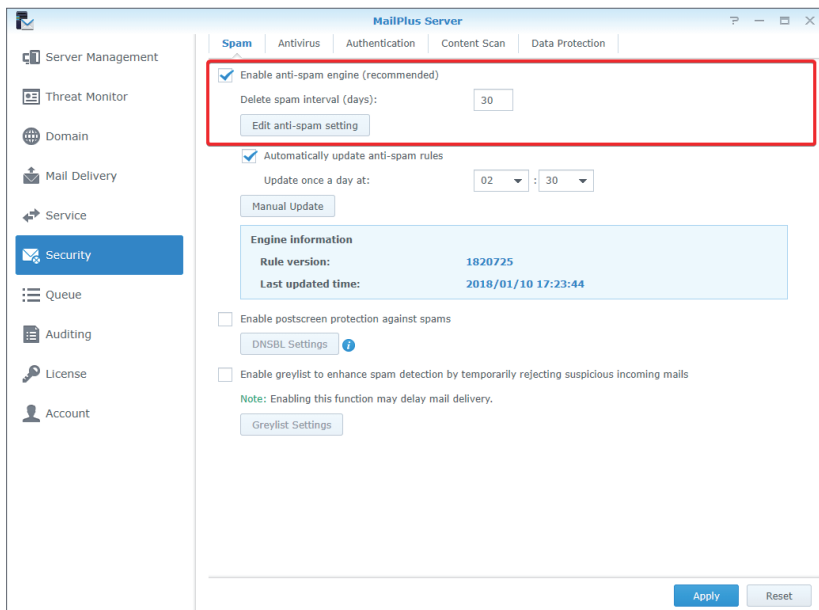
Enable anti-spam

MailPlus Server uses the anti-spam engine, Rspamd, along with rules from the SpamAssassin database to detect spam and then filters out spam based on the spam score threshold. When an email matches a pre-set detection rule, a point will be added to the score. Emails exceeding the threshold will be marked as spam. Please refer to the following steps to enable anti-spam:

1. Go to **Security > Spam** to adjust the following settings:
 - **Enable anti-spam engine:** For more information on the anti-spam functionality, please refer to [Anti-spam general settings](#), [Update anti-spam rules](#), [Custom spam filter](#), and [Auto learning and spam reporting settings](#).
 - **Delete spam interval (days):** Messages marked as spam will be sent to the spam mailbox. Spam messages will be automatically deleted after the specified number of days. You can customize the spam auto-delete interval, which is 30 days by default.

Note:

- Even if the anti-spam engine is not enabled, spam will still be regularly deleted.

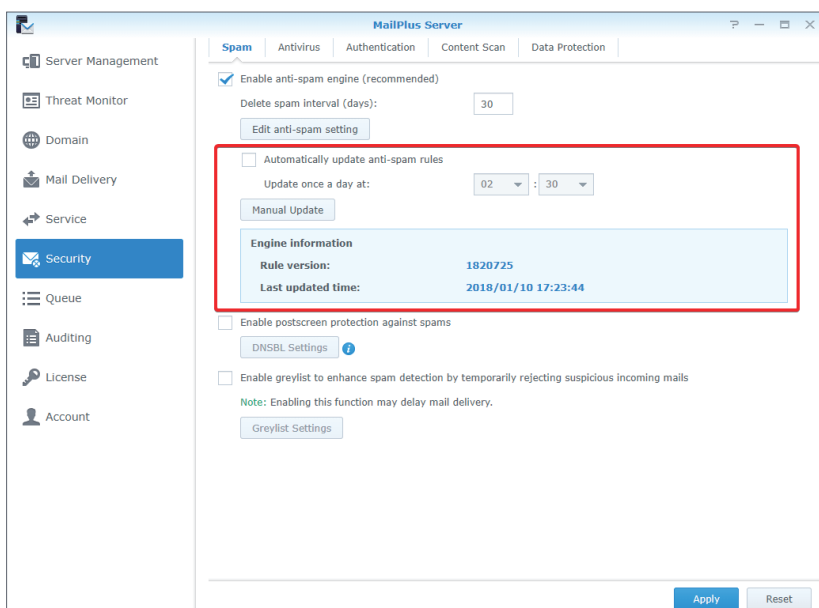


Update anti-spam rules

A regular update of anti-spam rules is required to ensure mail protection features are up-to-date. Please refer to the following steps:

1. Go to **Security > Spam** to adjust the following settings:

- **Automatically update anti-spam rules:** Tick this option to set up an update schedule, and the system will download the latest anti-spam rules from the official SpamAssassin website on schedule.
- **Update once a day at:** Set up a daily schedule to download rules.
- **Manual Update:** Click the button to update anti-spam rules immediately. The **Engine Information** section under the button displays the last updated time and the version of spam detection rules.



Anti-spam general settings

The anti-spam feature provides various customizable settings. You can adjust the anti-spam engine according to your needs. Please refer to the following steps to edit general anti-spam settings:

1. Go to **Security > Spam** and click the **Edit Anti-spam Settings** button.
2. Go to the **General** tab in the **Edit Anti-spam Settings** window, you can adjust the following settings:
 - **Mark as spam if score is higher than:** A message that exceeds the threshold you set will be marked as spam.
 - **Add the following to spam subjects:** When a message exceeds the spam score threshold and is marked as spam, you can add specific content to the subject of spam to notify users. Tick the **Add the following to spam subjects** checkbox and modify the default content.
 - **Encapsulate spam as attachment:** Emails marked as spam will be reported as an attachment encapsulated in a new message. The options from the drop-down menu include:

Options	Description
No	Reports spam without taking further action.
Yes	Reports spam as an attachment encapsulated in a new message.
Yes, as plain text only	Reports spam as plain text to avoid web bugs and malicious scripts; then, encapsulates it as an attachment and send it to recipients.

- **Auto white list:** This function allows the system to analyze inbound and outbound email communication to determine if an external email address has been replied by a user in the past. This avoids emails being mistreated as spam.

The screenshot shows the 'Edit anti-spam setting' dialog box with the 'General' tab selected. The 'Auto learning' tab is also visible. The settings are as follows:

- Mark as spam if score is higher than:** A dropdown menu set to '5 (Standard)'.
- Add the following to spam subjects:** A checkbox that is unchecked. Below it is a text input field containing '*****SPAM*****'.
- Encapsulate spam as attachment:** A dropdown menu set to 'No'.
- Auto white list:** A checkbox that is unchecked.
- At the bottom left, there are two buttons: 'SpamAssassin Rules' and 'Custom Spam Filter'.
- At the bottom right, there are 'OK' and 'Cancel' buttons.

SpamAssassin rules

1. Go to **Security > Spam** and click the **Edit Anti-spam Settings** button.
2. Go to the **General** tab in the **Edit Anti-spam Settings** window and click the **SpamAssassin Rules** button.
3. Click the **Import** button to add SpamAssassin rules.

Note:

- Imported files must have the file extension ".cf". Rules will be enabled once being imported. You can refer to [the rules](#) provided by SpamAssassin, or add rules based on [the rules' guideline](#).

4. Select the rule you want to edit and choose an action to take, such as **Enable**, **Export**, and **Delete**.
5. Click **Finish** to complete the settings.

Custom spam filter

There are two types of spam filters that you can set up to filter out suspicious emails: **Address Filter** and **Keyword Filter**. You can customize filters according to your needs. Please refer to the following steps to create a spam filter:

1. Go to **Security > Spam** and click the **Edit Anti-spam Settings** button.
2. Go to the **General** tab in the **Edit Anti-spam Settings** window and click the **Custom Spam Filter** button.
3. Go to the **Address Filter** tab in the **Custom Spam Filter** window and click the **Create** button.

The screenshot shows the 'Custom Spam Filter' window with the 'Address Filter' tab selected. The 'Keyword Filter' tab is also visible. Below the tabs, there are buttons for 'Create', 'Edit', 'Delete', and 'Tools'. A search bar with a magnifying glass icon and the text 'Search' is on the right. Below these buttons is a table with two columns: 'Criteria' and 'Do this'. The table is currently empty. At the bottom right, there is a 'Finish' button. A 'No data' message with a refresh icon is also visible.

4. Messages will be marked as spam or non-spam based on the sender and recipient criteria. Wildcard characters (*) can be used in the entered addresses.
5. From the **Do this** drop-down menu, select **Mark as spam** or **Mark as non-spam**.

Note:

- The spam score will be ignored regarding the configuration of these actions.

The screenshot shows the 'Black & White List - Create' window. It prompts the user to 'Create a rule to automatically mark certain messages as spam or non-spam.' There are two radio buttons: 'From:' address is (selected) and 'To:' address is. Both have text input fields with 'username@domain.com' entered. Below these is a 'Do this:' label and a dropdown menu currently showing 'Mark as spam'. A dropdown menu is open, showing three options: 'Mark as spam' (highlighted in blue), 'Mark as spam', and 'Mark as non-spam'. Below the dropdown, there is a note: 'You can specify the address in the following' followed by two bullet points: 'Single address: admin@synology.com' and 'Wildcards: *@synology.com, admin@*, *@*.com'. At the bottom, there are 'OK' and 'Cancel' buttons.

6. Click **OK** to complete the settings.
7. Go to the **Keyword Filter** tab in the **Custom Spam Filter** window.
8. Click the **Group setting** button to create a group. You can set up multiple groups to categorize keyword filters and then manage the filters by group:
 - Tick the checkbox in the **Enable** field to enable or disable an entire group.
 - To create, edit, or delete a group, select a group and click the action buttons in the upper toolbar.

9. Before creating a keyword filter, select the group the filter belongs to from the drop-down menu.

10. Click the **Create** button to customize the rule:

- **Target:** From the **Target** drop-down menu, you can select the following options to be filtered:

Options	Description
Title	Email title
Contents (including Subject)	Email content and title

- **Keyword:** Enter the keywords to be filtered. A regular expression can be used here. For more information on regular expression, please refer to [Wikipedia](#).
- **Score:** Specify the number of points that will be added to the total spam score of an email when the keyword is detected.

Note:

- An email will be marked as spam if the total spam score exceeds the spam score threshold.

Note:

- When making these modifications, you may want to re-adjust the spam score threshold. Please go back to the **General** tab in the **Edit Anti-Spam Setting** window to adjust the spam score threshold. The higher the spam score threshold, the looser the criteria for spam, so emails will be less likely to be marked as spam. The lower the spam score threshold, the stricter the criteria for spam, so emails will be more likely to be marked as spam.

Auto learning and spam reporting settings

After the anti-spam engine starts running, you can train MailPlus Server to better detect spam with specialized algorithms. Auto-learning and spam reporting help improve the accuracy of spam detection to meet individual needs.

- Auto-learning:** During spam detection by the anti-spam engine, the system will automatically select an email that matches the criteria based on its score so that the email can be further analyzed.
- Spam reporting:** Users can report spam when the anti-spam engine has failed to detect spam, or when a message has been mistreated as spam. Reporting incorrect categorization to the anti-spam engine helps the engine relearn to improve the accuracy.

Please refer to the following steps to set up auto-learning and spam reporting:

- Go to **Security > Spam** and click the **Edit Anti-spam Settings** button.
- Go to the **Auto learning** tab in the **Edit Anti-spam Settings** window.

The screenshot shows the 'Edit anti-spam setting' window with the 'Auto learning' tab selected. The 'General' tab is also visible. The 'Auto learning' section has a checked checkbox. Below it, there are three settings: 'Mark as spam if score is higher than:' set to '5 (Standard)', 'Learn as spam if score is higher than:' set to '12 (Strict)', and 'Learn as non-spam if score is lower than:' set to '-1 (Strict)'. The 'Enable spam reporting' checkbox is also checked. Below this, there are two text input fields for 'Forward spam to:' and 'Forward false spam to:', both with '@NO.Synology.io' as the placeholder. A button labeled 'Reported Spam' is present. At the bottom, there is an unchecked checkbox for 'Set daily schedule for learning reported spam' and a 'Daily schedule:' field set to '02 : 00'. 'OK' and 'Cancel' buttons are at the bottom right.

- Tick the **Auto learning** checkbox to adjust the following settings:

- Mark as spam if score is higher than:** You will see the spam score threshold set up at the **General** tab.

- **Learn as spam if score is higher than:** During spam detection, if the spam score is higher than this value, the anti-spam engine will further analyze the keywords in message content to expand the anti-spam engine database and improve its learning capability. When the same keywords are detected in the future, messages will be more likely to be determined as spam.
- **Learn as non-spam if score is lower than:** During spam detection, if the spam score is lower than this value, the anti-spam will further analyze the keywords in message content to expand the anti-spam engine database and improve its learning capability. When the same keywords are detected in the future, messages will be more likely to be determined as non-spam.

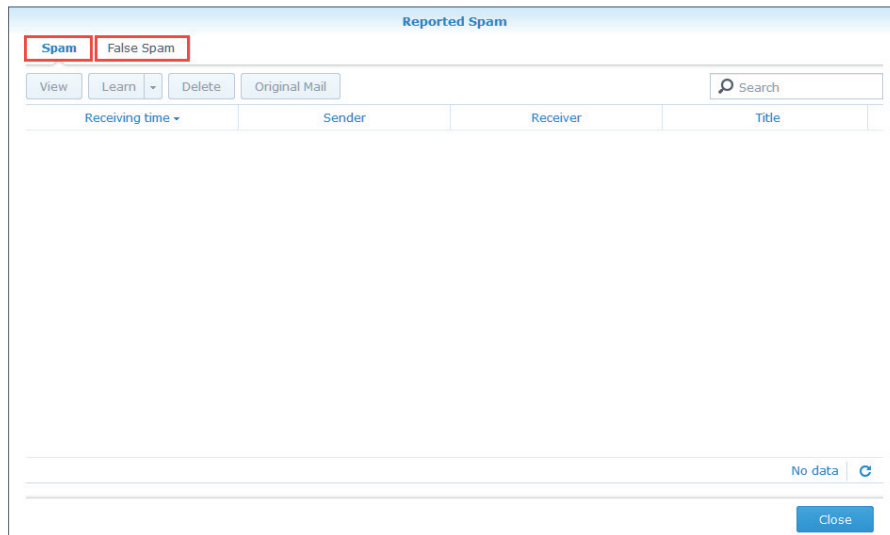
4. Tick the **Enable spam reporting** checkbox to adjust the following settings:

Note:

- The reporting process involves collecting spam to a specific mailbox to undergo the learning process. Therefore, after enabling spam reporting, users can report spam and non-spam based on the following two methods:
 - If users receive messages using MailPlus, the forward mailbox has already been configured for these users. Users only need to mark messages as spam in MailPlus or go to the spam mailbox of MailPlus to mark messages as non-spam.
 - If users receive messages using third-party email clients, they must use the **forward as attachment** feature on email clients to forward emails as attachments to the reporting mailbox.
- **Forward spam to:** Enter an email address that reported spam will be forwarded to when users use third-party mail clients to receive and report emails. The original email will be forwarded as an attachment to this email address.
- **Forward false spam to:** Enter an email address that reported non-spam will be forwarded to when users use third-party mail clients to receive and report emails. The original email will be forwarded as an attachment to this email address.
- **Reported Spam:** Click the **Reported Spam** button to view all reported spam and false spam. On the email list, select an email and click the **Learn** button to allow the anti-spam engine to improve spam detection for the selected email type. Emails that have been learned will be removed. You can allow the system to learn from emails in the spam and non-spam mailboxes. Please refer to the following spam management:

Function	Description
View	View message content.
Learn	Allow the anti-spam engine to quickly learn from the selected email. After an email has been learned, it will be removed from the list.
Learn All	Allow the anti-spam engine to learn from all email messages. Learn All can be found from the drop-down menu next to the Learn button.
Delete	Remove selected emails to prevent them from being learned by the anti-spam engine.

Function	Description
Original Mail	Open the original mail in a new browser tab.
Search	Enter keywords (senders, recipients, and subjects) in the search field in the upper-right corner to search for certain email messages.



- **Set daily schedule for learning reported spam:** Tick this option to specify the time for the system to auto-learn all reported spam and non-spam messages.

Note:

- The email address entered in **Forward spam to** cannot share the same username as existing users. The email address will not be counted as a licensed user and will only be used to receive email samples.
- The email address entered in **Forward false spam to** cannot share the same username as existing users.

5. Click **OK** to complete the settings.

Postscreen

Postscreen tests the connection source during the connection stage and determines whether or not to continue services. Postscreen includes the following two main functions:

- Checks if a sender follows SMTP standards and sends commands after the SMTP server greeting. If a sender sends a command before the SMTP server greeting, this sender will be blocked.
- Checks other DNSBL servers based on the sender's IP address. If a sender's IP address is blacklisted by other servers, this sender will be blocked.

DNSBL settings

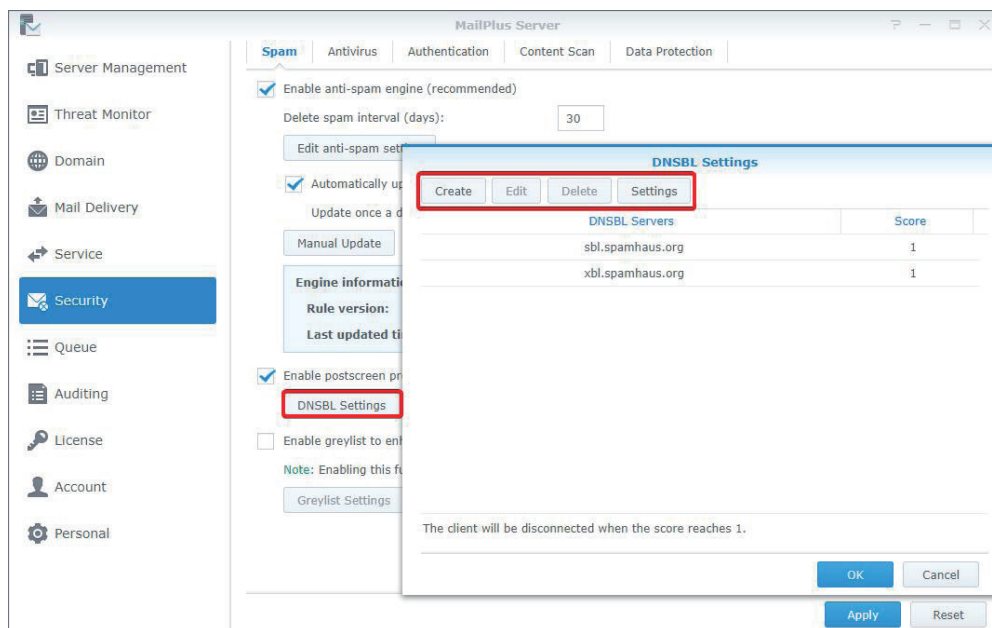
Postscreen allows the setup of multiple DNSBL servers. Matching criteria during the server check results in spam points, and spam points generated from different servers will be accumulated. When the total score exceeds the value specified in the **DNSBL Score Threshold**, services will be rejected. Please refer to the steps below to adjust DNSBL settings:

1. Go to **Security > Spam** and click the **Enable postscreen protection against spams** checkbox.
2. Click the **DNSBL Settings** button to edit the servers that should be checked.
3. Click the **Settings** button to specify the **DNSBL Score Threshold** for rejecting services.
4. Click the **Create** button to add servers to be checked.

Note:

- You can add DNSWL (DNS-Based Whitelist) servers here and enter negative numbers in the corresponding **Score** fields.

5. You can **Edit** or **Delete** a selected DNSBL server.



6. Click **OK** to complete the settings.

Enable greylist

When there is a new inbound message, the system will check if there are records of the same IP address, sender, or recipient as that of this inbound message. If no records are found, the message will be considered suspicious, and an error message will be sent back to its sender, requesting the sender to send the message again later. According to SMTP standards, senders receiving error messages will try to send messages again at a later time. However, most spam senders will give up sending messages. When ordinary senders send messages again after a while, the system will receive them. The greylist mechanism uses this method to block spam.

With the greylist enabled, the greylist will take the following default actions on emails from all sources:

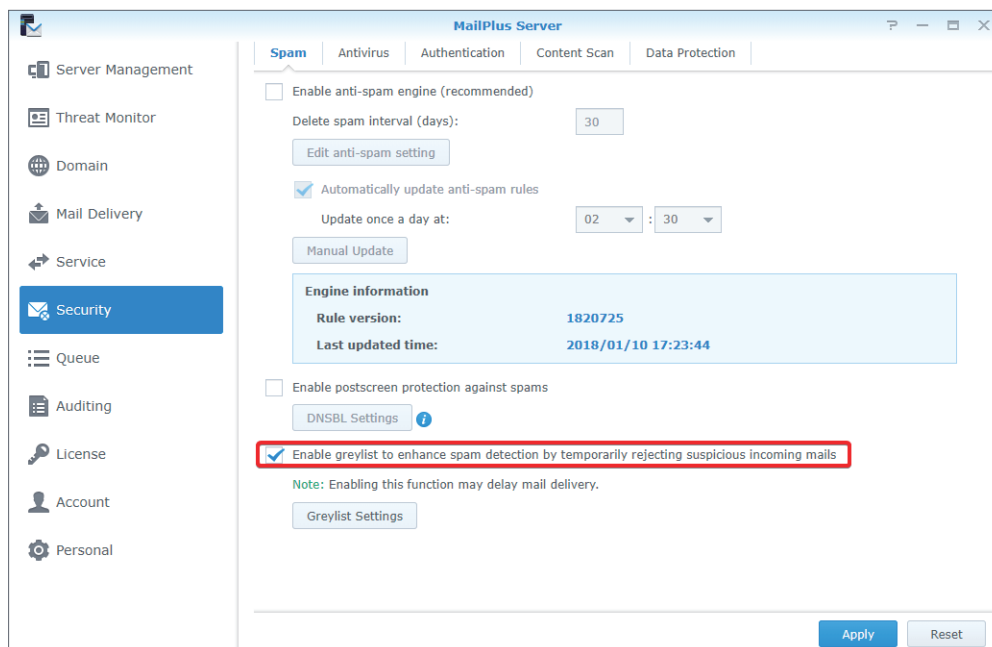
- **Whitelist:** Passes the test directly, and temporary error messages will not be sent back.
- **Greylist:** Sends error messages to senders without communication history.
- **Blacklist:** Rejects messages directly.

Note:

- The greylist mechanism may delay the delivery of legitimate messages. Please make sure you fully understand the greylist mechanism before enabling the greylist.

Please refer to the following steps to enable greylist:

1. Go to **Security > Spam** and tick the **Enable greylist to enhance spam detection by temporarily rejecting suspicious incoming mails** checkbox.



2. Click the **Greylist Settings** button to set up default actions for all sources or actions for a specific IP address or domain name.
3. In the **Greylist Settings** window, click the **Settings** button to set up the default action for all sources.

Greylist Settings

Create Edit Delete **Settings**

IP / Domain	Action
<p>Greylist Settings</p> <p>Action: Greylist</p> <p>Greylist time period: 30 minutes</p> <p>OK Cancel</p>	

Action: Greylist / Greylist time period: 30 minutes

OK Cancel

- From the **Action** drop-down menu, select a default action. In the **Greylist time period** field, enter a greylist delay time, which will be applied to all greylist actions.
- Click **Create** to set up different actions for specific sender sources. You can set up different greylist commands other than the default action for specific users.

Greylist Settings

Create Edit Delete Settings

IP / Domain	Action
<p>Greylist Settings - Create</p> <p><input type="radio"/> Source</p> <p>IP address: 192.168.1.1</p> <p>Netmask: 24</p> <p><input type="radio"/> Domain</p> <p>Domain name: example.com</p> <p>Action: Whitelist</p> <p>OK Cancel</p>	

Action: Greylist / Greylist time period: 30 minutes

OK Cancel

- In the pop-up window, select a sender source and select an action from the **Action** drop-down menu.

Note:

- The domain source here is fetched from the IP address searched via DNS, not from **MAIL FROM** of a message.

- Click **OK** to complete the settings.

Antivirus Scan

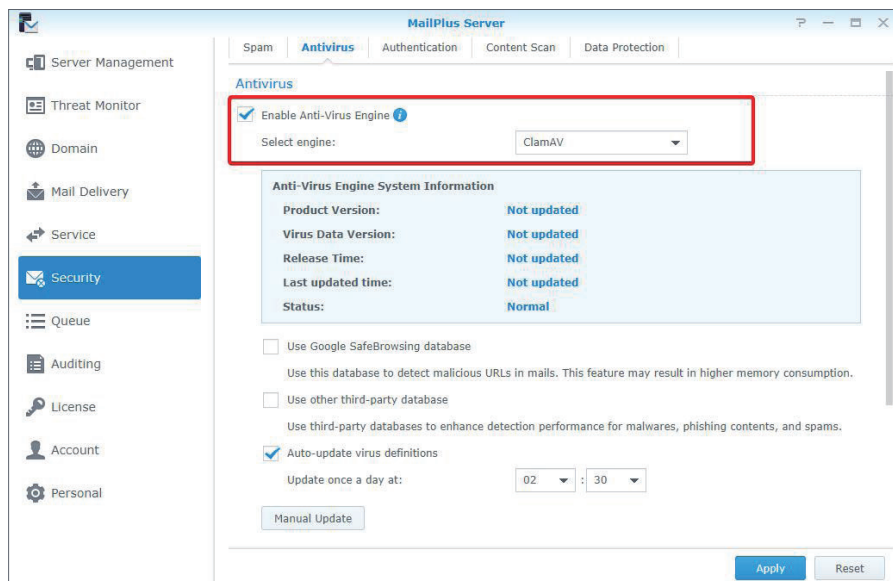
MailPlus Server provides ClamAV, a free anti-virus engine, and McAfee, a paid and subscription-based anti-virus engine, to defend against malware threats. You can set up actions to take upon the detection of viruses.

Through antivirus detection, you can check if your emails contain malicious software or malware.

- **ClamAV:** ClamAV is the default antivirus system in MailPlus Server, which provides complete protection for your server at no cost.
- **McAfee:** MailPlus Server integrates with a paid antivirus package, **Antivirus by McAfee**. Subscribe to the **Antivirus by McAfee** and select **McAfee** as your antivirus engine for convenient management, antivirus scheduling, log, and more advanced settings. Please note that MailPlus Server will not scan emails larger than 20 MB to avoid prolonged scanning times.

Enable anti-virus engine

1. Go to **Security > Antivirus** and tick the **Enable Anti-Virus Engine** checkbox.



2. Select either of the following from the **Select engine** drop-down menu:

- **ClamAV:** ClamAV is a free antivirus engine supported by MailPlus Server.
- **McAfee:** McAfee is a subscription-based antivirus engine that requires additional installation. (Please go to **Package Center** to install **Antivirus by McAfee**.)

3. Please refer to the following sections to complete the settings.

ClamAV

If you choose ClamAV as the antivirus engine, please refer to the following steps to configure the settings:

1. Under **Anti-Virus Engine System Information**, you can view the antivirus engine information. Please update the antivirus engine regularly.
2. ClamAV uses the following external databases to enhance detection accuracy:
 - **Use Google Safe Browsing database:** Uses the integrated Google Safe Browsing database to detect if a message contains malicious links.
 - **Use other third-party database:** Uses Sanesecurity and other **third-party databases** to enhance virus detection.
3. You can choose to automatically or manually update virus definitions:
 - **Auto-update virus definitions:** Enable auto-update to allow the system to download the latest virus definition files on a daily schedule.
 - **Manual Update:** Click the button to immediately update virus definitions.

The screenshot shows the 'MailPlus Server' interface with the 'Antivirus' tab active. The 'Enable Anti-Virus Engine' checkbox is checked. The 'Select engine:' dropdown is set to 'ClamAV'. A red box highlights the 'Anti-Virus Engine System Information' section, which displays the following details:

Product Version:	0.99.4
Virus Data Version:	25004
Release Time:	2018/10/04 04:51:19
Last updated time:	2018/10/04 09:58:09
Status:	Normal

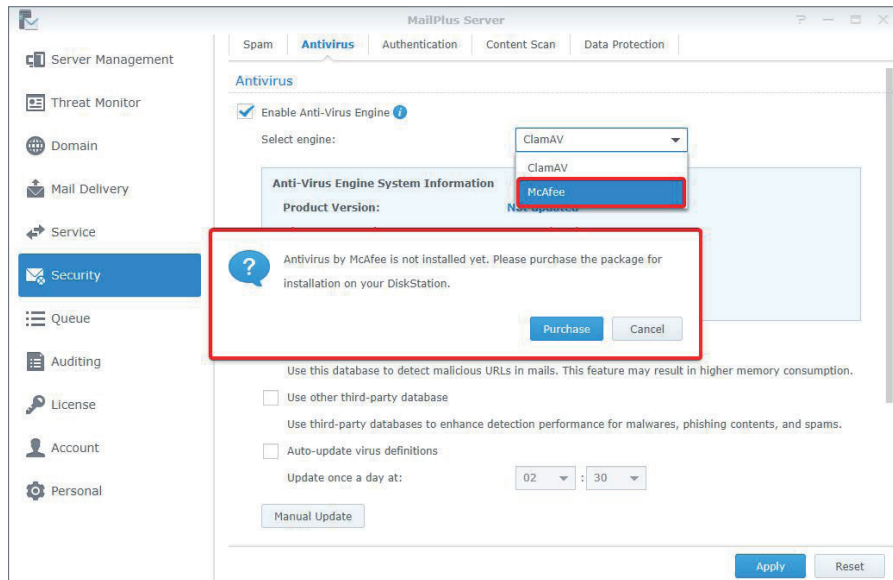
Below this, there are two unchecked checkboxes: 'Use Google SafeBrowsing database' and 'Use other third-party database'. A third red box highlights the 'Auto-update virus definitions' checkbox, which is checked, and the 'Update once a day at:' field, which is set to 01:00. A 'Manual Update' button is located below the auto-update settings. At the bottom right of the configuration area, there are 'Apply' and 'Reset' buttons.

4. Click **Apply** to save the settings.

McAfee

Selecting McAfee as your antivirus engine will require you to go to **Package Center** to purchase the package.

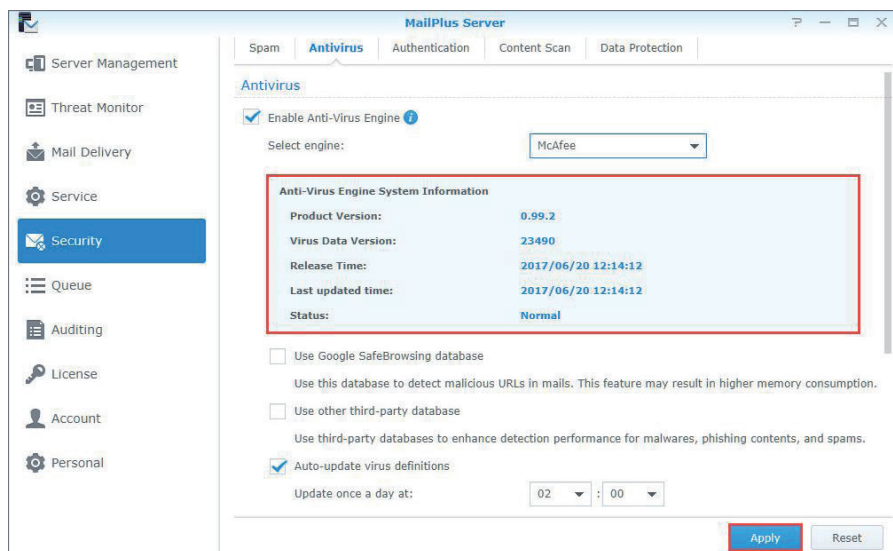
1. If you have not installed McAfee or if the license has expired, an alert window will appear to inform you to go to **Package Center** to install **Antivirus by McAfee** and purchase the license using **Synology Account**.



2. Under **Anti-Virus Engine System Information**, you can view McAfee's information.

Note:

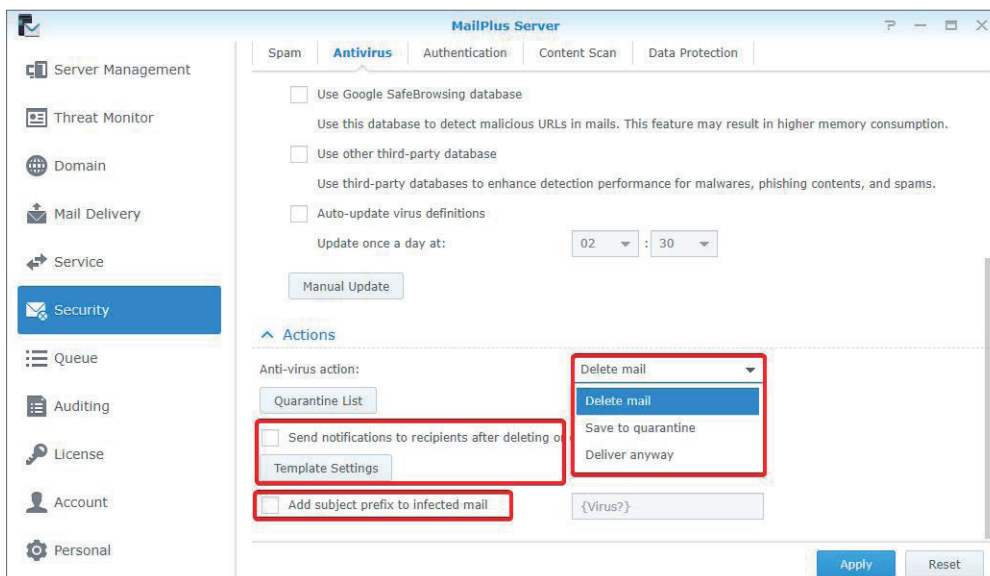
- McAfee settings must be configured in the **Antivirus by McAfee** package.
- If the status is abnormal (possibly due to license issues or corrupted virus definition files, etc.), **Antivirus by McAfee** will not scan messages. Please resolve the problem or switch back to ClamAV. If a user manually disables **Antivirus by McAfee**, MailPlus Server will automatically switch to ClamAV.



3. Click **Apply** to save the settings.

Anti-virus action settings

1. Go to **Security > Antivirus**.
2. Select an action to take on emails containing viruses from the **Anti-virus action** drop-down menu:
 - **Delete mail**: Deletes emails.
 - **Save to quarantine**: Blocks emails and saves them to the quarantine section.
 - **Deliver anyway**: Delivers emails.
3. If you have selected **Delete mail** or **Save to quarantine**, you can tick the **Send notifications to recipients after deleting or quarantining viruses** checkbox to inform the situation. A notification message will be sent to the recipient of the original email. You can click on the **Template Settings** button below to adjust the notification message templates for quarantined and deleted emails respectively.
4. If you have selected **Delver anyway**, you can tick the **Add subject prefix to infected mail** checkbox to label suspicious emails.



5. Click **Apply** to save the settings.

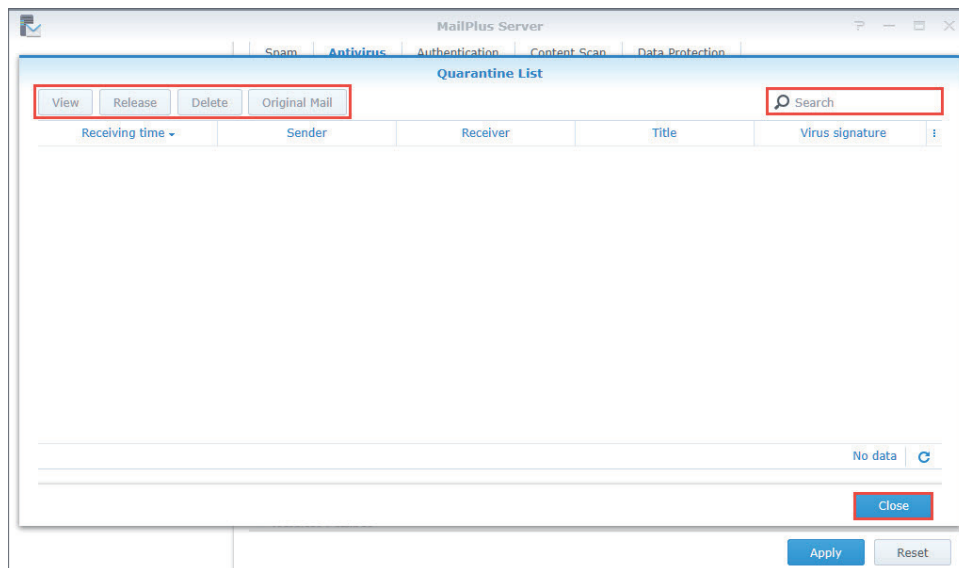
Quarantine list

If you have saved emails to the quarantine section, you can view and manage the quarantined emails. Please refer to the following instructions to adjust the settings of quarantine list:

1. Go to **Security > Antivirus** and click the **Quarantine List** button.
2. You can search for senders, recipients, titles, and virus definitions in the search bar in the upper-right corner of the **Quarantine List** window.
3. Select a quarantined email and click the **View** or **Original Mail** button to check the content.

4. Choose one of the following actions based on the email content:

- **Release:** Releases the email to its recipient.
- **Delete:** Deletes the email.



5. Click **Close** to complete the settings.

Authentication

The purpose of authentication is to verify a sender's identity to block fraudulent messages and protect against identity theft.

- **SPF (Sender Policy Framework):** SPF mechanism verifies the legitimacy of a sender's host. SPF records for many domains are currently published in DNS and they provide the location of the hosts that are authorized to send emails using a domain. Therefore, when a host from a network delivers messages to MailPlus Server, the system will verify the SPF records of the sender's domain in DNS and determine if the host is authorized to send emails using this domain. If the SPF authentication fails, it will be categorized as **fail** or **softfail** depending on the SPF records, and the system will treat the two results differently.
- **DKIM (DomainKeys Identified Mail):** DKIM mechanism verifies a sender's identity using encryption methods to check if email content has been modified. With the DKIM mechanism, a sender's host will generate a set of the public key and private key and will publish the public key in DNS, while using the private key to create a digital signature to be affixed to emails. When the receiving host receives a message, it will check the public key for the sender's domain in DNS and use the public key to verify the signature, the sender identity, and whether the message has been modified or not.
- **DMARC (Domain-based Message Authentication, Reporting & Conformance):** DMARC mechanism is based on SPF and DKIM verification methods. When the system receives a message, it will check if the sender passes the SPF and DKIM verification, thereby determining if the sender is fraudulent.

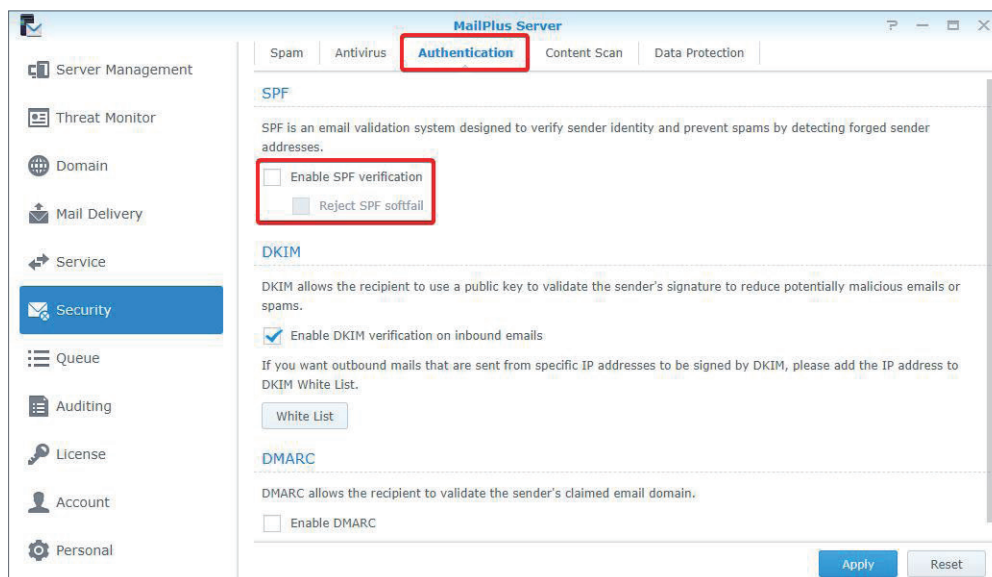
SPF

Enabling SPF verification allows the system to check the SPF records of a sender's domain in DNS to prevent email fraud. When SPF verification fails, the result will be identified as **fail** or **softfail**. Please refer to the following steps to adjust SPF verification settings:

Note:

- If your MailPlus Server is set up to receive messages forwarded from other mail servers, the SPF mechanism may block relayed messages since a relay server location is not included in a sender's SPF records. (For more information, please refer to [this article](#).) Please add the relay server to the whitelist or disable SPF verification.

1. Go to **Security > Authentication**.
2. Under the **SPF** section, tick the **Enable SPF verification** checkbox.
 - If the verification result is **fail**, the message will be rejected.
 - If the verification result is **softfail**, you can tick the **Reject SPF softfail** checkbox to reject **softfail** messages; otherwise, all messages with the **softfail** result will be received.



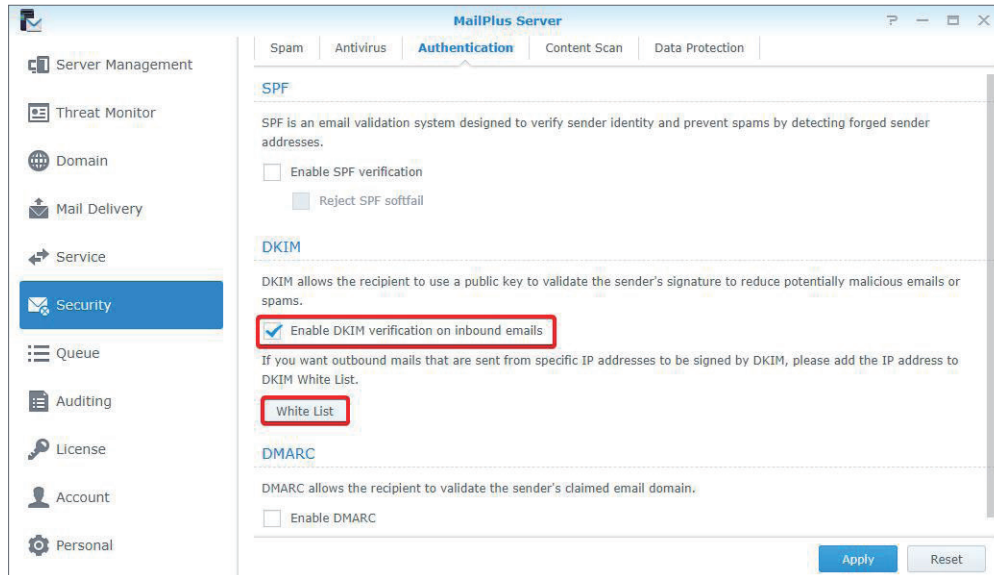
3. Click **Apply** to save the settings.

DKIM

You can enable DKIM verification to prevent messages from being modified and to protect against identity theft. Please refer to the following steps to adjust DKIM verification settings:

1. Go to **Security > Authentication**.
2. Under the **DKIM** section, tick the **Enable DKIM verification on inbound emails** checkbox if you want to verify a sender's identity for inbound messages and reduce messages from unknown sources.

3. Select a value for **Minimum key length for DKIM verification**. DKIM will reject an email if the key length for DKIM signing is shorter than the selected value. Increasing the minimum key length can prevent emails from less secure domains passing the DKIM verification.
4. Click the **White List** button to add specific IP address ranges to the whitelist which will allow specific senders to pass authentication and attach DKIM signatures to messages. When a host within the range connects to MailPlus Server to send outbound messages, the system will attach DKIM signatures to the messages.



5. Click **Apply** to save the settings.

Note:

- Emails rejected by DKIM will be moved into the **Spam** mailbox in MailPlus 2.1 and above versions. A warning will appear when these emails are viewed on MailPlus clients.

DMARC

Since DMARC is based on SPF and DKIM verification, please set up SPF for your domain and generate a public key to enable DKIM signing on outbound emails before proceeding with the DMARC settings. Please refer to the following steps to enable DMARC verification:

1. Go to **Security > Authentication**.
2. Tick the **Enable DMARC** checkbox to enable DMARC.

Note:

- Emails quarantined by DMARC will be moved into the **Spam** mailbox in MailPlus 2.1 and above versions. A warning will appear when these emails are viewed on MailPlus clients.

Content Protection

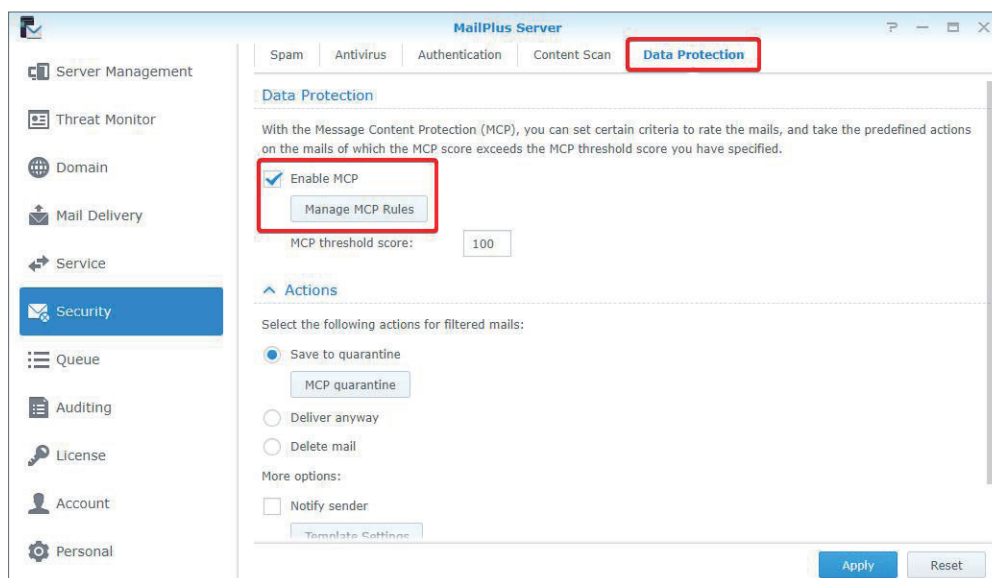
The content protection feature can filter out suspicious emails based on your settings.

- **MCP Rules:** Searches based on the content of the original email. If too much suspicious content has been identified, the email will be placed in the quarantine section, or other specified actions will be performed.
- **Attachment Filter:** Filters email messages according to attachment types.
- **Content Scan:** Enhances email content scanning. Rejects or rewrites emails containing phishing links or HTML tags to ensure security.

MCP rules

Set up MCP (Message Content Protection) rules and specify an MCP threshold score. When an email matches a rule's criteria, the rule score will be summed up to the total MCP score. If the total score exceeds the MCP threshold score, the system will filter out or block the email. Please refer to the following steps to enable and manage MCP.

1. Go to **Security > Data Protection** and tick the **Enable MCP** checkbox in the **Data Protection** section.
2. In the **MCP threshold score** field, enter a score.
3. Click the **Manage MCP Rules** button to add new rules.



4. In the **Manage MCP Rules** window, click the **Create** button.
5. The **Add MCP Rules** window includes the following items:
 - **Name:** Enter a rule name.
 - **Target:** Choose a section of emails from the **Target** drop-down menu as the target to be matched:

Section	Description
Title	Email message title
Contents (including Subject)	Email message content and subject
Sender	The sender of an email message
Receiver	The recipient of an email message
Custom header	The specific header of an original email message

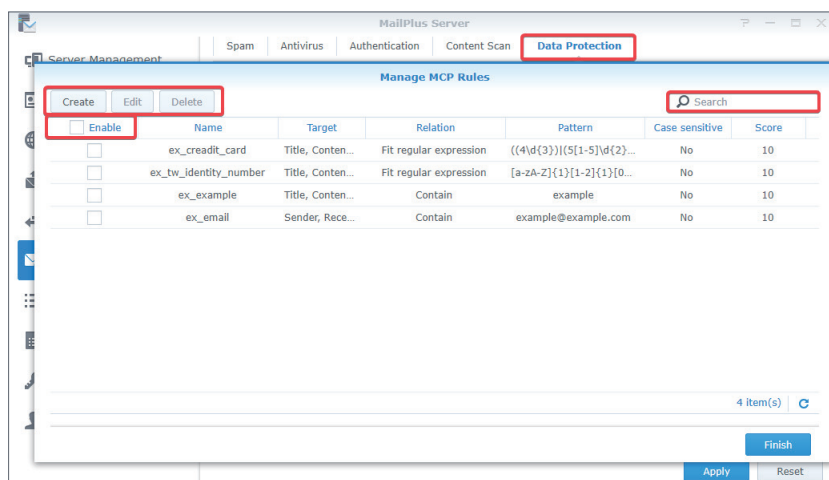
- **Custom header:** When the **Custom header** is selected from the **Target** drop-down menu, the **Custom header** field will appear. Enter a specific header here.
- **Relation:** Choose a matching criterion from the **Relation** drop-down menu:

Criteria	Description
Contain	If the target section of an email contains the matching content, the email matches the rule.
Equal to	If the target section of an email is identical to the matching content, the email matches the rule.
Fit regular expression	If the target section of an email contains the matching content, the email matches the rule. A regular expression can be used for the matching content.

- **Pattern:** Enter matching content for the rule.
- **Case sensitive:** Choose **Yes** or **No** to determine if the matching is case sensitive.
- **Score:** Specify the number of points that will be generated when the criteria of this rule are matched.

6. Click **OK** to finish creating rules.

7. In the **Manage MCP Rules** window, you can create, enable, edit, or delete a rule. You can also search for a rule in the search bar in the upper-right corner.



8. Click **Finish** to complete the settings.

Actions

When the total score of matching rules exceeds the **MCP threshold score**, specific actions will be taken. Please refer to the following steps to set up actions:

1. Go to **Security > Data Protection** and enter a value in the **MCP threshold score** field under the **Data Protection** section.
2. Under the **Actions** section, you can set up actions that will be taken when the **MCP threshold score** has been exceeded:
 - **Save to quarantine:** Blocks email messages and saves them to the quarantine section. You can click the **MCP quarantine** button to view the content of quarantine messages. Please refer to [Quarantine list](#) for more information on managing quarantined messages.
 - **Deliver anyway:** Delivers email messages.
 - **Delete mail:** Deletes email messages.
 - **More options:** Notifies senders or forwards email messages to a specific mailbox.

Function	Description
Notify sender	Sends a notification email to notify senders that their emails have been blocked. You can click the Template Settings button to set up notification content.
Forward to	Forwards original emails to a specific mailbox.

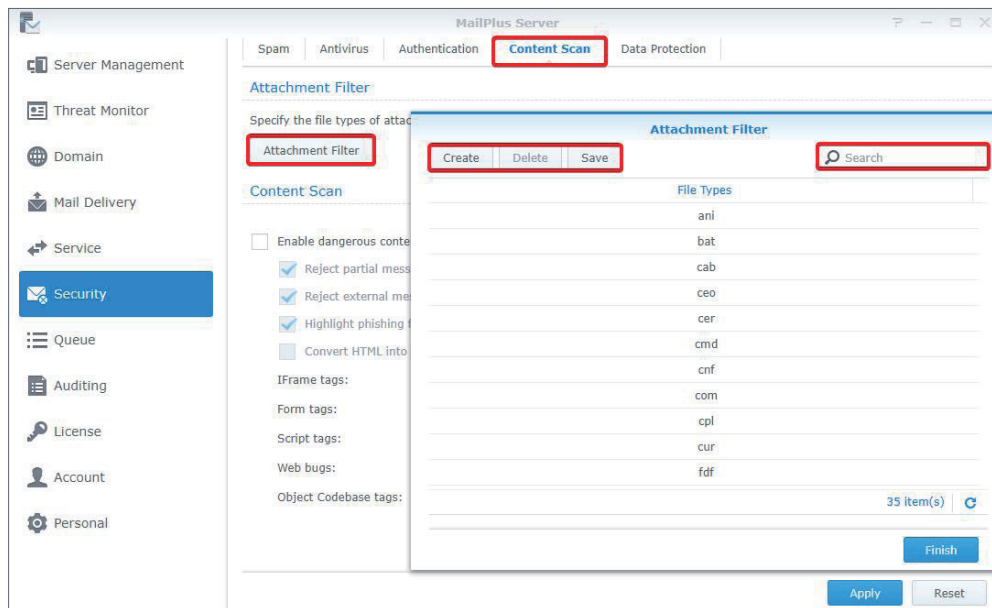
The screenshot shows the 'MailPlus Server' interface with the 'Data Protection' tab selected. The 'Data Protection' section includes an 'Enable MCP' checkbox (checked) and an 'MCP threshold score' field set to '100'. Below this is the 'Actions' section, which prompts the user to 'Select the following actions for filtered mails:'. Under this, 'Save to quarantine' is selected with a radio button, and there is an 'MCP quarantine' button. Below that are 'Deliver anyway' and 'Delete mail' options, both unchecked. The 'More options' section includes 'Notify sender' (checked) with a 'Template Settings' button, and 'Forward to:' (checked) with a text field containing 'admin@yourdomain.com'. At the bottom right are 'Apply' and 'Reset' buttons.

3. Click **Apply** to save the settings.

Attachment filter

This attachment filter feature blocks messages based on attachment file types. Please refer to the following steps to set up attachment filters:

1. Go to **Security > Content Scan**.
2. Under the **Attachment Filter** section, click the **Attachment Filter** button.
3. In the **Attachment Filter** window, click the **Create** button to add new file types. You can select a file type to **Delete** or search for certain file types in the upper-right corner.



4. Click **Save**.
5. Click **Finish** to complete the settings.

Content scan

The content scan feature blocks suspicious messages or modifies their content. Please refer to the following steps to adjust **content scan** settings:

Note:

- Modified content may not meet expectations. Please make sure you enable functions according to your needs.

1. Go to **Security > Content Scan**.
2. Under the **Content Scan** section, tick the **Enable dangerous content scan** checkbox and adjust the following settings:
 - **Reject partial messages:** Rejects emails that are split across multiple incomplete messages (specifically email messages with Content-Type value of header message/partial).
 - **Reject external message bodies:** Rejects emails that point to external resources (specifically email messages with Content-Type value of message/external-body).

- **Highlight phishing fraud:** Highlights detected phishing links in an email to alert recipients.
- **Convert HTML into plain text:** Converts messages in HTML format to plain text.
- You can set up one of the following actions for each tag:

Action	Description
Allow	Delivers messages.
Reject	Rejects messages.
Make tags ineffective	Delivers messages after making tags ineffective.

Note:

- Please specify the settings for each tag.

Chapter 10: Monitor Settings

Monitor Server Status

You can quickly oversee the server operation status via a graphical interface:

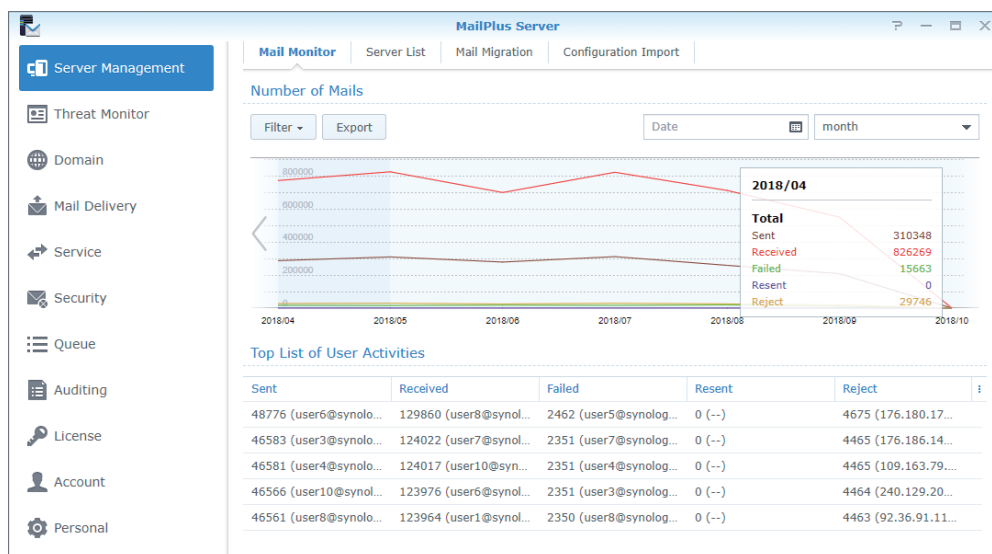
- **Mail Traffic Monitor:** Monitors the server's mail traffic by specific time intervals.
- **Threat Monitor:** Shows the number of email threats blocked by each security setting of your server. You can quickly identify all threat sources and adjust security settings accordingly.
- **Server List:** Displays a list of server clusters and their operation statuses.

Mail traffic monitor

The **Mail Monitor** tab in **Server Management** displays mail activity statistics over a past period of time. Under the **Top List of User Activities** section is a list of the most active email addresses from each traffic type. For more information on email traffic types, please refer to [View mail logs](#).

Note:

- If you have already set up a [High-availability cluster](#), please view logs on the primary server.



Monitor traffic by different time interval lengths

You can monitor email traffic in MailPlus Server by **hour**, **day**, **week**, or **month**. Every data point on the **Number of Mails** chart represents the total number of emails (of a specific email traffic type) during the time interval. Please refer to the steps below to adjust the time interval:

1. Go to **Server Management > Mail Monitor**.
2. You can select date and time intervals from the **Date** field and the drop-down menu in the upper-right corner of the **Number of Mails** section.

Monitor traffic from a specific time interval

You can use the following two methods to monitor a specific time point:

1. Hover the cursor to the left or right end of the chart and click the arrow icons to move forward or backward to a different point of time.
2. Select a desired date from the **Date** field in the upper-right corner of the **Number of Mails** section.

Note:

- MailPlus Server reserves different numbers of mail data for different time lengths. You can only switch to time intervals with available data.

Fix display of detailed data from a specific time

Data displayed in the detailed information panel on the chart change as you hover over different time points. To view detailed information of a selected time interval, move the cursor to the desired time interval and left-click to fix the detailed information panel.

Show or hide data from certain traffic types

1. Go to **Server Management > Mail Monitor**.
2. Click the **Filter** button under the **Number of Mails** section and tick the checkboxes to show or hide data of certain traffic types.

Export data from a specific time interval

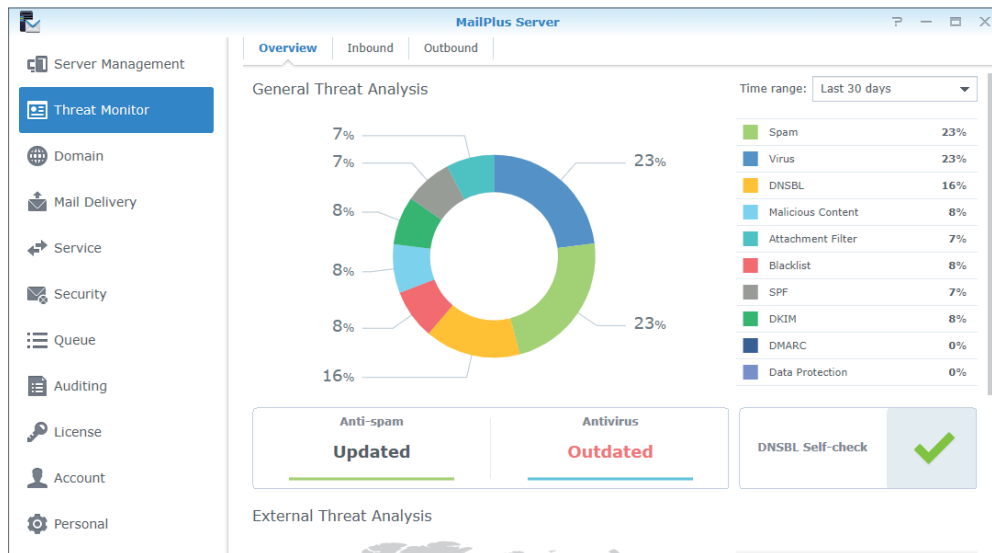
1. Go to **Server Management > Mail Monitor**.
2. Under the **Number of Mails** section, click the time interval you want to further investigate on the chart.
3. Click the **Export** button on the top.
4. MailPlus Server will export the data into an .html file.

Threat monitor

Detailed information on email threats and their sources are displayed in **Threat Monitor**. You can adjust settings according to threat analysis to secure MailPlus Server.

Note:

- If you have already set up a **High-availability cluster**, please view logs on the primary server.



View general threat analysis

General Threat Analysis displays threat data and statistics for outbound and inbound emails with a graphical display. Please refer to the following steps to adjust **General Threat Analysis** settings.

1. Go to **Threat Monitor > Overview**.
2. Threat data and statistics along with their corresponding settings will be displayed in the **General Threat Analysis** section:
 - **Time range:** Select to show threat statistics over a specific time range.
 - **Threat list:** See percentage statistics of each threat type. To see count statistics, hover the mouse to a specific type.
 - **Threat doughnut chart:** See percentage statistics of each threat type. Select or deselect threat types on the right list to suit your needs.
 - **Anti-spam function:** See the anti-spam engine status. To modify its relevant settings, click to jump to the page.
 - **Antivirus function:** See the anti-virus engine status. To modify its relevant settings, click to jump to the page.
 - **DNSBL Self-check:** See if the Synology NAS is on a DNSBL blacklist. Click to see more details.

View external threat analysis

The external threat analysis displays sources of blocked inbound emails and the corresponding count statistics.

1. Go to **Threat Monitor > Overview**.
2. Under the **External Threat Analysis** section, you can find a threat map and count statistics of each source:
 - **Threat map:** Each circle represents a threat source area. A circle expands when more blocked emails come from the area. To see count statistics, hover the mouse to the circle.
 - **Threat Source:** This list shows the top six sources of blocked emails with their corresponding counts.

View blocked inbound and outbound mail

At **Inbound** and **Outbound**, you can find statistics of blocked inbound and outbound emails respectively, along with top senders/recipients of such emails.

1. Go to **Threat Monitor**.
2. Click the **Inbound** or **Outbound** tabs.
 - **Time range:** Select the time range to see statistics of blocked outbound or inbound emails over a specific period.
 - **Blocked Mail Statistics:** The chart shows the trends of each threat type of inbound emails (at **Inbound**) or outbound emails (at **Outbound**) over the selected time range.

Note:

- To change threat types on the display, select or deselect legends under the chart.
- To see count statistics of each threat type, hover the mouse to the chart.

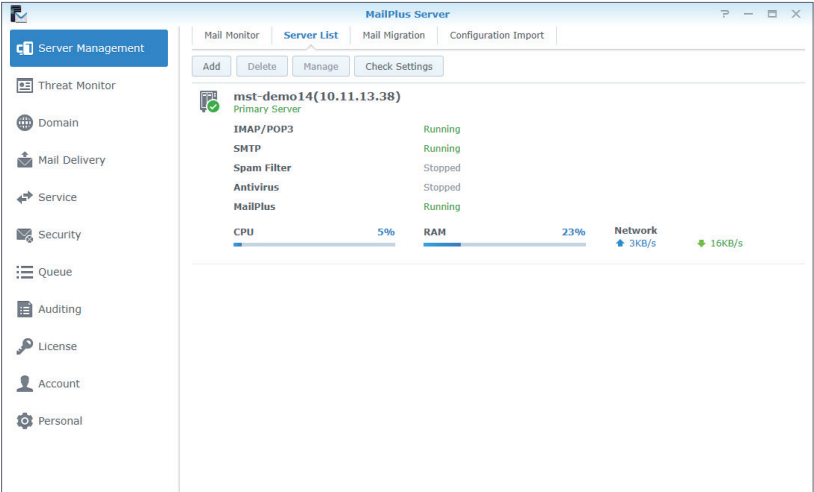
- **Top Senders of Blocked Mail:** The table shows the top 10 senders of blocked inbound emails (at **Inbound**) or outbound emails (at **Outbound**) with count statistics. For a complete list, click **Show All**.
- **Top Recipients of Blocked Mail:** The table shows the top 10 recipients of blocked inbound emails (at **Inbound**) or outbound emails (at **Outbound**) with count statistics. For a complete list, click **Show All**.

Server list

Get a quick overview of MailPlus Server at the **Server List** tab of the **Server Management** page, including information on CPU, RAM, and network usage. Please refer to the following list of possible statuses for each MailPlus Server function:

- **Running:** The function is running properly.
- **Stopped:** The function has not been enabled.
- **Abnormal:** The function is abnormal.

- **Not Installed:** Only applies to MailPlus. This status means you have not installed MailPlus.
- **Getting ready:** This status means you have just enabled or disabled this function, and it is ready to switch the status.
- **Syncing mails:** When you are setting up or removing a MailPlus high-availability cluster, the system will sync emails. This status means the system is syncing emails.



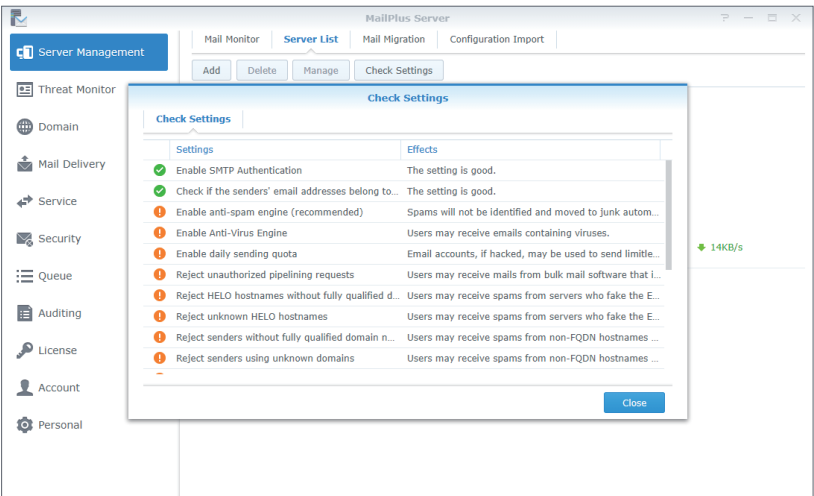
Note:

- If **Antivirus** or **MCP** are enabled, **Spam Filter** will also be enabled even if **Anti-Spam** is not enabled; however, the spam scanning will not be conducted.

Check settings

You can check if your MailPlus Server settings are the same as Synology's suggested settings in **Check Settings**. You can also see the effects of different settings here. Please refer to the following steps:

1. Go to **Server Management > Server List**.
2. Click the **Check Settings** button.



Monitor Mail Queue

You can view pending emails in the mail queue and determine which action to take.

Monitor messages in mail queue

In the **Queue** page, you can check all emails that are pending to be sent to other servers or are to be resent to other servers after the emails have been rejected.

The information regarding emails in the queue will be displayed as follows:

- Date and time when an email entered the queue
- Email sender and recipient
- Why a message is waiting in the mail queue (The **Description** column shows why an email failed to be delivered.)

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

Mail queue statuses are categorized into the following three types:

- **Hold:** Messages are to be processed.
- **Active:** Messages are now being processed.
- **Deferred:** Messages failed to be delivered and will be resent later.

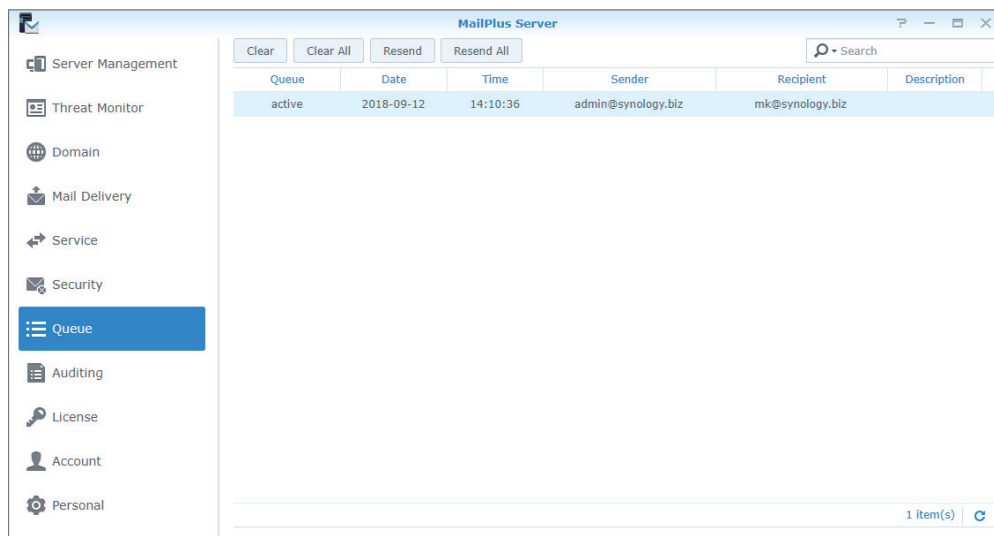
Note:

- Deferred emails will be returned to senders if all redelivery attempts fail during the following five days.

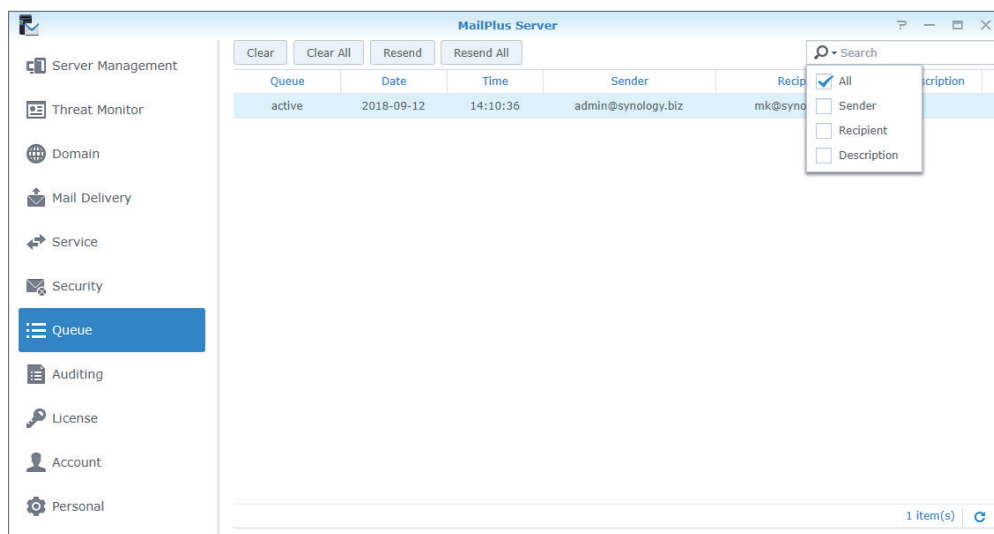
Manage messages in mail queue

You can choose to immediately redeliver or cancel the delivery for messages in the queue. Please refer to the following steps to manage messages in the mail queue:

- Go to **Queue** to do the following:
 - To redeliver a message, select the message in the mail queue and click the **Resend** button. The status of the message will switch from **Hold** to **Active**.
 - To remove a message, select the message in the mail queue and click the **Clear** button. The message will be removed from the queue.
 - To resend all messages, click the **Resend All** button.
 - To remove all messages, click the **Clear All** button.



- You can also search for messages in the search bar in the upper-right corner of the page to view the statuses of the messages.



Monitor Mail Log

Mail logs record all activities of the server. You can view log content to find the root problems and the solutions to problems. Please note that log files may account for a large capacity of storage space.

The following log settings can be configured in the **Auditing** page.

- **View Logs:** View, search, and analyze the messages recorded in logs.
- **Archive and Manage Logs:** Configure various management settings such as archive intervals, backup, rotation rules, and sending logs to the secondary server.
- **Log Report:** Allow logs to be sent through email notification regularly.

View mail logs

Please refer to the following steps to view mail logs:

1. Go to **Auditing > Log**.
2. From the drop-down menus at the top, select **Mail log** and **Internal database**.
3. Mail logs display the message ID, the date and time generated, the sender, recipient, title, size, and status of each message. The statuses are categorized as follows:
 - **Received:** This status means a MailPlus user has received a message. If a MailPlus user has sent a message to another MailPlus user, then the status on the log records will be shown as **Received**. If multiple MailPlus users receive the same message, multiple log records will be generated. However, if the message is sent to an alias email address in MailPlus Server, the log record will be generated for the alias email address even if the alias includes multiple recipient addresses, and that some of the users in the alias are from other servers. If auto-forwarding is enabled, log records with **Received** status will be generated whether the **Keep mail copy in the Inbox** checkbox is ticked or not.
 - **Sent:** When messages are sent to email addresses from other servers, multiple log records will be generated if the recipient includes multiple email addresses from other servers.
 - **Resent:** This status means there have been several attempts to resend messages to email addresses from other servers. This status will no longer be used in MailPlus Server 1.3.0-0370 and above.
 - **Failed:** This status means messages sent to other servers failed to be delivered.

Note:

- If you have set up **Auto BCC** rules, **Auto-Forwarding**, or **Auto Reply**, additional log content may be generated.
- If you have set up a **High-availability cluster**, please view logs on the primary server.

View security logs

Security logs display the time and date an event is generated, along with the source, sender, recipient, title, type, and event description. Security logs are categorized as follows: **Rejected**, **Spam**, **Virus**, **DNSBL**, **Malicious Content**, **Attachment Filter**, **Blacklist**, **SPF**, **DKIM**, **DMARC**, and **Data Protection**, all of which are related to security settings in MailPlus Server. The **Rejected** type means that MailPlus Server has rejected a message after running full analysis. Please refer to the following steps to view security logs:

Note:

- If you have already set up a [High-availability cluster](#), please view logs on the primary server.

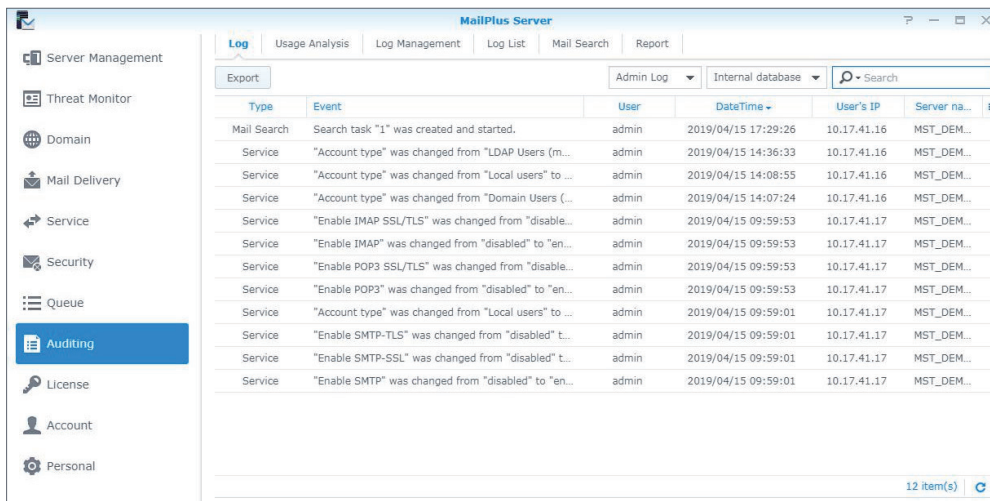
1. Go to **Auditing > Log**.
2. From the drop-down menus at the top, select **Security log** and **Internal database**.

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...	test5@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

View administration logs

Administration logs record changes made to MailPlus Server settings. Each log shows a brief description of the event, along with the type, user, time and date, user's IP address, and server name. Please refer to the following steps to view administration logs:

1. Go to **Auditing > Log**.
2. From the drop-down menus at the top, select **Admin log** and **Internal database**.



The screenshot shows the MailPlus Server interface with the 'Auditing' tab selected. The 'Log' sub-tab is active, displaying a table of log entries from the internal database. The table has columns for Type, Event, User, DateTime, User's IP, and Server name. The log entries show various system events such as 'Search task "1" was created and started', 'Account type' changes, and 'Enable IMAP/POP3/SMTP' status changes, all performed by the 'admin' user.

Type	Event	User	DateTime	User's IP	Server name
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...

View external database

If you have archived logs, generated a log database, or downloaded log files, you can view log content stored in **External database**.

Please refer to the following steps to view the external database:

1. Go to **Auditing > Log**.
2. From the drop-down menus at the top, select **Mail log**, **Security log**, or **Admin log** and select **External database**.

Server Management

Threat Monitor

Domain

Mail Delivery

Service

Security

Queue

Auditing

License

Account

Personal

Log

Usage Analysis

Log Management

Log List

Mail Search

Report

Export

Mail Log

Internal database

External database

Search

Search

Message ...	Date	Time	Sender	Original Re...	Title	Ma...	Status
442875c...	201...	19:14:47	Jonathan@...	-	Test Mail	1.1...	Sent
c737a3d...	201...	12:33:11	Jonathan@...	-	jps@texteri... Test from MailPl...	0.8...	Sent
0bf953a...	201...	13:09:23	Jonathan@...	Jonathan@...	Jonathan Testing the look...	0.8...	Recei...
827bc2b...	201...	15:32:20	MK@synolo...	-	andrew802... test	0.9...	Sent
527dbdc...	201...	15:33:45	MK@synolo...	-	andrew802... test	0.9...	Sent
f21bffb...	201...	15:56:06	MK@synolo...	admin@sy...	admin test	0.9...	Recei...
201...	201...	15:33:29	SYSTEM	-	patrick@sy...	5.1...	Failed
201...	201...	15:37:24	SYSTEM	-	patrick@sy...	1.5...	Failed
201...	201...	12:00:04	SYSTEM	-	patrick@sy...	1.4...	Failed
201...	201...	09:37:14	SYSTEM	-	patrick@sy...	3.7...	Failed
201...	201...	13:59:41	SYSTEM	-	synology@...	95...	Failed
201...	201...	22:29:07	SYSTEM	-	synology@...	1.4...	Failed
201...	201...	21:06:53	SYSTEM	-	synology@...	1.2...	Failed
201...	201...	16:51:02	SYSTEM	-	jero@synol... Undelivered Ma...	1.0...	Failed
2017101...	201...	22:47:11	SYSTEM	-	patrick@sy... Undelivered Ma...	38...	Failed

<<

1

2

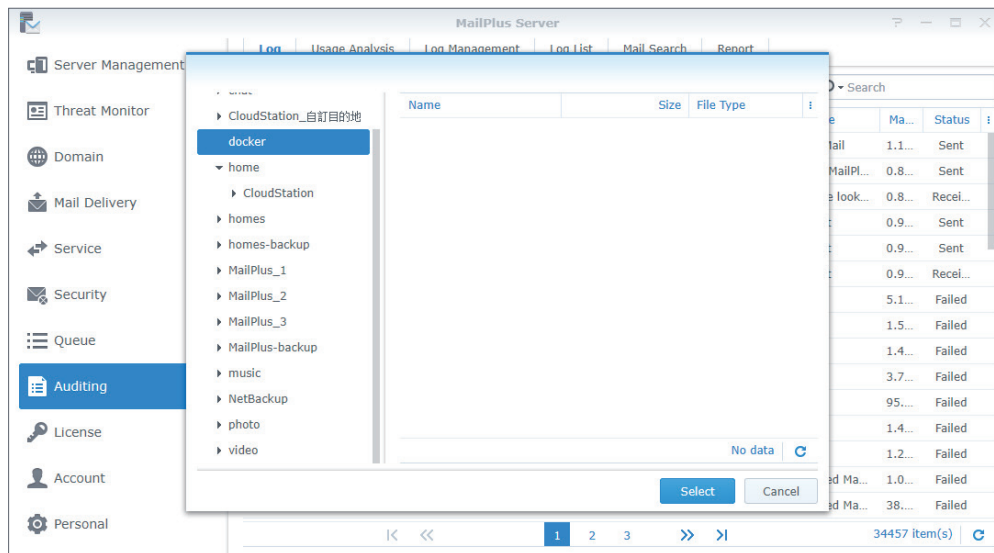
3

>>

>

34453 Item(s)

3. Find the location of your external database on the Synology NAS.
4. Click the **Select** button.

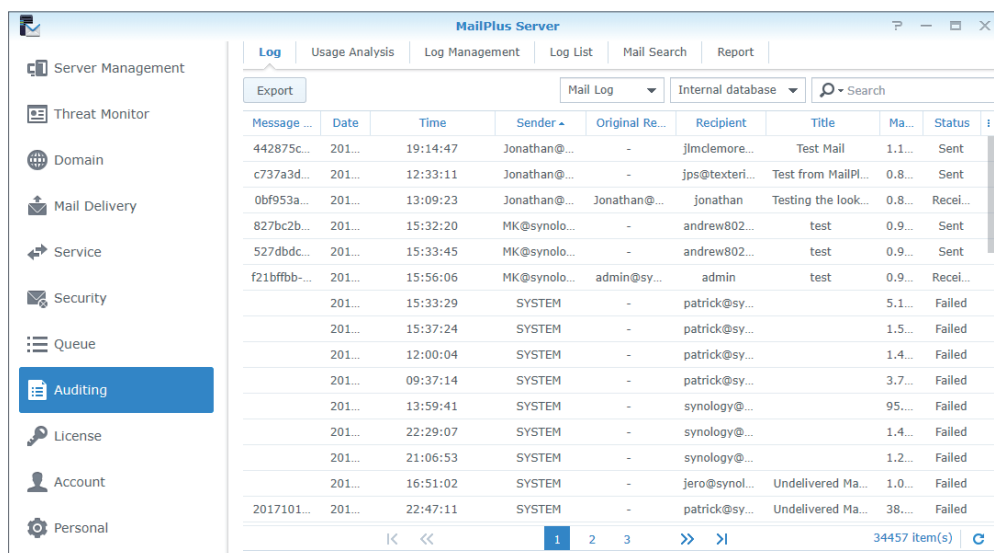


Search logs

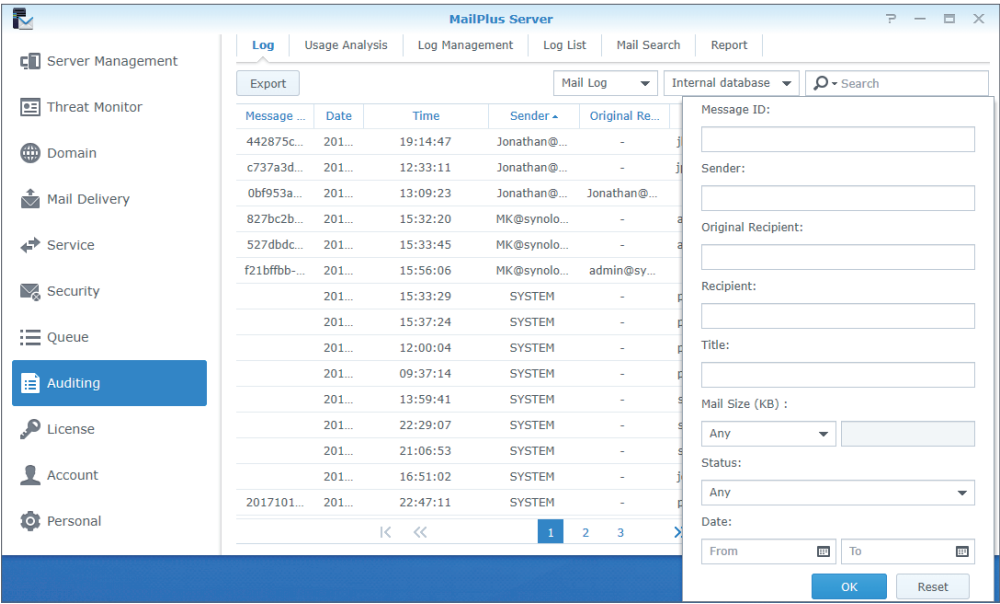
At **Auditing > Log**, you can search for logs using the simple search or the advanced search.

- **Simple search:** You can enter keywords in the search field in the upper-right corner of the page:

- For **Mail log**, the entered keywords are used to search for content in the **Message ID**, **Sender**, **Recipient**, and **Title** columns.
- For **Security log**, the entered keywords are used to search for content in the **Source**, **Sender**, **Recipient**, **Title**, and **Event** columns.
- For **Admin log**, the entered keywords are used to search for content in the **Type**, **Event**, **User**, **User's IP**, and **Server name** columns.



- **Advanced search:** You can click the magnifying glass icon in the search bar in the upper-right corner of the page. Set up search criteria for each item to conduct a precise advanced search. Click **OK** after you finish the settings. From the **Status** drop-down menu, you can select **Within domain** to search for messages sent within internal users.

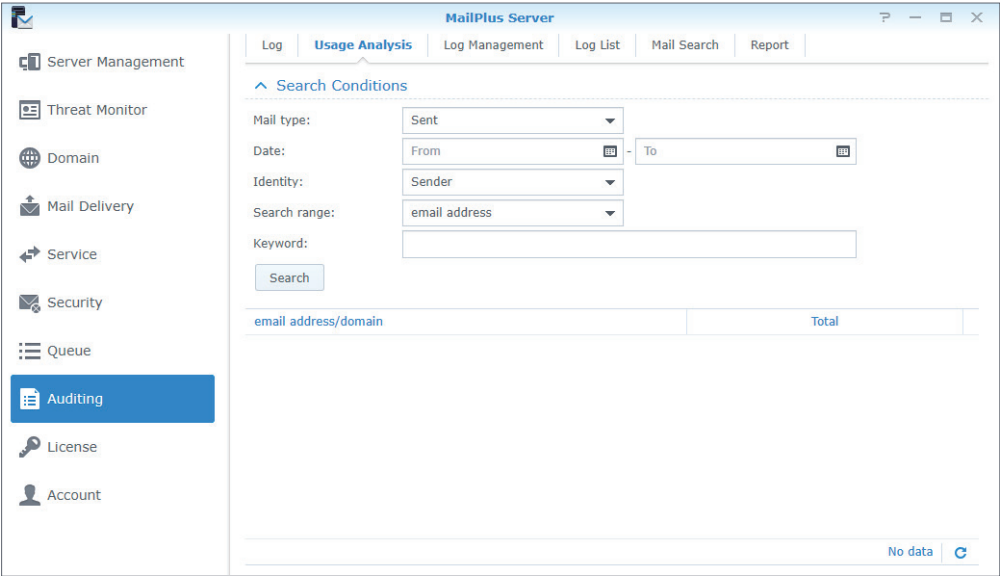


Export log content

You can export logs as an .html file at **Auditing > Log**. If you click the **Export** button after log search, the search results will be exported. Please refer to [Search logs](#).

Usage analysis

You can conduct usage analysis at **Auditing > Usage Analysis** to analyze inbound and outbound messages sent by each email address or domain.



Archive logs

You can configure log archiving settings. MailPlus Server will archive mail logs, security logs, and Postfix logs on a user-defined schedule. Please note that the archive feature will be automatically disabled once you cannot access the shared folder.

Please refer to the following steps to archive logs:

1. Go to **Auditing > Log Management**.
2. Under the **Log Archiving** section, tick the **Enable log archiving** checkbox.
3. Click the **Select** button next to the **Archive destination** field and select the destination for archive files.
4. Select the time to run archiving tasks.
5. Click **Apply** to save the settings.

The screenshot shows the MailPlus Server web interface. The left sidebar contains navigation links: Server Management, Threat Monitor, Domain, Mail Delivery, Service, Security, Queue, Auditing (highlighted), License, and Account. The main content area has tabs for Log, Usage Analysis, Log Management (active), Log List, Mail Search, and Report. Under the Log Management tab, there are two sections: Log Archiving and Log Transfer. The Log Archiving section is highlighted with a red box and contains:

- ☐ Enable log archiving
- Archive destination: Select shared folders (button) and Select (button)
- Run on the following days: Sat (dropdown)
- Run task: 01 (dropdown) : 00 (dropdown)

 The Log Transfer section contains:

- ☐ Transfer logs to the secondary server
- ☐ Transfer logs to a syslog server
- Server: Enter the server IP (text input)
- Port: 514 (text input)
- Transfer protocol: UDP (dropdown)
- Log format: BSD (RFC 3164) (dropdown)
- ☐ Enable secure connection (SSL)
- Import Certificate (button)

 At the bottom right of the main content area are Apply and Reset buttons.

Transfer logs to the secondary server

After a **High-availability cluster** is set up, logs will be collected to the primary server. You can send a copy to the secondary server. Sending logs to the secondary server requires a log database to be generated (please refer to **Generate log database**). Please refer to the following steps to send logs to the secondary server:

1. Go to **Auditing > Log Management**.
2. Under the **Log Transfer** section, tick the **Transfer logs to the secondary server** checkbox.
3. Click **Apply** to save the settings.

Transfer Postfix logs to other syslog servers

Please refer to the following steps to send Postfix logs to other syslog servers:

1. Go to **Auditing > Log Management**.
2. Under the **Log Transfer** section, tick the **Transfer logs to a syslog server** checkbox.
3. Enter the information of the syslog server.
4. If you tick the **Enable secure connection (SSL)** checkbox, you might need to click the **Import Certificate** button to import the certificate of the syslog server before sending logs.
5. Click **Apply** to save the settings.

The screenshot shows the MailPlus Server interface with the 'Log Management' tab selected. The 'Log Transfer' section is highlighted with a red box. It contains the following settings:

- ☐ Transfer logs to the secondary server
- ☐ Transfer logs to a syslog server
 - Server: Enter the server IP
 - Port: 514
 - Transfer protocol: UDP
 - Log format: BSD (RFC 3164)
 - ☐ Enable secure connection (SSL)
 - Import Certificate

At the bottom right of the 'Log Transfer' section are 'Apply' and 'Reset' buttons.

Set up log rotation rules

You can set up the rotation period and the file size for Postfix logs. The 400 million most recent entries from the mail log database and security log database will be retained.

Please refer to the following steps to set up log rotation rules:

1. Go to **Auditing > Log Management**.
2. Under the **Log Rotation Rules** section, enter a value in the **Log file size is larger than (MB)** field.
3. Under the **Log Rotation Rules** section, tick the **Log rotation period** checkbox and select a rotation period from the drop-down menu.
4. Click **Apply** to save the settings.

The screenshot shows the MailPlus Server interface with the 'Log Management' tab selected. The 'Log Transfer' section has two unchecked checkboxes: 'Transfer logs to the secondary server' and 'Transfer logs to a syslog server'. Below these are input fields for 'Server' (placeholder: 'Enter the server IP'), 'Port' (514), 'Transfer protocol' (UDP), and 'Log format' (BSD (RFC 3164)). There is also an unchecked checkbox for 'Enable secure connection (SSL)' and an 'Import Certificate' button. The 'Log Rotation Rules' section, highlighted with a red box, contains the text 'Rotate the Postfix logs when any one of the following conditions occurs'. It has two settings: 'Log file size is larger than (MB)' set to 30, and 'Log rotation period' set to Daily. At the bottom right are 'Apply' and 'Reset' buttons.

Download and delete log files

You can save or remove mail logs, security logs, admin logs, or Postfix logs at **Auditing > Log List**.

Please refer to the following steps to download and delete log files:

1. Go to **Auditing > Log List**.
2. Select **Mail Log**, **Security Log**, **Admin Log**, or **Postfix Logs** from the drop-down menu at the top.
3. If you have set up a MailPlus high-availability cluster and enabled **Transfer logs to the secondary server**, you can select **Received logs** from the drop-down menu on the secondary server; otherwise, select **Main log**.
4. After selecting a log file, you can click the **Download** button to download the file or click the **Delete** button to delete the file from the server.

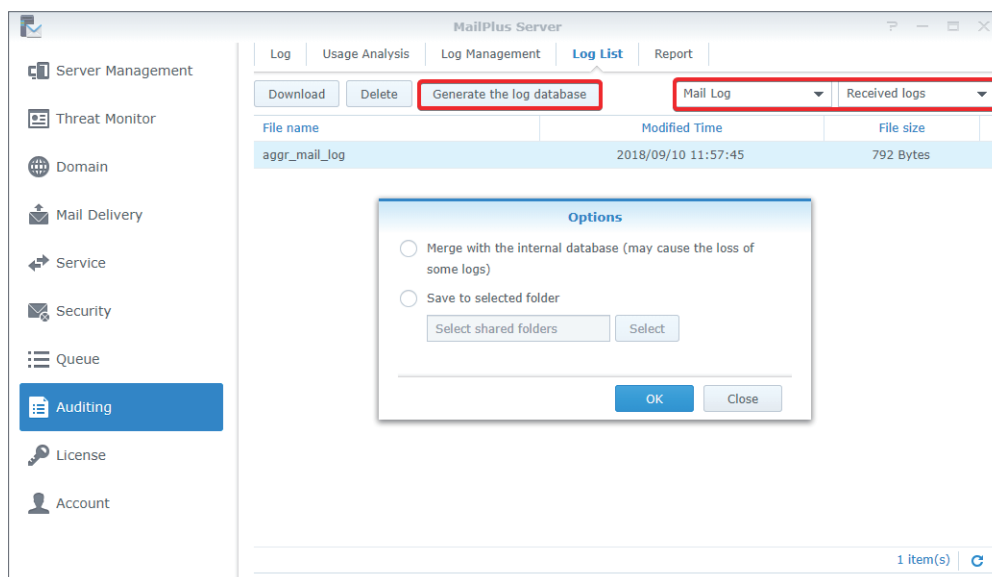
The screenshot shows the MailPlus Server interface with the 'Log List' tab selected. At the top, there are buttons for 'Download', 'Delete', and 'Generate the log database'. Below these are two dropdown menus: 'Mail Log' and 'Main log'. A table displays log files with columns for 'File name', 'Modified Time', and 'File size'. The table contains one row: 'aggr_mail_log.db' with a modified time of '2018/08/06 10:53:45' and a file size of '12.0 KB'. At the bottom right, it says '1 item(s)' with a refresh icon.

File name	Modified Time	File size
aggr_mail_log.db	2018/08/06 10:53:45	12.0 KB

Generate log database

If you have enabled **Transfer logs to the secondary server**, you can convert received log content back to database files using the **Generate log database** feature. You can **View external database** at **Auditing > Log** to view files in the log database.

1. Go to **Auditing > Log List**.
2. Select **Mail log**, **Security log**, or **Postfix log** from the drop-down menu.
3. Select **Received log** from the drop-down menu.
4. Select a log file and click the **Generate Log Database** button.
5. Select the **Merge with the internal database (may cause the loss of some logs)** or **Save to selected folder** option and choose a destination folder.
6. Click **OK** to finish the settings.



Note:

- You do not need to generate a log database for **Admin log**. You can view it on both servers after enabling the **Transfer logs to the secondary server** option.
- Only logs that are generated after you enabled the **Transfer logs to the secondary server** option will be synchronized to the other server.

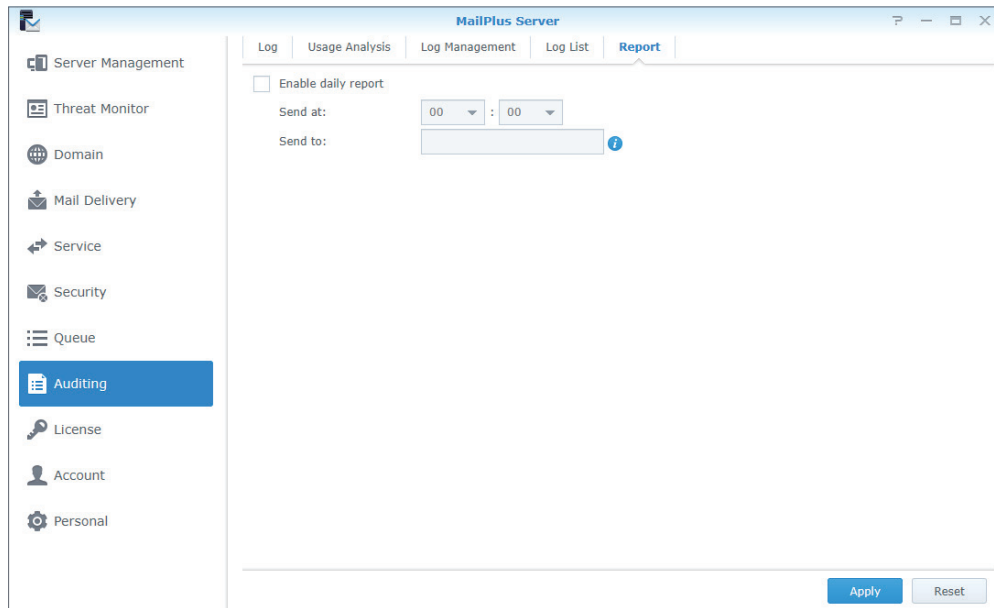
Set up daily reports

You can enable the daily report feature to allow Postfix logs from the previous day to be sent to a specific email address.

Please refer to the following steps to set up daily reports.

1. Go to **Auditing > Report**.
2. Tick the **Enable daily report** checkbox.
3. Select a delivery time.

4. In the **Send to** field, enter the destination address for daily reports. You can specify up to two email addresses which should be separated by a semicolon (;).



Set up mail searches

You can find all indexed emails in MailPlus Server, as well as view, delete, and export search results.

Please refer to the following steps to create a mail search task:

1. Go to **Auditing > Mail Search**.
2. Click the plus icon (+) to create a new task.
3. Enter a **Task name**.
4. Set **Search Conditions**:
 - **Pre-defined conditions**: You can add multiple search conditions to a search task. Select from the drop-down menu to find emails that match **All** or **Any** of conditions and define the conditions by **Sender**, **Recipient**, **Subject**, **Keyword**, **Mail Size (MB)**, or **Date** that **includes** or **excludes** the entered keywords.
 - **Custom**: You can also customize search conditions using search operators and keywords. For example, to look for an email about *GDPR* sent after *May 25th, 2018* from the address *admin@synology.com*, you can enter *after:2018/05/25 AND from:admin@synology.com AND GDPR* as your search condition.

Search Operator	Usage	Example
from:	Messages from the specified sender	from:amy
to:	Messages sent to the specified recipient	to:david

Search Operator	Usage	Example
subject:	Messages with certain words in the subject line	subject:dinner
OR	Messages that match multiple specified terms	from:amy OR from:david
- or NOT	Messages that should be removed from search results	dinner - movie
()	Messages containing the specified terms grouped together	subject:(dinner movie)
in:	Messages in the specified mailbox	in:"feature suggestions"
label:	Messages that have a certain label	label:friends
before: or after:	Messages sent during a certain period	after:2004/04/16
larger: or smaller:	Messages larger or smaller than a certain size in MB	larger:10M
filename:	Attachments with a certain name or file type	filename:pdf
has:attachment	Messages with attachments	has:attachment
is:starred	Starred messages	is:starred
is:unread	Unread messages	is:unread

5. Set **Target User**. If no target users are specified, the task will search all users by default.
6. Click **OK** and the search task will start immediately.
7. You can stop a task in progress by selecting the task and clicking **Stop tasks** on the right panel. Click **Search** if you want to restart a task.
8. You can **Edit**, **Copy**, or **Delete** a task by selecting it and clicking on the corresponding icon.

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

View mail search results

1. Go to **Auditing > Mail Search** and select a complete search task.
2. On the right panel, you can **Download task reports** or click **View Result** for further details and actions. Task reports allow you to view the details of a task, including the number of searched emails as well as which emails have been deleted.
3. In the **View Result** window, you can view, delete, or export each email. Details of each email will appear in the right section when you select it. You can also download the original mail or its attachments or open the email in a new tab.

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

Export mail search results

We recommend that you always export important mail search results and keep them on your local device as backup files in case of future needs.

1. Go to **Auditing > Mail Search** and select a complete search task.
2. Select a task and click **View Result** on the right panel.
3. Select the search results you wish to export and click **Export**.
4. You can click the arrow icon next to the **Export** button to further specify whether to export both the mail list and the original emails or only the mail list.
5. The exported mail list can be found as a file named **export_list.csv** and can be edited with editors supporting .csv files. If you wish to distribute an auditing task, you can split the record into multiple files. Exported original mails can be found as .eml files in the **eml** folder.

Import mail search results

If you have exported mail search results and saved them to your local device, you can always import the mail list to check the emails.

1. Go to **Auditing > Mail Search**.
2. Click the **Import tasks** icon next to the trash can icon.
3. Upload a mail list in CSV format and enter a task name.
4. Click **Import**.
5. Once the import is complete, the task will appear at the top of the task list.

Chapter 11: Disaster Recovery

High-Availability Cluster

MailPlus Server provides two solutions: **single node** configuration and **high-availability** configuration. Single node configuration requires one Synology NAS to run mail services while high-availability configuration requires two Synology NAS to form a high-availability (HA) cluster, which can ensure uninterrupted mail services during unexpected events.

High-availability (HA) configuration introduction

The high-availability (HA) cluster is composed of two Synology NAS, one of which takes the role of the "primary server" and the other acts as the "secondary server". Users and other mail servers connect to the main IP address of the MailPlus HA cluster. The primary server runs on the main IP address of the MailPlus HA cluster and receives all service requests. These requests will then be assigned to either the primary or secondary server to be processed.

A two-way synchronization will be performed to ensure mail data and server settings remain consistent and synchronized across primary and secondary servers. When two servers process different service requests or when you edit settings of MailPlus Server on one of the servers, the two-way synchronization feature can minimize the probability of data inconsistency.

Unlike mail data and server settings, logs will be collected to the primary server under the HA configuration. Please view logs on the primary server or [Transfer logs to the secondary server](#) to send a copy.

The HA configuration minimizes service disruptions caused by server malfunctions. When the primary server malfunctions, the secondary server will temporarily take over all mail service requests. After the primary server recovers, data modifications that have been processed during the failover period will be synchronized back to the primary server. When the secondary server malfunctions, the primary server will assume all workload and data modifications processed during the period will also be synchronized to the secondary server after it recovers.

Note:

- MailPlus high-availability cluster and Synology High Availability (SHA) are two different cluster systems and cannot run on the same Synology NAS simultaneously.
- Synology High Availability is supported for MailPlus 2.2 and above.
- If service continuity is required, please consider MailPlus high-availability cluster designed for mail services. After a high-availability cluster recovers, data will remain consistent across both servers, preventing the loss of data updated during the split-brain error.
- Under SHA, two MailPlus servers will be considered as one and will share 5 free licenses. In comparison, under MailPlus HA, 10 free licenses will be available for use.

Before configuring high-availability (HA)**1. Prepare two Synology NAS:**

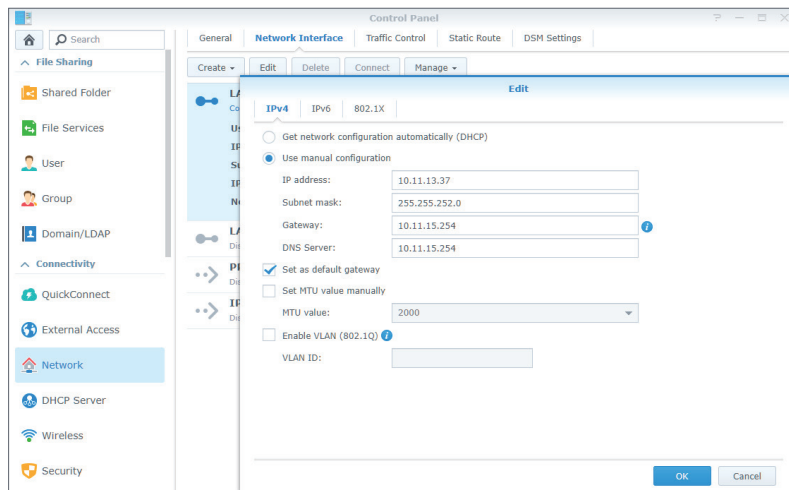
- Sign in to the same Synology Account at **Control Panel > Info Center > Synology Account** on the two Synology NAS.
- Synchronize the system time between the two Synology NAS at **Control Panel > Regional Options > Time**.
- Go to **Package Center** to install and initialize **MailPlus Server** and **MailPlus** on both Synology NAS. For more information on how to set up MailPlus Server, you can refer to the [Set up MailPlus Server](#) section.
- After you set up MailPlus Server, a **MailPlus** shared folder will be automatically added to the Synology NAS. To ensure client users can access MailPlus, we do not recommend that you edit permissions on your own. Please set the permission settings of the **MailPlus** shared folder as default.
- Set the target users' or groups' privileges to MailPlus Server and MailPlus at **Control Panel > Privileges**. The settings should be identical between the two Synology NAS.

Note:

- The size of the volumes on which MailPlus Server is located should be the same. In addition, since all inbound and outbound emails will be fully synchronized to both volumes, please make sure the volume size can meet the email storage requirement.
- If you have mounted SSD caches on both volumes, please note the following:
 - They should be read-write caches in a RAID 1 configuration.
 - The cache size should be the same.
- The 2-step verification feature must be temporarily disabled on the secondary server during the HA cluster creation.

2. Assign two sets of static IP addresses for the primary and secondary servers:

- The IP addresses for both Synology NAS must be under the same LAN.
- The IP addresses must not be retrieved via PPPoE or DHCP.
- The network card of the IP address should be set up to perform manual network configuration.



3. Both Synology NAS must join the same domain:

- Both Synology NAS must join a Windows Active Directory or an LDAP server. For information on how to join a Windows Active Directory, please refer to [this tutorial](#). For more information on how to join an LDAP server, please refer to [this help article](#).
- If you do not have Windows Active Directory or LDAP server in your environment, you can go to **Package Center** and install **Synology Directory Server** or **LDAP Server** to set up a domain or an LDAP server for account management. Please note that using self-hosted LDAP or domain services has the risk of mail service interruption when the Synology NAS hosting the directory is abnormal or unresponsive.

4. Prepare an internal IP address and external IP address for the HA cluster:

- Reserve an unused static internal IP address which should be in the same LAN as the two Synology NAS' IP addresses, and an unused external IP address for the HA cluster.
- Configure port-forwarding rules on the router to forward traffic between the internal and external cluster IP addresses.
- Register the external cluster IP address on a public DNS (Domain Name System) server.

Configure high-availability (HA)

1. Launch MailPlus Server after it has been set up.
2. Go to **Service** and check if you have selected **Domain Users** or **LDAP Users** from the **Account type** drop-down menu under the **SMTP** section.

The screenshot shows the 'MailPlus Server' configuration window. On the left is a sidebar with navigation options: Server Management, Threat Monitor, Domain, Mail Delivery, Service (highlighted), Security, Queue, Auditing, License, Account, and Personal. The main panel is divided into sections: SMTP, Network Interface, and IMAP/POP3. Under SMTP, there are checkboxes for 'Enable SMTP', 'Enable SMTP-SSL', and 'Enable SMTP-TLS', all of which are checked. Below these are input fields for 'Account type' (set to 'LDAP Users (synology.mst)'), 'Port' (25), 'Port' (465), and 'Port' (587). The 'Network Interface' section has a dropdown menu set to 'LAN 1 (10.11.13.38)'. The 'IMAP/POP3' section has checkboxes for 'Enable POP3', 'Enable POP3 SSL/TLS', 'Enable IMAP', and 'Enable IMAP SSL/TLS', all of which are checked. At the bottom right are 'Apply' and 'Reset' buttons.

3. Go to **Server Management > Server List** and click the **Add** button.

4. Enter the main internal IP address for the HA cluster and click **Next**.

The screenshot shows the 'MailPlus Server' 'Server List' window. The sidebar is the same as in the previous screenshot. The main panel has tabs for 'Mail Monitor', 'Server List' (active), 'Mail Migration', and 'Configuration Import'. Below the tabs are buttons for 'Add', 'Delete', 'Manage', and 'Check Settings'. A list of servers is shown, with 'MailPlus_demo(172.22.1.15)' selected and labeled as 'Primary Server'. An 'Add server node' dialog box is open in the foreground. It contains the text: 'To use two servers as the mail system, please create the mail cluster. Set the information of the mail cluster.' Below this are input fields for 'Mail System IP:' (172.22.1.19) and 'Subnet mask:' (255.255.255.0). At the bottom of the dialog are 'Next' and 'Cancel' buttons. In the background, a 'Network' status bar shows '5KB/s' and '8KB/s'.

5. Enter the IP address of the secondary server in the **Server Address** field or select a Synology NAS to use as the secondary server from the **Server Address** drop-down menu. Synology NAS under the same LAN will be searched and included in this drop-down menu.

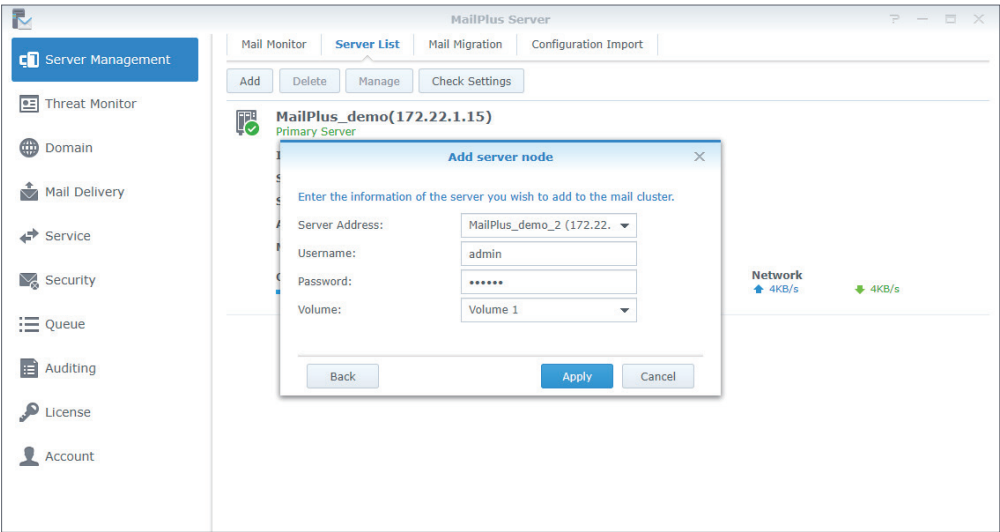
Note:

- Secondary servers need to bind to a **Network Interface**. You will need to enter the IP address of the bound network interface.

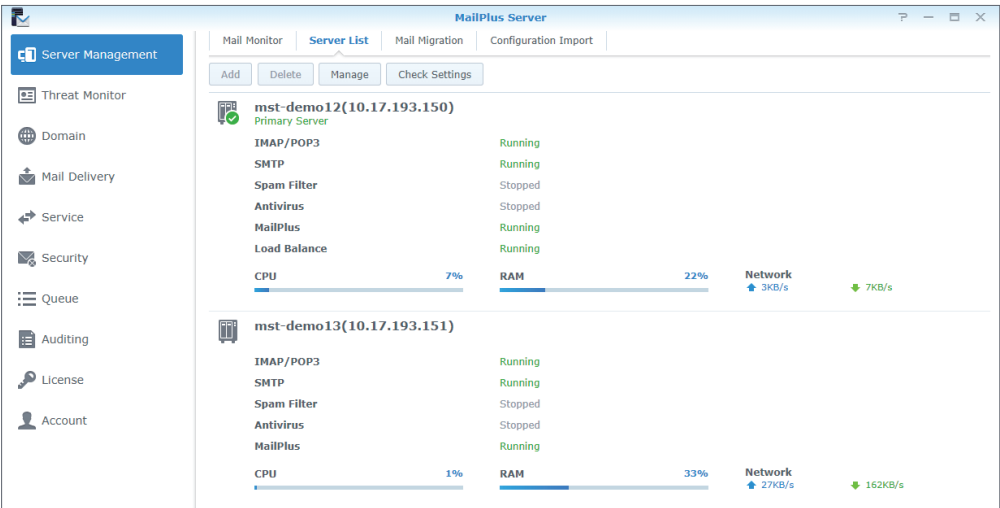
6. Enter the credentials of an account from the administrator group on the secondary server in the **Username** and **Password** fields. Please note that the 2-step verification must be temporarily disabled on the secondary server during the HA cluster creation.

7. In the **Volume** drop-down menu, you will find a list of volumes that have been created on the secondary server. Please select the volume used for saving mail data and MailPlus related files on the secondary server.

8. Click **Apply** after confirming that the settings are correct.



9. After you complete the settings, emails will be synchronized to the secondary server. The time required for the synchronization depends on the number of emails stored on the primary server. During the synchronization, you can still send and receive emails. All services will be processed by the primary server until the synchronization is complete. After the synchronization is complete, the primary and secondary server will share the workload.



Note:

- During the first synchronization, MailPlus services are available but relatively slow due to the high server load. Therefore, if you have used MailPlus Server for quite a while and there is a large number of emails, we recommend that you copy most emails to the secondary server using **Hyper Backup** in advance to shorten the loading time and speed up the synchronization. For detailed instructions on using **Hyper Backup** to back up emails, please refer to [Back up and Restore Email](#).

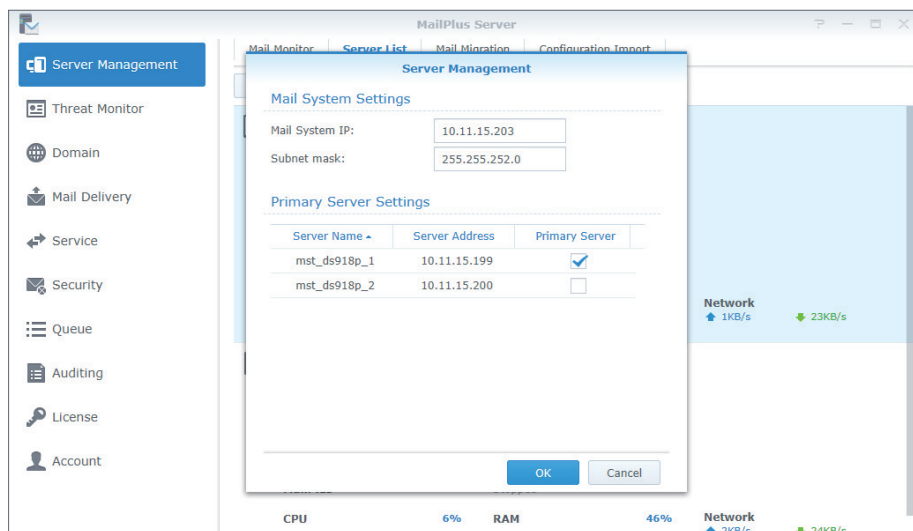
Modify high-availability (HA) cluster configuration

1. Launch MailPlus Server after it has been set up.
2. Go to **Server Management > Server List**.
3. Click the **Manage** button.
4. Under the **Mail System Settings** section, you can modify the IP address and subnet mask settings of the HA cluster.

Note:

- The modified IP address and subnet mask must be under the same LAN as the IP address of the primary and secondary servers.

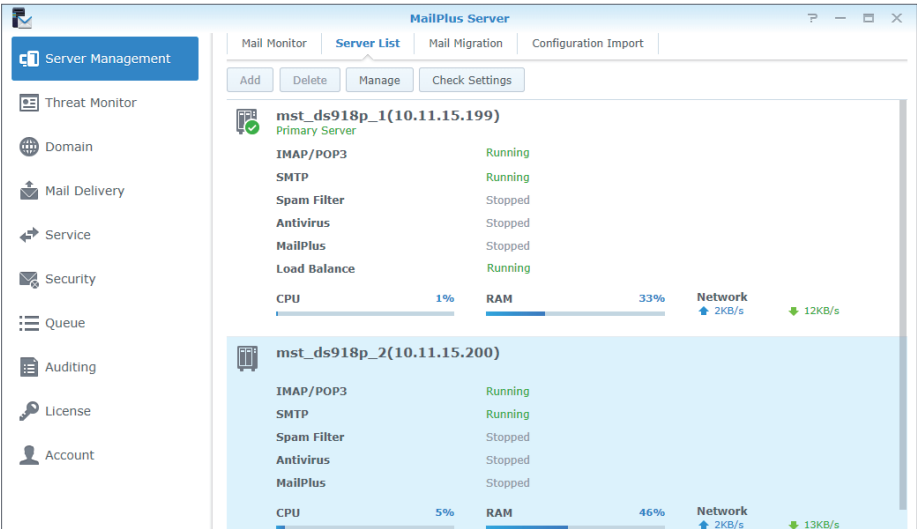
5. Under the **Primary Server Settings** section, you can select a Synology NAS to act as the primary server of the HA cluster. The primary server runs on the internal IP address of the HA cluster and receives all mail service requests. These requests will then be assigned to either the primary or the secondary server.



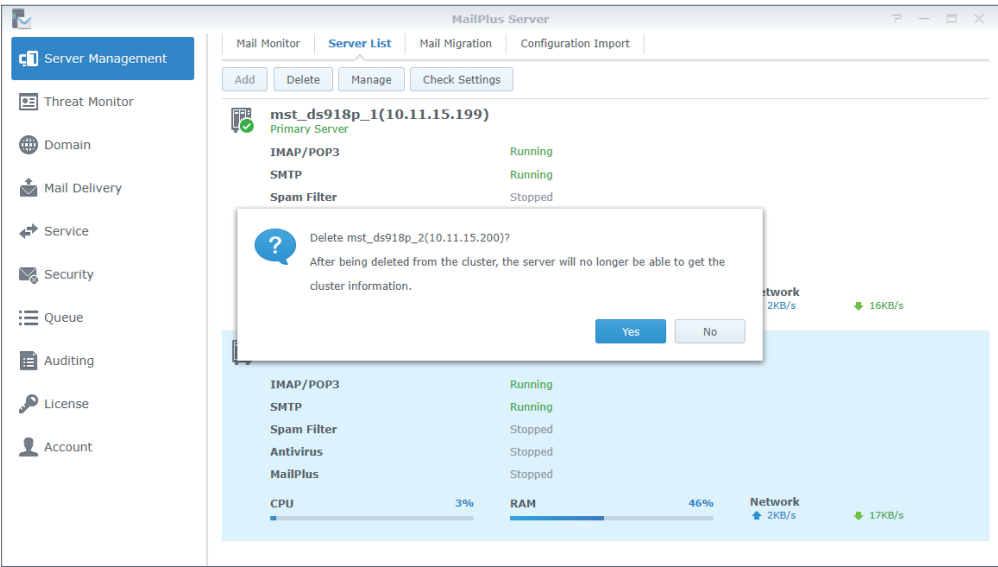
Remove high-availability (HA) configuration

When you remove a HA configuration, mail data will be synchronized across the two Synology NAS to ensure data consistency. After the configuration removal, the internal IP address of the HA cluster will no longer be used by any of the Synology NAS. You may need to adjust the port forwarding and demilitarized zone (DMZ) settings of your firewall device or modify relevant DNS records. Please refer to the following steps to remove one of the Synology NAS from the HA cluster:

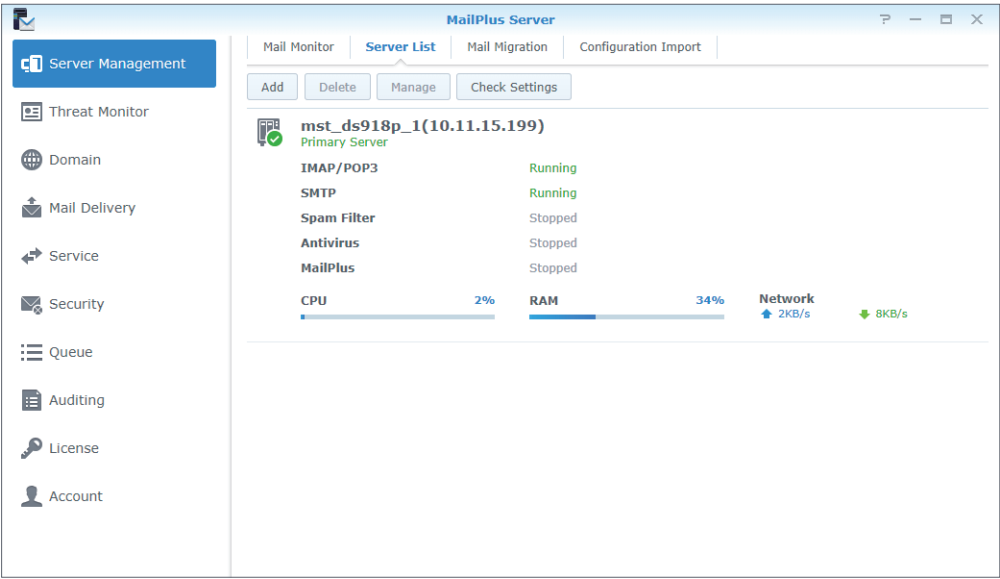
1. Sign in to DSM of the Synology NAS you wish to keep and launch MailPlus Server.
2. Go to **Server Management > Server List**.
3. Select the Synology NAS you want to remove.



- 4. Click the **Delete** button.
- 5. Click **Yes** in the pop-up confirmation box.



- 6. After all emails are synchronized, the HA cluster will be dissolved. The server you would like to keep will continue to receive and process mail service requests. Please check if you need to adjust port forwarding or demilitarized zone (DMZ) settings of your firewall device or modify your DNS records.



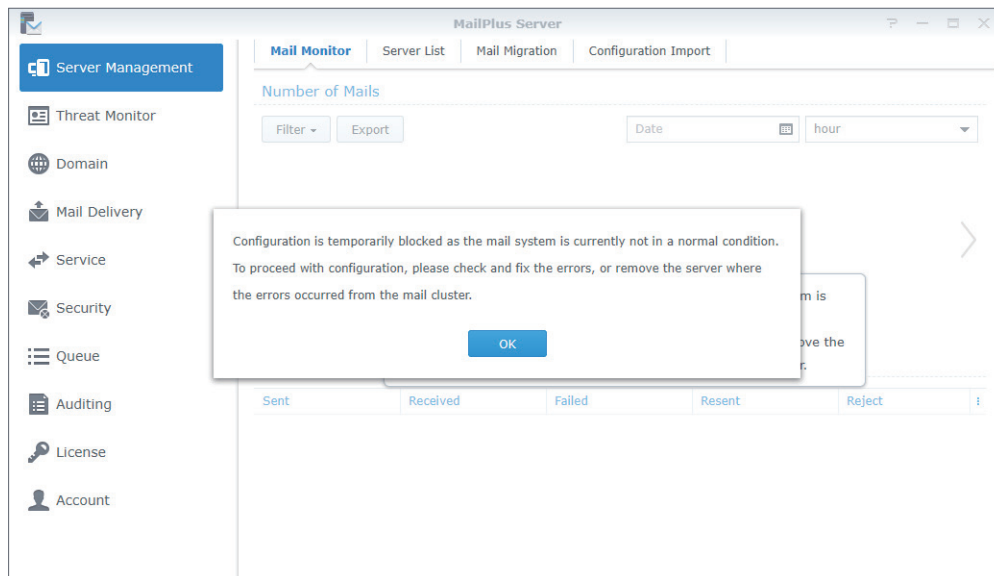
Server malfunction

When one of the Synology NAS in the HA cluster malfunctions, the other one will continue to provide mail services. The primary and secondary servers mentioned in the following sections refer to the original roles of the servers under HA configuration, not the roles after the switchover.

Primary server malfunction

When the original primary server malfunctions, the original secondary server will take over the internal IP address of the HA cluster. It starts to receive and process service requests independently. Under the circumstances, when you launch MailPlus Server on the original secondary server, a mail system alert window will appear, and you will not be able to adjust settings of the MailPlus Server during the switchover.

The primary server needs to be recovered at the earliest opportunity. If the original primary server cannot be recovered, please refer to [Remove High-availability \(HA\) configuration](#) to remove it. After the removal, MailPlus Server will run on a single-node configuration.



Secondary server malfunction

When the original secondary server malfunctions, the original primary server will take over the internal IP address of the HA cluster and process all service requests independently. Please recover the original secondary server at the earliest opportunity. If the original secondary server cannot be recovered, please refer to [Remove High-availability \(HA\) configuration](#) to remove it. After the removal, MailPlus Server will run on a single-node configuration.

Back up and Restore Email

You can use backup features on DSM to back up MailPlus Server. MailPlus Server backup includes the following:

- **System configuration backup**
- **Mailbox and email backup**

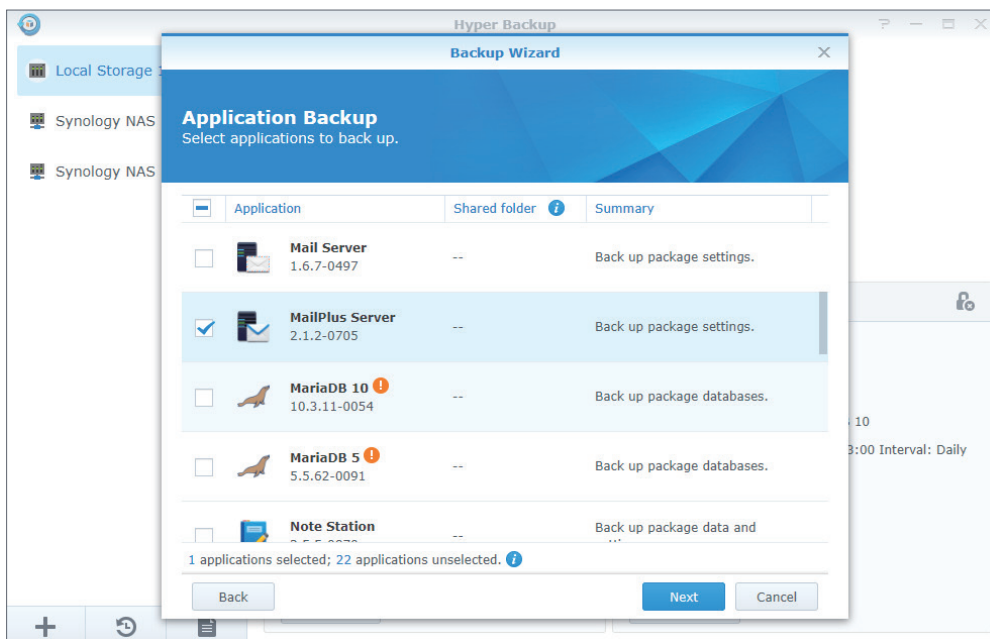
Fewer modifications occur in MailPlus Server's system settings; therefore, you can use **Hyper Backup** to run scheduled backup tasks. However, mailboxes and email messages in the mail system are constantly changing and may require real-time backup. Therefore, it is recommended that you use **Shared Folder Sync** to back up mailboxes and email messages and to prevent data loss when only scheduled backup is performed.

System configuration backup

Back up mail system configuration to a MailPlus compatible Synology NAS using Hyper Backup.

1. Launch **Hyper Backup** on the source Synology NAS.
2. Click the plus icon (+) in the lower-left corner to create a new data backup task.
3. Select a backup destination type:

- **Local folder & USB:** This option backs up data to a local Synology NAS or an external USB/SD storage device.
 - **Remote NAS device:** Hyper Backup Vault needs to be installed and launched on the remote destination in advance.
- Specify task settings. For more information on how to create backup tasks, please refer to [this help article](#).
 - Select **MailPlus Server** when the system asks you to select an application to back up.



- After backup task settings are complete, the system will be ready to back up the following MailPlus Server settings (on the left panel of the MailPlus Server interface):

- Domain
- Mail Delivery
- Service
- Security
- Auditing
- License
- Account

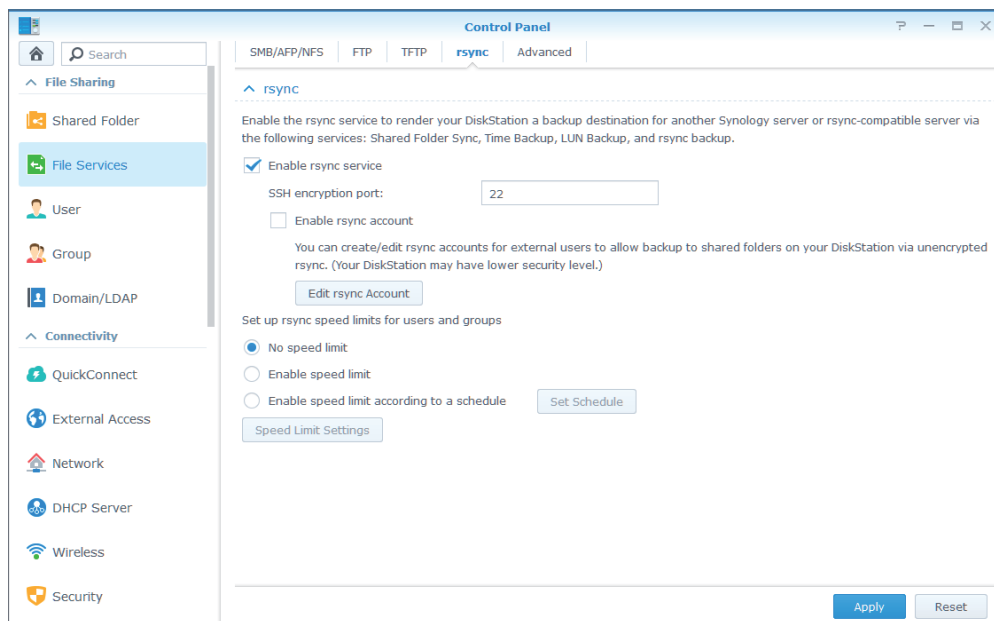
Mailbox and email backup

Please refer to the following sections to back up the entire mailbox and email messages to a MailPlus compatible Synology NAS through sync tasks:

Enable shared folder sync

You need to enable **Shared Folder Sync** on the destination Synology NAS.

1. Sign in to DSM.
2. Go to **Control Panel > File Services > rsync**.
3. Tick the **Enable rsync service** checkbox to enable **Shared Folder Sync**.



4. Click **Apply**.

Create a sync task

Sign in to the source Synology NAS and refer to the following steps to create a sync task:

1. Go to **Control Panel > Shared Folder Sync** and click the **Task List** button.
2. Click the **Create** button in the **Task List** window.
3. Enter a task name in the **Task Name** field.
4. Select a shared folder to sync.
5. Specify destination Synology NAS details and the following sync settings:
 - **Customize SSH encryption port for encrypted shared folder sync:** Uses your desired encryption port for SSH transfer encryption.
 - **Enable SSH transfer encryption:** Encrypts data during transfer. This option provides better security, while non-encrypted transfer has better performance.

- **Enable transfer compression:** Compresses data during transfer. This option reduces bandwidth usage but increases the CPU workload.
 - **Enable block-level synchronization:** Syncs only modified portions instead of an entire file. This option reduces bandwidth usage but increases the CPU workload.
6. When prompted, you can select any of the following options to decide when to sync from the source to the destination:
- **Run sync on modification:** Syncs immediately once any changes occur to the source shared folder.
 - **Run sync manually:** Syncs from the source shared folder only when you click the button.
 - **Advanced schedule:** Syncs based on the schedule you set. Click the **Schedule Plan** button to specify when to run sync tasks.
7. Click **Apply**. Now you can see the sync task on the task list. The system will automatically run tasks according to the specified schedule.

Manage sync tasks

Sign in to the source Synology NAS and refer to the following steps to manage sync tasks:

1. Go to **Control Panel > Shared Folder Sync** and click the **Task List** button.
2. Select a task in the **Task List** window and do the following:
 - Click the **Edit** button to edit tasks.
 - Click the **Delete** button to delete tasks.
 - If a sync task is not in progress, please click the **Sync Now** button to perform the task right away.
 - If a sync task is in progress, please click the **Cancel** button to stop the ongoing task.
 - When running sync tasks for the first time, **Shared Folder Sync** will run **Full Sync**. After this first sync task is complete, only modified parts will be synced. You can click **Full Sync** to manually sync all data again.

Note:

- If the schedule for a sync task is set as **Run sync on modification**, clicking **Cancel** would stop the ongoing sync task. However, if any changes are made to any shared folders included in the sync task, Shared Folder Sync would resume the task.
- Please do not use Synology Drive, Cloud Station Server, and Cloud Sync to run backup since its two-way sync feature may corrupt data.
- If the **MailPlus** shared folder already exists in the destination, the folder will be renamed as **MailPlus_1** after the backup is complete.
- If you would like to use data from **MailPlus_1**, please manually move data to the **MailPlus** shared folder.
- To prevent account errors, please connect the destination to the same directory server as the one used for the source (e.g., LDAP server or Windows Active Directory domain).

Restore system configuration, mailbox, and email

The system configuration, mailboxes, and emails are stored in the local shared folder on the destination Synology NAS. Please refer to the following steps to restore system configuration, mailboxes, and emails:

1. Launch **Hyper Backup**.
2. Restore the backed-up configuration from the local shared folder. For more information, please refer to [this help article](#).
3. After the restoration, the current MailPlus Server configuration will be overwritten.
4. The backed-up mailboxes and emails do not require restoration. They can be used immediately.

Note:

- Currently, the backup and restore feature is compatible with MailPlus Server 1.0-164 (and above) running on DSM 6.0 (and above).

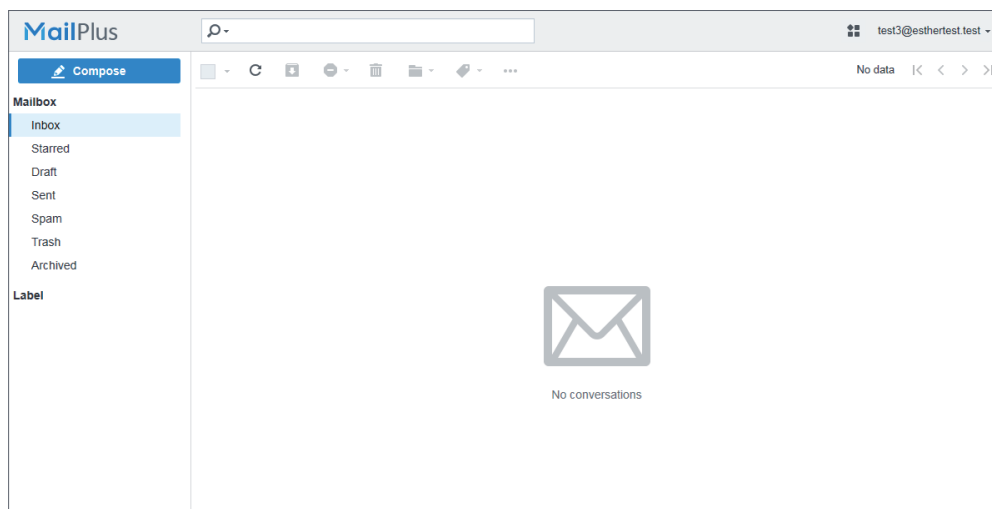
MailPlus provides client users with an easy-to-use webmail service for viewing, managing, and sending emails. For detailed information on the MailPlus setup, please refer to the [Set up MailPlus Client](#) section.

This chapter will guide you through MailPlus configuration and interface navigation. For detailed instructions, please refer to [the help articles](#).

Chapter 12: MailPlus Navigation

Basic Operations

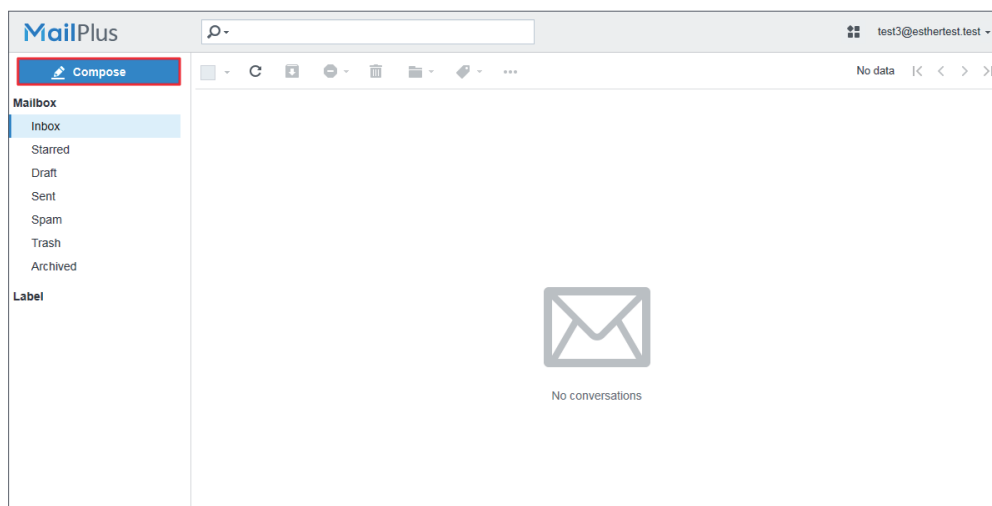
By default, you will see your **Mailbox** after you sign in.



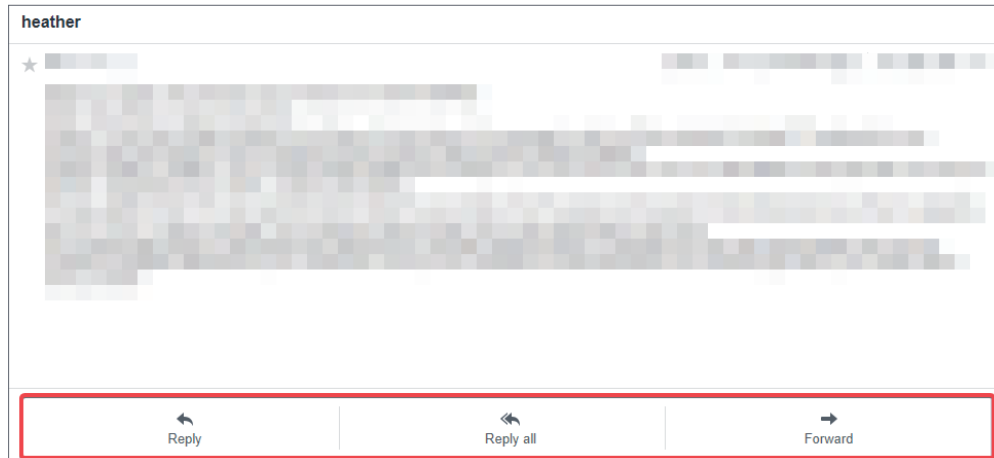
Access and manage emails

You can perform the followings actions in **Mailbox**:

- **Compose an email:** Click the **Compose** button in the upper-left corner to start drafting an email. MailPlus will auto-save email drafts. You can close the **Compose** window at any time and open it again from the **Draft** box to resume writing.



- **Reply to an email:** There are three ways to reply to an email in MailPlus:
 - **Reply:** Click **Reply** to reply to the sender.
 - **Reply all:** Click **Reply all** to reply to all recipients (including CC recipients) at once.
 - **Forward:** Click **Forward** if you want to send an email to someone other than original recipients.



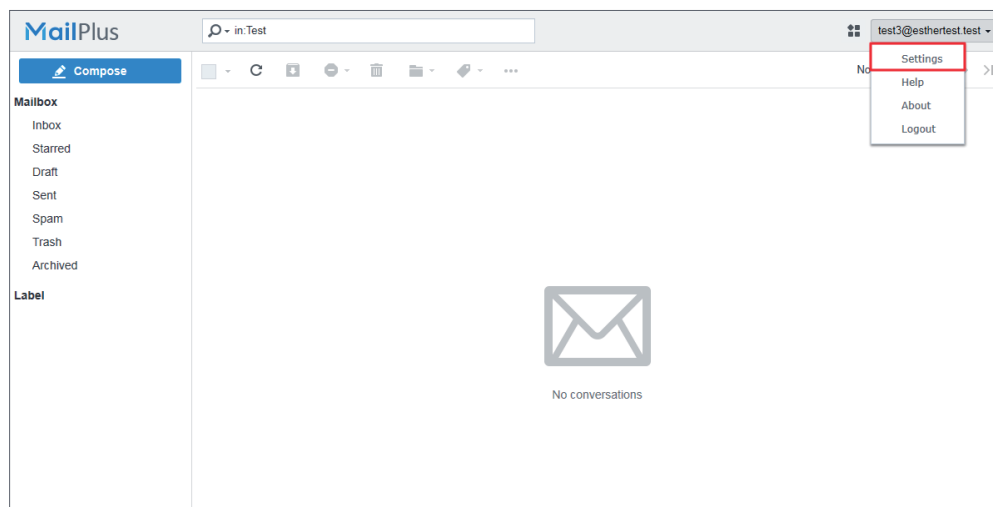
- **Organize emails by mailbox:** You can create multiple mailboxes according to your needs. Hover the cursor over **Mailbox** in the upper-left corner and you will see a plus icon (+) appearing next to it. Click the plus icon (+) to add a new mailbox.
- **Manage emails by label:** You can customize labels to categorize your emails. Hover the cursor over **Label** on the left panel and you will see a plus icon (+) appearing next to it. Click the plus icon (+) to add a new label. Enter a name and select a label color for easy identification.

Advanced Settings

MailPlus allows client users to customize their webmail layout, auto-reply/forward messages, mailbox settings, and even protocols (e.g., SMTP and OpenPGP) used for mail delivery. General settings applied to all users can be managed by MailPlus administrators in Synology MailPlus Server. **Contacts** and its related settings can be found in the App Launcher.

In this chapter, we will guide you through the configuration of **SMTP**, **OpenPGP**, and **Blacklist/Whitelist**. If you need detailed instructions on other settings, please refer to [this help article](#).

Click your account name in the upper-right corner and click **Settings** from the drop-down menu to start configuring your MailPlus.

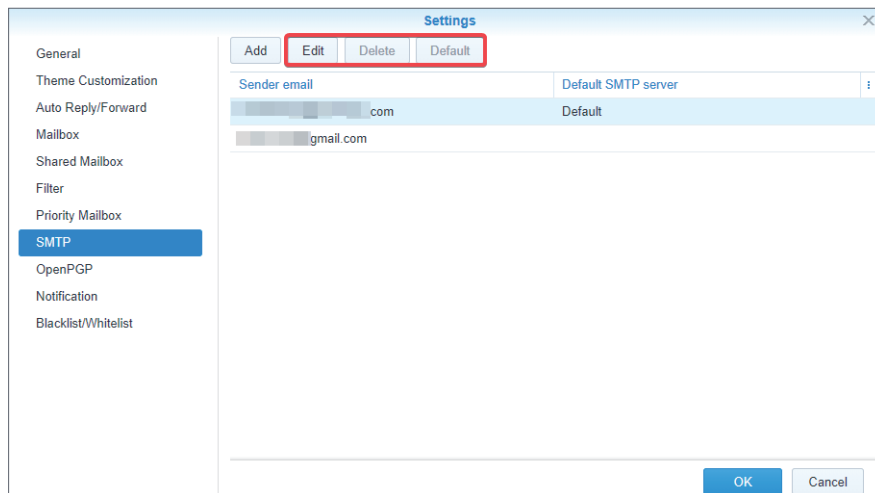


Add additional SMTP servers

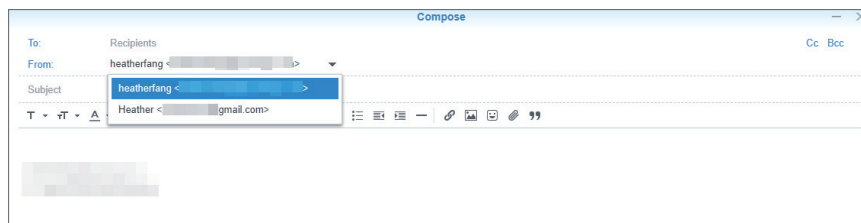
MailPlus supports multiple SMTP servers used for mail delivery. With no extra SMTP servers added, MailPlus Server will be automatically set as the default SMTP server to deliver all emails. No settings can be edited except for the **Sender name**.

Users may add other SMTP servers to send emails in MailPlus. For example, you can add Google's SMTP server to send emails via your Google account in MailPlus. Please follow the steps below to add an SMTP server:

1. Go to **Settings > SMTP**.
2. Fill in the following information:
 - **SMTP server:** Find the SMTP server from the help articles or tutorials of your mail service provider.
 - **SMTP port:** The port number will be automatically updated to the required value for SMTP connections over SSL/TLS. By default, port 465 is for SMTP connections over SSL, and port 587 is for SMTP connections over TLS. If you tick none of the SSL and TLS checkboxes, the standard port used for SMTP connections is 25.
 - **Authentication required:** Tick the checkbox if your SMTP server requires authentication.
 - **Username:** Enter your email address.



- When composing an email, you can switch between SMTP servers in the **From:** field.

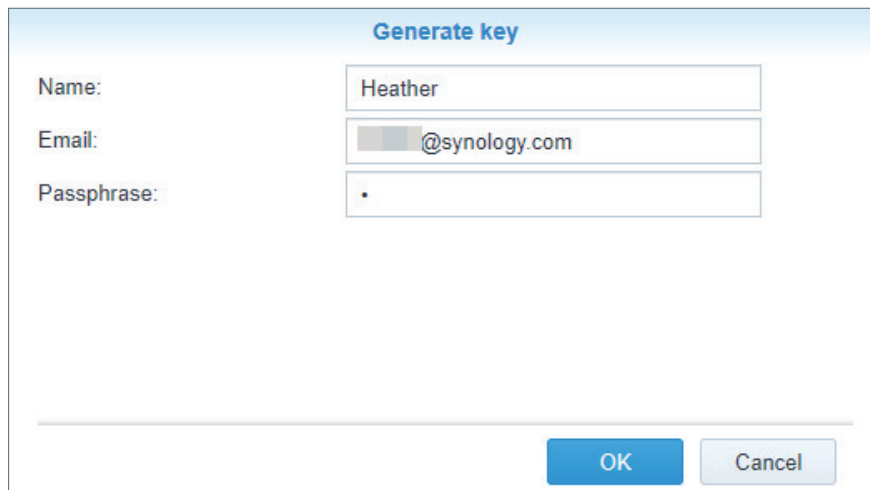


Encrypt emails via OpenPGP

OpenPGP (Pretty Good Privacy) is a key-based encryption technology used for email encryption. OpenPGP encrypts emails so that only intended recipients can access email content. In this way, sensitive email communication and transmitted data can be well-protected from privacy attacks.

Generate OpenPGP keys

1. Tick **Enable OpenPGP** and click the **Key Management** button.
2. Click **Generate** to generate a new OpenPGP key pair.
 - **Name:** Enter a name you like.
 - **Email:** Enter your MailPlus account.
 - **Passphrase:** Enter a passphrase that is used to encrypt and decrypt the private key.



Generate key

Name:

Email:

Passphrase:

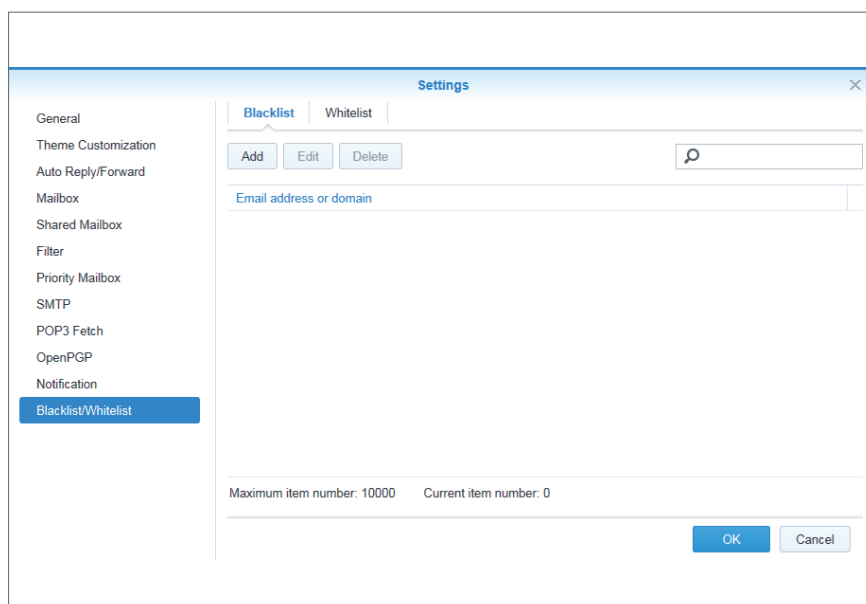
3. Click **OK** to generate a pair of public and private keys.

Manage OpenPGP keys

- **Public key:** Click the **Export** button to export the public key and give it to senders who should encrypt emails for you.
- **Private key:** Keep the private key to yourself because it is used to decrypt emails sent to you.
- If you need to send others encrypted emails, please click the **Import** button to import their public keys from files or text input.

Manage Blacklist/Whitelist

You can create a personal blacklist and whitelist to block or allow specific email addresses/ domains in the **Blacklist/Whitelist** page. You can block email addresses or domains that are persistently sending spam by adding them to the **Blacklist**. Similarly, if you notice legitimate emails being blocked, you can add the email addresses or domain names to the **Whitelist**.



Settings [X]

General | **Blacklist** | Whitelist

Email address or domain

Maximum item number: 10000 Current item number: 0

Add Email Address or Domain Name

1. Click on **Add** to add a new entry to your blacklist/whitelist.
2. Specify the email address or domain name and click **OK** to save the settings.
3. Now you should see the newly added email address or domain name appear on the list.

Delete Existing Email Address or Domain Name

1. Click on the email address or domain name you want to remove, then click **Delete**.
2. Click **Yes** to confirm or **No** to cancel.

Edit Existing Email Address or Domain Name

1. Click on the email address or domain name you want to edit, then click **Edit**.
2. Make the changes you want, then click **Ok**.
3. The email address or domain name is now removed from your list.



**SYNOLOGY
INC.**

9F, No. 1, Yuandong Rd.
Banqiao Dist., New Taipei City 220545
Taiwan
Tel.: +886 2 2955 1814

**SYNOLOGY
AMERICA CORP.**

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

**SYNOLOGY
UK LTD.**

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

**SYNOLOGY
FRANCE**

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

**SYNOLOGY
GMBH**

Grafenberger Allee 295
40237 Düsseldorf
Deutschland
Tel.: +49 211 9666 9666

**SYNOLOGY
SHANGHAI**

200070, Room 201,
No. 511 Tianmu W. Rd.,
Jingan Dist., Shanghai,
China

**SYNOLOGY
JAPAN CO., LTD.**

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

Synology®



synology.com

Synology may make changes to specifications and product descriptions at any time, without notice. Copyright © 2020 Synology Inc. All rights reserved. ® Synology and other names of Synology Products are proprietary marks or registered trademarks of Synology Inc. Other products and company names mentioned herein are trademarks of their respective holders.